Szakdolgozat

# Kvaterniók és Cayley-számok

Rőmer Gábor

*Matematika BSc, alkalmazott matematikus szakirány*

Témavezető:

Fialowski Alice
egyetemi docens

**Eötvös Loránd Tudományegyetem**
Természettudományi Kar

Algebra és Számelmélet Tanszék

**2015**

# Tartalomjegyzék

## Célkitűzés

A szakdolgozatom célja, hogy egy rövid számtörténeti áttekintőt követően megvizsgáljuk, miként lehet a komplex számoknál magasabb dimenziós valós algebrákat előállítani, hogyan értelmezhetjük ezen algebrákon a műveleteket, illetve mely műveleti szabályokat vagyunk kénytelenek elhagyni ahhoz, hogy a kvaterniók négydimenziós, illetve a Cayley-számok nyolcdimenziós algebráját megkaphassuk.

Az első fejezetben megkonstruáljuk a kvaterniók algebráját, megnézzük, hogyan állnak elő ezen számok mátrixos alakban, illetve annak segítségével, hogy az előbb említett két struktúra izomorf, belátjuk, hogy a kvaterniók algebrája ferdetest. Ezután nézünk egy példát a kvaterniók alkalmazására, vagyis megvizsgáljuk, hogyan feleltethetők meg a kvaterniók, háromdimenziós vektorok forgatásainak.

A második fejezet elején bevezetjük az alternáló és a kvadratikus algebrák fogalmát, melynek célja, hogy a ferdetestnél általánosabb, a szorzás asszociativitását nélkülöző struktúrát hozzunk létre. Ezek segítségével először bizonyítjuk a Frobenius-tételt, amely kimondja a kvaternió-algebra egyértelműségét, vagyis hogy a valós számok felett nem létezik négynél magasabb dimenziójú ferdetest, majd előállítjuk a Cayley-számok algebráját. Végezetül, a kvaterniókhoz hasonlóan belátjuk, hogy nem bővíthető a dimenziószám úgy, hogy a Cayley-algebra minden tulajdonságát megőrizzük.

A történeti részekhez az [1], [2], [3] és [4] irodalmat használom, a kvaterniók és Cayley-számok tárgyalásában pedig a [5], [6], [7], [8], [9] és [10] forrásokat dolgozom fel.

## Köszönetnyilvánítás

Szeretnék köszönetet mondani a témavezetőmnek, Fialowski Alicenak, aki a felkészülés során mindvégig segítségemre volt az anyag megértésében, kezdettől fogva figyelemmel kísérte és támogatta a munkámat.

## A számfogalom fejlődése

A számról alkotott első fogalmaink egészen a paleolit korszakba nyúlnak vissza. Az akkori emberek barlangokban laktak, és elsősorban elemi szükségleteik kielégítésével foglalkoztak, növényeket és gyümölcsöket gyűjtöttek, vadásztak és halakat fogtak. Idővel fegyvereket és szerszámokat készítettek, kialakították a nyelvet, a gondolatközlés eszközét, majd megjelentek az első, kezdetleges edények, képzőművészeti alkotások, szobrok, festmények. Ez a fajta nomád életmód azonban nem igényelt többet annál, hogy különbséget tudjanak tenni az egy, a kettő és a sok között. A mennyiség és a tér fogalmának megértésében az ember mindaddig keveset haladt, amíg át nem tért a puszta élelemgyűjtésről a földművelésre, a vadászatról és halászatról az állattenyésztésre. Az emberek a folytonos vándorlás helyett letelepedtek, falvakba tömörültek, s addig maradtak egy helyben, amíg a talaj termelőereje ki nem merült. Az állandóbb lakóhelyek időt és lehetőséget biztosítottak, hogy fokozatosan fejlődésnek indulhassanak a kézműves mesterségek, a fazekas, ács és szövőmesterség. Egyszerű épületek, a falu köré falak épültek, hogy védelmet nyújtsanak a rabló ellenség és az időjárás viszontagságai ellen. A megtermelt gabonából kenyeret sütöttek, sört főztek, majd a neolit korszak utolsó szakaszában rezet és bronzot öntöttek, szerszámokat készítettek, majd beindult a falvak közötti cserekereskedelem. A kézművesség és a kereskedelem serkentette a számfogalom kibővülését, az emberek új számokat alkottak, nagyobb egységekbe fűzték őket, rendszerint a kezek ujjainak felhasználásával. Ennek az lett a következménye, hogy kezdetben ötös, majd tízes alapon számoltak, vagyis megjelent az összeadás és néha a kivonás művelete, például a 12-t 10+2-nek, a 9-et 10-1-nek fogták fel. Megjelent az igény a számok feljegyzésére is, amit botba vésett rovásokkal, zsinórra kötött csomókkal, esetleg ötös csoportokba rendezett kagylókkal, kavicsokkal oldottak meg. Idővel az is szükségessé vált, hogy az ember megmérje a tárgyak hosszúságát, űrtartalmát. A mértékegységek durvák voltak, amelyeket gyakran az emberi test részeiről vettek, így keletkeztek az olyan egységek, mint a hüvelyk, láb vagy az arasz. Amikor már házakat építettek, szabályként mondták ki, hogy egyenes vonalban, illetve derékszögben kell építkezni, majd a képzőművészetben is megjelentek az egyre szabályosabb formák, lassan kialakult az érdeklődés a geometria kibővítése iránt.

A matematika gyakorlati tudományként keletkezett, amelyet a kor elvárásai bővítettek. Kezdetben csak tárgyak számosságának, a mértékegységek megjelenésével a darabonként megszámlálhatatlan dolgok mennyiségének adtak az emberek értelmet. A földművelés és építkezés a hosszmérés és területszámítás kialakulását igényelte, amely kibővítette a természetes számok körét a törtekkel, vagyis az arány fogalmával. Kezdetben a fél, mint az egész, a teljesség fele, a harmad és a negyed jelent meg, de az egyiptomi aritmetikában tetszőleges törteket is előállítottak, úgynevezett törzstörtek, azaz $1/n$ alakú számok összegeként, például a $2/7$-et $1/4 + 1/28$ formájában állították elő. Később, amikor már szervezetebb közösségek, városok jöttek létre, a matematika a naptárszámítást, a termés betakarítását és az adózást volt hivatott megkönnyíteni. Ha azonban egy tudományt évszázadokon át egy külön hivatási ág művel, akkor azt egy idő után önmagáért kezdik tanulmányozni. Így fejlődött algebrává az egyszerű aritmetika, és ezen oknál fogva alakult ki a mérésből az elméleti geometria. Idővel, amikor már a hatékonyság, a számolás sebessége is szerepet kapott, használatba került az addig csak felszínesen ismert szorzás művelet és kialakultak a szorzótáblák, amik az addig jellemzően additív számolást voltak hivatottak felgyorsítani. A matematikai elméletek fejlődésének egyik nagyhatású ösztönzője volt az irracionális számok felfedezése, vagyis az összemérhetetlen szakaszok létezésének megállapítása. Ezek közül alighanem a $\sqrt{2}$, vagyis az egységoldalú négyzet átlója volt az első.

Az addig ismert számkör kibővítésének fontos állomása volt a negatív számok megjelenése. Noha a negatív számok mai szemmel nézve elég egyszerű fogalomnak tűnnek, tudatos használatukra utalást csak az időszámításunk kezdetén megjelent, bár később többször kiegészített és átdolgozott, a "Matematika kilenc könyvben" című műben találunk. Ezen írás Kína matematikai eredményeinek sajátos összefoglalása, melynek hetedik könyve a "Felesleg-hiány" címet viseli, ami a lineáris egyenletre és egyenletrendszerre vezető feladatok gyűjteménye. Az ilyen feladatok negatív megoldása a "hiány", amelyet írásban az eredeti számnak megfelelő, de eltérő színű ábrákkal jelöltek. Ezen feladatok vívmánya a nulla is, amely a "semmi", az "egyensúly" jele. Noha ismeretes volt a fogalom, az absztrakt nullával, mint számmal, nagyjából ezer évvel később, Indiában kezdtek foglalkozni az akkori matematikusok, amikor kialakulóban volt az egységes tízes számrendszer.

Valamikor a középkor elején az emberek már jól ismerték a pozitív egészekkel és közönséges törtekkel való számolást, tudták, hogy vannak irracionális számok, fel tudták írni minden szám negatív ellentettjét, kialakulóban volt a nullával való kalkulus, illetve a végtelen fogalma sem volt újdonság, elég csak az ókori görög filozófus, Zénón munkásságára és paradoxonjaira gondolni. Kimondhatjuk tehát, hogy ekkoriban már rendelkezésre állt a teljes számegyenes, azonban a valós számok matematikailag is precíz, axiomatikus felépítésére még sokáig nem került sor. A XIX. század elejére érett meg az elvárás, hogy az addig a tapasztalatokon és megszokáson alapuló számrendszereket egységes és precízen definiált csoportokba foglaljuk. Ezen törekvés első eredménye a természetes számok halmazának, pontosabban félcsoportjának axiomatikus felírása volt, amely Georg Cantor, Gottlob Frege és Giuseppe Peano nevéhez köthető. Innen már természetes módon adódott az egész számok halmazának, Leopold Kronecker által felírt értelmezése. Ezen folyamat csak a XX. század elején ért el következő állomásához, amikor definiálták az algebrai test fogalmát, így a racionális, valós és végül a komplex számok halmaza is precíz értelmezést kapott.

Érdekesség azonban, hogy a komplex számok, a logikusnak tűnő feltételezéssel ellentétben, nem a valós számok pontos definiálása után kerültek előtérbe. Már a reneszánsz korban észrevették, hogy a harmadfokú, vagy némely másodfokú egyenletnek úgynevezett "lehetetlen megoldása" van. Ezen probléma leküzdése szintén a XIX. századra tehető, amikor Carl Friedrich Gauss átfogó geometriai értelmezést, később pedig algebrai felírást adott a komplex számoknak.

# 1. Kvaterniók

## 1.1. A kvaterniók kialakulása

Sir William Rowan Hamilton 1805-ben született Dublinban, azonban hároméves korától nagybátyja, James Hamilton felügyelete alatt nevelkedett. Már kiskorában fény derült az áltag feletti intelligenciájára, ugyanis kitűnő nyelvérzékkel rendelkezett. Ezen tehetségét nyelvész nagybátyja segítségével kamatoztathatta is, már elképesztően fiatalon, ötéves korában latin, görög és héber szövegeket olvasott. Tanulmányait nagybátyja nyomdokain, 1823-tól a Trinity Collegeben végezte, ahol még a diplomájának megszerzése előtt fontos titulusokat tudhatott magáénak. Elnyerte a Csillagászat Andrews-professzora címet, illetve az Írország Királyi Csillagásza címet, amellyel egyidőben betöltötte a Dunsink Obszervatórium igazgatói posztját. Egyetemi évei alatt folytatott tanulmányokat többek között az optika és a dinamika területein is. 1835-ben lovaggá ütötték, majd 1837-től 1845-ig az Ír Királyi Akadémia elnöke volt. A szakdolgozatom témáját képző kvaterniók felfedezésére 1843-ban került sor, amely szinte kizárólagos kutatási témájává vált, egészen az 1865-ben bekövetkező haláláig.

Ahogy a számtörténeti áttekintőből is kiderült, Hamilton munkásságának idején még nem létezett, vagy éppen kialakulóban volt a különböző algebrai struktúrák pontos, axiomatikus definíciója. A szakdolgozatban azonban minden struktúrát a ma ismert definíciójával határozunk meg, mert annak ellenére, hogy akkoriban ez a fajta rendszerezés még nem állt rendelkezésre, a felhasznált axiómákat, műveleti szabályokat, például az asszociativitást vagy a kommutativitást, már ismerték és használták a matematikusok.

A kvaterniók felfedezésében fontos szerepet játszott a komplex számok valós számpárként történő értelmezése. A komplex számok geometriai szemléletben kétdimenziós síkon lévő pontok, illetve vektorok sokasága, azonban ez a fajta megközelítés a velük való számolást megnehezíti. Éppen ezért játszott fontos szerepet, hogy tekinthetünk a komplex számokra valós számpárokként. Ezt a fajta felírást először Hamilton publikálta 1835-ben, az "Elmélet a Konjugált Függvényekről, avagy Algebrai Párokról, és egy Bevezető Elemi Esszé az Algebráról, mint az Idő Tudományáról" című munkájában. Ebben Hamilton a már jól ismert aritmetikai törvényeknek (asszociativitás, kommutativitás és disztributivitás) megfelelően definiálta a komplex számok, mint $\mathbb{R}^2$ feletti vektorok közötti összeadást és szorzást.

Ez adta az ötletet, hogy a komplex számok közötti összeadás és szorzás nem örökíthető-e a háromdimenziós térbe, vagyis az addig még nem létező, hiperkomplex számok körébe. A valós számhármasok feletti összeadás és kivonás megfelelően működött, de Hamilton annak ellenére, hogy sok évet szánt rá, nem talált olyan szorzás műveletet, ami a korábban említett három törvénynek eleget tett volna.

