Algebrallista lukuteoriaa: Pellin yhtälöstä ja aritmetiikan peruslauseen yleistämisestä

Jenna Ojaniemi

Matematiikan pro gradu -tutkielma

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kesäkuu 2019

JYVÄSKYLÄN YLIOPISTO

Tutkielman nimi
Algebrallista lukuteoriaa: Pellin yhtälöstä ja aritmetiikan peruslauseen yleistämisestä.
Algebraic number theory. Pell's equation and the fundamental theorem of arithmetic.

Tiedekunta	**Laitos**
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen laitos

Tekijä
Jenna Ojaniemi

Opintosuunta	**Työn laji**
Matematiikan aineenopettaja	Matematiikan pro gradu -tutkielma (20 op)
Aika	**Sivumäärä**
Kesäkuu 2019	65

Tiivistelmä

Tutkielman tarkoituksena on Pellin yhtälön ratkaiseminen ja aritmetiikan peruslauseen voimassaolon tutkiminen algebrallisten kokonaislukujen muodostamissa renkaissa $\mathbb{Z}[\sqrt{-2}], \mathbb{Z}[\sqrt{-3}], \mathbb{Z}[\sqrt{\zeta_3}]$ ja $\mathbb{Z}[\sqrt{-5}]$. Aritmetiikan peruslauseella tarkoitetaan yleisimmin positiivisten kokonaislukujen yksikäsitteistä alkulukuhajotelmaa. Pellin yhtälön ratkaisussa käytetyt tavat käsitellä algebrallisia kokonaislukuja ovat apuna aritmetiikan peruslauseen yleistämisessä muihin lukuluokkiin. Tutkielmassa tutustutaan myös ketjumurtolukujen tarjoamaan ratkaisualgoritmiin Pellin yhtälölle. Lisäksi tutkielmassa käsitellään ideaalien teoriaa, sillä jos varsinaista määritelmän mukaista yksikäsitteistä tekijöihinjakoa ei pystytä renkaalle yleistämään, voidaan alkutekijähajotelmaa tarkastella alkuideaalien avulla.

Tutkielmassa aloitetaan algebran ja lukuteorian kurssilla käsitellyistä määritelmistä ja edetään asteittain vaativampiin algebrallisiin rakenteisiin. Tutkielmassa käytetään kuvia ja geometriaa algebrallisten todistusten rinnalla. Lisäksi perehdytään hieman käsiteltävien aiheiden historiaan sekä tietokonelaskemiseen. Tutkielman kahdessa ensimmäisessä luvussa käydään läpi tutkielman kannalta tärkeitä tuloksia ja esitetään aritmetiikan peruslauseen todistus positiivisilla kokonaisluvuilla. Kolmas luku käsittelee Pellin yhtälöä ja neljäs luku aritmetiikan peruslauseen yleistämistä. Viidennessä luvussa tutkitaan yksikäsitteisen tekijöihinjaon epäonnistumista ja perehdytään ideaaleihin.

Tuloksena saadaan yksikäsitteisen tekijöihinjaon onnistuminen renkaissa $\mathbb{Z}[\sqrt{-2}]$ ja $\mathbb{Z}[\zeta_3]$. Yksikäsitteinen tekijöihinjako epäonnistuu renkaissa $\mathbb{Z}[\sqrt{-3}]$ ja $\mathbb{Z}[\sqrt{-5}]$. Toisaalta renkaalle $\mathbb{Z}[\sqrt{-5}]$ voidaan määrittää alkutekijähajotelma käyttäen alkuideaaleja, ja alkutekijähajotelma on yksikäsitteinen.

Avainsanat
Aritmetiikan peruslause, algebrallisten kokonaislukujen muodostama rengas, Eukleideen alue, ideaali, jakoyhtälö, Pellin yhtälö, pääideaalialue

Säilytyspaikka
JYX

Sisältö

Johdanto

Algebrassa on perinteisesti tavoitteena etsiä ratkaisuja yhtälöille ja kehittää metodeja, joilla erilaisia yhtälöitä voidaan ratkaista. Algebran yksi tunnetuimmista tutkimussuunnista on kokonaislukuratkaisujen etsiminen yhtälöille, mikä on myös yksi klassisen lukuteorian tärkeimmistä tutkimuskohteista. Tämän tutkielman aihe sijoittuu algebran ja lukuteorian välimaastoon, mitä yliopistokursseilla tarkastellaan vain vähän. Vaikka laskujen pohjana ovatkin kokonaisluvut, vaativat ongelmat muidenkin lukuluokkien, kuten esimerkiksi kompleksilukujen, mukaan ottamista. Tutkielman pohjana toimii lukion pitkästä matematiikastakin tuttu aritmetiikan peruslause. Lukiotasolla todistus tehdään joko luonnollisten lukujen tai kokonaislukujen joukossa. Tässä tutkielmassa lähdetään siitä, mihin lukion kursseilla ollaan jääty ja mitä yliopiston ensimmäisillä kursseilla on esitelty. Tutkielman tavoitteena on kuitenkin kuljettaa lukija asteittain algebrallisen lukuteorian maailmaan aloittamalla yksinkertaisista määritelmistä ja rakenteista edeten haastavampiin tuloksiin.

