Kvaterniot

Anna-Kaisa Markkanen

Matematiikan pro gradu -tutkielma

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kesä 2014

Tiivistelmä: A-K. Markkanen, *Kvaterniot* (engl. *Quaternions*), matematiikan pro gradu -tutkielma, 53 sivua, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, kesä 2014.

Kvaterniot ovat muotoa $x_1 + ix_2 + jx_3 + kx_4$ olevia neliulotteisia lukuja, jotka muodostavat omien yhteen- ja kertolaskusääntöjensä kanssa kvaternioiden joukon $\mathbb{H}$. Irlantilainen matemaatikko Sir William Hamilton kehitti kvaterniot vuonna 1843 etsiessään kompleksiluvuista seuraavaa lukualueiden laajennusta.

Kuten jokainen kompleksiluku voidaan esittää kahden reaaliluvun avulla, voidaan jokainen kvaternio esittää kahden kompleksiluvun avulla muodossa $q = z + jw$, missä $z = x_1 + ix_2$ ja $w = x_3 + ix_4$. Kvaterniot voidaan esittää vaihtoehtoisesti myös matriisimuodossa siten, että kvaterniota $q = x_1 + ix_2 + kx_3 + kx_4$ vastaa matriisi

$$q = \begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{bmatrix}.$$

Joitakin kvaternioiden ominaisuuksia on helpompi tutkia niiden matriisimuotojen kautta.

Kvaternioiden kertolasku ei ole kommutatiivinen, joten kvaternioiden joukko $\mathbb{H}$ varustettuna kvaternioiden yhteen- ja kertolaskulla ei ole kunta. Se on kuitenkin jakorengas.

Kvaterniot voidaan jakaa *reaalisiin kvaternioihin* $\alpha = x_1$ ja *imaginaarisiin kvaternioihin* $u = ix_2 + jx_3 + kx_4$, ja jokainen kvaternio voidaan esittää muodossa $q = \alpha + u$. Imaginaariset kvaterniot voidaan samaistaa avaruuden $\mathbb{R}^3$ vektoreihin $x = (x_1, x_2, x_3)$, ja tällöin avaruuden $\mathbb{R}^3$ vektoreiden ominaisuuksia voidaan tarkastella kvaternioiden avulla.

Erityisesti avaruuden $\mathbb{R}^3$ kiertoja voidaan tarkastella imaginaaristen kvaternioiden avulla. Kun määritellään kuvaus $T_{q_0} : Im(\mathbb{H}) \to Im(\mathbb{H})$,

$$T_{q_0}(q) = q_0 q q_0^{-1},$$

missä $q_0 \in \mathbb{H}$, saadaan kuvausten T_{q_0} ja imaginaaristen kvaternioiden avulla esitettyä kaikki avaruuden $\mathbb{R}^3$ kierrot.

Kvaternioiden avulla voidaan myös osoittaa, että jokainen alkuluku voidaan esittää neljän kokonaisluvun neliön summana. Tämä tapahtuu määrittelemällä *Hurwitzin kvaterniot*, jotka ovat sellaisia kvaternioita, joiden reaalilukukomponentit ovat kaikki joko kokonaislukuja tai parittomien kokonaislukujen puolikkaita. Koska jokainen kokonaisluku voidaan esittää alkulukujen tulona, saadaan osoitettua, että jokainen kokonaisluku voidaan esittää neljän kokonaisluvun neliön summana.

Kvaternioista seuraava lukualueiden laajennus on kahdeksanulotteisten *oktonioiden* joukko. Kuten jokainen kvaternio voidaan esittää kahden kompleksiluvun avulla, voidaan jokainen oktonio esittää kahden kvaternion avulla. Oktonioiden kertolasku ei ole kommutatiivinen eikä edes assosiatiivinen, joten oktoniot eivät muodosta ryhmää.

Sisältö

Johdanto

Kvaterniot ovat neliulotteisia lukuja, jotka ovat muotoa $x_1 + ix_2 + kx_3 + kx_4$, missä $x_1, x_2, x_3, x_4 \in \mathbb{R}$ ja i, j ja k ovat *imaginaariyksiköitä*. Kvaternioille on määritelty omat yhteen- ja kertolaskusäännöt.

Kvaterniot keksi pitkän tutkimisen jälkeen irlantilainen Sir William Hamilton vuonna 1843. Hän yritti pitkään laajentaa kompleksilukuja kolmiulotteisiksi *hyperkompleksiluvuiksi*, joiden kertolasku toteuttaisi reaalilukujen kertolaskun säännöt. Nykyään voidaan helposti osoittaa, että tällaista lukukolmikoiden kertolaskua ei voida löytää. Hamilton keksi lopulta laajentaa lukukolmikot neliulotteisiksi luvuiksi, kvaternioiksi. Kappaleessa 1 käydään läpi hieman Hamiltonin henkilöhistoriaa sekä enemmän kvaternioiden löytymisen historiaa.

Kvaternioiden joukko $\mathbb{H}$ on neliulotteinen avaruus varustettuna kvaternioiden yhteen- ja kertolaskuilla. Peruskvaternioiden kertolaskusäännöt ovat

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

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Näistä johtamalla saadaan laskettua kertolaskusääntö kahdelle kvaterniolle. Luvussa 2 esitellään kvaternioiden laskusäännöt sekä käydään läpi kvaternioiden yleisiä ominaisuuksia. Luvussa 2 kerrotaan, että kvaterniot voidaan esittää muodossa $q = \alpha + u$, missä $\alpha = x_1$ on *reaalinen kvaternio* ja $u = ix_2 + jx_3 + kx_4$ *imaginaarinen kvaternio*. Myöhemmissä luvuissa huomataan, että erityisesti imaginaariset kvaterniot ovat hyödyllisiä monissa sovelluksissa.

Jokainen kvaternio voidaan esittää myös kahden kompleksiluvun avulla, jolloin voidaan merkitä $q = z + jw$, missä $z = x_1 + ix_2$ ja $w = x_3 + ix_4$ ovat kompleksilukuja. Vaihtoehtoinen tapa merkitä kvaternioita on esittää kvaternio $q = x_1 + ix_2 + jx_3 + kx_4$ matriisina

$$q = \begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{bmatrix}.$$

Luvussa 3 näytetään, että kvaternioiden laskutoimitukset vastaavat matriisien laskutoimituksia. Matriisimuodossa esittäessä monia kvaternioiden ominaisuuksia on helpompi todistaa.

Luvussa 4 tutkitaan kvaternioiden algebraa. Tässä luvussa osoitetaan, että peruskvaternioiden joukko $G = \{\pm 1, \pm i, \pm j, \pm k\}$ varustettuna kvaternioiden kertolaskulla on ryhmä ja että kvaternioiden joukko $\mathbb{H}$ varustettuna kvaternioiden yhteenlaskulla ja kertolaskulla on vino jakorengas, jonka keskus on $Re(\mathbb{H})$ eli reaalisten kvaternioiden joukko.

Imaginaariset kvaterniot voidaan samaistaa avaruuden $\mathbb{R}^3$ vektoreihin niin, että imaginaarista kvaterniota $u = ix_1 + jx_2 + kx_3$ vastaa avaruuden $\mathbb{R}^3$ vektori $x = (x_1, x_2, x_3)$. Luvussa 5 huomataan, että imaginaaristen kvaternioiden kertolasku voidaan kirjoittaa muodossa

$$uv = -\langle u, v\rangle + u \times v,$$

missä $\langle u, v\rangle$ on vektoreiden u ja v *sisätulo* ja $u \times v$ *ristitulo*. Luvussa 5 käydään läpi avaruuden $\mathbb{R}^3$ vektoreiden, eli imaginaaristen kvaternioiden, ominaisuuksia, muun muassa sisätulon ja ristitulon laskusääntöjä.

Luvussa 6 näytetään, kuinka avaruuden $\mathbb{R}^3$ kiertoja voidaan esittää kvaternioiden avulla määrittelemällä kuvaus $T_{q_0} : \mathbb{H} \to \mathbb{H}$,

$$T_{q_0}(q) = q_0 q q_0^{-1},$$

missä q_0 on yksikkökvaternio. Tässä luvussa käydään läpi kuvauksen T_{q_0} ominaisuuksia ja osoitetaan muun muassa että kuvaus T_{q_0} on bijektio ja että se kuvaa imaginaariset kvaterniot imaginaarisiksi. Luvun lopussa osoitetaan, että kuvausten T_{q_0} avulla saadaan esitettyä kaikki avaruuden $\mathbb{R}^3$ kierrot. Esimerkin avulla näytetään, kuinka tämä käytännössä toimii.

Luvussa 7 määritellään *Hurwitzin kvaterniot*, eli sellaiset kvaterniot, joiden kaikki reaalilukukomponentit ovat joko kokonaislukuja tai parittomien kokonaislukujen puolikkaita. Hurwitzin kvaternioita apuna käyttäen todistetaan, että mikä tahansa alkuluku voidaan esittää neljän kokonaisluvun neliön summana. Tätä tulosta apuna käyttäen osoitetaan, että mikä tahansa kokonaisluku voidaan esittää neljän kokonaisluvun neliön summana.

Kun Hamilton oli löytänyt kvaterniot, alettiin luonnollisesti etsiä seuraavia lukualueiden laajennuksia. Luvussa 8 tutustutaan lyhyesti oktonioihin, kahdeksanulotteisiin lukuihin, jotka käyttäytyvät hyvin samankaltaisesti kuin kvaterniot. Kuten jokainen kvaternio voidaan esittää kahden kompleksiluvun avulla, voidaan jokainen oktonio esittää kahden kvaternion avulla. Oktonioille ei voida määritellä kommutatiivista eikä edes assosiatiivista kertolaskua, joten oktonioiden joukko $\mathbb{O}$ ei muodosta ryhmää.

LUKU 1

Historiaa

Historian tietojen lähteenä on käytetty teoksia [**9**] ja [**11**].

Sir Willian Hamilton (1805-1865) oli irlantilainen matemaatikko. Hän oli jo lapsena poikkeuksellisen älykäs ja opiskeli setänsä johdolla koko lapsuutensa ajan useita eri kieliä, muun muassa latinaa, kreikkaa ja hepreaa. 13-vuotiaana hän koki saaneensa tarpeekseen kielistä, ja hänen kiinnostuksensa matematiikkaa kohtaan heräsi. Hän aloitti opiskelut Dublinin Trinity Collegessa 18-vuotiaana ja toimi siellä myös astronomian opettajana jo ennen valmistumistaan. Hänen uransa eteni vauhdilla. Hänet nimitettiin vuonna 1827, 22-vuotiaana, Irlannin kuninkaalliseksi astronomiksi. Vuonna 1835, vain 30-vuotiaana, hänet lyötiin ritariksi ja hänestä tuli sir William Hamilton.

Hamiltonin kiinnostus kvaternioita kohtaan alkoi kompleksiluvuista. Yksi hänen aiemmista tunnetuista saavutuksista olikin, kun hän vuonna 1835 esitti, että kompleksiluvut voidaan määritellä reaalilukupareina $x + iy = (x, y)$ ja että reaalilukujen yhteen- ja kertolaskun lait assosiatiivisuus, kommutatiivisuus ja distributiivisuus pätevät myös kompleksiluvuille.

Hamilton mietti, kuinka lukualueita voisi laajentaa kompleksiluvuista eteenpäin. Hän halusi laajentaa kompleksiluvut kolmiulotteisiksi *hyperkompleksiluvuiksi*, eli sellaisiksi lukukolmikoiksi, jotka ovat muotoa $\alpha + i\beta + j\gamma = (\alpha, \beta, \gamma)$, missä i ja j ovat *imaginaariyksiköitä* joille pätee $i^2 = j^2 = -1$. Ehtona oli, että lukujen täytyisi käyttäytyä yhteen- ja kertolaskun suhteen samoin kuin reaalilukujen. Lisäksi kun luvuille määritellään normi $N(\alpha+i\beta+j\gamma) = \alpha^2+\beta^2+\gamma^2$, tulisi kertolaskun olla yhteensopiva sen kanssa, eli $N(xy) = N(x)N(y)$ kaikilla lukukolmikoilla x ja y.

Lukukolmikoille oli helppo määritellä yhteenlasku, joka toimii kuten reaalilukujen yhteenlasku; lasketaan luvut yhteen komponenteittain kuten kompleksilukujenkin yhteenlaskussa, $(\alpha, \beta, \gamma)+(a, b, c) = (\alpha+a, \beta+b, \gamma+c)$. Kertolaskun määritteleminen kuitenkin aiheutti ongelmia. Hamilton yritti vuosia keksiä lukukolmikolle kertolaskua $(\alpha, \beta, \gamma)(a, b, c) = (A, B, C)$, joka toimisi kuten reaalilukujen kertolasku ja joka olisi yhteensopiva normin kanssa, mutta ei yrityksistään huolimatta koskaan onnistunut. Ennen kuolemaansa hän kirjoitti kirjeessä pojalleen: ”Joka aamu, kun tulin aamiaiselle, kysyit minulta: 'Isä, joko sinä osaat kertoa lukukolmikoita?' Joka kerta jouduin vastaamaan pään pudistuksen kera 'Ei, osaan vain laskea niitä yhteen ja vähentää.' ”

Nykyään on helppo osoittaa, että tällaista kertolaskua ei voida määritellä lukukolmikolle:

Olkoot $1 = (1, 0, 0)$, $i = (0, 1, 0)$ ja $j = (0, 0, 1)$ perusyksiköitä siten, että
$i^2 = j^2 = -1$. Tällöin olisi

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

joillakin $\alpha, \beta, \gamma \in \mathbb{R}$. Jos oletetaan, että kertolasku on assosiatiivinen, niin pätee $i(ij) = (ii)j = -j$. Nyt

$$\begin{aligned} -j = i(ij) &= i(\alpha + \beta i + \gamma j) = (\alpha i - \beta + \gamma ij) \\ &= \alpha i - \beta + \gamma(\alpha + \beta i + \gamma j) \\ &= (\gamma\alpha - \beta) + (\gamma\beta + \alpha)i + (\gamma^2)j. \end{aligned}$$

Siis olisi $\gamma^2 = -1$, mikä ei voi olla mahdollista, sillä $\gamma \in \mathbb{R}$.

Itse asiassa ranskalainen matemaatikko Adrien Marie Legendre osoitti jo 1830-luvulla, että lukukolmikoille ei voida määritellä reaalilukujen tapaan toimivaa kertolaskua. Jos Hamilton olisi lukenut lukuteoriaa ja kuullut tästä tuloksesta, hän ei luultavasti olisi käyttänyt turhaan vuosia tällaisen kertolaskun etsimiseen.

Kvaternioiden löytymisen läpimurto tapahtui vuonna 1843. Tarinan mukaan Hamilton oli 16. lokakuuta vuonna 1843 kävelemässä vaimonsa Lady Hamiltonin kanssa tapaamiseen Kuninkaalliseen Irlannin Akatemiaan. Kävellessään Broughamin sillalla hän viimein tajusi, että kahden imaginaarisen yksikön sijaan hän tarvitsisi kolme. Hän raapusti keksimänsä imaginaariyksiköiden laskusäännöt sillan kiveen:

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

Hamiltonista tuli kvaternioiden luoja, ja kvaternioita kutstutaankin myös Hamiltonin kvaternioiksi. Hamilton käytti lähes koko loppuelämänsä kvaternioiden tutkimiseen ja kirjoitti niistä myös kirjallisuutta. Kvaternioista tuli Dublinin yliopistossa myös oma opetettava aineensa.

Monet matemaatikot vähättelivät kvaternioiden merkitystä, sillä niiden kertolasku ei ollut kommutatiivinen, eli ne eivät toimineet kuten ”tavalliset” luvut. Hamilton kuitenkin uskoi, että kvaternioilla tulisi olemaan tärkeä rooli fysiikassa. 1880-luvulla Josiah Willard Gibbs ja Oliver Heaviside kehittelivät nykymuotoista vektorianalyysia ja keksivät käyttää kvaternioita vektoreina erottamalla niistä reaali- ja imaginaariosan erilleen. Tässä tarkoituksessa kvaternioita käytetään yhä edelleen fysiikan ja tekniikan sovelluksissa. Kvaternioiden löytymisellä oli toinenkin tärkeä seuraus; ne olivat ensimmäiset luvut jotka eivät toteuttaneet ”tavallista” algebraa. Vaikka kaikki eivät heti hyväksyneetkään kvaternioita oikeiksi luvuiksi, niiden kehittäminen vapautti algebrallista ajattelua ja avasi ovia uudenlaiselle matemaattiselle ajattelulle.

LUKU 2

Kvaterniot

Luvun 2 tietoja on poimittu lähes kaikista lähteistä. Pääasiallisina lähteinä on käytetty luentomonistetta [**4**] sekä teoksia [**1**], [**2**] ja [**10**].

Merkitään vektoriavaruudessa $\mathbb{R}^4$

$$1 = (1,0,0,0), \qquad i = (0,1,0,0),$$

$$j = (0,0,1,0), \qquad k = (0,0,0,1).$$

Tällöin kaikki avaruuden $\mathbb{R}^4$ alkiot voidaan kirjoittaa muodossa

$$x = (x_1, x_2, x_3, x_4) = x_1 1 + x_2 i + x_3 j + x_4 k = x_1 + ix_2 + jx_3 + kx_4,$$

missä $x_1, x_2, x_3, x_4 \in \mathbb{R}$. Tällaisia neliulotteisia lukuja kutsutaan *kvaternioiksi*. Kvaternioita 1, i, j ja k kutsutaan *peruskvaternioiksi*. Kvaternioiden joukko $\mathbb{H}$ on neliulotteinen avaruus varustettuna kvaternioiden yhteen- ja kertolaskulla.

Olkoot $q = x_1 + ix_2 + jx_3 + kx_4$ ja $p = y_1 + iy_2 + jy_3 + ky_4$ kvaternioita. Vektoriavaruuden laskusääntöjen nojalla kvaternion q ja reaaliluvun s tulo on

$$sq = s(x_1 + ix_2 + jx_3 + kx_4) = sx_1 + isx_2 + jsx_3 + ksx_4,$$

kvaternioiden q ja p yhteenlasku on

$$\begin{aligned} q + p &= (x_1 + ix_2 + jx_3 + kx_4) + (y_1 + iy_2 + jy_3 + ky_4) \\ &= (x_1 + y_1) + i(x_2 + y_2) + j(x_3 + y_3) + k(x_4 + y_4) \end{aligned}$$

ja vähennyslasku

$$\begin{aligned} q - p &= (x_1 + ix_2 + jx_3 + kx_4) - (y_1 + iy_2 + jy_3 + ky_4) \\ &= (x_1 - y_1) + i(x_2 - y_2) + j(x_3 - y_3) + k(x_4 - y_4). \end{aligned}$$

Kvaternioiden q ja p kertolaskun määrittelemiseksi määritellään ensin peruskvaternioiden kertolaskusäännöt, joiden avulla voidaan johtaa yleinen kahden kvaternion kertolasku. Peruskvaternioiden kertolaskukaavat ovat

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

$$ij = -ji = k$$

$$jk = -kj = i$$

$$ki = -ik = j.$$

Peruskvaternioiden kertolaskut voidaan esittää taulukkona:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Taulukko 1. Peruskvaternioiden kertolasku

Olettaen, että tavalliset kertolaskusäännöt pätevät kvaternioille, saadaan peruskvaternioiden kertolaskukaavojen avulla saadaan johdettua lauseke kahden kvaternion kertolaskulle:

$$\begin{aligned}
qp &= (x_1 + ix_2 + jx_3 + kx_4)(y_1 + iy_2 + jy_3 + ky_4)\\
&= x_1y_1 + x_1iy_2 + x_1jy_3 + x_1ky_4 + ix_2y_1 + ix_2iy_2 + ix_2jy_3 + ix_2ky_4\\
&+ jx_3y_1 + jx_3iy_2 + jx_3jy_3 + jx_3ky_4 + kx_4y_1 + kx_4iy_2 + kx_4jy_3 + kx_4ky_4\\
&= x_1y_1 + ix_1y_2 + jx_1y_3 + kx_1y_4 + ix_2y_1 - x_2y_2 + kx_2y_3 - jx_2y_4\\
&+ jx_3y_1 - kx_3y_2 - x_3y_3 + ix_3y_4 + kx_4y_1 + jx_4y_2 - ix_4y_3 - x_4y_4\\
&= x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4\\
&+ (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)i\\
&+ (x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)j\\
&+ (x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)k.
\end{aligned}$$

Kvaternioiden kertolasku on assosiatiivinen, mutta ei kommutatiivinen, sillä esimerkiksi $ij = k$, mutta $ji = -k$. Kvaternioiden kertolasku on myös distributiivinen, ja distributiivisuudelle saadaan kaksi eri sääntöä:

$$q_1(q_2 + q_3) = q_1q_2 + q_1q_3 \quad \text{ja} \quad (q_2 + q_3)q_1 = q_2q_1 + q_3q_1.$$

Seuraavassa luvussa käydään läpi vaihtoehtoinen tapa tutkia kvaternioiden ominaisuuksia ja siellä osoitamme, että nämä laskusäännöt pätevät.

