Tampereen yliopisto

Noona Suomalainen

EUKLIDISET ALUEET

Informaatioteknologian ja viestinnän tiedekunta
Pro gradu -tutkielma
Kesäkuu 2024

Tiivistelmä

Noona Suomalainen: Euklidiset alueet
Pro gradu -tutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Kesäkuu 2024

Tässä tutkielmassa syvennytään yhteen abstraktin algebran keskeiseen osa-alueeseen: rengasteoriaan, erityisesti euklidisten alueiden käsitteeseen. Tutkielma koostuu neljästä pääluvusta, joista jokainen rakentaa perustan seuraaville ja laajentaa käsitteitä yhä syvemmälle.

Ensimmäisessä luvussa käsitellään rengasteorian peruskäsitteitä ja rakenteita. Luvussa esitellään ryhmien ja renkaiden määritelmät, josta edetään kokonaisalueiden, kuntien, ideaalien ja polynomirenkaiden käsitteisiin.

Toisessa luvussa keskitytään tutkielman pääaiheeseen eli euklidisiin alueisiin. Luvussa esitellään euklidisen alueen käsite ja sen astefunktion ominaisuudet. Näytetään, että euklidisella alueella on ainakin yksi universaali sivutekijä ja että kuntakertoiminen polynomirengas on euklidinen alue. Lisäksi tarkastellaan Gaussin kokonaislukuja ja osoitetaan, että ne muodostavat euklidisen alueen sopivalla astefunktiolla varustettuna. Luvun lopussa esitellään eukleideen algoritmin, joka on tunnettu menetelmä suurimman yhteisen tekijän laskemiseen.

Kolmannessa luvussa käsitellään euklidisen alueen yleistyksiä ja laajennetaan tietämystä euklidisuudesta sekä siihen liittyvästä terminologiasta.

Viimeisessä luvussa tarkastellaan pääideaalialuetta, joka ei ole euklidinen alue. Osoitetaan, että vaikka jokainen euklidinen alue on pääideaalialue, sama ei päde yleisesti toisinpäin.

Avainsanat: rengas, kokonaisalue, pääideaalialue, euklidinen alue

Sisällys

Johdanto

Kiinnostukseni tämän tutkielman aiheeseen juontaa juurensa vuonna 2022 yliopisto-opintojen aikana suorittamaani Renkaat ja kunnat -kurssiin. Kurssin aikana pääsin tutustumaan rengasteoriaan ja renkaiden ominaisuuksiin. Rengasteoria tarjoaa erinomaisen mahdollisuuden ymmärtää syvällisesti algebrallisia rakenteita ja niiden sovelluksia. Rengasteoria mahdollistaa myös työkaluja erilaisten matemaattisten ongelmien ratkaisemiseen ja sitä voi soveltaa moniin matemaattisiin ongelmiin.

Rengas on siis yksi algebran peruskäsitteistä ja se esiintyy eri tilanteissa matematiikassa. Mielenkiintoinen yksityiskohta rengasteoriassa on, että se ei rajoitu vain matematiikkaan. Sitä voidaankin hyödyntää myös matematiikan ulkopuolella esimerkiksi koodauksessa, muun muassa, kun käsitellään algebrallisia rakenteita, ja virheenkorjaavia koodeja, kuten BCH-koodit, jotka käyttävät polynomirenkaita tietojen tarkkuuden varmistamiseksi ja virheiden korjaamiseksi tietoliikenteessä. Näihin sovelluksiin ei kuitenkaan paneuduta tässä tutkielmassa. Voidaan kuitenkin todeta, että rengasteoria on keskeinen työkalu teoreettisessa ja soveltavassa matematiikassa, ja sen ymmärtäminen avaa ovia tärkeisiin ja käytännöllisiin sovelluksiin.

Rengasteoria on abstraktin algebran osa-alue, joka keskittyy algebrallisten rakenteiden tutkimiseen ja ominaisuuksien ymmärtämiseen. Rengasteoria on kehittynyt vähitellen 1800-luvulta nykypäivään saakka, ja sen kehitys on saanut vaikutteita monista eri matemaattisista suuntauksista ja kehityskuluista. Esimerkiksi tässä tutkielmassa myöhemmin esitettävät teoreemat ovat saksalaisten matemaatikkojen Carl Friedrich Gaussin ja Richard Dedekindin aikaansaannoksia. Dedekind muun muassa määritteli ideaalin ja modulin käsitteen. He ovat olleet merkittävästi osana vaikuttamassa rengasteorian kehityksessä.

Yksi rengasteorian osa-alue on euklidiset alueet, johon tässä tutkielmassa keskitytään. Euklidisten alueiden ominaisuuksien ymmärtäminen tarjoaa välineitä monenlaisten abstraktin algebran tulosten muotoiluun ja todistamiseen. Rengas on siis algebrallinen rakenne, joka koostuu joukosta, jossa on määritelty kaksi laskutoimitusta: yhteenlasku ja kertolasku, joille on asetettu tiettyjä ominaisuuksia. Yksi tavoitteista on ymmärtää ja luokitella erilaisia renkaiden tyyppejä niiden ominaisuuksien perusteella. Euklidiset alueet ovat renkaita, jotka on varustettu astefunktiolla, mikä toteuttaa jakoalgoritmin. Yleisesti euklidiset alueet määritellään myös kokonaisalueiksi. Kokonaisalue on vaihdannainen rengas, joka ei sisällä nollajakajia. Tässä tutkielmassa tullaan kuitenkin myös yleistämään ja laajentamaan euklidisen alueen

määritelmää. Euklidisten alueiden teoria on saanut paljon vaikutteita algebrallisesta lukuteoriasta.

Tämän tutkielman tavoitteena on tutkia syvällisesti rengasteoriaa ja euklidisten alueiden ominaisuuksia, rakennetta ja sovelluksia rengasteoriassa. Aluksi käsitellään rengasteorian perustavanlaatuisia käsitteitä, kuten renkaan, kokonaisalueen ja kunnan määritelmät, josta edetään tarkastelemaan pääideaalialueiden ja polynomirenkaiden rakenteita ja ominaisuuksia, jotka ovat oleellisia, kun siirrytään kohti monimutkaisempia rengasteoreettisia rakenteita. Kun peruskäsitteet ovat hallussa, tutkielmassa siirrytään tarkemmin euklidisten alueiden tutkimukseen. Tutkielmassa Käsitellään myös euklidisen alueen yleistyksiä, jotta voidaan laajentaa ymmärrystä euklidisuudesta ja siihen liittyvästä terminologiasta. Tavoitteena on tarjota kattava ymmärrys rengasteorian ja euklidisten alueiden keskeisistä ominaisuuksista, sekä ymmärtää paremmin, miten rengasteoria voi auttaa ratkaisemaan monimutkaisia matemaattisia ongelmia. Toivon, että tämä tutkielma ei ainoastaan syventäisi omaa ymmärrystäni aiheesta, vaan myös innostaisi lukijoita tutkimaan lisää rengasteorian kiehtovaa maailmaa.

1 Rengasteoriaa

Tässä luvussa käsitellään yleisesti rengasteoriaa. Ensimmäiseksi esitellään ryhmän ja renkaan käsitteet, josta edetään loogisessa järjestyksessä kokonaisalueisiin, kuntiin, ideaaleihin sekä polynomirenkaisiin. Osoitetaan muun muassa, että vaihdannainen rengas on kokonaisalue supistussäännön toteutuessa ja että jokainen kunta on kokonaisalue. Luvun päälähteenä on käytetty Joseph J. Rotmanin teosta A First Course in Abstract Algebra [5] sekä Kerkko Luoston laatimaa luentomonistetta Renkaat ja kunnat [2].

1.1 Ryhmä ja rengas

Määritelmä 1.1. *Ryhmä* on epätyhjä joukko A, joka on varustettu laskutoimituksella $\circ$ siten, että se toteuttaa seuraavat ominaisuudet:

1. (*liitännäisyys*) jokaisella $a, b, c \in A$ pätee $a \circ (b \circ c) = (a \circ b) \circ c$,
2. (*neutraalialkio*) on olemassa sellainen $e \in A$, että $e \circ a = a \circ e = a$, jokaisella $a \in A$,
3. (*käänteisalkio*) jokaiselle $a \in A$ on olemassa sellainen alkio $a^{-1} \in A$, että $a \circ a^{-1} = a^{-1} \circ a = e$, missä e on laskutoimituksen neutraalialkio.

Ryhmää sanotaan *Abelin ryhmäksi*, jos se toteuttaa kolmen edellä olevan ominaisuuden lisäksi *vaihdannaisuuden* $a \circ b = b \circ a$ kaikilla $a, b \in A$.

Määritelmä 1.2. Kahden laskutoimituksen rakenne $(R, +, \cdot)$ on *rengas*, jos seuraavat ehdot toteutuvat:

1. $(R,+)$ on Abelin ryhmä,
2. kertolasku $\cdot$ on liitännäinen,
3. kertolaskulla $\cdot$ on neutraalialkio,

4. yhteen- ja kertolaskut osittelevat: kaikilla $x,y,z \in R$ pätevät

   - $(x+y)\cdot z = xz + yz$ ja
   - $x \cdot (y+z) = xy + xz$.

Rengasta voidaan kutsua *vaihdannaiseksi renkaaksi*, jos lisäksi kertolasku $\cdot$ on vaihdannainen: $xy = yx$ kaikilla $x,\ y \in R$.

Määritelmä 1.3. Vaihdannaisen renkaan $(R, +, \cdot)$ alkiota u kutsutaan *yksiköksi*, jos u jakaa *ykkösalkion* 1. Siis $u \mid 1$.

Huomautus. Jos renkaassa on yksikkö, sitä kutsutaan yleisesti *yksiölliseksi renkaaksi*. Tässä tutkielmassa renkaan ykkösalkio on aina yksikkö. Tätä ei mainita määrittelyissä erikseen.

Määritelmä 1.4. (Alirengaskriteerit) Rengas $(S, +, \cdot)$ on renkaan $(R, +, \cdot)$ *alirengas*, jos

1. renkaan R ykkösalkio $1_R \in S$,
2. $a - b \in S$, kun $a,b \in S$ ja
3. $ab \in S$, kun $a,b \in S$.

Jos siis $S \subseteq R$ toteuttaa edellä olevat ehdot, niin S on renkaan R alirengas, missä renkaan S laskutoimitukset + ja $\cdot$ ovat periytyneet renkaasta R.