Tutkielman tavoitteena on aritmetiikan peruslauseen yleistäminen tiettyjen algebrallisten kokonaislukujen muodostamiin renkaisiin ja ratkaisun yksikäsitteisyyden tutkiminen. Tutkielmassa käytetään Diofantoksen yhtälöiden ratkaisumenetelmiä apuna ja tutustutaan tarkemmin Pellin yhtälön ratkaisujen etsimiseen jakoyhtälön avulla. Ideat, joita käytetään Pellin yhtälön ratkaisussa, voidaan yhdistää moniin muihin algebrallisen lukuteorian ajatuksiin, ja niitä voidaan käyttää apuna aritmetiikan peruslauseen yleistyksessä. Monimutkaisemmalla tasolla algebrallisten ajatuksien hyödyntäminen osoittaa, että aritmetiikan peruslause voidaan yleistää tietyille algebrallisten kokonaislukujen muodostamille renkaille. Osassa renkaista yleistys onnistuu, mutta osassa se epäonnistuu. Epäonnistumista yritetään korjata eri tavoin renkaasta riippuen, mikä kuljettaakin lukijan ideaali-käsitteen syntyhistoriaan ja käyttöönottoon.

Yleensä termeillä ”alkuluku” ja ”alkutekijä” tarkoitetaan kokonaisluvun tekijää, joka on alkuluku. Tässä tutkielmassa kutsutaan alkuluvuiksi määritelmän mukaisia alkulukuja (esimerkiksi 3 ja 7). Käsitettä ”alkutekijä” käytetään tarkasteltaessa sellaisia tekijöitä, jotka eivät ole kokonaislukuja, mutta käyttäytyvät kuten alkuluvut. Alkuideaalit määritellään luvussa 5.

Tutkielmassa lähestytään asioita algebrallisesta näkökulmasta, mutta siihen on pyritty ottamaan mukaan geometrisia piirteitä havainnollistamaan aihealueita. On todettu, että ihmisten matematiikan oppiminen voidaan jakaa karkeasti geometriseen ja algebralliseen oppimiseen. Osa oppii helpommin kuvien kautta, kun taas osa suoraviivaisemmin algebrallisella tavalla laskemalla ja kaavojen kautta. Päälähteinä tutkielmassa on käytetty John Stillwellin kirjaa Elements of Number Theory, Godfrey Harold Hardyn ja Edward Maitland Wrightin kirjaa An Introduction to Theory of Numbers sekä John Beachyn ja William Blairin kirjaa Abstract Algebra.

1. Aritmetiikan perusteita

Tässä luvussa esitellään aritmetiikan peruslauseen todistus positiivisten kokonaislukujen joukossa sekä muita tärkeitä määritelmiä, joita tarvitaan myöhemmissä vaiheissa tätä tutkielmaa. Tässä luvussa esitellään myös *Eukleideen algoritmi* ja näytetään miten sitä voi käyttää työkaluna tutkittaessa lukujen irrationaalisuutta. Tämän luvun tuloksissa ja todistuksissa on seurattu lähteitä [5], [6] ja [7].

Lause 1 (**Hyvinjärjestysominaisuus**)**.** *Jokaisella epätyhjällä luonnollisten lukujen osajoukolla on pienin alkio.*

Todistus. Käytetään epäsuoraa todistusta ja induktiota väitteen todistamiseksi. Oletetaan, että joukolla A ei ole pienintä alkiota. Tällöin $n = 1 \notin A$, joten alkuaskel toteutuu. Olkoon induktio-oletus $1, 2, ..., n \notin A$ ja induktioväite $1, 2, ..., n + 1 \notin A$. Induktio-oletuksesta seuraa, että $1, 2, ..., n \notin A$. Jos $n + 1 \in A$, niin $n + 1$ olisi joukon A pienin alkio, mikä on ristiriidassa oletuksen kanssa. Tästä seuraa, että joukolla A ei ole pienintä alkiota ja A on tyhjä joukko. Tämä osoittaa alkuperäisen väitteen todeksi. □

Lause 2 (**Jakoyhtälö**)**.** *Olkoot a ja $b > 0$ kokonaislukuja. Tällöin on olemassa kokonaisluvut q ja r siten, että*

$$a = bq + r \text{ ja } 0 \leq r < b. \tag{1}$$

Luvut q ja r ovat yksikäsitteiset: jos parit (q_1, r_1) ja (q_2, r_2) toteuttavat ehdon (1) samoilla luvuilla a ja b, niin $q_1 = q_2$ ja $r_1 = r_2$.

Todistus. Olkoot $a, b \in \mathbb{Z}$ siten, että $b > 0$. Osoitetaan ensin, että luvut q ja r ovat olemassa. Olkoon

$$A = \{a - bx : x \ \in \mathbb{Z}, a - bx \geq 0\}.$$

Voidaan todeta, että joukko A on epätyhjä. Valitaan $x = -|a|$ ja oletuksen mukaan $b \geq 1$. Tällöin

$$a - bx = a + b|a| \geq -|a| + b|a| = |a|(b - 1) \geq 0.$$

Koska joukko A koostuu vain ei-negatiivisista kokonaisluvuista, se sisältää pienimmän alkion (lause 1). Olkoon tämä pienin alkio $r = a - bq \in A$ ja $r \geq 0$. Osoitetaan, että $r < b$ tekemällä antiteesi: Olkoon $r \geq b$ ja tällöin

$$a - bq = r \geq b,$$

joten siis

$$r' = a - b(q + 1) \geq 0.$$

Nyt $r' \in A$ ja $r' < r$, koska tiedetään, että $b > 0$. Tästä seuraa ristiriita, sillä r on joukon A pienin alkio. Tämä todistaa lukujen q ja r olemassaolon.

