# KOCKARÁCSOK

KUTAS PÉTER

A szakdolgozatom alapobjektumai olyan egész vektorok, amik páronként ortogonálisak és ugyanolyan hosszúak. Ha ilyenből dimenziószámnyi van, akkor ezeket rácskockának nevezzük (ahogy azt 3-dimenzióban megszoktuk). Számos megoldatlan és érdekes kérdés kapcsolódik ehhez a témakörhöz. Megkérdezhetjük például az alábbiakat:

(1) Mik azok az egész vektorok melyekhez van rá merőleges és vele azonos hosszú egész vektor? (Az ilyeneket ikervektoroknak hívjuk.)
(2) Adott $n$-dimenzióban $n-1$ egész vektor, amik páronként ortogonálisak és ugyanolyan hosszúak. Található-e hozzájuk egy $n$-edik egész vektor amelyik mindegyikre merőleges és szintén ugyanolyan hosszú?
(3) Milyen dimenzióban igaz az, hogy minden vektor kiterjeszthető rácskockává?
(4) Általánosan: $n$-dimenzióban adott $k$ vektor, melyek páronként ortogonálisak és ugyanolyan hosszúak. Kiterjeszthetők-e rácskockává?
(5) Hány rácskocka van adott élhosszúsággal?

A legtöbb kérdésre 3-dimenzióban választ ad a [3] cikk. Az eredményeket röviden ismertetjük majd az első fejezetben, de nem ez lesz a centrális része a szakdolgozatnak. A második fejezetben összefoglalunk ismert eredményeket, amiket használunk majd.

A harmadik fejezetben megvizsgáljuk az $n = 4$ esetet a (4) és (5) kérdések szempontjából. Ezek nagy része új eredmény, amelyeket közösen csináltunk Kiss Emillel.

A negyedik fejezetben (2)-re megadjuk a pontos választ, (3)-ra pedig egy speciális permutációs kiterjesztést adunk 1, 2, 4 és 8-dimenzióban, majd belátjuk, hogy más dimenzióban ilyen speciális kiterjesztés nem lehetséges. Megismerkedünk a Cayley-számokkal, amelyek szorzótáblája adja a megfelelő kiterjesztést.

Külön köszönettel tartozom témavezetőmnek, Kiss Emilnek, aki rengeteget segített a dolgozat elkészítésében, nemcsak tanácsokkal és útmutatásokkal, hanem a közös gondolkodásokkal is. Köszönettel tartozom továbbá John W. Balesnek, aki ismeretlenként is segítőkészen válaszolt a kérdéseimre. Mindemellett köszönöm családomnak és barátaimnak is a támogatásukat.

## 1. Rácskockák 3 dimezióban

**1.1. Definíció.** Ha $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^n$ vektorok ortogonálisak és ugyanolyan hosszúak akkor ikervektoroknak nevezzük őket. Ha ez $k$ darab vektorra teljesül (hogy páronként ortogonálisak és ugyanolyan hosszúak), akkor őket $k$-as ikreknek, $k = n$ esetén pedig rácskockának nevezzük.

Elsőként az $n = 3$ esetet fogjuk vizsgálni, ez lesz az első fejezet témája. Az $n = 2$ dimenzió ugyanis nem túl érdekes a bevezetőben tárgyalt kérdések szempontjából.

**1.2. Tétel.** *Egy $\mathbb{Z}^3$-beli rácskockának az élhossza egész szám.*

*Bizonyítás.* Legyen a rácskockát kifeszítő három vektor $\mathbf{a}(a_1, a_2, a_3)$, $\mathbf{b}(b_1, b_2, b_3)$ és $\mathbf{c}(c_1, c_2, c_3)$. Az ezek által kifeszített paralellepipedon (jelen esetben kocka) térfogata az alábbi determináns:

$$\det \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}.$$

Mivel a koordináták egészek, ezért ez is egész lesz, tehát a kocka térfogata egész. Legyen a kocka élhossza $d$. Ekkor a kocka térfogata $d^3$, ami egész az előbbiek szerint. De $d^2$-ről tudjuk, hogy egész, hiszen a koordináták egészek, tehát $d^3/d^2 = d$ racionális. Mivel ez egy egész szám négyzetgyöke, ezért egész is, és ezt akartuk bizonyítani. □

Ebből a tételből rögtön következik, hogy nem minden egész vektor terjeszthető ki rácskockává, hiszen szükséges feltétel, hogy egész normájú legyen. Természetesen felmerül a kérdés, hogy ez elégséges-e? A válasz igenlő, ezt mondja ki a következő tétel.

**1.3. Tétel.** *Legyenek $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^3$ ikervektorok, melyeknek hossza $d \in \mathbb{Z}$. Ekkor $d$ osztója $\mathbf{a}$ és $\mathbf{b}$ vektoriális szorzatának (pontosabban annak minden koordinátájának).*

Mielőtt rátérnénk a bizonyításra vegyük észre, hogy ebből következik, hogy kiegészülnek rácskockává, hiszen fogjuk a vektoriális szorzatukat és leosztjuk egy egész számmal, hogy $d$ legyen a normája, és az a vektor nyilván megfelelő. A kiterjesztés persze egyértelmű is, hiszen a két vektor által kifeszített altérre merőleges altér egydimenziós.

*Bizonyítás.* Belátjuk egy koordinátára, a többire hasonlóan megy a bizonyítás. Tehát az alábbit kell belátnunk: $d \mid a_2b_3 - a_3b_2$. Ehhez azt látjuk be, hogy $d^2 \mid (a_2b_3 - a_3b_2)^2$.

$$(a_2b_3 - a_3b_2)^2 = (a_2^2 + a_3^2)(b_2^2 + b_3^2) - (a_2b_2 + a_3b_3)^2 = (d^2 - a_1^2)(d^2 - b_1^2) - a_1^2b_1^2\,.$$

Ez pedig nyilván osztható $d^2$-el. Közben kihasználtuk, hogy $a_1b_1 + a_2b_2 + a_3b_3 = 0$, illetve azt is, hogy $a_1^2 + a_2^2 + a_3^2 = b_1^2 + b_2^2 + b_3^2 = d^2$. □

Ezt az eredményt általánosítjuk majd a 4.1. Tételben tetszőleges dimenzióra. Egy másik bizonyítás olvasható Horváth Márton szakdolgozatában [4], ami a háromdimenziós rácsgeometriát használja.