Määritelmä 2.1. Olkoon $q = x_1 + ix_2 + jx_3 + kx_4$ kvaternio. Sanotaan, että q on *reaalinen kvaternio*, jos $x_2 = x_3 = x_4 = 0$ eli $q = x_1$. Jos taas $x_1 = 0$, eli $q = ix_2+jx_3+kx_4$, sanotaan, että q on *imaginaarinen kvaternio*. Merkitään reaalisten kvaternioiden joukkoa $Re(\mathbb{H}) = \{x \in \mathbb{R}\}$ ja imaginaaristen kvaternioiden joukkoa $Im(\mathbb{H}) = \{ix_2 + jx_3 + kx_4 : x_2, x_3, x_4 \in \mathbb{R}\}$.

Huomautus 2.2. Jokainen kvaternio $q = x_1 + ix_2 + jx_3 + kx_4$ voidaan kirjoittaa muodossa $q = \alpha + u$, missä $\alpha = x_1 \in Re(\mathbb{H})$ ja $u = ix_2 + jx_3 + kx_4 \in Im(\mathbb{H})$.

Huomautus 2.3. Koska $Re(\mathbb{H}) = \{x \in \mathbb{R}\} = \mathbb{R}$, voidaan reaalilukujen joukko $\mathbb{R}$ tulkita kvaternioiden $\mathbb{H}$ osajoukoksi, kun samaistetaan reaaliluku x kvaternioksi $(x, 0, 0, 0)$.

Määritelmä 2.4. Kvaternion $q = x_1 + ix_2 + jx_3 + kx_4$

- *konjugaatti* eli *liittoluku* on $\overline{q} = x_1 - ix_2 - jx_3 - kx_3$
- *moduli* eli *itseisarvo* on $|q| = \sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2}$
- *normi* on $N(q) = |q|^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

HUOMAUTUS 2.5. Kaikille $q, p \in \mathbb{H}$ pätee

(1) $\overline{\overline{q}} = q$
(2) $\overline{q+p} = \overline{q} + \overline{p}$
(3) $N(\overline{q}) = N(q)$
(4) jos $q \in Re(\mathbb{H})$, niin $N(q) = q^2$
(5) jos $q \in Im(\mathbb{H})$, niin $\overline{q} = -q$.

LAUSE 2.6. *Olkoot q ja p kvaternioita. Tällöin*

(1) $q\overline{q} = \overline{q}q = N(q)$
(2) $\overline{qp} = \overline{p}\ \overline{q}$
(3) $N(qp) = N(q)N(p)$.
(4) $|qp| = |q||p|$

TODISTUS. Olkoot $q = x_1 + ix_2 + jx_3 + kx_4$ ja $p = y_1 + iy_2 + jy_3 + ky_4$ kvaternioita.

(1) Laskemalla saadaan

$$
\begin{aligned}
q\overline{q} &= (x_1 + ix_2 + jx_3 + kx_4)(x_1 - ix_2 - jx_3 - kx_4) \\
&= (x_1^2 + x_2^2 + x_3^2 + x_4^2) + (-x_1x_2 + x_2x_1 - x_3x_4 + x_4x_3)i \\
&+ (-x_1x_3 + x_3x_1 + x_2x_4 - x_4x_2)j + (-x_1x_4 + x_4x_1 - x_2x_3 + x_3x_2)k \\
&= x_1^2 + x_2^2 + x_3^2 + x_4^2.
\end{aligned}
$$

Vastaavasti

$$
\begin{aligned}
\overline{q}q &= (x_1 - ix_2 - jx_3 - kx_4)(x_1 + x_2 + x_3 + x_4) \\
&= (x_1^2 + x_2^2 + x_3^2 + x_4^2) + (-x_1x_2 + x_2x_1 - x_3x_4 + x_4x_3)i \\
&+ (-x_1x_3 + x_3x_1 + x_2x_4 - x_4x_2)j + (-x_1x_4 + x_4x_1 - x_2x_3 + x_3x_2)k \\
&= x_1^2 + x_2^2 + x_3^2 + x_4^2.
\end{aligned}
$$

Siis $q\overline{q} = \overline{q}q = N(q)$.

(2) Nyt saadaan

$$
\begin{aligned}
\overline{qp} &= \overline{(x_1 + ix_2 + jx_3 + kx_4)(y_1 + iy_2 + jy_3 + ky_4)} \\
&= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4) - (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)i \\
&- (x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)j - (x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)k \\
&= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4) + (-x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3)i \\
&+ (-x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2)j + (-x_1y_4 - x_4y_1 - x_2y_3 + x_3y_2)k
\end{aligned}
$$

ja

$$
\begin{aligned}
\overline{p}\ \overline{q} &= (y_1 - iy_2 - jy_3 - ky_4)(x_1 - ix_2 - jx_3 - kx_4) \\
&= (y_1x_1 - y_2x_2 - y_3x_3 - y_4x_4) + (-y_1x_2 - y_2x_1 + y_3x_4 - y_4x_3)i \\
&+ (-y_1x_3 - y_3x_1 - y_2x_4 + y_4x_2)j + (-y_1x_4 - y_4x_1 + y_2x_3 - y_3x_2)k.
\end{aligned}
$$

Koska $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{R}$, niin $\overline{qp} = \overline{p}\ \overline{q}$.

(3) Edellisten kohtien perusteella

$$
N(qp) \overset{(1)}{=} (qp)(\overline{qp}) \overset{(2)}{=} qp\overline{p}\ \overline{q} \overset{(1)}{=} qN(p)\overline{q} = q\overline{q}N(p) = N(q)N(p)
$$

(4) Normin määritelmän ja edellisen kohdan nojalla

$$|qp|^2 = N(qp) = N(q)N(p) = |q|^2|p|^2.$$

Siis $|qp| = |q||p|$.

□

HUOMAUTUS 2.7. Merkitään $q = \alpha + u$, missä $\alpha \in Re(\mathbb{H})$ ja $u \in Im(\mathbb{H})$. Tällöin

$$N(q) = N(\alpha + u) = N(\alpha) + N(u),$$

sillä jos $q = x_1 + ix_2 + jx_3 + kx_4$, niin

$$N(q) = x_1^2 + x_2^2 + x_3^2 + x_4^2 = (x_1^2) + (x_2^2 + x_3^2 + x_4^2) = N(\alpha) + N(u).$$

MÄÄRITELMÄ 2.8. Kvaternio q on *parillinen* (tai *pariton*), jos sen normi $N(q) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ on parillinen (tai pariton) kokonaisluku.

MÄÄRITELMÄ 2.9. Kvaternio q on *yksikkökvaternio*, jos $N(q) = 1$. Erityisesti imaginaarinen kvaternio u, jolle pätee $N(u) = 1$, on *imaginaarinen yksikkökvaternio.*

Jos $q \neq 0$, on kvaterniolla q olemassa käänteiskvaternio q^{-1}, jolle pätee $qq^{-1} = q^{-1}q = 1$. Käänteiskvaternion lauseke saadaan ratkaistua lauseen 2.6 avulla:

$$q\overline{q} = N(q) \Leftrightarrow q = \frac{1}{\overline{q}}N(q) \Leftrightarrow q^{-1} = \frac{\overline{q}}{N(q)}$$

HUOMAUTUS 2.10. Jos q on yksikkökvaternio, myös q^{-1} on yksikkökvaternio ja $q^{-1} = \overline{q}$.

Osoitetaan seuraavaksi kvaternioiden avulla, että jos kerrotaan keskenään kaksi sellaista lukua, jotka koostuvat neljän kokonaisluvun neliön summasta, saadaan tulokseksi taas luku, joka koostuu neljän kokonaisluvun neliön summasta.

LAUSE 2.11. *Jokaiselle* $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z}$ *pätee*

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

joillakin $z_1, z_2, z_3, z_4 \in \mathbb{Z}$.

TODISTUS. Olkoot $q = x_1 + ix_2 + jx_3 + kx_4$ ja $p = y_1 + iy_2 + jy_y + ky_4$ kvaternioita siten, että $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z}$. Nyt

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = N(q)N(p).$$

Kvaternioiden kertolaskusääntöjen nojalla

$$\begin{aligned} qp = {} & x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 \\ & + (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)i \\ & + (x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)j \\ & + (x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)k, \end{aligned}$$

joten

$$\begin{aligned} N(qp) = {} & (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 \\ & + (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 \\ & + (x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)^2 \\ & + (x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2. \end{aligned}$$

Normin laskusääntöjen nojalla $N(q)N(p) = N(qp)$, joten

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = N(q)N(p) = N(qp)$$

on muotoa $z_1^2 + z_2^2 + z_3^2 + z_4^2$, joten lause pätee. $\square$

LUKU 3

Kvaternioiden matriisiesitys

Tämän kappaleen pääasiallisina lähteinä on käytetty teosta [**1**] sekä tutkielmaa [**6**].

Hamilton osoitti, että jokainen kompleksiluku voidaan esittää kahden reaaliluvun avulla:

$$x + iy = (x, y).$$

Samalla tavoin jokainen kvaternio voidaan esittää kahden kompleksiluvun avulla:

$$\begin{aligned} q &= x_1 + ix_2 + jx_3 + kx_4 \\ &= (x_1 + ix_2) + (x_3 + ix_4)j \\ &= z + jw \\ &= (z, w), \end{aligned}$$

missä $z = x_1 + ix_2 \in \mathbb{C}$ ja $w = x_3 + ix_4 \in \mathbb{C}$.

Osoitetaan seuraavaksi, että kvaternio $q = x_1 + ix_2 + jx_3 + kx_4$ voidaan esittää myös matriisina

$$q = x_1 + ix_2 + jx_3 + kx_4 = \begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{bmatrix} = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{C}).$$

Tällöin kvaternioiden joukko voidaan esittää muodossa

$$\mathbb{H} = \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} : z, w \in \mathbb{C} \right\}.$$

Näytetään, että matriisimuotoisten kvaternioiden joukko $\mathbb{H}$ todellakin on sama kuin luvussa 2 määritelty kvaternioiden joukko. Määritellään kuvaus $h : \mathbb{R}^4 \to \mathbb{H}$ asettamalla

$$\begin{aligned} h(x) &= h(x_1, x_2, x_3, x_4) \\ &= \begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{bmatrix} = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}. \end{aligned}$$

Kuvaus h on lineaarikuvaus, sillä

$$\begin{aligned} h(ax + by) &= h(ax_1 + by_1, ax_2 + by_2, ax_3 + by_3, ax_4 + by_4) \\ &= \begin{bmatrix} ax_1 + by_1 + i(ax_2 + by_2) & ax_3 + by_3 + i(ax_4 + by_4) \\ -ax_3 - by_3 + i(ax_4 + by_4) & ax_1 + by_1 - i(ax_2 + by_2) \end{bmatrix} \\ &= a \begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{bmatrix} + b \begin{bmatrix} y_1 + iy_2 & y_3 + iy_4 \\ -y_3 + iy_4 & y_1 - iy_2 \end{bmatrix} \\ &= ah(x) + bh(y) \end{aligned}$$

kaikilla $a, b \in \mathbb{R}$. Osoitetaan, että kuvaus h on bijektio.

Lause 3.1. *Kuvaus h on bijektio.*

Todistus. Osoitetaan, että kuvaus h on (1) injektio ja (2) surjektio.

(1) Olkoot
$$q = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \text{ ja } p = \begin{bmatrix} z' & w' \\ -\overline{w'} & \overline{z'} \end{bmatrix}$$
matriisimuotoisia kvaternioita. Merkitään $z = x_1 + ix_2$, $z' = x_1' + ix_2'$, $w = x_3 + ix_4$, $w' = x_3' + ix_4'$. Olkoon $q = p$, eli $\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} = \begin{bmatrix} z' & w' \\ -\overline{w'} & \overline{z'} \end{bmatrix}$. Tällöin $z = z'$ ja $w = w'$, mistä seuraa, että $x_1 = x_1'$, $x_2 = x_2'$, $x_3 = x_3'$ ja $x_4 = x_4'$, eli $(x_1, x_2, x_3, x_4) = (x_1', x_2', x_3'.x_4')$. Kuvaus h on siis injektio.

(2) Osoitetaan, että $h(\mathbb{R}^4) = \mathbb{H}$. Selvästi $h(\mathbb{R}^4) \subset \mathbb{H}$. Osoitetaan siis, että $\mathbb{H} \subset h(\mathbb{R}^4)$. Olkoon $q \in \mathbb{H}$. Tällöin $q = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}$ joillakin $z = x_1 + ix_2$ ja $w = x_3 + ix_4$. Merkitään $x = (x_1, x_2, x_3, x_4)$, jolloin
$$h(x) = h(x_1, x_2, x_3, x_4) = \begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_4 \end{bmatrix} = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} = q,$$
joten kuvaus h on surjektio.

Kuvaus h on siis bijektio. □

Koska kuvaus h on bijektio, jokaista avaruuden $\mathbb{R}^4$ alkiota eli myös jokaista kvaterniota vastaa täsmälleen yksi matriisimuotoinen kvaternio. Osoitetaan vielä, että matriisien yhteen- ja kertolasku vastaavat kvaternioiden yhteen- ja kertolaskua.

Olkoot
$$q = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} = \begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{bmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{C})$$
ja
$$p = \begin{bmatrix} t & v \\ -\overline{v} & \overline{t} \end{bmatrix} = \begin{bmatrix} y_1 + iy_2 & y_3 + iy_4 \\ -y_3 + iy_4 & y_1 - iy_2 \end{bmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{C}).$$
Tällöin kun lasketaan matriisien yhteenlaskusäännön avulla, saadaan matriisien q ja p summaksi
$$\begin{aligned} q + p = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} + \begin{bmatrix} t & v \\ -\overline{v} & \overline{t} \end{bmatrix} &= \begin{bmatrix} z + t & w + v \\ -\overline{w} - \overline{t} & \overline{z} + \overline{v} \end{bmatrix} \\ &= \begin{bmatrix} x_1 + y_1 + i(x_2 + y_2) & x_3 + y_3 + i(x_4 + y_4) \\ -x_3 - y_3 + i(x_4 + y_4) & x_1 + y_1 - i(x_2 - y_2) \end{bmatrix}. \end{aligned}$$

Matriisia $q+p$ vastaa siis kvaternio $(x_1+y_1)+i(x_2+y_2)+j(x_3+y_3)+k(x_4+y_4)$, mikä on sama kuin kvaternioiden $q = (x_1+ix_2+jx_3+kx_4)$ ja $p = (y_1+iy_2+jy_3+ky_4)$ summa. Matriisien kertolaskusäännön avulla taas saadaan
$$qp = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \begin{bmatrix} t & v \\ -\overline{v} & \overline{t} \end{bmatrix} = \begin{bmatrix} zt - w\overline{v} & zv + w\overline{t} \\ -\overline{w}t - \overline{z}\,\overline{v} & -\overline{w}v + \overline{z}\,\overline{t} \end{bmatrix}.$$

Lasketaan matriisin alkiot auki yksitellen:

$$\begin{aligned}
zt - w\overline{v} &= (x_1 + ix_2)(y_1 + iy_2) - (x_3 + ix_4)(y_3 - iy_4) \\
&= (x_1y_1 - x_2y_2) + i(x_1y_2 + x_2y_1) - ((x_3y_3 + x_4y_4) + i(-x_3y_4 + x_4y_3) \\
&= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4) + i(x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)
\end{aligned}$$

$$\begin{aligned}
zv + w\overline{t} &= (x_1 + ix_2)(y_3 + iy_4) + (x_3 + ix_4)(y_1 - iy_2) \\
&= (x_1y_3 - x_2y_4) + i(x_1y_4 + x_2y_3) + (x_3y_1 + x_4y_2) + i(-x_3y_2 + x_4y_1) \\
&= (x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2) + i(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)
\end{aligned}$$

$$\begin{aligned}
-\overline{w}t - \overline{z}\,\overline{v} &= -(x_3 - ix_4)(y_1 + iy_2) - (x_1 - ix_2)(y_3 - iy_4) \\
&= -((x_3y_1 + x_4y_2 + i(x_3y_2 - x_4y_1)) - ((x_1y_3 - x_2y_4) + i(-x_1y_4 - x_2y_3)) \\
&= (-x_3y_1 - x_4y_2 - x_1y_3 + x_2y_4) + i(-x_3y_2 + x_4y_1 + x_1y_4 + x_2y_3)
\end{aligned}$$

$$\begin{aligned}
-\overline{w}v + \overline{z}\,\overline{t} &= -(x_3 - ix_4)(y_3 + iy_4) + (x_1 - ix_2)(y_1 - iy_2) \\
&= -((x_3y_3 + x_4y_4) + i(x_3y_4 - x_4y_3)) + (x_1y_1 - x_2y_2 + i(-x_1y_2 - x_2y_1) \\
&= (-x_3y_3 - x_4y_4 + x_1y_2 - x_2y_2) + i(-x_3y_4 + x_4y_3 - x_1y_2 - x_2y_1).
\end{aligned}$$

Matriisia qp vastaa siis kvaternio

$$\begin{aligned}
qp = (&x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4) \\
&+ (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)i \\
&+ (x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2)j \\
&+ (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)k,
\end{aligned}$$

mikä on sama kuin kvaternioiden $q = x_1 + ix_2 + jx_3 + kx_4$ ja $p = y_1 + iy_2 + jy_3 + ky_4$ tulo.

Nyt on osoitettu, että joukko

$$\mathbb{H} = \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} : z, w \in \mathbb{C} \right\}$$

todellakin vastaa luvussa 2 määriteltyä kvaternioiden joukkoa $\mathbb{H}$. Kvaternioita voidaan siis nyt tutkia myös niiden matriisiesityksen kautta. Erityisesti matriisiesitys on kätevä kvaternioiden ominaisuuksien tarkastelulle. Matriisien avulla laskemalla voidaan säästyä pitkiltä laskutoimituksilta.

Kvaternioille pätevät nyt siis luonnollisesti samat laskusäännöt kuin matriiseille. Esimerkiksi matriisien yhteenlasku on tunnetusti assosiatiivinen ja kommutatiivinen, joten myös kvaternioiden yhteenlasku on assosiatiivinen ja kommutatiivinen. Kvaternioiden kertolasku taas on assosiatiivinen, mutta ei kommutatiivinen, sillä esimerkiksi

$$\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \cdot \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \cdot \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}.$$

Matriisien kertolasku on myös tunnetusti distributiivinen, joten luvussa 2 annetut kvaternioiden distributiivisuussäännöt $q_1(q_2 + q_3) = q_1q_2 + q_1q_3$ ja $(q_2 + q_3)q_1 = q_2q_1 + q_3q_1$ voidaan nyt perustella matriisien laskusääntöjen nojalla.

Tutkitaan seuraavaksi kvaternioiden ominaisuuksia niiden matriisiesityksen kautta. Määritellään joukon $\mathbb{H}$ nolla- ja yksikkömatriisi

$$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad \text{ja} \qquad 1 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Tiedetään, että kaikille $A \in \mathcal{M}_{2\times 2}$ pätee $A + 0 = 0 + A = A$ ja $AI = IA = A$.