Tarkistetaan vielä, että yksikäsitteisyys on voimassa. Oletetaan, että

$$a = bq_1 + r_1 = bq_2 + r_2, \text{ kun } q_1, q_2, r_1, r_2 \in \mathbb{Z} \text{ ja } 0 \leq r_1, r_2 < b,$$

mistä seuraa

$$bq_1 + r_1 = bq_2 + r_2$$
$$b(q_1 - q_2) = r_1 - r_2.$$

Jos $q_1 = q_2$, niin seuraisi, että myös $r_1 = r_2$. Jos $q_1 \neq q_2$, niin $|q_2 - q_1| \geq 1$, mistä seuraisi $|r_1 - r_2| \geq b$. Verrataan saatua tulosta alun oletukseen $0 \leq r_1, r_2 < b$ ja oletetaan lisäksi $r_2 > r_1$, jolloin saadaan

$$|r_1 - r_2| = r_2 - r_1 < b - r_1 \leq b - 0 = b,$$

missä $q_1 = q_2$ ja $r_1 = r_2$. Päädytään ristiriitaan, mikä todistaa yksikäsitteisyyden. □

Määritelmä 3. Olkoot a ja $b \neq 0$ kokonaislukuja. Kun luku b jakaa luvun a, niin $a = bc$, jollain $c \in \mathbb{Z}$. Lukua b kutsutaan luvun a **jakajaksi** tai **tekijäksi**. Tällöin merkitään $b \mid a$. Jos b ei jaa lukua a merkitään $b \nmid a$.

Määritelmä 4. Kokonaislukujen a ja b **suurin yhteinen tekijä** on suurin kokonaisluku d, joka jakaa sekä luvun a että luvun b, kun ainakin toinen luvuista a tai b on nollasta poikkeava. Lukujen a ja b suurinta yhteistä tekijää merkitään $\text{syt}(a, b)$. Jos

$$\text{syt}(a, b) = 1$$

sanotaan, että luvut a ja b ovat *keskenään jaottomia*.

Lause 5. *Olkoot a ja b kokonaislukuja, joista ainakin toinen nollasta poikkeava. Tällöin on olemassa kokonaisluvut x ja y siten, että*

$$\text{syt}(a, b) = ax + by. \tag{2}$$

Todistus. Olkoon $\text{syt}(a, b) = d$. Merkitään

$$A = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}.$$

Valitaan $a = x$ ja $b = y$, jolloin yhtälö tulee muotoon

$$a^2 + b^2 > 0.$$

Tästä nähdään, että joukko on epätyhjä joukko, joka koostuu luonnollisista luvuista. Tiedetään, että joukolla A on pienin alkio (lause 1). Merkitään pienintä alkiota $t = ax + by$ (> 0). Osoitetaan, että luku t täyttää ehdon $t = d = \text{syt}(a, b)$.

Aloitetaan osoittamalla, että $t \mid a$. Jakoyhtälön (lause 2) nojalla on olemassa luvut $q, r \in \mathbb{Z}$ ja $0 \leq r < t$ siten, että $a = tq + r$. Jos $r > 0$, niin

$$r = a - tq = a - (ax + by)q = a(1 - xq) - b(yq) \ \in \ A.$$

Nyt $r < t$, mistä seuraa ristiriita, sillä luku t on joukon pienin alkio. Tällöin siis täytyy olla $r = 0$ ja $a = tq$, jollain $q \in \mathbb{Z}$. Saadaan $t \mid a$, mikä haluttiinkin osoittaa. Vastaavalla päättelyllä saataisiin myös $t \mid b$.

Osoitetaan vielä, että t on jakajista suurin. Olkoon $c \in \mathbb{Z}$ siten, että $c \mid a$ ja $c \mid b$. Näytetään, että $c \mid t$:

$$t = ax + by = (ck)x + (cs)y = ckx + csy = c(kx + sy), \text{ jollain } k, s \in \mathbb{Z}.$$

Tästä huomataan, että $c \mid t$, joten täytyy olla $c \leq t$. Tämä osoittaa, että $\text{syt}(a, b) = t$, mikä todistaa väitteen. □

Seuraavat väitteet on helppo todistaa aiempien tulosten avulla.

Seuraus 6.

(1) *Jos* $c \mid a$ *ja* $c \mid b$, *niin* $c \mid \text{syt}\,(a, b)$.

(2) *Jos* $a \mid bc$ *ja* $\text{syt}\,(a, b) = 1$, *niin* $a \mid c$.

Todistus.

(1) Olkoon $\text{syt}\,(a, b) = ax + by$. Nyt jos $c \mid a$ ja $c \mid b$, niin $a = mc$ ja $b = nc$, joillain $n, m \in \mathbb{Z}$. Tällöin

$$ax + by = (mc)x + (nc)y = c(mx + ny),$$

joten väite on todistettu.

(2) Oletuksen nojalla on olemassa kokonaisluku s siten, että $bc = as$. Lauseen 5 nojalla on olemassa kokonaisluvut x ja y siten, että $1 = ax + by$. Kerrotaan yhtälön molemmat puolet luvulla c, mistä saadaan

$$c = cax + cby = cax + asy = a(cx + sy).$$

Tämä todistaa, että $a \mid c$.

□

Lause 7. *Yhtälöllä* $ax + by = c$ *on kokonaislukuratkaisu* (x, y), *jos ja vain jos* $\text{syt}(a, b) \mid c$.

Todistus.
"⇒": Oletetaan, että yhtälöllä $ax + by = c$ on kokonaislukuratkaisu (x, y). Halutaan osoittaa, että $\text{syt}(a, b) \mid c$. Tiedetään, että $\text{syt}(a, b) \mid a$ ja $\text{syt}(a, b) \mid b$, joten

$$\text{syt}(a, b) \mid ax + by = c.$$

"⇐": Oletetaan, että $\text{syt}(a, b) \mid c$, jolloin on olemassa kokonaisluku d siten, että $c = \text{syt}\,(a, b)d$. Lauseen 5 nojalla on olemassa kokonaisluvut x' ja y' siten, että $\text{syt}(a, b) = ax' + by'$. Saadaan

$$c = (ax' + by')d = a(x'd) + b(y'd),$$

ja siten yhtälölle $ax + by = c$ löytyy ratkaisut $x = x'd$, $y = y'd$.