**1.1.1. Megjegyzés.** Ma már könnyen igazolható, hogy nem létezhet $\mathbb{R}$-lineáris szorzás művelet a valós számhármasok fölött, amely a komplexek feletti szorzás kibővítése lenne. Ha $e := (1,0,0)$, $i := (0,1,0)$ és $j := (0,0,1)$ jelöli az $\mathbb{R}^3$ feletti kanonikus bázist, akkor az $ij$ szorzat, $ij = \varrho e + \sigma i + \tau j$ alakban kellene előálljon, ahol $\varrho, \sigma, \tau \in \mathbb{R}$. Ha azonban feltesszük, hogy $i^2 = -e$ (mint $\mathbb{C}$-ben) és $i(ij) = (ii)j = -j$ (vagyis kihasználjuk az asszociativitást), akkor

$$-j = \varrho i - \sigma e + \tau ij = \varrho i - \sigma e + \tau(\varrho e + \sigma i + \tau j) = (\tau\varrho - \sigma)e + (\tau\sigma + \varrho)i + \tau^2 j.$$

Mivel azonban $e$, $i$ és $j$ lineárisan függetlenek, ezért a fenti levezetés eredménye $\tau^2 = -1$, ami azt jelenti, hogy $\tau \notin \mathbb{R}$, tehát ellentmondásra jutottunk. Ennél azonban egy sokkal általánosabb állítást is érdemes megemlíteni:

**1.1.1. Tétel.** *Minden páratlan dimenziójú $\mathcal{A}$ valós ferdetest izomorf $\mathbb{R}$-rel, vagyis csak egydimenziós lehet.*

**1.1.1. Definíció.** *Az $\mathcal{A}$* ***ferdetest*** *$\mathbb{R}$ felett, más szóval* ***valós ferdetest****, ha $\mathcal{A}$-ban értelmezve van az összedás, a szorzás, és az $\mathbb{R}$ elemeivel, mint skalárokkal való szorzás úgy, hogy*

1. *$\mathcal{A}$ az összeadásra és a skalárral való szorzásra vektortér $\mathbb{R}$ fölött;*
2. *$\mathcal{A}$ az összeadásra nézve Abel-csoport (kommutatív csoport);*
3. *$\mathcal{A}$ a szorzásra nézve csoport (vagyis a szorzás asszociatív és minden elemnek van inverze);*
4. *érvényes a disztributivitás, azaz $\forall x, y, z \in \mathcal{A}$ elemre*

$$(x+y)z = xz + yz \quad \text{és} \quad z(x+y) = zx + zy.$$

**Bizonyítás.** Legyen $a \in \mathcal{A}$ és jelölje $L_a : \mathcal{A} \to \mathcal{A}$ az $x \mapsto ax$ bal oldali szorzás műveletét. Mivel $\mathcal{A}$ dimenziója páratlan, ezért az $L_a$ operátor karakterisztikus polinomja is páratlan fokú. Kihasználva azt a Bolzano tételéből[1] következő állítást, miszerint páratlan fokú valós együtthatós polinomnak van valós gyöke, arra jutunk, hogy $L_a$-nak van valós $\lambda$ sajátértéke. Ha $v \neq 0$ jelöli a megfelelő sajátvektort, akkor $av = \lambda v$, azaz $(a - \lambda e)v = 0$, ahol $e$ az $\mathcal{A}$ egységeleme. $\mathcal{A}$ azonban ferdetest, ezáltal nullosztómentes[2], így azt kaptuk, hogy $a = \lambda e$, avagy más szavakkal $a \in \mathbb{R}e$. Mivel ez tetszőleges $a \in \mathcal{A}$-ra teljesül, ezért $\mathcal{A} \simeq \mathbb{R}$. □

Hamiltonnak azonban még nem állt rendelkezésére a fenti tétel, így érthető módon a szorzás megalkotása terén tett első próbálkozásai sikertelennek bizonyultak. Kezdetben olyan szorzás műveletet szeretett volna kapni, ami a párokhoz hasonlóan, a számhármasok felett is asszociatív, kommutatív, illetve disztributív az összeadásra nézve. Első kísérlete a komplex számok analógiáján az

$$\alpha + \beta i + \gamma j$$

alakú számok voltak, ahol $i^2 = j^2 = -1$. A szorzást pedig a szokásos, valós számkörben értelmezett szorzás műveletével állította elő, feltételezve és kihasználva a kommutativitást, azaz

$$(\alpha + \beta i + \gamma j)^2 = \alpha^2 - \beta^2 - \gamma^2 + 2\alpha\beta i + 2\alpha\gamma j + 2\beta\gamma ij. \tag{1}$$

A szorzat helyességét a komplex számoknál is használt tulajdonsággal tesztelte, azaz két vektor szorzatának a hossza meg kell egyezzen a vektorok hosszainak szorzatával. Egy $\alpha + \beta i + \gamma j$ szám euklideszi hossza $\sqrt{\alpha^2 + \beta^2 + \gamma^2}$, azonban az (1) jobb oldalán álló szám hosszát nem ilyen egyszerű megállapítani a benne szereplő $ij$ miatt. Ha viszont megnézzük az előbb említett számban 1, $i$ és $j$ együtthatóinak négyzetösszegét, akkor a következőt kapjuk:

$$(\alpha^2-\beta^2-\gamma^2)^2+(2\alpha\beta)^2+(2\alpha\gamma)^2 = \alpha^4+\beta^4+\gamma^4-2\alpha^2\beta^2-2\alpha^2\gamma^2+2\beta^2\gamma^2+4\alpha^2\beta^2+4\alpha^2\gamma^2 =$$

$$= \alpha^4 + \beta^4 + \gamma^4 + 2\alpha^2\beta^2 + 2\alpha^2\gamma^2 + 2\beta^2\gamma^2 = (\alpha^2 + \beta^2 + \gamma^2)^2.$$

Eszerint a hosszakra elvárt összefüggés teljesül, ha az $ij$ szorzatot 0-nak választjuk. Hamilton azonban ezt furcsának és kényelmetlennek vélte, ezért az (1) összefüggés újbóli megvizsgálása után észrevette, hogy a jobb oldalon álló $2ij$ helyett valójában

[1] **Bolzano tétele**: Legyen $f : \mathbb{R} \to \mathbb{R}$ folytonos függvény az $[a, b]$ zárt intervallumon. Ha $f(a) < 0$ és $f(b) > 0$, akkor van olyan $a < c < b$, melyre $f(c) = 0$. [6]

[2] $\mathcal{A}$ nullosztómentes, ha $uv = 0$ $(u, v \in \mathcal{A})$ esetén, $u = 0$ és/vagy $v = 0$.

$ij + ji$ kellene álljon. Ahhoz, hogy ez eltűnjön, $ji = -ij$ kell legyen, vagyis le kell mondani a kommutativitásról. Annak érdekében, hogy általánosabban tudja vizsgálni a problémát, vagyis ne kelljen eldöntenie, hogy $ij = 0$ vagy sem, Hamilton bevezetett egy új $k$ változót, amire a következő teljesül: $ij = k$ és $ji = -k$.

Ez adta az ötletet, ami egészen új megvilágításba helyezte a problémát: "szükség van egy negyedik dimenzióra ahhoz, hogy számhármasokkal tudjunk számolni". Már csak az maradt kérdés, hogy $k^2$ mi legyen, azonban az asszociativitást kihasználva rögtön adódik, hogy

$$k^2 = (ij)(ij) = i(ji)j = -i(ij)j = -i^2j^2 = -1,$$

$$i^2 = j^2 = k^2 = ijk = -1.$$

## 1.2. A kvaterniók $\mathbb{H}$ algebrája

A kvaterniókat kétféle módon is szokás reprezentálni. Hamilton módszerével, vagyis az $\mathbb{R}^4$ feletti kanonikus bázisvektorok szorzat-táblázatával, ezen algebrát jelölje $\mathbb{H}$, de speciális $2 \times 2$-es komplex értékű mátrixokként is előállíthatók, amit jelöljön $\mathcal{H}$. Megadható, és később meg is adunk, egy $F : \mathbb{H} \to \mathcal{H}$ természetes, azaz műveelettartó izomorfizmust, aminek ismeretében nyilvánvalóvá válik, hogy $\mathbb{H}$ ferdetest $\mathbb{R}$ felett. Hamiltonnak az asszociativitást még direkt módszerrel kellett ellenőriznie, akkoriban ugyanis a mátrixok még nem voltak ismertek. A mátrix fogalmát és a mátrix kalkulust Arthur Cayley vezette be, az 1858-ban megjelent "Értekezés a Mátrixok Elméletéről" című munkájában. Ebben Cayley a mátrixok speciális eseteként foglalkozik a kvaterniókkal.

Mielőtt rátérnénk a kvaterniók algebrájának előállítására, rögzítsünk néhány fogalmat, elsőként a *valós algebrák* definícióját:

**1.2.1. Definíció.** *Azt mondjuk, hogy $\mathcal{A}$ **algebra** $\mathbb{R}$ **fölött** (röviden $\mathbb{R}$-**algebra** vagy **valós algebra**), ha $\mathcal{A}$-ban értelmezve van az összedás, a szorzás, és az $\mathbb{R}$ elemeivel, mint skalárokkal való szorzás úgy, hogy*

1. *$\mathcal{A}$ az összeadásra és a skalárral való szorzásra vektortér $\mathbb{R}$ fölött;*
2. *tetszőleges $a, b \in \mathcal{A}$ és $\alpha, \beta \in \mathbb{R}$ esetén teljesülnek az alábbi disztributív azonosságok:*

$$(\alpha x + \beta y)z = \alpha(xz) + \beta(yz) \quad \textit{és} \quad x(\alpha y + \beta z) = \alpha(xy) + \beta(xz).$$

*Az $\mathcal{A}$ algebra egységelemes, ha létezik egy $e \in V$ elem, melyre $ex = xe = x$, tetszőleges $x \in \mathcal{A}$ esetén.*

A definícióból rögtön látszik, hogy egy általános algebrától nem követeljük meg sem az asszociativitást ($x(yz) = (xy)z$ minden $x, y, z \in \mathcal{A}$-ra), sem a kommutativitást ($xy = yx$ minden $x, y \in \mathcal{A}$-ra).

**1.2.2. Definíció.** *Az $\mathcal{A} \neq 0$ algebrát **division algebrának** nevezzük, ha $\forall a, b \in \mathcal{A}$ elemre, ahol $a \neq 0$, az $ax = b$ és $ya = b$ azonosságoknak egyértelmű megoldása van.*

A definícióból adódik az észrevétel, miszerint minden division algebra nullosztómentes, sőt véges dimenziós esetben, egy ennél erősebb állítást is megfogalmazhatunk:

**1.2.1. Állítás.** *Legyen $\mathcal{A}$ egy véges dimenziós algebra. Ekkor azt mondhatjuk, hogy $\mathcal{A}$ pontosan akkor division algebra, ha nullosztómentes.*

**Bizonyítás.** Mivel a division algebrák definíciójából következik, hogy $\mathcal{A}$ nullosztómentes, így elég a fordított irányt igazolnunk.

Legyen $a \in \mathcal{A}\backslash\{0\}$. Ekkor az $\mathcal{A} \to \mathcal{A}$, $x \mapsto ax$ leképezés injektív, mert ha indirekt módon feltesszük, hogy nem az, akkor találunk olyan $x, y \in \mathcal{A}$ elemeket, melyekre $x \neq y$, viszont $ax = ay$, azaz $a(x-y) = 0$. $\mathcal{A}$ azonban nullosztómentes, ezért vagy $a$ vagy $(x-y)$ nulla kell legyen, ami ellentmond a feltevéseinknek, így ellentmondásra jutunk.

Mivel $n := \dim \mathcal{A} < \infty$, így az előbb definiált leképezés az $e_1, \ldots, e_n$ bázishoz az $ae_1, \ldots, ae_n$ elemeket rendeli, amelyek az injektivitás miatt továbbra is lineárisan függetlenek, azaz generálják az $\mathcal{A}$ algebrát. Ez azt jelenti, hogy $\mathcal{A}$ minden eleme előáll képként, vagyis a leképezés bijekció, ezáltal minden $ax = b$ egyenlet $x$ megolása egyértelmű.

Hasonlóan, az $y \mapsto ya$ leképezést megvizsgálva kapjuk, hogy minden $ya = b$ egyenlet $y$ megoldása is egyértelmű, vagyis $\mathcal{A}$ division algebra. □

**1.2.1. Megjegyzés.**

1. Szintén a definíció következménye, hogy ha $\mathcal{A}$ asszociatív divison algebra, akkor a $G := \mathcal{A}\backslash\{0\}$, vagyis $\mathcal{A}$ nem nulla elemei csoportot alkotnak, ahol $G$ egységeleme megegyezik az $\mathcal{A}$ algebra egységelemével. Ez azt jelenti, hogy véges dimenzióban az asszociatív division algebra és a ferdetest definíció szerint azonos.

2. A 1.1.1 tétel (7. oldal) általánosabb formában is kimondható, azaz minden páratlan dimenziójú $\mathcal{A}$ valós, egységelemes division algebra izomorf $\mathbb{R}$-rel. Ez a tétel bizonyításából triviálisan adódik, hiszen a benne szereplő $\mathcal{A}$ ferdetestnek csak olyan tulajdonságait használtuk fel, amellyel az egységelemes division algebrák is rendelkeznek.