Jokainen matriisi $q \in \mathbb{H}$ voidaan pilkkoa osiin seuraavasti:

$$\begin{aligned} q &= \begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{bmatrix} \\ &= \begin{bmatrix} x_1 & 0 \\ 0 & x_1 \end{bmatrix} + \begin{bmatrix} ix_2 & 0 \\ 0 & -ix_2 \end{bmatrix} + \begin{bmatrix} 0 & x_3 \\ -x_3 & 0 \end{bmatrix} + \begin{bmatrix} 0 & ix_4 \\ ix_4 & 0 \end{bmatrix} \\ &= x_1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + x_2 \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + x_3 \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + x_4 \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \end{aligned}$$

Merkitään

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},$$

$$j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \qquad k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix},$$

jolloin q voidaan taas kirjoittaa muodossa

$$q = x_1 + ix_2 + jx_3 + kx_4.$$

Luvussa 2 annettiin kvaternion $q \neq 0$ käänteiskvaterniolle lauseke

$$q^{-1} = \frac{1}{N(q)}\overline{q}.$$

Johdetaan tästä käänteiskvaterniolle matriisiesitys:

$$\begin{aligned} q^{-1} &= \frac{1}{N(q)}(x_1 - ix_2 - j_3 - kx_4) \\ &= \frac{1}{N(q)} \begin{bmatrix} x_1 - ix_2 & -x_3 - ix_4 \\ x_3 - ix_4 & x_1 + ix_2 \end{bmatrix}. \end{aligned}$$

Jos merkitään $z' = \frac{1}{N(q)}(x_1 - ix_2)$ ja $w' = \frac{1}{N(q)}(-x_3 - ix_4)$, saadaan käänteiskvaternion matriisiesitys muotoon

$$q^{-1} = \begin{bmatrix} z' & w' \\ -\overline{w'} & \overline{z'} \end{bmatrix}.$$

Koska $x', w' \in \mathbb{C}$, niin $q^{-1} \in \mathbb{H}$. Tutkitaan, millainen matriisimuotoisen kvaternion konjugaatti on:

$$\begin{aligned} \overline{q} &= x_1 - ix_2 - jx_3 - kx_4 \\ &= \begin{bmatrix} x_1 - ix_2 & -x_3 - ix_4 \\ x_3 - ix_4 & x_1 + ix_2 \end{bmatrix} \\ &= \begin{bmatrix} \overline{z} & -w \\ \overline{w} & z \end{bmatrix}, \end{aligned}$$

kun $z = x_1 + ix_2$ ja $w = x_3 + ix_4$. Huomataan, että kvaternion q konjugaatti saadaan ottamalla konjugaatti sen transpoosin q^T jokaisesta alkiosta, sillä

$$q^T = \begin{bmatrix} z & -\overline{w} \\ w & \overline{z} \end{bmatrix}.$$

Kun lasketaan matriisimuotoisen kvaternion determinantti, saadaan yhteys determinantin ja kvaternion normin välille:

$$\begin{aligned}
\det q &= \det \begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{bmatrix} \\
&= (x_1 + ix_2)(x_1 - ix_2) - ((-x_3 + ix_4)(x_3 + ix_4)) \\
&= (x_1^2 + x_2^2) + i(-x_1x_2 + x_2x_1) - ((-x_3^2 - x_4^2)(-x_3x_4 + x_4x_3)) \\
&= x_1^2 + x_2^2 + x_3^2 + x_4^2.
\end{aligned}$$

Nähdään siis, että $\det q = N(q)$.

LUKU 4

Kvaternioiden algebraa

Tutkitaan seuraavaksi kvaternioiden joukon $\mathbb{H}$ algebraa. Osoitetaan, että peruskvaternioiden joukko $G = \{\pm 1, \pm i, \pm j, \pm k\}$ varustettuna kvaternioiden kertolaskulla on ryhmä sekä että joukko $\mathbb{H}$ varustettuna kvaternioiden yhteenlaskulla ja kertolaskulla on jakorengas. Tämän luku perustuu pääasiassa lähteisiin [**5**] ja [**6**].

LAUSE 4.1. *Joukko* $G = \{\pm 1, \pm i, \pm j, \pm k\}$ *varustettuna kvaternioiden kertolaskulla,* $(G, \cdot)$, *on ryhmä.*

TODISTUS. Jotta joukko olisi ryhmä, sille täytyy päteä seuraavat ominaisuudet:

(1) Kertolasku on joukon G sisäinen laskutoimitus
(2) Kertolasku on assosiatiivinen
(3) Kertolaskulla on neuraalialkio
(4) Jokaisella joukon G alkiolla on käänteisalkio kertolaskun suhteen.

Osoitetaan, että nämä ominaisuudet pätevät joukolle $(G, \cdot)$:

(1) Olkoot $q, p \in G$. Tällöin peruskvaternioiden kertolaskusääntöjen nojalla esimerkiksi taulukosta 1 nähdään, että $qp \in G$. Kertolasku on siis joukon G sisäinen laskutoimitus.
(2) Kuten jo aiemmin on todettu, kvaternioiden kertolasku on assosiatiivinen.
(3) Joukossa G on neutraalialkio kertolaskun suhteen, $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, sillä $1 \cdot q = q \cdot 1 = q$ kaikilla $q \in G$.
(4) Koska $1 \cdot 1 = 1$, $-ii = i(-i) = 1$, $-jj = j(-j) = 1$ ja $-kk = k(-k) = 1$, on jokaisella $q \in G$ käänteisalkio kertolaskun suhteen, ja jokaisen $q \in G$ käänteisalkio on myös joukon G alkio.

Joukko $G = \{\pm 1, \pm i, \pm j, \pm k\}$ varustettuna kvaternioiden kertolaskulla on siis ryhmä.
$\square$

LAUSE 4.2. *Joukko* $\mathbb{H}$ *varustettuna yhteenlaskulla ja kertolaskulla,* $(\mathbb{H}, +, \cdot)$, *on jakorengas.*

TODISTUS. Jotta joukko $(\mathbb{H}, +, \cdot)$ olisi jakorengas, sille täytyy päteä seuraavat ominaisuudet:

(1) Joukko $(\mathbb{H}, +)$ on kommutatiivinen ryhmä
(2) Kertolasku on distributiivinen yhteenlaskun suhteen
(3) Kertolaskulla on neutraalialkio
(4) Kaikki nollasta poikkeavat alkiot ovat yksiköitä, eli jokaisella joukon $\mathbb{H}$ nollasta poikkeavalla alkiolla on käänteisalkio kertolaskun suhteen.

Osoitetaan, että nämä ominaisuuden pätevät joukolle $(\mathbb{H}, +, \cdot)$:

(1) Jo aiemmin on todettu, että kvaternioiden yhteenlasku on assosiatiivinen ja kommutatiivinen. Joukossa $\mathbb{H}$ on myös neutraalialkio yhteenlaskun suhteen,
$$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$
sillä $q+0 = 0+q = q$ kaikilla $q \in \mathbb{H}$. Jokaisella $q \in \mathbb{H}$ on lisäksi käänteisalkio yhteenlaskun suhteen, $-q \in \mathbb{H}$, sillä $q + (-q) = -q + q = 0$. Joukko $(\mathbb{H}, +, \cdot)$ on siis kommutatiivinen ryhmä.

(2) Luvussa 2 on todettu, että kvaternioiden kertolasku on distributiivinen yhteenlaskun suhteen.

(3) Joukossa $\mathbb{H}$ on neutraalialkio kertolaskun suhteen,
$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$
sillä $1 \cdot q = q \cdot 1 = q$ kaikilla $q \in \mathbb{H}$.

(4) Olkoon $q = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} = \begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{bmatrix} \in \mathbb{H}$ siten, että $q \neq 0$. Luvussa 3 määritettiin kvaternion q käänteiskvaternio $q^{-1} = \begin{bmatrix} z' & w' \\ -\overline{w'} & \overline{z'} \end{bmatrix}$, missä $z' = \frac{1}{N(q)}(x_1 - ix_2)$ ja $w' = \frac{1}{N(q)}(-x_3 - ix_4)$. Koska nyt $q^{-1} \in \mathbb{H}$ ja $qq^{-1} = q^{-1}q = 1$, niin jokaisella kvaterniolla $q \neq 0$ on käänteisalkio q^{-1} kertolaskun suhteen, eli jokainen $q \in \mathbb{H}$ on yksikkö.

Joukko $(\mathbb{H}, +, \cdot)$ on siis jakorengas. □

Joukko $\mathbb{H}$ ei kuitenkaan ole kunta, sillä kuten jo aiemmin on todettu, kvaternioiden kertolasku ei ole kommutatiivinen. Tutkitaan vielä, mikä on joukon $\mathbb{H}$ *keskus*.

MÄÄRITELMÄ 4.3. Renkaan $(G, +, \cdot)$ *keskus* on joukko
$$Z(G) = \{z \in G : zg = gz \text{ kaikilla } g \in G\}$$
eli joukko, jonka jokainen alkio on kertolaskun suhteen vaihdannainen jokaisen joukon G alkion kanssa.

Osoitetaan, että kvaternioiden joukon $\mathbb{H}$ keskus on joukko $Re(\mathbb{H})$. Todistetaan ensin yksi aputulos:

LEMMA 4.4. *Olkoon* $q = x_1 + ix_2 + jx_3 + kx_4 \in \mathbb{H}$ *joillakin* $x_1, x_2, x_3, x_4 \in \mathbb{R}$. *Tällöin*

(1) *jos* $qi = iq$, *niin* $x_3 = x_4 = 0$
(2) *jos* $qj = jq$, *niin* $x_2 = x_4 = 0$
(3) *jos* $qk = kq$, *niin* $x_2 = x_3 = 0$.

TODISTUS. (1) Kvaternioiden kertolaskusäännön nojalla saadaan
$$\begin{aligned} qi &= (x_1 + ix_2 + jx_3 + kx_4)i \\ &= x_1 i + ix_2 i + jx_3 i + kx_4 i \\ &= ix_1 - x_2 - kx_3 + jx_4 \\ &= x_2 + ix_1 + jx_4 - kx_3, \end{aligned}$$

ja vastaavasti

$$\begin{aligned} iq &= i(x_1 + ix_2 + jx_3 + kx_4) \\ &= ix_1 + iix_2 + ijx_3 + ikx_4 \\ &= ix_1 - x_2 + kx_3 - jx_4 \\ &= x_2 + ix_1 - jx_4 + kx_3. \end{aligned}$$

Näistä huomataan, että $qi = iq \Leftrightarrow x_3 = x_4 = 0$.

Kohtien (2) ja (3) todistus saadaan vastaavilla laskuilla. $\square$

LAUSE 4.5. *Olkoon* $q = x_1 + ix_2 + jx_3 + kx_4 \in \mathbb{H}$ *joillakin* $x_1, x_2, x_3, x_4 \in \mathbb{R}$. *Tällöin* $zq = qz$ *kaikilla* $z \in \mathbb{H}$ *jos, ja vain jos* $x_2 = x_3 = x_4 = 0$.

TODISTUS. "$\Rightarrow$" Olkoon $q \in \mathbb{H}$. Oletetaan, että $zq = qz$ kaikilla $z \in \mathbb{H}$. Valitaan ensin $z = i$. Edellisen lemman perusteella jos $iq = qi$, niin $x_3 = x_4 = 0$. Valitaan sitten $z = j$. Tällöin jos $jq = qj$, niin $x_2 = x_4 = 0$. Yhdistämällä nämä huomataan, että jos $zq = qz$ kaikilla $z \in \mathbb{H}$, niin $x_2 = x_3 = x_4 = 0$.
"$\Leftarrow$" Jos taas $x_2 = x_3 = x_4 = 0$, niin $q = x_1 \in \mathbb{R}$, ja $zq = qz$ kaikilla $z \in \mathbb{H}$. $\square$

Edellisen lauseen perusteella siis renkaan $(\mathbb{H}, +, \cdot)$ keskus on joukko

$$Z(\mathbb{H}) = \{z = x_1 + ix_2 + jx_3 + kx_4 \in \mathbb{H} : x_2 = x_3 = x_4 = 0\} = Re(\mathbb{H}).$$

LUKU 5

Imaginaariset kvaterniot avaruuden $\mathbb{R}^3$ vektoreina

Imaginaariset kvaterniot $ix_1 + jx_2 + kx_3$ voidaan samaistaa kolmiulotteisiin vektoreihin siten, että imaginaarista kvaterniota $ix_1 + jx_2 + kx_3$ vastaa avaruuden $\mathbb{R}^3$ vektori (x_1, x_2, x_3). Avaruuden $\mathbb{R}^3$ vektoreiden ominaisuuksia voidaan siis tutkia imaginaaristen kvaternioiden avulla.

Muistellaan ensin hieman avaruuden $\mathbb{R}^3$ vektoreiden ominaisuuksia. Lähteinä esitiedoille on käytetty pääasiassa luentomonisteita **[7]** ja **[8]**. Olkoot $x = (x_1, x_2, x_3)$ ja $y = (y_1, y_2, y_3)$ kolmiulotteisen avaruuden vektoreita. Vektoreiden x ja y *sisätulo* on

$$\langle x, y \rangle = x_1y_1 + x_2y_2 + x_3y_3 \in \mathbb{R}.$$

Vektoreiden sisätulo on tunnetusti assosiatiivinen, distributiivinen ja kommutatiivinen. Tiedetään myös, että

$$\langle x, y \rangle = 0 \text{ jos ja vain jos } x \perp y. \tag{5.1}$$

Vektoreiden x ja y välinen *ristitulo* on

$$x \times y = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1) \in \mathbb{R}^3.$$

Vektoreiden ristitulo taas ei ole assosiatiivinen eikä kommutatiivinen. Sen sijaan se on distributiivinen sekä antikommutatiivinen eli $x \times y = -(y \times x)$.

Tutkitaan seuraavaksi imaginaaristen kvaternioiden kertolaskun yhteyttä kolmiulotteisten vektoreiden sisätuloon ja ristituloon. Tämän luvun lähteenä on käytetty pääasiassa teosta **[2]**. Olkoot $u = ix_1 + jx_2 + kx_3 = (x_1, x_2, x_3)$ ja $v = iy_1 + jy_2 + ky_3 = (y_1, y_2, y_3)$ imaginaarisia kvaternioita. Kvaternioiden kertolaskusääntöjen mukaan

$$\begin{aligned} uv &= (ix_1 + jx_2 + kx_3)(iy_1 + jy_2 + ky_3) \\ &= -(x_1y_1 + x_2y_2 + x_3y_3) + (x_2y_3 - x_3y_2)i + (x_3y_1 - x_1y_3)j + (x_1y_2 - x_2y_1)k. \end{aligned}$$

Huomataan, että alkuosa $x_1y_1 + x_2y_2 + x_3y_3$ on vektoreiden u ja v sisätulo, ja loppuosa $(x_2y_3 - x_3y_2)i + (x_3y_1 - x_1y_3)j + (x_1y_2 - x_2y_1)k$ on vektoreiden u ja v ristitulo. Nämä yhdistämällä saadaan imaginaaristen kvaternioiden kertolasku muotoon

$$uv = -\langle u, v \rangle + u \times v. \tag{5.2}$$

Tästä saadaan kvaternioiden sisätulo ja ristitulo seuraavanlaiseen muotoon:

$$u \times v = \frac{1}{2}(uv - vu) \tag{5.3}$$

ja

$$\langle u, v \rangle = -\frac{1}{2}(uv + vu), \tag{5.4}$$

sillä

$$\begin{aligned}\frac{1}{2}(uv - vu) &= \frac{1}{2}(-\langle u, v\rangle + (u \times v) + \langle v, u\rangle - (v \times u))\\ &= \frac{1}{2}(-\langle u, v\rangle + (u \times v) + \langle u, v\rangle + (u \times v))\\ &= u \times v\end{aligned}$$

ja

$$\begin{aligned}-\frac{1}{2}(uv + vu) &= -\frac{1}{2}(-\langle u, v\rangle + (u \times v) - \langle v, u\rangle + (v \times u))\\ &= (-\langle u, v\rangle + (u \times v) - \langle u, v\rangle - (u \times v))\\ &= \langle u, v\rangle.\end{aligned}$$

Käydään seuraavaksi läpi joitakin lauseita vektoreiden sisätuloon ja ristituloon liittyen.

Lemma 5.1. *Kaikilla $u, v \in Im(\mathbb{H})$ pätee*

$$\langle u, v\rangle = \frac{1}{2}(\overline{u}v + \overline{v}u). \tag{5.5}$$

Todistus. Olkoot $u = ix_1 + jx_2 + kx_3 \in Im(\mathbb{H})$ ja $v = iy_1 + jy_2 + ky_3 \in Im(\mathbb{H})$. Tällöin kvaternioiden kertolaskusäännön nojalla saadaan laskettua

$$\begin{aligned}\overline{u}v + \overline{v}u &= (-ix_1 - jx_2 - kx_4)(iy_1 + jy_2 + ky_4) + (-iy_1 - jy_2 - ky_4)(ix_1 + jx_2 + kx_4)\\ &= (x_1y_1 + x_2y_2 + x_3y_3) + (y_1x_1 + y_2x_2 + y_3x_3) + \big((-x_2y_3 + x_3y_2) + (-y_2x_3 + y_3x_2)\big)i\\ &+ \big((x_1y_3 - x_3y_1) + (y_1x_3 - y_3x_1)\big)j + \big((-x_1y_2 + x_2y_1) + (-y_1x_2 + y_2x_1)\big)k\\ &= 2(x_1y_1 + x_2y_2 + x_3y_3) = 2\langle u, v\rangle.\end{aligned}$$

□

Lause 5.2. *Kaikilla $u, v, w \in Im(\mathbb{H})$ pätee $u \times (v \times w) = \frac{1}{2}(uvw - vwu)$.*

Todistus. Koska

$$uvw = u(-\langle v, w\rangle + (v \times w)) = -\langle v, w\rangle u + u(v \times w)$$

ja

$$vwu = (-\langle v, w\rangle + (v \times w))u = -\langle v, w\rangle u + (v \times w)u,$$

niin

$$\begin{aligned}
\frac{1}{2}(uvw - vwu) &= \frac{1}{2}(-\langle v, w\rangle u + u(v \times w) - (-\langle v, w\rangle u + (v \times w)u)) \\
&= \frac{1}{2}(u(v \times w) - (v \times w)u) \\
&\overset{5.2}{=} \frac{1}{2}(-\langle u, v \times w\rangle + u \times (v \times w) - (-\langle v \times w, u\rangle + (v \times w) \times u)) \\
&= \frac{1}{2}(u \times (v \times w) - (v \times w) \times u) \\
&= \frac{1}{2}(u \times (v \times w) - (-u \times (v \times w)) \\
&= \frac{1}{2}(2(u \times (v \times w))) \\
&= u \times (v \times w).
\end{aligned}$$

□

LAUSE 5.3 (Grassman). *Kaikilla $u, v, w \in Im(\mathbb{H})$ pätee*

$$u \times (v \times w) = \langle u, w\rangle v - \langle u, v\rangle w.$$

TODISTUS. Kaavan (5.4) nojalla

$$\begin{aligned}
uvw - vwu &= (uv + vu)w - v(uw + wu) \\
&= -2\langle u, v\rangle w + 2\langle u, w\rangle v \\
&= 2(\langle u, w\rangle v - \langle u, v\rangle w).
\end{aligned}$$

Lauseen 5.2 nojalla

$$u \times (v \times w) = \frac{1}{2}(uvw - vwu) = \langle u, w\rangle v - \langle u, v\rangle w.$$

□

LAUSE 5.4 (Jacobi). *Kaikilla $u, v, w \in Im(\mathbb{H})$ pätee*

$$u \times (v \times w) + v \times (w \times u) + w \times (u \times v) = 0.$$

TODISTUS. Lause seuraa suoraan edellisestä lauseesta, sillä

$$\begin{aligned}
&u \times (v \times w) + v \times (w \times u) + w \times (u \times v) \\
&\quad = \langle u, w\rangle v - \langle u, v\rangle w + \langle v, u\rangle w - \langle v, w\rangle u + \langle w, v\rangle u - \langle w, u\rangle v \\
&\quad = 0.
\end{aligned}$$

□

Tunnettu ja monissa matematiikan sovelluksissa hyödyllinen Cauchyn epäyhtälö sanoo, että

$$|\langle u, v\rangle|^2 \leq \langle u, u\rangle \cdot \langle v, v\rangle.$$

Avaruudessa $\mathbb{R}^3$ tälle epäyhtälölle on olemassa vahvempi muoto, joka on hyvin keskeinen vektorialgebrassa:

LAUSE 5.5 (Cauchy–Schwarz). *Kaikilla $u, v \in Im(\mathbb{H})$ pätee*

$$\langle u, v\rangle^2 + N(u \times v) = N(u)N(v).$$

TODISTUS. Lauseen todistus seuraa suoraan lauseesta 2.6 sekä kaavasta (5.2):

$$\begin{aligned} N(u)N(v) &\overset{2.6}{=} N(uv) \overset{(5.2)}{=} N(-\langle u,v\rangle + (u\times v)) \\ &\overset{2.7}{=} N(-\langle u,v\rangle) + N(u\times v) \\ &= \langle u,v\rangle^2 + N(u\times v). \end{aligned}$$

Viimeinen yhtäsuuruus pätee, koska jos $\langle u,v\rangle \in \mathbb{R}$, niin $|\langle u,v\rangle|^2 = \langle u,v\rangle^2$. □