□

1.1. **Alkuluvut.** Tässä luvussa määritellään, mitä alkuluvuilla tarkoitetaan ja millaisia ominaisuuksia niillä on positiivisten kokonaislukujen joukossa. Myöhemmässä vaiheessa tätä tutkielmaa huomataan, että myös muiden lukuluokkien alkutekijöillä on samoja ominaisuuksia. Käsitteellä alkutekijä yleensä tarkoitetaan kokonaislukua, joka on alkuluku. Tässä tutkielmassa käytetään käsitettä alkuluku, kun puhutaan alkutekijästä kokonaislukujen joukossa ja käsitettä alkutekijä muissa lukuluokissa. Pysytään kuitenkin vielä hetki kokonaislukujen käsittelyssä ja määritellään alkuluvut täsmällisesti ennen **aritmetiikan peruslauseen** esittelyä.

Määritelmä 8. Kokonaisluvun $p > 1$ sanotaan olevan **alkuluku**, jos se on jaollinen ainoastaan luvuilla 1 ja p.

Lause 9. *Olkoon p alkuluku. Jos $p \mid ab$, niin $p \mid a$ tai $p \mid b$.*

Todistus. Oletetaan, että alkuluku p jakaa luvun ab, mutta p ei jaa lukua a. Tästä seuraa, että lukujen a ja p suurin yhteinen tekijä on 1. Merkitään

$$1 = \text{syt}(a, p) = ax + py, \text{ joillain } x, y \in \mathbb{Z}.$$

Kertomalla molemmat puolet luvulla b saadaan

$$b = abx + pby.$$

Nyt huomataan, että p jakaa kaikki termit yhtälön oikealta puolelta. Oletuksen mukaan $p \mid ab$, joten täytyy olla myös $p \mid pby$. Tämä todistaa, että $p \mid b$. □

Lemma 10. *Jokainen kokonaisluku $n > 1$ voidaan esittää alkulukujen tulona siten, että*

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

missä luvut $p_1, p_2, ..., p_i$ ovat alkulukuja.

Todistus. Olkoon

$$A = \{n > 1 : n \text{ ei ole alkulukujen tulo}\}.$$

Tehdään antiteesi ja oletetaan, että A ei ole tyhjä joukko. Silloin joukolla A on pienin alkio $t > 0$. Koska t ei voi olla alkuluku, voidaan merkitä $t = ab$, kun $a, b \in \mathbb{Z}$ ja $a, b > 1$. Tällöin t on joukon A pienin alkio ja luvut a ja b ovat alkulukujen tuloja. Merkitään

$$a = p_1 p_2 \cdots p_r \quad \text{ja} \quad b = q_1 q_2 \cdots q_s.$$

Nyt kuitenkin huomataan, että

$$t = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s,$$

joten t voidaan esittää alkulukujen tulona. Tästä seuraa ristiriita, joka osoittaa alkuperäisen väitteen todeksi. □

Seuraus 11. *Jos p on alkuluku ja $p \mid (a_1 a_2 \cdots a_n)$, niin p jakaa ainakin yhden luvuista a_i.*

Todistus. Olkoon $b_1 = a_2 \cdots a_n$. Lauseen 9 nojalla tiedetään, että $p \mid a_1$ tai $p \mid b_1$ ja väite pätee selvästi kun $n = 2$. Oletetaan, että $p \nmid a_1$ ja $n \geq 3$. Jälleen käyttämällä samaa lausetta saadaan, että $p \mid a_2$ tai $p \mid b_2 = a_3 \cdots a_n$. Toistamalla operaatiota, väite todistuu viimeistään askeleen $n - 1$ jälkeen. □

1.2. **Aritmetiikan peruslause positiivisilla kokonaisluvuilla.**

Lause 12. *Jokainen kokonaisluku $n > 1$ voidaan esittää alkulukujen tulona*

$$n = p_1 p_2 ... p_r,$$

joka on järjestystä vaille yksikäsitteinen.

Todistus. Lemman 10 mukaan jokainen positiivinen kokonaisluku voidaan esittää alkulukujen tulona. Osoitettavaksi jää ainoastaan yksikäsitteisyys.

Merkitään

$$r = p_1p_2p_3...p_s \quad \text{ja} \quad r = q_1q_2q_3....q_t,$$

missä luvut p_i ja q_j ovat alkulukuja. Tulo on yksikäsitteinen, jos $s = t$ ja lukujen q_j järjestystä vaihtamalla saadaan

$$p_1 = q_1, \quad p_2 = q_2, \quad ... \quad , \quad p_r = p_s.$$

Muokataan luvun r ensimmäistä esitystä:

$$p_1p_2p_3...p_s = p_1(p_2p_3...p_s) = q_1q_2q_3....q_t.$$

Nyt seurauksen 11 nojalla luku p_1 jakaa jonkin luvuista q_j. Järjestystä vaihtamalla voidaan todeta, että

$$p_1 \mid q_1.$$

Oletuksen mukaan molemmat ovat alkulukuja, joten $p_1 = q_1$. Vaihtamalla lukujen q_j järjestystä ja jatkamalla käsittelyä saadaan $p_i = q_i$ kaikilla $i = 1, 2, ..., i$, kun $s = t$.

Osoitetaan vielä, että todella $s = t$. Tehdään vastaoletus $s \neq t$. Oletetaan, että $s > t$. Kun toistetaan aiempaa toimenpidettä t kertaa, jäljelle jää

$$p_{t+1}...p_s = 1.$$

Jokainen p_i jakaa luvun 1, kun $i \geq t + 1$. Tästä seuraa, että $p_i = 1$. Päädytään ristiriitaan, sillä luvut p_i ovat alkulukuja ja luku $p = 1$ ei ole alkuluku. Tilanne $s < t$ voitaisiin osoittaa vastaavasti. Tämä osoittaa yksikäsitteisyyden.

