Algebra kvaterniona i primjene

Barbarić, Brigita

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Brigita Barbarić

ALGEBRA KVATERNIONA I PRIMJENE

Diplomski rad

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

Zagreb, travanj 2021.

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

1. ____________________________, predsjednik
2. ____________________________, član
3. ____________________________, član

Povjerenstvo je rad ocijenilo ocjenom _______________.

Potpisi članova povjerenstva:

1. ____________________________
2. ____________________________
3. ____________________________

Zahvaljujem se mentorici dr. sc. Sonji Žunar na strpljenju, pomoći, savjetima, vodstvu i uloženom vremenu pri izradi ovog rada.
Veliko hvala prijateljicama i kolegicama na divnih pet godina i puno nezaboravnih trenutaka.
Naposljetku, najveću zahvalu dugujem mojoj obitelji, prvenstveno roditeljima i sestrama, na ljubavi i podršci tijekom cijelog školovanja. Hvala i ostalim članovima uže i šire obitelji koji su me pratili kroz studij, a posebno mom striki Dragi.

Sadržaj

Uvod

Pojam kvaterniona vezan je za irskog matematičara i fizičara Williama Rowana Hamiltona. On je pokušao pronaći analogiju između trodimenzionalnog realnog vektorskog prostora i nekog sustava brojeva po uzoru na analogiju dvodimenzionalnog realnog vektorskog prostora i kompleksnih brojeva. Godinama mu je problem predstavljala definicija množenja u trodimenzionalnom realnom vektorskom prostoru, što je zaustavljalo razvoj Hamiltonove teorije. Rješenje je uspio pronaći tek u četverodimenzionalnom prostoru kvaterniona. Godine 1843. hodajući ulicama Dublina sa svojom suprugom, pronašao je rješenje za množenje kvaterniona te je nožićem urezao čuvenu formulu $i^2 = j^2 = k^2 = ijk = -1$ u kamen mosta kojim je prolazio. Ova formula je obilježila cjelokupan Hamiltonov budući rad, stoga je ostatak života posvetio proučavanju kvaterniona.

Riječ kvaternion dolazi od latinske riječi *quaternio* što znači četvorka, cjelina od četiri dijela. Kvaternion je broj q oblika $q = a + bi + cj + dk$, gdje su $a, b, c, d \in \mathbb{R}$, dok $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ označava prostor kvaterniona. S operacijama zbrajanja, množenja i množenja skalarom $\mathbb{H}$ čini realnu asocijativnu algebru s dijeljenjem. Tako su $\mathbb{R}$, $\mathbb{C}$ i $\mathbb{H}$ do na izomorfizam jedine konačnodimenzionalne realne asocijativne algebre s dijeljenjem (Frobenius 1877.).

U prvom poglavlju rada iznesene su osnovne definicije i tvrdnje koje će biti korištene kroz rad i čije poznavanje je neophodno za razumijevanje rada. U drugom poglavlju detaljno je opisano polje kompleksnih brojeva i njegova algebarska struktura te je dana jedna njegova matrična realizacija, dok su u trećem poglavlju opisane osnove o kvaternionima i algebarska svojstva kvaterniona. U četvrtom poglavlju opisane su dvije primjene kvaterniona. Prva od njih je *Lagrangeov teorem o četirima kvadratima* koji kaže da se svaki prirodan broj može prikazati kao suma četiriju kvadrata. Druga primjena kvaterniona je u opisivanju prostornih rotacija. Kako bismo pomoću kvaterniona dokazali *Lagrangeov teorem o četirima kvadratima*, najprije definiramo *Hurwitzove cijele brojeve* i dokazujemo niz pomoćnih lema, propozicija i teorema, primjerice teorem o dijeljenju s ostatkom u prstenu Hurwitzovih cijelih brojeva. Na samom kraju rada uvodi se vektorski zapis kvaterniona pomoću kojih se opisuje rotacija vektora u prostoru.

Poglavlje 1

Osnovni pojmovi

Definicija 1.0.1. *Neka je S neprazan skup. Preslikavanje*

$$\theta : S \times S \to S$$

naziva se ***binarna operacija****. Binarna operacija svakom uređenom paru $(x, y) \in S \times S$ pridružuje element $z = \theta(x, y) \in S$.*

Definicija 1.0.2. *Neka je $S \neq \emptyset$ i $\cdot$ binarna operacija na $S \times S$. Uređeni par $(S, \cdot)$ je* ***grupa*** *ako vrijede sljedeća svojstva:*

1. *$(xy)z = x(yz)$ za sve $x, y, z \in S$, (asocijativnost)*
2. *Postoji $e \in S$ takav da je $ex = xe = x$ za sve $x \in S$, (neutralni element)*
3. *Za svaki $x \in S$ postoji $y \in S$ takav da je $xy = yx = e$. (inverzni element)*

   Ako vrijedi i svojstvo

4. *$xy = yx$ za sve $x, y \in S$, (komutativnost)*

onda je $(S, \cdot)$ ***komutativna*** *ili* ***Abelova grupa****.*

Definicija 1.0.3. *Neka je S neprazan skup na kojem su definirane dvije binarne operacije $+$ i $\cdot$. Kažemo da je uređena trojka $(S, +, \cdot)$* ***prsten*** *ako vrijedi*

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

3. *svojstvo distributivnosti operacije $\cdot$ s obzirom na operaciju $+$:*

$$x(y+z) = xy + xz, (x+y)z = xz + yz,$$

za sve $x, y, z \in S$.

Neutralni element grupe $(S, +)$ naziva se nula i označava s 0.
*Ukoliko postoji neutralni element strukture $(S, \cdot)$ onda se on naziva jedinica i označava s 1, a $(S, +, \cdot)$ se tada naziva **prsten s jedinicom**. Ako dodatno svaki $a \in S \setminus \{0\}$ ima (obostrani) multiplikativni inverz, tada se $(S, +, \cdot)$ naziva **prsten s dijeljenjem**.*
*Ukoliko je operacija $\cdot$ komutativna, onda govorimo o **komutativnom prstenu**.*

Definicija 1.0.4. *Komutativni prsten s jedinicom $(S, +, \cdot)$ u kojem je svaki element $x \in \mathbb{R}\setminus\{0\}$ invertibilan naziva se **polje**.*

Ekvivalentno, polje se može definirati na sljedeći način. Uređena trojka $(S, +, \cdot)$ je polje ako zadovoljava sljedeća svojstva:

1. *$(S, +)$ je Abelova grupa,*

2. *$(S\setminus\{0\}, \cdot)$ je Abelova grupa,*

3. *svojstvo distributivnosti operacije $\cdot$ s obzirom na operaciju $+$.*

Definicija 1.0.5. *Neka je $(V, +)$ Abelova grupa, zatim $\mathbb{K}$ polje. Ako postoji preslikavanje $\cdot : \mathbb{K} \times V \to V$ koje zadovoljava sljedeća svojstva:*

1. *$\alpha \cdot (\beta \cdot a) = (\alpha\beta) \cdot a$, za sve $\alpha, \beta \in \mathbb{K}, a \in V$,*

2. *$(\alpha + \beta) \cdot a = \alpha \cdot a + \beta \cdot a$, za sve $\alpha, \beta \in \mathbb{K}, a \in V$,*

3. *$\alpha \cdot (a + b) = \alpha \cdot a + \alpha \cdot b$, za sve $\alpha \in \mathbb{K}, a, b \in V$*

4. *$1 \cdot a = a$,za sve $a \in V$,*

*tada se uređena trojka $(V, +, \cdot)$ naziva **vektorski** ili **linearni prostor nad poljem** $\mathbb{K}$.*
*Ako je $\mathbb{K} = \mathbb{R}$, onda govorimo o **realnom vektorskom prostoru**, a ako je $\mathbb{K} = \mathbb{C}$, onda o **kompleksnom vektorskom prostoru**.*
*Elemente skupa V zovemo **vektorima**, a elemente polja $\mathbb{K}$ **skalarima.** Operaciju $\cdot$ nazivamo **množenje vektora skalarom** i umjesto $\alpha \cdot a$ često pišemo αa.*

Definicija 1.0.6. ***Algebra** nad poljem $\mathbb{K}$ ili **$\mathbb{K}$-algebra** je algebarska struktura $(V, +, \cdot, *)$, gdje su $+$ i $\cdot$ binarne operacije, a $*$ vanjska $\mathbb{K}$-operacija u skupu V, koja zadovoljava:*

1. *$(V, +, \cdot)$ je prsten,*

2. $(V, +, *)$ *je vektorski prostor nad poljem* $\mathbb{K}$,

3. $(\alpha * u) \cdot (\beta * v) = (\alpha \cdot \beta) * (u \cdot v)$, *za sve* $\alpha, \beta \in \mathbb{K}, u, v \in V$.

Binarne operacije $+$ *i* $\cdot$ *nazivamo zbrajanje i množenje, a vanjsku operaciju* $*$ *množenje skalarima.*

Definicija 1.0.7. *Algebra nad poljem* $\mathbb{K}$ *je* ***komutativna*** *ako je operacija množenja komutativna.*

Definicija 1.0.8. *Algebra nad poljem* $\mathbb{K}$ *je* ***algebra s dijeljenjem*** *ako je ona prsten s dijeljenjem.*

Vektorski prostori

Neka je V vektorski prostor nad poljem $\mathbb{K}$, gdje je $\mathbb{K}$ polje $\mathbb{R}$ ili $\mathbb{C}$. Tada definiramo:

Definicija 1.0.9. *Neka je* $k \in \mathbb{N}$. *Za* $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ *i* $a_1, \ldots, a_k \in V$ *vektor oblika*

$$\alpha_1 a_1 + \ldots \alpha_k a_k$$

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

Definicija 1.0.10. *Neka je* $S \subseteq V$. *Skup svih linearnih kombinacija vektora iz* S *naziva se* ***linearna ljuska*** *ili* ***linearni omotač skupa*** S *i označava* $[S]$. *Dakle,*

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

Definicija 1.0.11. *Neka je* V *vektorski prostor nad poljem* $\mathbb{K}$ *i* $G \subseteq V$. *Ako je*

$$V = [G],$$

odnosno ako se svaki vektor iz V *može prikazati kao linearna kombinacija (konačno mnogo) vektora iz* G, *onda kažemo da je* G ***sustav izvodnica*** *ili* ***generatora*** *za prostor* V, *odnosno skup izvodnica ili generatora za* V. *Još se može reći da skup* G ***razapinje*** *ili* ***generira*** *prostor* V.

Primjer 1.0.12. *Ako* $V = [G]$, *onda za svaki* $x \in V$ *postoje vektori* $a_1, \ldots, a_k \in G$ *i skalari* $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ *takvi da se* x *prikazuje kao*

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

Definicija 1.0.13. *Neka je V vektorski prostor nad poljem $\mathbb{K}$ i neka je $S = \{a_1, \ldots, a_k\}$ njegov podskup. Kažemo da je S* ***linearno nezavisan*** *skup vektora ako se nulvektor 0_V može na jedinstven način prikazati pomoću vektora iz S, to jest ako iz*

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots \alpha_k a_k = 0_V \tag{1.1}$$

slijedi da je $\alpha_1 = \alpha_2 = \ldots \alpha_k = 0$. U suprotnom, to jest ako postoji izbor skalara $\alpha_1, \ldots \alpha_k$ takav da je bar jedan skalar $\alpha_i \neq 0$ i da vrijedi (1.1), *onda kažemo da je skup S* ***linearno zavisan****.*

Definicija 1.0.14. *Podskup B vektorskog prostora V je* ***baza*** *prostora V ako je B sustav izvodnica za V i linearno nezavisan skup u V.*

Definicija 1.0.15. *Kažemo da je vektorski prostor V* ***konačnogeneriran*** *ako postoji konačan skup izvodnica za V.*

Teorem 1.0.16. *Neka je V konačnogeneriran i netrivijalan vektorski prostor. Ako je $G = \{a_1, \ldots, a_n\} \subset V$ sustav izvodnica za V, onda G sadrži podskup koji je baza za V.*

Korolar 1.0.17. *Svaki netrivijalan konačnogeneriran vektorski prostor V ima konačnu bazu.*

Definicija 1.0.18. *Vektorski prostor koji ima konačnu bazu naziva se* ***konačnodimenzionalan****. U suprotnom je* ***beskonačnodimenzionalan****. Trivijalan prostor $V = \{0_V\}$ je konačnodimenzionalan.*

Definicija 1.0.19. *Neka je V netrivijalan konačnodimenzionalan vektorski prostor. Broj elemenata bilo koje baze za V zove se* ***dimenzija*** *vektorskog prostora V i označava sa* $\dim V$. *Ako je* $\dim V = n$, *kažemo da je V n-dimenzionalan vektorski prostor. Dodatno, definiramo* $\dim\{0_V\} = 0$.

Definicija 1.0.20. *Neka su V i W vektorski prostori nad istim poljem $\mathbb{K}$. Preslikavanje*

$$A : V \to W$$

zove se ***linearni operator*** *ako vrijede svojstva*

1. $A(a + b) = A(a) + A(b)$, *(aditivnost)*

2. $A(\alpha a) = \alpha A(a)$, *(homogenost)*

za sve $a, b \in V$, $\alpha \in \mathbb{K}$. Skup svih linearnih operatora s $V \to W$ označavat ćemo s $\mathcal{L}(V, W)$.