Määritellään seuraavaksi avaruuden $\mathbb{R}^3$ kolmen vektorin *kolmitulo.*

MÄÄRITELMÄ 5.6. Kolmen imaginaarisen kvaternion u, v ja w *kolmitulo* on

$$\langle u\times v, w\rangle.$$

LAUSE 5.7. *Kaikilla $u,v,w \in Im(\mathbb{H})$ pätee*

$$\langle u\times v, w\rangle = \langle uv, w\rangle.$$

TODISTUS. Olkoot $u,v,w \in Im(\mathbb{H})$. Nyt yhtälöstä (5.2) seuraa, että

$$\begin{aligned} \langle uv, w\rangle &= \langle(-\langle u,v\rangle + (u\times v)), w\rangle \\ &= \langle -\langle u,v\rangle, w\rangle + \langle (u\times v), w\rangle. \end{aligned}$$

Viimeinen yhtäsuuruus seuraa siitä, että vektoreiden sisätulo on assosiatiivinen. Nyt tiedetään, että $\mathbb{R}\perp Im(\mathbb{H})$. Koska $-\langle u,v\rangle \in \mathbb{R}$ ja $w \in Im(\mathbb{H})$, niin $\langle -\langle u,v\rangle, w\rangle = 0$, joten

$$\langle -\langle u,v\rangle, w\rangle + \langle (u\times v), w\rangle = \langle (u\times v), w\rangle.$$

□

Vektorin sisätulon ja ristitulon määritelmien avulla voidaan osoittaa, että

$$\langle u\times v, u\rangle = 0, \text{ kun } u,v \in Im(\mathbb{H}) : \tag{5.6}$$

Olkoon $u = ix_1 + jx_2 + kx_3 = (x_1,x_2,x_3)$ ja $v = (iy_1 + jy_2 + ky_3) = (y_1,y_2,y_3)$. Tällöin

$$\begin{aligned} \langle u\times v, u\rangle &= \langle (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1), (x_1,x_2,x_3)\rangle \\ &= (x_2y_3 - x_3y_2)x_1 + (x_3y_1 - x_1y_3)x_2 + (x_1y_2 - x_2y_1)x_3 \\ &= x_2y_3x_1 - x_1y_3x_2 + x_3y_1x_2 - x_2y_1x_3 + x_1y_2x_3 - x_3y_2x_1 \\ &= 0. \end{aligned}$$

Edellisten ominaisuuksien perusteella voidaan todistaa seuraava lause:

LAUSE 5.8. *Kaikilla $u,v,w \in Im(\mathbb{H})$ pätee*

$$\langle u\times v, w\rangle = \langle u, v\times w\rangle.$$

TODISTUS. Kaavan (5.6) perusteella

$$\langle (u-w)\times v, (u-w)\rangle = 0.$$

Koska vektoreiden sisätulo on distributiivinen ja ristitulo on distributiivinen ja antikommutatiivinen, niin

$$\begin{aligned}
\langle (u-w)\times v, (u-w)\rangle &= \langle (u\times v) - (w\times v), (u-w)\rangle \\
&= \langle (u\times v), (u-w)\rangle - \langle (w\times v), (u-w)\rangle \\
&= \langle (u\times v), u\rangle - \langle (u\times v), w\rangle - \langle (w\times v), u\rangle + \langle (w\times v), w\rangle \\
&\overset{(5.6)}{=} -\langle (u\times v), w\rangle - \langle u, (w\times v)\rangle \\
&= -\langle (u\times v), w\rangle - \langle u, -(v\times w)\rangle \\
&= -\langle (u\times v), w\rangle + \langle u, (v\times w)\rangle \\
&= 0,
\end{aligned}$$

joten $\langle u\times v, w\rangle = \langle u, v\times w\rangle$. $\square$

LUKU 6

Kvaterniot kolmiulotteisen avaruuden kiertoina

Olkoon $q_0 \in \mathbb{H}$ sellainen kvaternio, jolle $|q_0| = 1$. Määritellään kuvaus $T_{q_0} : \mathbb{H} \to \mathbb{H}$,

$$T_{q_0}(q) = q_0 q q_0^{-1}$$

kaikilla $q \in \mathbb{H}$.

Huomautus 6.1. Ehto $|q_0| = 1$ ei ole välttämätön; Olkoon $|q_0| \neq 1$. Tällöin kvaternio $\tilde{q_0} = \frac{q_0}{|q_0|}$, jolle siis $|\tilde{q_0}| = 1$, antaa

$$\tilde{q_0} q \tilde{q_0}^{-1} = \frac{q_0}{|q_0|} q \frac{|q_0|}{q_0} = q_0 q q_0^{-1}.$$

Tarkastellaan joitakin kuvauksen T_{q_0} ominaisuuksia. Tämän luvun lähteinä on käytetty teosta [**10**] sekä tutkielmaa [**6**].

Lause 6.2. *Olkoon $q_0 \in \mathbb{H}$ siten, että $|q_0| = 1$, ja olkoon kuvaus $T_{q_0} : \mathbb{H} \to \mathbb{H}$, $T_{q_0}(q) = q_0 q q_0^{-1}$. Tällöin*

(1) $T_{q_0}(q + p) = T_{q_0}(q) + T_{q_0}(p)$ *kaikilla* $q, p \in \mathbb{H}$.
(2) $T_{q_0}(qp) = T_{q_0}(q) T_{q_0}(p)$ *kaikilla* $q, p \in \mathbb{H}$.
(3) $T_{q_0}(\alpha q) = \alpha T_{q_0}(q)$ *kaikilla* $\alpha \in \mathbb{R}$, $q \in \mathbb{H}$.

Todistus. Olkoot $q, p \in \mathbb{H}$ ja $\alpha \in \mathbb{R}$. Tällöin

(1) $T_{q_0}(q + p) = q_0(q + p)q_0^{-1} = q_0 q q_0^{-1} + q_0 p q_0^{-1} = T_{q_0}(q) + T_{q_0}(p)$.
(2) $T_{q_0}(q) T_{q_0}(p) = (q_0 q q_0^{-1})(q_0 p q_0^{-1}) = q_0 q p q_0^{-1} = T_{q_0}(qp)$.
(3) Koska $\alpha \in \mathbb{R} = Re(\mathbb{H})$, ja $Re(\mathbb{H})$ on joukon $\mathbb{H}$ keskus, niin

$$T_{q_0}(\alpha q) = q_0 \alpha q q_0^{-1} = \alpha q_0 q q_0^{-1} = \alpha T_{q_0}(q).$$

□

Lause 6.3. *Kuvaus $T_{q_0} : \mathbb{H} \to \mathbb{H}$, $T_{q_0}(q) = q_0 q q_0^{-1}$ on lineaarinen isometria.*

Todistus. Kuvauksen T_{q_0} lineaarisuus seuraa suoraan lauseesta 6.2:

$$T_{q_0}(\alpha q + \beta p) = \alpha T_{q_0}(q) + \beta T_{q_0}(p).$$

Osoitetaan, että kuvaus T_{q_0} on isometria. Täytyy osoittaa, että kaikille $q, p \in \mathbb{H}$ pätee

$$|q - p| = |T_{q_0}(q) - T_{q_0}(p)|.$$

Tämä voidaan osoittaa suoraan itseisarvon laskusääntöjen avulla laskemalla:

$$\begin{aligned}|T_{q_0}(q) - T_{q_0}(p)| &= |q_0 q q_0^{-1} - q_0 p q_0^{-1}| \\ &= |q_0(q-p)q_0^{-1}| \\ &= |q_0||q-p||q_0^{-1}| \\ &= |q_0||\frac{1}{q_0}||q-p| \\ &= |q-p|.\end{aligned}$$

□

HUOMAUTUS 6.4. Koska $T_{q_0}(0) = 0$, seuraa lauseesta 6.3 suoraan, että

$$|T_{q_0}(q)| = |q|$$

kaikilla $q \in \mathbb{H}$.

LAUSE 6.5. *Kuvaus* $T_{q_0} : \mathbb{H} \to \mathbb{H}$, $T_{q_0}(q) = q_0 q q_0^{-1}$ *on bijektio.*

Kuvauksen T_{q_0} bijektiivisyys osoitetaan kolmen seuraavan lauseen avulla.

LAUSE 6.6. *Kuvauksen* T_{q_0} *rajoittuma reaalisten kvaternioiden joukkoon,* $T_{q_0}|_{Re(\mathbb{H})}$, *on identtinen kuvaus.*

TODISTUS. Olkoon $\alpha \in Re(\mathbb{H})$. Koska $Re(\mathbb{H})$ on joukon $\mathbb{H}$ keskus, niin

$$T_{q_0}(\alpha) = q_0 \alpha q_0^{-1} = \alpha q_0 q_0^{-1} = \alpha \cdot 1 = \alpha.$$

□

Koska $T_{q_0}(\alpha) = \alpha$ kaikilla $\alpha \in Re(\mathbb{H})$, on selvää, että jos $q \in Re(\mathbb{H})$, niin $T_{q_0}(q) \in Re(\mathbb{H})$. Osoitetaan seuraavaksi, että jos $q \in Im(\mathbb{H})$, niin $T_{q_0}(q) \in Im(\mathbb{H})$.

LAUSE 6.7. *Jos* $q \in Im(\mathbb{H})$, *niin* $T_{q_0}(q) \in Im(\mathbb{H})$.

TODISTUS. Osoitetaan ensin yksi aputulos:

APUTULOS 6.8. Olkoon q kvaternio. Nyt $q \in Im(\mathbb{H})$ jos, ja vain jos q^2 on ei-positiivinen reaaliluku.

TODISTUS. Olkoon $q = \alpha + u \in \mathbb{H}$, missä $\alpha \in Re(\mathbb{H})$, $0 \neq u = ix_2 + jx_3 + kx_4 \in Im(\mathbb{H})$. Tällöin

$$q^2 = (\alpha + u)^2 = \alpha^2 + 2\alpha u + u^2.$$

Nyt kvaternioiden kertolaskusäännön avulla saadaan laskettua

$$\begin{aligned}u^2 &= (ix_2 + jx_3 + kx_4)^2 = (ix_2 + jx_3 + kx_4)(ix_2 + jx_3 + kx_4) \\ &= -(x_2^2 + x_3^2 + x_4^2) + (x_3x_4 - x_4x_3)i + (-x_2x_4 + x_4x_2)j + (x_2x_3 - x_3x_2)k \\ &= -(x_2^2 + x_3^2 + x_4^2).\end{aligned}$$

Luku u^2 on siis ei-positiivinen reaaliluku. Tarkastellaan nyt kvaternion q^2 osaa $\alpha^2 + 2\alpha u$.

Jos $q \in Im(\mathbb{H})$, niin $\alpha = 0$, eli $q^2 = u^2$ on ei-positiivinen reaaliluku.

Jos taas q^2 on ei-positiivinen reaaliluku, täytyy olla $\alpha u \in \mathbb{R}$, sillä $q^2 = \alpha^2 + 2\alpha u + u^2$ ja $\alpha^2, u^2 \in \mathbb{R}$. Koska $u \in Im(\mathbb{H})$, pätee $\alpha u \in \mathbb{R}$ vain siinä tapauksessa, että $\alpha = 0$.

Siis $q \in Im(\mathbb{H})$. □

Nyt siis $q \in Im(\mathbb{H})$, joten aputuloksen perusteella q^2 on ei-positiivinen reaaliluku. Aputuloksen perusteella myös $T_{q_0}(q) \in Im(\mathbb{H})$, jos $(T_{q_0}(q))^2$ on ei-positiivinen reaaliluku. Laskemalla saadaan

$$\begin{aligned}((T_{q_0}(q))^2 &= (q_0 q q_0^{-1})^2 = (q_0 q q_0^{-1})(q_0 q q_0^{-1}) = q_0 q^2 q_0^{-1}\\ &= q^2 q_0 q_0^{-1} = q^2.\end{aligned}$$

Siis $T_{q_0}(q) \in Im(\mathbb{H})$, joten lause 6.7 on nyt todistettu. □

Lause 6.9. *Kuvauksen T_{q_0} rajoittuma imaginaaristen kvaternioiden joukkoon, $T_{q_0}|_{Im(\mathbb{H})}$, on bijektio.*

Todistus. Määritellään kuvaus $P_{q_0} : Im(\mathbb{H}) \to Im(\mathbb{H})$, $P_{q_0}(q) = q_0^{-1} q q_0$. Tällöin

$$T_{q_0} \circ P_{q_0}(q) = T_{q_0}(q_0^{-1} q q_0) = q_0(q_0^{-1} q q_0) q_0^{-1} = q,$$

ja

$$P_{q_0} \circ T_{q_0}(q) = P_{q_0}(q_0 q q_0^{-1}) = q_0^{-1} q_0 q q_0^{-1} q_0 = q.$$

Siis kuvauksella $T_{q_0} : Im(\mathbb{H}) \to Im(\mathbb{H})$, $T_{q_0}(q) = q_0 q q_0^{-1}$ on käänteiskuvaus $P_{q_0} : Im(\mathbb{H}) \to Im(\mathbb{H})$, $P_{q_0}(q) = q_0^{-1} q q_0$, joten $T_{q_0}|_{Im(\mathbb{H})}$ on bijektio. □

Jos nyt kvaternio q esitetään muodossa $q = \alpha + u$, missä $\alpha \in Re(\mathbb{H})$ ja $u \in Im(\mathbb{H})$, niin kuvaus $T_{q_0}(q)$ saadaan muotoon

$$T_{q_0}(q) = T_{q_0}(\alpha + u) = T_{q_0}(\alpha) + T_{q_0}(u).$$

Koska kuvaus T_{q_0} kuvaa jokaisen reaalisen kvaternion reaaliseksi kvaternioksi ja imaginaarisen kvaternion imaginaariseksi kvaternioksi, ja lisäksi kuvauksen T_{q_0} rajoittuma sekä reaalisten että imaginaaristen kvaternioiden joukkoon on bijektio, on kuvaus T_{q_0} bijektio.

Tutkitaan vielä tarkemmin, mitä kuvaus T_{q_0} tekee geometrisesti avaruudessa $\mathbb{R}^3$. Luvussa 5 näytettiin, että imaginaariset kvaterniot voidaan samaistaa avaruuden $\mathbb{R}^3$ vektoreiksi. Seuraavassa lauseessa tutkitaankin avaruuden $\mathbb{R}^3$ vektoreita, tasoja ja kiertoja käyttäen apuna imaginaarisia kvaternioita tulkiten ne avaruuden $\mathbb{R}^3$ vektoreina.

Lause 6.10. *Olkoon $q_0 = \alpha_0 + u_0 \in \mathbb{H}$, missä $\alpha_0 \in Re(\mathbb{H})$ ja $u_0 \in Im(\mathbb{H})$, ja $|q_0| = 1$. Olkoon kuvaus $T_{q_0} : Im(\mathbb{H}) \to Im(\mathbb{H})$, $T_{q_0}(q) = q_0 q q_0^{-1}$.*

(1) *Jos $\alpha_0 = 0$ eli $q_0 = u_0 \in Im(\mathbb{H})$, niin kuvaus $-T_{q_0}(q) = -q_0 q q_0^{-1}$ on peilaus tason $P \subset \mathbb{R}^3$, jolle $P \perp q_0$, suhteen.*

(2) *Jos $\alpha_0 \neq 0$ eli $q_0 = \alpha_0 + u_0$, niin kuvaus T_{q_0} on kierto kvaternion u_0 suuntaisen vektorin suhteen kulmalla $0 < \theta < \pi$, joka saadaan lausekkeesta $\tan(\frac{\theta}{2}) = \frac{|u_0|}{\alpha_0}$.*

Todistus. Osoitetaan ensin yksi aputulos.

Aputulos 6.11. Olkoon $q_0 = \alpha_0 + u_0 \in \mathbb{H}$ siten että $\alpha_0 \in Re(\mathbb{H})$ ja $u_0 \in Im(\mathbb{H})$. Tällöin

$$T(u_0) = q_0 u_0 q_0^{-1} = u_0.$$

Todistus. Koska $q_0 = \alpha_0 + u_0$, niin u_0 saadaan muotoon $u_0 = q_0 - \alpha_0$. Koska kvaternion ja reaaliluvun välinen kertolasku on kommutatiivinen, saadaan

$$q_0 u_0 q_0^{-1} = q_0(q_0 - \alpha_0) q_0^{-1} = q_0 q_0 q_0^{-1} - q_0 \alpha_0 q_0^{-1} = q_0 - \alpha_0 = u_0.$$

□

Aputuloksen nojalla kuvaus T_{q_0} kuvaa siis vektorin u_0 itsekseen. Koska $T_{q_0}(\alpha u_0) = \alpha T_{q_0}(u_0) = \alpha u_0$, kuvaa T_{q_0} myös kaikki muut vektorin u_0 kanssa yhdensuuntaiset vektorit itsekseen.

Olkoon $P \subset \mathbb{R}^3$ taso siten, että $P \perp u_0$, ja olkoon $q \in Im(\mathbb{H})$. Jaetaan q komponentteihin q_{u_0} ja q_p niin, että $q_{u_0} = \alpha u_0$ jollakin $\alpha \in \mathbb{R}$ ja $q_p \in P$. Nyt tiedetään, että kuvaus T_{q_0} säilyttää komponentin q_{u_0} itsenään, joten tutkitaan, mitä se tekee komponentille q_p. Osoitetaan ensin, että $T_{q_0}(q_p) \in P$.

Aputulos 6.12. Olkoon P taso ja $q_0 = \alpha_0 + u_0$ yksikkökvaternio siten, että $P \perp u_0$. Tällöin $T_{q_0}(q) \in P$ kaikilla $q \in P$.

Todistus. Koska $P \perp u_0$, ja $q \in P$, niin myös $q \perp u_0$. Kaavojen (5.1) ja (5.4) nojalla

$$\begin{aligned} &\langle q, u_0 \rangle = 0 \\ \Leftrightarrow\ & -\frac{1}{2}(qu_0 + u_0 q) = 0 \\ \Leftrightarrow\ & qu_0 + u_0 q = 0. \end{aligned}$$

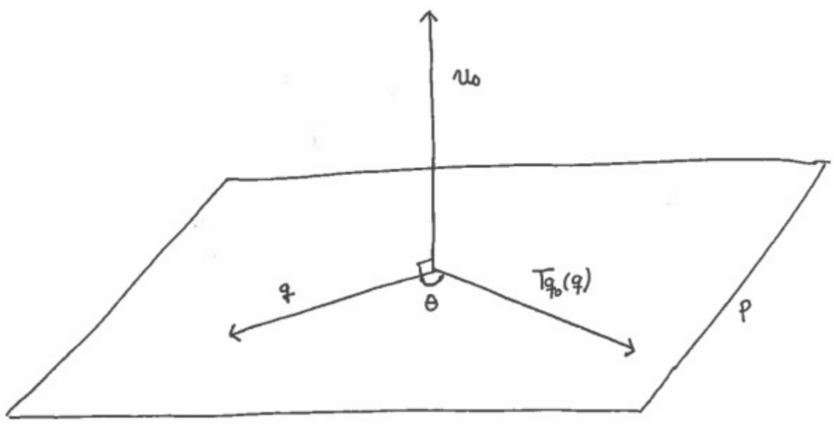
Nyt kaavan (5.1) nojalla $T_{q_0}(q) \in P$ jos, ja vain jos $\langle T_{q_0}(q), u_0 \rangle = 0$, eli $\langle q_0 q q_0^{-1}, u_0 \rangle = 0$. Koska $q_0 = \alpha_0 + u_0$ on yksikkökvaternio, niin $q_0^{-1} = \alpha_0 - u_0$. Lisäksi koska $u_0 \in Im(\mathbb{H})$, niin aputuloksen 6.8 nojalla $u_0^2 \in \mathbb{R}$. Nyt kaavan (5.4) nojalla saadaan laskettua

$$\begin{aligned} \langle q_0 q q_0^{-1}, u_0 \rangle &= -\frac{1}{2}(q_0 q q_0^{-1} u_0 + u_0 q_0 q q_0^{-1}) \\ &= -\frac{1}{2}((\alpha_0 + u_0) q (\alpha_0 - u_0) u_0 + u_0 (\alpha_0 + u_0) q (\alpha_0 - u_0)) \\ &= -\frac{1}{2}((\alpha_0 q + u_0 q)(\alpha_0 u_0 - u_0^2) + (u_0 \alpha_0 + u_0^2)(q \alpha_0 - q u_0)) \\ &= -\frac{1}{2}(\alpha_0^2 q u_0 - \alpha_0 q u_0^2 + u_0 q \alpha_0 u_0 - u_0 q u_0^2 + u_0 \alpha_0^2 q - u_0 \alpha_0 q u_0 + u_0^2 q \alpha_0 - u_0^2 q u_0) \\ &= -\frac{1}{2}(\alpha_0^2 q u_0 + \alpha_0^2 u_0 q - \alpha_0 q u_0^2 + u_0^2 q \alpha_0 + u_0 q \alpha_0 u_0 - u_0 \alpha_0 q u_0 - u_0 q u_0^2 - u_0 q u_0) \\ &= -\frac{1}{2}(\alpha_0^2 (q u_0 + u_0 q) - u_0^2 (u_0 q + q u_0)) \\ &= -\frac{1}{2}((\alpha_0^2 - u_0)(q u_0 + u_0 q)) \\ &= 0, \end{aligned}$$

koska $qu_0 + u_0 q = 0$. Siis $T_{q_0}(q) \in P$ kaikilla $q \in P$. □

Olkoon θ vektoreiden q_p ja $T_{q_0}(q_p) = q_0 q_p q_0^{-1}$ välinen kulma. Koska $|q_0 q_p q_0^{-1}| = |q_0||q_p||q_0^{-1}| = |q_p|$, saadaan sisätulon (kaavan (5.5)) avulla laskettua:

$$\begin{aligned} \cos\theta = \frac{\langle q_p, q_0 q_p q_0^{-1} \rangle}{|q_p|^2} &= \frac{1}{2|q_p|^2}(\overline{q_p}(q_0 q_p q_0^{-1}) + (\overline{q_0 q_p q_0^{-1}}) q_p) \\ = \frac{1}{2|q_p|^2}(\frac{\overline{q_p} q_0 q_p \overline{q_0}}{q_0 \overline{q_0}} + \frac{q_0 \overline{q_0} \overline{q} q_p}{q_0 \overline{q_0}}) &= \frac{1}{2|q_p|^2 |q_0|^2}(\overline{q_p} q_0 q_p \overline{q_0} + q_0 \overline{q_p}\ \overline{q_0} q_p) \\ = \frac{1}{2|q_p|^2 |q_0|^2}(-q_p q_0 q_p \overline{q_0} - q_0 q_p \overline{q_0} q_p) &= -\frac{1}{2|q_p|^2 |q_0|^2}(q_p q_0 q_p \overline{q_0} + q_0 q_p \overline{q_0} q_p). \end{aligned}$$