1.2 Kokonaisalue

Määritelmä 1.5. Vaihdannainen rengas $(R, +, \cdot)$ on *kokonaisalue*, mikäli *supistussääntö* toteutuu:

$$\text{Jos } ab = ac \text{ ja } a \neq 0, \text{ niin } b = c \text{ kaikilla } a,b,c \in R.$$

Toisin sanoen vaihdannainen rengas R on kokonaisalue, jos se ei sisällä nollajakajia.

Määritelmä 1.6. Sanotaan, että vaihdannaisessa renkaassa R on voimassa *tulon nollasääntö*, jos kaikille $a,b \in R$ pätee $ab = 0$, jos ja vain jos $a = 0$ tai $b = 0$.

Määritelmä 1.7. Renkaan R alkiota x, $x \neq 0$ kutsutaan *nollajakajaksi*, jos on olemassa sellainen $y \in R$, $y \neq 0$, että $xy = 0$.

Lause 1.8. *Olkoon R vaihdannainen rengas. Tällöin R on kokonaisalue, jos ja vain jos sen kertolasku toteuttaa tulon nollasäännön.*

Todistus. Oletetaan, että R on kokonaisalue ja $ab = 0$, $a \neq 0$. Tällöin saadaan $ab = a \cdot 0$, josta supistussäännön nojalla seuraa että $b = 0$.

Oletetaan, sitten että R on vaihdannainen rengas ja että tulon nollasääntö on voimassa. Olkoot $a,b,c \in R$ ja $ab = ac$, missä $a \neq 0$. Osoitetaan nyt, että $b = c$ pätee:

$$ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow a(b - c) = 0.$$

Koska edelleen $a \neq 0$, niin tulon nollasäännön nojalla on oltava $b - c = 0$, joten $b = c$. □

1.3 Kunta

Määritelmä 1.9. Kahden laskutoimituksen rakenne $(K, +, \cdot)$ on *kunta*, jos

1. $(K,+)$ on Abelin ryhmä,
2. $(K^*,\cdot)$ on Abelin ryhmä, missä $K^* = K \setminus \{0\}$,
3. (*osittelulait* pätevät) kaikilla $x,y,z \in K$
   - $(x + y) \cdot z = xz + yz$ ja
   - $x \cdot (y + z) = xy + xz$.

Lause 1.10. *Jokainen kunta on kokonaisalue.*

Todistus. Tiedetään, että jokainen kunta on vaihannainen rengas, joten riittää osoittaa, että kunnassa pätee supistussääntö.

Oletetaan, että kunnan alkioille a, b ja c pätee $ab = ac$ ja $a \neq 0$. Jokaisella kunnan nollasta poikkeavalla alkiolla on käänteisalkio. Kertomalla puolittain alkion a käänteisalkiolla a^{-1} saadaan:

$$ab = ac \Leftrightarrow a^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot c \Leftrightarrow b = c.$$

□

Huomautus. Edellisen kohdan tulos ei toimi käänteisesti. Esimerkiksi $\mathbb{Z}$ on kokonaisalue, mutta ei kunta.

Jokainen kunta on siis kokonaisalue. Lisäksi jokainen kunnan alirengas on aina kokonaisalue. Itseasiassa jokainen kokonaisalue R voidaan laajentaa kunnaksi konstruoimalla kokonaisalueen R *osamääräkunta*. Tällaista kuntaa K kutsutaan renkaan R *jakokunnaksi*. Konstruktiossa liitetään joukkoon R sen nollasta poikkeavien alkioiden käänteisalkiot.

Määritelmä 1.11. Jokaista kokonaisaluetta R vastaa sellainen kunta K, että R on kunnan alirengas. Lisäksi jokainen $a \in K$ voidaan esittää muodossa $a = bc^{-1}$, missä $b \neq 0$ ja $b, c \in R$. Tällaista kuntaa K kutsutaan renkaan R *jakokunnaksi*.

1.4 Pääideaalialueet

Määritelmä 1.12. Olkoon R vaihdannainen rengas. Epätyhjää joukkoa $I \subseteq R$ sanotaan renkaan *ideaaliksi*, jos

1. $0_R \in I$,
2. $a + b \in I$ kaikilla a,$b \in I$,
3. $ar \in I$ kaikilla $a \in I$ ja $r \in R$.

Jos ideaali $I \neq R$, niin I:tä kutsutaan *aidoksi ideaaliksi*.

Määritelmä 1.13. Yhden alkion virittämää ideaalia kutsutaan *pääideaaliksi*. Pääideaali esitetään usein muodossa $I = \langle a \rangle = \{ra \mid r \in R\}$, kun $a \in R$. Jos vaihdannaisen renkaan jokainen ideaali on pääideaali, niin on rengas *pääideaalialue*.

Esimerkki 1.14. Itseasiassa ideaaleiksi kelpaavat ainoastaan renkaan aliryhmät. Kaikki kokonaislukurenkaan aliryhmät ovat muotoa $n\mathbb{Z} = \langle n \rangle$, missä n on jokin kokonaisluku. Näin ollen $(\mathbb{Z}, +, \cdot)$ on pääideaalialue.

1.5 Polynomirengas

Polynomit ovat olennainen osa renkaiden tutkimuksessa. Tässä luvussa käsitellään polynomeja ja niiden muodostamia renkaita. Renkaaseen R littyvien polynomien kokoelmaa kutsutaan *polynomirenkaaksi* $R[x]$. Tässä luvussa osoitetaan jakoalgoritmin polynomirenkaille ja, että jokainen kuntakeroiminen polynomirengas $K[x]$ on pääideaalialue.

Määritelmä 1.15. Olkoon R rengas. Renkaan R polynomi $f(x)$ on summa

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

missä $a_i \in R$. Symboli x ei ole muuttuja vaan sen potenssit ilmaisevat kertoimensa paikan. Joukon R alkioita a_i sanotaan polynomin $f(x)$ kertoimiksi.

Huomautus. Jos polynomin $f(x)$ kaikki kertoimet a_i ovat nollia, niin polynomia sanotaan *nollapolynomiksi*. Tällöin merkitään $f(x) = 0$.

Määritelmä 1.16. Määritellään polynomirenkaan $R[x]$ yhteen- ja kertolaskut seuraavasti:

$$(a_0,a_1,a_2,\dots) + (b_0,b_1,b_2,\dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$$

ja

$$(a_0,a_1,a_2,\dots) \cdot (b_0,b_1,b_2,\dots) = (c_0,c_1,c_2,\dots),$$

missä $c_j = \sum_{i=0}^{j} a_i b_{j-1}$, kun $j = 0,1,2,\dots$.

Merkintä. Olkoon R rengas. Kuvausta

$$f\colon\ R \to R,\ f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

jossa $f(x) \in R[x]$ sanotaan polynomin $f(x)$ määräämäksi polynomikuvaukseksi, jossa yhteen- ja kertolaskut ovat renkaan R laskutoimituksia.

Lause 1.17. *(Jakoalgoritmi polynomirenkaille) Olkoon R vaihdannainen rengas ja $f(x), g(x) \in R[x]$. Oletetaan, että $g(x)$:n korkeimman asteen termin kerroin on yksikkö renkaassa R. Tällöin on olemassa polynomit $q(x), r(x) \in R[x]$, joille pätee $f(x) = q(x)\,g(x) + r(x)$, missä joko $r(x) = 0$ tai $\deg(r) < \deg(g)$.*

Todistus. (vrt. [1, s. 210]) Olkoon $S = \{f(x) - g(x)\,s(x) \mid s(x) \in R[x]\}$. Jos $0 \in S$, niin on olemassa $s(x)$, jolla $f(x) - g(x)\,s(x) = 0 \implies f(x) = g(x)\,s(x)$, tällöin $q(x) = s(x)$ ja $r(x) = 0$.

Olkoon nyt $r(x)$ pienintä astetta oleva S:n alkio. Oletetaan, että $0 \notin S$. Tällöin $f(x) = q(x)\,g(x) + r(x)$, jollain $q(x) \in R[x]$. Osoitetaan nyt, että $\deg(r) < \deg(g)$. Merkitään polynomeja $f(x)$, $g(x)$ ja $r(x)$ seuraavasti:

- $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$,
- $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$

- $r(x) = c_t x^t + c_{t-1}x^{t-1} + \cdots + c_0$,

missä a_n, b_m ja c_t ovat nollasta poikkeavia R:n alkioita. Tehdään vastaoletus, että $t \geq m$. Koska $b_m \in R$ on nollasta poikkeava, niin sillä on käänteisalkio b_m^{-1}. Voidaan siis muodostaa polynomi

$$\begin{aligned} s(x) &= f(x) - g(x)\, q(x) - \left(\frac{c_t}{b_m}\right) x^{t-m} \cdot g(x) \\ &= f(x) - g(x) \cdot \left(q(x) - \left(\frac{c_t}{b_m}\right) x^{t-m}\right) \\ &= r(x) - \left(\frac{c_t}{b_m}\right) x^{t-m} \cdot g(x). \end{aligned}$$

Polynomi $s(x) \in S$ ja sen astetta t olevan termin kerroin on

$$c_t - \frac{c_t}{b_m} \cdot b_m = 0.$$

Siis $\deg(s) < \deg(r)$, mikä on ristiriita sen kanssa, että $r(x)$ on pienintä astetta oleva S:n alkio. Täten vastaoletus on väärä ja $t < m$.

Osoitetaan vielä polynomien $q(x)$ ja $r(x)$ yksikäsitteisyys. Oletetaan, että on olemassa polynomit $q'(x)$ ja $r'(x)$, joille $g(x) = q'(x) f(x) + r'(x)$ ja $\deg(r') < \deg(f)$. Tällöin

$$r(x) - r'(x) = (q'(x) - q(x)) \cdot f(x),$$

missä $\deg(r - r') < \deg(f)$. Toisaalta $\deg(r - r') = \deg(q' - q) + \deg(f)$, joten on oltava $q'(x) - q(x) = 0$. Tästä seuraa, että $r'(x) - r(x) = 0 \cdot f(x) = 0$. Siis $q(x) = q'(x)$ ja $r(x) = r'(x)$. □

Määritelmä 1.18. Olkoon $(K, +, \cdot)$ kunta. Joukon

$$K[x] = \left\{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in K, n \geq 0\right\}$$

alkioita kutsutaan *K-kertoimisiksi polynomeiksi* yleisemmin *kuntakertoimisiksi* polynomeiksi. Polynomirengas $K[x]$ varustettuna polynomien yhteen- ja kertolaskulla on $(K[x], +, \cdot)$.