□

Seuraavasta esimerkistä huomataan, että yksikäsitteisen tekijöihinjaon avulla voidaan osoittaa lukujen irrationaalisuus.

Esimerkki 13. Osoitetaan, että $\sqrt{2}$ on irrationaaliluku näyttämällä, että ei ole olemassa kokonaislukuja m ja n siten, että $m^2 = 2n^2$.

Olkoot n ja m kokonaislukuja. Tutkitaan erikseen tilanteet, joissa alkulukuhajotelmassa on parillinen tai pariton määrä alkulukuja:

$$m = \underbrace{\pm a_1 \cdots a_n}_{\text{pariton määrä}} \Rightarrow m^2 = \underbrace{(a_1 \cdots a_n)(a_1 \cdots a_n)}_{\text{parillinen määrä}}$$

tai

$$m = \underbrace{\pm a_1 \cdots a_n}_{\text{parillinen määrä}} \Rightarrow m^2 = \underbrace{(a_1 \cdots a_n)(a_1 \cdots a_n)}_{\text{parillinen määrä}}.$$

Vastaavanlaisella päättelyllä saadaan selville, että myös luvun n^2 alkutekijöiden määrä on parillinen. Kun yhtälön oikealle puolelle lisätään kerroin 2, yhtälön vasemmalle puolelle tulee parillinen määrä ja yhtälön oikealle puolelle pariton määrä tekijöitä. Tästä seuraa ristiriita, mikä todistaa, että ei ole olemassa kokonaislukuja m ja n, jotka toteuttaisivat yhtälön $m^2 = 2n^2$. Yhtälö voitaisiin myös muokata muotoon

$$m^2 = 2n^2 \Rightarrow 2 = \frac{m^2}{n^2},$$

ja todeta ettei luku $\sqrt{2}$ ole rationaaliluku.

1.3. **Kongruenssin määritelmät.** Määritellään kongruenssi, kuten se tehdään lukuteoriassa. Kongruenssit liittyvät olennaisesti jakoyhtälöön, sillä jakoyhtälön avulla voidaan määrittää kongruenssi kahden kokonaisluvun välille. Toisin sanoen kongruenssit ovat tapa merkitä jakoyhtälöä ja siihen liittyvää jakojäännöstä. Myöhemmin määritellään kongruenssi ideaaleille (katso 5.5.1). Kongruenssien avulla voidaan löytää myös luvun a käänteisalkio m käyttäen apuna tietoa $\text{syt}\,(a,b) = ma + nb$.

Määritelmä 14. Olkoot a, b, n kokonaislukuja, $n > 0$. Sanotaan, että luku a on kongruentti luvun b kanssa modulo n, jos n jakaa luvun $a - b$. Merkitään

$$a \equiv b \pmod{n}.$$

Luku a on siis kongruentti luvun b kanssa modulo n, jos on olemassa $k \in \mathbb{Z}$ siten, että $a - b = kn$.

Määritelmä 15. Olkoot a ja $n > 0$ kokonaislukuja. Luvun a jäännösluokkaa modulo n merkitään

$$[a]_n = \{nk + a : k \in \mathbb{Z}\}.$$

Jäännösluokka on siis niiden kokonaislukujen joukko, jotka ovat kongruentit luvun a kanssa modulo n.

Lause 16. *Olkoon p alkuluku. Jos $a \not\equiv 0 \pmod{p}$, niin on olemassa luku $b \in \mathbb{Z}$ siten, että*

$$ab \equiv 1 \pmod{p}.$$

Todistus. Ehdoista p on alkuluku ja $a \not\equiv 0 \pmod{p}$ seuraa, että $syt(a,p) = 1$. Nyt lauseen 5 nojalla

$$ma + np = 1, \text{ joillain } m, n \in \mathbb{Z}.$$

Toisin sanoen

$$ma \equiv 1 \pmod{p},$$

ja m on luvun a käänteisalkio modulo p.

□

Sanotaan, että jokaisella $a \not\equiv 0 \pmod{p}$ on multiplikatiivinen käänteisalkio modulo p.

Esimerkki 17. Olkoon $p = 7$. Tällöin

- 1:n käänteisalkio 1,
- 2:n käänteisalkio 4,
- 3:n käänteisalkio 5,
- 4:n käänteisalkio 2,
- 5:n käänteisalkio 3,
- 6:n käänteisalkio 6.

1.4. **Eukleideen algoritmi.** Eukleideen algoritmi on tärkeä työkalu muihin sovelluksiin. Esimerkiksi tässä tutkielmassa käytetään Eukleideen algoritmia Pellin yhtälön ratkaisujen selvittämisessä ja myöhemmin samoja ajatuksia käytetään aritmetiikan peruslauseen yleistyksessä. Eukleideen algoritmin avulla saadaan etsittyä kokonaisluvut x ja y yhtälöstä $ax + by = \text{syt}(a,b)$ (kaava (2)).

Oletetaan, että $a \geq b > 0$. Jakamalla luku a luvulla b saadaan

$$a = q_1 b + r_2,$$

jossa $0 \leq r_2 < b$. Jos $r_2 \neq 0$, toistetaan jako uudelleen. Saadaan

$$b = q_2 r_2 + r_3,$$

jossa $0 \leq r_3 < r_2$. Jos jakojäännös $r_2 \neq 0$ jatketaan prosessia ja saadaan

$$r_2 = q_3 r_3 + r_4,$$

jossa $0 \leq r_4 < r_3$ ja niin edelleen. Prosessia jatketaan niin kauan, kunnes jakojäännökseksi jää 0. Olkoon $a = r_0$ ja $b = r_1$. Tällöin

$$\begin{cases} r_0 = q_1 r_1 + r_2, & (0 < r_2 < r_1) \\ r_1 = q_2 r_2 + r_3, & (0 < r_3 < r_2) \\ r_2 = q_3 r_3 + r_4, & (0 < r_4 < r_3) \\ \quad \vdots & \\ r_{n-2} = q_{n-1} r_{n-1} + r_n & (0 < r_n < r_{n-1}) \\ r_{n-1} = q_n r_n + r_{n+1}, & \end{cases}$$

ja sovitaan, että $r_{n+1} = 0$. Tällaista ”yhtälön järjestämistä” kutsutaan **Eukleideen algoritmiksi**, ja jakojäännös $r_n = \text{syt}(a, b)$.