Térjünk rá a kvaternió algebra előállítására: jelölje $e_1 = (1,0,0,0)$, $e_2 = (0,1,0,0)$, $e_3 = (0,0,1,0)$ és $e_4 = (0,0,0,1)$ a négydimenziós valós tér, azaz $\mathbb{R}^4$ feletti kanonikus bázisvektorokat, ahol legyen $e_1$ az egységelem. Így tehát a *Hamilton-féle szorzástáblázat*, ahol a szorzat első tényezője a bal oldali oszlopból, második tényezője pedig a fenti sorból kerül ki, a következőképpen néz ki:

| | $e_2$ | $e_3$ | $e_4$ |
|---|---|---|---|
| $e_2$ | $-e_1$ | $e_4$ | $-e_3$ |
| $e_3$ | $-e_4$ | $-e_1$ | $e_2$ |
| $e_4$ | $e_3$ | $-e_2$ | $-e_1$ |

Tehát még egyszer, ami a bevezetőben már elhangzott: *kvaternió algebrának* nevezzük és $\mathbb{H}$-val jelöljük azt a négydimenziós $\mathbb{R}$-algebrát, ahol a fenti táblázat szerint definiáljuk a szorzást. Mivel a táblázatból rögtön kiolvasható, hogy például $e_2e_3 \neq e_3e_2$, ezért világos, hogy $\mathbb{H}$ a szorzásra nem kommutatív. Az asszociativitás viszont könnyen ellenőrizhető, hiszen minden $2 \leq \lambda, \mu, \nu \leq 4$-re teljesül, hogy $(e_\lambda e_\mu)e_\nu = e_\lambda(e_\mu e_\nu)$, például:

$$(e_2e_3)e_4 = e_4e_4 = -e_1, \qquad e_2(e_3e_4) = e_2e_2 = -e_1.$$

**1.2.2. Megjegyzés.** A könnyebb átláthatóság érdekében, a bázisvektorokat $e_1, e_2, e_3, e_4$ helyett $e, i, j, k$-val szokás jelölni, ahol $e$ továbbra is az egységelem.

## 1.3. A $\mathcal{H}$ mátrixalgebra

Motivációul szolgál a következő ötlet: jelölje $\mathcal{C}$ a $\begin{pmatrix}\alpha & -\beta\\ \beta & \alpha\end{pmatrix}$ alakú, valós értékű ($\alpha, \beta \in \mathbb{R}$) mátrixok halmazát. Ekkor $\mathcal{C}$ $\mathbb{R}$-részalgebrája[3] $M_2(\mathbb{R})$-nek, az $\alpha + \beta i \mapsto \begin{pmatrix}\alpha & -\beta\\ \beta & \alpha\end{pmatrix}$ leképezés pedig egy $\mathbb{C} \to \mathcal{C}$ $\mathbb{R}$-algebra izomorfizmus [5]. Ennek analógiájaként mondhatjuk ki az alábbi tételt.

**1.3.1. Tétel.** *A* $\mathcal{H} := \left\{\begin{pmatrix}w & -z\\ \overline{z} & \overline{w}\end{pmatrix} : w, z \in \mathbb{C}\right\}$ *halmaz az* $M_2(\mathbb{C})$*-nek* $\mathbb{R}$*-részalgebrája, ahol* $E := \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ *az egységelem, továbbá* $\mathcal{H}$ *négydimenziós ferdetest.*

**Bizonyítás.** A komplex konjugált $\overline{z+w} = \overline{z} + \overline{w}$ tulajdonságát felhasználva [8], könnyen ellenőrizhető, hogy $\mathcal{H}$ $\mathbb{R}$-fölötti altere $M_2(\mathbb{C})$-nek, vagyis

$$\lambda \cdot \left(\begin{pmatrix}w_1 & -z_1\\ \overline{z}_1 & \overline{w}_1\end{pmatrix} + \begin{pmatrix}w_2 & -z_2\\ \overline{z}_2 & \overline{w}_2\end{pmatrix}\right) = \begin{pmatrix}\lambda(w_1 + w_2) & -\lambda(z_1 + z_2)\\ \lambda(\overline{z}_1 + \overline{z}_2) & \lambda(\overline{w}_1 + \overline{w}_2)\end{pmatrix},$$

ahol $\lambda \in \mathbb{R}$, így $\overline{\lambda} = \lambda$.

Direkt módon beláható az is, hogy $\mathcal{H}$ zárt az $M_2(\mathbb{C})$-ben értelmezett mátrixszorzásra. Legyen $A = \begin{pmatrix}w_1 & -z_1\\ \overline{z}_1 & \overline{w}_1\end{pmatrix}$ és $B = \begin{pmatrix}w_2 & -z_2\\ \overline{z}_2 & \overline{w}_2\end{pmatrix}$, azaz $A, B \in \mathcal{H}$. Ekkor

$$AB = \begin{pmatrix}w_1 & -z_1\\ \overline{z}_1 & \overline{w}_1\end{pmatrix} \cdot \begin{pmatrix}w_2 & -z_2\\ \overline{z}_2 & \overline{w}_2\end{pmatrix} = \begin{pmatrix}w_1 w_2 - z_1\overline{z}_2 & -w_1 z_2 - z_1\overline{w}_2\\ \overline{z}_1 w_2 + \overline{w}_1\overline{z}_2 & -\overline{z}_1 z_2 + \overline{w}_1\overline{w}_2\end{pmatrix} = \begin{pmatrix}u & v\\ x & y\end{pmatrix},$$

ahol teljesülnek az alábbi összefüggések:

$$u = w_1 w_2 - z_1\overline{z}_2 = \overline{-\overline{z}_1 z_2 + \overline{w}_1\overline{w}_2} = \overline{y}$$

$$v = -w_1 z_2 - z_1\overline{w}_2 = -(\overline{\overline{z}_1 w_2 + \overline{w}_1\overline{z}_2}) = -\overline{x},$$

vagyis a kapott $AB$ szorzatmátrix tetszőleges $A, B \in \mathcal{H}$ esetén $\mathcal{H}$-beli.

Hátra van azonban még annak a bizonyítása, hogy $\mathcal{H}$ ferdetest. Az asszociativitás következik, hiszen $M_2(\mathbb{C})$ is asszociatív, de ahhoz, hogy ferdetest legyen, be kell

[3] Az $A$ algebrának a $B \subset A$ nem üres részhalmaz **részalgebrája**, ha $B$ zárt az $A$ műveleteire.

látnunk, hogy nullosztómentes. Tegyük fel, hogy $A, B \in \mathcal{H}$ olyan, hogy $AB = 0$. Ekkor $\det A \cdot \det B = 0$, tehát $\det A = 0$ és/vagy $\det B = 0$. Mivel azonban $\det \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} = |w|^2 + |z|^2 = 0$ pontosan akkor teljesül, ha $w = z = 0$, tehát $\mathcal{H}$ ferdetest. □

**1.3.1. Lemma.** *Az* $F : \mathbb{H} \to \mathcal{H} : (\alpha, \beta, \gamma, \delta) \mapsto \begin{pmatrix} \alpha + \beta i & -\gamma - \delta i \\ \gamma - \delta i & \alpha - \beta i \end{pmatrix}$ *leképezés* $\mathbb{R}$-*algebra izomorfizmus, ahol*

$$F(e_1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} =: E \qquad F(e_2) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} =: I$$

$$F(e_3) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} =: J \quad F(e_4) = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} =: K$$

**Bizonyítás.** A fenti $F$ leképezés nyilvánvalóan $\mathbb{R}$-lineáris és bijektív, azonban be kell még látni, hogy $F(e_\mu)F(e_\nu) = F(e_\mu e_\nu)$ minden $(\mu, \nu = 1, 2, 3, 4)$-re. Ezt az alábbi számolás analógiáján könnyen igazolhatjuk az összes esetre:

$$F(e_1)F(e_1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = F(e_1 e_1), \qquad F(e_1)F(e_2) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = F(e_1 e_2)\ .$$

Továbbá az $I^2 = J^2 = -E$ és $IJ = -JI = K$ összefüggések is könnyen ellenőrizhetők:

$$I^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = J^2$$

$$IJ = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = -\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = -JI,$$

amelyekből az asszociativitást kihasználva már következik a többi reláció, például

$$K^2 = (IJ)(-JI) = -IJ^2I = I^2 = -E.$$

□

**1.3.1. Következmény.** A $\mathbb{H}$ kvaternió algebra ferdetest.

## 1.4. Vektoralgebra kvaterniókkal

A kvaterniók legelterjedtebb alkalmazásai a vektoralgebra területén ismertek. A következőkben megnézzük, miként hozható kapcsolatba a kvaterniók algebrája a háromdimenziós euklideszi tér vektoraival, hogyan áll elő a vektorok skaláris és vektoriális szorzata, illetve miként lehet a tér vektorainak forgatását kvaterniókkal felírni.

Tekintsük a $\mathbb{H}$, mint vektortér, projekcióját a tisztán képzetes $(i, j, k)$ bázisvektorok által generált háromdimenziós altérre. Ezen altér nyilvánvalóan izomorf az $\mathbb{R}^3$ térrel, így a két tér bázisvektorainak jelölésére egyaránt használhatjuk az $i, j, k$ betűket. Ez más szóval azt jelenti, hogy minden tisztán képzetes kvaternió meghatároz egy pontot a közönséges háromdimenziós térben, így annak érdekében, hogy közelebb hozzuk a kvaterinókat a háromdimenziós vektorokhoz, nevezzük el a kvaterniók valós részét skaláris résznek, a képzetes részt pedig vektoriális résznek.

Vegyünk most két tisztán képzetes kvaterniót, vagyis legyen $q_1 := b_1 i + c_1 j + d_1 k$ és $q_2 := b_2 i + c_2 j + d_2 k$. A kvaterinószorzás szabálya szerint összeszorozva őket azt kapjuk, hogy

$$q_1 q_2 = -(b_1 b_2 + c_1 c_2 + d_1 d_2) + (c_1 d_2 - d_1 c_2) i + (d_1 b_2 - b_1 d_2) j + (b_1 c_2 - c_1 b_2) k.$$

Vizsgáljuk most meg ezen szorzat skaláris és vektoriális részét:

$$\operatorname{Re} q_1 q_2 = -(b_1 b_2 + c_1 c_2 + d_1 d_2) \tag{1}$$

$$\operatorname{Im} q_1 q_2 = (c_1 d_2 - d_1 c_2) i + (d_1 b_2 - b_1 d_2) j + (b_1 c_2 - c_1 b_2) k \tag{2}$$

Ezen felírásból látszik, hogy a $b_1 b_2 + c_1 c_2 + d_1 d_2$ összeg a $q_1$ és $q_2$ tisztán képzetes kvaterniók által meghatározott háromdimenziós vektorok skaláris szorzata, tehát adódik a következő állítás:

**1.4.1. Állítás.** *Legyenek $v_1 = (b_1, c_1, d_1)$ és $v_2 = (b_2, c_2, d_2)$ a $q_1$ és $q_2$ tisztán képzetes kvaterniók által meghatározott vektorok. Ekkor*

$$-\operatorname{Re} q_1 q_2 = \langle v_1, v_2 \rangle = |q_1||q_2| \cos\varphi$$

*ahol $\langle ., . \rangle$ a szokásos háromdimenziós térben értelmezett skaláris szorzatot jelöli, $\varphi$ pedig a $v_1$ és $v_2$ vektorok által bezárt szög.*

**Bizonyítás.** Jelölje $M_1$ és $M_2$ a $v_1$ és $v_2$ vektorok végpontjait a koordinátarendszerben, majd vegyük fel az origó $(O)$, $M_1$ és az $M_2$ által kifeszített háromszöget. Vegyük most sorra az $OM_1$, $OM_2$ és $M_1M_2$ vektorok önmagukkal vett skaláris szorzatát, azaz a hosszuk négyzetét:

$$(OM_1)^2 = b_1^2 + c_1^2 + d_1^2$$

$$(OM_2)^2 = b_2^2 + c_2^2 + d_2^2$$

$$(M_1M_2)^2 = (b_1 - b_2)^2 + (c_1 - c_2)^2 + (d_1 - d_2)^2 =$$
$$= (b_1^2 + c_1^2 + d_1^2) + (b_2^2 + c_2^2 + d_2^2) - 2(b_1b_2 + c_1c_2 + d_1d_2),$$

vagyis azt kaptuk, hogy

$$(M_1M_2)^2 = (OM_1)^2 + (OM_2)^2 - 2(b_1b_2 + c_1c_2 + d_1d_2).$$

A koszinusztétel szerint azonban

$$(M_1M_2)^2 = (OM_1)^2 + (OM_2)^2 - 2(OM_1) \cdot (OM_2) \cdot \cos\varphi,$$

ahol $\varphi$ a $v_1$ és $v_2$ vektorok által bezárt szög. A két egyenlőség összvetéséből már adódik, amit bizonyítani akartunk, azaz

$$(OM_1) \cdot (OM_2) \cdot \cos\varphi = b_1b_2 + c_1c_2 + d_1d_2.$$

□

Megkaptuk tehát, hogy a $q_1$ és $q_2$ tisztán képzetes kvaternió szorzatának valós része egyenlő a $v_1$ és $v_2$ vektorok negatív előjellel vett skaláris szorzatával. Az összefüggésből az is adódik, hogy egymásra merőleges $v_1$, $v_2$ vektorok esetén $\operatorname{Re} q_1q_2 = 0$.