Definicija 1.0.21. *Bijektivan linearan operator $A : V \to W$ zovemo* ***izomorfizmom*** *vektorskih prostora V i W.*

Definicija 1.0.22. *Vektorski prostori V i W su* ***izomorfni*** *ako postoji izomorfizam $A : V \to W$. Pišemo $V \simeq W$.*

Teorem 1.0.23. *Konačnodimenzionalni vektorski prostori su izomorfni ako i samo ako su im dimenzije jednake.*

Korolar 1.0.24. *Svaki vektorski prostor nad poljem $\mathbb{K}$ dimenzije n je izomorfan prostoru $\mathbb{K}^n$.*

Definicija 1.0.25. *Neka je V vektorski prostor nad poljem $\mathbb{K}$. Preslikavanje $s : V \times V \to \mathbb{K}$ koje svakom uređenom paru vektora pridružuje skalar $s(a,b) = \langle a|b\rangle \in \mathbb{K}$ naziva se* ***skalarno množenje*** *na prostoru V ako su ispunjena sljedeća svojstva:*

1. $\langle a|a\rangle \geq 0$, *za sve $a \in V$, pri čemu je $\langle a|a\rangle = 0$ ako i samo ako je $a = 0_V$;*
2. $\langle a|b\rangle = \overline{\langle b|a\rangle}$, *za sve $a, b \in V$;*
3. $\langle \lambda a|b\rangle = \lambda\langle a|b\rangle$, *za sve $a, b \in V, \lambda \in \mathbb{K}$;*
4. $\langle a + b|c\rangle = \langle a|c\rangle + \langle b|c\rangle$, *za sve $a, b, c \in V$.*

Skalar $\langle a|b\rangle$ se zove ***skalarni produkt*** *ili* ***umnožak vektora*** *a i b. Uređeni par (V, s) (ili $(V, \langle\cdot|\cdot\rangle)$) nazivamo* ***unitarni prostor nad poljem*** *$\mathbb{K}$.*

Definicija 1.0.26. *Skup vektora $S = \{a_1, \ldots, a_k\}$ unitarnog prostora V je* ***ortonormiran*** *ako za sve $i, j \in \{1, \ldots, k\}$ vrijedi*

$$\langle a_i|a_j\rangle = \delta_{i,j},$$

gdje je

$$\delta_{i,j} = \begin{cases} 1, & \text{ako je } i = j \\ 0, & \text{ako je } i \neq j. \end{cases}$$

Specijalno, ako je S baza prostora V i uz to ortonormiran skup, onda S nazivamo ***ortonormiranom bazom****.*

Definicija 1.0.27. *Neka su V i W unitarni prostori takvi da je $\dim V = \dim W$. Kažemo da je $A \in \mathcal{L}(V, W)$* ***unitaran operator*** *ako vrijedi*

$$\langle Ax|Ay\rangle = \langle x|y\rangle \qquad \forall x, y \in V.$$

Skalarni i vektorski produkt u prostoru V^3

Označimo sa V^3 skup vektora u prostoru, tj. klasa ekvivalencije usmjerenih dužina u prostoru po sljedećoj relaciji ekvivalencije:

$$\overrightarrow{AB} \sim \overrightarrow{CD} \Leftrightarrow \text{dužine } \overline{AD} \text{ i } \overline{BC} \text{ imaju zajedničko polovište.}$$

Elemente iz V^3 kratko ćemo zvati vektorima. Uz standardno definirane operacije zbrajanja vektora i množenja vektora skalarom (vidi npr. [6]), V^3 je realan vektorski prostor.

Definicija 1.0.28. ***Skalarno množenje*** *vektora je operacija* $\cdot : V^3 \times V^3 \to \mathbb{R}$ *koja vektorima* $\vec{a}, \vec{b}$ *različitim od nulvektora pridružuje skalar*

$$\vec{a} \cdot \vec{b} = |\vec{a}|\, |\vec{b}| \cos \angle \left(\vec{a}, \vec{b}\right).$$

Ako je neki od vektora $\vec{a}, \vec{b}$ *nulvektor, tada definiramo* $\vec{a} \cdot \vec{b} = 0$.
Vrijednost $\vec{a} \cdot \vec{b} \in \mathbb{R}$ *nazivamo* ***skalarnim umnoškom*** *ili* ***skalarnim produktom*** *vektora* $\vec{a}$ *i* $\vec{b}$.

Teorem 1.0.29. *Za sve* $\vec{a}, \vec{b} \in V^3$ *i* $\lambda \in \mathbb{R}$ *vrijedi:*

1. $\vec{a} \cdot \vec{a} \geq 0$,
2. $\vec{a} \cdot \vec{a} = 0$ *ako i samo ako je* $\vec{a} = \vec{0}$,
3. $\vec{a} \cdot \vec{b} = \vec{b} \cdot \vec{a}$, *(komutativnost)*
4. $(\lambda \vec{a}) \cdot \vec{b} = \lambda \left(\vec{a} \cdot \vec{b}\right)$, *(kvaziasocijativnost)*
5. $\vec{a} \cdot \left(\vec{b} + \vec{c}\right) = \vec{a} \cdot \vec{b} + \vec{a} \cdot \vec{c}$, *(distributivnost prema zbrajanju).*

Dakle, $(V^3, \cdot\,)$ je realni unitarni prostor.

Propozicija 1.0.30. *Neka su* $\vec{a} \neq \vec{0}, \vec{b} \neq \vec{0}$ *vektori u* V^3. *Vektori* $\vec{a}, \vec{b}$ *su okomiti ako i samo ako je* $\vec{a} \cdot \vec{b} = 0$.

Propozicija 1.0.31. *Neka je* $\left\{\vec{i}, \vec{j}, \vec{k}\right\}$ *ortonormirana baza vektorskog prostora* V^3 *i neka su* $\vec{a} = (\alpha_1, \alpha_2, \alpha_3)\,, \vec{b} = (\beta_1, \beta_2, \beta_3)$ *koordinatni prikazi vektora* $\vec{a}, \vec{b}$ *u toj bazi. Tada je*

$$\vec{a} \cdot \vec{b} = \alpha_1 \beta_1 + \alpha_2 \beta_2 + \alpha_3 \beta_3 = \sum_{i=1}^{3} \alpha_i\, \beta_i.$$

Definicija 1.0.32. ***Modul*** *vektora* $a \in V^3$ *je broj*

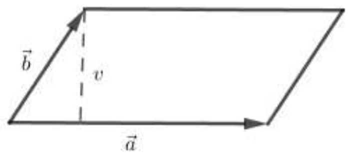
$$|\vec{a}| = \sqrt{\vec{a} \cdot \vec{a}}.$$

Definicija 1.0.33. ***Vektorsko množenje*** *je operacija* $\times : V^3 \times V^3 \to V^3$ *koja paru vektora* $\left(\vec{a}, \vec{b}\right)$ *pridružuje vektor* $\vec{c} = \vec{a} \times \vec{b}$ *definiran na sljedeći način:*

1. *ako su vektori* $\vec{a}, \vec{b}$ *kolinearni, (tj. istog smjera) tada je* $\vec{c} = \vec{0}$*;*
2. *ako su vektori* $\vec{a}, \vec{b}$ *nekolinearni, tada je*
   (a) $|\vec{c}| = |\vec{a}|\, |\vec{b}| \sin \angle \left(\vec{a}, \vec{b}\right)$
   (b) *smjer od* $\vec{c}$ *je smjer okomit na smjer od* $\vec{a}$ *i na smjer od* $\vec{b}$*,*
   (c) *orijentacija od* $\vec{c}$ *je takva da je uređena trojka* $\left\{\vec{a}, \vec{b}, \vec{c}\right\}$ *desna baza od* V^3*.*

Sliku $\vec{a} \times \vec{b}$ *vektora* $\vec{a}, \vec{b}$ *nazivamo* ***vektorskim umnoškom*** *ili* ***vektorskim produktom*** *vektora* $\vec{a}, \vec{b}$*.*

Modul vektorskog produkta nekolinearnih vektora ima i geometrijsku interpretaciju: skalar $|\vec{a} \times \vec{b}|$ jednak je površini paralelograma određenog vektorima $\vec{a}, \vec{b}$.



Slika 1.1: Geometrijska interpretacija vektorskog množenja

Površina paralelograma dana je s

$$P = |\vec{a}|\, v = |\vec{a}|\, |\vec{b}| \sin \angle \left(\vec{a}, \vec{b}\right) = |\vec{a} \times \vec{b}|.$$

Propozicija 1.0.34. *Vrijedi* $\vec{a} \times \vec{b} = \vec{0}$ *ako i samo ako su vektori* $\vec{a}, \vec{b}$ *kolinearni.*

Teorem 1.0.35. *Za svaki* $\vec{a}, \vec{b}, \vec{c} \in V^3, \lambda \in \mathbb{R}$ *vrijedi:*

1. $\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}$*, (antikomutativnost)*
2. $(\lambda \vec{a}) = \lambda \left(\vec{a} \times \vec{b}\right)$*, (kvaziasocijativnost)*
3. $\vec{a} \times \left(\vec{b} + \vec{c}\right) = \vec{a} \times \vec{b} + \vec{a} \times \vec{c}$ *(distributivnost prema zbrajanju).*

Propozicija 1.0.36. *Neka je* $\left\{\vec{i}, \vec{j}, \vec{k}\right\}$ *desna ortonormirana baza vektorskog prostora* V^3 *i neka su* $\vec{a} = (\alpha_1, \alpha_2, \alpha_3)\,, \vec{b} = (\beta_1, \beta_2, \beta_3)$ *koordinatni prikazi vektora* $\vec{a}, \vec{b}$ *u toj bazi. Tada vrijedi*

$$\vec{a} \times \vec{b} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{vmatrix} = (\alpha_2\beta_3 - \alpha_3\beta_2)\vec{i} - (\alpha_1\beta_3 - \alpha_3\beta_1)\vec{j} + (\alpha_1\beta_2 - \alpha_2\beta_1)\vec{k}.$$

Poglavlje 2

Polje kompleksnih brojeva

Definicija

Definicija 2.0.1. *Skup kompleksnih brojeva je skup svih brojeva oblika $z = x + yi$, gdje su $x, y \in \mathbb{R}$. Realni broj $x = \operatorname{Re} z$ zove se realni dio kompleksnog broja z, a realni broj $y = \operatorname{Im} z$ zove se imaginarni dio kompleksnog broja z, dok i označava imaginarnu jedinicu.*
Skup kompleksnih brojeva označavamo s $\mathbb{C}$.

Neka su $(x+yi)$ i $(u+vi)$ dva kompleksna broja. Zbrajanje i množenje dano je sljedećim pravilima:

$$(x + yi) + (u + vi) = (x + u) + (y + v)i \tag{2.1}$$

$$(x + yi) \cdot (u + vi) = (xu - yv) + (xv + yu)i. \tag{2.2}$$

U prethodnoj definiciji kompleksnog broja nije definirano što je to imaginarna jedinica i. Sir William Hamilton je 1833. godine definirao skup $\mathbb{C}$ na način na koji je izbjegao definiranje imaginarne jedinice i. Izraz $x + yi$ proglasio je uređenim parom (x, y). Odnosno, $\mathbb{C}$ je definirao na sljedeći način:

$$\mathbb{C} := \{z = (x, y); x, y \in \mathbb{R}\}.$$

Dakle, njegovi su elementi uređeni parovi realnih brojeva, a kao skup, $\mathbb{C}$ je isto što i $\mathbb{R}^2$.

Zbrajanje i množenje kompleksnih brojeva

Operacije zbrajanja i množenja definirane su po koordinatama, kao i u $\mathbb{R}^2$:

$$(x, y) + (u, v) = (x + u, y + v).$$

Neutralni element zbrajanja je $(0, 0)$.
Novost nastupa uvođenjem množenja kompleksnih brojeva $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ formulom

$$(x, y) \cdot (u, v) = (xu - yv, xv + yu).$$

Ovako definirano množenje je asocijativno, komutativno, ima neutralan element - kompleksan broj $(1, 0)$, distributivno je prema zbrajanju i svaki kompleksan broj $z = (x, y) \in \mathbb{C}^* := \mathbb{C} \setminus \{(0, 0)\}$ ima inverz oblika

$$\frac{1}{z} = z^{-1} = \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y} \right).$$

Svojstva kompleksnih brojeva

Skup realnih brojeva $\mathbb{R}$ podskup je skupa kompleksnih brojeva $\mathbb{C}$ jer svaki $x \in \mathbb{R}$ možemo zapisati u obliku:

$$x = x + 0 \cdot i = (x, 0)$$

tj. $x = (x, 0) \in \mathbb{C}$.
Prema tome, realne brojeve identificiramo s kompleksnim brojevima kojima je imaginarni dio jednak nuli, $x \equiv (x, 0)$, odnosno možemo pisati $\mathbb{R} \equiv \{(x, 0) | x \in \mathbb{R}\}$, tj $\mathbb{R} \subset \mathbb{C}$.
Skup brojeva oblika $x \equiv (x, 0), x \in \mathbb{R}$ naziva se *realna os*.

Definicija 2.0.2. *Kompleksan broj* $(0, 1)$ *naziva se* ***imaginarna jedinica*** *i označava se s i.*

Skup brojeva oblika $yi \equiv (0, y), y \in \mathbb{R}$ naziva se *imaginarna os*.

Propozicija 2.0.3. *Svaki kompleksan broj $z = (x, y)$ se na jedinstven način može predstaviti u obliku $x + yi$. Takav zapis kompleksnog broja se naziva* ***algebarski oblik kompleksnog broja****.*

Dokaz.

$$x + yi = (x, 0) + (y, 0)(0, 1) = (x, 0) + (0, y) = (x, y).$$

□

Definicija 2.0.4. *Zrcaljenje kompleksne ravnine s obzirom na realnu os, naziva se* ***konjugiranje*** *kompleksnih brojeva. To je funkcija $z \to \bar{z}$, definirana kao $\bar{z} := (x, -y)$.*

Definicija 2.0.5. *Broj $\bar{z} = x - yi$ naziva se* ***kompleksno konjugirani broj*** *kompleksnog broja z.*

Definicija 2.0.6. ***Modul kompleksnog broja*** *$z = x + yi$ je nenegativan realan broj*

$$|z| = \sqrt{x^2 + y^2}.$$

Algebarska svojstva skupa $\mathbb{C}$

Propozicija 2.0.7. *Algebarska struktura* $(\mathbb{C}, +, \cdot)$ *je polje.*

Dokaz.

1. $(\mathbb{C}, +)$ je Abelova grupa jer je po definiciji zbrajanje zatvoreno, komutativno i asocijativno. Neutralni element za zbrajanje je $0 \in \mathbb{C}$, a svaki $z \in \mathbb{C}$ ima inverz $-z \in \mathbb{C}$.

2. $(\mathbb{C}\backslash\{0\}, \cdot)$ je Abelova grupa. Množenje je po definiciji zatvoreno, komutativno i asocijativno. Neutral za množenje je $1 \in \mathbb{C}$, a svaki nenul element ima inverz oblika $\frac{1}{z}$.