Felmerül a kérdés, hogy ha egy darab olyan egész vektort veszünk, aminek a normája egész, akkor az kiegészül-e rácskockává. Ehhez az alábbi segédtételt fogjuk használni:

**1.4. Tétel** [A pitagoraszi-számnégyesek Euler-féle paraméterezése]. *Tegyük fel, hogy* $a, b, c, d \in \mathbb{Z}$, *amikre* $(a, b, c) = 1$ *és* $a^2 + b^2 + c^2 = d^2$, *továbbá* $a$ *páratlan és* $d > 0$. *Ekkor léteznek* $m, n, p, q$ *egész számok, hogy*

$$a = m^2 + n^2 - p^2 - q^2$$
$$b = 2(mq + np)$$
$$c = 2(-mp + nq)$$
$$d = m^2 + n^2 + p^2 + q^2$$

A tétel bizonyítása elolvasható Erdős Pál és Surányi János számelmélet könyvében ([2], 7. fejezet), továbbá az [3] cikkben is, mi ezt most nem bizonyítjuk. Azonban ennek segítségével belátjuk, hogy minden egész normájú egész vektornak van ikre, és ebből az 1.3. Tétel segítségével következik, hogy minden ilyen vektor kiegészül rácskockává (ez Sárközy András eredménye).

**1.5. Tétel.** *Minden egész normájú egész vektornak van ikre.*

*Bizonyítás.* Legyen a kiegészítendő vektorunk $(a, b, c)$. Föltehető, hogy a koordináták legnagyobb közös osztója 1. Ekkor van köztük egy páratlan legyen ez $a$. Ekkor az 1.4. Tételt alkalmazva

$$a = m^2 + n^2 - p^2 - q^2$$
$$b = 2(mq + np)$$
$$c = 2(-mp + nq)$$

teljesül valamilyen $m, n, p, q \in \mathbb{Z}$-re. Ekkor az alábbi vektor ikre lesz $(a, b, c)$ -nek:

$$(-2mq + 2np, m^2 - n^2 + p^2 - q^2, 2mn + 2pq)\,.$$

Ez nagyon könnyen ellenőrizhető és ezzel az állítást igazoltuk. □

Számos egyéb kérdés merül fel viszonylag természetesen. Tudjuk-e valamilyen módon paraméterezni az ikervektorokat? Egy vektornak hány ikre lehet? Meg lehet-e valahogy ránézésre állapítani egy vektorról, hogy van-e ikre? Ezekre az utolsó kivételével (részben) ismert a válasz. Ezek az [3] cikk szerzőinek eredményei. Ezekről próbálunk most némi képet adni bizonyítások nélkül.

**1.6. Definíció.** Egy $a\sigma + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ alakú kvaterniót Hurwitz-kvaterniónak nevezünk ha $a, b, c, d \in \mathbb{Z}$ és $\sigma = (1 + i + j + k)/2$. Jelölésük $\mathbb{E}$. Az $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ alakú kvaterniók az egész együtthatós, vagy Lipschitz-kvaterniók, ezek halmaza $\mathbb{L}$.

Ezek az alapobjektumai az [3] cikknek. Ezek segítségével lehet paraméterezni a háromdimenziós ikervektorokat. Először is rendeljünk hozzá minden térbeli vektorhoz egy tiszta kvaterniót a következő módon: $(a, b, c) \mapsto a\mathbf{i} + b\mathbf{j} + c\mathbf{k}$. Most már kimondhatjuk a tételt.

**1.7. Tétel.** *Minden* $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^3$ *ikerpár előáll* $(\alpha z k \overline{\alpha}, \alpha z j \overline{\alpha})$ *alakban ahol* $\alpha$ *Hurwitz-kvaternió,* $z$ *pedig Gauss-egész.*

Ezt persze úgy kell érteni, hogy a tiszta kvaterniónak megfelelő háromdimenziós vektorok lesznek ikrek és minden ilyen iker előáll ilyen módon.

Egy másik fontos tétel ebben a témakörben az alábbi:

**1.8. Tétel.** *Ha egy vektornak van ikre, akkor a normájának a négyzete előáll, mint két négyzetszám összege.*

**1.9. Definíció.** Egy $M$ szám iker-teljes ha minden $M$ hossznégyzetű vektornak van ikre.

**1.10. Tétel.** *Egy négyzetmentes szám akkor és csak akkor iker-teljes ha a hossznégyzete felírható két négyzetszám összegeként, de három pozitív négyzetszám összegeként nem. Továbbá ha egy a szám iker-teljes akkor* $an^2$ *is az minden* $n \in \mathbb{Z}$*-re.*

Egy híres számelméleti sejtésből következne, hogy az iker-teljes számok az alábbiak:

$$n^2, 2n^2, 5n^2, 10n^2, 13n^2, 37n^2, 58n^2, 85n^2, 130n^2\,.$$

Zárásképpen megemlítjük Sárközy András 1961-es eredményét, amelyre fent hivatkoztunk, és amely leírja a háromdimenziós rácskockákat. Egy rácskockát primitívnek nevezünk, ha az őt alkotó vektorok koordinátáinak legnagyobb közös osztója 1.

**1.11. Tétel.** *Minden primitív rácskockához léteznek* $m, n, p, q \in \mathbb{Z}$ *számok, hogy a rácskocka vektorai az alábbi mátrix oszlopaiból megkaphatók oszlopcserékkel és előjelváltoztatásokkal:*

$$\begin{pmatrix} m^2+n^2-p^2-q^2 & -2mq+2np & 2mp+2nq \\ 2mq+2np & m^2-n^2+p^2-q^2 & -2mn+2pq \\ -2mp+2nq & 2mn+2pq & m^2-n^2-p^2+q^2 \end{pmatrix}$$

Még számos eredményről beszámolhattunk volna (például az ikrek számáról), ezekről az olvasó tájékozódhat az [3] és [4] cikkekből.

## 2. Kvaterniók és a Cayley–Dickson-konstrukció

Ebben a fejezetben megismerkedünk azokkal a segédobjektumokkal, amiket később használni fogunk. Néhány fontos segédtételt is bizonyítunk.

A kvaterniók elég gyakran előfordulnak a matematika különböző területein, ők a legismertebb ferdetest. Emiatt számos állítást ismertnek fogunk feltételezni (például a norma multiplikativitását). Miután a szorzás nem kommutatív, már nem annyira alapvető számelméletet nézni a kvaterniók körében. A kvaterniók számelméletének alapvető objektumai a Hurwitz-kvaterniók, amiket az első fejezetben már definiáltunk. Az [3] cikkben számos állítás vonatkozik rájuk, ezek közül néhányat bizonyítunk most.