A (2) egyenlet jobb oldalán álló kifejezés, azaz a $q_1q_2$ szorzat vektoriális része nem más, mint a $v_1$ és $v_2$ vektorok vektoriális szorzata, hiszen

$$v_1 \times v_2 = (c_1d_2 - d_1c_2)i + (d_1b_2 - b_1d_2)j + (b_1c_2 - c_1b_2)k.$$

**1.4.2. Állítás.** *Legyenek $v_1 = (b_1, c_1, d_1)$ és $v_2 = (b_2, c_2, d_2)$ a $q_1$ és $q_2$ tisztán képzetes kvaterniók által meghatározott vektorok. Ekkor*

$$|\operatorname{Im} q_1q_2| = |v_1 \times v_2| = |q_1||q_2| \sin\varphi,$$

*ahol $\varphi$ a $v_1$ és $v_2$ vektorok által bezárt szög.*

**Bizonyítás.** A vektoriális szorzat definíciója szerint a $v_1 \times v_2$ vektor a $v_1$ és a $v_2$ vektorra is merőleges, hossza pedig $|v_1||v_2|\sin\varphi$. Két vektor akkor merőleges egymásra, ha skaláris szorzatuk 0, azaz $v_1 \times v_2$ és $v_1$ merőlegességéhez, az előzőek alapján, azt kell megmutatnunk, hogy

$$\operatorname{Re}(q_1 \cdot \operatorname{Im} q_1 q_2) = 0.$$

A $q_1 q_2$ szorzat definíciójából, illetve a skaláris szorzatra kapott összefüggésből adódik, hogy

$$|\operatorname{Im} q_1 q_2| = |v_1 \times v_2| = q_1 q_2 + \langle v_1, v_2 \rangle = q_1 q_2 - \operatorname{Re} q_1 q_2,$$

ezért

$$q_1 \cdot |\operatorname{Im} q_1 q_2| = q_1 \cdot (q_1 q_2 - \operatorname{Re} q_1 q_2) = q_1^2 q_2 - q_1 \cdot \operatorname{Re} q_1 q_2 = -|q_1|^2 q_2 - q_1 \cdot \operatorname{Re} q_1 q_2,$$

mert $q_1^2 = -(b_1^2 + c_1^2 + d_1^2) + 0i + 0j + 0k = -|q_1|^2$. Már csak azt kell belátni, hogy a jobb oldalon álló kvaternió tisztán képzetes. Ez azonban nyilvánvaló, hiszen $q_1$ és $q_2$ definíció szerint vektoriális, így a skalárszorosuk és a különbségük is az marad. A $v_1 \times v_2$ és $v_2$ vektorok merőlegessége hasonló módon igazolható.

Hátra van még az $|\operatorname{Im} q_1 q_2|$ értékre vonatkozó összefüggés bizonyítása. Ez azonban egyszerűen belátható, hiszen a $v_1 \times v_2$ vektor hosszának négyzete

$$(c_1d_2-d_1c_2)^2+(d_1b_2-b_1d_2)^2+(b_1c_2-c_1b_2)^2 = (b_1^2+c_1^2+d_1^2)(b_2^2+c_2^2+d_2^2)-(b_1b_2+c_1c_2+d_1d_2)^2,$$

ami a kvaterniók szorzásának és a skaláris szorzat definíciójának következtében

$$|q_1|^2|q_2|^2 - (\operatorname{Re} q_1 q_2)^2 = |q_1|^2|q_2|^2 - |q_1|^2|q_2|^2\cos^2\varphi = |q_1|^2|q_2|^2\sin^2\varphi.$$

□

## 1.5. Forgatások

Az előző bekezdésben megvizsgáltuk, miként fedi le a kvaterniószorzás a háromdimenziós vektorok közti skaláris és vektoriális szorzatot, de eddig kizárólag tisztán képzetes kvaterniókkal számoltunk. A következő lépés, hogy megvizsgáljuk, mi egy tetszőleges és egy tisztán vektoriális kvaternió szorzatának geometriai jelentése.

Mielőtt azonban teljes általánosságban vizsgálnánk a fent említett kérdést, nézzünk meg egy speciális esetet. Legyen $q := a + bi + cj + dk$ egy tetszőleges, de 1 abszolút értékű kvaternió, azaz legyen $a^2 + b^2 + c^2 + d^2 = 1$. Írjuk fel $q$-t a következő alakban:

$$q = a + q',$$

ahol $q' = bi + cj + dk$ tisztán képzetes kvaternió, avagy geometriai szemléletben $q' = (b, c, d)$ vektor. Mivel a feltevésünk szerint $a^2 + |q'|^2 = 1$, ezért a trigonometrikus Pitagorasz-tétel következtében létezik olyan $\varphi$ szög, amelyre

$$a = \cos\varphi; \qquad |q'| = \sin\varphi.$$

Ha $p$ a $q'$ vektorral megegyező irányú egységvektor, akkor $q'$ felírható $q' = |q'|p$ alakban, következésképpen

$$q = \cos\varphi + p\sin\varphi.$$

Vegyünk most egy $v$ tisztán vektoriális kvaterniót, de szorítkozzunk egyelőre arra az esetre, amikor a $v$ vektor merőleges a $p$-re, így azt kapjuk, hogy

$$qv = (\cos\varphi + p\sin\varphi)v = v\cos\varphi + pv\sin\varphi.$$

Mivel a $p$ és $v$ vektorok merőlegesek, a $pv$ szorzat skaláris része 0, vektoriális része pedig $p \times v$, vagyis a $|p| \cdot |v| \cdot \sin{}^{\pi}/_{2}$ hosszúságú, $p$-re és $v$-re egyaránt merőleges vektorral egyenlő, amely $p$-hez és $v$-hez viszonyítva ugyanolyan irányítású, mint $i$-hez és $j$-hez képest a $k$ vektor. Ezen vektort jelölje $\widetilde{v}$, ami tehát a $v$-ből a $p$ vektor körüli ${}^{\pi}/_{2}$ nagyságú elforgatással adódik, tehát

$$qv = v\cos\varphi + \widetilde{v}\sin\varphi.$$

**1.5.1. Megjegyzés.** Mivel a $p$ körüli elforgatás fogalma nem egyértelmű, a továbbiakban mindig arra a forgatásra gondolunk, amely ugyanolyan irányú, mint az $i$-t $j$-be vivő, $k$ körüli legrövidebb elforgatás.

Összegzésül, ha $p$ valamilyen egységvektor, $v$ pedig egy tetszőleges, de $p$-re merőleges vektor, akkor a $v$ vektort balról megszorozva a $q = \cos\varphi + p\sin\varphi$ kvaternióval, a $v$ vektor $p$ tengely körüli $\varphi$ szögű elforgatottját kapjuk.

Ahhoz, hogy tetszőleges $v$ vektor $p$ tengely körüli elforgatását felírhassuk kvaterniókkal, a balról vett szorzás helyett a $qvq^{-1}$ műveletre lesz szükség, ahol $q^{-1}$ a $q$ inverze, azaz $qq^{-1} = e$.

**1.5.2. Megjegyzés.** $q^{-1} = \cos\varphi - p\sin\varphi$, hiszen

$$qq^{-1} = (\cos\varphi + p\sin\varphi)(\cos\varphi - p\sin\varphi) = \cos^2\varphi - p^2\sin^2\varphi = \cos^2\varphi + \sin^2\varphi = 1,$$

mert $p$ vektoriális, egységhosszú kvaternió, így $p^2 = -1^2 + 0$.

Nézzük meg mit kapunk, ha elvégezzük egy tetszőleges $v$ vektorra a $qvq^{-1}$ műveletet:

$$qvq^{-1} = qv(\cos\varphi - p\sin\varphi) = qv\cos\varphi - (qv)p\sin\varphi.$$

Az előzőekben láttuk, hogy $qv$ is vektor, azaz tisztán képzetes kvaternió, amely merőleges $p$-re, ezért a skaláris és vektoriális szorzatra kapott összefüggésekből adódóan $(qv)p = -p(qv)$, továbbá a $p(qv)$ kvaternió is vektor, amely $qv$-ből a $p$ tengely körüli $\pi/2$ szögű elforgatással áll elő. Jelöljük ezt $\widetilde{qv}$-mal, így

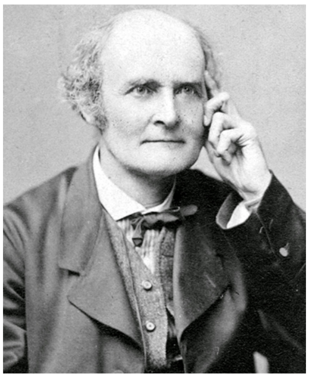
$$qvq^{-1} = qv\cos\varphi + \widetilde{qv}\sin\varphi.$$

Vegyük észre, hogy a jobb oldalon álló kifejezés egy vektor, amelyet $qv$-ből a $p$ tengely körüli $\varphi$ nagyságú elforgatással kaptunk. Azonban a $qv$ vektort is ugyanilyen elforgatással kaptuk $v$-ből, tehát arra jutottunk, hogy $qvq^{-1}$ a $v$ vektor $p$ körüli $2\varphi$ szögű elforgatásával áll elő.

A fentiekre való tekintettel kimondhatjuk, hogy a $q = \cos\varphi + p\sin\varphi$ kvaternió megfeleltetésbe állítható a $p$ tengely körüli $2\varphi$ szögű elforgatással.

# 2. Cayley-számok

## 2.1. Arthur Cayley és az oktonionok kialakulása



Arthur Cayley 1821-ben született az angliai Richmondban (London). Édesapja Henry Cayley, ősi yorkshirei család leszármazottja volt, aki kereskedőként Szentpéterváron telepedett le. Édesanyja az orosz születésű, de feltehetően angol gyökerekkel rendelkező, Maria Antonia Doughty volt. Cayley életének első nyolc évét Szentpéterváron töltötte, amíg végül 1829-ben a család végleg a Londonhoz közeli Blackheath városba költözött. Tanulmányait magániskolában kezdte, ahol már megmutatkozott a matematika iránti érdeklődése. 14 évesen a wimbledoni King's College School növendéke lett, ahol a matematikában mutatott kiemelkedő tehetsége magára vonta tanárai figyelmét, így az oktatók végül Cayley édesapját is meggyőzték, hogy az eredetileg tervezett kereskedői pálya helyett, a Cambridge-i Egyetemre készítse fel a fiát.

Miután Hamilton megalkotta a hiperkomplex számok rendszerét, a matematikusok ráeszméltek, hogy ha nem ragaszkodnak minden megszokott aritmetikai törvényhez, akkor egészen új, még a kvaterniókon is túlmutató rendszerek jöhetnek létre. Így fordulhatott elő, hogy csupán két hónappal a kvaterniók felfedezése után, 1843 decemberében, John T. Graves megalkotta az oktávok nyolcdimenziós division algebráját, amely a szorzásra nézve már nem csak a kommutativitást, de az asszociativitást is elhagyta. Graves 1844 januárjában egy levélben tudatta Hamiltonnal a felfedezését, de eredményei 1848-ig nem kerültek kiadásra. A kimaradt négy év sajnos el is vette Gravestől a felfedezésért járó elismerést, ugyanis 1845-ben Cayley szintén felfedezte az oktávokat, amelyekről szóló írását még abban az évben kiadta, egy az elliptikus függvényekről szóló tanulmányának mellékleteként.

Mivel az oktávok körében az asszociativitás nem érvényes, így a kvaterniókkal ellentétben, a műveletek definiálásához nem hívhatjuk segítségül a mátrixokat, vagyis más módon kell megközelíteni a velük való számolást. Ismét a természetesen adódó trükköt felhasználva, a kvaterniók $\mathbb{H}$ algebrájának megduplázásával fogjuk előállítani az oktávok algebráját. Ehhez azonban szükségünk lesz némi előkészületre.

## 2.2. Alternáló kvadratikus algebrák

Ahogy a bevezetőből is kiderült, az oktávok feletti műveletek helyes értelmezéséhez el kell hagynunk a szorzás asszociativitását. Bár a számnyolcasok algebrája még így is sok szép tulajdonságot megőriz, így már biztosan nem lehet ferdetest. Szükségünk lesz tehát egy olyan struktúra definiálására, amely a szorzás művelet asszociativitásán és kommutativitásán kívül az összes szükséges tulajdonsággal rendelkezik: ezek lesznek a nullosztómentes alternáló kvadratikus algebrák.

Bár az előbb említett algebrákkal a Cayley-algebra előállítása a célunk, a segítségükkel egy másik problémára is megoldást találunk. Az előző fejezetben megvizsgáltuk a kvaterinók ferdetestének algebrai és mátrixos felírását, majd láttunk példát az alkalmazására, de hátramaradt egy fontos kérdés: létezik-e magasabb dimenziós ferdetest $\mathbb{R}$ felett? Azt már tudjuk, hogy minden páratlan dimenziójú ferdetest izomorf $\mathbb{R}$-rel (1.1.1 tétel (7. oldal)), azonban a páros dimenziós eset ennél valamivel bonyolultabb. Ahhoz, hogy a választ megadó Frobenius-tételt bizonyíthassuk, meg kell ismernünk az alternáló és kvadratikus algebrák néhány tulajdonságát, illetve be kell vezetnünk a hamiltoni számhármasok fogalmát.