3. Dokaz distributivnosti množenja prema zbrajanju je trivijalan.

□

Definicija 2.0.8. *Restrikciju preslikavanja* $\cdot : \mathbb{C}\times\mathbb{C} \to \mathbb{C}$ *na* $\mathbb{R}\times\mathbb{C}$ *označavamo s* $*$. *Ovako definiranu vanjsku* $\mathbb{R}$*-operaciju nazivamo* ***množenje skalarima****.*

Propozicija 2.0.9. $(\mathbb{C}, +, *)$ *je vektorski prostor nad* $\mathbb{R}$.

Dokaz.

1. $(\mathbb{C}, +)$ je Abelova grupa.

2. Ostali aksiomi vektorskog prostora se dokazuju po definiciji.

□

Propozicija 2.0.10. $(\mathbb{C}, +, \cdot, *)$ *je komutativna i asocijativna* $\mathbb{R}$*-algebra s dijeljenjem.*

Dokaz. Prema prethodnim propozicijama $(\mathbb{C}, +, \cdot)$ je polje, a $(\mathbb{C}, +, *)$ vektorski prostor nad $\mathbb{R}$.

Preostaje pokazati

$$(\alpha * u) \cdot (\beta * v) = (\alpha \cdot \beta) * (u \cdot v), \forall \alpha, \beta \in \mathbb{R}, u, v \in V.$$

Neka su $u = x + yi, v = a + bi$, gdje su $x, y, a, b \in \mathbb{R}$. Tada je:

$$\begin{aligned}
(\alpha * u) \cdot (\beta * v) &= (\alpha x + \alpha yi) \cdot (\beta a + \beta bi) \\
&= \alpha\beta xa + \alpha\beta yai + \alpha\beta xbi - \alpha\beta yb \\
&= \alpha\beta * ((xa - yb) + (ya + xb)i) \\
&= (\alpha\beta) * (u \cdot v).
\end{aligned}$$

□

Prikaz kompleksnih brojeva kao 2×2 realnih matrica

Kompleksne brojeve možemo identificirati s realnim matricama 2×2:

$$z = x + yi \leftrightarrow \begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix} = x \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + y \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = x \cdot 1 + y \cdot i,$$

pri čemu se matrica

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

ponaša kao broj 1, a matrica

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

kao $i = \sqrt{-1}$.

Zbrajanje i množenje kompleksnih brojeva sada možemo promatrati kao zbrajanje i množenje matrica.

$$(x + yi) + (u + vi) = \begin{bmatrix} x & -y \\ y & x \end{bmatrix} + \begin{bmatrix} u & -v \\ v & u \end{bmatrix} = \begin{bmatrix} x + u & -(y + v) \\ y + v & x + u \end{bmatrix} = (x + u) + (y + v)i$$

$$(x + yi) \cdot (u + vi) = \begin{bmatrix} x & -y \\ y & x \end{bmatrix} \cdot \begin{bmatrix} u & -v \\ v & u \end{bmatrix} = \begin{bmatrix} xu - yv & -(xv + yu) \\ xv + yu & xu - yv \end{bmatrix} = (xu - yv) + (xv + yu)i$$

Normu kompleksnog broja $x + yi$ definiramo na sljedeći način:

$$N(x + yi) = det \begin{bmatrix} x & -y \\ y & x \end{bmatrix} = x^2 + y^2.$$

Za $z_1 = x + yi, z_2 = u + vi \in \mathbb{C}$ vrijedi

$$det \begin{bmatrix} x & -y \\ y & x \end{bmatrix} \cdot det \begin{bmatrix} u & -v \\ v & u \end{bmatrix} = det \left[\begin{bmatrix} x & -y \\ y & x \end{bmatrix} \cdot \begin{bmatrix} u & -v \\ v & u \end{bmatrix} \right],$$

dakle $N(z_1) \cdot N(z_2) = N(z_1 z_2)$.

Poglavlje 3

Algebra kvaterniona

3.1 Osnove o kvaternionima

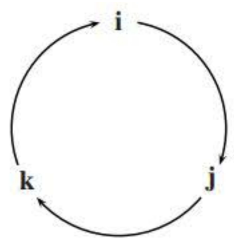
Definicija

Definicija 3.1.1. *Četverodimenzionalni realni vektorski prostor* $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ *zove se* ***prostor kvaterniona****.*

Kako bismo definirali množenje kvaterniona, najprije definiramo množenje kvaterniona i, j, k sljedećim formulama:

- $i^2 = j^2 = k^2 = -1$,
- $ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j.$

Pravilo množenja i, j, k može se predstaviti sljedećom shemom. Naime, umnožak će imati pozitivan predznak ukoliko se krećemo u smjeru kazaljke na satu i negativan, ako se krećemo u smjeru suprotnom od smjera kazaljke na satu.



Slika 3.1: Pravilo predznaka

Dodamo li gornjim pravilima množenja kvaterniona i, j, k zahtjev da svaki $a \in \mathbb{R}$ mora komutirati sa i, j, k te zahtjev da množenje kvaterniona treba biti distributivno prema zbrajanju, jedinstveno smo zadali pravilo množenja bilo kojih dvaju kvaterniona. To ilustrira sljedeći primjer:

Primjer 3.1.2. $(i + j)(i - j) = i^2 - ij + ji - j^2 = -1 - k - k - (-1) = -2k.$

Zbrajanje i množenje kvaterniona

Operacije s kvaternionima se mogu definirati na sljedeći način.

Definicija 3.1.3. *Neka su $q_1, q_2 \in \mathbb{H}$, pri čemu su $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ i $q_2 = a_2 + b_2 i + c_2 j + d_2 k$.*
Zbroj kvaterniona q_1 i q_2 je:

$$\begin{aligned} q_1 + q_2 &= (a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) \\ &= (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k. \end{aligned}$$

Zbrajanje kvaterniona ima svojstva asocijativnosti i komutativnosti jer se zbrajanje kvaterniona svodi na zbrajanje realnih brojeva.

Pravilo za množenje kvaterniona jednako je kao za množenje polinoma, prošireno za multiplikativna svojstva elemenata i, j, k.

Definicija 3.1.4. *Neka su $q_1, q_2 \in \mathbb{H}$, pri čemu su $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ i $q_2 = a_2 + b_2 i + c_2 j + d_2 k$.*
Umnožak kvaterniona q_1 i q_2 je:

$$\begin{aligned} q_1 \cdot q_2 &= (a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k) \\ &= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)i \\ &+ (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2)j + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2)k. \end{aligned}$$

Propozicija 3.1.5. *Za svaki $q_1, q_2, q_3 \in \mathbb{H}$ vrijedi:*

1. $q_1 \cdot (q_2 + q_3) = q_1 q_2 + q_1 q_3$,
2. $(q_1 + q_2) \cdot q_3 = q_1 q_3 + q_2 q_3$.

*Ovo svojstvo nazivamo **distributivnost** množenja kvaterniona s obzirom na zbrajanje kvaterniona.*

Dokaz. Neka su $q_1, q_2, q_3 \in \mathbb{H}$, $q_1 = a_1 + b_1 i + c_1 j + d_1 k$, $q_2 = a_2 + b_2 i + c_2 j + d_2 k$, $q_3 = a_3 + b_3 i + c_3 j + d_3 k$.

1. Tada imamo

$$\begin{aligned}
q_1 \cdot (q_2 + q_3) &= (a_1 + b_1 i + c_1 j + d_1 k)((a_2 + a_3) + (b_2 + b_3)i + (c_2 + c_3)j + (d_2 + d_3)k) \\
&= (a_1 + b_1 i + c_1 j + d_1 k)(a_2 + a_3 + b_2 i + b_3 i + c_2 j + c_3 j + d_2 k + d_3 k) \\
&= a_1a_2 + a_1a_3 + a_1b_2 i + a_1b_3 i + a_1c_2 j + a_1c_3 j + a_1d_2 k + a_1d_3 k \\
&+ b_1a_2 i + b_1a_3 i - b_1b_2 - b_1b_3 + b_1c_2 k + b_1c_3 k - b_1d_2 j - b_1d_3 j \\
&+ c_1a_2 j + c_1a_3 j - c_1b_2 k - c_1b_3 k - c_1c_2 - c_1c_3 + c_1d_2 i + c_1d_3 i \\
&+ d_1a_2 k + d_1a_3 k + d_1b_2 j + d_1b_3 j - d_1c_2 i - d_1c_3 i - d_1d_2 - d_1d_3 \\
&= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i \\
&+ (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k \\
&+ (a_1a_3 - b_1b_3 - c_1c_3 - d_1d_3) + (a_1b_3 + b_1a_3 + c_1d_3 - d_1c_3)i \\
&+ (a_1c_3 - b_1d_3 + c_1a_3 + d_1b_3)j + (a_1d_3 + b_1c_3 - c_1b_3 + d_1a_3)k \\
&= q_1q_2 + q_1q_3.
\end{aligned}$$

2. Odnosno,

$$\begin{aligned}
(q_1 + q_2) \cdot q_3 &= ((a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k)(a_3 + b_3 i + c_3 j + d_3 k) \\
&= (a_1 + a_2 + b_1 i + b_2 i + c_1 j + c_2 j + d_1 k + d_2 k)(a_3 + b_3 i + c_3 j + d_3 k) \\
&= a_1a_3 + a_1b_3 i + a_1c_3 j + a_1d_3 k + a_2a_3 + a_2b_3 i + a_2c_3 j + a_2d_3 k \\
&+ b_1a_3 i - b_1b_3 + b_1c_3 k - b_1d_3 j + b_2a_3 i - b_2b_3 + b_2c_3 k - b_2d_3 j \\
&+ c_1a_3 j - c_1b_3 k - c_1c_3 + c_1d_3 i + c_2a_3 j - c_2b_3 k - c_2c_3 + c_2d_3 i \\
&+ d_1a_3 k + d_1b_3 j - d_1c_3 i - d_1d_3 + d_2a_3 k + d_2b_3 j - d_2c_3 i - d_2d_3 \\
&= (a_1a_3 - b_1b_3 - c_1c_3 - d_1d_3) + (a_1b_3 + b_1a_3 + c_1d_3 - d_1c_3)i \\
&+ (a_1c_3 - b_1d_3 + c_1a_3 + d_1b_3)j + (a_1d_3 + b_1c_3 - c_1b_3 + d_1a_3)k \\
&+ (a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3) + (a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3)i \\
&+ (a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3)j + (a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3)k \\
&= q_1q_3 + q_2q_3
\end{aligned}$$

čime je distributivnost dokazana.

□

Definicija 3.1.6. *Za svaki $\alpha \in \mathbb{R}$ i za svaki $q \in \mathbb{H}, q = a + bi + cj + dk$ definiramo*

$$\alpha * q = \alpha a + \alpha bi + \alpha cj + \alpha dk.$$

Vanjsku operaciju $*$ množenje kvaterniona skalarom.

Definicija 3.1.7. *Neka je $q = a + bi + cj + dk \in \mathbb{H}$.*
Realan broj a naziva se ***realni dio kvaterniona*** *q i označava se $\Re(q)$.*
Kvaternion $bi + cj + dk$ naziva se ***imaginarni dio kvaterniona*** *q i označava se $\Im(q)$.*

Primjer 3.1.8. *Kvaternion q u kojem je $a = 0$ naziva se* ***čisti kvaternion*** *i njegov kvadrat je negativan zbroj tri kvadrata.*
Neka je $q = bi + cj + dk$. Tada je njegov kvadrat:

$$\begin{aligned}
(bi + cj + dk)^2 &= (bi + cj + dk)(bi + cj + dk)\\
&= b^2i^2 + bicj + bidk + cjbi + c^2j^2 + cjdk + dkbi + dkcj + d^2k^2\\
&= -b^2 + bcij + bdik + cbji - c^2 + cdjk + dbki + dckj - d^2\\
&= -b^2 + bck - bdj - cbk - c^2 + cdi + dbj - dci - d^2\\
&= -(b^2 + c^2 + d^2).
\end{aligned}$$

Konjugiranje kvaterniona

Definicija 3.1.9. *Kvaternion $\overline{q} = a - bi - cj - dk$ naziva se* ***konjugirani kvaternion*** *kvaterniona $q = a + bi + cj + dk$.*

Konjugiranje u $\mathbb{H}$ definirano je analogno konjugiranju u $\mathbb{C}$. Također, konjugiranje kvaterniona ima slična svojstva kao konjugiranje u $\mathbb{C}$.

Propozicija 3.1.10. *Neka su $q_1, q_2 \in \mathbb{H}$, $q_1 = a_1 + b_1i + c_1j + d_1k$ i $q_2 = a_2 + b_2i + c_2j + d_2k$. Tada vrijedi:*

1. $\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$
2. $\overline{q_1 \cdot q_2} = \overline{q_2} \cdot \overline{q_1}$
3. $\overline{\overline{q}} = q$.

Dokaz. 1. Po definiciji zbrajanja i konjugiranja kvaterniona imamo

$$\begin{aligned}
\overline{q_1 + q_2} &= \overline{(a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k}\\
&= a_1 + a_2 - (b_1 + b_2)i - (c_1 + c_2)j - (d_1 + d_2)k\\
&= a_1 + a_2 - b_1i - b_2i - c_1j - c_2j - d_1k - d_2k\\
&= (a_1 - b_1i - c_1j - d_1k) + (a_2 - b_2i - c_2j - d_2k)\\
&= \overline{q_1} + \overline{q_2}.
\end{aligned}$$

2. Analogno prethodnom dokazu imamo

$$\begin{aligned}
\overline{q_1 \cdot q_2} &= \overline{(a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k)} \\
&= \overline{(a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i} \\
&\quad \overline{+ (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k} \\
&= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) - (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i \\
&\quad - (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j - (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k.
\end{aligned}$$

Raspišimo sada desnu stranu jednakosti:

$$\begin{aligned}
\overline{q_2} \cdot \overline{q_1} &= (a_2 - b_2 i - c_2 j - d_2 k)(a_1 - b_1 i - c_1 j - d_1 k) \\
&= (a_2a_1 - b_2b_1 - c_2c_1 - d_2d_1) - (a_2b_1 + b_2a_1 - c_2d_1 + d_2c_1)i \\
&\quad - (a_2c_1 + b_2d_1 + c_2a_1 - d_2b_1)j - (a_2d_1 - b_2c_1 + c_2b_1 + d_2a_1)k.
\end{aligned}$$

Raspisivanjem lijeve i desne strane jednakosti došli smo do istih izraza, čime je ova jednakost dokazana.
Primijetimo da konjugiranje mijenja redoslijed množenja.