Lause 1.19. *Kunnan polynomirengas $(K[x], +, \cdot)$ on pääideaalialue.*

Todistus. Olkoon $I \neq \{0\}$ kuntakertoimisen polynomin $K[x]$ ideaali. Valitaan $p(x) \in I$, $p \neq 0$ siten, että se on asteen suhteen minimaalinen. Olkoon lisäksi $f(x) \in I$. Jakoalgoritmin nojalla on olemassa $q(x), r(x) \in K[x]$, joille

$$f(x) = p(x)\, q(x) + r(x),$$

missä $\deg(r) < \deg(p)$ tai $r(x) = 0$. Nyt

$$f(x) = p(x)\,q(x) + r(x) \;\Rightarrow\; r(x) = f(x) - p(x)\,q(x) \in I.$$

Koska $\deg(p)$ on minimaalinen, niin on oltava $r(x) = 0$. Näin ollen $f(x) \in \langle p(x)\rangle$ ja $K[x]$ on pääideaalialue. □

Edellisessä luvussa todettiin, että rengas $(\mathbb{Z}, +, \cdot)$ on pääideaalialue. Seuraavaksi osoitetaan esimerkin avulla, että kuitenkaan kokonaislukukertoiminen polynomirengas $\mathbb{Z}[x]$ ei ole pääideaalialue.

Esimerkki 1.20. Osoitetaan nyt, että ideaali $I = \langle 2,x\rangle$ renkaassa $\mathbb{Z}[x]$ ei ole pääideaali.

Todistus. Tehdään vastaoletus, että I on pääideaali renkaassa $\mathbb{Z}[x]$. Tällöin on olemassa $f(x) \in \mathbb{Z}[x]$ siten, että $I = \langle f(x)\rangle$. Nyt koska $2 \in I$, niin on olemassa $g(x) \in \mathbb{Z}[x]$ siten, että $2 = g(x)\,f(x)$. Tällöin

$$\deg(f(x)) + \deg(g(x)) = \deg(f(x)\,g(x)) = \deg(2) = 0,$$

joten $\deg(f(x)) = \deg(g(x)) = 0$. Olkoon nyt siis $f(x) = a$, $g(x) = b$, missä $a,b \in \mathbb{Z}$. Nyt siis $2 = ab$, joten $a = \pm 1$ tai $a = \pm 2$.

- Jos $a = \pm 1$, niin $\langle f(x)\rangle = \langle 2,x\rangle = \langle \pm 1\rangle$. Tällöin on olemassa $s(x), t(x) \in \mathbb{Z}[x]$ siten, että $1 = 2 \cdot s(x) + x \cdot t(x)$, josta seuraa, että $1 = 2 \cdot s(0)$, joten $s(0) = \frac{1}{2}$. Mutta $\frac{1}{2} \notin \mathbb{Z}$, joten tämä on ristiriita.
- Jos $a = \pm 2$, niin $\langle f(x)\rangle = \langle 2,x\rangle = \langle \pm 2\rangle$. Tällöin on olemassa $r(x) \in \mathbb{Z}[x]$ siten, että $x = 2 \cdot r(x) \Leftrightarrow r(x) = \frac{1}{2} \cdot x$. Mikä on ristiriidassa sen kanssa, että $r(x) \in \mathbb{Z}[x]$.

Nyt on osoitettu, että $I = \langle 2,x\rangle$ ei ole pääideaali renkaassa $\mathbb{Z}[x]$, joten $\mathbb{Z}[x]$ ei ole pääideaalialue.

□

2 Euklidiset alueet

Tässä luvussa tarkastellaan euklidisten alueiden käsitettä. Luvussa on käytetty ja sovellettu monipuolisesti lähes kaikkia lähdeluettelon lähteitä [1], [2], [3], [5] ja [6]. Aluksi määritellään, mikä on euklidinen alue ja osoitetaan, miksi kokonaislukurengas on eräs esimerkki euklidisesta alueesta. Lisäksi näytetään, että euklidisella alueella on aina ainakin yksi universaalisivutekijä ja että kuntakertoiminen polynomirengas on euklidinen alue. Tarkastellaan myös Gaussin kokonaislukujen rengasta, joka on euklidinen alue, kun sille on määritelty sopiva astefunktio, joka myöhemmin viimeisessä luvussa nimetään normiksi. Tämän jälkeen osoitetaan, että jokainen euklidinen alue on olennaisesti pääideaalialue. Lopuksi esitellään eukleideen algoritmin toiminta ja näytetään tästä eräs esimerkki.

2.1 Euklidisen alueen määritelmä

Euklidinen alue on astefunktiolla varustettu kokonaisalue, joka toteuttaa jakoalgoritmin. Tässä luvussa esitellään euklidisen alueen perusominaisuuksia ja todetaan, että erityisesti kuntakertoiminen polynomirengas on euklidinen alue.

Määritelmä 2.1. Kokonaisalue R on *euklidinen alue*, jos on olemassa kuvaus $d\colon R \setminus \{0\} \to \mathbb{N}$, jolle pätevät seuraavat kohdat:

1. Kun $a,b \in R \setminus \{0\}$, niin $d(a) \leq d(ab)$.
2. (Jakoalgoritmi) Kaikilla $a,b \in R \setminus \{0\}$ on olemassa $q,r \in R$, joille $a = qb + r$, missä $r = 0$ tai $d(r) < d(b)$.

Kuvausta d kutsutaan kokonaisalueen R *astefunktioksi*.

Esimerkki 2.2. Kokonaislukurengas $(\mathbb{Z}, +, \cdot)$, jonka yksi astekuvaus $d\colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}$, $d(m) = |m|$ on euklidinen alue.

Todistus. Osoitetaan, että tämä astekuvaus täyttää euklidisen alueen määritelmän ehdot.

1. Kaikilla $m,n \in \mathbb{Z} \setminus \{0\}$ pätee $d(m) = |m| \leq |mn| = d(mn)$.
2. Selvästi myös jos $m = qn + r$, missä $q,r \in \mathbb{Z}$ ja $0 \leq r < |n|$, niin $r = 0$ tai $r = |r| = d(r) < d(n) = |n|$.

□

Seuraavaksi määritellään *universaali sivutekijä* ja osoitetaan, että euklidisella alueella on ainakin yksi universaali sivutekijä. Tämä on olennainen tulos viimeisen luvun todistuksessa.

Määritelmä 2.3. Kokonaisalueen R alkio x on *universaali sivutekijä*, jos se ei ole yksikkö ja jokaiselle $a \in R$ pätee $x \mid a$ tai $x \mid a + u$, missä u on yksikkö.

Lause 2.4. *Olkoon R euklidinen alue, d sen astefunktio ja $u \in R$. Alkio u on yksikkö, jos ja vain jos $d(u) = d(1)$.*

Todistus. Oletetaan ensin, että u on yksikkö. Tällöin $u \mid 1$ ja jollakin $n \in \mathbb{Z}$ on oltava $un = 1$. Nyt euklidisen alueen astefunktion määritelmän nojalla $d(u) \leq d(u \cdot n) = d(1)$. Koska $u = 1 \cdot u$, niin $d(1) \leq d(1 \cdot u) = d(u)$, joten $d(1) = d(u)$.

Oletetaan sitten, että $d(1) = d(u)$. Koska $u \neq 0$, niin voidaan kirjoittaa $1 = qu+r$, missä $q,r \in R$. Jos $r \neq 0$, niin $d(r) < d(u) = d(1) \leq d(r \cdot 1) = d(r)$, mikä on selvästi ristiriita. Näin ollen $r = 0$ ja $1 = q \cdot u$, joten u on yksikkö. □

Lause 2.5. *Jos R on euklidinen alue, niin siinä on ainakin yksi universaali sivutekijä.*

Todistus. Tiedetään, että kunnan universaali sivutekijä on 0. Oletetaan nyt siis, että R ei ole kunta ja valitaan $a \in R$ siten, että $d(a)$ minimoi $d(x)$:n, kun x ei ole yksikkö ja $x \neq 0$. Osoitetaan nyt, että a on renkaan R universaali sivutekijä.

Olkoon $b \in R$. Koska R on euklidinen alue, niin on olemassa $q,r \in R$ siten, että $b = aq + r$, missä $r = 0$ tai $d(r) < d(a)$. Nyt jos $r = 0$, niin $b = aq \Rightarrow a \mid b$. Jos $r \neq 0$, niin $d(r) < d(a)$ ja $b = aq + r \Rightarrow b - r = aq \Rightarrow a \mid b - r \Rightarrow a \mid b + (-r)$.

Nyt koska $d(r) < d(a)$ ja $d(a)$ on minimaalinen, niin $-r$ on yksikkö. Siis $a \in R$ on universaali sivutekijä. □

Seuraavaksi osoitetaan, että jos K on kunta, niin $K[x]$ on euklidinen alue. Lauseen 1.10 nojalla jokainen kunta on kokonaisalue. Koska euklidinen alue on kokonaisalue, niin on syytä osoittaa myös että jos rengas R on kokonaisalue, niin myös polynomirengas $R[x]$ on kokonaisalue. Seuraavat todistukset perustuvat lähteeseen [3].

Lause 2.6. *Jos R on kokonaisalue, niin $R[x]$ on kokonaisalue.*

Todistus. Olkoon R kokonaisalue. Näin ollen R on vaihdannainen rengas ja myös polynomirengas $R[x]$ on vaihdannainen rengas. On osoitettava, että polynomirenkaassa $R[x]$ ei ole nollajakajia.

Olkoot nyt polynomit $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ ja $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ renkaan $R[x]$ alkioita. Tällöin on olemassa sellaiset a_i ja b_j, että $a_i \neq 0$ ja $b_j \neq 0$, sekä a_{i+t} ja b_{j+t} nollasta eroavia kaikilla $t \geq 1$. Olkoon $r(x) = f(x)\,g(x) = c_{n+m}x^{n+m} + \ldots + c_1 x + c_0$. Polynomien kertolaskusäännön nojalla termin x^{i+j} kerroin polynomissa $r(x)$ on

$$c_{i+j} = a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_i b_j + \cdots + a_{i+j} b_0 = a_i b_j \neq 0,$$

koska R on kokonaisalue ja $a_i, b_j \in R \setminus \{0\}$. Näin ollen vähintään yksi polynomin $r(x)$ kertoimista on erisuuri kuin nolla, joten $r(x) \neq 0$ ja $R[x]$ on kokonaisalue. □

Lause 2.7. *Jos K on kunta, niin $K[x]$ on euklidinen alue.*

Todistus. On jo osoitettu, että $K[x]$ on kokonaisalue. Määritellään nyt kuntakertoimisen polynomin astefunktio

$$d\colon\ K[x] \setminus \{0\} \to \mathbb{N}, \quad d(f(x)) = \deg(f(x)),$$

kun $f(x) \in K[x] \setminus \{0\}$. Nyt koska $\deg(f(x)) \geq 0$, niin $d(f(x)) \in \mathbb{N}$, kun $f(x) \in K[x] \setminus \{0\}$. Olkoot $f(x), g(x) \in K[x] \setminus \{0\}$ ja $g(x) \neq 0$.