**2.2.1. Definíció.** *Egy $\mathcal{A}$ algebrát **alternáló**nak nevezünk, ha $\forall x, y \in \mathcal{A}$ elemre teljesül a következő:*

$$x(xy) = x^2y, \qquad (xy)y = xy^2.$$

**2.2.2. Definíció.** *Egy $\mathcal{A}$ egységelemes algebrát, ahol az egységelemet $e$ jelöli, **kvadratikus**nak nevezünk, ha $\forall x \in \mathcal{A}$ elemre teljesül az*

$$x^2 = \alpha e + \beta x$$

*kvadratikus egyenlet, ahol $\alpha, \beta \in \mathbb{R}$.*

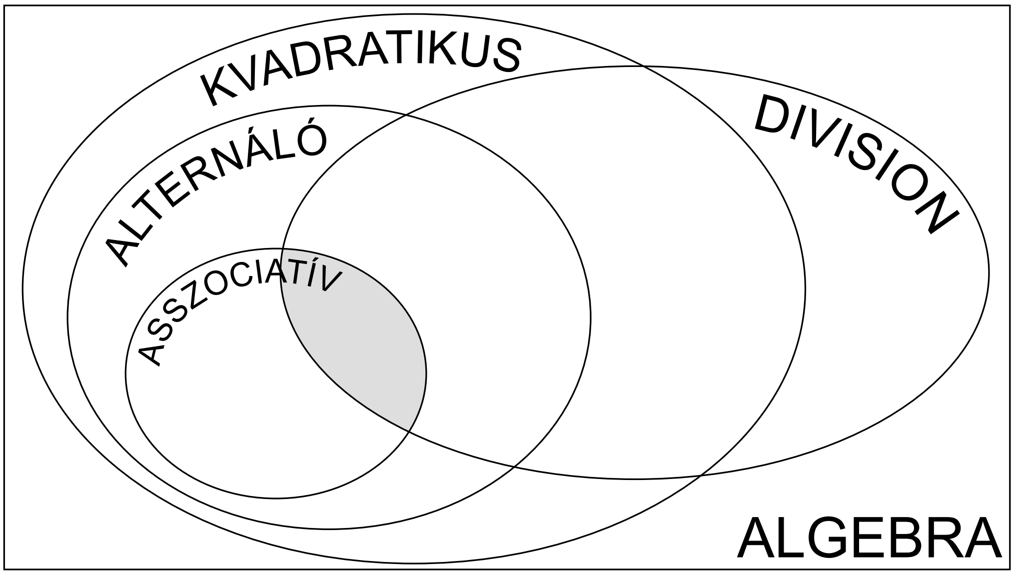
Következzen most néhány állítás az alternáló és kvadratikus algebrák kapcsolatáról, azok tulajdonságairól. Mivel a Cayley-algebra előállításához nem szükséges ezen algebrák teljes részletességgel való megismerése, ezért az alábbi állítások bizonyításától eltekintünk [5]:

**2.2.1. Állítás.**

- *Minden asszociatív algebra egyben alternáló is.*
- *Minden alternáló algebra erősen asszociatív, azaz bármely részalgebrája asszociatív.*

- *Minden alternáló division algebra egységelemes.*
- ***Artin-tétel**: Egy $\mathcal{A}$ algebra akkor és csak akkor alternáló, ha bármely két $x, y \in \mathcal{A}$ elem az $\mathcal{A}$ egy asszociatív részalgebráját generálja.*
- *Minden véges dimenziós alternáló algebra kvadratikus.*

Ezen állítás alapján az alábbi megállapítást tehetjük a **véges dimenziós algebák** tartalmazására nézve, ahol a szürke rész a ferdetestet jelöli:




**2.2.1. Lemma** (Frobenius-lemma)**.** *Ha $\mathcal{A}$ kvadratikus algebra, akkor* $\operatorname{Im}\mathcal{A} = \{x \in \mathcal{A} : x^2 \in \mathbb{R}e$ *és* $x \notin \mathbb{R}e \setminus \{0\}\}$ *altere $\mathcal{A}$-nak és $\mathcal{A} = \mathbb{R}e \oplus \operatorname{Im}\mathcal{A}$.*

A lemma bizonyításához szükségünk lesz az úgynevezett Függetlenségi lemmára, ami a következőképpen hangzik:

**2.2.2. Lemma** (Függetlenségi-lemma)**.** *Legyen $\mathcal{A}$ algebra. Ha $u, v \in \operatorname{Im}\mathcal{A}$ vektorok lineárisan függetlenek, akkor az $e, u, v$ vektorok is függetlenek egymástól.*

**Bizonyítás.** Tegyük fel indirekt módon, hogy az állítás nem igaz, vagyis legyen $v = \alpha e + \beta u$, ahol $\alpha, \beta \in \mathbb{R}$. Ekkor

$$2\alpha\beta u = v^2 - \alpha^2 e - \beta^2 u^2 \in \mathbb{R}e,$$

vagyis $\alpha\beta = 0$ kell legyen. $\alpha \neq 0$, hiszen $u$ és $v$ lineárisan függetlenek, továbbá $\beta \neq 0$, mert $v \in \operatorname{Im}\mathcal{A}$, így ellentmondásra jutottunk. $\square$

Ennek felhasználásával következzen tehát a Frobenius-lemma bizonyítása:

**Bizonyítás.** Először lássuk be, hogy ha $u, v \in \operatorname{Im}\mathcal{A}$, akkor $u+v \in \operatorname{Im}\mathcal{A}$ is teljesül. Amennyiben $u$ és $v$ lineárisan összefüggők, például $v = \alpha u$, akkor $u+v = (1+\alpha)v \in \operatorname{Im}\mathcal{A}$, ezért feltehetjük, hogy $u$ és $v$ lineárisan függetlenek egymástól. Mivel $\mathcal{A}$ kvadratikus, ezért $\forall \alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{R}$ számra teljesülnek az alábbi egyenlőségek:

$$(u+v)^2 = \alpha_1 e + \beta_1(u+v), \qquad (u-v)^2 = \alpha_2 e + \beta_2(u-v).$$

A szorzásokat elvégezve és az egyenleteket összeadva a következő összefüggés adódik:

$$(\beta_1+\beta_2)u + (\beta_1-\beta_2)v = 2u^2 + 2v^2 - (\alpha_1+\alpha_2)e \in \mathbb{R}e,$$

mivel $u, v \in \operatorname{Im}\mathcal{A}$. A Függetlenségi-lemmából következik, hogy $\beta_1+\beta_2 = \beta_1-\beta_2 = 0$, azaz $\beta_1 = \beta_2 = 0$, így tehát $(u+v)^2 = \alpha_1 e \in \mathbb{R}e$. Mivel azonban a Függetlenségi-lemma szerint $u+v \notin \mathbb{R}e$, következik, hogy $u+v \in \operatorname{Im}\mathcal{A}$.

Tegyük föl ezek után, hogy $x \in \mathcal{A}$, de $x \notin \mathbb{R}e$. Mivel $\mathcal{A}$ kvadratikus, ezért létezik olyan $\alpha, \beta \in \mathbb{R}$, hogy $x^2 = \alpha e + 2\beta x$, így

$$(x-\beta e)^2 = x^2 - 2\beta x + \beta^2 e = (\alpha + \beta^2)e.$$

Azonban $x - \beta e \notin \mathbb{R}e$, ezért $x = \beta e + u$, ahol $u := x - \beta e \in \operatorname{Im}\mathcal{A}$. Megmutattuk tehát, hogy $\mathcal{A} = \mathbb{R} + \operatorname{Im}\mathcal{A}$, de mivel $\mathbb{R}e \cap \operatorname{Im}\mathcal{A} = \{0\}$, ezért $\mathcal{A} = \mathbb{R}e \oplus \operatorname{Im}\mathcal{A}$. □

**2.2.3. Definíció.** *Az $\mathcal{A}$ algebra $u, v, w$ elemét akkor nevezzük **hamiltoni számhármasnak**, ha teljesülnek rájuk az alábbi egyenlőségek:*

$$u^2 = v^2 = w^2 = -e, \quad w = uv = -vu, \quad u = vw = -wv, \quad v = wu = -uw.$$

Már csak két állítás van hátra a Frobenius-tétel bizonyításáig, az úgynevezett Kvaternió-lemma, illetve egy a hamiltoni számhármasok létezéséről szóló tétel, mely a következőképpen hangzik:

**2.2.1. Tétel.** *Legyen $\mathcal{A}$ egy nullosztómentes, egységelemes, alternáló algebra, és legyen $U$ az $\operatorname{Im}\mathcal{A}$ kétdimenziós altere. Ekkor az $U$ minden $u$ eleméhez, melyre $u^2 = -e$, létezik egy $v \in U$ elem, hogy $u, v$ és $uv$ hamiltoni számhármast alkotnak.*

**Bizonyítás.** Először lássuk be, hogy minden fenti $u$-hoz van olyan $v \in U \setminus \mathbb{R}u$, amelyre $uv = -vu$. Legyen $x \in U$ az $u$-tól lineárisan független, így $ux + xu = \beta e$, ahol $\beta \in \mathbb{R}$, hiszen

$$ux + xu = (u+x)^2 - u^2 - x^2 \in \mathbb{R}e.$$

A jobb oldalon a Frobenius-lemma értelmében csupa tisztán képzetes elem áll, melyek négyzetösszege definíció szerint valós, tehát a $v = x + (\beta/2)u$ teljesíti az elvárt $uv + vu = 0$ összefüggést. Világos, hogy olyan $v \in U$ elemet is találhatunk, amelyre $v^2 = -e$.

Ezt felhasználva ellenőrizhetjük a hamiltoni számhármasokra elvárt összefüggéseket:

$$v(uv) = -v(vu) = -v^2u = u, \qquad (uv)v = uv^2 = -u.$$

Hasonlóan belátható, hogy $(uv)u = v = -u(uv)$, azonban hátra van még az $(uv)^2 = -e$ egyenlőség. Mivel

$$v(uv)^2 = v(uv)(uv) = -v(vu)(uv) = -(vv)(uu)v = -v,$$

így adódik, hogy $v((uv)^2 + e) = 0$. $\mathcal{A}$ viszont nullosztómentes, illetve $v \neq 0$, így $(uv)^2 = -e$ kell legyen, tehát $u, v$ és $(uv)$ valóban hamiltoni számhármas. □

**2.2.3. Lemma** (Kvaternió-lemma)**.** *Minden nullosztómentes, valós, alternáló kvadratikus $\mathcal{A}$ algebra, amelyre $\dim \mathcal{A} \geq 3$, tartalmaz hamiltoni számhármast, ezáltal létezik olyan $\mathcal{B} \subset \mathcal{A}$ részalgebra, amelyre $e \in \mathcal{B}$ és $\mathcal{B} \simeq \mathbb{H}$.*

**Bizonyítás.** A Frobenius-lemma szerint $\operatorname{Im} \mathcal{A}$ altere az $\mathcal{A}$-nak, és mivel $\dim \mathcal{A} \geq 3$, így $\dim \operatorname{Im} \mathcal{A} \geq 2$. Ezért, az előző tétel értelmében, van $\mathcal{A}$-ban hamiltoni számhármas, amely elemek a tisztán képzetes kvaterniók bázisvektorainak tulajdonságaival bírnak. Kimondhatjuk tehát, hogy ez a hamiltoni számhármas és az $e \in \mathcal{A}$ egységelem az $\mathcal{A}$ olyan $\mathcal{B}$ részalgebráját generálja, amely izomorf a kvaterniók $\mathbb{H}$ algebrájával. □

**2.2.1. Megjegyzés.** Ellentmondásnak tűnik, hogy a lemmában a $\dim \mathcal{A} = 3$ esetet is megengedjük, hiszen nyilvánvalóan nem lehet egy háromdimenziós algebrának részalgebrája a négydimenziós $\mathbb{H}$. Azonban ez az eset nem is áll fenn, hiszen $\mathcal{A}$-ról feltettük, hogy nullosztómentes alternáló algebra, ami véges dimenzióban azt jelenti, hogy egységelemes division algebra (2.2.1 állítás 3. pontja (21. oldal)). A páratlan dimenziójú egységelemes division algebrák a 1.2.1 megjegyzés (11. oldal) 2. pontja szerint izomorfak $\mathbb{R}$-rel, azaz egydimenziósak, így a lemmában szereplő $\mathcal{A}$ algebra valójában legalább négydimenziós.

A kvadratikus algebrák és az előző állítások segítségével, most már felírható Ferdinand Georg Frobenius tétele, amely az alternálónál speciálisabb, asszociatív kvadratikus algebrák izomorfiáját adja meg:

**2.2.2. Tétel** (Frobenius-tétel)**.** *Legyen $\mathcal{A} \neq 0$ asszociatív, nullosztómentes, valós, kvadratikus algebra (azaz véges dimenzióban ferdetest). Ekkor az alábbi három eset közül pontosan egy teljesül:*

1. *$\mathcal{A}$ izomorf a valós számok $\mathbb{R}$ testével;*

2. *$\mathcal{A}$ izomorf a komplex számok $\mathbb{C}$ testével;*

3. *$\mathcal{A}$ izomorf a kvaterniók $\mathbb{H}$ ferdetestével.*

**Bizonyítás.** Mivel $\mathcal{A} \neq 0$, ezért $\dim \mathcal{A} \geq 1$, és létezik $e \in \mathcal{A}$ egységelem. Bontsuk fel az $\mathcal{A}$ dimenziója szerint a bizonyítást három esetre:

- $\dim \mathcal{A} = 1$: mivel $\mathcal{A}$ egy egységelemes $\mathbb{R}$-algebra, így az $f : \mathbb{R} \to \mathcal{A}$, $\alpha \mapsto \alpha e$ leképezés izomorfizmus, vagyis minden egydimenziós, egységelemes algebra izomorf $\mathbb{R}$-rel.

- $\dim \mathcal{A} = 2$: ekkor létezik $u \in \mathcal{A}$, melyre $u^2 = -e$, így az $f : \mathbb{C} \to \mathcal{A}$, $x+yi \mapsto xe+yu$ leképezés egy algebra homomorfizmus. Mivel $e$ és $u$ lineárisan függetlenek, így az $f$ injektív, továbbá $\dim \mathbb{C} = \dim \mathcal{A}$ miatt bijektív is, tehát $f$ izomorfizmus.