**2.1. Állítás.** *Legyen $\alpha \in \mathbb{E}$ és $p \in \mathbb{Z}$ prím, amely nem osztója $\alpha$-nak. Ekkor $\alpha$ felírható $\pi\alpha'$ alakban, ahol $N(\pi) = p$, és ez a $\pi$ jobb-asszociáltságtól eltekintve egyértelmű.*

*A $\pi$ akkor és csak akkor $p$ normájú balosztója $\alpha$-nak, ha $\pi$ generátoreleme az $(\alpha, p)_r$ jobbideálnak.*

*Bizonyítás.* Az $\mathbb{E}$ gyűrű jobb-euklideszi, ezért az $R = (\alpha, p)_r$ jobbideál főideál. Generátoreleme legyen $\pi$. Mivel $\alpha, p \in R$, ezért $\pi$ balosztója $\alpha$-nak és $p$-nek is. Legyen $p = \pi\tau$. Ekkor $N(\pi)N(\tau) = p^2$. Ha $N(\pi) = p^2$, akkor $\tau$ egység, így $p$ asszociáltja $\pi$-nek, ezért $p$ osztója $\alpha$-nak, ez pedig ellentmond a feltételünknek.Ha $N(\pi) = 1$, akkor $\pi$ egység. Ekkor létezik $\tau_1, \tau_2 \in \mathbb{E}$, hogy $\alpha\tau_1 + p\tau_2 = 1$. Ha ezt az egyenlőséget balról beszorozzuk $\overline{\alpha}$-val, akkor azt kapjuk, hogy $p \mid \overline{\alpha}$ és ebből következik, hogy $p \mid \alpha$, ami ellentmondás. A norma multiplikativitása miatt csak az lehet, hogy $N(\pi) = p$ és ezt akartuk igazolni. Az állítás megfordítása könnyen meggondolható. □

**2.2. Állítás.** *Legyen $\theta, \eta, \pi \in \mathbb{E}$ és $N(\pi) = p$, ahol $p$ egész prím. Ha $\pi \mid \tau$ és $p \mid \overline{\theta}\eta$, de $p$ nem osztója $\theta$-nak, akkor $\pi \mid \eta$.*

*Bizonyítás.* Az előző állítás miatt $(p, \theta)_r = (\pi)_r$, ezért $\pi = \theta\tau_1 + p\tau_2$ valamilyen $\tau_1, \tau_2 \in \mathbb{E}$-re. Ebből kifolyólag $\overline{\pi}\eta = \overline{\tau_1}\overline{\theta}\eta + \overline{\tau_2}p\eta$, tehát a feltétel miatt $p \mid \overline{\pi}\eta$. Mivel $p = \overline{\pi}\pi$, ezért $\pi \mid \eta$ és ezt akartuk igazolni. □

**2.3. Definíció.** Egy egész együtthatós $\alpha = a + bi + cj + dk$ kvaterniót *primérnek* nevezünk, ha

$$a - 1 \equiv b \equiv c \equiv d \ (2) \quad \text{és} \quad a + b + c + d \equiv 1 \ (4) \, .$$

**2.4. Állítás.** *Minden $\alpha \in \mathbb{E}$-nek van egész együtthatós bal-, illetve jobbasszociáltja. Ha $N(\alpha)$ páratlan, akkor pontosan egy primér bal-, illetve jobbasszociáltja van. A primér kvaterniók félcsoportot alkotnak a szorzásra. Ráadásul, ha két primér kvaternió hányadosa $\mathbb{E}$-ben van, akkor a hányados is primér.*

**2.5. Állítás.** *Legyen $\alpha = a + bi + cj + dk$ egész együtthatós kvaternió.*

1. *Létezik $\beta \in \mathbb{L}$, hogy $\alpha = (1 + i)\beta \Leftrightarrow a \equiv b \ (2)$ és $c \equiv d \ (2)$. Hasonló teljesül $1 + j$-re és $1 + k$-ra.*
2. *Ha $8 \mid N(\alpha)$, akkor $\alpha$ minden együtthatója páros.*
3. *Ha $N(\alpha) \equiv 4 \ (8)$, akkor $\alpha = (1 + i)\beta$, ahol $\beta \in \mathbb{L}$.*
4. *Ha $N(\alpha) \equiv 2 \ (4)$, akkor létezik pontosan egy $\eta \in \{1 + i, 1 + j, 1 + k\}$, amire $\alpha = \eta\beta$ valamilyen $\beta \in \mathbb{L}$-re.*

Ez a négy állítás nagyon fontos lesz a későbbiekben, amikor a ortogonális vektorpárokat szeretnénk kiterjeszteni és megszámolni 4-dimenzióban. Számos egyéb fontos állítás mondható el a Hurwitz-kvaterniókról, ezekre majd csak hivatkozni fogunk. Bizonyításuk megtalálható [3]-ban és [5]-ben.

**A Cayley–Dickson konstukció.** Az algebra egyik alapvető tétele a Frobenius-tétel, ami azt mondja ki, hogy egy valósak feletti nullosztómentes, véges dimenziós algebra izomorf a valós számok, a komplex számok vagy a kvaterniók algebrájával. Itt mindhárom feltétel nagyon szükséges, azaz valamelyiket elhagyva már nem igaz az állítás. Például ha a nullosztómentességet elhagyjuk, akkor egy jó példa az $n \times n$-es mátrixok algebrája. Egy burkolt negyedik feltételt is tartalmaz a tétel: a szorzás asszociativitását. Most egy olyan algebrát mutatunk először be, amire ez mind teljesül, kivéve a szorzás asszociativitása.

**2.6. Definíció.** Vegyünk egy $A$ algebrát. Az $A \times A$-n definiálunk szorzást az alábbi módon: $(a,b)(c,d) = (ac - d^*b, da + bc^*)$ és $(a,b)^* = (a^*, -b)$ ahol a $^*$ egy involúció az eredeti algebrán. A kapott algebrát az A algebra megkettőzésének nevezzük.

Általában a $^*$ a konjugálást jelenti az $A$ algebrán. Nézzünk példákat! Ha $A = \mathbb{R}$, akkor a megkettőzése $\mathbb{C}$ lesz. Ha $A = \mathbb{C}$, akkor megkettőzésével megkapjuk a kvaterniókat. Egy ilyen megkettőzés során az algebra dimenziója is megkettőződik. Ha az $A$ nem kommutatív , akkor a megkettőzése nem lesz asszociatív! Ha kvaterniók algebráját megkettőzzük, akkor kapjuk az úgynevezett Cayley-számokat (másnéven októniókat). A Cayley-számok szorzástábláját a negyedik fejezetben használjuk majd egy tetszőleges nyolcdimenziós vektor rácskockává való kiterjesztéséhez.

A Cayley-számok algebrája nem asszociatív, de teljesülnek az alábbi gyengébb azonosságok: $x(yy) = (xy)y$, $x(xy) = (xx)y$ és $(yx)y = y(xy)$. Belátható, hogy a Cayley-számok minden olyan részalgebrája asszociatív, amit két elem generál.

Egy Cayley-szám normáját hasonlóan definiálhatjuk, mint a kvaterniónál, és a norma itt is multiplikatív lesz. Sőt ennél sokkal több is igaz:

**2.7. Tétel.** *Legyen az $A$ algebrán adott egy euklideszi vektortérstruktúra úgy, hogy tetszőleges $x, y \in A$ esetén $N(xy) = N(x)N(y)$. Akkor $A$ dimenziószáma* 1, 2, 4 *vagy* 8 *lehet.*

Tehát lényegében meg is adtuk a valósak fölötti normált algebrákat. Ez az alábbi tételen múlik (lásd [6], 41.7. szakasz).