Olkoot nyt polynomit $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, missä $a_n \neq 0$ ja $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$, missä $b_m \neq 0$. Koska K on kokonaisalue, niin $a_n b_m \neq 0$ ja polynomien laskusääntöjen nojalla saadaan, että $\deg(f(x)\,g(x)) = n + m$. Näin ollen

$$d(f(x)) = \deg(f(x)) = n \leq n + m = \deg(f(x)\,g(x)) = d(f(x)\,g(x)).$$

Lisäksi euklidisen alueen jakoalgoritmin määritelmän nojalla on olemassa $q(x), r(x) \in K[x]$ siten, että

$$f(x) = q(x)\,g(x) + r(x), \ \text{ missä } \ r(x) = 0 \ \text{ tai } \ \deg(r(x)) < \deg(g(x)).$$

Tästä seuraa astefunktion määritelmän nojalla, että

$$f(x) = q(x)\,g(x) + r(x), \ \text{ missä } \ r(x) = 0 \ \text{ tai } \ d(r(x)) < d(g(x)).$$

Nyt on osoitettu määritelmän 2.1 molemmat kohdat ja voidaan todeta, että jos K on kunta, niin sen kuntakertoiminen polynomirengas $K[x]$ on euklidinen alue.

□

2.2 Gaussin kokonaisluvut

Määritelmä 2.8. Gaussin kokonaislukujen joukko on kompleksilukujen osajoukko $\mathbb{Z}[i] = \{a + bi \mid a,b \in \mathbb{Z}\}$.

Lause 2.9. *Gaussin kokonaislukujen joukko $\mathbb{Z}[i]$ on suljettu yhteen- ja kertolaskutoimituksen suhteen.*

Todistus. Olkoon nyt $z = a + bi$, $w = c + di \in \mathbb{Z}[i]$, missä $a,b,c,d \in \mathbb{Z}$. Nyt

$$\begin{aligned} z + w &= (a + bi) + (c + di) \\ &= a + bi + c + di \\ &= a + c + bi + di \\ &= \underbrace{(a + c)}_{\in\mathbb{Z}} + \underbrace{(b + d)}_{\in\mathbb{Z}} i \end{aligned}$$

ja

$$\begin{aligned} z \cdot w &= (a + bi) \cdot (c + di) \\ &= ac + adi + bic + bidi \\ &= ac + adi + bic - bd \\ &= ac - bd + adi + bci \\ &= \underbrace{(ac - bd)}_{\in\mathbb{Z}} + \underbrace{(ad + bc)}_{\in\mathbb{Z}} i. \end{aligned}$$

Siis summa $z + w \in \mathbb{Z}$ ja tulo $z \cdot w \in \mathbb{Z}$, joten Gaussin kokonaislukujen joukko on varustettu yhteen- ja kertolaskutoimituksilla. □

Lause 2.10. *Gaussin kokonaislukujen joukko on rengas.*

Todistus. Käydään nyt läpi määritelmän 1.2 mukaiset ehdot osoittaaksemme, että $(\mathbb{Z}[i], +, \cdot)$ on rengas. Olkoot nyt $x,y,z \in \mathbb{Z}$ siten, että $x = a + bi$, $y = c + di$ ja $z = e + fi$, missä $a,b,c,d,e,f \in \mathbb{Z}$.

1. $(\mathbb{Z}[i], +)$ on Abelin ryhmä,

   - Yhteenlaskutoimitus on liitännäinen:

$$\begin{aligned} x + (y + z) &= a + bi + (c + di + e + fi) \\ &= a + bi + c + di + e + fi \\ &= (a + bi + c + di) + e + fi \\ &= (x + y) + z. \end{aligned}$$

   - Yhteenlaskutoimituksella on neutraalialkio:

$$x + 0 = a + bi + 0 = a + bi = x.$$

   - Yhteenlaskulla on vasta-alkio:

$$\begin{aligned} x + (-x) &= (a + bi) + (-a - bi) \\ &= a + bi - a - bi \\ &= a - a + bi - bi \\ &= 0. \end{aligned}$$

   - Yhteenlaskutoimitus on vaihdannainen:

$$\begin{aligned} x + y &= a + bi + c + di \\ &= c + di + a + bi \\ &= y + x. \end{aligned}$$

2. Kertolasku $\cdot$ on liitännäinen,

$$\begin{aligned} x \cdot (y \cdot z) &= x \cdot ((c + di) \cdot (e + fi)) \\ &= x \cdot ((ce - df) + (cf + de)\, i) \\ &= x \cdot (ce - df) + x \cdot (cf + de)\, i \\ &= xce - xdf + xcfi + xdei \\ &= (a + bi) \cdot ce - (a + bi) \cdot df + (a + bi) \cdot cfi + (a + bi) \cdot dei \\ &= ace + bice - adf - bidf + acfi + bicfi + adei + bidei \\ &= ace + acfi - bidf + bidei - adf + adei + bice + bicfi \end{aligned}$$

$$
\begin{aligned}
&= ac \cdot (e + fi) - bd \cdot (e + fi) + adi \cdot (e + fi) + bci \cdot (e + fi) \\
&= ((ac - bd) + adi + bci) \cdot (e + fi) \\
&= ((ac - bd) + (ad - bc)\, i) \cdot z \\
&= ((a + bi) \cdot (c + di)) \cdot z \\
&= (x \cdot y) \cdot z.
\end{aligned}
$$

3. Laskutoimituksella $(\mathbb{Z}\,[i]\,, \cdot)$ on neutraalialkio,

$$x \cdot 1 = (a + bi) \cdot 1 = a + bi = x.$$

4. Osittelulaki toteutuu:

$$
\begin{aligned}
x \cdot (y + z) &= (a + bi) \cdot (c + di + e + fi) \\
&= (a + bi) \cdot c + (a + bi) \cdot di + (a + bi) \cdot e + (a + bi) \cdot fi \\
&= ac + bic + adi + bidi + ae + bie + afi + bifi \\
&= ac + bic + adi - bd + ae + bie + afi - bf \\
&= ac - bd + adi + bic + ae - bf + afi + bie \\
&= (ac - bd) + (ad + bc)\, i + (ae - bf) + (af - be)\, i \\
&= (a + bi) \cdot (c + di) + (a + bi) \cdot (e + fi) \\
&= x \cdot y + x \cdot z.
\end{aligned}
$$

Näin on osoitettu, että Gaussin kokonaislukujen joukko $\mathbb{Z}\,[i]$ on rengas. □

Lause 2.11. *Gaussin kokonaislukujen rengas on vaihdannainen rengas.*

Todistus. Olkoon $z = a + bi$, $w = c + di \in \mathbb{Z}\,[i]$, missä a,b,c,$d \in \mathbb{Z}$.

$$
\begin{aligned}
z \cdot w &= (a + bi) \cdot (c + di) \\
&= (ac - bd) + (ad + bc)\, i \\
&= (ca - db) + (da + cb)\, i \\
&= (c + di) \cdot (a + bi) \\
&= w \cdot z.
\end{aligned}
$$

Siis Gaussin kokonaislukujen kertolaskutoimitus on vaihdannainen, joten $\mathbb{Z}\,[i]$ on vaihdannainen rengas. □

Seuraavaksi osoitetaan, että itse asiassa Gaussin kokonaislukujen rengas on euklidinen alue, kun se varustetaan sopivalla astefunktiolla. Kyseinen astefunktio tunnetaan normina N, johon tutustutaan lähemmin viimeisessä luvussa. Euklidisen alueen määritelmän nojalla aloitetaan osoittamalla, että $\mathbb{Z}[i]$ on kokonaisalue.

Lause 2.12. *Gaussin kokonaislukujen rengas* $(\mathbb{Z}[i], +, \cdot)$ *on kokonaisalue.*

Todistus. On jo osoitettu, että $\mathbb{Z}[i]$ on vaihdannainen rengas. Tämän lisäksi selvästi $\mathbb{Z}[i]$ on yksiköllinen ja $1 = 1 + 0i \neq 0 + 0i = 0$. Olkoon nyt $z = a + bi$, $w = c + di \in \mathbb{Z}[i]$. Osoitetaan, että jos $zw = 0$, niin $z = 0$ tai $w = 0$. Nyt siis

$$zw = (a + bi)(c + di) = (ac - bd) + (ad + bc)i = 0 + 0i = 0,$$

joten $ac - bd = 0$ ja $ad + bc = 0$. Oletetaan ensin, että $a \neq 0$, jolloin

$$\begin{aligned}
\begin{cases} ac - bd = 0 \\ ad + bc = 0 \end{cases} &\Leftrightarrow \begin{cases} c = \frac{bd}{a} \\ ad + bc = 0 \end{cases} \\
&\Rightarrow ad + b\left(\frac{bd}{a}\right) = 0 \\
&\Leftrightarrow ad + \frac{b^2 d}{a} = 0 \\
&\Leftrightarrow a^2 d + b^2 d = 0 \\
&\Leftrightarrow d\left(a^2 + b^2\right) = 0.
\end{aligned}$$

Siis tulon nollasäännön nojalla $d = 0$ tai $a^2 + b^2 = 0$. Jos $a^2 + b^2 = 0$, niin tällöin olisi $a = b = 0$, mikä ei ole mahdollista, sillä oletuksen mukaan $a \neq 0$. On siis oltava, että $d = 0$ ja koska $c = \frac{bd}{a}$, niin myös $c = 0$.Tästä seuraa, että $w = c + di = 0 + 0i = 0$. Mikäli $a = 0$, niin saadaan että

$$\begin{cases} ac - bd = 0 \\ ad + bc = 0 \end{cases} \Leftrightarrow \begin{cases} -bd = 0 \\ bc = 0. \end{cases}$$

Jos nyt $b = 0$, niin $z = a + bi = 0 + 0i = 0$. Jos taas $b \neq 0$, niin on oltava $c = 0$ ja $d = 0$, jolloin päästään taas tilanteeseen, että $w = 0$.