- $\dim \mathcal{A} \geq 3$: ebben az esetben a Kvaternió-lemma értelmében léteznie kell $u, v, w \in \operatorname{Im} \mathcal{A}$ hamiltoni számhármasnak, ahol $w = uv$. Legyen $x \in \operatorname{Im} \mathcal{A}$ tetszőleges. Ekkor

  $$xu + ux = \alpha e, \quad xv + vx = \beta e, \quad xw + wx = \gamma e,$$

  ahol $\alpha, \beta, \gamma \in \mathbb{R}$, hiszen minden $u, v \in \operatorname{Im} \mathcal{A}$ elemre

  $$uv + vu = (u + v)^2 - u^2 - v^2 \in \mathbb{R}e,$$

  mert a jobb oldalon a Frobenius-lemma értelmében csupa tisztán képzetes elem áll, melyek négyzetösszege definíció szerint valós. Ha az első kifejezést jobbról megszorozzuk $v$-vel, a másodikat pedig balról $u$-val, majd kivonjuk őket egymásból, akkor az

  $$xw - wx = \alpha v - \beta u$$

  egyenlőséget kapjuk, mivel $\mathcal{A}$ asszociatív. Ezt adjuk hozzá a harmadik kifejezéshez, így

  $$2xw = \alpha v - \beta u + \gamma e,$$

amit jobbról $w$-vel megszorozva:

$$-2x = \alpha u + \beta v + \gamma w,$$

azaz megmutattuk, hogy $\operatorname{Im} \mathcal{A} = \mathbb{R}u + \mathbb{R}v + \mathbb{R}w$, vagyis $\mathcal{A} \simeq \mathbb{H}$.

$\square$

**2.2.1. Következmény.** A tétel kimondja tehát, hogy a kvaterniók $\mathbb{H}$ algebrája izomorfia erejéig egyértelmű, azaz minden négy, vagy annál magasabb dimenziós $\mathbb{R}$ feletti ferdetest izomorf $\mathbb{H}$-val.

## 2.3. Kvadratikus algebrák lineáris és bilineáris formája

Ahhoz, hogy az oktávokat a kvaterniók összeillesztésének módszerével megkaphassuk, szükségünk lesz a konjugálás és a skaláris szorzat műveletekre is, azaz meg kell nézni, hogyan működnek ezek a kvadratikus algebrák esetében.

Legyen $\mathcal{A}$ egy $\mathbb{R}$ feletti kvadratikus algebra. Erre teljesül a Frobenius-lemma, ezért pontosan egy olyan $\lambda : \mathcal{A} \to \mathbb{R}$ lineáris forma, esetünkben lineáris funkcionál létezik, amire $\lambda(e) = 1$ és $\ker \lambda = \operatorname{Im} \mathcal{A}$. Mivel ez egyértelmű, ezt nevezzük a *kvadratikus algebra lineáris formájának.*

A konjugálás minden kvadratikus $\mathbb{R}$-algebrában definiálható a fenti $\lambda$ forma segítségével, a bázisra való tekintet nélkül, ugyanis

$$x \mapsto \overline{x} := 2\lambda(x)e - x.$$

Illetve, ha $u \in \operatorname{Im} \mathcal{A}$, akkor az $x = \lambda(x)e + u$ felírás használatával a következő definíciót nyerjük:

$$\overline{x} = \lambda(x)e - u.$$

A konjugálás, akárcsak a komplex számok és a kvaterniók esetében, itt is $\mathbb{R}e$-re való tükrözést jelent, így tehát adódnak azon tulajdonságok, miszerint $\overline{\overline{x}} = x$ és $\lambda(\overline{x}) = \lambda(x)$, vagyis a konjugálás fixpontjainak halmaza nem más, mint $\mathbb{R}e = \{x \in \mathcal{A} : \overline{x} = x\}$.

Most, hogy a konjugálás művelete már a rendelkezésünkre áll, természetesnek tűnik a feltételezés, miszerint $\mathcal{A}$-ban a skaláris szorzat a $\mathbb{C}$-ben és $\mathbb{H}$-ban megismert $\langle x, y\rangle = \lambda(x\overline{y}) = 2\lambda(x)\lambda(y) - \lambda(xy)$ alakban áll elő[4] [5]. Bár ez nullosztómentes esetben valóban igaz [5], az általánossag kedvéért, más módon fogjuk definiálni az $\langle x, y\rangle$ műveletet.

**2.3.1. Lemma.** *Legyen $\mathcal{A}$ kvadratikus algebra, amely lineáris formáját jelölje $\lambda$. Továbbá legyen a $\langle .\,, .\rangle : \mathcal{A} \times \mathcal{A} \to \mathbb{R}$ művelet a következő:*

$$(x, y) \mapsto \langle x, y\rangle := 2\lambda(x)\lambda(y) - \frac{1}{2}\lambda(xy + yx).$$

*Ez egy szimmetrikus bilineáris forma, amelyre $\forall x, y \in \mathcal{A}$ esetén teljesülnek az alábbi tulajdonságok:*

[4] $\mathbb{C}$-ben és $\mathbb{H}$-ban a $\lambda$ formára általában a valós rész kifejezést használjuk, melynek jele Re.

1. $\langle x, x\rangle = 2\lambda(x)^2 - \lambda(x^2)$;

2. $\langle x, e\rangle = \lambda(x)$, *illetve* $\langle e, e\rangle = 1$;

3. $x^2 = 2\lambda(x)x - \langle x, x\rangle e$;

4. $xy + yx = 2\lambda(x)y + 2\lambda(y)x - 2\langle x, y\rangle e$.

*Ha $\mathcal{A}$ nullosztómentes, akkor $\langle x, x\rangle > 0$ $\forall x \neq 0$ esetén.*

**Bizonyítás.** Mivel $\langle x, y\rangle$ definíció szerint szimmetrikus bilineáris forma, így az 1. és a 2. tulajdonság triviálisan következik. A 3. pont bizonyításához használjuk fel, hogy $x - \lambda(x)e \in \ker\lambda = \operatorname{Im}\mathcal{A}$. Mivel $\operatorname{Im}\mathcal{A} = \{x \in \mathcal{A} : x^2 \in \mathbb{R}e \text{ és } x \notin \mathbb{R}e\backslash\{0\}\}$ definíció szerint, ezért következik, hogy $(x - \lambda(x)e)^2 = -\omega(x)e$, ahol $\omega(x) \in \mathbb{R}$ és $x \in \mathcal{A}$. Ha ezt átrendezzük $x^2$-re, majd alkalmazzuk rá $\lambda$-t, akkor a következőt kapjuk:

$$x^2 = 2\lambda(x)x - [\lambda(x)^2 + \omega(x)]e,$$

$$\lambda(x^2) = 2\lambda(x)^2 - \lambda(x)^2 - \omega(x) = \lambda(x)^2 - \omega(x).$$

Ha összevetjük ezt az 1. tulajdonsággal: $\lambda(x^2) = 2\lambda(x)^2 - \langle x, x\rangle$, akkor arra jutunk, hogy

$$2\lambda(x)^2 - \langle x, x\rangle = \lambda(x)^2 - \omega(x),$$

$$\langle x, x\rangle = \lambda(x)^2 + \omega(x),$$

ami az $x^2$-re rendezett képletbe helyettesítve a 3. tulajdonságot adja. A 4. tulajdonság egyszerűen következik a linearitásból és a 3. tulajdonságból, ha $x$ helyére $(x + y)$-t helyettesítünk. Mivel $(x + y)^2 = x^2 + xy + yx + y^2$ és az előzőek alapján $x^2 = 2\lambda(x)x - \langle x, x\rangle e$ és $y^2 = 2\lambda(y)y - \langle y, y\rangle e$, így

$$(x + y)^2 = 2\lambda(x + y)(x + y) - \langle x + y, x + y\rangle e =$$

$$= 2[\lambda(x)x + \lambda(x)y + \lambda(y)x + \lambda(y)y] - [\langle x, x\rangle + \underbrace{\langle x, y\rangle + \langle y, x\rangle}_{2\langle x,y\rangle} + \langle y, y\rangle]e,$$

amelybe az $x^2$-re és $y^2$-re kapott összefüggéseket behelyettesítve, a 4. tulajdonságot kapjuk.

Hátra van még, hogy nullosztómentes esetben $\langle x, x\rangle > 0$ $\forall x \neq 0$-ra. Azt állítjuk, hogy ha $\mathcal{A}$ nullosztómentes, akkor minden $u \in \operatorname{Im}\mathcal{A}$, $u \neq 0$ esetén $u^2 = -\omega e$, ahol $\omega > 0$.

Mivel $u \in \operatorname{Im} \mathcal{A}$ és $u \neq 0$, így $u^2 = \alpha e$, ahol $\alpha \in \mathbb{R} \backslash \{0\}$. Tegyük fel, hogy $\alpha > 0$, ekkor $\alpha = \beta^2$ alakba írható, ahol $\beta \in \mathbb{R}$, így a következő teljesül:

$$(u - \beta e)(u + \beta e) = u^2 - \beta^2 e = u^2 - \alpha e = 0.$$

Feltettük, hogy $\mathcal{A}$ nullosztómentes, ezért $(u - \beta e)$ vagy $(u + \beta e)$ nulla kell legyen, ami azt jelenti, hogy $u \in \mathbb{R}e$, vagyis ellentmondásra jutottunk.

Az $\langle x, x \rangle = \lambda(x)^2 + \omega(x)$ összefüggés jobb oldalán $\lambda(x)^2 \geq 0$, illetve az előző állítás értelmében $w(x) > 0$, tehát $\langle x, x \rangle > 0$ minden $x \neq 0$ esetén. □

**2.3.1. Következmény.** A bizonyítás végén lévő állításból kapjuk, hogy a nullosztómentes $\mathcal{A}$ algebrákban, minden $u' \in \operatorname{Im} \mathcal{A}$, $u' \neq 0$, azaz tisztán képzetes, nem nulla elemet normalizálhatunk, azaz létezik olyan $u = \gamma u'$ ($\gamma \in \mathbb{R}$), hogy $u^2 = -e$.

A fenti $\langle . , . \rangle$ bilineáris forma, mivel a $\lambda$ lineáris formával definiáltuk, szintén egyértelműen létezik minden kvadratikus algebra esetén, ezért a továbbiakban úgy hivatkozunk rá, mint a *kvadratikus algebra bilineáris formája.* Nézzünk most meg néhány összefüggést a lineáris és bilineáris formák között, amelyekre a későbbiek során szükségünk lesz:

**2.3.1. Tétel.** *Legyen $\mathcal{A}$ egy alternáló kvadratikus algebra, $x, y, z \in \mathcal{A}$ és jelölje $\lambda$, illetve $\langle . , . \rangle$ az algebra lineáris és bilineáris formáját. Ekkor*

1. $\lambda(xy) = \lambda(yx)$, *következésképpen* $\langle x, y \rangle = 2\lambda(x)\lambda(y) - \lambda(xy)$,
2. $\lambda(xyz) := \lambda(xy \cdot z) = \lambda(x \cdot yz)$, *vagyis* $\lambda$ *asszociatív,*
3. $\langle xy, z \rangle + \langle xz, y \rangle = 2\lambda(x)\langle y, z \rangle$,
4. $\langle xy, xy \rangle = \langle x, x \rangle \langle y, y \rangle$.
5. *Ha $\mathcal{A}$ bilineáris formája pozitív definit, akkor $\mathcal{A}$ nullosztómentes.*

**Bizonyítás.** Az első három összefüggés igazolásához feltehetjük, hogy $x, y, z \in \operatorname{Im} \mathcal{A}$, hiszen ezen multilineáris azonosságok akkor is érvényben maradnak, ha az $\mathcal{A}$ bármely eleméhez az $e$ egységelem skalárszorosát hozzáadjuk.

Ahhoz, hogy a kívánt összefüggéseket beláthassuk, vezessünk le néhány segédállítást:

- Az alternáló algebrák definíciója szerint $\forall x, y \in \mathcal{A}$ elemre igaz, hogy $(xy)y = xy^2$. Ha $y$ helyére $x + y$ kerül, akkor

$$[x(x+y)](x+y) = x(x+y)^2$$

$$(x^2 + xy)(x+y) = x(x^2 + xy + yx + y^2)$$

$$x^3 + (xy)x + x^2y + xy^2 = x^3 + x^2y + x(yx) + xy^2,$$

ahol két tagot leszámítva minden kiesik, így az

$$(xy)x = x(yx) \tag{1}$$

egyenlőségre jutunk.