**2.8. Tétel** [Hurwitz-Radon]. *Írjuk fel az $n$ egész számot $n = (2a+1)2^b$ alakban, ahol $b = c+4d$ és $0 \leq c \leq 3$. Legyen $\rho(n) = 2^c + 8d$. Ekkor azon $A_i : \mathbb{R}^n \to \mathbb{R}^n$ ortogonális leképezések maximális száma, amikre $A_i^2 = -I$ és $A_iA_j + A_jA_i = 0$ pontosan $\rho(n) - 1$.*

Az ilyen leképezések számának vizsgálata nem természetellenes, ilyen leképezés például 8-dimenzióban az $i, j, ..., h$ elemekkel való szorzás. Ennek tételnek amúgy számos alkalmazása van, mi is használni fogjuk a negyedik fejezetben. Talán az egyik legérdekesebb egy differenciáltopológiai alkalmazás:

**2.9. Tétel.** *Az $S^{n-1}$ felületen $\rho(n) - 1$ lineárisan független vektormező létezik.*

A Cayley–Dickson-konstrukció folytatható tovább is, tetszőleges 2-hatvány dimenzióig eljuthatunk, azonban ekkor már elvész a szorzás nullosztómentessége is. A báziselemek szorzástáblája megtalálható például John W. Bales 2003-as cikkében, lásd [1].

## 3. A 4 dimenziós eset

Ebben a fejezetben megvizsgáljuk a 4-dimenziós esetet több szempontból. Először megnézzük, hogy milyen vektorok egészülnek ki rácskockává, majd ugyanezt megnézzük a kettes és harmasikrekre. Végül megszámoljuk az adott normájú hármasikreket és rácskockákat. Ezen fejezet legfontosabb eszközei a Hurwitz-kvaterniók lesznek, amiket már korábban bevezettünk.

**3.1. Tétel.** *Legyen* $\mathbf{u} \in \mathbb{Z}^4$. *Ekkor* $\mathbf{u}$ *kiterjed rácskockává.*

*Bizonyítás.* Legyen $\mathbf{u} = (a, b, c, d)$. Ekkor az alábbi 4 vektor egy rácskockát határoz meg:

$$(a, b, c, d)$$
$$(b, -a, -d, c)$$
$$(c, d, -a, -b)$$
$$(d, -c, b, -a)$$

Könnyen ellenőrizhetjük, hogy ez valóban rácskocka. □

Azonban érdemes ezt egy mátrix alakban fölírni, ahol ezek a vektorok az oszlopok.

$$\begin{pmatrix} a & b & c & d \\ b & -a & d & -c \\ c & -d & -a & b \\ d & c & -b & -a \end{pmatrix}.$$

Ha itt az $a$-nak megfeleltetjük az 1-et, a $b$-nek az **i**-t, a $c$-nek a **j**-t és a $d$-nek a **k**-t, akkor éppen a kvaterniók báziselemeinek a szorzástábláját kapjuk.

**3.2. Definíció.** Két kvaterniót ikernek nevezünk, ha mint négydimenziós vektorok ikrek.

Innentől kezdve az összes kérdést lefordítjuk a Hurwitz-kvaterniók nyelvére és ezek segítségével válaszoljuk meg őket. Mostantól ebben a fejezetben az $i$, $j$, $k$ kvaterniókat nem írjuk vastag betűvel. Az első lépés az alábbi lemma.

**3.3. Állítás.** *Az* $\alpha$ *és* $\beta$ *kvaterniók akkor és csak akkor ikrek, ha egyenlő a normájuk és* $\overline{\alpha}\beta = -\overline{\beta}\alpha$ *(vagy ami ezzel ekvivalens,* $\alpha\overline{\beta} = -\beta\overline{\alpha}$*).*

*Bizonyítás.* Legyen $\alpha = a_1 + a_2 i + a_3 j + a_4 k$ és $\beta = b_1 + b_2 i + b_3 j + b_4 k$. Ekkor $\alpha\beta$ valós része $a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4$, azaz az $\alpha$-hoz és $\beta$-hoz tartozó vektorok akkor és csak akkor ortogonálisak, ha $\alpha\overline{\beta}$ valós része 0 (vagy hasonlóan $\overline{\alpha}\beta$ valós része 0). Viszont egy kvaternió valós része akkor és csak akkor 0, ha a konjugáltja az ellentettje. □

**3.4. Következmény.** *Ha* $\gamma \neq 0$*, akkor* $\alpha$ *és* $\beta$ *akkor és csak akkor ikrek, ha* $\alpha\gamma$ *és* $\beta\gamma$ *azok (illetve akkor és csak akkor ha* $\gamma\alpha$ *és* $\gamma\beta$ *azok).*

**3.5. Állítás.** *Legyenek* $\alpha, \beta \in \mathbb{L}$ *ikrek és* $p \in \mathbb{Z}$ *prím, ami osztja a közös normát. Ekkor létezik* $\pi \in \mathbb{E}$*, aminek a normája* $p$ *és vagy közös balosztója, vagy közös jobbosztója* $\alpha$*-nak és* $\beta$*-nak.*

Ez a lemma teszi lehetővé az ikrek „lebontását”. Mivel egy egész vektort egy Lipschitz-kveternió reprezentál, figyelnünk kell majd arra, hogy a $\pi$ alkalmas asszociáltját használjuk.

*Bizonyítás.* Először belátjuk, hogy $\alpha$-nak van egy $p$ normájú $\pi_1$ balosztója. Ha $p \mid \alpha$, akkor ez világos, hiszen $p = \pi_1\overline{\pi_1}$ minden $p$ normájú $\pi_1 \in \mathbb{E}$ -re. Ilyen elem pedig a Lagrange-féle négy négyzetszám tétel miatt létezik. Ha $\alpha$ nem osztható $p$-vel, akkor a 2.1. Lemma biztosít ilyen $\pi_1$-et. Hasonlóan $\beta$-nak is van egy $p$ normájú $\pi_2$ balosztója. Ugyanígy látható, hogy $\alpha$-nak és $\beta$-nak is van egy-egy $p$ normájú $\pi_3$ és $\pi_4$ jobbosztója. Azt kell belátnunk, hogy vagy $\pi_1$ és $\pi_2$ jobbasszociáltak, vagy $\pi_3$ és $\pi_4$ balasszociáltak. A 3.3. Állítás miatt $\alpha\overline{\beta} = -\beta\overline{\alpha}$. Tegyük fel először, hogy $p$ nem osztója ennek a kvaterniónak. A 2.1. Állítás egyértelműségi részét használjuk $\alpha\overline{\beta} = -\beta\overline{\alpha}$-ra, ekkor $\pi_1$ és $\pi_2$ jobbasszociáltak és készen vagyunk.