On siis osoitettu, että Gaussin kokonaislukujen renkaassa pätee tulon nollasääntö ja näin ollen rengas on kokonaisalue. □

Lause 2.13. *Gaussin kokonaislukujen rengas* $(\mathbb{Z}[i], +, \cdot)$ *varustettuna astefunktiolla* $d\colon \mathbb{Z}[i] \setminus 0 \to \mathbb{N}$, $d(a+bi) = (a+bi)(a-bi) = a^2+b^2$, $a,b \in \mathbb{Z}$ *on euklidinen alue.*

Todistus. Olkoon $a+bi, c+di \in \mathbb{Z}[i] \setminus \{0\}$. Tällöin

$$\begin{aligned} d((a+bi)(c+di)) &= d((ac-bd)+(bc+ad)i) \\ &= (ac-bd)^2+(bc+ad)^2 \\ &= a^2c^2-2acbd+b^2d^2+b^2c^2+2bcad+a^2d^2 \\ &= a^2c^2+b^2d^2+b^2c^2+a^2d^2 \\ &= \left(a^2+b^2\right)\left(c^2+d^2\right) \\ &= d(a+bi)\cdot d(c+di). \end{aligned}$$

Koska $d(a+bi) = a^2+b^2$ on positiivinen kokonaisluku, niin $d(a+bi) \leq d(a+bi)\,d(c+di) = d((a+bi)(c+di))$.

Olkoot nyt $a+bi, c+di \in \mathbb{Z}[i]$ ja $c+di \neq 0$. Osoitetaan, että on olemassa $q+q'i, r+r'i \in \mathbb{Z}[i]$ siten, että

$$a+bi = (q+q'i)(c+di)+(r+r'i),$$

missä $r+r'i = 0$ tai $d(r+r'i) < d(c+di)$. Asetetaan, että $(a+bi)(c+di)^{-1} = u+vi$, missä $u,v, \in \mathbb{R}$. Jos on olemassa halutunlaiset $q+q'i$ ja $r+r'i$, niin kompleksilukujen joukossa $\mathbb{C}$ on voimassa:

$$\begin{aligned} a+bi &= (q+q'i)(c+di)+(r+r'i) \\ &\Leftrightarrow \\ r+r'i &= (a+bi)-(q+q'i)(c+di) \\ &= (c+di)\left((a+bi)(c+di)^{-1}-(q+q'i)\right) \\ &= (c+di)((u+vi)-(q+q'i)) \\ &= (c+di)((u-q)+(v-q')i) \\ &= cu-cq+diu-diq+cvi-cq'i+divi-diq'i \\ &= (cu-cq-dv+dq')+(du-dq+cv-cq')i \\ &= (c(u-q)-d(v-q'))+(c(v-q')+d(u-q))i. \end{aligned}$$

Tällöin saadaan

$$\begin{aligned} d(r+r'i) &= (c(u-q)-d(v-q'))^2 + (d(u-q)+c(v-q'))^2 \\ &= \left(c^2+d^2\right)\left((u-q)^2+(v-q')^2\right). \end{aligned}$$

Jos $(u-q)^2+(v-q')^2 < 1$, niin $d(r+r'i) < d(c+di)$. Valitaan $q,q' \in \mathbb{Z}$, niin että lukujen $u-q$ ja $v-q'$ itseisarvot ovat mahdollisimman pienet. Tällöin $(u-q)^2 \leq \frac{1}{4}$ ja $(v-q')^2 \leq \frac{1}{4}$, joten $(u-q)^2+(v-q')^2 < 1$. Näin on osoitettu, että kun $a+bi = (q+q'i)(c+di)+(r+r'i)$, niin $r+r'i = 0$ tai $d(r+r'i) < d(c+di)$.

Siis Gaussin kokonaislukujen rengas varustettuna astefunktiolla $d(a+bi) = a^2+b^2$ on euklidinen alue. □

2.3 Euklidisen alueen ideaalit

Todettiin aikaisemmin, että jos vaihdannaisen renkaan jokainen ideaali on pääideaali, niin rengas on pääideaalialue. Euklidisten alueiden yksi ominaisuus on se, että jokainen alueen ideaali on pääideaali, josta siis seuraa, että jokainen euklidinen alue on pääideaalialue.

Lause 2.14. *Jokainen euklidinen alue on pääideaalialue.*

Todistus. Olkoon R euklidinen alue, jolloin se on myös kokonaisalue, ja olkoon I sen ideaali. Kiinnitetään euklidiselle alueelle R astefunktio d. Jos $I = \{0\}$, niin tällöin $I = \langle 0 \rangle$ on pääideaali. Oletetaan, että $I \neq \{0\}$. Kaikkien nollasta poikkeavien alkioiden asteiden joukossa on pienin alkio. Olkoon pienin alkio n. Nyt siis $n = \min d[I \setminus \{0\}]$.

Olkoon $a \in I$. Valitaan sellainen $t \in I \setminus \{0\}$, että $n = d(t)$. Osoitetaan, että $I = \langle t \rangle$. Jakoyhtälön nojalla on olemassa sellaiset $q,r \in I$, että $a = qt - r$, missä $r = 0$ tai $d(r) < d(t)$. Koska $r = qt - a \in I$ ja $d(t) = n = \min d[I \setminus \{0\}]$, niin on oltava $r = 0$. Näin ollen $a = qt \in \langle t \rangle$ ja $I = \langle t \rangle$.

□

2.4 Eukleideen algoritmi

Eukleideen algoritmi on tunnettu menetelmä kahden kokonaisluvun suurimman yhteisen tekijän (syt) laskemiseen. Algoritmin toiminta perustuu toistuvaan jakoon ja jakojäännöksen hyödyntämiseen. Esitetään seuraavaksi Eukleideen algoritmi kokonaisluvuille sekä Eukleideen algoritmi polynomeille, minkä voi yleistää euklidisissa alueissa toimivaksi.

Eukleideen algoritmi 2.15. Olkoon a ja b positiivisia kokonaislukuja. On olemassa algoritmi, joka löytää suurimman yhteisen tekijän syt $(a,b) = d$ sekä parin kokonaislukuja s ja t, joille pätee $d = sa + tb$.

Eukleideen algoritmin todistus kokonaisluvulle on vastaava kuin polynomien esityksessä, joten todistus esitetään vain kerran.

Eukleideen algoritmi polynomeille 2.16. Olkoon K kunta ja $f(x), g(x) \in K[x]$. On olemassa algoritmi suurimman yhteisen tekijän syt(f,g) laskemiseksi, sekä polynomien $s(x)$ ja $t(x)$ löytämiseksi siten, että syt $(f,g) = s(x) f(x) + t(x) g(x)$.

Todistus. (vrt. [6, s. 138]) Todistus perustuu yksinkertaisesti jakoalgoritmin toistoon niin kauan kunnes jakojäännös on 0:

$$
\begin{aligned}
g &= q_1 f + r_1 \\
f &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\dots \\
r_{n-4} &= q_{n-2} r_{n-3} + r_{n-2} \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n + 0.
\end{aligned}
$$

Algoritmin on pakko pysähtyä lopulta vain äärelliseen määrään askelia, koska astejono ei voi olla ääretön. Väite on, että $d = r_n$ on suurin yhteinen tekijä, kunhan sen korkeimman asteen termin kerroin on 1. Nähdään, että d on yhteinen tekijä polynomeille f ja g, kun lasketaan alhaalta ylöspäin. Nähdäksemme, että d on suurin yhteinen tekijä, edetään ylhäältä alas osoittaaksemme, että jos c on mikä tahansa

f ja g yhteinen tekijä, niin $c \mid r_i$ jokaisella indeksillä i. Lopuksi, jotta löydetään sellaiset s ja t, joille $d = sa + tb$, työskennellään jälleen alhaalta ylöspäin:

$$\begin{aligned}
r_n &= r_{n-2} - q_n r_{n-1} \\
&= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\
&= (1 + q_n \cdot q_{n-1})r_{n-2} - q_n r_{n-3} \\
&= (1 + q_n \cdot q_{n-1})(r_{n-4} - q_{n-2}r_{n-3}) - q_n r_{n-3} \\
&= (1 + q_n \cdot q_{n-1})r_{n-4} - [(1 + q_{n-1})q_{n-2} + q_n]r_{n-3} \\
&\dots \\
&= sf + tg.
\end{aligned}$$

Näin on osoitettu jakoalgoritmin toiminnan polynomeille. □

Esimerkki 2.17. Olkoon $f(x) = x^4$, $g(x) = x^3 - x \in \mathbb{R}[x]$. Selvitetään polynomien suurin yhteinen tekijä.

$$\begin{aligned}
x^4 &= x \cdot \left(x^3 - x\right) + x^2 \\
x^3 - x &= x \cdot x^2 - x \\
x^2 &= (-x) \cdot (-x) + 0
\end{aligned}$$

Siis $-x$ on polynomien f ja g suurin yhteinen tekijä.

3 Euklidisen alueen yleistyksiä

Yleisesti euklidinen alue määritellään, kuten määritelmässä 2.1 on ilmaistu. Määritelmän mukaan euklidinen alue R on kokonaisalue, jos on olemassa astekuvaus $d\colon\ R \setminus \{0\} \to \mathbb{N}$, joka toteuttaa läpikäydyt ominaisuudet. Astekuvaus kuvautuu siis luonnollisten lukujen joukolle $\mathbb{N}$. Tässä luvussa laajennetaan näkemystä euklidisuudesta tutkimalla euklidisen alueen yleistyksiä. Ensin yleistetään astekuvauksen käsitteen hyvin määritellylle joukolle, jota kutsutaan transfiniittiseksi euklidiseksi alueeksi. Tämän jälkeen esitetään, että euklidinen rengas ei edellytä kokonaisalueen määritelmää. Lisäksi määritellään transfiniittisen euklidisen renkaan ja osoitetaan, että kahden transfiniittisen renkaan tulo ei ole euklidinen alue, mutta se on silti transfiniittinen euklidinen rengas. Tämän luvun tarkoituksena on avata euklidisen alueen käsitteen monimuotoisuutta. Luvun lähteenä on käyetty erityisesti Nagatan [4] ja Pierren [7] artikkelien tietoja.

3.1 Transfiniittinen euklidinen alue

Yksi yleistys euklidisista alueista on *transfiniittinen euklidinen alue*, jossa astekuvaus d kuvautuu *hyvinjärjestettyjen* lukujen joukolle. Tämä tarkoittaa siis sitä, että jos R on euklidinen alue, niin voidaan valita hyvinjärjestetyn joukon H ja kuvauksen $d\colon R \setminus \{0\} \to H$.

Määritelmä 3.1. Olkoon $\leq$ relaatio joukossa H. Sanotaan, että $\leq$ on *osittainen järjestys* jos seuraavat kolme ehtoa pätevät. Olkoon nyt $h,j,k \in H$.