3. Imamo

$$\overline{\overline{q}} = \overline{\overline{(a + bi + cj + dk)}} = \overline{a - bi - cj - dk} = a + bi + cj + dk = q$$

čime je jednakost dokazana.

$\square$

Definicija 3.1.11. ***Modul kvaterniona*** *$q = a + bi + cj + dk$ je nenegativan realan broj*

$$|q| = \sqrt{a^2 + b^2 + c^2 + d^2}.$$

Propozicija 3.1.12. *Neka je $q = a + bi + cj + dk \in \mathbb{H}$ i $\overline{q} = a - bi - cj - dk \in \mathbb{H}$ njemu konjugirani kvaternion. Tada vrijedi:*

$$q\overline{q} = |q|^2.$$

Dokaz. Primjenjujući svojstva množenja kvaterniona, desna strana jednaka je:

$$\begin{aligned}
q\overline{q} &= (a + bi + cj + dk)(a - bi - cj - dk) \\
&= a^2 - abi - acj - adk + bia - b^2i^2 - bicj - bidk + cja - cjbi - c^2j^2 - cjdk \\
&\quad + dka - dkbi - dkcj - d^2k^2 \\
&= a^2 + b^2 - bcij - bdik - cbji + c^2 - cdjk - dbki - dckj + d^2 \\
&= a^2 + b^2 + c^2 + d^2 - bck + bdj + cbk - cdi - dbj + dci \\
&= a^2 + b^2 + c^2 + d^2.
\end{aligned}$$

Kako je po definiciji modula $|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$, onda je $|q|^2 = a^2 + b^2 + c^2 + d^2$ čime je jednakost dokazana. □

Na osnovu ovoga definiramo sljedeći pojam.

Norma kvaterniona

Definicija 3.1.13. ***Norma kvaterniona*** *$q = a + bi + cj + dk$ je nenegativan realan broj*

$$N(q) = q \cdot \overline{q} = |q|^2 = a^2 + b^2 + c^2 + d^2.$$

Iz definicije norme slijedi da svaki kvaternion komutira sa svojim konjugiranim kvaternionom: $\overline{q}q = q\overline{q}$.

Propozicija 3.1.14. *Neka su $q_1, q_2 \in \mathbb{H}$ proizvoljni. Tada vrijedi*

$$N(q_1 q_2) = N(q_1)N(q_2).$$

Dokaz. Po definiciji norme raspišemo desnu stranu jednakosti:

$$N(q_1 q_2) = |q_1 q_2|^2 = (q_1 q_2)(\overline{q_2}\,\overline{q_1}).$$

Prema propoziciji 3.1.10.2 slijedi:

$$N(q_1 q_2) = (q_1 q_2)(\overline{q_2}\,\overline{q_1}) = q_1(q_2\overline{q_2})\overline{q_1} = q_1|q_2|^2\overline{q_1},$$

pri čemu u drugoj jednakosti koristimo asocijativnost množenja u $\mathbb{H}$, koju ćemo dokazati u poglavlju 3.2. Kako je norma kvaterniona realan broj, možemo pisati:

$$N(q_1 q_2) = q_1\overline{q_1}|q_2|^2 = |q_1|^2|q_2|^2 = N(q_1)N(q_2).$$

□

3.2 Prikaz kvaterniona kao 2x2 kompleksnih matrica

U prethodnom poglavlju vidjeli smo kako se kompleksni brojevi mogu prikazati kao 2×2 realne matrice. U ovom poglavlju identificirat ćemo kvaternione s $M_2(\mathbb{C})$.

Kako bi elemente iz $\mathbb{H}$ prikazali kao kompleksne matrice, prestajemo o kvaternionima razmišljati kao o četverodimenzionalnom prostoru s realnim skalarima i bazom $1, i, j, k$ te prelazimo u dvodimenzionalan prostor, kompleksne skalare i bazu $1, j$. Odnosno, kvaternione zapisujemo na sljedeći način:

$$q = a + bi + cj + dk = (a + bi) + (c + di)j = z + wj,$$

gdje je $z = a + bi$ i $w = c + di$.
Svaki kvaternion $q, q = z + wj$ možemo prikazati kao matricu u $M_2(\mathbb{C})$ na sljedeći način:

$$m_q = \begin{bmatrix} z & -w \\ \overline{w} & \overline{z} \end{bmatrix}.$$

Primjer 3.2.1. *Matrični zapisi elemenata baze* $1, i, j, k$:

$$m_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, m_i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, m_j = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, m_k = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}.$$

Propozicija 3.2.2. *Neka su* $m_q, m_{q'} \in M_2(\mathbb{C})$*, tada vrijedi:*

1. $m_{q+q'} = m_q + m_{q'}$
2. $m_{qq'} = m_q \cdot m_{q'}$.

Dokaz. Neka su $q, q' \in \mathbb{H}$, $q = z + wj, q' = z' + w'j$ gdje su $z = a + bi, w = c + di$ za neke $a, b, c, d \in \mathbb{R}$ i $z' = a' + b'i, w' = c' + d'i$ za neke $a', b', c', d' \in \mathbb{R}$.

1. Tada imamo

$$m_{q+q'} = \begin{bmatrix} z + z' & -(w + w') \\ \overline{w + w'} & \overline{z + z'} \end{bmatrix} = \begin{bmatrix} z + z' & -w - w' \\ \overline{w} + \overline{w'} & \overline{z} + \overline{z'} \end{bmatrix} = \begin{bmatrix} z & -w \\ \overline{w} & \overline{z} \end{bmatrix} + \begin{bmatrix} z' & -w' \\ \overline{w'} & \overline{z'} \end{bmatrix} = m_q + m_{q'}.$$

2. Najprije raspišimo desnu stranu jednakosti.

$$\begin{aligned} m_q \cdot m_{q'} &= \begin{bmatrix} z & -w \\ \overline{w} & \overline{z} \end{bmatrix} \cdot \begin{bmatrix} z' & -w' \\ \overline{w'} & \overline{z'} \end{bmatrix} = \begin{bmatrix} zz' - w\overline{w'} & -zw' - w\overline{z'} \\ \overline{w}z' + \overline{z}\overline{w'} & -\overline{w}w' - \overline{z}\overline{z'} \end{bmatrix} = \begin{bmatrix} zz' - w\overline{w'} & -(zw' + w\overline{z'}) \\ \overline{zw' + w\overline{z'}} & \overline{zz' - w\overline{w'}} \end{bmatrix} \\ &= m_{zz' - w\overline{w'} + (zw' + w\overline{z'})j} \end{aligned}$$

Želimo pokazati

$$m_{zz' - w\overline{w'} + (zw' + w\overline{z'})j} = m_{q \cdot q'},$$

odnosno

$$q \cdot q' = zz' - w\overline{w'} + (zw' + w\overline{z'})j.$$

Raspišimo obje strane jednakosti:

$$\begin{aligned} & q \cdot q' = zz' - w\overline{w'} + (zw' + w\overline{z'})j \\ & \Leftrightarrow (z + wj)(z' + w'j) = zz' - w\overline{w'} + (zw' + w\overline{z'})j \\ & \Leftrightarrow \cancel{zz'} + z(w'j) + (wj)z' + (wj)(w'j) = \cancel{zz'} - w\overline{w'} + (zw')j + (w\overline{z'})j \\ & \Leftrightarrow z(w'j) + (wj)z' + (wj)(w'j) = -w\overline{w'} + (zw')j + (w\overline{z'})j. \end{aligned} \tag{3.1}$$

Izračunat ćemo posebno svaki od pribrojnika iz prethodne jednakosti. Imamo

$$\begin{aligned} z(w'j) &= (a+bi)((c'+d'i)j) = (a+bi)(c'j+d'k) \\ &= ac'j + ad'k + bc'k - bd'j \\ &= (ac'-bd')j + (ad'+bc')ij \\ &= (ac'-bd' + (ad+bc')i)j, \end{aligned}$$

$$\begin{aligned} (wj)z' &= ((c+di)j)(a'+b'i) = (cj+dij)(a'+b'i) = (cj+dk)(a'+b'i) \\ &= ca'j + cb'(-k) + da'k + db'j \\ &= (ca'+db')j + (da'-cb')ij \\ &= ((ca'+db') + (da'-cb')i)j, \end{aligned}$$

$$\begin{aligned} (wj)(w'j) &= ((c+di)j)((c'+d'i)j) = (cj+dk)(c'j+d'k) \\ &= -cc' + cd'i + dc'(-i) - dd' \\ &= -cc' - dd' + (cd'-dc')i, \end{aligned}$$

$$\begin{aligned} w\overline{w'} &= (c+di)(c'-d'i) = cc' - cd'i + dc'i + dd' \\ &= cc' + dd' - (cd'-dc')i, \end{aligned}$$

$$\begin{aligned} (zw')j &= ((a+bi)(c'+d'i)j) = (ac' + ad'i + bc'i - bd')j \\ &= (ac'-bd' + (ad'+bc')i)j, \end{aligned}$$

$$\begin{aligned} (w\overline{z'})j &= ((c+di)(a'-b'i))j = (ca' - cb'i + da'i + db')j \\ &= (ca'+db' - (cb'-da')i)j. \end{aligned}$$

Uvrstimo li odgovarajuće jednakosti u (3.1) slijedi

$$\begin{aligned} \Leftrightarrow &(ac'-bd' + (ad+bc')i)j + ((ca'+db') + (da'-cb')i)j - cc' - dd' + (cd'-dc')i = \\ &-cc' - dd' + (cd'-dc')i + (ac'-bd' + (ad'+bc')i)j + (ca'+db' - (cb'-da')i)j \\ \Leftrightarrow &-cc' - dd' + (cd'-dc')i + (ac'-bd'+ca'+db' + (ad'+bc'-cb'+da')i)j = \\ &-cc' - dd' + (cd'-dc')i + (ac'-bd'+ca'+db' + (ad'+bc'-cb'+da')i)j \end{aligned}$$

čime je tvrdnja dokazana.

$\square$

Prema prethodnoj propoziciji slijedi kako je preslikavanje $q \to m_q$ očuvalo pravila zbrajanja i množenja. Odnosno, svojstva zbrajanja i množenja koja vrijede za matrice, sada vrijede i u $\mathbb{H}$. Prema tome množenje kvaterniona je asocijativno.

Konjugiranje kvaterniona i norma kvaterniona se mogu opisati u terminima matrica:

- $m_{\overline{q}} = \overline{m_q}^\top$
- $N(q) = \det m_q$.

Primjer 3.2.3. *Neka je* $m_q = \begin{bmatrix} z & -w \\ \overline{w} & \overline{z} \end{bmatrix} \in M_2(\mathbb{C})$. *Tada su*
$m_{\overline{q}} = \overline{m_q}^\top = \begin{bmatrix} \overline{z} & w \\ -\overline{w} & z \end{bmatrix}$,
$N(q) = det\ m_q = \begin{vmatrix} z & -w \\ \overline{w} & \overline{z} \end{vmatrix} = z\overline{z} + w\overline{w} = |z|^2 + |w|^2.$

3.3 Algebarska svojstva kvaterniona

Propozicija 3.3.1. $(\mathbb{H}, +, \cdot)$ *ima strukturu nekomutativnog prstena s dijeljenjem.*

Dokaz. Po definiciji $\mathbb{H}$ je realan vektorski prostor, stoga je $(\mathbb{H}, +)$ Abelova grupa. Dokažimo da $(\mathbb{H}, +, \cdot)$ ima i ostala svojstva iz definicije prstena s dijeljenjem te da je množenje u $\mathbb{H}$ nekomutativno.

1. Asocijativnost množenja kvaterniona pokazana je u prethodnom potpoglavlju.
2. $1 \in \mathbb{H}$ je neutralni element za množenje.
   Naime, za svaki $q \in \mathbb{H}$ očito vrijedi
$$\begin{aligned} q \cdot 1 &= q \\ 1 \cdot q &= q. \end{aligned}$$
3. Svaki $q \in \mathbb{H}, q \neq 0$ ima inverz $q^{-1} = \frac{\overline{q}}{N(q)}$.
   Naime, q^{-1} dan gornjom formulom je i lijevi i desni inverz od q:
$$q \cdot q^{-1} = q \cdot \frac{\overline{q}}{N(q)} = \frac{q \cdot \overline{q}}{N(q)} = \frac{N(q)}{N(q)} = 1,$$
$$q^{-1} \cdot q = \frac{\overline{q}}{N(q)} \cdot q = \frac{\overline{q} \cdot q}{N(q)} = \frac{N(q)}{N(q)} = 1.$$

4. Množenje kvaterniona nije komutativna operacija. Primjerice,

$$ij = k,$$
$$ji = -k.$$

5. Distributivnost množenja prema zbrajanju vrijedi po propoziciji 3.1.5.

□

Primjer 3.3.2. *Odredite inverz kvaternionu $q = i + j$.*

Najprije izračunamo normu kvaterniona: $N(q) = |q| = 1^2 + 1^2 = 2$. Kako je $\overline{q} = -i - j$, slijedi $q^{-1} = \frac{\overline{q}}{N(q)} = \frac{1}{2}(-i - j)$.