KUVA 6.1. Lauseen 6.10 taso P ja vektorit u_0, q ja $T_{q_0}(q)$

Jotta tämä yhtälö saadaan helpompaan muotoon, todistetaan seuraava aputulos:

APUTULOS 6.13. Olkoon $q \in Im(\mathbb{H})$ ja $q_0 \in \mathbb{H}$ siten, että $q_0 = \alpha_0 + u_0$. Tällöin, jos $q \perp u_0$, niin $qq_0 = \overline{q_0}q$

TODISTUS. Koska $q, u_0 \in Im(\mathbb{H})$, niin $\overline{q} = -q$ ja $\overline{u_0} = -u_0$. Jos nyt $q \perp u_0$, niin

$$\langle q, u_0 \rangle = \frac{\overline{q}u_0 + \overline{u_0}q}{2} = \frac{-(qu_0 + u_0 q)}{2} = 0$$
$$\Leftrightarrow qu_0 = -u_0 q.$$

Tästä seuraa, että

$$qq_0 = q(\alpha_0 + u_0) = q\alpha_0 + qu_0 = \alpha_0 q - u_0 q = (\alpha_0 - u_0)q = \overline{q_0}q.$$

□

Nyt yhtälö saadaan muotoon

$$\begin{aligned}
\cos\theta &= -\frac{1}{2|q_p|^2|q_0|^2}(\overline{q_p}q_0 q_p \overline{q_0} + q_0 q_p \overline{q_0} q_p) = -\frac{1}{2|q_p|^2|q_0|^2}(\overline{q_0}q_p^2\overline{q_0} + q_0 q_p^2 q_0) \\
&= -\frac{q^2}{2|q_p|^2|q_0|^2}(\overline{q_0}^2 + q_0^2) = -\frac{q_p^2}{2q_p\overline{q_p}|q_0|^2}(\overline{q_0}^2 + q_0^2) \\
&= \frac{1}{2\overline{q_0}q_0}(\overline{q_0}^2 + q_0^2).
\end{aligned}$$

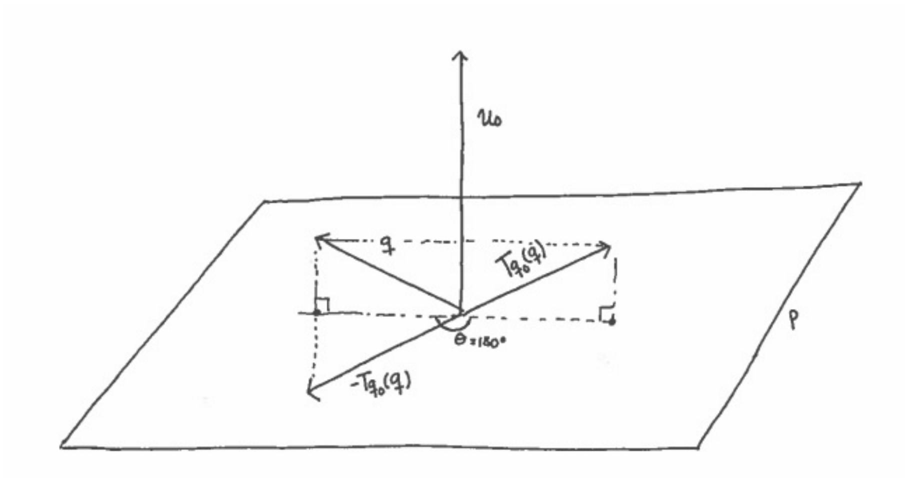
Kun merkitään $q_0 = \alpha_0 + u_0$, saadaan yhtälö edelleen muotoon

$$\begin{aligned}
\cos\theta &= \frac{1}{2(\alpha_0 - u_0)(\alpha_0 + u_0)}((\alpha_0 - u_0)^2 + (\alpha_0 + u_0)^2) \\
&= \frac{1}{2(\alpha_0^2 - u_0^2)}2(\alpha_0^2 + u_0^2) = \frac{\alpha_0^2 + u_0^2}{\alpha_0^2 - u_0^2}.
\end{aligned}$$

Kohta (1): Nyt $\alpha_0 = 0$, joten

$$\cos\theta = \frac{u_0^2}{-u_0^2} = -1,$$

eli $\theta = \pi$. Vektoreiden q_p ja $T_{q_0}(q_p) = q_0 q_p q_0^{-1}$ välinen kulma on siis $180°$ ja $q_p \perp q_0$, joten kuvaus T_{q_0} tasossa P on kierto kulmalla π. Kuvaus $-T_{q_0}$ on siis identiteettikuvaus tasossa P. Kun vektori q jaetaan komponentteihin q_p ja q_{u_0}, niin $-T_{q_0}(q_p) = q_p$ ja $-T_{q_0}(q_{u_0}) = -q_{u_0}$, joten kuvaus $-T_{q_0}$ on peilaus tason P suhteen.



KUVA 6.2. Tapaus $q_0 = u_0$

Kohta (2): Trigonometristen kaavojen mukaan $\tan^2(\frac{\theta}{2}) = \frac{1-\cos\theta}{1+\cos\theta}$, joten

$$\begin{aligned}
\tan^2(\frac{\theta}{2}) = \frac{1-\cos\theta}{1+\cos\theta} &= \frac{1 - \frac{\alpha_0^2+u_0^2}{\alpha_0^2-u_0^2}}{1 + \frac{\alpha_0^2+u_0^2}{\alpha_0^2-u_0^2}} \\
&= \frac{\frac{(\alpha_0^2-u_0^2)-(\alpha_0^2+u_0^2)}{\alpha_0^2-u_0^2}}{\frac{(\alpha_0^2-u_0^2)+(\alpha_0^2+u_0^2)}{\alpha_0^2-u_0^2}} \\
&= \frac{-2u_0^2}{2\alpha_0^2} = \frac{-u_0^2}{\alpha_0^2}.
\end{aligned}$$

Koska $u_0 \in Im(\mathbb{H})$, niin $|u_0|^2 = u_0\overline{u_0} = -u_0^2$, joten $\tan^2(\frac{\theta}{2}) = \frac{|u_0|^2}{\alpha_0^2}$. Siis kuvaus T_{q_0} on kierto kvaternion u_0 suuntaisen akselin suhteen kulmalla θ, jolle $\tan(\frac{\theta}{2}) = \frac{|u_0|}{\alpha_0}$ tai $\tan(\frac{\theta}{2}) = -\frac{|u_0|}{\alpha_0}$.

Vielä täytyy tarkastella, mihin suuntaan kierto tapahtuu. Lasketaan vektoreiden q_p ja $T_{q_0}(q_p)$ ristitulo:

$$
\begin{aligned}
q_p \times T_{q_0}(q_p) &= q_p \times q_0 q_p q_0^{-1} \\
&\overset{(5.3)}{=} \frac{1}{2}(q_p q_0 q_p q_0^{-1} - q_0 q_p q_0^{-1} q_p) \\
&\overset{2.10}{=} \frac{1}{2}(q_p q_0 q_p \overline{q_0} - q_0 q_p \overline{q_0} q_p) \\
&\overset{6.13}{=} \frac{1}{2}(\overline{q_0} q_p q \overline{q_0} - q_0 q_p q_p q_0) \\
&= \frac{1}{2}(q_p^2 \overline{q_0}^2 - q_p^2 q_0^2) \\
&= \frac{1}{2} q_p^2 (\overline{q_0}^2 - q_0^2).
\end{aligned}
$$

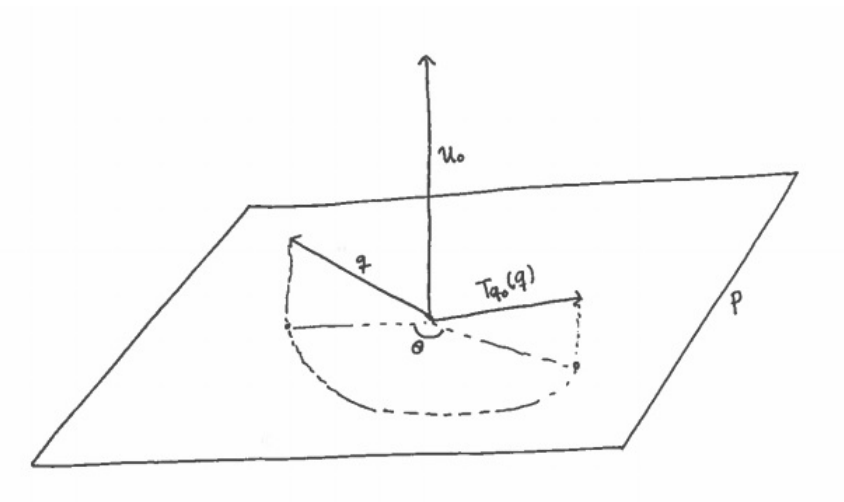
Kun merkitään $q_0 = \alpha_0 + u_0$, saadaan yhtälö edelleen muotoon

$$
\begin{aligned}
q_p \times T_{q_0}(q_p) &= \frac{1}{2} q_p^2 ((\alpha_0 - u_0)^2 - (\alpha_0 + u_0)^2) \\
&= \frac{1}{2} q_p^2 (-4\alpha_0 u_0) = -2q_p^2 \alpha_0 u_0.
\end{aligned}
$$

Koska $q_p \in Im(\mathbb{H})$, niin aputuloksen 6.8 nojalla q_p^2 on negatiivinen reaaliluku. Nyt siis $-2q_p^2\alpha_0 \in \mathbb{R}$, joten vektoreiden q_p ja $T_{q_0}(q_p)$ ristitulo on vektorin u_0 kanssa samansuuntainen vektori. Jos nyt $-2q_p^2\alpha_0 > 0$, tapahtuu kierto oikean käden säännön nojalla positiiviseen suuntaan ja jos $-2q_p^2\alpha_0 < 0$, tapahtuu kierto negatiiviseen suuntaan.

Koska $q_p^2 < 0$, määrää α_0 kierron suunnan; Jos $\alpha_0 > 0$, niin $-2q_p^2\alpha_0 > 0$, joten kierto tapahtuu positiiviseen suuntaan eli vastapäivään. Jos taas $\alpha_0 < 0$, niin $-2q_p^2\alpha_0 < 0$, joten kierto tapahtuu negatiiviseen suuntaan eli myötäpäivään.

Koska nyt tiedetään, mihin suuntaan kierto tapahtuu, voidaan todeta, että kulma θ saadaan lausekkeesta $\tan(\frac{\theta}{2}) = \frac{|u_0|}{\alpha_0}$, missä luvun α_0 merkki määrää kierron suunnan.



KUVA 6.3. Tapaus $q_0 = \alpha_0 + u_0$

□

Tarkastellaan vielä esimerkin avulla, kuinka lausetta 6.10 voidaan käyttää avaruuden $\mathbb{R}^3$ kiertojen tarkastelussa. Tutkitaan ensin, kuinka yksikkökvaterniot voidaan esittää sellaisessa muodossa, että niitä on helpompi soveltaa lauseeseen.

Olkoon $q_0 = x_1+ix_2+jx_3+kx_4$ yksikkökvaternio eli $N(q_0) = x_1^2+x_2^2+x_3^2+x_4^2 = 1$. Valitaan kulma θ siten, että $x_1 = \cos\frac{1}{2}\theta$. Tällöin

$$\sin^2\frac{1}{2}\theta = 1-\cos^2\frac{1}{2}\theta = x_1^2+x_2^2+x_3^2+x_4^2-x_1^2 = x_2^2+x_3^2+x_4^2.$$

Määritellään reaaliluvut x_2', x_3' ja x_4' siten, että $x_2 = x_2'\sin\frac{1}{2}\theta$, $x_3 = x_3'\sin\frac{1}{2}\theta$ ja $x_4 = x_4'\sin\frac{1}{2}\theta$. Tällaiset luvut löydetään aina, sillä $\sin\frac{1}{2}\theta$ on reaaliluku väliltä $[-1,1]$. Merkitään $u = ix_2'+jx_3'+kx_4'$. Nyt q_0 saadaan muotoon

$$\begin{aligned}
q_0 &= x_1+ix_2+jx_3+kx_4\\
&= \cos\frac{1}{2}\theta + ix_2'\sin\frac{1}{2}\theta + jx_3'\sin\frac{1}{2}\theta + kx_4'\sin\frac{1}{2}\theta\\
&= \cos\frac{1}{2}\theta + u\sin\frac{1}{2}\theta.
\end{aligned}$$

Jos $\sin\frac{1}{2}\theta = 0$, niin $q_0 = x_1 = \cos\frac{1}{2}\theta$. Oletetaan, että $\sin\frac{1}{2}\theta \neq 0$. Tällöin

$$\sin^2\frac{1}{2}\theta = x_2^2+x_3^2+x_4^2 = ((x_2')^2+(x_3')^2+(x_4')^2)\sin^2\frac{1}{2}\theta,$$

eli $(x_2')^2+(x_3')^2+(x_4')^2 = 1$, joten u on yksikkökvaternio. Jokainen yksikkökvaternio voidaan siis kirjoittaa muodossa

$$q_0 = \cos\frac{1}{2}\theta + u\sin\frac{1}{2}\theta,$$

missä u on imaginaarinen yksikkökvaternio. Tämä muoto helpottaa kiertojen tutkimista.

Esimerkki 6.14. Kierretään vektoria $q = ix_2+jx_3+kx_4 \in Im(\mathbb{H})$ vektorin $i+j$ suuntaisen akselin suhteen $90°$.

Olkoon $\theta = 90° = \frac{\pi}{2}$ ja $\overrightarrow{v} = i+j$. Vektorin $\overrightarrow{v}$ pituus on $\sqrt{2}$, ja $\cos\frac{1}{2}\theta = \cos\frac{\pi}{4} = \frac{1}{\sqrt{2}}$ ja $\sin\frac{1}{2}\theta = \sin\frac{\pi}{4} = \frac{1}{\sqrt{2}}$. Määritellään yksikkökvaternio q_0 siten, että

$$q_0 = \cos\frac{1}{2}\theta + \overrightarrow{u}\sin\frac{1}{2}\theta,$$

missä $\overrightarrow{u}$ on vektorin $\overrightarrow{v}$ suuntainen yksikkövektori, eli

$$\begin{aligned}
q_0 &= \cos\frac{1}{2}\theta + \overrightarrow{u}\sin\frac{1}{2}\theta = \cos\frac{\pi}{4} + \sin\frac{\pi}{4}\cdot\frac{1}{|\overrightarrow{v}|}\cdot\overrightarrow{v}\\
&= \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\cdot\frac{i+j}{\sqrt{2}} = \frac{1}{\sqrt{2}} + \frac{i+j}{2}\\
&= \frac{\sqrt{2}+i+j}{2}.
\end{aligned}$$

Nyt kvaternio q_0 on siis muotoa $\alpha_0 + u_0$, missä $\alpha_0 = \frac{\sqrt{2}}{2}$ ja $u_0 = \frac{i+j}{2}$ on vektorin $\overrightarrow{v} = i + j$ suuntainen kvaternio. Lisäksi

$$\frac{|u_0|}{\alpha_0} = \frac{\sqrt{(\frac{1}{2})^2 + (\frac{1}{2})^2}}{\frac{\sqrt{2}}{2}} = \frac{1}{\sqrt{2}} \cdot \frac{2}{\sqrt{2}} = 1,$$

eli kun $\theta = 90°$, niin $\tan\frac{\theta}{2} = \frac{|u_0|}{\alpha_0}$. Lauseen 6.10 mukaan 90 asteen kierto vektorin $i+j$ suuntaisen akselin suhteen saadaan nyt kuvauksen T_{q_0} avulla.

Koska q_0 on yksikkökvaternio, niin huomautuksen 2.10 nojalla

$$q_0^{-1} = \overline{q_0} = \frac{\sqrt{2} - i - j}{2}.$$

Nyt laskemalla saadaan

$$\begin{aligned}
T_{q_0}(q) = q_0 q q_0^{-1} &= \Big(\frac{\sqrt{2}+i+j}{2}\Big)(ix_2 + jx_3 + kx_4)\Big(\frac{\sqrt{2}-i-j}{2}\Big) \\
&= \Bigg(\Big(-\frac{1}{2}x_2 - \frac{1}{2}x_3\Big) + \Big(\frac{\sqrt{2}}{2}x_2 + \frac{1}{2}x_4\Big)i + \Big(\frac{\sqrt{2}}{2}x_3 - \frac{1}{2}x_4\Big)j \\
&\quad + \Big(\frac{\sqrt{2}}{2}x_4 + \frac{1}{2}x_3 - \frac{1}{2}x_2\Big)k\Bigg)\Big(\frac{\sqrt{2}-i-j}{2}\Big) \\
&= \Big(\frac{\sqrt{2}(-x_2 - x_3)}{4} + \frac{\sqrt{2}x_2 + x_4}{4} + \frac{\sqrt{2}x_3 + x_4}{4}\Big) \\
&\quad + \Big(-\frac{-x_2 - x_3}{4} + \frac{\sqrt{2}(\sqrt{2}x_2 + x_4)}{4} + \frac{\sqrt{2}x_4 + x_3 - x_2}{4}\Big)i \\
&\quad + \Big(-\frac{(-x_2 - x_3)}{4} + \frac{\sqrt{2}(\sqrt{2}x_3 - x_4)}{4} - \frac{\sqrt{2}x_4 + x_3 - x_2}{4}\Big)j \\
&\quad + \Big(-\frac{(\sqrt{2}x_2 + x_4)}{4} + \frac{\sqrt{2}x_3 - x_4}{4} + \frac{\sqrt{2}(\sqrt{2}x_4 + x_3 - x_2)}{4}\Big)k \\
&= \Big(\frac{2x_2 + 2x_3 + 2\sqrt{2}x_4}{4}\Big)i + \Big(\frac{2x_2 + 2x_3 - 2\sqrt{2}x_4}{4}\Big)j + \Big(\frac{-2\sqrt{2}x_2 + 2\sqrt{2}x_3}{4}\Big)k \\
&= \Big(\frac{1}{2}x_2 + \frac{1}{2}x_3 + \frac{\sqrt{2}}{2}x_4\Big)i + \Big(\frac{1}{2}x_2 + \frac{1}{2}x_3 - \frac{\sqrt{2}}{2}x_4\Big)j + \Big(-\frac{\sqrt{2}}{2}x_2 + \frac{\sqrt{2}}{2}x_3\Big)k.
\end{aligned}$$

Eli kun kvaterniota $q = ix_2 + jx_3 + kx_4$ kierretään 90° vektorin $i+j$ suuntaisen akselin suhteen, saadaan tulokseksi kvaternio

$$\Big(\frac{1}{2}x_2 + \frac{1}{2}x_3 + \frac{\sqrt{2}}{2}x_4\Big)i + \Big(\frac{1}{2}x_2 + \frac{1}{2}x_3 - \frac{\sqrt{2}}{2}x_4\Big)j + \Big(-\frac{\sqrt{2}}{2}x_2 + \frac{\sqrt{2}}{2}x_3\Big)k.$$

Nyt tiedämme, kuinka avaruuden $\mathbb{R}^3$ peilauksia ja kiertoja voidaan esittää lauseen 6.10 avulla. Varmistetaan vielä, että kaikki avaruuden $\mathbb{R}^3$ peilaukset ja kierrot saadaan esitettyä kvaternioiden ja kuvausten T_{q_0} avulla.