1. (*relaation refleksiivisyys*) Kaikilla $h \in H$ pätee $h \leq h$.
2. (*relaation antisymmetrisyys*) Jos $h \leq j$ ja $j \leq h$, niin $h = j$.
3. (*relaation transitiivisuus*) Jos $h \leq j$ ja $j \leq k$, niin $h \leq k$.

Lisäksi jos kaikilla $h,j \in H$ pätee $h \leq j$ tai $j \leq h$, niin relaatio on *täysi järjestys*.

Määritelmä 3.2. *Hyvinjärjestetty joukko* on sellainen täysin järjestetty joukko $(H, \leq)$, jonka jokaisella epätyhjällä osajoukolla on joukossa H pienin alkio.

Jos $(H, \leq)$ on hyvinjärjestetty joukko, niin relaatiota $\leq$ kutsutaan joukon H *hyvinjärjestykseksi*.

Huomautus. Lähteestä riippuen transfiniittinen euklidinen alue voidaan ilmaista myös kuvauksena ordinaaleille. Joukon H voi korvata ordinaalilla, missä ordinaali on hyvinjärjestetyn joukon H ordinaali. Ordinaalit ovat hyvinjärjestyksen invariantteja, mikä tarkoittaa sitä, että ordinaali säilyttää saman arvon riippumatta siitä, miten hyvinjärjestys esitetään, eli jos kaksi hyvinjärjestystä ovat isomorfisia, niin niillä on sama ordinaali.

Määritelmä 3.3. Olkoon H hyvinjärjestetty joukko. Kokonaisalue R on *transfiniittinen euklidinen alue*, jos on olemassa astekuvaus $d\colon\ R \setminus \{0\} \to H$, jolle pätee seuraavat euklidisuuden ehdot.

1. Kun $a,b \in R \setminus \{0\}$, niin $d\,(a) \leq d\,(ab)$.
2. Kaikilla $a,b \in R \setminus \{0\}$ on olemassa $q,r \in R$, joille $a = qb + r$, missä $r = 0$ tai $d\,(r) < d\,(b)$.

Transfiniittinen euklidinen alue siis laajentaa niinsanotun perinteisen euklidisen alueen käsitettä sallimalla astefunktion arvojoukoksi mikä tahansa joukon hyvinjärjestettyjä ordinaaleja. Tämä yleistys mahdollistaa monimutkaisempien rakenteiden tutkimisen algebrassa, erityisesti alueissa, jotka käsittelevät äärettömyyksiä ja transfiniittisiä lukuja.

Lause 3.4. *On olemassa sellainen transfiniittisen euklidisen alueen R minimaalinen astefunktio $d_{\min}$, että kuvauksen $d_{\min}$ maalijoukko on ordinaalijoukko ja jos d on toinen tällainen alueen R astefunktio, niin kaikilla $x \in R$, $x \neq 0$, pätee $d_{\min(x)} \leq\ d\,(x)$.*

Todistus. Olkoon α ordinaali, jolle $\alpha > |R|$. Asetetaan $d_{\min}\colon\ R \setminus \{0\} \to R$,

$$d_{\min}(x) = \min\{d(x) \mid d \text{ on astefunktio } R \setminus \{0\} \to \alpha\}.$$

.

On helppoa tarkastaa, että d täyttää astefunktion vaatimukset. Siis transfiniittisen euklidisen alueen astefunktioiden joukossa on olemassa minimaalinen astefunktio. □

3.2 Euklidinen rengas

Monissa lähteissä euklidisesta renkaasta ja euklidisesta alueesta puhutaan ikään kuin ne olisivat sama asia. Vaikka näillä käsitteillä on paljon yhteistä, niiden välillä on merkittävä ero. Euklidinen rengas ei edellytä kokonaisalueen 1.2 määritelmää. Euklidi-

sen alueen kuin myös transfiniittisen euklidisen alueen käsitteitä voidaan siis yleistää luopumalla vaatimuksesta, että rengas on kokonaisalue.

Määritelmä 3.5. Vaihdannainen rengas R on *euklidinen rengas*, jos on olemassa astekuvaus $d\colon\ R \setminus \{0\} \to \mathbb{N}$, jolle pätevät seuraavat kohdat

1. Kun $a,b \in R \setminus \{0\}$, niin $d(a) \leq d(ab)$.
2. (*Jakoalgoritmi*) Kaikilla $a,b \in R \setminus \{0\}$ on olemassa $q,r \in R$, joille $a = qb + r$, missä $r = 0$ tai $d(r) < d(b)$.

Euklidinen rengas on *transfiniittinen euklidinen rengas*, jos määritelmässä astekuvauksen maalijoukko on hyvinjärjestetty joukko luonnollisten lukujen joukon sijasta.

Voidaan siis todeta, että euklidinen rengas on laajempi käsite, joka sisältää euklidiset alueet. Vaikka jokainen euklidinen alue on siis euklidinen rengas, kaikki euklidiset renkaat eivät välttämättä ole euklidisia alueita.

Lähteissä esitetään, että äärellisen määrän euklidisia renkaita tulo on euklidinen rengas yksinkertaistettuna kahden renkaan tuloon. Esitetään ensin joukko-opista tuttu karteesisen tulon määritelmä ja edetään tämän jälkeen todistukseen.

Määritelmä 3.6. Kahden renkaan S ja T *karteesinen tulo* on joukko

$$S \times T = \{(s,t) \mid s \in S, t \in T\}.$$

Laskutoimitukset karteesisessa tulossa määritellään komponenteittain seuraavasti:

$$(s_1, t_1) + (s_2, t_2) = (s_1 + s_2, t_1 + t_2) \quad \text{ja} \quad (s_1, t_1) \cdot (s_2, t_2) = (s_1 \cdot s_2, t_1 \cdot t_2),$$

missä $s_1, s_2 \in S$ ja $t_1, t_2 \in T$.

Renkaiden S ja T karteesinen tulo on siis sellainen järjestettyjen parien joukko, joissa ensimmäinen alkio kuuluu renkaaseen S ja toinen alkio renkaaseen T. Kahden ja myös useamman joukon karteesinen tulo on vastaavasti järjestettyjen jonojen joukko. Osoitetaan tämä seuraavaksi transfiniittiselle euklidiselle alueelle.

Lause 3.7. *Kahden transfiniittisen euklidisen renkaan tulo $R_1 \times R_2$ on transfiniittinen euklidinen rengas.*

Todistus. Olkoon R_i euklidinen rengas. Olkoon renkaan R_i astefunktio $d_i\colon\ R_i \setminus \{0\} \to H_i$, missä H_i on hyvinjärjestetty joukko ja $i \in \{1,2\}$. Merkitään $H' = H_1 \times H_2$, jolle $(\alpha_1,\alpha_2) < (\beta_1,\beta_2)$ siten, että joko $\alpha_1 < \beta_1$ tai $\alpha_1 = \beta_1$ ja $\alpha_2 < \beta_2$. Kutsutaan

nyt joukoksi H kahden joukon H' kopion järjestyssummaa. Koska H on hyvinjärjestetty joukko, niin voidaan muodostaa järjestyksen säilyttävät injektiiviset kuvaukset $h',h'' \colon\ H' \to H$, missä $h'(\lambda) < h''(\mu)$ kaikilla $\lambda,\mu \in H'$. Määritellään astefunktio $d \colon\ R_1 \times R_2 \setminus \{0\} \to H$ seuraavasti: Olkoon $x_1 \in R_1$ ja $x_2 \in R_2$.

- Jos $x_1 \neq 0$ ja $x_2 \neq 0$, niin $d(x_1,x_2) = h'(d_1(x_1),d_2(x_2))$.
- Jos $x_1 = 0$ ja $x_2 \neq 0$, niin $d(x_1,x_2) = h''(d_1(1),d_2(x_2))$.
- Jos $x_1 \neq 0$ ja $x_2 = 0$, niin $d(x_1,x_2) = h''(d_1(x_1),d_2(1))$.

Pyritään nyt osoittamaan, että jos $a_i = b_i q_i + r_i$, niin $d(r_i) < d(b_i)$ kaikilla $i = 1,2$.

Oletetaan, ensin että $b_1 \neq 0$ ja $b_2 \neq 0$. Jos $r_1 \neq 0$ ja $r_2 \neq 0$, niin

$$d(r_1,r_2) = h'(d_1(r_1),d_2(r_2)) < h'(d_1(b_1),d_2(b_2)) = d(b).$$

Tällöin $r = (r_1,r_2)$ ja $q = (q_1,q_2)$. Nyt jos $r_1 = 0$ ja $r_2 \neq 0$, niin $a_1 = b_1 q_1 = b_1(q_1 - 1) + b_1$ ja $a_2 = b_2 q_2 + r_2$, joten $r = (b_1,r_2)$ ja $q = (q_1 - 1,q_2)$. Saadaan, että

$$d(r) = h'(d_1(b_1),d_2(r_2)) < h'(d_1(b_1),d_2(b_2)) = d(b).$$

Vastaavasti voidaan todeta tapaus $r_1 \neq 0$ ja $r_2 = 0$.

Oletetaan sitten, että $b_1 = 0$ ja $b_2 \neq 0$. Jos $a_1 \neq 0$, niin $a_2 = b_2 q_2 + r_2$, missä $r_2 \neq 0$. Tällöin $r = (a_1,r_2)$, $q = (0,q_2)$ ja $d(r) \in h'(H')$, $d(b) \in h''(H'')$, jolloin selvästi $d(r) < d(b)$. Jos $a_1 = 0$, niin $a_2 = b_2 q_2 + r_2$ ja $r = (0,r_2)$, $q = (0,q_2)$. Tällöin

$$d(r) = h''(d_1(1),d_2(r_2)) < h''(d_1(1),d_2(b_2)) = d(b).$$

Vastaavasti voidaan käydä läpi tapaus $b_1 \neq 0$ ja $b_2 = 0$. Näin on osoitettu, että transfiniittisen euklidisen renkaan tulo on transfiniittinen euklidinen rengas, sillä $R_1 \times R_2$ säilyttää euklidisen renkaan ominaisuudet.

□

Esimerkin 2.2 avulla todettiin, että kokonaislukujen rengas $\mathbb{Z}$ on euklidinen alue. Edellä olevien läpikäyntien perusteella voidaan siis todeta, että $\mathbb{Z}$ on myös transfiniittinen euklidinen rengas ja sen tulo itsensä kanssa $\mathbb{Z} \times \mathbb{Z}$ on transfiniittinen euklidinen rengas. Tulo $\mathbb{Z} \times \mathbb{Z}$ ei ole kuitenkaan kokonaisalue, joten se ei säilytä euklidisen alueen ominaisuutta. Todetaan tämä seuraavan esimerkin avulla.