Propozicija 3.3.3. *Skup $\mathbb{H}$ je vektorski prostor nad poljem $\mathbb{R}$ u odnosu na zbrajanje kvaterniona i množenje skalarima.*

Dokaz. Po definiciji je $(\mathbb{H}, +, *)$ četverodimenzionalni realni vektorski prostor. □

Propozicija 3.3.4. $(\mathbb{H}, +, \cdot, *)$ *je $\mathbb{R}$-algebra s dijeljenjem.*

Dokaz. Pokazali smo da je $(\mathbb{H}, +, \cdot)$ nekomutativan prsten s dijeljenjem i $(\mathbb{H}, +, *)$ vektorski prostor nad poljem $\mathbb{R}$. Preostaje pokazati:

$$(\alpha * q_1) \cdot (\beta * q_2) = (\alpha \cdot \beta) * (q_1 \cdot q_2)$$

za sve $\alpha, \beta \in \mathbb{R}, q_1, q_2 \in \mathbb{H}$.
Neka su $q_1, q_2 \in \mathbb{H}$, $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ i $q_2 = a_2 + b_2 i + c_2 j + d_2 k$. Tada je:

$$\begin{aligned}(\alpha * q_1) \cdot (\beta * q_2) &= (\alpha a_1 + \alpha b_1 i + \alpha c_1 j + \alpha d_1 k) \cdot (\beta a_2 + \beta b_2 i + \beta c_2 j + \beta d_2 k) \\
&= \alpha\beta a_1 a_2 + \alpha\beta b_1 a_2 i + \alpha\beta c_1 a_2 j + \alpha\beta d_1 a_2 k \\
&+ \alpha\beta a_1 b_2 i + \alpha\beta b_1 b_2 i^2 + \alpha\beta c_1 b_2 ji + \alpha\beta d_1 b_2 ki \\
&+ \alpha\beta a_1 c_2 j + \alpha\beta b_1 c_2 ij + \alpha\beta c_1 c_2 j^2 + \alpha\beta d_1 c_2 kj \\
&+ \alpha\beta a_1 d_2 k + \alpha\beta b_1 d_2 ik + \alpha\beta c_1 d_2 jk + \alpha\beta d_1 d_2 k^2 \\
&= (\alpha\beta) * (a_1 a_2 + b_1 a_2 i + c_1 a_2 j + d_1 a_2 k + a_1 b_2 i - b_1 b_2 - c_1 b_2 k + d_1 b_2 j \\
&+ a_1 c_2 j + b_1 c_2 k - c_1 c_2 - d_1 c_2 i + a_1 d_2 k + b_1 d_2 j + c_1 d_2 i - d_1 d_2 \\
&= (\alpha \cdot \beta) * (q_1 \cdot q_2).\end{aligned}$$

Tvrdnja slijedi. □

Poglavlje 4

Primjena kvaterniona

4.1 Lagrangeov teorem o četirima kvadratima

Hurwitzovi cijeli brojevi

Definicija 4.1.1. ***Hurwitzov kvaternion*** *ili* ***Hurwitzov cijeli broj*** [1] *je kvaternion čiji koeficijenti su svi cijeli brojevi ili polovine neparnog cijelog broja (miješanje koeficijenata nije dozvoljeno).*

Skup svih Hurwitzovih cijelih brojeva označavamo:

$$\mathbf{H} = \left\{ a + bi + cj + dk \in \mathbb{H}, a, b, c, d \in \mathbb{Z} \vee a, b, c, d \in \mathbb{Z} + \frac{1}{2} \right\}.$$

Hurwitzovi cijeli brojevi se mogu zapisati i na sljedeći način:

$$A\frac{1 + i + j + k}{2} + Bi + Cj + Dk = a + bi + cj + dk$$

gdje su $A, B, C, D \in \mathbb{Z}$. Ovisno je li A paran ili neparan, koeficijenti a, b, c, d su cijeli brojevi ili polovine neparnih brojeva.

Lako se pokaže da je skup $\mathbf{H}$ zatvoren za zbrajanje i množenje kvaterniona, dakle $\mathbf{H}$ je potprsten od $\mathbb{H}$. Hurwitzovi kvaternioni se najčešće označavaju slovima grčkog alfabeta.

Definicija 4.1.2. *Hurwitzov cijeli broj α je* ***Hurwitzov prost broj*** *ako se α ne može napisati kao produkt dvaju Hurwitzovih cijelih brojeva strogo manje norme.*

Propozicija 4.1.3. *Norma Hurwitzovog kvaterniona je cijeli broj.*

[1] Adolf Hurwitz (1859-1919), njemački matematičar

Dokaz. Neka je $\alpha \in \mathbf{H}$. Tada je $\alpha = a + bi + cj + dk$ za neke $a, b, c, d \in \mathbb{Z}$ ili $\alpha = \frac{a'}{2} + \frac{b'}{2}i + \frac{c'}{2}j + \frac{d'}{2}k$ za neke neparne $a' = 2l+1, b' = 2m+1, c' = 2n+1, d' = 2p+1 \in \mathbb{Z}$. Tada je:

$$N(\alpha) = a^2 + b^2 + c^2 + d^2 \in \mathbb{Z}$$

ili

$$\begin{aligned} N(\alpha) &= \left(\frac{a'}{2}\right)^2 + \left(\frac{b'}{2}\right)^2 + \left(\frac{c'}{2}\right)^2 + \left(\frac{d'}{2}\right)^2 \\ &= \frac{a'^2}{4} + \frac{b'^2}{4} + \frac{c'^2}{4} + \frac{d'^2}{4} \\ &= \frac{(2l+1)^2}{4} + \frac{(2m+1)^2}{4} + \frac{(2n+1)^2}{4} + \frac{(2p+1)^2}{4} \\ &= \frac{4l^2 + 4l + 1 + 4m^2 + 4m + 1 + 4n^2 + 4n + 1 + 4p^2 + 4p + 1}{4} \\ &= \frac{4 \cdot (l^2 + l + m^2 + m + n^2 + n + p^2 + p + 1)}{4} \\ &= l^2 + l + m^2 + m + n^2 + n + p^2 + p + 1 \in \mathbb{Z}. \end{aligned}$$

□

Definicija 4.1.4. *Hurwitzov kvaternion norme 1 je* ***jedinični Hurwitzov kvaternion****.*

Jediničnih Hurwitzovih kvaterniona ima konačno mnogo. Naime, ako je $\alpha = a + bi + cj + dk$ jedinični Hurwitzov kvaternion, postoje sljedeće dvije mogućnosti:

1. ako su $a, b, c, d \in \mathbb{Z}$, tada jedan od brojeva a^2, b^2, c^2, d^2 mora biti 1, a ostali 0,
2. ako su $a, b, c, d \in \mathbb{Z} + \frac{1}{2}$, tada svaki od brojeva a^2, b^2, c^2, d^2 mora biti $\frac{1}{4}$.

Za prvu mogućnost imamo 8 različitih jediničnih Hurwitzovih kvaterniona: $\pm 1, \pm i, \pm j, \pm k$, odnosno 16 različitih kvaterniona za drugu mogućnost: $\pm\frac{1}{2} \pm \frac{i}{2} \pm \frac{j}{2} \pm \frac{k}{2}$.

Lema 4.1.5. *Neka je $\alpha \in \mathbf{H}$. Tada je α invertibilan u prstenu $\mathbf{H}$ ako i samo ako je α jedinični Hurwitzov kvaternion.*

Dokaz. Pretpostavimo da je α invertibilan u prstenu $\mathbf{H}$. Dokazat ćemo da je norme 1. Po pretpostavci postoji $\beta \in \mathbf{H}$ takav da je $\alpha\beta = \beta\alpha = 1$, odakle slijedi da je

$$\begin{aligned} & N(\alpha\beta) = N(1) = 1, \\ & \Rightarrow N(\alpha)N(\beta) = 1 \ \text{ gdje su } \ N(\alpha), N(\beta) \in \mathbb{Z}_{\geq 0}, \\ & \Rightarrow N(\alpha) = N(\beta) = 1. \end{aligned}$$

Posebno, $N(\alpha) = 1$ pa je α jedinični Hurwitzov kvaternion.

Pogledajmo drugi smjer. Neka je α jedinični kvaternion, stoga je $\alpha \in \mathbb{H}\backslash\{0\}$, odnosno α je invertibilan u $\mathbb{H}$. Pritom je

$$\alpha^{-1} = \frac{\overline{\alpha}}{N(\alpha)} = \overline{\alpha} \in \mathbf{H}.$$

Dakle, α^{-1} je inverz od α u $\mathbf{H}$. □

Za Hurwitzove cijele brojeve vrijedi teorem o dijeljenju s ostatkom.

Teorem 4.1.6. *Za $\alpha, \beta \in \boldsymbol{H}\backslash\{0\}$ postoje $\mu, p \in \boldsymbol{H}$, $N(p) < N(\beta)$ takvi da vrijedi $\alpha = \mu \cdot \beta + p$.*

Dokaz. Neka je $\alpha\beta^{-1} = a + bi + cj + dk \in \mathbb{H}$ za neke $a, b, c, d \in \mathbb{R}$.
Odaberemo $a', b', c', d' \in \mathbb{Z}$ takve da vrijedi:

$$|a - a'| \leq \frac{1}{2}, |b - b'| \leq \frac{1}{2}, |c - c'| \leq \frac{1}{2}, |d - d'| \leq \frac{1}{2}.$$

Definiramo $\mu_1 := a' + b'i + c'j + d'k \in \mathbf{H}$.
Primijetimo da vrijedi sljedeće:

$$\begin{aligned}
&N(\alpha\beta^{-1} - \mu_1) = N((a + bi + cj + dk) - (a' + b'i + c'j + d'k)) = \\
&N(a - a' + (b - b')i + (c - c')j + (d - d')k) = \\
&(a - a')^2 + (b - b')^2 + (c - c')^2 + (d - d')^2 = \\
&|a - a'|^2 + |b - b'|^2 + |c - c'|^2 + |d - d'|^2 \leq \\
&\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = 1.
\end{aligned}$$

Razlikujemo dva slučaja.

- Ako je $N(\alpha\beta^{-1} - \mu_1) < 1$ stavimo:

$$\mu := \mu_1, \quad p := \alpha - \mu_1\beta.$$

Očito su $\mu, p \in \mathbf{H}$ i vrijedi $\alpha = \mu \cdot \beta + p$.
Također, imamo:

$$N(p) = N(\alpha - \mu_1\beta) = N((\alpha\beta^{-1} - \mu_1)\beta) = N(\alpha\beta^{-1} - \mu_1)N(\beta) < N(\beta).$$

- Ako je $N(\alpha\beta^{-1} - \mu_1) = 1$, tada je:

$$\begin{aligned}
&|a - a'| = |b - b'| = |c - c'| = |d - d'| = \frac{1}{2} \\
&\Rightarrow a - a', b - b', c - c', d - d' \in \left\{\pm\frac{1}{2}\right\} \\
&\Rightarrow a, b, c, d \in \mathbb{Z} + \frac{1}{2} \\
&\Rightarrow \alpha\beta^{-1} = a + bi + cj + dk \in \mathbf{H}.
\end{aligned}$$

Stoga možemo staviti $\mu := \alpha\beta^{-1}$ i $p := 0$. Naime, za ovako definirane μ i p vrijedi

$$\begin{aligned}
&\mu\beta + p = (\alpha\beta^{-1})\beta + 0 = \alpha, \\
&N(p) = N(0) = 0 < N(\beta),
\end{aligned}$$

čime je dokaz završen.

□

Primjer 4.1.7. *Neka su $\alpha = 4j + 1$ i $\beta = 2k$ Hurwitzovi cijeli brojevi. Prateći dokaz teorema 4.1.6 pokažimo da za njih vrijedi teorem o dijeljenju s ostatkom.*
Najprije računamo:

$$\beta^{-1} = \frac{\overline{\beta}}{N(\beta)} = \frac{-2k}{4} = \frac{-1}{2}k,$$

$$\alpha\beta^{-1} = (4j + 1)\left(\frac{-1}{2}k\right) = -2i - \frac{1}{2}k \Rightarrow a = 0, b = -2, c = 0, d = \frac{-1}{2}.$$

Tražimo $\mu_1 = a' + b'i + c'j + d'k$ takav da su koeficijenti $a', b', c', d' \in \mathbb{Z}$ i da vrijede nejednakosti:

$$\begin{aligned}
&|a - a'| \leq \frac{1}{2} \Rightarrow \frac{-1}{2} \leq a' \leq \frac{1}{2} \Rightarrow a' = 0, \\
&|b - b'| \leq \frac{1}{2} \Rightarrow \frac{-1}{2} \leq -2 - b' \leq \frac{1}{2} \Rightarrow \frac{-5}{2} \leq b' \leq \frac{-3}{2} \Rightarrow b' = -2, \\
&|c - c'| \leq \frac{1}{2} \Rightarrow \frac{-1}{2} \leq c' \leq \frac{1}{2} \Rightarrow c' = 0, \\
&|d - d'| \leq \frac{1}{2} \Rightarrow \frac{-1}{2} \leq -\frac{1}{2} - d' \leq \frac{1}{2} \Rightarrow 1 \leq d' \leq 0 \Rightarrow d' = 0, \\
&\Rightarrow \mu_1 = -2i.
\end{aligned}$$

Računamo normu:

$$N\left(\alpha\beta^{-1} - \mu_1\right) = N\left(-2i - \frac{1}{2}k + 2i\right) = N\left(\frac{-1}{2}k\right) = \frac{1}{4} < 1.$$

Dakle, možemo staviti $\mu := \mu_1 = -2i$,

$$p = \alpha - \mu_1\beta = 4j + 1 + 2i \cdot 2k = 4j + 1 - 4j = 1.$$

Tada je $\alpha = -2i \cdot 2k + 1$.

Budući da je množenje kvaterniona općenito nekomutativno u prstenu $\mathbf{H}$, razlikujemo desnog i lijevog djelitelja.