Most tegyük fel, hogy $p \mid \alpha\overline{\beta} = -\beta\overline{\alpha}$. Alkalmazzuk a 2.2 Állítást a $\pi = \overline{\pi_3}$, $\theta = \overline{\alpha}$ és $\eta = \overline{\beta}$ szereposztásban. Ekkor $\overline{\pi_3} \mid \overline{\beta}$, tehát $\pi_3$ jobbosztója $\beta$-nak és így ismét készen vagyunk. □

**3.6. Állítás.** *Legyen $(\alpha_1, ..., \alpha_m)$ egy $m$-es iker és $p \in \mathbb{Z}$ prím, ami osztja $N(\alpha_1)$-et. Ekkor létezik egy olyan $p$ normájú $\pi \in \mathbb{E}$, hogy $\pi$ bal- vagy jobbosztója minden $\alpha_\ell$-nek.*

*Bizonyítás.* A 2.1. Állítás miatt van $\alpha_\ell$-nek $p$ normájú $\rho_\ell$ jobbosztója és $\pi_\ell$ balosztója is. Ha $p$ nem osztója $\alpha_\ell$-nek akkor ezek lényegében egyértelműek, egyébként tetszőlegesen választhatók. Emiatt feltehető, hogy semelyik $\alpha_\ell$ sem osztható $p$-vel.

Tekintsük a teljes gráfot az $\{1, 2, ...m\}$ halmazon. Egy $(u, v)$ élt színezzünk Lila színnel, ha $\pi_u$ és $\pi_v$ jobbasszociáltak, és Rózsaszínnel, ha $\rho_u$ és $\rho_v$ balasszociáltak. Az előző állítás miatt minden élnek van színe. Könnyen látható, hogy mindkét színosztály egy tranzitív relációt indukál és emiatt a gráf minden éle ugyanolyan színű, és ezt akartuk igazolni. □

**3.7. Tétel.** *Legyen $(\varepsilon_1, \ldots, \varepsilon_m)$ egy $m$-es iker, ahol mindegyik $\varepsilon_\ell$ a kvaterniócsoport egy eleme és $\varepsilon_1 = 1$. Ekkor minden $\gamma, \delta \in \mathbb{E}$-re*

$$C = (\gamma\varepsilon_1\delta, \ldots, \gamma\varepsilon_m\delta)$$

*egy $m$-es iker. Ráadásul minden $m$-es iker megkapható ilyen alakban.*

*Bizonyítás.* A tétel első fele következik a 3.4. Következményből. A megfordításhoz tegyük fel, hogy $C = (\alpha_1, \ldots, \alpha_m)$ egy $m$-es iker. Ha a 3.6-ot és a 3.4-et alkalmazzuk sokszor, akkor azt kapjuk, hogy $C = (\gamma\varepsilon_1\delta, \ldots, \gamma\varepsilon_m\delta)$, valamilyen $\gamma, \delta \in \mathbb{E}$ és $\varepsilon \in \mathbb{E}$ egységre. Föltehető, hogy $\varepsilon_1 = 1$ ($\gamma$ helyébe $\gamma\varepsilon_1$-t rakunk). A 3.4. Következmény következmény miatt ez egy $m$-es iker és az $\varepsilon_1 = 1$ feltétel miatt $\varepsilon_\ell$ koordinátái egészek, azaz a kvaterniócsoport elemei. □

Az előző állításban nem láttuk be, hogy ha az eredeti $m$-es iker egész együtthatós kvaterniókból áll, akkor $\gamma$ és $\delta$ is választható egész együtthatósnak. Ezért a fenti felbontáson finomítanunk kell, amivel nemcsak azt tudjuk majd belátni, hogy 4-dimenzióban minden $m$-es iker kiterjed rácskockává, hanem meg is tudjuk majd

számolni a rácskockákat. Ehhez visszavezetjük a problémát arra az esetre, amikor a közös norma páratlan.

**3.8. Állítás.** *Legyen $N = 2^n D$, ahol $n \geq 2$ és $D$ páratlan. Ekkor minden $N$ normájú $m$-es iker egyértelműen írható $((1+i)^{n-1}\beta_1, \ldots, (1+i)^{n-1}\beta_m)$ alakba, ahol $(\beta_1, \ldots, \beta_m)$ egy $m$-es iker.*

*Bizonyítás.* Triviálisan következik a 2.5. Állításból. □

**3.9. Állítás.** *Legyen $N = 2D$, ahol $D$ páratlan. Ekkor minden $N$ normájú $m$-es iker egyértelműen írható $(\eta\beta_1, \ldots, \eta\beta_m)$ alakban, ahol $(\beta_1, \ldots, \beta_m)$ egy $m$-es iker és $\eta \in \{1+i, 1+j, 1+k\}$.*

*Bizonyítás.* Ismét könnyen következik a 2.5. Állításból. □

**3.10. Definíció.** Jelölje $f_m(N)$ az $N$ normájú $m$-es ikrek számát.

Ekkor az előbbi két állítás alapján mondhatunk valamit erről az $f_m$ függvényről.

**3.11. Következmény.** *Legyen $N = 2^n D$, ahol $D$ páratlan.*

(1) *Ha $n \geq 2$, akkor $f_m(N) = f_m(2D)$.*
(2) *Ha $n = 1$, akkor $f_m(N) = 3f_m(D)$.*

Tehát most már elég a páratlan normájú ikreket vizsgálni. Legyen $K = \{1, i, j, k\}$. Minden $g \in K$-hoz definiálunk egy $S_g$ halmazt az alábbi módon:

$$S_g = \{a_1 + a_i i + a_j j + a_k k \in \mathbb{L} \mid a_g \not\equiv a_h \ (2) \text{ minden } h \neq g\text{-re (ahol } h \in K).\}$$

Vagyis például $S_i$ elemeinél $i$ együtthatója páros és a többi együttható páratlan, vagy pont fordítva. A furcsa jelölést az alábbi állítás indokolja.

**3.12. Állítás.** *Legyenek $\alpha, \beta \in \mathbb{L}$ páratlan normájúak és $2\sigma = 1 + i + j + k$.*

(1) *$\alpha$ és $\beta$ is benne van valamelyik $S_g$-ben. Ha ikrek, akkor nem lehetnek ugyanabban az $S_g$-ben.*
(2) *Ha $N(\alpha) \equiv 1$ (4), akkor $\alpha \in S_g$ akkor és csak akkor, ha $\alpha \equiv g$ (2) az $\mathbb{L}$-ben, akkor és csak akkor ha $\alpha \equiv g$ (2) az $\mathbb{E}$-ben.*
(3) *Ha $N(\alpha) \equiv 3$ (4), akkor $\alpha \in S_g$ akkor és csak akkor, ha $\alpha \equiv 2\sigma - g$ (2) az $\mathbb{L}$-ben, akkor és csak akkor ha $\alpha \equiv 2\sigma - g$ (2) az $\mathbb{E}$-ben.*
(4) *Legyen $\alpha \in S_g$ és $\beta \in S_h$, ekkor $\alpha\beta \in S_{g*h}$, ahol a $*$ a $K$-n definiált szorzás ami nem veszi figyelembe az előjelet (azaz tulajdonképpen a kvaterniócsoport azon faktorcsoportját nézzük, ami izomorf a Klein-csoporttal).*
(5) *A primér kvaterniók $S_1$-ben vannak. Ha $\alpha$ primér, akkor $\alpha\beta$ és $\beta$ ugyanabba az $S_g$-be tartoznak.*