Esimerkki 3.8. Nyt $(0,1),(1,0) \in \mathbb{Z} \times \mathbb{Z}$. Karteesisen tulon määritelmän nojalla saadaan

$$(0,1) \cdot (1,0) = (0 \cdot 1, 1 \cdot 0) = (0,0)\,.$$

Siis renkaalla $\mathbb{Z} \times \mathbb{Z}$ on nollajakaja, joten se ei ole kokonaisalue. Näin ollen se ei ole myöskään euklidinen alue.

On osoitettu, että $\mathbb{Z} \times \mathbb{Z}$ on transfiniittinen euklidinen rengas, mutta ei euklidinen alue. Osoitetaan seuraavaksi vielä, että $\mathbb{Z} \times \mathbb{Z}$ ei ole myöskään euklidinen rengas, sillä $\mathbb{N}$ ei riitä astekuvauksen maalijoukoksi.

Lause 3.9. *Jos R on euklidinen rengas ja $a \mid b$ ja $b \nmid a$, missä $b \neq 0$, niin $d(a) < d(b)$ mille tahansa astefunktiolle d.*

Todistus. Olkoon d euklidisen renkaan R astefunktio. Jos $a \mid b$, niin on olemassa $q \in \mathbb{Z}$ siten, että $b = qa$. Tällöin astefunktion määritelmän nojalla $d(a) \leq d(b)$. Tehdään nyt vastaoletus, että $d(a) \geq d(b)$. Olkoon $a = sb + r$, missä $s, r \in R$ ja $0 \leq d(r) < d(b)$. Koska $a \nmid b$, niin $r \neq 0$. Saadaan, että $a = sb+t \Leftrightarrow r = a-sb \Leftrightarrow r = a - s(qa) = a(1 - sq)$. Tästä nähdään, että $a \mid r$, joten $d(a) \leq d(r)$. Mutta koska $r \neq 0$ ja $0 \leq d(r) < d(b)$, niin $d(r) < d(b)$. Siis nyt $d(a) \leq d(r) < d(b)$, mikä on ristiriita vastaoletuksen $d(a) \geq d(b)$ kanssa. Näin ollen vastaoletus on väärä ja $d(a) < d(b)$ pätee. □

Osoitetaan esimerkin avulla, että edellä todistettu lause ei päde renkaassa $\mathbb{Z} \times \mathbb{Z}$.

Esimerkki 3.10. Ensinnäkin jokaisella $k \in \mathbb{N}$ pätee $(1,2^k) \mid (1,2^{k+1})$, sillä $(1,2^{k+1}) = (1,2^k) \cdot (1,2)$ mutta $(1,2^{k+1}) \nmid (1,2^k)$. Edellisen lauseen 3.9 nojalla tästä seuraa, että asteilla $d(1,2^k)$ ei ole ylärajaa.

Tarkastellaan nyt renkaan $\mathbb{Z} \times \mathbb{Z}$ alkioita $(2,0)$ ja $\left(1,2^k\right)$, missä $k \in \mathbb{N}$. Tällöin edellisen lauseen nojalla pätee, että jos $\left(1,2^k\right) \mid (2,0)$, niin $d\left(1,2^k\right) < d(2,0)$ kaikilla $k \in \mathbb{N}$. Tämä on kuitenkin selvästi ristiriita, sillä astefunktion arvot kasvavat rajatta, joten luonnollisten lukujen joukko $\mathbb{N}$ ei riitä astefunktion maalijoukoksi. Näin ollen $\mathbb{Z} \times \mathbb{Z}$ ei ole euklidinen rengas.

Seuraus 3.11. *Rengas $\mathbb{Z} \times \mathbb{Z}$ ei ole euklidinen alue tai euklidinen rengas, mutta se on transfiniittinen euklidinen rengas.*

4 Pääideaalialue, joka ei ole euklidinen alue

Tässä luvussa esitellään eräs pääideaalirengas, joka ei ole euklidinen alue. Aikaisemmin lauseessa 2.3 on osoitettu, että jokainen euklidinen alue on pääideaalialue, mutta tässä luvussa todetaan, että tämä ei päde yleisesti toisinpäin. Luvussa esitellään Gaussin kokonaisluvuille määritetty astekuvaus, jota kutsutaan normiksi, sekä Dedekind-Hasse -normin. Näiden käsitteiden avulla osoitetaan, että kokonaislukurengas on pääideaalirengas, jos sillä on Dedekind-Hasse -normi. Lopuksi näytetään, että pääideaalirengas ei ole euklidinen alue sillä siinä ei ole universaaleja sivutekijöitä, jotka on osoitettu lauseessa 2.5 aina euklidisella alueella olevan.

Edellisessä luvussa on osoitettu, että kaikki euklidiset alueet ovat pääideaalialueita. Esitellään seuraavaksi esimerkki pääideaalirenkaasta, joka ei ole euklidinen alue. Tämä rengas on määritelty seuraavasti:

$$R = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] = \left\{a + b \cdot \frac{1+i\sqrt{19}}{2} \;\middle|\; a,b \in \mathbb{Z}\right\}$$

Kyseessä on siis kompleksilukujen osajoukko, jossa pätevät tavalliset yhteen- ja kertolaskun säännöt. Seuraavaksi läpikäytävä todistus pohjautuu pääasiassa tutkielman lähteeseen [8], mutta luonnollisesti tukena on käytetty aikaisemmin tutkielmassa läpikäytyä teoriaa.

Osoitetaan ensin, että R on pääideaalialue, jonka jälkeen osoitetaan, ettei se täytä euklidisen alueen ominaisuuksia. Aloitetaan määrittelmällä Dedekind-Hasse -normi.

Määritelmä 4.1. Olkoon R vaihdannainen rengas. *Dedekind-Hasse -normi* on funktio $N\colon\ R \to \mathbb{N}$, jolle pätee:

1. Kaikilla $a \in R$, $N(a) = 0$ pätee jos ja vain jos $a = 0_R$,
2. Kaikilla $a,b \in R$, $a,b \neq 0$, joko $b \mid a$ tai on olemassa $c,d \in R$, joille $0 < N(ac - bd) < N(b)$.

Esimerkki 4.2. Gaussin kokonaisluvuille määriteltyä astekuvausta kutsutaan yleisesti *normiksi*

$$N\colon\ \mathbb{Z}[i] \to \mathbb{N},\ N(a+bi) = (a+bi)(a-bi) = a^2 + b^2.$$

Normi N on siis Gaussin kokonaisluvun ja sen kompleksikonjugaatin tulo.

Lause 4.3. *Olkoon R vaihdannainen rengas. Rengas R on pääideaalirengas, jos sillä on Dedekind-Hasse -normi.*

Todistus. Olkoon I epätriviaali R:n ideaali. Merkitään, että
$m = \min\{N(t) \mid t \in I, t \neq 0\}$. Valitaan sitten $y \neq 0$ siten, että $N(y) = m$, $y \in I$.

Olkoon $x \in I$. Osoitetaan, että $y \mid x$. Tämä on selvää, jos $x = 0$, joten oletetaan nyt, että $x \neq 0$ ja $N(y) \leq N(x)$. Tehdään vastaoletus, että $y \nmid x$, tällöin on olemassa w ja z siten, että $0 < N(xz - yw) < N(y)$ ja $xz - yw \in I$, mutta koska $N(y) = m$ on minimaalinen niin ei voi olla $N(xz - yw) < N(y)$. Tämä on siis ristiriita. Näin ollen $y \mid x$ ja $x \in I$. □

Lause 4.4. *Rengas $R = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ on pääideaalirengas.*

Todistus. Merkitään, että $\alpha = \frac{1+i\sqrt{19}}{2}$. Olkoon renkaan R normi tyypillinen kompleksiluvun itseisarvon neliö $N\colon R \to \mathbb{N},\ N(x + y\alpha) = |x + y\alpha|^2$. Nyt

$$\begin{aligned}
|x + y\alpha|^2 &= \left(x + \frac{y}{2}\right)^2 + \left(\frac{y\sqrt{19}}{2}\right)^2 \\
&= \left(x + \frac{y}{2}\right)^2 + \frac{19y^2}{4} \\
&= x^2 + xy + \frac{y^2}{4} + \frac{19y^2}{4} \\
&= x^2 + xy + 5y^2.
\end{aligned}$$

Oletetaan, että $x, y \in R$ ja $y \nmid x$. Osoitetaan, nyt että $\mathbb{Z}[\alpha]$ on pääideaalirengas, koska se toteuttaa Dedekind-Hasse -normin. Näytetään, että kaikilla x,$y \in R$ on olemassa z,$w \in R$, joille pätee $0 < N(xz - yw) < N(y)$. Havaitaan, että $0 < N(xz - yw) < N(y) \Leftrightarrow 0 < N\left(\frac{x}{y}z - w\right) < 1$.

Todistus etenee tapaustarkastelulla. Jokaisessa tapauksessa z ja w valitaan omalla tavallaan. Tunnetusti renkaan $\mathbb{Z}[\alpha]$ jakokunta on $\mathbb{Q}[\alpha]$, sillä

$$\alpha + \bar{\alpha} = \frac{1 + i\sqrt{19}}{2} + \frac{1 - i\sqrt{19}}{2} = \frac{1 + 1 + i\sqrt{19} - i\sqrt{19}}{2} = 1$$

ja

$$\alpha \cdot \bar{\alpha} = \left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{19}}{2}\right)^2 = \frac{1}{4} + \frac{19}{4} = 5.$$

Merkitään, että $\frac{x}{y} = \frac{a+bi\sqrt{19}}{c}$, missä $c \neq 1$ ja $\mathrm{syt}(a, b, c) = 1$. Tällöin on olemassa alkiot $e, d, f \in \mathbb{Z}$, joille $ae + bd + cf = 1$.

- Tarkastellaan ensin tapausta $c \geq 5$. Asetetaan, että $ad - 19be = cq + r$. Jakoalgoritmin nojalla voidaan valita $q, r \in \mathbb{Z}$ niin, että $|r| \leq \frac{c}{2}$. Huomiona, että tapaustarkastelun erivaiheissa q ja r valitaan omalla tavallaan ja valinta liittyy oletukseen $c \geq 5$.