Koska voimme valita lauseen 6.10 kvaternion $q_0 = \alpha_0 + u_0$ mielivaltaisesti, niin voimme kiertää mitä tahansa imaginaarista kvaterniota q, eli mitä tahansa avaruuden $\mathbb{R}^3$ vektoria, minkä tahansa kvaternion u_0 suuntaisen akselin suhteen millä tahansa kulmalla, jolle $\tan(\frac{\theta}{2}) = \frac{|u_0|}{\alpha_0}$. Saamme siis näin esitettyä minkä tahansa avaruuden $\mathbb{R}^3$ kierron.

Määritellään vielä kuvaus $h : q_0 \to T_{q_0}$, joka liittää jokaisen yksikkökvaternion q_0 kuvaukseen $T_{q_0}(q) = q_0 q q_0^{-1}$. Kuvaukset T_{q_0} kuuluvat avaruuden $\mathbb{R}^3$ ortogonaaliseen ryhmään, joka koostuu avaruuden $\mathbb{R}^3$ lineaarisista isometrioista. Kuvaus h on siis kuvaus yksikkökvaternioiden joukosta avaruuden $\mathbb{R}^3$ ortogonaaliseen ryhmään. Osoitetaan, että h on homomorfismi.

LAUSE 6.15. *Kuvaus* $h : q_0 \to T_{q_0}$, *missä* $|q_0| = 1$, *eli toisin sanoen kuvaus* h *yksikkökvaternioiden joukosta avaruuden* $\mathbb{R}^3$ *ortogonaaliseen ryhmään, on ryhmähomomorfismi, jonka ydin on* $\{\pm 1\}$.

TODISTUS. Olkoot u ja v yksikkökvaternioita. Tällöin myös uv on yksikkökvaternio, ja siten $(uv)^{-1} = \overline{uv}$. Nyt

$$\begin{aligned} T_{uv}(q) &= (uv)q(uv)^{-1} = (uv)q(\overline{uv}) = u(vq\overline{v})\overline{u} \\ &= uT_v(q)\overline{u} = T_u(T_v(q)) = T_u \circ T_v(q). \end{aligned}$$

Kuvaus h on siis homomorfismi.

Kuvauksen h ydin muodostuu sellaisista yksikkökvaternioista q_0, joille kuvaus T_{q_0} on identtinen kuvaus, eli joille $T_{q_0}(q) = q_0 q q_0^{-1} = q$ kaikilla $q \in Im(\mathbb{H})$. Yhtälö $q_0 q q_0^{-1} = q$ saadaan muotoon $q_0 q = q q_0$. Lauseen 4.5 nojalla tämä pätee kaikille $q \in \mathbb{H}$ vain, kun $q_0 \in \mathbb{R}$. Tiedetään siis, että $q_0 \in \mathbb{R}$ ja $|q_0| = 1$, eli täytyy olla $q_0 = 1$ tai $q_0 = -1$. Kuvauksen h ydin on siis $\{\pm 1\}$. $\square$

Kuvaus h on siis homomorfismi, joten jos halutaan kiertää jotakin avaruuden $\mathbb{R}^3$ vektoria usean kerran peräkkäin eri akselien suhteen, sen voi tehdä kuvausten T_{q_0} yhdisteinä.

Voidaan myös osoittaa, että kuvaus h on surjektio (ks. esim [**10**] Theorem 16). Koska se on surjektio, niin kuvaukset T_{q_0} muodostavat koko avaruuden $\mathbb{R}^3$ ortogonaalisen ryhmän.

LUKU 7

Neljän neliön summa

Luvussa 2 osoitettiin, että jos kerrotaan keskenään kaksi sellaista lukua, jotka koostuvat neljän kokonaisluvun neliön summasta, saadaan tulokseksi taas luku, joka koostuu neljän kokonaisluvun neliön summasta. Tätä tulosta apuna käyttäen osoitamme nyt, että mikä tahansa kokonaisluku voidaan esittää neljän kokonaisluvun neliön summana.

Italialais-ranskalainen Joseph-Louis Lagrange toi ensimmäisenä tämän väitteen julki ja todisti sen jo vuonna 1772. Lause tunnetaankin yleisesti nimellä 'Lagrangen neljän neliön lause'. Lagrangen jälkeen muutama muukin matemaatikko on antanut oman todistuksensa lauseelle. Saksalainen Adolf Hurwitz määritteli vuonna 1896 *Hurwitzin kvaterniot*, ja niiden avulla antoi lauseelle puhtaasti algebrallisen todistuksen. Todistamme tässä luvussa lauseen käyttäen apuna Hurwitzin kvaternioita.

LAUSE 7.1. *Mikä tahansa kokonaisluku $n \geq 0$ voidaan esittää neljän kokonaisluvun neliön summana*

$$n = a_1^2 + a_2^2 + a_3^2 + a_4^2.$$

Osoitetaan ensin, että lause pätee mille tahansa alkuluvulle.

LAUSE 7.2. *Mikä tahansa alkulukuluku p voidaan esittää neljän kokonaisluvun neliön summana*

$$p = a_1^2 + a_2^2 + a_3^2 + a_4^2.$$

Lähdetään todistamaan lausetta *Hurwitzin kvaternioiden* avulla. Todistus seuraa pitkälti teosta [**3**].

MÄÄRITELMÄ 7.3. Kvaternio q on *Hurwitzin kvaternio*, jos sen reaalilukukomponentit ovat joko kaikki kokonaislukuja tai kaikki parittomien kokonaislukujen puolikkaita. *Hurwitzin kvaternioiden joukkoa* merkitään

$$\mathcal{H} = \{x_1 + ix_2 + jx_3 + kx_4 : x_1, x_2, x_3, x_4 \in \mathbb{Z} \text{ tai } x_1, x_2, x_3, x_4 \in \mathbb{Z} + \frac{1}{2}\}.$$

LEMMA 7.4. *Mikä tahansa Hurwitzin kvaternio q voidaan kirjoittaa muodossa*

$$q = a_1 r + a_2 i + a_3 j + a_4 k,$$

missä $r = \frac{1}{2}(1 + i + j + k) \in \mathcal{H}$ ja a_1, a_2, a_3 ja a_4 ovat kokonaislukuja.

TODISTUS. Olkoon $q = x_1 + ix_2 + jx_3 + kx_4 \in \mathcal{H}$. Nyt jos $a_1, a_2, a_3, a_4 \in \mathbb{Z}$, niin

$$\begin{aligned}
&a_1 r + a_2 i + a_3 j + a_4 k \\
&= \frac{1}{2}a_1 + \frac{1}{2}a_1 i + \frac{1}{2}a_1 j + \frac{1}{2}a_1 k + a_2 i + a_3 j + a_4 k \\
&= \frac{1}{2}a_1 + (\frac{1}{2}a_1 + a_2)i + (\frac{1}{2}a_1 + a_3)j + (\frac{1}{2}a_1 + a_4)k,
\end{aligned}$$

ja luvut a_1, a_2, a_3 ja a_4 voidaan valita siten, että $x_1 = \frac{1}{2}a_1$, $x_2 = \frac{1}{2}a_1 + a_2$, $x_3 = \frac{1}{2}a_1 + a_3$ ja $x_4 = \frac{1}{2}a_1 + a_4$. Siis kvaternio q voidaan kirjoittaa muodossa $q = a_1 r + a_2 i + a_3 j + a_4 k$, eli väite pätee. □

LEMMA 7.5. *Jos $q, p \in \mathcal{H}$, niin $\overline{q} \in \mathcal{H}$, $q + p \in \mathcal{H}$, $qp \in \mathcal{H}$ ja $N(q) \in \mathbb{Z}$.*

TODISTUS. Olkoot $q, p \in \mathcal{H}$. Selvästi $\overline{q} \in \mathcal{H}$ ja $q + p \in \mathcal{H}$. Osoitetaan, että $qp \in \mathcal{H}$. Olkoon $r = \frac{1}{2}(1 + i + j + k)$. Nyt lemman 7.4 nojalla q ja p voidaan esittää muodossa $q = a_1 r + a_2 i + a_3 j + a_4 k$ ja $p = b_1 r + b_2 i + b_3 j + b_4 k$, missä $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{Z}$. Tällöin

$$\begin{aligned}
qp &= (a_1 r + a_2 i + a_3 j + a_4 k)(b_1 r + b_2 i + b_3 j + b_4 k) \\
&= a_1 b_1 r^2 - a_2 b_2 - a_3 b_3 - a_4 b_4 \\
&+ (a_1 b_2 r + a_2 b_1 r + a_3 b_4 - a_4 b_3) i \\
&+ (a_1 b_3 r + a_3 b_1 r - a_2 b_4 + a_4 b_2) j \\
&+ (a_1 b_4 r + a_4 b_1 r + a_2 b_3 - a_3 b_2) k.
\end{aligned}$$

Nyt kvaternioiden laskusääntöjen nojalla

$$\begin{aligned}
ri &= -\frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j - \frac{1}{2}k, & ir &= -\frac{1}{2} + \frac{1}{2}i - \frac{1}{2}j + \frac{1}{2}k, \\
rj &= -\frac{1}{2} - \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k, & jr &= -\frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j - \frac{1}{2}k, \\
rk &= -\frac{1}{2} + \frac{1}{2}i - \frac{1}{2}j + \frac{1}{2}k, & kr &= -\frac{1}{2} - \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k, \\
r^2 &= -\frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k.
\end{aligned}$$

Siis $r^2, ri, ir, rj, jr, rk, kr \in \mathcal{H}$. Koska myös $zr \in \mathcal{H}$ kaikilla $z \in \mathbb{Z}$, niin nyt kaikki kvaternion qp komponentit ovat Hurwitzin kvaternioita, joten $qp \in \mathcal{H}$.

Osoitetaan vielä, että $N(q) \in \mathbb{Z}$. Nyt $N(q) = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Jos $x_i \in \mathbb{Z}$ kaikilla $i \in \{1, \ldots, 4\}$, niin selvästi $N(q) \in \mathbb{Z}$. Jos taas $x_i \in \mathbb{Z} + \frac{1}{2}$ kaikilla $i \in \{1, \ldots, 4\}$, niin $x_i^2 \in \mathbb{Z} + \frac{1}{4}$ kaikilla $i \in \{1, \ldots, 4\}$, ja

$$\begin{aligned}
x_1^2 + x_2^2 + x_3^2 + x_4^2 &= z_1 + \frac{1}{4} + z_2 + \frac{1}{4} + z_3 + \frac{1}{4} + z_4 + \frac{1}{4} \\
&= z_1 + z_2 + z_3 + z_4 + 1,
\end{aligned}$$

missä $z_i \in \mathbb{Z}$ kaikilla $i \in \{1, \ldots, 4\}$. Siis $N(q) \in \mathbb{Z}$. □

Kuten luvussa 2 määriteltiin, yksikkökvaterniot ovat kvaternioita, joille pätee $N(q) = 1$. Tutkitaan seuraavaksi, millaiset Hurwitzin kvaterniot ovat yksikkökvaternioita. Olkoon $q = x_1 + ix_2 + jx_3 + kx_4 \in \mathcal{H}$. Jos $x_1, x_2, x_3, x_4 \in \mathbb{Z}$, niin $N(q) = x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$ vain silloin, kun jokin luvuista $x_1^2, x_2^2, x_3^2, x_4^2$ on 1 ja muut nollia, eli jos jokin luvuista x_1, x_2, x_3, x_4 on 1 tai -1 ja muut nollia. Jos taas $x_1, x_2, x_3, x_4 \in \mathbb{Z} + \frac{1}{2}$, niin $N(q) = 1$ vain silloin, kun $x_1^2 = x_2^2 = x_3^2 = x_4^2 = \frac{1}{4}$ eli jos $x_1 = x_2 = x_3 = x_4 = \pm\frac{1}{2}$. Siis Hurwitzin kvaternioilla on 24 yksikkökvaterniota:

$$\pm 1, \quad \pm i, \quad \pm j, \quad \pm k, \quad \frac{1}{2}(\pm 1 \pm i \pm j \pm k).$$

MÄÄRITELMÄ 7.6. Olkoon q Hurwitzin kvaternio. Jos $\epsilon \in \mathcal{H}$ on mikä tahansa yksikkökvaternio, niin ϵq ja $q\epsilon$ ovat kvaternion q *liittolaisia*.

HUOMAUTUS 7.7. Koska Hurwitzin kvaternioiden tulo on Hurwitzin kvaternio, niin kaikki Hurwitzin kvaternion liittolaiset ovat myös Hurwitzin kvaternioita, ja koska $N(\epsilon) = 1$ kaikilla yksikkökvaternioilla ϵ, niin $N(\epsilon q) = N(\epsilon)N(q) = N(q)$.

LAUSE 7.8. *Jos q on Hurwitzin kvaternio, niin ainakin yhdellä sen liittolaisista on kokonaislukukomponentit. Jos q on pariton eli $N(q)$ on pariton, niin sillä on ainakin yksi liittolainen, jolla ei ole kokonaislukukomponentteja.*

TODISTUS. Kohta (1): Olkoon $q = x_1 + ix_2 + jx_3 + kx_4 \in \mathcal{H}$. Jos $x_1, x_2, x_3, x_4 \in \mathbb{Z}$, niin ainakin kvaternion q liittolaisella $1q = q$ on kokonaislukukomponentit. Jos taas $x_1, x_2, x_3, x_4 \in \mathbb{Z} + \frac{1}{2}$, niin valitsemalla merkit oikein voidaan merkitä

$$q = (a_1 + ia_2 + ja_3 + ka_4) + \frac{1}{2}(\pm 1 \pm i \pm j \pm k) = p + r,$$

missä $p = (a_1 + ia_2 + ja_3 + ka_4)$, a_1, a_2, a_3 ja a_4 ovat parillisia kokonaislukuja, ja $r = \frac{1}{2}(\pm 1 \pm i \pm j \pm k)$ on yksikkökvaternio. Nyt

$$q\overline{r} = (p + r)\overline{r} = p\overline{r} + r\overline{r}.$$

Koska kvaternion p kaikki komponentit ovat parillisia kokonaislukuja, niin kvaternioiden kertolaskusäännön nojalla kaikki kvaternion $p\overline{r}$ komponentit ovat kokonaislukuja. Koska r on yksikkökvaternio, niin $r\overline{r} = 1$. Siis kvaternion $q\overline{r}$ komponentit ovat kokonaislukuja. Koska $\overline{r}$ on yksikkökvaternio, niin $q\overline{r}$ on kvaternion q etsitty liittolainen.

Kohta (2): Olkoon $q = x_1 + ix_2 + jx_3 + kx_4 \in \mathcal{H}$ pariton, eli $N(q)$ on pariton. Jos $x_1, x_2, x_3, x_4 \in \mathbb{Z} + \frac{1}{2}$, niin $1q = q$ on kvaternion q haluttu liittolainen. Jos taas $x_1, x_2, x_3, x_4 \in \mathbb{Z}$, niin nyt voidaan taas merkitä

$$q = (a_1 + ia_2 + ja_3 + ka_4) + (b_1 + ib_2 + jb_3 + kb_4) = p + r,$$

missä $p = (a_1 + ia_2 + ja_3 + ka_4)$, a_1, a_2, a_3 ja a_4 ovat parillisia kokonaislukuja, ja $r = (b_1 + ib_2 + jb_3 + kb_4)$ siten, että jokainen b_1, b_2, b_3 ja b_4 on joko 0 tai 1. Koska nyt $N(q) = (a_1 + b_1)^2 + (a_2 + b_2)^2 + (a_3 + b_3)^2 + (a_4 + b_4)^2$ on pariton, niin luvuista b_1, b_2, b_3, b_4 joko yksi on 1 ja muut 0 tai yksi on 0 ja muut 1. Siis

$$r \in \{1,\ i,\ j,\ k,\ 1 + i + j,\ 1 + i + k,\ 1 + j + k,\ i + j + k\}.$$

Nyt taas millä tahansa kvaternion p liittolaisella on kokonaislukukompontentit, joten riittää osoittaa, että kvaterniolla r on liittolainen, jolla ei ole kokonaislukukomponentteja.

Olkoon $\epsilon = \frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k$. Nyt ϵ on yksikkökvaternio, ja kvaternioiden kertolaskusäännöön nojalla

$$\begin{aligned}
1\epsilon &= \frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k, & i\epsilon &= -\frac{1}{2} + \frac{1}{2}i - \frac{1}{2}j + \frac{1}{2}k \\
j\epsilon &= -\frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j - \frac{1}{2}k, & k\epsilon &= -\frac{1}{2} - \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k \\
(1 + i + j)\epsilon &= -\frac{1}{2} + \frac{3}{2}i + \frac{1}{2}j + \frac{1}{2}k, & (1 + i + k)\epsilon &= -\frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{3}{2}k \\
(1 + j + k)\epsilon &= -\frac{1}{2} + \frac{1}{2}i + \frac{3}{2}j + \frac{1}{2}k, & (i + j + k)\epsilon &= -\frac{3}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k.
\end{aligned}$$

Siis kvaterniolla $r\epsilon$ ei ole kokonaislukukomponentteja. Nyt $q\epsilon = (p+r)\epsilon = p\epsilon + r\epsilon$. Kvaterniolla $p\epsilon$ on kokonaislukukomponentit, mutta kvaterniolla $r\epsilon$ ei, joten kvaterniolla $q\epsilon$ ei ole kokonaislukukomponentteja. Koska ϵ on yksikkökvaternio, on $q\epsilon$ kvaternion q etsitty liittolainen. □

LAUSE 7.9. *Jos $q \in \mathcal{H}$ ja m on positiivinen kokonaisluku, niin on olemassa $p \in \mathcal{H}$ siten, että*

$$N(q - mp) < m^2.$$

TODISTUS. Jos $m = 1$ niin lause on selvä; valitaan $p = q$, jolloin $N(q - mp) = N(q - q) = 0 < 1$. Voidaan siis olettaa, että $m > 1$.