Definicija 4.1.8. *Kažemo da je $\delta \in \boldsymbol{H}$ **desni djelitelj** Hurwitzovog cijelog broja α ako je*

$$\alpha = \gamma\delta \text{ za neki } \gamma \in \boldsymbol{H}.$$

Ako $\alpha, \beta \in \mathbf{H}$ imaju zajedničkog desnog djelitelja $\delta \in \mathbf{H}$, onda vrijedi:

$$\alpha = \gamma\delta,\ \beta = \epsilon\delta \text{ za neke } \gamma, \epsilon \in \mathbf{H}.$$

Nadalje, ako je δ desni djelitelj Hurwitzovih kvaterniona α i β, tada je δ također desni djelitelj ostatka p pri dijeljenju α s β:

$$\alpha = \mu\beta + p \Rightarrow p = \alpha - \mu\beta = \gamma\delta - \mu\epsilon\delta = (\gamma - \mu\epsilon)\delta.$$

Definicija 4.1.9. *Neka su $\alpha, \beta \in \boldsymbol{H}\backslash\{0\}$. **Desni najveći zajednički djelitelj** od α i β je desni djelitelj δ od α i β sa sljedećim svojstvom: svaki desni djelitelj γ od α i β desni je djelitelj od δ.*

Lema 4.1.10. *Neka su $\alpha, \beta \in \boldsymbol{H}\backslash\{0\}$. Neka su δ i δ' desni najveći zajednički djelitelji od α i β. Tada postoji jedinični Hurwitzov kvaternion ω takav da je $\delta' = \omega\delta$.*

Dokaz. Iz definicije 4.1.9 slijedi da je δ desni djelitelj od δ' i da je δ' desni djelitelj od δ, dakle postoje $\omega, \omega' \in \mathbf{H}$ takvi da je $\delta' = \omega\delta$ i $\delta = \omega'\delta'$.
Imamo

$$\delta' = \omega\delta = \omega\omega'\delta',$$

odakle množenjem zdesna s δ'^{-1} slijedi da je

$$\omega\omega' = 1,$$

dakle

$$N(\omega)N(\omega') = 1.$$

S obzirom da su $N(\omega)N(\omega') \in \mathbb{Z}_{\geq 0}$, slijedi

$$N(\omega) = N(\omega') = 1,$$

dakle ω i ω' su jedinični Hurwitzovi kvaternioni.
Kako je $\delta' = \omega\delta$ ovo dokazuje tvrdnju. □

Lema 4.1.10 pokazuje da je desni najveći zajednički djelitelj δ od $\alpha, \beta \in \mathbf{H} \backslash \{0\}$ jedinstven do na množenje jediničnim Hurwitzovim kvaternionom. Pomalo neprecizno (jer δ nije jedinstven), označavat ćemo ga s

$$desni\ NZD(\alpha, \beta).$$

Njegova egzistencija može se dokazati pomoću Euklidova algoritma:

Teorem 4.1.11. *(Euklidov algoritam za Hurwitzove kvaternione) Neka su $\alpha, \beta \in \boldsymbol{H} \backslash \{0\}$. Uzastopnom primjenom teorema o dijeljenju s ostatkom u* $\mathbf{H}$ *dobivamo niz jednakosti*

$$\begin{array}{lll}
(N_1) & \alpha = \mu_1\beta + p_1, & 0 < N(p_1) < N(\beta), \\
(N_2) & \beta = \mu_2 p_1 + p_2, & 0 < N(p_2) < N(p_1), \\
(N_3) & p_1 = \mu_3 p_2 + p_3, & 0 < N(p_3) < N(p_2), \\
\vdots & & \\
(N_n) & p_{n-2} = \mu_n p_{n-1} + p_n, & 0 < N(p_n) < N(p_{n-1}), \\
(N_{n+1}) & p_{n-1} = \mu_{n+1} p_n. &
\end{array}$$

Vrijedi

$$desni\ NZD(\alpha, \beta) = p_n, \tag{4.1}$$

dakle desni $NZD(\alpha, \beta)$ je posljednji ostatak različit od nule.

Dokaz. Primijetimo najprije da je niz jednakosti $(N_i)_i$ konačan (tj. nakon konačno mnogo dijeljenja s ostatkom dobivamo ostatak 0) jer je niz $(N(p_i))$ strogo padajući niz u $\mathbb{Z}_{\geq 0}$ pa je nužno konačan.
Dokažimo sad (4.1). Po definiciji 4.1.9 trebamo dokazati:

1. p_n je desni djelitelj od α i β.

2. Svaki desni djelitelj γ od α i β desni je djelitelj od p_n.

Dokaz 1:

$$
\begin{aligned}
&\text{Iz } (N_{n+1}) \text{ slijedi da je } p_n \text{ desni djelitelj od } p_{n-1}\text{. Nadalje,}\\
&\overset{N_n}{\Longrightarrow} \; p_n \text{ je desni djelitelj od } p_{n-1} \text{ i } p_{n-2},\\
&\overset{N_{n-1}}{\Longrightarrow} \; p_n \text{ je desni djelitelj od } p_{n-2} \text{ i } p_{n-3},\\
&\overset{N_{n-2}}{\Longrightarrow} \; \ldots\\
&\vdots\\
&\overset{N_3}{\Longrightarrow} \; p_n \text{ je desni djelitelj od } p_2 \text{ i } p_1,\\
&\overset{N_2}{\Longrightarrow} \; p_n \text{ je desni djelitelj od } p_1 \text{ i } \beta,\\
&\overset{N_1}{\Longrightarrow} \; p_n \text{ je desni djelitelj od } \beta \text{ i } \alpha,
\end{aligned}
$$

pa je prva tvrdnja dokazana.
Dokaz 2:

$$
\begin{aligned}
&\text{Neka je } \gamma \text{ desni djelitelj od } \alpha \text{ i } \beta\text{. Implikacije povlače}\\
&\overset{N_1}{\Longrightarrow} \; \gamma \text{ je desni djelitelj od } \beta \text{ i } p_1,\\
&\overset{N_2}{\Longrightarrow} \; \gamma \text{ je desni djelitelj od } p_1 \text{ i } p_2,\\
&\vdots\\
&\overset{N_n}{\Longrightarrow} \; \gamma \text{ je desni djelitelj od } p_{n-1} \text{ i } p_n,
\end{aligned}
$$

čime je teorem dokazan. □

Lema 4.1.12. *Neka su $\alpha, \beta \in \boldsymbol{H} \backslash \{0\}$. Tada postoje $\mu, \nu \in \mathbf{H}$ takvi da je*

$$desni\ NZD(\alpha, \beta) = \mu\alpha + \nu\beta.$$

Dokaz. Sjetimo se da vrijedi (4.1). Uz oznake iz teorema 4.1.11, iz jednakosti (N_n) vidimo da je

$$p_n = p_{n-2} - \mu_n p_{n-1},$$

dakle

$$desni\ NZD(\alpha, \beta) = \delta_1 p_{n-2} + \epsilon_1 p_{n-1} \tag{4.2}$$

za neke $\delta_1, \epsilon_1 \in \mathbf{H}$.
Sada izražavanjem p_{n-1} iz jednakosti

$$(N_{n-1}) \qquad p_{n-3} = \mu_{n-1} p_{n-2} + p_{n-1}$$

i uvrštavanjem dobivenog izraza u (4.1) dobivamo

$$\begin{aligned} desni\ NZD(\alpha,\beta) &= \delta_1 p_{n-2} + \epsilon_1 (p_{n-3} - \mu_{n-1} p_{n-2}) \\ &= \epsilon_1 p_{n-3} + (\delta_1 - \epsilon_1 \mu_{n-1}) p_{n-2}, \end{aligned}$$

dakle

$$desni\ NZD(\alpha,\beta) = \delta_2 p_{n-3} + \epsilon_2 p_{n-2} \text{ za neke } \delta_2, \epsilon_2 \in \mathbf{H}.$$

$$\vdots$$

$$\begin{aligned} &\overset{N_3}{\Longrightarrow} desni\ NZD(\alpha,\beta) = \delta_{n-2} p_1 + \epsilon_{n-2} p_2 \text{ za neke } \delta_{n-2}, \epsilon_{n-2} \in \mathbf{H}, \\ &\overset{N_2}{\Longrightarrow} desni\ NZD(\alpha,\beta) = \delta_{n-1} \beta + \epsilon_{n-1} p_1 \text{ za neke } \delta_{n-1}, \epsilon_{n-1} \in \mathbf{H}, \\ &\overset{N_1}{\Longrightarrow} desni\ NZD(\alpha,\beta) = \delta_n \alpha + \epsilon_n \beta \text{ za neke } \delta_n, \epsilon_n \in \mathbf{H} \end{aligned}$$

što dokazuje tvrdnju. □

Primjer 4.1.13. *Odredimo pomoću Euklidovog algoritma desni* $NZD(2j + 8k, -4 + 2j)$.

Označimo $\alpha := 2j + 8k, \beta := -4 + 2j$.
<u>1. korak:</u> Kao u dokazu teorema 4.1.6 podijelimo α *s* β *s ostatkom. Imamo*

$$\alpha\beta^{-1} = \alpha \frac{\overline{\beta}}{N(\beta)} = (2j + 8k) \frac{-4 - 2j}{20} = \frac{1}{5} + \frac{4}{5} i - \frac{2}{5} j - \frac{8}{5} k.$$

Budući da koordinate od $\alpha\beta^{-1}$ *nisu sve u* $\frac{1}{2} + \mathbb{Z}$*, za količnik* μ_1 *možemo uzeti kvaternion s cjelobrojnim koordinatama koje su najbliže moguće odgovarajućim koordinatama od* $\alpha\beta^{-1}$*, dakle stavimo*

$$\mu_1 = i - 2k$$

pa je ostatak p_1 *dan s*

$$p_1 = \alpha - \mu_1 \beta = (2j + 8k) - (i - 2k)(-4 + 2j) = 2j - 2k.$$

Dakle, jednakost (N_1) *u ovom primjeru glasi:*

$$2j + 8k = (i - 2k) \cdot (-4 + 2j) + (2j - 2k).$$

<u>2. korak:</u> Podijelimo β s p_1 s ostatkom. Imamo

$$\beta p_1^{-1} = \beta \frac{\overline{p_1}}{N(p_1)} = (-4 + 2j)\frac{-2j + 2k}{8} = \frac{1}{2} + \frac{1}{2}i + j - k.$$

Kao u 1. koraku za količnik μ_2 možemo uzeti kvaternion s cjelobrojnim kooridnatama koje su najbliže moguće odgovarajućim koorinatama od βp_1^{-1}, dakle bilo koji od kvaterniona

$$j - k, \quad 1 + j - k, \quad i + j - k, \quad 1 + i + j - k.$$

Stavimo primjerice

$$\mu_2 = j - k$$

pa je ostatak p_2 dan s

$$p_2 = \beta - \mu_2 p_1 = -4 + 2j - (j - k)(2j - 2k) = 2j.$$

Prema tome, jednakost (N_2) u ovom primjeru glasi:

$$-4 + 2j = (j - k) \cdot (2j - 2k) + 2j.$$

<u>3. korak:</u> Podijelimo p_1 s p_2 s ostatkom. Imamo

$$p_1 p_2^{-1} = p_1 \frac{\overline{p_2}}{N(p_2)} = (2j - 2k)\frac{-2j}{4} = 1 - i \in \mathbf{H}$$

pa možemo staviti

$$\mu_3 := 1 - i$$
$$p_3 := 0.$$

Dakle, jednakost (N_3) u ovom primjeru glasi:

$$2j - 2k = (1 - i) \cdot 2j + 0.$$

Kako je $p_3 = 0$ ovime je Euklidov algoritam završen. Prema teoremu 4.1.11

$$\textit{desni NZD}(\alpha, \beta) = p_2 = 2j.$$

Teorem o četiri kvadrata

Kako bismo dokazali Lagrangeov teorem o četiri kvadrata, iskazat ćemo i dokazati nekoliko pomoćnih tvrdnji potrebnih za dokaz samog teorema.

Propozicija 4.1.14. *Neka je $p \in \mathbb{R}$ Hurwitzov prost broj. Ako p dijeli produkt Hurwitzovih cijelih brojeva $\alpha \cdot \beta$, tada p dijeli α ili p dijeli β.*

Dokaz. Pretpostavimo da p ne dijeli α, a dijeli $\alpha \cdot \beta$. Tada su p i α relativno prosti, tj.

$$1 = desni\ NZD(p, \alpha) = \mu p + \nu\alpha,\ \ za\ neke\ \mu, \nu \in \mathbf{H}.$$

Množenjem zdesna dobivamo

$$\beta = \mu p\beta + \nu\alpha\beta.$$

Kako p očito dijeli $\mu p\beta$ i po pretpostavci p dijeli $\nu\alpha\beta$, tada p dijeli i lijevu stranu, odnosno p dijeli β.

Analogno se dokaže za pretpostavku da p ne dijeli β, čime je tvrdnja dokazana. □

Propozicija 4.1.15. *(Uvjet teorema o četiri kvadrata) Neka je p prost broj koji nije Hurwitzov prost broj, tada:*

$$p = a^2 + b^2 + c^2 + d^2\ za\ neke\ a, b, c, d\ \in \mathbb{Z}.$$

Dokaz. Neka je $p = p + 0i + 0j + 0k$ prost broj koji nije Hurwitzov prost broj. Tada ga možemo faktorizirati na sljedeći način:

$$p = \alpha\beta$$

gdje su $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ i $\beta = b_0 + b_1 i + b_2 j + b_3 k$ dva Hurwitzova kvaterniona norme strogo veće od 1. Norme kvaterniona p, α, β su cijeli brojevi. Dakle, imamo:

$$N(p) = p^2 = N(\alpha\beta) = N(\alpha)N(\beta),$$

pri čemu su $N(\alpha) > 1$ i $N(\beta) > 1$ cijeli brojevi. Prema tome, obje norme $N(\alpha)$ i $N(\beta)$ jednake su p. Tada imamo:

$$p = N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2,$$

čime je tvrdnja dokazana u slučaju kad α ima cjelobrojne koeficijente.

Ako je α kvaternion koji za koeficijente ima polovine neparnih cijelih brojeva, možemo ga zamijeniti drugim Hurwitzovim kvaternionom na sljedeći način. Izaberemo $\omega = \frac{\pm 1 \pm i \pm j \pm k}{2}$ tako da $\gamma := \omega + \alpha$ ima parne cjelobrojne koeficijente. Tada je $\alpha = \gamma - \omega$, odnosno

$$\begin{aligned} p = N(\alpha) &= (\overline{\gamma - \omega})(\gamma - \omega) \\ &= (\overline{\gamma} - \overline{\omega})\omega \cdot \overline{\omega}(\gamma - \omega) \\ &= (\overline{\gamma}\omega - 1)(\overline{\omega}\gamma - 1) \\ &= N(\overline{\omega}\gamma - 1), \end{aligned}$$

gdje $\overline{\omega}$ ima polovine, a γ ima parne koeficijente. Samim time $\overline{\omega} \cdot \gamma$ ima cjelobrojne koeficijente, odnosno i $\alpha = \overline{\omega} \cdot \gamma - 1$ ima cjelobrojne koeficijente. □

Propozicija 4.1.16. *Neka je p neparan prost broj. Tada postoje $x, y \in \mathbb{Z}$ takvi da p dijeli $1 + x^2 + y^2$.*

Dokaz. Promotrimo brojeve

$$0^2, 1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2.$$

Nikoja dva među njima nisu kongruentna modulo p. Jednako vrijedi i za brojeve

$$-1 - 0^2, -1 - 1^2, -1 - 2^2, \dots, -1 - \left(\frac{p-1}{2}\right)^2.$$

Ovdje smo naveli ukupno $\frac{p+1}{2} + \frac{p+1}{2} = p + 1$ brojeva pa po Dirichletovom principu dva među njima daju isti ostatak pri dijeljenju s p. Što znači da postoje $x, y \in \left\{0, 1, 2, ..., \frac{p-1}{2}\right\}$ takvi da je $x^2 \equiv -1 - y^2 \pmod{p}$, tj $1 + x^2 + y^2 \equiv 0 \pmod{p}$. □

Propozicija 4.1.17. *Neka su $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2 \in \mathbb{Z}$. Tada je*

$$\left(a_1^2 + b_1^2 + c_1^2 + d_1^2\right)\left(a_2^2 + b_2^2 + c_2^2 + d_2^2\right) = A^2 + B^2 + C^2 + D^2$$

za neke $A, B, C, D \in \mathbb{Z}$.