Esimerkki 18. Eukleideen algoritmi luvuille 112 ja 26

$$\begin{aligned} 112 &= 4 \cdot 26 + 8 \\ 26 &= 3 \cdot 8 + 2 \\ 8 &= 4 \cdot 2. \end{aligned}$$

Saadaan $\text{syt}(112, 26) = 2$ ja kertoimet x ja y löydetään laskemalla:

$$\begin{aligned} \text{syt}\,(112, 26) &= 2 \\ &= 26 - 3 \cdot 8 \\ &= 26 - (3 \cdot (112 - 4 \cdot 26)) \\ &= 26 - 3 \cdot 112 + 12 \cdot 26 \\ &= 13 \cdot 26 - 3 \cdot 112. \end{aligned}$$

Tietokoneella saadaan laskettua helposti ja nopeasti myös vaikeampia esimerkkejä. WxMaximan komento IGCDEX(a, b) palauttaa listan $[x, y, c]$, jossa c on lukujen suurin yhteinen tekijä ja x ja y ovat kokonaislukuja, jotka toteuttavat yhtälön $ax+by = c$. Komento GCDEX toimisi tässä tilanteessa samalla tavalla, sillä käsittelyssä on kokonaisluvut. Komento GCDEX hyväksyy myös muita lukuja, kuten esimerkiksi polynomeja. Seuraavan esimerkin ensimmäisessä vaiheessa tarkistetaan ensin yläpuolella oleva lasku ja sen jälkeen esitetään kaksi esimerkkiä isommilla luvuilla.

Esimerkki 19. Eukleideen algoritmi wxMaximalla

```
(% i1)  load("gcdex")$
(% i2)  igcdex(112,26);
(% o2)                          [-3, 13, 2]
```

```
(% i3)  igcdex(6547,6000);
```

$$(\%\ o3) \qquad [-2117, 2310, 1]$$

```
(% i4)  igcdex(1526757668, 7835626735733);
```

$$(\%\ o4) \qquad [-1080356577169, 210505521, 1]$$

```
(% i5)  -1080356577169*1526757668+210505521*7835626735733;
```

$$(\%\ o5) \qquad 1$$

1.4.1. ***Laajennettu Eukleideen algoritmi.*** Laajennetussa Eukleideen algoritmissa yleistetään ajatus, jossa Eukleideen algoritmia kuljetaan ”takaperin”, kuten esimerkissä 18 tehtiin

$$2 = 26 - 3 \cdot 8 = 26 - (3 \cdot (112 - 4 \cdot 26)) = 26 - 3 \cdot 112 + 12 \cdot 26 = 13 \cdot 26 - 3 \cdot 112.$$

Tavoitteena on etsiä sellaiset kertoimet, joiden avulla laskeminen tietokoneella helpottuu, kun jokaista välivaihetta ei tarvitse tallettaa erikseen muistiin.

Aiemmin esitetyn perinteisen Eukleideen algoritmin (katso 1.4) perusteella tiedetään, että

$$r_n = \text{syt}\,(a, b) \quad \text{ja} \quad r_n = r_{n-2} - q_{n-1}r_{n-1} \quad (0 \leq r_n < r_{n-1}).$$

Olkoot $a = r_0$, $b = r_1$ ja $r_n = s_n a + t_n b$. Tällöin

$$\begin{aligned} r_n &= r_{n-2} - q_{n-1}r_{n-1} \\ &= (s_{n-2}r_0 + t_{n-2}r_1) - q_{n-1}(s_{n-1}r_0 + t_{n-1}r_1) \\ &= (s_{n-2} - q_{n-1}s_{n-1})r_0 + (t_{n-2} + q_{n-1}t_{n-1})r_1. \end{aligned}$$

Edelleen

$$s_n = s_{n-2} - s_{n-1}q_{n-1} \text{ ja } t_n = t_{n-2} - t_{n-i}q_{n-1}.$$

Nyt alkuarvot voidaan määrittää yhtälöistä

$$a = r_0 = s_0 a + t_0 b \Rightarrow s_0 = 1, \quad t_0 = 0.$$

$$b = r_1 = s_1 a + t_1 b \Rightarrow s_1 = 0, \quad t_1 = 1.$$

Laajennettu Eukleideen algoritmi voidaan muotoilla seuraavasti, kun alkoarvot s_0, t_0, s_1 ja t_1 tiedetään.

$$\begin{cases} s_0 = 1, t_0 = 0 \\ s_1 = 0, t_1 = 1 \\ r_n = r_{n-2} - q_{n-1}r_{n-1} \\ s_n = s_{n-2} - q_{n-1}s_{n-1} \\ t_n = t_{n-2} - q_{n-1}t_{n-i}. \end{cases}$$

Prosessia jatketaan niin kauan kunnes $r_{n+1} = 0$. Tämä tarkoittaa, että silloin

$$\text{syt}\,(a, b) = \text{syt}\,(r_0, r_1)\ldots. = \text{syt}\,(r_{n-2}, r_{n-1}) = \text{syt}\,(r_n, 0) = r_n,$$

mikä on yksi laajennetun Eukleideen algoritmin tärkeimmistä ominaisuuksista. Saadaan

$$\text{syt}\,(a, b) = r_n = s_n a + t_n b.$$

Laajennettu Eukleideen algoritmi on varsin käyttökelpoinen tietokoneella laskettaessa. Ajatukset määritelmien taustalla ovat lähteistä [4, s. 62-67] ja [8, s. 45-47], joista löytyy myös lisätietoja laajennetusta Eukleideen algoritmista ja sen sovelluksista.