  Olkoot nyt $z = d + ei\sqrt{19}$ ja $w = q - fi\sqrt{19}$. Saadaan, että

$$\begin{aligned}
\frac{x}{y}z - w &= \frac{a + bi\sqrt{19}}{c} \cdot \left(d + ei\sqrt{19}\right) - \left(q - fi\sqrt{19}\right) \\
&= \frac{\left(a + bi\sqrt{19}\right)\left(d + ei\sqrt{19}\right)}{c} - q + fi\sqrt{19} \\
&= \frac{ad - 19eb + i\sqrt{19}ae + i\sqrt{19}bd}{c} - \frac{cq + cfi\sqrt{19}}{c} \\
&= \frac{ad - 19be + i\sqrt{19}ae + i\sqrt{19}bd - cq + i\sqrt{19}cf}{c} \\
&= \frac{ad - 19be - cq}{c} + \frac{i\sqrt{19}\,(ae + bd + cf)}{c}.
\end{aligned}$$

  Koska $ae + bd + cf = 1$ ja $ad - 19be = cq + r \;\Leftrightarrow\; ad - 19be - cq = r$, jossa $|r| < \frac{c}{2}$, niin

$$\frac{x}{y}z - w = \frac{r}{c} + \frac{\sqrt{19}}{c}i.$$

  Edelleen $N\left(\frac{x}{y}z - w\right) = \frac{r^2}{c^2} + \frac{19}{c^2}$. Koska $|r| < \frac{c}{2} \Leftrightarrow \frac{|r|}{c} < \frac{1}{2}$, niin $N\left(\frac{x}{y}z - w\right) \leq \frac{1}{4} + \frac{19}{c^2} < 1$, kun $c \geq 6$.

  Jos $c = 5$, niin $r \leq 2$ ja saadaan

$$N\left(\frac{x}{y}z - w\right) = \frac{r^2}{c^2} + \frac{19}{c^2} \leq \frac{4}{25} + \frac{19}{25} < 1.$$

Käydään seuraavaksi vielä läpi tapaukset $c = 2, 3$ ja 4.

- Kun $c = 2$: Asetetaan nyt $z = 1$ ja $w = \frac{(a-1)+bi\sqrt{19}}{2}$. Tarkastetaan, että z ja w ovat renkaassa R.

$$\begin{aligned}\frac{(a-1)+bi\sqrt{19}}{2} &= \frac{a-1}{2} + \frac{b}{2}i\sqrt{19} \\ &= \frac{a-1}{2} + \left(\frac{b}{2}i\sqrt{19} + \frac{b}{2}\right) - \frac{b}{2} \\ &= \frac{a-1-b}{2} + \frac{b}{2}\left(1+i\sqrt{19}\right) \\ &= \frac{a-b-1}{2} + b\alpha.\end{aligned}$$

Koska $c = 2$, $y \nmid x$ ja $syt(a,b,c) = 1$, niin lukujen a ja b on oltava eri pariteettia. Näin ollen $2 \mid (a-b-1)$ ja $\frac{a-b-1}{2} + b\alpha \in R$. Tällöin

$$\frac{x}{y}z - w = \frac{a+bi\sqrt{19}}{2} - \left(\frac{(a-1)+bi\sqrt{19}}{2}\right) = \frac{1}{2}.$$

Siis $N\left(\frac{x}{y}z - w\right) = N\left(\frac{1}{2}\right) < 1$.

- Kun $c = 3$: Valitaan $z = a - bi\sqrt{19}$. Tällöin

$$\frac{x}{y}z - w = \left(\frac{a+bi\sqrt{19}}{3}\right) \cdot \left(a - bi\sqrt{19}\right) - w = \frac{a^2+19b^2}{3} - w.$$

Koska $c = 3$ ja $syt(a,b,c) = 1$, niin $a^2 + 19b^2 \equiv a^2 + b^2 \not\equiv 0 \pmod 3$. Merkitään nyt, että $a^2 + 19b^2 = 3q + r$, missä $r = 1$ tai $r = 2$ ja $w = q$. Siis

$$\frac{x}{y}z - w = \frac{a^2+19b^2}{3} - q = \frac{3q+r}{3} - q = q + \frac{r}{3} - q = \frac{r}{3}.$$

Nyt, koska $r = 1$ tai $r = 2$, niin $\frac{r}{3} \neq 0$ ja edelleen $N(\frac{r}{3}) < 1$.

- Kun $c = 4$: Oletetaan ensin, että luvut a ja b ovat eri pariteettia. Valitaan, että $z = a - bi\sqrt{19}$. Tällöin

$$\frac{x}{y}z - w = \left(\frac{a+bi\sqrt{19}}{4}\right) \cdot \left(a - bi\sqrt{19}\right) - w = \frac{a^2+19b^2}{4} - w.$$

Koska a ja b ovat eri pariteettia, niin $a^2 + 19b^2 \not\equiv 0 \,(mod\ 4)$. Merkitään nyt, että $a^2 + 19b^2 = 4q + r$, missä $0 < r < 4$ ja $w = q$. Siis

$$\frac{x}{y}z - w = \frac{a^2+19b^2}{4} - q = \frac{4q+r}{4} - q = q + \frac{r}{4} - q = \frac{r}{4}.$$

Nyt, koska $0 < r < 4$, niin $\frac{r}{4} \neq 0$ ja edelleen $N(\frac{r}{4}) < 1$.

Oletetaan sitten, että a ja b ovat molemmat parittomia. Valitaan nyt $z = \frac{a-bi\sqrt{19}}{2}$ ja edelleen $w = q$. Tällöin

$$\frac{x}{y}z - w = \left(\frac{a + bi\sqrt{19}}{4}\right) \cdot \left(\frac{a - bi\sqrt{19}}{2}\right) - q = \frac{a^2 + 19b^2}{8} - q.$$

Koska nyt a ja b ovat molemmat parittomia, niin $a^2 + 19b^2 \not\equiv 0\,(mod\,8)$. Merkitään nyt, että $a^2 + 19b^2 = 8q + r$, missä $0 < r < 8$. Siis

$$\frac{x}{y}z - w = \frac{a^2 + 19b^2}{8} - q = \frac{8q + r}{8} - q = q + \frac{r}{8} - q = \frac{r}{8}.$$

Nyt, koska $0 < r < 8$, niin $\frac{r}{8} \neq 0$ ja edelleen $N(\frac{r}{8}) < 1$.

Näin on osoitettu, että $R = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ on pääideaalialue. □

Edellisessä lauseessa 2.5 osoitettiin, että euklidisessa alueessa on ainakin yksi universaali sivutekijä. Kokonaisulukujen renkaassa ainoat universaalit sivutekijät ovat ± 2 ja ± 3. Luku 2 on universaali sivutekijä, koska jokainen kokonaisluku on joko monikerta luvusta 2 tai eroaa yhdellä luvun 2 monikerrasta. Luku on vastaavasti 3 universaali sivutekijä, koska jokainen kokonaisluku on joko 0, 1 tai -1 modulo luvusta 3. Mille tahansa kokonaisluvulle n, jonka itseisarvo on suurempi kuin 3, ei ole mahdollista vähentää yksikköä tai nollaa luvusta 2 saadakseen monikerran luvusta n.

Osoitetaan seuraavaksi, että jos $a \in \mathbb{Z}[\alpha]$ on universaali sivutekijä, niin sille pätee $a \mid 2$ tai $a \mid 3$ euklidisessa alueessa $\mathbb{Z}[\alpha]$.

Lemma 4.5. Olkoon $\alpha \in \mathbb{C}$. Oletetaan, että $\mathbb{Z}[\alpha]$ on euklidinen alue, jonka yksiköt ovat ± 1. Jos $a \in \mathbb{Z}[\alpha]$ on universaali sivutekijä, niin $a \mid 2$ tai $a \mid 3$.

Todistus. Olkoon nyt siis $a \in \mathbb{Z}[\alpha]$ universaali sivutekijä. Voidaan olettaa, että $a \nmid 2$, tällöin $a \mid 2 - 1 = 1$, jolloin a olisi yksikkö (vastoin oletusta) tai $a \mid 2 - (-1) = a \mid 3$. □

On osoitettu, että jokaisessa euklidisessa alueessa on ainakin yksi universaali sivutekijä a ja renkaassa $\mathbb{Z}[\alpha]$ pätee, että $a \mid 2$ tai $a \mid 3$. Osoitetaan seuraavaksi, että rengas R ei ole euklidinen, sillä 2 ja 3 eivät ole jaollisia renkaassa.

Lause 4.6. *Luvut* 2 *ja* 3 *ovat jaottomia renkaassa* $\mathbb{Z}[\alpha] = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$.

Todistus. Oletetaan nyt, että $2 = (a + b\alpha)\,(c + d\alpha)$, missä $a,b,c,d \in \mathbb{Z}$. Tällöin

$$2^2 = 4 = |a + b\alpha|^2\,|c + d\alpha|^2\,,$$

joten oltava $|a + b\alpha|^2, |c + d\alpha|^2 = 2$ tai $\left\{|a + b\alpha|^2, |c + d\alpha|^2\right\} = \{1,4\}$.

Koska $|a + b\alpha|^2 > 2$ pätee, jos ja vain jos $a + b\alpha$ ei ole yksikkö ja jälkimmäisessä tapauksessa $a + b\alpha$ tai $c + d\alpha$ on yksikkö, joten 2 on oltava jaoton renkaassa $\mathbb{Z}[\alpha]$.

Vastaavasti voidaan osoittaa, että 3 on jaoton renkaassa $\mathbb{Z}[\alpha]$. □

Näin todistus on päättynyt ja on osoitettu, että rengas R on pääideaalialue, mutta ei euklidinen alue.

Seuraus 4.7. *Rengas* $R = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ *on pääideaalialue, mutta ei euklidinen alue.*

Lähteet

[1] Fraleigh, J. B. *A First Course in Abstract Algebra*, kolmas laitos. Pearson, 2014.

[2] Luosto, Kerkko. *Renkaat ja kunnat*. Luentomoniste, syksy 2022.

[3] Malik, D. S. & Mordeson, J. M & Sen, M. K. *Fundamentals of Abstract Algebra*. The McGraw-Hill Companies, Inc., 1997.

[4] Nagata, M. S. *On the Definition of a Euclid Ring*. Commutative Algebra and Combinatorics, pp. 167-171, 1987.

[5] Rotman, Joseph. J. *A First Course in Abstract Algebra*, kolmas laitos. Education Inc, 2006.

[6] Rotman, Joseph. J. *Advanced Modern Algebra*, ensimmäinen laitos. Prentice Hall, 2002.

[7] Pierre, Samuel. *About Euclidean Rings*. Journal of Algebra 19, (August, 1970) pp. 282-301, 1971.

[8] Wilson, Jack C. *A Principal Ideal Ring That Is Not a Euclidean Ring*. Mathematics Magazine, Vol. 46, No 1 (January, 1973) pp. 34-38, 2011.