Dokaz. Definiramo Hurwitzove kvaternione $\alpha, \beta \in \mathbf{H}$, $\alpha = a_1 + b_1 i + c_1 j + d_1 k$ i $\beta = a_2 + b_2 i + c_2 j + d_2 k$.
Očito je

$$\alpha\beta = A + Bi + Cj + Dk$$

za neke $A, B, C, D \in \mathbb{Z}$. Prema propoziciji 3.1.14 imamo

$$N(\alpha)N(\beta) = N(\alpha\beta),$$

tj.

$$\left(a_1^2 + b_1^2 + c_1^2 + d_1^2\right)\left(a_2^2 + b_2^2 + c_2^2 + d_2^2\right) = A^2 + B^2 + C^2 + D^2,$$

što dokazuje tvrdnju. □

Teorem 4.1.18. *(Lagrangeov teorem o četiri kvadrata) Svaki prirodan broj n se može prikazati kao suma kvadrata četiri cijela broja, tj.*

$$n = A^2 + B^2 + C^2 + D^2 \quad \textit{za neke } A, B, C, D \in \mathbb{Z}.$$

Dokaz. Prema propoziciji 4.1.17 produkt dva broja koja su sume četiri kvadrata je suma četiri kvadrata cijelih brojeva. Kako se svaki prirodan broj na jedinstven način može prikazati kao produkt prostih brojeva, preostaje nam teorem dokazati za sve proste brojeve.

Budući da je 2 jedini paran prost broj i da ga je moguće zapisati kao $2 = 0^2+0^2+1^2+1^2$, vidimo da teorem za njega vrijedi. Preostaje nam dokazati da se svaki neparan prost broj p može prikazati kao suma četiri kvadrata.

Prema propoziciji 4.1.16 svaki neparan prost broj p dijeli sumu $1 + x^2 + y^2$ za neke $x, y \in \mathbb{Z}$. Faktorizirajmo tu sumu u produkt Hurwitzovih cijelih brojeva:

$$1 + x^2 + y^2 = (1 - xi - yj)(1 + xi + yj),$$

prema tome p dijeli i ovaj produkt. Ako je p Hurwitzov prost broj, tada prema propoziciji 4.1.14 slijedi da p dijeli $1 - xi - yj$ ili p dijeli $1 + xi + yj$. No, nijedna od tih tvrdnji nije točna jer niti jedan od brojeva

$$\frac{1}{p} - \frac{xi}{p} - \frac{yj}{p}, \ \frac{1}{p} + \frac{xi}{p} + \frac{yj}{p}$$

nije Hurwitzov cijeli broj. Stoga, naš proizvoljan neparan prost p nije Hurwitzov prost broj pa prema propoziciji 4.1.15 slijedi da se p može prikazati kao suma četiri kvadrata. Preciznije,

$$p = a^2 + b^2 + c^2 + d^2 \ \textit{ za neke } a, b, c, d \in \mathbb{Z}.$$

Ovime smo pokazali da se svaki prirodan broj n može prikazati u obliku sume četiri kvadrata cijelih brojeva:

$$n = A^2 + B^2 + C^2 + D^2 \ \textit{ za neke } A, B, C, D \in \mathbb{Z}.$$

□

4.2 Kvaternioni i rotacije

Vektorski zapis kvaterniona

Dosad smo vidjeli dva različita zapisa kvaterniona $q \in \mathbb{H}$, opći zapis $q = a + bi + cj + dk$ te zapis pomoću 2×2 kompleksnih matrica. U ovom poglavlju kvaternion q prikazat ćemo kao zbroj skalara i vektora na sljedeći način:

$$q = a + bi + cj + dk = a + \mathbf{q},$$

gdje je a **skalarni (realni)** dio, a $\mathbf{q} = bi + cj + dk$ **vektorski** dio kvaterniona q.

Definirajući kvaternione na ovaj način, svaki kvaternion $q \in \mathbb{H}$ oblika $q = a + 0i + 0j + 0k = a$ možemo identificirati s realnim brojem. Takve kvaternione zovemo **realni kvaternioni**. Jasno je da je produkt realnih kvaterniona realan kvaternion te da je množenje realnih kvaterniona komutativno i asocijativno.

Definicija 4.2.1. *Kvaternion oblika $q = bi + cj + dk$ naziva se **vektorski (imaginarni) kvaternion**. Skup*

$$\Im(\mathbb{H}) = \{bi + cj + dk | b, c, d \in \mathbb{R}\} = \{q \in \mathbb{H} | q + \overline{q} = 0\}$$

*naziva se **skup imaginarnih kvaterniona**.*

Skup vektorskih kvaterniona očito je potprostor od $\mathbb{H}$ izomorfan sa $\mathbb{R}^3$, tj. $\Im(\mathbb{H}) \equiv \mathbb{R}^3$. Prema prethodno navedenom, prostor kvaterniona može se predstaviti kao:

$$\mathbb{H} = \mathbb{R} \oplus \Im(\mathbb{H}) = \mathbb{R} \oplus \mathbb{R}^3.$$

Produkt realnog i vektorskog kvaterniona je vektorski kvaternion. Takvo množenje je komutativno jer prema definiciji množenja kvaternioni komutiraju sa skalarima.

Skalarni i vektorski produkt kvaterniona

Definicija 4.2.2. ***Skalarni produkt** kvaterniona $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ i $q_2 = a_2 + b_2 i + c_2 j + d_2 k$ je realan broj definiran na sljedeći način:*

$$q_1 \circ q_2 = a_1 a_2 + b_1 b_2 + c_1 c_2 + d_1 d_2 = \frac{q_1 \overline{q_2} + q_2 \overline{q_1}}{2}.$$

Definicija 4.2.3. ***Vektorski produkt** kvaterniona $q_1, q_2 \in \Im(\mathbb{H})$ je kvaternion*

$$q_1 \times q_2 = \frac{q_1 q_2 - q_2 q_1}{2}.$$

Budući da smo prostor $\Im(\mathbb{H})$ identificirali s vektorskim prostorom $\mathbb{R}^3$, tako vektorski produkt imaginarnih kvaterniona predstavlja vektorski produkt odgovarajućih vektora u $\mathbb{R}^3$. Prema tome, njegovu definiciju možemo zapisati i pomoću determinanti. Dakle, vektorski produkt kvaterniona $q_1 = b_1 i + c_1 j + d_1 k, q_2 = b_2 i + c_2 j + d_2 k \in \Im(\mathbb{H})$ je:

$$q_1 \times q_2 = \begin{vmatrix} i & j & k \\ b_1 & c_1 & d_1 \\ b_2 & c_2 & d_2 \end{vmatrix} = (c_1 d_2 - c_2 d_1)i - (b_1 d_2 - b_2 d_1)j + (b_1 c_2 - b_2 c_1)k.$$

Poznavajući skalarni i vektorski produkt kvaterniona, možemo izvesti elegantniju formulu za množenje dva kvaterniona. Prema definiciji 3.1.4 umnožak kvaterniona q_1 i q_2 dan je s

$$\begin{aligned} q_1 \cdot q_2 &= (a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k) \\ &= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i \\ &+ (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) j + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2) k. \end{aligned}$$

Ako kvaternion q_1 zapišemo kao $q_1 = a_1 + \mathbf{q_1}$, a kvaternion q_2 kao $q_2 = a_2 + \mathbf{q_2}$, gdje su $\mathbf{q_1} = b_1 i + c_1 j + d_1 k$ i $\mathbf{q_2} = b_2 i + c_2 j + d_2 k$, tada umnožak $q_1 \cdot q_2$ možemo zapisati na sljedeći način:

$$\begin{aligned} q_1 \cdot q_2 &= a_1 a_2 - (b_1 b_2 + c_1 c_2 + d_1 d_2) + a_1 (b_2 i + c_2 j + d_2 k) + a_2 (b_1 i + c_1 j + d_1 k) \\ &+ (c_1 d_2 - c_2 d_1) i + (b_2 d_1 - b_1 d_2) j + (b_1 c_2 - b_2 c_1) k. \\ &= a_1 a_2 - \mathbf{q_1} \circ \mathbf{q_2} + a_1 \mathbf{q_2} + a_2 \mathbf{q_1} + \mathbf{q_1} \times \mathbf{q_2}. \end{aligned}$$

Specijalno, ako su $q_1, q_2 \in \Im(\mathbb{H})$, odnosno ako su $a_1 = a_2 = 0$, tada je

$$q_1 \cdot q_2 = -\mathbf{q_1} \circ \mathbf{q_2} + \mathbf{q_1} \times \mathbf{q_2}. \tag{4.3}$$

Produkt dva vektorska kvaterniona je opći kvaternion, osim u dva posebna slučaja:

- ako su vektori $\mathbf{q_1}$ i $\mathbf{q_2}$ kolinearni, onda je produkt $q_1 \cdot q_2$ realni kvaternion oblika $-\mathbf{q_1} \circ \mathbf{q_2}$,
- ako su vektori $\mathbf{q_1}$ i $\mathbf{q_2}$ okomiti, onda je produkt $q_1 \cdot q_2$ vektorski kvaternion oblika $\mathbf{q_1} \times \mathbf{q_2}$.

Definicija 4.2.4. *Kažemo da su kvaternioni $q_1, q_2 \in \mathbb{H}$ **paralelni** ako su njihovi vektorski dijelovi kolinearni, tj. ako vrijedi $\mathbf{q_1} \times \mathbf{q_2} = 0$.*

Definicija 4.2.5. *Kažemo da su kvaternioni $q_1, q_2 \in \mathbb{H}$ **okomiti** ako su njihovi vektorski dijelovi okomiti, tj. ako vrijedi $\mathbf{q_1} \circ \mathbf{q_2} = 0$.*

Jedinični kvaternioni

Definicija 4.2.6. *Kvaternion $q = a + bi + cj + dk \in \mathbb{H}$ kod kojeg vrijedi*

$$N(q) = a^2 + b^2 + c^2 + d^2 = 1,$$

*nazivamo **jedinični (normirani) kvaternion**.*

Lema 4.2.7. *Svaki jedinični kvaternion $q = a + bi + cj + dk$ može se prikazati u obliku*

$$q = \cos\phi + \mathbf{u}\sin\phi,$$

gdje je $\mathbf{u}$ *jedinični vektorski kvaternion, a* $\phi \in [0, \pi]$.

Dokaz. Razložimo kvaternion q na skalarni i vektorski dio na sljedeći način:

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

gdje su $q_0 = a$ i $\mathbf{q} = bi + cj + dk$.
Kako je q kvaternion norme 1, možemo pisati

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

Prema tome postoji kut ϕ takav da vrijedi

$$q_0^2 = \cos^2\phi, \quad |\mathbf{q}|^2 = \sin^2\phi.$$

Odnosno, postoji jedinstven kut $\phi \in [0, \pi]$ takav da

$$q_0 = \cos\phi, \quad |\mathbf{q}| = \sin\phi.$$

Dakle, svaki jedinični kvaternion q može se zapisati u obliku

$$q = \cos\phi + \mathbf{u}\sin\phi,$$

gdje su $\mathbf{u} \in \mathbb{H}$ i $\phi \in [0, \pi]$ određeni uvjetima

$$\mathbf{u} = \begin{cases} \frac{\mathbf{q}}{|\mathbf{q}|}, & \text{ako je } \mathbf{q} \neq 0, \\ \text{proizvoljan jedinični kvaternion}, & \text{ako je } \mathbf{q} = 0 \end{cases}$$

i

$$\begin{cases} \cos\phi = q_0 \\ \sin\phi = |\mathbf{q}|. \end{cases}$$

□

Obratno, imamo sljedeću lemu:

Lema 4.2.8. *Neka su* $\mathbf{u}$ *jedinični vektorski kvaternion i* $\phi \in \mathbb{R}$. *Tada je* $q := \cos\phi + \mathbf{u}\sin\phi \in \mathbb{H}$ *jedinični kvaternion.*

Dokaz. Imamo

$$\begin{aligned}
N(q) &= q \cdot \overline{q} \\
&= (\cos\phi + \mathbf{u}\sin\phi)\left(\overline{\cos\phi + \mathbf{u}\sin\phi}\right) \\
&= (\cos\phi + \mathbf{u}\sin\phi)(\cos\phi + \overline{\mathbf{u}}\sin\phi) \\
&= \cos^2\phi + \overline{\mathbf{u}}\sin\phi\cos\phi + \mathbf{u}\sin\phi\cos\phi + \mathbf{u}\overline{\mathbf{u}}\sin^2\phi \\
&= \cos^2\phi + \sin^2\phi + \sin\phi\cos\phi(\mathbf{u} + \overline{\mathbf{u}}) \\
&= \cos^2\phi + \sin^2\phi \\
&= 1.
\end{aligned}$$

□

Rotacije

Pomoću jediničnih kvaterniona opisujemo rotacije vektora u prostoru. Sjetimo se (vidi poglavlje 1) da je skup

$$V^3 := \left\{ b\vec{i} + c\vec{j} + d\vec{k} : \ b, c, d \in \mathbb{R} \right\}$$

vektora u prostoru trodimenzionalni realni unitarni prostor sa skalarnim produktom $\circ : V^3 \times V^3 \to \mathbb{R}$,

$$\left(b_1\vec{i} + c_1\vec{j} + d_1\vec{k}\right) \cdot \left(b_2\vec{i} + c_2\vec{j} + d_2\vec{k}\right) := b_1b_2 + c_1c_2 + d_1d_2,$$

pripadnom normom $\|\cdot\| : V^3 \to \mathbb{R}_{\geq 0}$,

$$\left\| b_1\vec{i} + c_1\vec{j} + d_1\vec{k} \right\| = \sqrt{b_1^2 + c_1^2 + d_1^2}$$

i vektorskim produktom $\times : V^3 \times V^3 \to V^3$,

$$\left(b_1\vec{i} + c_1\vec{j} + d_1\vec{k}\right) \times \left(b_2\vec{i} + c_2\vec{j} + d_2\vec{k}\right) := \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ b_1 & c_1 & d_1 \\ b_2 & c_2 & d_2 \end{vmatrix} = (c_1d_2 - c_2d_1)\vec{i} - (b_1d_2 - b_2d_1)\vec{j} + (b_1c_2 - b_2c_1)\vec{k},$$

$b_1, c_1, d_1, b_2, c_2, d_2 \in \mathbb{R}$.
Iz naših definicija jasno je da vrijedi:

Lema 4.2.9. *Pravilo*

$$b\vec{i} + c\vec{j} + d\vec{k} \mapsto bi + cj + dk, \quad b, c, d \in \mathbb{R} \tag{4.4}$$

definira unitarni izomorfizam

$$V^3 \to \Im(\mathbb{H})$$

koji čuva vektorski produkt.