Kirjoitetaan kvaternio q lemman 7.4 muodossa $q = a_1r + a_2i + a_3j + a_4k$, missä a_1, a_2, a_3 ja a_4 ovat reaalilukuja. Olkoon p jokin Hurwitzin kvaternio. Myös p voidaan kirjoittaa muodossa $p = b_1r + b_2i + b_3j + b_4k$, missä b_1, b_2, b_3 ja b_4 ovat joitakin reaalilukuja. Tällöin

$$\begin{aligned}
q - mp &= (a_1 - mb_1)r + (a_2 - mb_2)i + (a_3 - mb_3)j + (a_4 - mb_4)k \\
&= \frac{1}{2}(a_1 - mb_1) + (\frac{1}{2}(a_1 - mb_1) + (a_2 - mb_2))i \\
&\quad + ((\frac{1}{2}(a_1 - mb_1) + (a_3 - mb_3))j + \frac{1}{2}((a_1 - mb_1) + (a_4 - mb_4))k \\
&= \frac{1}{2}(a_1 - mb_1) + \frac{1}{2}(a_1 - mb_1 + 2a_2 - 2mb_2)i \\
&\quad + \frac{1}{2}(a_1 - mb_1 + 2a_3 - 2mb_3)j + \frac{1}{2}(a_1 - mb_1 + 2a_4 - 2mb_4)k \\
&= \frac{1}{2}(a_1 - mb_1) + \frac{1}{2}(a_1 + 2a_2 - m(b_1 + 2b_2))i \\
&\quad + \frac{1}{2}(a_1 + 2a_3 - m(b_1 + 2b_3))j + \frac{1}{2}(a_1 + 2a_4 - m(b_1 + 2b_4))k.
\end{aligned}$$

Nyt kun valitaan (alempana selvitetään, miksi näin voidaan tehdä) b_1, b_2, b_3 ja b_4 siten, että

$$|a_1 - mb_1| \le \frac{1}{2}m,$$

$$|a_1 + 2a_2 - m(b_1 + 2b_2)| \le m,$$

$$|a_1 + 2a_3 - m(b_1 + 2b_3)| \le m,$$

ja

$$|a_1 + 2a_4 - m(b_1 + 2b_4)| \le m,$$

niin

$$\begin{aligned}
N(q - mp) &= \frac{1}{4}(a_1 - mb_1)^2 + \frac{1}{4}(a_1 + 2a_2 - m(b_1 + 2b_2))^2 \\
&\quad + \frac{1}{4}(a_1 + 2a_3 - m(b_1 + 2b_3))^2 + \frac{1}{4}(a_1 + 2a_4 - m(b_1 + 2b_4))^2 \\
&\le \frac{1}{16}m^2 + 3 \cdot \frac{1}{4}m^2 < m^2.
\end{aligned}$$

Varmistetaan vielä, että luvut b_1, b_2, b_3 ja b_4 voidaan valita niin, että epäyhtälöt pätevät. Koska $m > 0$, niin $|m| = m$. Ensimmäinen epäyhtälö saadaan muotoon

$$\begin{aligned} |a_1 - mb_1| &\leq \frac{1}{2}m \\ \Leftrightarrow \frac{|a_1 - mb_1|}{|m|} &\leq \frac{1}{2} \\ \Leftrightarrow |\frac{a_1}{m} - b_1| &\leq \frac{1}{2}. \end{aligned}$$

Epäyhtälö pätee, kun valitaan b_1 siten, että se on lähinnä lukua $\frac{a_1}{m}$ oleva kokonaisluku. Nyt kun luku b_1 on valittu, saadaan toinen epäyhtälö muotoon

$$\begin{aligned} |a_1 + 2a_2 - m(b_1 + 2b_2)| &\leq m \\ \Leftrightarrow \frac{|a_1 + 2a_2 - m(b_1 + 2b_2)|}{|m|} &\leq 1 \\ \Leftrightarrow |\frac{a_1}{m} - b_1 + 2(\frac{a_2}{m} - b_2)| &\leq 1 \\ \Leftrightarrow |\frac{a_1}{2m} - \frac{b_1}{2} + \frac{a_2}{m} - b_2| &\leq \frac{1}{2}. \end{aligned}$$

Epäyhtälö pätee, kun valitaan b_2 siten, että se on lähinnä lukua $\frac{a_1}{2m} - \frac{b_1}{2} + \frac{a_2}{m}$ oleva kokonaisluku. Vastaavasti kaksi viimeistä epäyhtälöä pätevät, kun valitaan b_3 siten, että se on lähinnä lukua $\frac{a_1}{2m} - \frac{b_1}{2} + \frac{a_3}{m}$ oleva kokonaisluku ja b_4 siten, että se on lähinnä lukua $\frac{a_1}{2m} - \frac{b_1}{2} + \frac{a_4}{m}$ oleva kokonaisluku.

Halutut luvut b_1, b_2, b_3 ja b_4 löydettiin, joten lause on nyt todistettu. □

LAUSE 7.10. *Jos $q, p \in \mathcal{H}$ ja $p \neq 0$, niin löytyy $r \in \mathcal{H}$ ja $s \in \mathcal{H}$ siten, että*

$$q = rp + s, \text{ ja } N(s) < N(p).$$

TODISTUS. Olkoot $q, p \in \mathcal{H}$. Määritellään $t = q\overline{p}$ ja $m = p\overline{p} = N(p)$. Valitaan Hurwitzin kvaternio r siten, että lauseen 7.9 tapaus pätee: $N(t - mr) < m^2$. Olkoon $s = q - rp$. Nyt

$$(q - rp)\overline{p} = q\overline{p} - rp\overline{p} = t - rm = t - mr$$

ja

$$N(q - rp)N(\overline{p}) = N((q - rp)\overline{p}) = N(t - mr) < m^2,$$

joten $N(q - rp) < m$. Nyt myös

$$N(s) = N(q - rp) < m = N(p),$$

joten lause pätee. □

MÄÄRITELMÄ 7.11. Olkoot $q, p, r \in \mathcal{H}$. Jos $q = pr$, niin p on kvaternion q *vasemmanpuoleinen jakaja* ja r on kvaternion q *oikeanpuoleinen jakaja*.

MÄÄRITELMÄ 7.12. Olkoon $S \subset \mathcal{H}$, $S \neq \emptyset$ joukko Hurwitzin kvaternioita, jotka kaikki eivät ole nollia. Joukko S on *oikeanpuoleinen ideaali*, jos

- $q, p \in S \Rightarrow q \pm p \in S$
- $q \in S \Rightarrow rq \in S$ kaikilla $r \in \mathcal{H}$.

Jos $q \in \mathcal{H}$ ja S on se oikeanpuoleinen ideaali, joka muodostuu kaikista kvaternion q vasemmanpuoleisista monikerroista rq, niin sanotaan, että S on oikeanpuoleinen pääideaali.

LAUSE 7.13. *Jokainen oikeanpuoleinen ideaali on oikeanpuoleinen pääideaali.*

TODISTUS. Koska S on oikeanpuoleinen ideaali, on siellä vähintään yksi kvaternio, joka ei ole 0. Olkoon $v \in S$ sellainen kvaternio, jolla on pienin positiivinen normi. Nyt siis jos $t \in S$ ja $N(t) < N(v)$, niin $t = 0$.

Olkoon $q \in S$. Määritelmän nojalla $q - pv \in S$ kaikilla $p \in \mathcal{H}$. Valitaan $r \in \mathcal{H}$ siten, että lauseen 7.10 tapaus pätee:

$$q = pv + r, \text{ ja } N(r) < N(v).$$

Koska $r = q - pv$, niin nyt $N(q - pv) < N(v)$, joten $q - pv = 0$, eli $q = pv$. Siis mikä tahansa $q \in S$ on muotoa $q = pv$, joten joukko S muodostuu kaikista kvaternion $v \in S$ vasemmanpuoleisista monikerroista, eli se on oikeanpuoleinen pääideaali. $\square$

MÄÄRITELMÄ 7.14. Olkoot $q, p \in \mathcal{H}$. Kvaternioilla q ja p on *suurin yhteinen oikeanpuoleinen jakaja* r, jos

- r on kvaternioiden q ja p oikeanpuoleinen jakaja
- Jokainen kvaternioiden q ja p oikeanpuoleinen jakaja on myös kvaternion r oikeanpuoleinen jakaja.

Merkitään $r = (q, p)_R$.

Vastaavasti määritellään *suurin yhteinen vasemmanpuoleinen jakaja.*

LAUSE 7.15. *Millä tahansa kahdella Hurwitzin kvaterniolla q ja p, joista ainakin toinen on erisuuri kuin 0, on (vasemmanpuoleista yksikkötekijää vaille) yksikäsitteinen suurin yhteinen oikeanpuoleinen jakaja r, joka voidaan esittää muodossa*

$$r = sq + tp,$$

missä $s, t \in \mathcal{H}$.

TODISTUS. Olkoot $q, p \in \mathcal{H}$. Olkoon S sellainen joukko, joka sisältää kaikki muotoa $sq + tp$ olevat kvaterniot, kun $s, t \in \mathcal{H}$. Koska $0 \in \mathcal{H}$ ja $1 \in \mathcal{H}$ niin $q \in S$ ja $p \in S$. Olkoot $v, w \in S$. Tällöin v ja w ovat muotoa $v = sq + tp$ ja $w = s'q + t'p$ joillakin $s, s', t, t' \in \mathcal{H}$. Nyt

$$v \pm w = (sq + tp) \pm (s'q + t'p) = (s \pm s')q + (t \pm t')p \in S$$

ja

$$av = a(sq + tp) = asq + atp \in S \text{ kaikilla } a \in \mathcal{H},$$

joten joukko S on oikeanpuoleinen ideaali, ja täten lauseen 7.13 nojalla oikeanpuoleinen pääideaali. Joukko S on siis muodostunut jonkin kvaternion $r \in \mathcal{H}$ kaikista moninkerroista λr, $\lambda \in \mathcal{H}$. Koska nyt $1r \in S$, niin $r \in S$, ja se voidaan esittää muodossa

$$r = sq + tp.$$

Koska $q, p \in S$, niin ne ovat muotoa $q = \lambda_1 r$ ja $p = \lambda_2 r$, eli r on niiden yhteinen oikeanpuoleinen jakaja.

Olkoon s kvaternioiden q ja p mikä tahansa yhteinen oikeanpuoleinen jakaja. Tällöin $q = s_1 s$ ja $p = s_2 s$ joillakin $s_1, s_2 \in \mathcal{H}$. Nyt $r = \lambda_1^{-1} q = \lambda_1^{-1} s_1 s$ ja $r = \lambda_2^{-1} p =$

$\lambda_2^{-1}s_2s$. Koska $\lambda_1^{-1}, \lambda_2^{-1} \in \mathcal{H}$, niin s on myös kvaternion r oikeanpuoleinen jakaja. Mikä tahansa kvaternioiden q ja p yhteinen oikeanpuoleinen jakaja on siis myös kvaternion r oikeanpuoleinen jakaja. Siis r on kvaternioiden q ja p suurin yhteinen oikeanpuoleinen jakaja.

Osoitetaan vielä yksikäsitteisyys. Olkoot nyt r ja r' kvaternioiden q ja p suurimmat yhteiset oikeanpuoleiset jakajat. Tällöin ne voidaan kirjoittaa muodossa $r = v'r'$ ja $r' = vr$, missä $v, v' \in \mathcal{H}$. Nyt $r = v'r' = v'vr$, joten $v'v = 1$. Koska $v'v = 1$, on $N(v'v) = 1$, eli $N(v')N(v) = 1$. Koska $N(v'), N(v) \in \mathbb{N}$, täytyy olla $N(v') = N(v) = 1$. Siis v ja v' ovat yksikkökvaternioita.

Suurin yhteinen oikeanpuoleinen jakaja on siis vasemmanpuoleista yksikkötekijää vaille yksikäsitteinen. □

LAUSE 7.16. *Olkoot $q \in \mathcal{H}$ ja $p = m$ on positiivinen kokonaisluku. Tällöin $(q,p)_R = 1$ jos ja vain jos* $\mathrm{syt}(N(q), N(p)) = 1$ *(eli yhtäpitävästi jos* $\mathrm{syt}(N(q), m) = 1$*).*

TODISTUS. Jos $(q,p)_R = 1$, niin $sq + tp = 1$ joillakin $s, t \in \mathcal{H}$. Nyt

$$\begin{aligned} N(s)N(q) &= N(sq) = N(1-tp) = N(1-mt) = (1-mt)(\overline{1-mt}) \\ &= (1-mt)(1-m\bar{t}) = 1 - m\bar{t} - mt + m^2N(t). \end{aligned}$$

Siis $N(s)N(q) = 1 + m(-\bar{t} - t + mN(t)) = 1 + mk$ jollakin $k \in \mathbb{Z}$, sillä $\bar{t} + t \in \mathbb{Z}$ ja $mN(t) \in \mathbb{Z}$. Tästä seuraa, että $N(s)N(q) - mk = 1$. Koska $\mathrm{syt}(N(q), m)$ jakaa sekä luvun $N(q)$ että luvun m, se jakaa myös luvun $N(s)N(q) - mk$ eli luvun 1. Koska $\mathrm{syt}(N(q), m) \in \mathbb{Z}$, niin $\mathrm{syt}(N(q), m) = 1$.

Koska $N(p) = m^2$, niin $\mathrm{syt}(N(q), N(p)) = 1$ ja $\mathrm{syt}(N(q), m) = 1$ ovat yhtäpitävät.

Jos taas $\mathrm{syt}(N(q), N(p)) = 1$ eli $\mathrm{syt}(N(q), m) = 1$, niin lauseen 7.15 nojalla on olemassa Hurwitzin kvaterniot s ja t siten, että

$$1 = sN(q) + tm.$$

Koska $N(q) = \bar{q}q$, saadaan yhtälö muotoon

$$1 = s\bar{q}q + tm.$$

Nyt $s \in \mathcal{H}$ ja $\bar{q} \in \mathcal{H}$, joten $s\bar{q} \in \mathcal{H}$. Siis lauseen 7.15 nojalla nyt $(q,m)_R = 1$, eli $(q,p)_R = 1$. □

MÄÄRITELMÄ 7.17. Olkoon $q \in \mathcal{H}$. Kvaternio q on *jaoton*, jos sen ainoat jakajat ovat yksikkökvaternioita tai sen liittolaisia.

HUOMAUTUS 7.18. Toisin sanoen kvaternio q on jaoton, jos ehdosta $q = st$ seuraa, että s tai t on yksikkökvaternio.

HUOMAUTUS 7.19. Selvästi kaikki jaottoman Hurwitzin kvaternion liittolaiset ovat jaottomia.

LAUSE 7.20. *Hurwitzin kvaternio q on jaoton jos ja vain jos sen normi $N(q)$ on alkuluku.*

TODISTUS. "⇐": Olkoon $N(q)$ alkuluku. Merkitään $q = st$, $s, t \in \mathcal{H}$. Nyt

$$N(q) = N(st) = N(s)N(t).$$

Koska $N(q)$ on alkuluku, niin täytyy olla $N(s) = 1$ tai $N(t) = 1$, eli s tai t on yksikkökvaternio, eli $q = st$ on jaoton.

Lauseen todistuksen toinen suunta tehdään seuraavan lauseen avulla:

LAUSE 7.21. *Alkuluku p ei voi olla jaoton kvaternio.*

TODISTUS. Olkoon p alkuluku. Koska $2 = (1+i)(1-i)$, ja $(1+i)$ ja $(1-i)$ eivät ole yksikkökvaternioita, niin 2 ei ole jaoton kvaternio. Voidaan siis olettaa, että p on pariton. Osoitetaan yksi aputulos:

APUTULOS 7.22. Jos p on pariton alkuluku, niin on olemassa $x, y \in \mathbb{Z}$ siten, että

$$1 + x^2 + y^2 = mp \text{ jollakin } m \in \mathbb{Z}, \text{ jolle } 0 < m < p$$

TODISTUS. Käydään läpi todistuksen idea. Määritellään joukot A ja B siten, että

$$A = \left\{ a^2 : 0 \leq a \leq \frac{p-1}{2} \right\}$$

ja

$$B = \left\{ -b^2 - 1 : 0 \leq b \leq \frac{p-1}{2} \right\}.$$

Olkoot $x_i, x_j \in A$. Tällöin $x_i = a_i^2$ ja $x_j = a_j^2$ joillakin $a_i, a_j \in \mathbb{Z}$, ja

$$x_1 - x_j = a_i^2 - a_j^2 = (a_i + a_j)(a_i - a_j).$$

Voidaan olettaa että $a_i \geq a_j$, jolloin $a_i - a_j \geq 0$. Nyt $(a_i + a_j), (a_i - a_j) \in [1, p-1]$. Nyt ei löydy sellaista lukua $n \in \mathbb{Z}$, jolle $x_i - x_j = np$, eli $(a_i + a_j)(a_i - a_j) = np$. Jos tällainen luku n löytyisi, niin luku n olisi jaollinen sekä luvulla $(a_i + a_j)$ että luvulla $(a_i - a_j)$, koska np on jaollinen näillä molemmilla ja p on alkuluku. Tällöin olisi $n = k(a_i + a_j)$ jollakin $k \in \mathbb{Z}$, jolloin yhtälö $(a_i + a_j)(a_i - a_j) = np$ saadaan muotoon $(a_i - a_j) = kp$. Tämä on kuitenkin mahdotonta, sillä $(a_i - a_j) < p$ ja koska $a_i - a_j \geq 0$, niin $k \geq 0$, joten $kp \geq p$. Luvuilla x_i ja x_j ei siis voi olla sama jakojäännös jaettaessa luvulla p.

Samoin jos $y_i, y_j \in B$, niin ei löydy lukua $l \in \mathbb{Z}$ siten, että $y_i - y_j = lp$, eli luvuilla y_i ja y_j ei voi olla sama jakojäännös jaettaessa luvulla p.

Koska molemmissa joukoissa A ja B on $\frac{p+1}{2}$ alkiota, $A \cap B = \emptyset$ ja luvulla p jaettaessa jakojäännöksiä on p kappaletta, niin täytyy olla

$$x_i^2 = mp + (-1 - y_j^2)$$

joillakin $x_i^2 \in A$, $-y_j^2 - 1 \in B$ ja $m \in \mathbb{Z}$, eli toisin sanoen

$$x_i^2 + y_j^2 + 1 = mp$$

jollain $m \in \mathbb{Z}$.

$\square$

Aputuloksen perusteella on olemassa $x, y \in \mathbb{Z}$ siten, että $1 + x^2 + y^2 = mp$ jollain m. Olkoon $q = 1 + ix + jy \in \mathcal{H}$. Nyt

$$N(q) = 1 + x^2 + y^2.$$

Aputuloksen perusteella siis $N(q) = mp$. Nyt $\text{syt}(N(q), p)) = \text{syt}(mp, p) = p > 1$, joten lauseen 7.16 nojalla kvaternioilla q ja p on suurin yhteinen oikeanpuoleinen jakaja r, joka ei ole yksikkökvaternio.

Olkoon $q = r_1 r$ ja $p = r_2 r$, $r_1, r_2 \in \mathcal{H}$. Nyt r_2 ei voi olla yksikkökvaternio, koska jos se olisi, niin myös r_2^{-1} olisi yksikkökvaternio, ja koska $r = pr_2^{-1}$, niin $q = r_1 r = r_1 p r_2^{-1}$, ja p jakaisi kaikki kvaternion $q = 1 + ix + jy$ koordinaatit, erityisesti komponentin 1, eli täytyisi olla $p = 1$. Siis $p = r_2 r$, ja kumpikaan r tai r_2 ei ole yksikkökvaternio, joten kvaternio p ei ole jaoton. □

Todistetaan seuraavaksi lauseen 7.20 toinen suunta:

"$\Rightarrow$": Olkoon q jaoton kvaternio ja p sellainen alkuluku, joka jakaa luvun $N(q)$. Lauseen 7.16 perusteella kvaternioilla p ja q on yhteinen oikeanpuoleinen jakaja r, joka ei ole yksikkökvaternio. Merkitään $q = r_1 r$, missä $r_1 \in \mathcal{H}$. Koska q on jaoton, on r_1 yksikkökvaternio, mistä seuraa, että myös r_1^{-1} on yksikkökvaternio, ja $r = qr_1^{-1}$ on kvaternion q liittolainen. Nyt

$$N(r) = N(qr_1^{-1}) = N(q).$$

Merkitään $p = r_2 r$, missä $r_2 \in \mathcal{H}$. Nyt

$$N(p) = p^2 = N(r_2)N(r) = N(r_2)N(q).$$

Koska p on alkuluku, niin $N(r_2) = 1$ tai $N(r_2) = p$.

Jos $N(r_2) = 1$, niin $p = r_2 r = r_2 r_1^{-1} q$ on kvaternioiden r ja q liittolainen, ja koska q on jaoton, niin tällöin myös p olisi jaoton kvaternio. Tämä on kuitenkin lauseen 7.21 nojalla mahdotonta. Jos taas $N(r_2) = p$, niin koska $p^2 = pp = N(r_2)N(q)$, niin myös $N(q) = p$, eli $N(q)$ on alkuluku.

□

Nyt edellisten tulosten avulla voidaan todistaa lause 7.2. Olkoon p alkuluku. Lauseen 7.21 nojalla kvaternio p ei voi olla jaoton, joten se voidaan kirjoittaa muodossa $p = qr$, missä $p = N(q) = N(r)$, ja $q, r \in \mathcal{H}$, ja kumpikaan q tai p ei ole yksikkökvaternio. Olkoon nyt $q = x_1 + ix_2 + jx_3 + kx_4$. Jos $x_1, x_2, x_3, x_4 \in \mathbb{Z}$, niin

$$p = N(q) = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

eli lause pätee. Jos taas $x_1, x_2, x_3, x_4 \notin \mathbb{Z}$, niin lauseen 7.8 nojalla löytyy q:n liittolainen q', jolla on kokonaislukukomponentit, merkitään $q' = x_1' + ix_2' + jx_3' + kx_4'$, $x_1', x_2', x_3', x_4' \in \mathbb{Z}$. Nyt koska $N(q) = N(q')$, niin

$$p = N(q') = (x_1')^2 + (x_2')^2 + (x_3')^2 + (x_4')^2,$$

eli mikä tahansa alkuluku voidaan esittää neljän kokonaisluvun neliön summana. Lause 7.2 on nyt todistettu.