*Bizonyítás.* Ha $N(\alpha) \equiv 1$ (4), akkor $\alpha$-nak pontosan egy páratlan komponense van. Ha $N(\alpha) \equiv 3$ (4), akkor $\alpha$-nak pontosan egy páros komponense van. Tegyük fel, hogy $\alpha$ és $\beta$ ikrek, és ugyanabban az $S_g$-ben vannak. Ha $N(\alpha) = N(\beta) \equiv 1$ (4), akkor a megfelelő vektorok skaláris szorzata páratlan, ami nem lehet, mert ortogonálisak. Ha viszont $N(\alpha) = N(\beta) \equiv 3$ (4), akkor a megfelelő vektorok skaláris szorzata szintén páratlan, ami lehetetlen. Ezzel beláttuk (1)-et. A többi állítás ellenőrzését az olvasóra bízzuk. □

Most megpróbálunk kapcsolatot teremteni az $m$-es ikrek száma és a rendezett $m$-es ikrek száma között. Ha $(\alpha_1, \dots, \alpha_m)$ egy páratlan normájú $m$-es iker, akkor rendeljük hozzá azt az egyértelmű $(g_1, \dots, g_m)$ sorozatot, melyre $\alpha_\ell \in S_{g_\ell}$ minden $1 \le \ell \le m$-re. Ezt nevezzük az $m$-es iker *típusának*. Egy $m$-es ikert *rendezettnek* nevezünk, ha a típusa $(1)$, $(1, i)$, $(1, i, j)$ vagy $(1, i, j, k)$ (az $m$-től függően). A komponensek permutációja megőrzi az ortogonalitást és a normát is. Ha $(g_1, \dots, g_m)$ és $(h_1, \dots, h_m)$ típusok, akkor rögzíthetjük $K$-nak egy permutációját, ami $g_\ell$-hez a $h_\ell$-et rendeli. Ez a fix permutáció egy bijekciót indukál az összes vektoron, ami miatt egy adott $(g_1, \dots, g_m)$ típusú $m$-es ikrek száma nem függ $(g_1, \dots, g_m)$-től. A lehetséges típusok száma $m!\binom{4}{m}$. Ebből adódik a következő állítás.

**3.13. Állítás.** *Legyen $N$ páratlan. Ekkor $f_m(N) = m!\binom{4}{m}M$, ahol $M$ a rendezett $N$-normájú $m$-es ikrek száma.*

**3.14. Állítás.** *Legyenek $\gamma, \delta \in \mathbb{E}$ primér kvaterniók, és $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm i$, $\varepsilon_3 = \pm j$, $\varepsilon_4 = \pm k$. Ekkor*

$$C = (\gamma\varepsilon_1\delta, \dots, \gamma\varepsilon_m\delta)$$

*egy $m$-es iker. Megfordítva, minden páratlan normájú rendezett $m$-es iker megkapható ilyen módon.*

*Bizonyítás.* Mivel $\gamma$ és $\delta$ primérek, ezért $C = (\gamma\varepsilon_1\delta, \dots, \gamma\varepsilon_m\delta)$ rendezett a 3.12. Állítás miatt. A megfordításhoz tegyük fel, hogy $C$ rendezett. Alkalmazzuk sokszor a 3.6. Állítást, csak arra figyeljünk, hogy minden lépésben $\pi$ primér kvaternió legyen. A 3.12. Állítás garantálja, hogy egy rendezett rácskockát kapunk a $\pi$ kihúzása után is. A végén egy olyan $C = (\gamma\varepsilon_1\delta, \dots, \gamma\varepsilon_m\delta)$ reprezentációt kapunk, ahol $\gamma$ és $\delta$ primér. Mivel $(\varepsilon_1, \dots, \varepsilon_m)$ rendezett, ezért azt kapjuk, hogy $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm i$, $\varepsilon_3 = \pm j$, $\varepsilon_4 = \pm k$. □

Az alábbi következmény a 3.7. Tétel keresett finomítása, ami nyilvánvaló a 3.8., 3.9. és a 3.14. Állítások miatt.

**3.15. Tétel.** *Minden egész együtthatós kvaterniókból álló $m$-es iker megkapható*

$$C = (\gamma\varepsilon_1\delta, \dots, \gamma\varepsilon_m\delta)$$

*alakban, ahol mindegyik $\varepsilon_\ell$ a kvaterniócsoport egy eleme, és $\gamma$ valamint $\delta$ is egész együtthatós.*

**3.16. Következmény.** *Minden $m$-es iker kiterjed rácskockává 4-dimenzióban.*

*Bizonyítás.* Legyen $C = (\gamma\varepsilon_1\delta, \dots, \gamma\varepsilon_m\delta)$, mint fönt (ahol $m < 4$). Ekkor $(\varepsilon_1, \dots, \varepsilon_m)$ kiterjed egy $(\varepsilon_1, \dots, \varepsilon_{m+1})$ $m+1$-es ikerré (a megfelelő egységkvaterniót vagy annak az ellentettjét veszem). Így $C = (\gamma\varepsilon_1\delta, \dots, \gamma\varepsilon_{m+1}\delta)$ egy $m+1$-es iker. Ezzel az állítást igazoltuk. □

Itt érdemes egy pillanatra megállni. Beláttuk, hogy akárhogyan veszünk egy egész vektorhoz mohón egy ikret (illetve vektorpárhoz egy 3-adikat) mindig ki tudjuk őket egészíteni rácskockává. Véleményem szerint ez egy igencsak meglepő állítás, érdekes kérdés, hogy rendelkezik-e más dimenzió még hasonló tulajdonsággal?

Most rátérünk a leszámlálási tétel bizonyítására. Ehhez a 3.14. Állításban adott felbontás egyértelműségét kell megvizsgálnunk.

**3.17. Lemma.** *Tegyük fel, hogy $\gamma_1\varepsilon_\ell\delta_1 = \gamma_2\varepsilon_\ell\delta_2$ teljesül $\ell = 1, 2$-re, ahol $\varepsilon_\ell$ egység, továbbá $N(\gamma_1\delta_1) = N(\gamma_2\delta_2) \neq 0$. Ekkor $\overline{\gamma_1}\gamma_2$ felcserélhető $\varepsilon_1\overline{\varepsilon_2}$-vel.*

A lemma bizonyítását az olvasóra bízzuk. Emlékeztetjük az olvasót, hogy egy $m$-es ikret primitívnek, nevezünk, ha a $4m$ komponensnek a legnagyobb közös osztója 1.