2. Algebralliset luvut

Algebrallisten lukujen teorian kehittyminen on tärkeä vaihe rengasteorian kehittymisen historiassa. Siinä algebrallisia lukuja (kuten esimerkiksi $\sqrt{2}$ tai i) käytetään kuvastamaan kokonaislukujen ominaisuuksia. Ensimmäinen merkittävä henkilö algebrallisen lukuteorian kehityksen historiassa oli Euler. Hän löysi yhtälön, jolle saadaan kokonaislukuratkaisut käyttäen apuna irrationaali- ja imaginäärilukuja. Toinen merkittävä henkilö oli Gauss, joka ymmärsi tiettyjen kompleksilukujen toimivan lähes samoin kuin kokonaisluvut. Tässä luvussa määritellään algebralliset kokonaisluvut, sekä esitellään Gaussin ja Eisensteinin kokonaisluvut. Tämän luvun määritelmät ja todistukset seuraavat lähteitä [1] ja [3].

Määritelmä 20. Luku $\alpha \in \mathbb{C}$ on algebrallinen, jos se toteuttaa yhtälön

$$a_0\alpha^n + a_1\alpha^{n-1} + ... + \alpha_n = 0, \text{ jossa } a_0, a_1, ..., a_n \in \mathbb{Z} \text{ ja jokin } a_j \neq 0.$$

Toisin sanoen luvun sanotaan olevan algebrallinen, jos se on jonkin kokonaislukukertoimisen polynomiyhtälön juuri. Esimerkiksi luku $\sqrt{2}$ on algebrallinen, koska se toteuttaa yhtälön $x^2 - 2 = 0$. Jos luku ei ole algebrallinen, sanotaan sen olevan *transkendenttinen luku* (esimerkiksi π). Transkendenttisia lukuja ovat siis kaikki ne luvut, jotka eivät ole algebrallisia. Luvun transkendenttisuuden selvittämiseen ei ole tiedossa yleistä menetelmää, mutta esimerkiksi käyttämällä Liouvillen lausetta voidaan todistaa luvun π transkendenttisuus. Lisää transkendenttilukujen teoriasta löytyy lähteestä [3, s. 205-208].

Määritelmä 21. Luku $\alpha \in \mathbb{C}$ on algebrallinen kokonaisluku, jos se toteuttaa yhtälön

$$\alpha^n + a_{n-1}\alpha^{n-1} + ...a_1\alpha + a_0 = 0, \text{ jossa } a_0, a_1, ..., a_{n-1} \in \mathbb{Z}.$$

Algebrallinen kokonaisluku on siis sellainen kompleksiluku, joka on kokonaislukukertoimisen polynomin juuri ja sen korkeimman asteen termin kerroin on yksi.

Todistetaan seuraavaksi tärkeä tulos jatkon kannalta. Todistamalla, että rationaaliluku algebrallisena kokonaislukuna käyttäytyy kuten tavallinen kokonaisluku, helpotetaan monia työläitä todistuksia.

Lause 22. *Jos rationaaliluku $r = x$ täyttää kokonaislukukertoimisen yhtälön*

$$x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 = 0, \textit{ missä } a_0, ..a_{m-1} \in \mathbb{Z},$$

niin r on tavallinen kokonaisluku.

Todistus. Oletetaan, että $r = \frac{s}{t}$, kun $s, t \in \mathbb{Z}$ ja $\text{syt}(s, t) = 1$. Sijoitetaan r yhtälöön. Muokkaamalla yhtälöä saadaan

$$\frac{s^m}{t^m} = -a_{m-1}\frac{s^{m-1}}{t^{m-1}} - \cdots - a_1\frac{s}{t} - a_0.$$

Kertomalla molemmat puolet luvulla t^m saadaan

$$\begin{aligned} s^m &= -a_{m-1}s^{m-1}t - \cdots - a_1st^{m-1} - a_0t^m \\ &= t(-a_{m-1}s^{m-1} - \cdots - a_1st^{m-2} - a_0t^{m-1}). \end{aligned}$$

Oletuksen mukaan $\text{syt}(s,t) = 1$. Yhtälöstä huomataan, että mikä tahansa luvun t alkutekijä jakaa yhtälön oikean puolen, mutta ei yhtälön vasenta puolta. Tämä osoittaa, että $t = \pm 1$ (lause 12). Luku r on siis tavallinen kokonaisluku. □

Algebrallisille kokonaisluvuille voidaan määrittää yhteen-, vähennys- ja kertolasku. Tämä tieto helpottaa tilanteissa, joissa halutaan osoittaa, että algebralliset kokonaisluvut muodostavat renkaan.

Määritelmä 23. Jos α ja β ovat algebrallisia kokonaislukuja, niin myös luvut $\alpha+\beta$, $\alpha-\beta$ ja $\alpha\beta$ ovat algebrallisia kokonaislukuja.

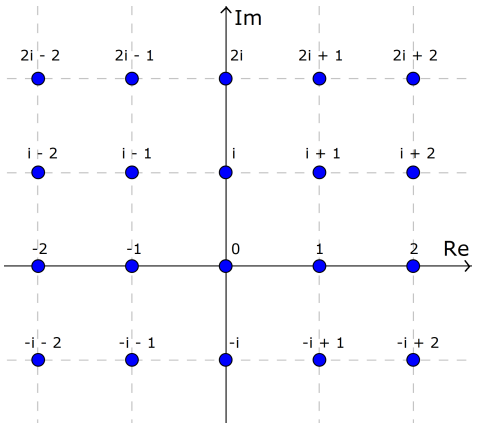
Todistus [1, s. 187]. Sivuutetaan täsmällinen todistus, sillä se on pitkähkö, eikä se tuo lisätyökaluja tämän tutkielman kannalta oleellisten kohtien ratkaisemiseksi.