Lause 2.11 sanoo, että jos kerrotaan keskenään kaksi sellaista lukua, jotka koostuvat neljän kokonaisluvun neliön summasta, saadaan tulokseksi taas luku, joka koostuu neljän kokonaisluvun neliön summasta. Toisin sanoen kaikilla $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z}$ pätee

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (z_1^2 + z_2^2 + z_3^2 + z_4^2)$$

joillakin $z_1, z_2, z_3, z_4 \in \mathbb{Z}$.

Tunnetusti jokainen kokonaisluku voidaan esittää yksikäsitteisesti alkulukujen tulona,

$$n = p_1 p_2 \cdots p_n,$$

missä p_i on alkuluku kaikilla $i \in \{1, \ldots, n\}$. Nyt jokainen alkuluku voidaan esittää neljän kokonaisluvun neliön summana ja jos kerrotaan keskenään kaksi sellaista lukua, jotka koostuvat neljän kokonaisluvun neliön summasta, on niiden tulo neljän kokonaisluvun neliön summa. Induktioperiaatteen nojalla jokainen kokonaisluku n voidaan esittää neljän kokonaisluvun neliön summana. Lause 7.1 on nyt siis todistettu.

LUKU 8

Oktoniot

Kvaternioiden löydyttyä matemaatikot alkoivat luonnollisesti tutkia seuraavia lukualueiden laajennuksia. Myöhemmin on selvinnyt, että 5-, 6- ja 7-ulotteisiin avaruuksiin ei voida määritellä kertolaskua, joka käyttäytyisi samalla tavalla kuin reaalilukujen kertolasku. Vuonna 1843 matemaatikko John Graves esitteli Hamiltonille kahdeksanulotteisia lukuja, oktaaveja. Löydös ei kuitenkaan ollut Hamiltonin mielestä merkittävä, sillä niiden kertolasku ei ollut kommutatiivisuuden lisäksi edes assosiatiivinen. Vuonna 1845 matemaatikko Arthur Cayley toi julkisuuteen samanlaiset kahdeksanulotteiset luvut, *oktoniot*, joita kutsutaan myös Cayleyn luvuiksi.

Tämän luvun tiedot on saatu pääasiassa teoksista [**1**], [**9**] ja [**11**].

Oktoniot ovat kahdeksanulotteisia lukuja, joissa on reaaliosan lisäksi seitsemän imaginaariosaa. Perusoktoniot ovat

$$\begin{aligned} 1 &= (1,0,0,0,0,0,0,0) \\ e_1 &= (0,1,0,0,0,0,0,0) \\ e_2 &= (0,0,1,0,0,0,0,0) \\ &\dots \\ e_7 &= (0,0,0,0,0,0,0,1). \end{aligned}$$

Oktoniot ovat muotoa

$$\begin{aligned} \alpha &= x_0 + e_1x_1 + e_2x_2 + e_3x_3 + e_4x_4 + e_5x_5 + e_6x_6 + e_7x_7 \\ &= x_0 + \sum_{i=1}^{7} e_ix_i, \end{aligned}$$

missä $x_1, x_2, \dots, x_7 \in \mathbb{R}$. Peruskvaterniot voidaan samaistaa perusoktonioiksi, eli

$$i = e_1, \qquad j = e_2, \quad \text{ja} \quad k = e_3.$$

Kuten kvaternioilla, myös oktonioilla jokaiselle perusoktoniolle (paitsi oktoniolle 1) pätee

$$e_1^2 = e_2^2 = \dots = e_7^2 = -1.$$

Oktonioiden joukko $\mathbb{O}$ on kahdeksanulotteinen avaruus varustettuna seuraavilla oktonioiden yhteen- ja kertolaskuilla:

Kahden oktonion yhteenlasku suoritetaan komponenteittain, eli

$$\alpha + \beta = (x_0 + \sum_{i=1}^{7} e_ix_i) + (y_0 + \sum_{i=1}^{7} e_iy_i) = (x_0 + y_0) + \sum_{i=1}^{7} e_i(x_i + y_i).$$

Perusoktonioiden kertolaskuille on määritelty omat laskusääntönsä, jotka esitetään seuraavassa taulukossa:

	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	e_2	$-e_3$	-1	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_3	e_2	$-e_1$	-1	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	-1	e_1	e_2	e_3
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	-1	$-e_3$	e_2
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	-1	$-e_1$
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	-1

TAULUKKO 1. Perusoktonioiden kertolasku

Taulukosta 1 nähdään, että peruskvaternioiden kertolaskulle pätevät seuraavat säännöt:

- antikommutatiivisuus:
$$e_ie_j = -e_je_i, \text{ kun } i \neq j,$$
- indeksien kasvattaminen yhdellä:
$$e_ie_j = e_k \Rightarrow e_{i+1}e_{j+1} = e_{k+1},$$
- indeksien kaksinkertaistaminen:
$$e_ie_j = e_k \Rightarrow e_{2i}e_{2j} = e_{2k}.$$

Kahdessa viimeisessä säännössä indeksit ovat modulo 7, eli $e_8 = e_1$, $e_9 = e_2$, jne.

Kuten kvaternioiden, myöskään oktonioiden kertolasku ei ole kommutatiivinen, eikä itse asiassa edes assosiatiivinen, sillä esimerkiksi

$$(e_1e_2)e_5 = e_3e_5 = -e_6 \neq e_6 = e_1(e_2e_5).$$

Laskusääntö kahden oktonion tulolle saadaan johdettua, kuten kvaternioillekin, käyttäen apuna perusoktonioiden kertolaskusääntöjä. Kertolaskusääntö saataisiin laskettua komponenteittain, mutta siitä tulisi hyvin pitkä lasku, joten tässä esitetään vain lopputulos:

$$\begin{aligned}
&(x_0 + e_1x_1 + e_2x_2 + e_3x_3 + e_4x_4 + e_5x_5 + e_6x_6 + e_7x_7)\cdot\\
&(y_0 + e_1y_1 + e_2y_2 + e_3y_3 + e_4y_4 + e_5y_5 + e_6y_6 + e_7y_7)\\
&= (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7)\\
&+ (x_0y_1 + x_1y_0 + x_2y_3 - x_3y_2 + x_4y_5 - x_5y_4 - x_6y_7 + x_7y_6)e_1\\
&+ (x_0y_2 + x_2y_0 - x_1y_3 + x_3y_1 + x_4y_6 - x_6y_4 + x_5y_7 - x_7y_5)e_2\\
&+ (x_0y_3 + x_3y_0 + x_1y_2 - x_2y_1 + x_4y_7 - x_7y_4 - x_5y_6 + x_6y_5)e_3\\
&+ (x_0y_4 + x_4y_0 - x_1y_5 + x_5y_1 - x_2y_6 + x_6y_2 - x_3y_7 + x_7y_3)e_4\\
&+ (x_0y_5 + x_5y_1 + x_1y_4 - x_4y_1 - x_2y_7 + x_7y_2 + x_3y_6 - x_6y_3)e_5\\
&+ (x_0y_6 + x_6y_0 + x_1y_7 - x_7y_1 + x_2y_4 - x_4y_2 - x_3y_5 + x_5y_3)e_6\\
&+ (x_0y_7 + x_7y_0 - x_1y_6 + x_6y_1 + x_2y_5 - x_5y_2 + x_3y_4 - x_4y_3)e_7
\end{aligned} \tag{8.1}$$

Huomataan, että oktonioiden kertolaskuja olisi työlästä laskea kertolaskusäännön avulla. Helpommalla päästään, kun huomataan, että jokainen oktonio voidaan esittää kahden kvaternion avulla.

Samalla tavalla kuin kompleksiluvut voidaan esittää reaalilukupareina $x_1 + ix_2 = (x_1, x_2)$ ja kvaterniot kompleksilukupareina $x_1+ix_2+jx_3+kx_4 = (x_1+ix_2, x_3+ix_4)$, voidaan oktoniot kirjoittaa kvaterniopareina:

$$\begin{aligned}\alpha &= x_0 + e_1x_1 + e_2x_2 + e_3x_3 + e_4x_4 + e_5x_5 + e_6x_6 + e_7x_7\\ &= x_0 + e_1x_1 + e_2x_2 + e_3x_3 + e_4x_4 - e_4e_1x_5 - e_4e_2x_6 - e_4e_3x_7\\ &= x_0 + e_1x_1 + e_2x_2 + e_3x_3 + e_4(x_4 + e_1(-x_5) + e_2(-x_6) + e_3(-x_7))\\ &= q + e_4p,\end{aligned}$$

missä $q = x_0 + e_1x_1 + e_2x_2 + e_3x_3 \in \mathbb{H}$ ja $p = x_4 + e_1(-x_5) + e_2(-x_6) + e_3(-x_7) \in \mathbb{H}$. Siis

$$\begin{aligned}&x_0 + e_1x_1 + e_2x_2 + e_3x_3 + e_4x_4 + e_5x_5 + e_6x_6 + e_7x_7\\ &\quad= (x_0 + ix_1 + jx_2 + kx_3, x_4 - ix_5 - jx_6 - kx_7).\end{aligned}$$

Kun oktoniot esitetään järjestettyinä pareina kvaternioista, niille määritellään summa

$$(q_1, q_2) + (p_1, p_2) = (q_1 + p_1, q_2 + p_2)$$

ja tulo

$$(q_1, q_2)(p_1, p_2) = (q_1p_1 - \overline{p_2}q_2, p_2q_1 + q_2\overline{p_1}).$$

Laskemalla (pitkillä, mutta suhteellisen helpoilla laskuilla) voitaisiin näyttää, että kaikki laskusäännöt, jotka on määritelty kvaternioparimuodoille, pätevät myös, jos ne laskettaisiin oktonioille suoraan komponenteittain.

Huomautus 8.1. Kvaternioiden joukko $\mathbb{H}$ voidaan tulkita oktonioiden joukon $\mathbb{O}$ osajoukoksi, kun samaistetaan kvaternio q oktonioksi $(q, 0)$.

Oktonioille voidaan määritellä konjugaatti ja normi:

Määritelmä 8.2. Olkoon $\alpha = (q_1, q_2)$ oktonio. Oktonion α

- *konjugaatti* on $\overline{\alpha} = (\overline{q_1}, -q_2)$
- *normi* on $N(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha = q_1\overline{q_1} + q_2\overline{q_2}$.

Huomataan, että

$$\begin{aligned}N(\alpha) &= q_1\overline{q_1} + q_2\overline{q_2} = N(q_1) + N(q_2)\\ &= x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_5^2 + x_7^2.\end{aligned}$$

Huomautus 8.3. Helposti nähdään, että jos $\alpha, \beta \in \mathbb{O}$, niin $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$, $\overline{\alpha\beta} = \overline{\beta}\ \overline{\alpha}$ ja $\overline{\overline{\alpha}} = \alpha$. Normille pätevät säännöt $N(\overline{\alpha}) = N(\alpha)$ ja $N(\alpha)N(\beta) = N(\alpha\beta)$.

Seuraava lause osoittaa, että oktonioiden joukko $\mathbb{O}$ on jakoalgebra, eli että jokaiselle $\alpha, \beta \in \mathbb{O}$ löytyy sellaiset yksikäsitteiset $\delta \in \mathbb{O}$ ja $\gamma \in \mathbb{O}$, joille $\delta\alpha = \beta$ ja $\alpha\gamma = \beta$.

Lause 8.4. *Olkoon $\alpha, \beta \in \mathbb{O}$. Tällöin yhtälöillä*

$$\delta\alpha = \beta \quad ja \quad \alpha\gamma = \beta$$

on yksikäsitteiset ratkaisut $\delta \in \mathbb{O}$ ja $\gamma \in \mathbb{O}$.

Todistus. Olkoot $\alpha = (q_1, q_2)$, $\beta = (p_1, p_2)$ ja $\delta = (r_1, r_2)$ oktonioita siten, että $\delta\alpha = \beta$. Nyt

$$\delta\alpha = (r_1, r_2)(q_1, q_2) = (r_1 q_1 - \overline{q_2} r_2, q_2 r_1 + r_2 \overline{q_1}).$$

Siis etsitään ratkaisua yhtälölle

$$(r_1 q_1 - \overline{q_2} r_2, q_2 r_1 + r_2 \overline{q_1}) = (p_1, p_2).$$

Tästä saamme kaksi yhtälöä:

$$r_1 q_1 - \overline{q_2} r_2 = p_1 \tag{8.2}$$

$$q_2 r_1 + r_2 \overline{q_1} = p_2. \tag{8.3}$$

Kun nyt kerrotaan yhtälöä (8.3) oikealta kvaterniolla q_1, saadaan

$$q_2 r_1 q_1 + r_2 \overline{q_1} q_1 = p_2 q_1.$$

Yhtälöstä (8.2) saadaan $r_1 q_1 = p_1 + \overline{q_2} r_2$. Sijoitetaan tämä edelliseen yhtälöön:

$$\begin{aligned} & q_2(p_1 + \overline{q_2} r_2) + r_2 \overline{q_1} q_1 = p_2 q_1 \\ \Leftrightarrow\ & q_2 p_1 + q_2 \overline{q_2} r_2 + r_2 \overline{q_1} q_1 = p_2 q_1 \\ \Leftrightarrow\ & (q_2 \overline{q_2} + \overline{q_1} q_1) r_2 = p_2 q_1 - q_2 p_1 \\ \Leftrightarrow\ & (N(q_1) + N(q_2)) r_2 = p_2 q_1 - q_2 p_1 \\ \Leftrightarrow\ & N(\alpha) r_2 = p_2 q_1 - q_2 p_1. \qquad (8.4) \end{aligned}$$

Samalla tavoin kun kerrotaan yhtälöä (8.2) oikealta kvaterniolla $\overline{q_1}$, saadaan

$$r_1 q_1 \overline{q_1} - \overline{q_2} r_2 \overline{q_1} = p_1 \overline{q_1}.$$

Yhtälöstä (8.3) saadaan $r_2 \overline{q_1} = p_2 - q_2 r_1$. Sijoitetaan tämä edelliseen yhtälöön:

$$\begin{aligned} & r_1 q_1 \overline{q_1} - \overline{q_2}(p_2 - q_2 r_1) = p_1 \overline{q_1} \\ \Leftrightarrow\ & r_1 q_1 \overline{q_1} - \overline{q_2} p_2 + \overline{q_2} q_2 r_1 = p_1 \overline{q_1} \\ \Leftrightarrow\ & r_1 (q_1 \overline{q_1} + \overline{q_2} q_2) = p_1 \overline{q_1} + \overline{q_2} p_2 \\ \Leftrightarrow\ & r_1 (N(q_1) + N(q_2) = p_1 \overline{q_1} + \overline{q_2} p_2 \\ \Leftrightarrow\ & r_1 N(\alpha) = p_1 \overline{q_1} + \overline{q_2} p_2 \qquad (8.5) \end{aligned}$$

Yhtälöistä (8.4) ja (8.5) saadaan

$$r_1 = N(\alpha)^{-1}(p_1 \overline{q_1} + \overline{q_2} p_2) \quad \text{ja} \quad r_2 = N(\alpha)^{-1}(p_2 q_1 - q_2 p_1).$$

Siis

$$\begin{aligned} \delta &= (r_1, r_2) \\ &= N(\alpha)^{-1}(p_1 \overline{q_1} + \overline{q_2} p_2, p_2 q_1 - q_2 p_1) \\ &= N(\alpha)^{-1} \beta \overline{\alpha}, \end{aligned}$$

joten $\delta \in \mathbb{O}$ on yksikäsitteinen.

Koska yhtälö $\alpha\gamma = \beta$ on yhtäpitävä sen kanssa, että $\overline{\alpha\gamma} = \overline{\beta}$, eli että $\overline{\gamma}\,\overline{\alpha} = \overline{\beta}$, niin koska $\overline{\alpha}, \overline{\beta} \in \mathbb{O}$, on yhtälöllä $\alpha\gamma = \beta$ on yksikäsitteinen ratkaisu $\gamma = N(\alpha)^{-1}\overline{\alpha}\beta$. $\square$

Oktonioiden joukko on siis jakoalgebra. Koska oktonioiden kertolasku ei ole assosiatiivinen, eivät oktoniot muodosta ryhmää.

Luvussa 2 osoitettiin kvaternioiden avulla, että jos kerrotaan keskenään kaksi sellaista lukua, jotka koostuvat neljän kokonaisluvun neliön summasta, saadaan tulokseksi luku, joka koostuu taas neljän kokonaisluvun neliön summasta. Kompleksilukujen avulla voisimme osoittaa, että että jos kerrotaan keskenään kaksi sellaista lukua, jotka koostuvat kahden kokonaisluvun neliön summasta, saadaan tulokseksi luku, joka koostuu taas kahden kokonaisluvun neliön summasta. Oktonioiden avulla voimme osoittaa saman luvulle, joka koostuu kahden kahdeksan kokonaisluvun neliön summan tulosta:

Lause 8.5. *Jokaiselle* $x_1, \ldots, x_8, y_1, \ldots, y_8 \in \mathbb{Z}$ *pätee*

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2 + y_7^2 + y_8^2) \\ = (z_1^2 + z_2^2 + z_3^2 + z_4^2 + z_5^2 + z_6^2 + z_7^2 + z_8^2)\end{aligned}$$

joillakin $z_1, \ldots, z_8 \in \mathbb{Z}$

Todistus. Lauseen todistus menee vastaavasti kuin lauseen 2.11 todistus: Jos

$$\alpha = x_1 + e_1x_2 + e_2x_3 + e_3x_4 + e_4x_5 + e_5x_6 + e_6x_7 + e_7x_8$$

ja

$$\beta = y_1 + e_1y_2 + e_2y_3 + e_3y_4 + e_4y_5 + e_5y_6 + e_6y_7 + e_7y_8,$$

niin

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2 + y_7^2 + y_8^2) \\ = N(\alpha)N(\beta).\end{aligned}$$

Koska oktonioille pätee $N(\alpha)N(\beta) = N(\alpha\beta)$, niin

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2 + y_7^2 + y_8^2) \\ = (z_1^2 + z_2^2 + z_3^2 + z_4^2 + z_5^2 + z_6^2 + z_7^2 + z_8^2),\end{aligned}$$

kun luvut z_i ovat yhtälön (8.1) muotoa. □

Tämän lauseen todisti tanskalainen C.P. Degen jo vuonna 1818. Myöhemmin, vuonna 1843 John Thomas Graves ja vuonna 1845 Arthur Cayley, todistivat lauseen oktonioiden avulla. Nykyään tiedetään, että lause

$$\begin{aligned}(x_1^2 + x_2^2 + \ldots + x_n^2)(y_1^2 + y_2^2 + \ldots + y_n^2) \\ = z_1^2 + z_2^2 + \ldots + z_n^2\end{aligned}$$

pätee kokonaisluvuille vain, kun $n \in \{1, 2, 4, 8\}$. Tämän osoitti Adolf Hurwitz 1800-luvun lopulla. Lause on itse asiassa yhtäpitävää sen kanssa, että luvun kertolasku on yhteensopiva normin kanssa. Hamilton etsi kompleksiluvuista seuraavaa lukulaajennusta, jolle tämä pätee, ja nykyään siis tiedetään, että tällaisia lukualueita ovat vain reaaliluvut $\mathbb{R}$, kompleksiluvut $\mathbb{C}$, kvaterniot $\mathbb{H}$ ja oktoniot $\mathbb{O}$.

Kirjallisuutta

[1] Coppel, W.A.: *Number Theory*, Springer 2009.
[2] Ebbinghaus, H.-D. ym.: *Numbers*, Springer, 1990.
[3] Hardy, G.H. & Wright, E.M.: *Theory of Numbers*, Oxford, 2008.
[4] Lehrbäck, Juha & Parkkonen, Jouni: *Lukualueet*, Luentomuistiinpanoja, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, 2009.
[5] Parkkonen, Jouni: *Algebra*, Luentomuistiinpanoja, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, 2007.
[6] Polvinen, Heikki: *Kompleksiluvut ja kvaterniot kiertoina*, Pro gradu -tutkielma, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, Syksy 2012.
[7] Purmonen, Veikko T.: *Lineaarinen algebra ja geometria 1*, Luentomuistiinpanoja, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, 2008.
[8] Purmonen, Veikko T.: *Lineaarinen algebra ja geometria 2*, Luentomuistiinpanoja, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, 2008.
[9] Stillwell, John: *Mathematics and Its History*, Springer, 2010.
[10] Toth, G.: *Glimpses of Algebra and Geometry*, Springer, 1998.
[11] van der Waerden, B.L.: *A History of Algebra*, Springer-Verlag, 1985.