**3.18. Tétel.** *Tegyük fel, hogy $C = (\gamma_1\varepsilon_1\delta_1, \ldots, \gamma_1\varepsilon_m\delta_1) = (\gamma_2\varepsilon_1\delta_2, \ldots, \gamma_2\varepsilon_m\delta_2)$ egy $m$-es iker két reprezentációja a 3.14. Állítás szerint, és $m \geq 3$. Ha $\gamma_1$ és $\gamma_2$ primitívek, akkor $\gamma_1 = \gamma_2$ és $\delta_1 = \delta_2$. Sőt, $C$ akkor és csak akkor primitív, ha $\gamma_1$ és $\delta_1$ primitívek.*

*Bizonyítás.* A 3.17. lemma miatt $\overline{\gamma_1}\gamma_2$ felcserélhető $\varepsilon_1\overline{\varepsilon_2} = \pm i$-vel és $\varepsilon_1\overline{\varepsilon_3} = \pm j$-vel is, tehát $d = \overline{\gamma_1}\gamma_2$ valós. Mivel $\gamma_1$ és $\gamma_2$ primérek, ezért $d$ egész szám. Tudjuk, hogy $d\gamma_1 = N(\gamma_1)\gamma_2$. Ha $\gamma_1$ és $\gamma_2$ primitívek, akkor vegyük az az előző egyenletben a két oldal együtthatóinak a legnagyobb közös osztóját. Azt kapjuk, hogy $d = \pm N(\gamma_1)$ és emiatt $\gamma_1 = \pm\gamma_2$. De ez két primér kvaternió, ezért egyenlőek. Így $\gamma_1\varepsilon_1\delta_1 = \gamma_2\varepsilon_1\delta_2$, amiből $\delta_1 = \delta_2$.

Legyen $C = (\gamma_1\varepsilon_1\delta_1, \ldots, \gamma_1\varepsilon_m\delta_1)$, ahol $\gamma_1$ és $\delta_1$ primitívek. Indirekten tegyük fel, hogy $C$ nem primitív. Legyen $n > 1$ egész szám, ami minden $C$-beli vektort oszt és tekintsük $C/n = (\gamma_1\varepsilon_1\delta_1/n, \ldots, \gamma_1\varepsilon_m\delta_1/n)$-et. Ez nyilván egy $m$-es iker tehát van egy $C/n = (\gamma_3\varepsilon_1\delta_3, \ldots, \gamma_3\varepsilon_m\delta_3)$ alakú reprezentációja. Legyen $\gamma_3 = d\gamma_2$, ahol $\gamma_2$ primitív és primér (azaz $d$ pozitív egész). Ekkor C-nek van egy másik reprezentációja: $C = (\gamma_2\varepsilon_1(nd)\delta_3, \ldots, \gamma_2\varepsilon_m(nd)\delta_3)$. Itt $(nd)\delta_3$ is primér, hiszen $nd$ pozitív egész. Az előző bekezdésben belátott egyértelműség miatt $\delta_1 = (nd)\delta_3$, ami ellentmond $\delta_1$ primitívségének. □

**3.19. Következmény.** *Tegyük fel, hogy $n \geq 3$ és $N$ páratlan. Ekkor a rendezett $N$ normájú primitív $m$-es ikrek száma:*

$$k(N) = 2^m \sum_{d|N} h(d)h(N/d)\,,$$

*ahol $h(d) = d\prod_p(1 + 1/p)$, és $p$ a $d$ pozitív prímosztóin fut.*

*Bizonyítás.* Ismert, hogy $h(d)$ éppen a $d$ normájú primitív, primér kvaterniók száma. Alkalmazzuk az előző tételt és legyen $d = N(\gamma_1)$. Ekkor $N(\delta_1) = N/d$. Ezt a két kvaterniót $h(d)h(N/d)$-féleképpen választhatom és $d$ az $N$-nek tetszőleges osztója lehet. Végül pedig $2^m$ lehetőség van az $\varepsilon_1, \ldots, \varepsilon_m$ előjelének a megválasztására. □

**3.20. Tétel.** *Ha $g(n) = f_4(N)/384$, akkor $g$ multiplikatív számelméleti függvény, aminek a prímhatvány helyeken vett helyettesítési értéke a következő:*

(1) *$g(2^n) = 3$ minden $n \geq 1$-re.*
(2) *Ha $p$ páratlan prím és $n \geq 1$, akkor*

$$g(p^n) = \frac{(n+1)p^n(p^2-1) - 2(p^{n+1}-1)}{(p-1)^2}\,.$$

*Emellett $f_3(N) = f_4(N)/2$.*

*Bizonyítás.* Legyen $N = 2^n D$, ahol $D$ páratlan. A 3.11. Következmény miatt $n \geq 2$ esetén $f_4(N) = 3f_4(D)$. A 3.13. Állítás miatt $f_4(D) = 24M$, ahol $M$ a $d$ normájú rendezett $m$-es ikrek száma. Végül minden rendezett $m$-es iker egyértelműen írható $C = cC'$ alakba, ahol $c$ pozitív egész, $C'$ pedig primitív. Nyilván $c \mid D^2$, ezért

$$M = \sum_{c^2 \mid N} k(N/c^2)\,,$$

ahol $k$ a 3.19-ben definiált függvény $m = 4$ esetén. Emiatt

$$f_4(D) = (16 \cdot 24) \sum_{c^2 \mid N} \sum_{d \mid (N/c^2)} h(d) h\big(N/(c^2 d)\big)\,.$$

Ismert, hogy multiplikatív számelméleti függvények konvolúciója is multiplikatív. Mivel $h$ nyilván multiplikatív, ezért $k/16$ is az, mert az éppen $h$-nak az önmagával vett konvolúciója. A négyzetszámokhoz 1-et, a többi számhoz nullát rendelő függvény is multiplikatív, ezért a fönti dupla szumma (ami éppen $f_4(D)/384$) is multiplikatív páratlan $D$-re. Végül a bizonyítás elején tett megjegyzések miatt $f_4(N)/384$ is multiplikatív minden pozitív egészre. A fenti bizonyításból nyilvánvalóan látszik, hogy $n \geq 2$-re $f_4(2^n) = 384 \cdot 3$. Ha $p$ páratlan prím, akkor a tételbeli formula előállítása egyszerű rutin számolással már levezethető. Ezt az olvasóra hagyjuk. □

Ezzel elérkeztünk a fejezet végére. A 4-dimenziós esetet lényegében teljesen lerendeztük, a 2-es ikrek számát leszámítva, ez továbbra is nyitott. Esetleg érdemes még azon elgondolkodnia az olvasónak, hogy miként lehetne egy 2-es ikernek megtalálni a rácskockává való kiterjesztését polinom időben (persze ennek egyelőre tudtommal nincsen semmilyen alkalmazása).