- A 2.3.1 lemma (27. oldal) 4. pontja szerint $xy+yx = 2\lambda(x)y+2\lambda(y)x-2\langle x, y\rangle e$, ami $x, y \in \operatorname{Im}\mathcal{A}$ esetén: $xy + yx = -2\langle x, y\rangle e$. Ha ezt jobbról megszorozzuk egy $z \in \operatorname{Im}\mathcal{A}$ elemmel, akkor az

$$xy \cdot z + yx \cdot z = -2\langle x, y\rangle z \tag{2}$$

azonosságot kapjuk. Hasonlóan, $xz + zx = -2\langle x, z\rangle e$, amit $y$-nal balról szorozva:

$$y \cdot xz + y \cdot zx = -2\langle x, z\rangle y. \tag{3}$$

- Ha az $xy + yx = 2\lambda(x)y + 2\lambda(y)x - 2\langle x, y\rangle e$ kifejezésben $y$-t $yz$-re cseréljük, akkor az alábbi azonosságot nyerjük:

$$x \cdot yz + yz \cdot x = 2\lambda(yz)x - 2\langle x, yz\rangle e. \tag{4}$$

Ha a (2) és (3) kifejezésekben $z = y$, majd alkalmazzuk az (1) összefüggést, akkor arra jutunk, hogy

$$0 = xy \cdot x - x \cdot yx = -2\left(\langle x, y\rangle + \lambda(xy)\right)x + 2\langle x, yx\rangle e,$$

azaz $\langle x, y\rangle + \lambda(xy) = 0$ és $\langle x, yx\rangle = 0$ minden $x, y \in \operatorname{Im}\mathcal{A}$-ra. Innen már adódik a tételben szereplő 1. és 3. azonosság, ugyanis $x, y \in \operatorname{Im}\mathcal{A}$-ra

$$\lambda(xy) = -\langle x, y\rangle = \frac{1}{2}\lambda(xy + yx) = \frac{1}{2}\lambda(xy) + \frac{1}{2}\lambda(yx),$$

ami 2-vel felszorozva, majd átrendezve a tétel 1. pontját adja. A korábban kapott $\langle x, yx\rangle = 0$ (minden $x, y \in \operatorname{Im}\mathcal{A}$-ra) összefüggést és a linearitást felhasználva:

$$0 = \langle y + z, x(y+z)\rangle = \langle y + z, xy + xz\rangle = \langle xy, z\rangle + \langle xz, y\rangle,$$

ahol $z \in \operatorname{Im} \mathcal{A}$. Legyen most $x$ az $\mathcal{A}$ tetszőleges eleme, azaz $x = ae + x'$, ahol $a \in \mathbb{R}$ és $x' \in \operatorname{Im} \mathcal{A}$. Ekkor

$$\langle xy, z\rangle + \langle xz, y\rangle = \langle (ae+x')y, z\rangle + \langle (ae+x')z, y\rangle = \langle ay, z\rangle + \langle x'y, z\rangle + \langle az, y\rangle + \langle x'z, y\rangle,$$

ahol $\langle x'y, z\rangle + \langle x'z, y\rangle = 0$ az előzőek alapján, így $\langle ay, z\rangle + \langle az, y\rangle = 2a\langle y, z\rangle = 2\lambda(x)\langle y, z\rangle$.

A 2. pont bizonyításához használjuk fel, hogy az (1) állítás következtében: $\lambda(x \cdot yx) = \lambda(xy \cdot x)$. Ha $x$ helyett $x + z$-t veszünk, akkor

$$\lambda\left[(x+z) \cdot [y \cdot (x+z)]\right] = \lambda(x \cdot yx + x \cdot yz + z \cdot yx + z \cdot yz) =$$

$$= \lambda(xy \cdot x + xy \cdot z + zy \cdot x + zy \cdot z) = \lambda\left[[(x+z) \cdot y] \cdot (x+z)\right],$$

ahol az előbbi észrevételt ismét kihasználva:

$$\lambda(x \cdot yz) + \lambda(z \cdot yx) = \lambda(xy \cdot z) + \lambda(zy \cdot x), \tag{5}$$

minden $x, y, z \in \operatorname{Im} \mathcal{A}$ elemre. A (2) összefüggésből adódik, hogy $\lambda(xy \cdot z) = -\lambda(yx \cdot z)$, a (3) azonosságból pedig azt kapjuk (a képletben $x$ és $y$ szerepét felcserélve), hogy $\lambda(x \cdot yz) = -\lambda(x \cdot zy)$, így a tétel 1. pontját és az előbbi két következményt felhasználva, az (5) egyenlet a bizonyítani kívánt 2. pontot adja.

A 4. pont igazolásához, vegyük a 3. pontban lévő összefüggést, legyen $z = xy$, majd alkalmazzuk az alternáló algebrák tulajdonságát, miszerint $x^2y = x \cdot xy$, minden $x, y \in \mathcal{A}$ esetén. Így, a 2.3.1 lemma 3. pontjában megfogalmazott $x^2 = 2\lambda(x)x - \langle x, x\rangle e$ azonosságot felhasználva:

$$\langle xy, xy\rangle = 2\lambda(x)\langle y, yx\rangle - \langle x^2y, y\rangle = -\left\langle \left(x^2 - 2\lambda(x)x\right) y, y\right\rangle =$$

$$= -\left\langle -\langle x, x\rangle y, y\right\rangle = \langle x, x\rangle\langle y, y\rangle.$$

Végezetül, ha $xy = 0$, akkor a tétel 4. pontja szerint $\langle x, x\rangle = 0$ vagy $\langle y, y\rangle = 0$, ami pozitív definit bilineáris forma esetén azt jelenti, hogy $x = 0$ vagy $y = 0$, vagyis $\mathcal{A}$ nullosztómentes. □

**2.3.2. Következmény.** Legyen $x, y \in \operatorname{Im} \mathcal{A}$. Ekkor az alábbi állítások ekvivalensek:

- $x$ és $y$ ortogonálisak, azaz $\langle x, y\rangle = 0$;
- $xy + yx = 0$;
- $\lambda(xy) = 0$.

## 2.4. A Cayley-számok $\mathbb{O}$ algebrája

Hamilton megmutatta, hogy a komplex számok előállnak $\mathbb{R} \times \mathbb{R}$ alakban, azaz valós számpárokként, ha a következőképpen definiáljuk a szorzást: $(a_1, a_2)(b_1, b_2) = (a_1 b_1 - b_2 a_2, a_2 b_1 + b_2 a_1)$, ahol $a_1, a_2, b_1, b_2 \in \mathbb{R}$. Analóg módon a kvaterniók $\mathbb{H}$ algebrája is előállítható, izomorfizmus erejéig egyértelműen, a komplex számok keresztszorzataként: $\mathbb{C} \times \mathbb{C}$-ben a szorzást $(a_1, a_2)(b_1, b_2) = (a_1 b_1 - \overline{b}_2 a_2, a_2 \overline{b}_1 + b_2 a_1)$ $(a_1, a_2, b_1, b_2 \in \mathbb{C})$ alakban definiálva.

Ahogy a fejezet elején is tárgyaltuk, ezt az ötletet kihasználva megnézzük, hogyan állítható elő $\mathbb{H}$ megduplázásának segítségével a Cayley-számok $\mathbb{O}$ algebrája. Az előző bekezdésben ismertettek alapján, definiáljuk $\mathbb{H} \times \mathbb{H}$-ban a szorzást a következőképpen:

$$xy = (x_1, x_2)(y_1, y_2) := (x_1 y_1 - \overline{y}_2 x_2, x_2 \overline{y}_1 + y_2 x_1),$$

ahol $x = (x_1, x_2)$ és $y = (y_1, y_2)$ a $\mathbb{H} \times \mathbb{H}$ tér egy-egy eleme, így egy nyolcdimenziós $\mathbb{R}$-algebrát kaptunk, amelyet a *Cayley-számok algebrájának* nevezünk és $\mathbb{O}$-val jelölünk. Mivel a kvaterniók körében a szorzás nem kommutatív, így fontos megjegyezni, hogy a fenti összefüggés jobb oldalán lévő szorzások sorrendje nem felcserélhető, például $x_1 y_2$ helyett $y_2 x_1$-et írva egészen más algebrát kapnánk.

A következő állításhoz szükségünk lesz a Cayley-algebra egységelemére, azaz $e$-re, amelyet azonban könnyen megkapunk a kvaterinó-algebra $e'$ egységelemét felhasználva, ugyanis $e := (e', 0)$.

**2.4.1. Állítás.** *Az $\mathbb{O}$ kvadratikus algebra, azaz $\forall x = (x_1, x_2) \in \mathbb{O}$ esetén:*

$$x^2 = 2\,\mathrm{Re}(x_1)x - (\langle x_1, x_1 \rangle + \langle x_2, x_2 \rangle)\, e.$$

**Bizonyítás.** A definícióból következik, hogy $x^2 = (x_1^2 - \overline{x}_2 x_2, x_2 \overline{x}_1 + x_2 x_1)$, és mivel kvaterniókra teljesülnek a következő összefüggések [5]:

- $x_1^2 = 2\,\mathrm{Re}(x_1)x_1 - \langle x_1, x_1 \rangle e'$;
- $\overline{x}_2 x_2 = \langle x_2, x_2 \rangle e'$;
- $\overline{x}_1 + x_1 = 2\,\mathrm{Re}(x_1)e'$,

így $x^2 = (2\,\mathrm{Re}(x_1)x_1 - (\langle x_1, x_1 \rangle + \langle x_2, x_2 \rangle)e', 2\,\mathrm{Re}(x_1)x_2)$, ami a linearitást kihasználva a kívánt összefüggést adja. □

Az $\mathbb{O}$ tehát kvadratikus algebra, így az $\operatorname{Im}\mathbb{Q}$ altér, a $\lambda$ lineáris forma, a $\langle\cdot,\cdot\rangle$ bilineáris forma és az $x \mapsto \overline{x}$ konjugálás definiálva vannak. Ha az előzőekhez hasonlóan, kvaternió párokként írjuk fel $\mathbb{O}$ elemeit, máris adódnak az alábbi összefüggések [5]:

**2.4.2. Állítás.**

1. $\lambda(x) = \operatorname{Re}(x_1)$;
2. $\langle x, y\rangle = \langle x_1, y_1\rangle + \langle x_2, y_2\rangle$;
3. $\operatorname{Im}\mathbb{O} = \operatorname{Im}\mathbb{H} \times \mathbb{H}$;
4. $\overline{x} = (\overline{x}_1, -x_2)$.

**2.4.1. Megjegyzés.** Mivel $\mathbb{H}$ bilineáris formája pozitív definit[5], így a 2. összefüggésből következik, hogy az $\mathbb{O}$ bilineáris formája is pozitív definit, vagyis $\mathbb{O}$ euklideszi vektortér[6].

Ezen tulajdonságok ismeretében már bizonyíthatjuk az alábbi állításokat:

**2.4.3. Állítás.** *Legyen $x, y \in \mathbb{O}$. Ekkor igazak az alábbi összefüggések:*

1. $\overline{xy} = \overline{y}\,\overline{x}$,
2. $x\overline{x} = \overline{x}x = \langle x, x\rangle e$,
3. $x(\overline{x}y) = \langle x, x\rangle y = (x\overline{x})y$.

**Bizonyítás.** Az 1. és 2. tulajdonságok következnek az oktávok szorzási szabályából, illetve a korábban említett $\overline{x} = (\overline{x}_1, -x_2)$ összefüggésből, hiszen

$$\overline{xy} = \overline{(x_1y_1 - \overline{y}_2x_2, x_2\overline{y}_1 + y_2x_1)} = (\overline{x_1y_1 - \overline{y}_2x_2}, -x_2\overline{y}_1 - y_2x_1) =$$

$$= (\overline{y}_1\overline{x}_1 - \overline{x}_2y_1, -x_2\overline{y}_1 - y_2x_1) = \overline{y}\,\overline{x},$$

$$x\overline{x} = (x_1\overline{x}_1 + \overline{x}_2x_2, x_2x_1 - x_2x_1) = \overline{x}x.$$

A fenti 2.4.2 állítás 2. pontja szerint $\langle x, y\rangle = \langle x_1, y_1\rangle + \langle x_2, y_2\rangle$, így

$$x\overline{x} = (x_1\overline{x}_1 + \overline{x}_2x_2, x_2x_1 - x_2x_1) = (\langle x_1, x_1\rangle + \langle x_2, x_2\rangle, 0) = \langle x, x\rangle e.$$

[5] $\mathbb{H}$ ferdetest, így nullosztómentes és kvadratikus is, amiből a 2.3.1 lemma (27. oldal) utolsó állítása szerint adódik, hogy a bilineáris formája pozitív definit.

[6] Ha $V$ egy valós vektortér, és értelmezve van egy $V \times V \to \mathbb{R}$, $(x, y) \to \langle x, y\rangle$ skaláris szorzatnak nevezett művelet, amely szimmterikus és pozitív definit, azaz $\langle x, y\rangle = \langle y, x\rangle$ és $\langle x, x\rangle > 0$ minden $x \neq 0$ esetén, akkor a $V$ teret, ezzel a skalárszorzattal együtt, *euklideszi vektortér*nek nevezzük.

A 3. tulajdonság bizonyításához vegyük az alábbi szorzatot:

$$\overline{x}y = (\overline{x}_1, -x_2)(y_1, y_2) = (\overline{x}_1 y_1 + \overline{y}_2 x_2, -x_2\overline{y}_1 + y_2\overline{x}_1).$$

Mivel $\mathbb{H}$ asszociatív, így

$$x(\overline{x}y) = (x_1[\overline{x}_1 y_1 + \overline{y}_2 x_2] - [-y_1\overline{x}_2 + x_1\overline{y}_2]x_2, x_2[\overline{y}_1 x_1 + \overline{x}_2 y_2] + [-x_2\overline{y}_1 + y_2\overline{x}_1]x_1) =$$

$$= (x_1\overline{x}_1 y_1 + y_1\overline{x}_2 x_2, x_2\overline{x}_2 y_2 + y_2\overline{x}_1 x_1) = (\langle x_1, x_1\rangle + \langle x_2, x_2\rangle)y,$$

ami a 2.4.2 állítás 2. pontja, illetve az imént igazolt 1. tulajdonság miatt, a kívánt összefüggést adja. □

**2.4.1. Tétel.** *Az $\mathbb{O}$ alternáló division algebra.*

**Bizonyítás.** Az $\mathbb{O}$ algebráról már tudjuk, hogy kvadratikus, ezért egy $x \in \mathbb{O}$ elemre igaz, hogy $\overline{x} = 2\lambda(x)e - x$, ahol $\lambda$ továbbra is az $\mathbb{O}$ lineáris formáját jelöli. Ezt felhasználva a 2.4.3 állítás (33. oldal) 3. tulajdonsága

$$x(2\lambda(x)y - xy) = (2\lambda(x)x - x^2)y$$

alakba írható, melyből következik, hogy $x(xy) = x^2y$ minden $x, y \in \mathbb{O}$ elemre. Továbbá konjugálással megkapjuk, hogy $(\overline{yx})\overline{x} = \overline{y}\,\overline{x}^2$, és mivel ez is minden $x, y \in \mathbb{O}$ elemre teljesül, így az $(yx)x = yx^2$ összefüggés is igaz az $\mathbb{O}$ minden elemére, következésképpen az $\mathbb{O}$ alternáló.