Lema 4.2.9 pokazuje da korespodencijom (4.4) možemo identificirati vektore u prostoru s vektorskim kvaternionima. Pritom skalarni i vektorski produkt ostaju očuvani. Nadalje:

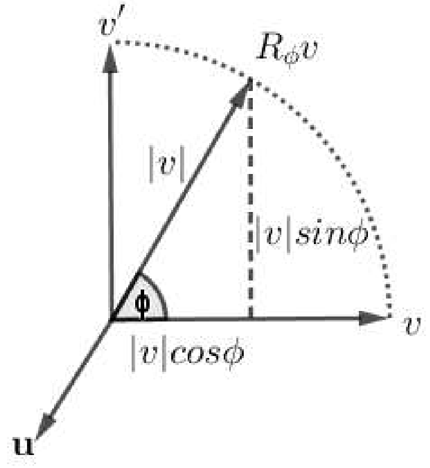
Lema 4.2.10. *Neka je $v \in V^3 \equiv \Im(\mathbb{H})$. Tada je v **jedinični vektor** u V^3 (tj. $\|v\| = 1$) ako i samo ako je v jedinični kvaternion.*

Dokaz. Zapišimo
$$v = b\vec{i} + c\vec{j} + d\vec{k} \equiv bi + cj + dk,$$
gdje su $b, c, d \in \mathbb{R}$. Imamo sljedeći niz ekvivalencija:
$$\|v\| = 1 \iff \sqrt{b^2 + c^2 + d^2} = 1 \iff b^2 + c^2 + d^2 = 1 \iff N(v) = 1.$$
Ovo dokazuje tvrdnju. □

Najprije promotrimo rotaciju okomitog vektora oko jediničnog vektora.

Lema 4.2.11. *Neka su $\mathbf{u}$ jedinični vektorski kvaternion (tj. jedinični vektor u V^3) i $\phi \in \mathbb{R}$. Neka je $v \in \Im(\mathbb{H}) \equiv V^3$ takav da vrijedi $v \perp \mathbf{u}$. Označimo*
$$q = \cos\phi + \mathbf{u}\sin\phi \ \in \mathbb{H}.$$
Tada je vektor
$$qv = (\cos\phi + \mathbf{u}\sin\phi)\, v = v\cos\phi + \mathbf{u}v\sin\phi \tag{4.5}$$
rotacija vektora v za kut ϕ oko $\mathbf{u}$ u pozitivnom smjeru.

Dokaz. Označimo
$$v' := \mathbf{u} \cdot v.$$
Po formuli (4.3) vrijedi
$$v' = -\mathbf{u} \circ v + \mathbf{u} \times v.$$
Iz okomitosti $\mathbf{u}$ i v slijedi da je $\mathbf{u} \circ v = 0$, dakle $v' = \mathbf{u} \times v$. Prema tome, v' je vektor duljine
$$|\mathbf{u}| \cdot |v| \cdot |\sin \measuredangle(\mathbf{u}, v)| = 1 \cdot |v| \cdot \left|\sin\frac{\pi}{2}\right| = |v|$$
koji je okomit na $\mathbf{u}$ i v i ima jednaku orijentaciju u odnosu na $\mathbf{u}$ i v kakvu ima vektor $\vec{k}$ u odnosu na $\vec{i}$ i $\vec{j}$. Sa slike 4.1 vidimo da je rotacija $R_\phi v$ vektora v za kut ϕ oko $\mathbf{u}$ dana s:
$$\begin{aligned} R_\phi v &= |v|\cos\phi \cdot \frac{v}{|v|} + |v|\sin\phi \cdot \frac{v'}{|v'|} \\ &= \cos\phi \cdot v + \sin\phi \cdot v' \\ &\overset{(4.5)}{=} qv. \end{aligned}$$
□



Slika 4.1: Rotacija vektora v za kut ϕ

Lema 4.2.12. *Neka su $q_1, q_2 \in \Im(\mathbb{H})$ međusobno okomiti. Tada je*

$$q_1 q_2 = -q_2 q_1.$$

Dokaz. Prema (4.3) imamo:

$$\begin{aligned} q_1 q_2 &= -q_1 \circ q_2 + q_1 \times q_2 \\ &= q_1 \times q_2 \\ &= -q_2 \times q_1 \\ &= -(-q_2 \circ q_1 + q_2 \times q_1) \\ &= -q_2 q_1. \end{aligned}$$

□

Lema 4.2.13. *Neka su $\mathbf{u}$ jedinični vektorski kvaternion i $\phi \in \mathbb{R}$. Neka je $v \in \Im(\mathbb{H}) \equiv V^3$ takav da vrijedi $v \perp \mathbf{u}$. Označimo*

$$q = \cos\phi + \mathbf{u}\sin\phi \ \in \mathbb{H}.$$

Tada je vektor

$$vq^{-1} = v\cos\phi + \mathbf{u}v\sin\phi$$

rotacija vektora v za kut ϕ oko $\mathbf{u}$ u pozitivnom smjeru, gdje je q^{-1} inverz kvaterniona q.

Dokaz. Prema lemi 4.2.8 $N(q) = 1$, stoga je inverz q^{-1} dan s:

$$q^{-1} = \frac{\overline{q}}{N(q)} = \overline{q} = \overline{\cos\phi + \mathbf{u}\sin\phi} = \cos\phi - \mathbf{u}\sin\phi.$$

Množenjem i primjenjivanjem leme 4.2.12 imamo

$$\begin{aligned} vq^{-1} &= v(\cos\phi - \mathbf{u}\sin\phi) \\ &= v\cos\phi - v\mathbf{u}\sin\phi \\ &= v\cos\phi + \mathbf{u}v\sin\phi. \end{aligned}$$

što prema lemi 4.2.11 predstavlja rotaciju vektora v za kut ϕ oko $\mathbf{u}$ u pozitivnom smjeru. □

Korolar 4.2.14. *Neka su $\mathbf{u}$ jedinični vektorski kvaternion i $\phi \in \mathbb{R}$. Neka je $v \in \Im(\mathbb{H}) \equiv V^3$ takav da vrijedi $v \perp \mathbf{u}$ te neka su*

$$q = \cos\phi + \mathbf{u}\sin\phi \;\in \mathbb{H}$$

i

$$q^{-1} = \cos\phi - \mathbf{u}\sin\phi \;\in \mathbb{H}$$

njegov inverz. Tada je vektor

$$qvq^{-1}$$

rotacija vektora v za kut 2ϕ oko $\mathbf{u}$ u pozitivnom smjeru.

Vidjeli smo kako operacija qvq^{-1} rotira okomiti vektor v oko jediničnog vektora $\mathbf{u}$. Promotrimo sada rotaciju proizvoljnog vektora $v \in \Im(\mathbb{H}) \equiv V^3$ oko jediničnog vektora $\mathbf{u}$.

Teorem 4.2.15. *Neka su $\mathbf{u}$ jedinični vektor u V^3 (tj. jedinični vektorski kvaternion) i $\phi \in \mathbb{R}$. Neka je $v \in \Im(\mathbb{H}) \equiv V^3$. Definiramo*

$$q = \cos\phi + \mathbf{u}\sin\phi \;\in \mathbb{H}.$$

Tada je vektor

$$qvq^{-1} \in \Im(\mathbb{H}) \equiv V^3$$

rotacija vektora v oko $\mathbf{u}$ za kut 2ϕ u pozitivnom smjeru.

Dokaz. Prikažimo vektor v kao zbroj vektora w kolinearnog s $\mathbf{u}$ i vektora r okomitog na $\mathbf{u}$ kao što je prikazano na slici 4.2.
Iz trigonometrije pravokutnog trokuta određenog vektorima v, r i w slijedi da je

$$\cos\varphi = \frac{|w|}{|v|} \Rightarrow |w| = \cos\varphi \cdot |v| = \cos\varphi \cdot |v| \cdot |\mathbf{u}| = v \circ \mathbf{u},$$

gdje je $\varphi := \measuredangle(\mathbf{u}, v)$.
Dakle,

$$\begin{aligned} v &= w + r \\ &= (v \circ \mathbf{u})\mathbf{u} + (v - (v \circ \mathbf{u})\mathbf{u}). \end{aligned}$$

Očito je w kolinearan s $\mathbf{u}$. Dokažimo da je r okomit na $\mathbf{u}$:

$$r \circ \mathbf{u} = (v - (v \circ \mathbf{u})\mathbf{u}) \circ \mathbf{u} = v \circ \mathbf{u} - (v \circ \mathbf{u})(\mathbf{u} \circ \mathbf{u}) = v \circ \mathbf{u} - (v \circ \mathbf{u})|\mathbf{u}|^2 = 0.$$

Neka je $R_{2\phi} : V^3 \to V^3$ linearni operator rotacije oko vektora $\mathbf{u}$ za kut 2ϕ u pozitivnom smjeru. Tada je

$$qvq^{-1} = q(w + r)q^{-1} = qwq^{-1} + qrq^{-1}.$$

Kako je $w \parallel \mathbf{u}$, vrijedi $w = \alpha\mathbf{u}$ za neki $\alpha \in \mathbb{R}$ pa imamo

$$qvq^{-1} = q(\alpha\mathbf{u})q^{-1} = \alpha q\mathbf{u}q^{-1} \overset{(4.6)}{=} \alpha\mathbf{u}qq^{-1} = \alpha\mathbf{u} = w = R_{2\phi}w,$$

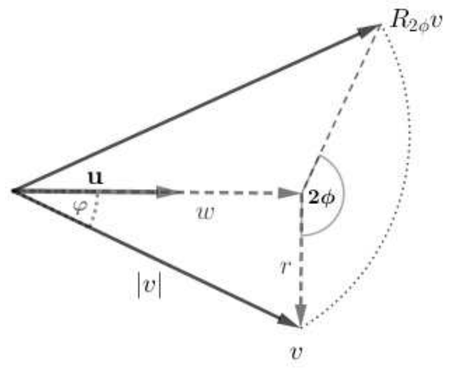
gdje treća jednakost vrijedi jer je

$$q\mathbf{u} = (\cos\phi + \mathbf{u}\sin\phi)\mathbf{u} = \cos\phi \cdot \mathbf{u} + \mathbf{u}\sin\phi \cdot \mathbf{u} = \mathbf{u}\cos\phi + \mathbf{u} \cdot \mathbf{u}\sin\phi = \mathbf{u}(\cos\phi + \mathbf{u}\sin\phi) = \mathbf{u}q. \tag{4.6}$$

Prema lemi 4.2.11 iz $r \perp \mathbf{u}$ slijedi da je $qrq^{-1} = R_{2\phi}r$.
Stoga, zaključujemo da je

$$qvq^{-1} = R_{2\phi}w + R_{2\phi}r = R_{2\phi}(w + r) = R_{2\phi}v,$$

čime je teorem dokazan. □



Slika 4.2: Rotacija vektora v za kut 2ϕ

Bibliografija

[1] K. Conrad, *Quaternion algebras*, dostupno na `https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf` (studeni 2020.).

[2] J. H. Conway i D. A. Smith, *On quaternions and octonions: their geometry, arithmetic, and symmetry*, A K Peters, Ltd., Natick, MA, 2003.

[3] Z. Franušić i J. Šiftar, *Linearna algebra 1, skripta*, dostupno na `https://web.math.pmf.unizg.hr/~fran/predavanja-LA1.pdf` (studeni 2020.).

[4] ______, *Linearna algebra 2, skripta*, dostupno na `https://web.math.pmf.unizg.hr/~fran/predavanja-LA2.pdf` (studeni 2020.).

[5] J. B. Kuipers, *Quaternions and rotation sequences. Proceedings of the International Conference on Geometry, Integrability and Quantization* (urednici: Ivaïlo, M. M., Naber, G. L.), Sofia: Coral Press Scientific Publishing.

[6] Ž. Milin Šipuš i M. Bombardelli, *Analitička geometrija, skripta*, dostupno na `http://www.mathos.unios.hr/analiticka/predavanja.pdf` (studeni 2020.).

[7] J. Stillwell, *Elements of Number Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2003.

[8] L. Vicci, *Quaternions and rotations in 3-space: the algebra and its geometric in- terpretation*, dostupno na `http://www.cs.unc.edu/techreports/01-014.pdf` (studeni 2020.).

Sažetak

U ovom radu izložena su osnovna svojstva algebre kvaterniona i dvije njene primjene. Prva primjena je dokaz Lagrangeova teorema o četirima kvadratima, prema kojemu se svaki prirodan broj može prikazati kao suma kvadrata četiriju cijelih brojeva. Druga primjena je prikaz rotacija u $\mathbb{R}^3$ pomoću kvaterniona.

Summary

In this thesis, the basic properties of the quaternion algebra and its two applications are presented. The first application is the proof of Lagrange's four-square theorem, according to which every natural number can be written as the sum of four integer squares. The second application is representing rotations in $\mathbb{R}^3$ using quaternions.

Životopis

Rođena sam 2. studenog 1996. u Žepču, malom mjestu u središnjoj Bosni. Nakon završetka osnovne škole Žepče, pohađala sam opću gimnaziju u Katoličkom školskom centru Don Bosco u Žepču. Nakon završetka gimnazije, 2015. godine upisala sam preddiplomski sveučilišni studij Matematika; smjer: nastavnički na Prirodoslovno-matematičkom fakultetu u Zagrebu. Nakon završetka istog, 2018. godine upisujem diplomski sveučilišni studij Matematika; smjer: nastavnički.