## 4. Mi a helyzet magasabb dimenzióban?

Magasabb dimenzióban sok nyitott kérdés van. Nem ismert, hogy $n$-dimenzióban milyen $k$–as iker terjed ki rácskockává. Ebben a fejezetben a $k = 1$ és a $k = n - 1$ esetekkel fogunk foglalkozni. A $k = n - 1$ esetben belátjuk, hogy minden $k$-as iker kiterjed rácskockává páros dimenzióban és minden egész hosszú $k$-as iker kiterjed rácskockává páratlan dimenzióban (ahogy azt láttuk $n = 3$ és $n = 4$ esetén). Fontos megjegyezni, hogy páratlan dimenzióban csak olyanok lehetnek eleve a rácskockák, hogy az élhosszuk egész, ennek a bizonyítását láttuk már az első fejezetben (ugyanaz a bizonyítás működik minden páratlan dimenzió esetén). Ezért páratlan dimenzióban az a feltétel, hogy a hossz egész szám legyen, szükséges a kiterjeszthetőséghez.

**4.1. Tétel.** *Ha $n$ páros, akkor minden $n-1$-es iker kiterjed rácskockává. Ha $n$ páratlan, akkor minden egész hosszú $n-1$-es iker kiterjed rácskockává.*

*Bizonyítás.* Legyen $(v_1, \ldots, v_{n-1})$ egy $n-1$-es iker és $L$ az az $n \times (n-1)$-es mátrix, aminek oszlopai rendre $v_1, \ldots, v_{n-1}$. Ekkor $L^T L = N I_{n-1}$, ahol $I_n$ az $n \times n$-es egységmátrix. A Cauchy-Binet formula miatt

$$\det(L_1)^2 + \cdots + \det(L_n)^2 = N^{n-1}\,,$$

ahol $L_i$ az i-edik sor elhagyásával keletkezett almátrix.

Legyen $M_i = (-1)^{n+i} \det L_i$. Vegyünk $L$-hez hozzá még egy utolsó oszlopot, aminek a koordinátái $M_i/N^{n-2/2}$. A kapott mátrixot nevezzük $K$-nak. Ekkor $K$ oszlopai páronként ortogonálisak a Laplace-kifejtés miatt. Így $K^T K = NI_n$. Legyenek $L$ sorai $s_1, \ldots, s_n$. Tekintsük $s_i$ önmagával vett skalárszorzatát. Ez egy egész szám és $N - M_i^2/N^{n-2}$-vel egyenlő. Emiatt $N^{n-2} \mid M_i$. Tehát ha $n$ páros, vagy $N$ négyzetszám, akkor $K$ utolsó oszlopának elemei egész számok, s ezt az oszlopot hozzávéve az $n-1$ vektorhoz egy rácskockát kaptunk. □

Most rátérünk a $k = 1$ esetre. A 3.1. Tétel mintájára a nyolcdimenziós esetben is kaphatunk kiterjesztést, csak most a kvaterniók helyett a Cayley-számok szorzástábláját kell használnunk. Egy ilyen kiterjesztés például a következő:

$$\begin{pmatrix} a & b & c & d & e & f & g & h \\ b & -a & d & -c & f & -e & -h & g \\ c & -d & -a & b & g & h & -e & -f \\ d & c & -b & -a & h & -g & f & -e \\ e & -f & -g & -h & -a & b & c & d \\ f & e & -h & g & -b & -a & -d & c \\ g & h & e & -f & -c & d & -a & -b \\ h & -g & f & e & -d & -c & b & -a \end{pmatrix}$$

Megmutatjuk, hogy hasonló kiterjesztés csak 1, 2, 4, illetve 8-dimenzióban lehetséges.

**4.2. Definíció.** Az $n \times n$-es $M$ mátrixot *permutációs kockának* nevezzük, ha $MM^T$ skalármátrix, és $M$ bármelyik sora megkapható az első sorból úgy, hogy annak elemeit permutáljuk és előjelezzük. Az *általános* permutációs kocka egy olyan permutációs kocka, melynek első sorában páronként különböző határozatlanok állnak.

A fenti $8 \times 8$-as mátrix tehát általános permutációs kocka, melynek a bal felső sarkában látható $4 \times 4$-es, $2 \times 2$-es és $1 \times 1$-es részmátrix is az.

**4.3. Tétel.** *Általános permutációs kocka pontosan az* 1, 2, 4, 8 *méretekben létezik.*

*Bizonyítás.* Legyen az $M$ általános permutációs kocka első sora $(x_1, \ldots, x_n)$. Ha az $M$ sorait permutáljuk és egyes sorokat $-1$-gyel megszorzunk, akkor $M$ továbbra is általános permutációs kocka marad, de elérhetjük, hogy hogy $M$ főátlójában végig $x_1$ álljon. Jelölje $x_i A_i$ azt a mátrixot, amit $M$-ből úgy kapunk, hogy minden $x_j$ helyébe nullát írunk, ha $j \neq i$. Nyilván $M = x_1 A_1 + \ldots + x_n A_n$ és $A_1 = I_n$. A feltétel szerint

$$MM^T = \sum_{i,j=1}^{n} x_i x_j A_i A_j^T = \lambda I_n \,,$$

ahol $\lambda$ egy polinom. Az első sor első elemét megnézve kapjuk, hogy $\lambda = x_1^2 + \ldots + x_n^2$. Innen $x_i$ helyébe 1-et, a többi $x_j$ helyébe nullát írva az adódik, hogy $A_i A_i^T = I_n$. Az $x_i x_j$ együtthatóját vizsgálva $A_i A_j^T + A_j A_i^T = 0$ adódik minden $i \neq j$-re. Ha $i = 1$, akkor innen $A_j^T = -A_j$, vagyis $j \geq 2$ esetén $A_j$ nemcsak ortogonális, hanem ferdén

szimmetrikus is, és így $A_j^2 = -A_j(-A_i) = -A_jA_j^T = -I_n$. Ha $i, j \geq 2$, akkor a fenti egyenletből $-A_iA_j - A_jA_i = A_iA_j^T + A_jA_i^T = 0$.

A 2.8. Hurwitz-Radon-tétel tehát alkalmazható, és azt adja, hogy $\rho(n) \geq n$. A tétel jelöléseivel így $2^c + 8d \geq (2a+1)2^{c+4d} \geq 2^c 16^d$. Innen nyilván $d = 0$, és akkor $a = 0$, vagyis $n$ tényleg csak 1, 2, 4 vagy 8 lehet. □

Elemi csoportelméleti megfontolásokkal könnyen adódik, hogy az $M_i$ mátrixok egy extraspeciális 2-csoportot generálnak. Így azt, hogy az $n$ szám 2-hatvány, könnyű belátni a topológiai apparátus nélkül is.

## Irodalom


[1] John W. Bales, *Cayley-Dickson and Clifford Algebras as Twisted Group Algebras*, 2003.
[2] Erdős Pál, Surányi János, *Válogatott fejezetek a számelméletből*, Polygon, 1996.
[3] L. M. Goswick, E. W. Kiss, G. Moussong, N. Simányi, *Sums of squares and orthogonal integral vectors*, preprint, 2008, lásd `http://arxiv.org/pdf/0806.3943`.
[4] Horváth Márton, *Kockarácsok*, Budapest, 2009.
[5] A. Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen*, Berlin, 1919.
[6] V. V. Praszolov, *Lineáris algebra*, TypoTEX, 2005.