Mivel az $\mathbb{O}$ véges dimenziós, ezért ahhoz, hogy division algebra, elég belátni, hogy nullosztómentes. Ez azonban következik a 2.3.1 tétel (29. oldal) 5. pontjából. □

## 2.5. A Cayley-algebra egyértelműsége

Megkaptuk tehát, hogy a Cayley-számok $\mathbb{O}$ algebrája alternáló division algebra. Természetesen adódik a kérdés, hogy létezik-e magasabb, de továbbra is véges dimenziós alternáló division algebra, azaz bővíthetjük-e a dimenziószámot úgy, hogy közben minden tulajdonságot megőrzünk. A válasz azonban nem, melynek magyarázatát Max August Zorn tétele adja.

**2.5.1. Tétel.** *Minden alternáló, kvadratikus, de nem asszociatív, nullosztómentes valós algebra izomorf a Cayley-számok $\mathbb{O}$ algebrájával.*

**Bizonyítás.** Legyen $\mathcal{A}$ alternáló, kvadratikus, nullosztómentes, nem asszociatív valós algebra. Ekkor a Frobenius-tétel szerint $\dim \mathcal{A} > 4$, ugyanis a tétel bizonyítását megvizsgálva adódik, hogy minden egy és kétdimenziós nullosztómentes kvadratikus algebra izomorf $\mathbb{R}$-rel vagy $\mathbb{C}$-vel, az asszociativitásra vagy alternálóságra való tekintet nélkül. Ha $\mathcal{A}$ legalább háromdimenziós, akkor a Kvaternió-lemma (24. oldal) szerint tartalmaz hamiltoni számhármast, amely az egységelemmel (minden alternáló division algebra egységelemes) egy $\mathbb{H}$-val izomorf algebrát generál, így négydimenzióban ez az egyetlen kvadratikus division algebra. Mivel $\mathbb{H}$ asszociatív, az $\mathcal{A}$-ról pedig feltettük, hogy nem az, így szükségképpen $\dim \mathcal{A} > 4$. Szintén a Kvaternió-lemma következtében, létezik egy $\mathcal{B} \subset \mathcal{A}$ részalgebra, amely izomorf a kvaterniók $\mathbb{H}$ algebrájával, így az is igaz, hogy van olyan $f : \mathbb{H} \to \mathcal{A}$ algebra izomorfizmus, amelyre $f(\mathbb{H}) = \mathcal{B}$.

Feltettük, hogy $\mathcal{A}$ nem asszociatív, azonban alternáló algebraként a 2.2.1 (21. oldal) állítás értelmében erősen asszociatív, így a $\mathcal{B}$ részalgebra asszociatív kell legyen, következésképpen $\mathcal{B} \neq \mathcal{A}$. A Frobenius-lemma szerint $\mathcal{A} = \mathbb{R}e \oplus \operatorname{Im} \mathcal{A}$ és $\mathcal{B} = \mathbb{R}e \oplus \operatorname{Im} \mathcal{B}$, de mivel $\mathcal{A} \neq \mathcal{B}$, ezért van olyan $0 \neq q \in \operatorname{Im} \mathcal{A}$, amire $q^2 = -e$ és $\langle \mathcal{B}, q \rangle = 0$, azaz ortogonális $\mathcal{B}$ minden elemére. Ekkor azt állítjuk, hogy a $\mathcal{B} \oplus \mathcal{B}q = \{u + vq : u, v \in \mathcal{B}\}$ olyan részalgebrája $\mathcal{A}$-nak, amelyre $\dim(\mathcal{B} \oplus \mathcal{B}q) = 2 \dim \mathcal{B}$, $e \in \mathcal{B} \oplus \mathcal{B}q$ és teljesülnek az alábbi tulajdonságok:

1. $u \cdot vq = vu \cdot q$;

2. $uq \cdot v = u\overline{v} \cdot q$, másképpen $qv = \overline{v}q$;

3. $uq \cdot vq = -\langle q, q \rangle \cdot \overline{v}u$,

ahol $u, v \in \mathcal{B}$. Az utóbbi három összefüggés igazolásához feltehetjük, hogy $u, v \in \operatorname{Im} \mathcal{B}$, ugyanis $u, v \in \mathbb{R}e$ esetén az 1. és 2. állítás triviális, a 3. állítás pedig a 2.3.1 lemma (27. oldal) 3. pontjában kimondott $q^2 = -\langle q, q\rangle$ összefüggésre vezet vissza. Az 1. állítás szerint

$$u \cdot vq - vu \cdot q = u \cdot vq + uv \cdot q - (uv + vu)q = 0.$$

Mivel $\mathcal{A}$ alternáló, így $v$-vel balról szorozva könnyen ellenőrizhető a következő az összefüggés: $vu \cdot q + vq \cdot u = v \cdot uq + v \cdot qu$. Továbbá a kvadratikus algebrák bilineáris formájára vonatkozó 2.3.1 lemma és 2.3.1 tétel (29. oldal) állításait kihasználva könnyen ellenőrizhetők az alábbi egyenlőségek:

(A) $uv \cdot q + vu \cdot q = -2\langle u, v\rangle q$;

(B) $v \cdot uq + v \cdot qu = -2\langle u, q\rangle v$;

(C) $u \cdot vq + vq \cdot u = 2\lambda(vq)u - 2\langle u, vq\rangle e$.

Ezen három tulajdonság és az előbb említett $vu \cdot q + vq \cdot u = v \cdot uq + v \cdot qu$ felhasználásával, az

$$u \cdot vq + uv \cdot q - (uv \cdot q + vu \cdot q) = (A) - (B) + (C) - (A) = 2\langle u, q\rangle v - 2\lambda(vq)u + 2\langle u, vq\rangle e =$$

$$= 2\lambda(u)\lambda(q)v - 2\lambda(uq)v - 2\lambda(vq)u + 2\lambda(u)\lambda(vq)e - 2\lambda(uvq)e$$

összefüggést kapjuk. Mivel $q$ definíció szerint merőleges minden $u, v \in \mathcal{B}$ elemre, így a 2.3.2 következmény (31. oldal) értelmében a jobb oldalon $\lambda$ minden értéke nulla.

A 2. állítás szintén adódik az előbb említett következményben megfogalmazott $qv = -vq$ tulajdonságból, hiszen $v \in \operatorname{Im} \mathcal{B}$, azaz $\overline{v} = -v$, ami szintén $\operatorname{Im} \mathcal{B}$ eleme, így $q$ rá is merőleges.

A 3. állításhoz először is lássuk be, hogy $u, q$ és $vq$ páronként merőlegesek egymásra. Azt állítjuk, hogy egy alternáló kvadratikus algebra bármely $x, y, z$ elemére igaz a következő két összefüggés:

$$\langle x, y\rangle = \lambda(x\overline{y}) = \lambda(\overline{x}y), \qquad \langle xy, z\rangle = \langle x, z\overline{y}\rangle = \langle y, \overline{x}z\rangle.$$

Mivel a lineáris forma definíciója szerint $x = 2\lambda(x)e - \overline{x}$, így adódik, hogy

$$\lambda(xy) = 2\lambda(x)\lambda(y) - \lambda(\overline{x}y),$$

ami a 2.3.1 tétel (29. oldal) 1. pontja szerint a kívánt összefüggést adja. Hasonlóan belátható az $\langle x, y\rangle = \lambda(x\overline{y})$ tulajdonság. Szintén az előbb említett tétel 1. és 2. pontjának következtében:

$$\langle xy, z\rangle = \lambda(xy \cdot \overline{z}) = \lambda(x \cdot y\overline{z}) = \langle x, z\overline{y}\rangle,$$

amellyel analóg módon vezethető le az $\langle y, \overline{x}z\rangle = \langle x, z\overline{y}\rangle$ összefüggés.

Ezt felhasználva kimondhatjuk, hogy $\langle u, vq\rangle = \langle \overline{v}u, q\rangle = 0$, továbbá $\lambda(vq \cdot q) = \lambda(vq^2) = -\langle q, q\rangle\lambda(v) = 0$, tehát $u, q$ és $vq$ valóban páronként merőlegesek egymásra, így az előzőek alapján arra jutunk, hogy

$$uq \cdot vq = -(vq \cdot q)u = -\langle q, q\rangle\overline{v}u.$$

Megkaptuk tehát a bizonyítani kívánt három tulajdonságot, melyek következménye, hogy a korábban definiált $\mathcal{B} + \mathcal{B}q$ valóban részalgebrája az $\mathcal{A}$-nak, ahol a dimenziószámra tett elvárás triviálisan teljesül, de be kell még látni, hogy $\langle \mathcal{B}, \mathcal{B}q\rangle = 0$, azaz $\langle u, vq\rangle = 0$ minden $u, v \in \mathcal{B}$-re. Ez viszont teljesül, az imént igazolt 1. és 2. tulajdonságok következtében:

$$\langle u, vq\rangle = -\frac{1}{2}\lambda(u \cdot vq + vq \cdot u) = -\frac{1}{2}\lambda(vu \cdot q + v\overline{u} \cdot q) = -\frac{1}{2}\lambda\left(v(u + \overline{u})q\right) =$$

$$= -\frac{1}{2}\lambda(vq) \cdot 2\lambda(u) = 0.$$

Mielőtt továbbléphetnénk, szükségünk lesz a Cayley-számok kvaterinópárokkal történő felírására, vagyis vizsgáljuk meg a következő állításokat: a Cayley-számok algebrája előáll $\mathbb{O} = \mathbb{H}e \oplus \mathbb{H}p$ alakban, ahol $p = (0, e')$ ($e'$ a $\mathbb{H}$ ferdetest egységeleme):

$$p^2 = -e, \qquad (a_1, a_2) = a_1 + a_2 p \text{ minden } (a_1, a_2) \in \mathbb{O}\text{-ra.}$$

Ekkor minden $u, v \in \mathbb{H}$ elemre teljesül, hogy

1. $u(vp) = (vu)p$;
2. $(up)v = (u\overline{v})p$, azaz $pv = \overline{v}p$;
3. $(up)(vp) = -\overline{v}u$.

Mivel $(a_1, a_2) = a_1e + a_2p$, ezért világos, hogy $\mathbb{O} = \mathbb{H} + \mathbb{H}p$. Továbbá minden elemre teljesül, hogy $\langle (a_1, 0), (0, a_2)\rangle = \langle a_1, 0\rangle + \langle 0, a_2\rangle = 0$, tehát a felírás a skaláris szorzatra nézve ortogonális, következésképpen direkt összeg. A három tulajdonság is könnyen ellenőrizhető:

1. $u(vp) = u(0, v) = (0, vu) = (vu)p$;
2. $(up)v = (0, u)v = (0, u\overline{v}) = (u\overline{v})p$;
3. $(up)(vp) = (0, u)(0, v) = (-\overline{v}u, 0) = -\overline{v}u$.

Az eddig bizonyított tételek felhasználásával megadhatjuk az

$$\mathbb{O} = \mathbb{H}e \oplus \mathbb{H}p \to \mathcal{B} \oplus \mathcal{B}q, \quad ue + vp \mapsto f(u) + f(v)q$$

leképezést, amely bijektív és $\mathbb{R}$-lineáris, és mivel a $\mathcal{B} \oplus \mathcal{B}q$-re igazolt 1-3 tulajdonságok megegyeznek az $\mathbb{O}$-ra bizonyított összefüggésekkel, ezért a fenti leképezés valóban algebra izomorfizmus.

Ha $\mathcal{B} \oplus \mathcal{B}q$ nem lenne egyenlő $\mathcal{A}$-val, akkor az erős asszociativitás miatt asszociatív kellene legyen, ami ellentmondás, hiszen $\mathbb{O}$-ról tudjuk, hogy nem asszociatív, tehát $\mathcal{A} = \mathcal{B} \oplus \mathcal{B}q \simeq \mathbb{O}$. □

Végezetül, a fenti tétel ismeretében kimondhatjuk a Frobenius-tétel általánosítását, miszerint minden nullosztómentes, alternáló, kvadratikus valós algebra izomorf $\mathbb{R}$-rel, $\mathbb{C}$-vel, $\mathbb{H}$-val vagy $\mathbb{O}$-val.

# Irodalom

[1] Dirk. J. Struik. *A matematika rövid története.* Gondolat Kiadó, 1958

[2] K.A. Ribnyikov. *A matematika története.* Tankönyvkiadó, 1968

[3] Sain Márton. *Nincs királyi út!.* Gondolat Kiadó, 1986

[4] R. Harré. *Some Nineteenth Century British Scientists.* Pergamon, 1969

[5] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch. *Graduate Texts in Mathematics: Numbers.* Springer, 1990

[6] Kiss Emil. *Bevezetés az algebrába.* Typotex, 2007

[7] Iszaj Lvovics Kantor, Alexandr Szamuilovics Szolodovnyikov. *Hiperkomplex számok.* Gondolat Kiadó, 1985

[8] J. P. Ward. *Quaternions and Cayley Numbers.* Springer, 1997

[9] John H. Conway, Derek A. Smith. *On Quaternions and Octonions.* A. K. Peters, 2003

[10] Nathan Jacobson. *Basic algebra I.* W. H. Freeman, 1985