2.1. **Gaussin kokonaisluvut.** Gaussin kokonaisluvut ovat yksinkertaisin yleistys perinteisille kokonaisluvuille, ja tämän vuoksi niiden sanotaan olevan kokonaislukujen vastineita kompleksilukujen joukossa. Luvut on nimetty saksalaisen matematiikon Johann Carl Friedrich Gaussin mukaan. Gauss oli ensimmäinen, joka huomasi joukolla $\mathbb{Z}[i]$ olevan paljon yhteisiä ominaisuuksia kokonaislukujen joukon $\mathbb{Z}$ kanssa. Tiedetään myös, että Gaussin kokonaislukujen summa, erotus ja kertolasku kuuluvat joukkoon $\mathbb{Z}[i]$. Tätä tietoa tullaan tarvitsemaan, kun todistetaan muutamia yleisiä tuloksia Gaussin kokonaisluvuille.

Gaussin kokonaisluvut ovat muotoa $a+ib$ muotoa olevia kompleksilukuja, joissa luvut a ja b ovat kokonaislukuja. Gaussin kokonaislukujen muodostamaa joukkoa merkitään

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Gaussin kokonaisluvut muodostavat kompleksitasoon neliöhilan, kuten huomataan kuvasta 1.



Kuva 1. Gaussin kokonaislukuja kompleksitasossa.

Gaussin kokonaisluvuille voidaan määritellä **normi** seuraavasti:

$$N(a+bi) = |a+bi|^2 = a^2 + b^2.$$

Yksiköt saadaan selvitettyä yhtälöstä $N(a+bi)=1$. Ainoat ratkaisut yhtälölle $a^2+b^2=1$ ovat $a=\pm 1$ ja $b=0$ tai $a=0$ ja $b=\pm 1$. Yksiköitä ovat siis ± 1 ja $\pm i$. Gaussin kokonaisluvun $\alpha=a+bi$ **konjugaatti** on $\bar{\alpha}=a-bi$.

Osoitetaan seuraavaksi Gaussin kokonaisluvuille eräs tärkeä ominaisuus.

Lause 24. *Kokonaisluvuille a_1, a_2, b_1 ja b_2 on voimassa*

$$(a_1^2+b_1^2)(a_2^2+b_2^2)=(a_1a_2-b_1b_2)^2+(a_1b_2+b_1a_2)^2.$$

Todistus. Lasketaan:

$$\begin{aligned}(a_1^2+b_1^2)(a_2^2+b_2^2) &= (a_1-b_1i)(a_1+b_1i)(a_2-b_2i)(a_2+b_2i)\\ &= (a_1-b_1i)(a_2-b_2i)(a_1+b_1i)(a_2+b_2i)\\ &= [a_1a_2-b_1b_2-(a_1b_2+b_1a_2)i][a_1a_2-b_1b_2+(a_1b_2+b_1a_2)i]\\ &= (a_1a_2-b_1b_2)^2+(a_1b_2+b_1a_2)^2.\end{aligned}$$

□

Sama identiteetti voidaan osoittaa olevan voimassa myös normille. Sanotaan, että normi on **multiplikatiivinen**, koska sille pätee seuraava ominaisuus:

Lemma 25. *Olkoot $\alpha, \beta \in \mathbb{C}$. Silloin*

$$N(\alpha\beta)=N(\alpha)N(\beta). \tag{3}$$

Todistus. Olkoot $\alpha=a+bi$ ja $\beta=c+di$. Tällöin

$$\begin{aligned}N(\alpha\beta) &= N((a+bi)(c+di))\\ &= N((ac-bd)+(ad+bc)i)\\ &= (ac-bd)^2+(ad+bc)^2\\ &= (ac)^2-2acbd+(bd)^2+(ad)^2+2adbc+(bc)^2\\ &= a^2c^2+a^2d^2+b^2d^2+b^2c^2\\ &= a^2(c^2+d^2)+b^2(d^2+c^2)\\ &= (a^2+b^2)(c^2+d^2)\\ &= N(\alpha)N(\beta).\end{aligned}$$

□

Normin multiplikatiivisuus voidaan esittää myös muodossa

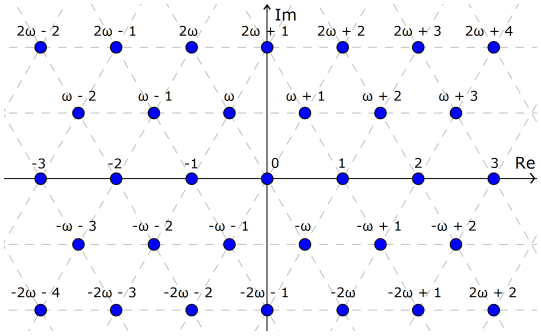
$$|z_1||z_2|=|z_1z_2|, \text{ jossa } |z|=\sqrt{a^2+b^2}.$$

Gaussin kokonaislukujen muodostamassa renkaassa yksikäsitteinen tekijöihinjako onnistuu. Se voitaisiin osoittaa samalla tavalla kuin luvussa 4 tehdään renkaille $\mathbb{Z}[\sqrt{-2}]$ ja $\mathbb{Z}[\sqrt{\zeta_3}]$. Renkaan $\mathbb{Z}[i]$ yksikäsitteisen tekijöihinjaon todistaminen sivuutetaan tässä tutkielmassa, mutta täsmällinen todistus on esitetty lähteessä [5, s. 227] ja jakoyhtälön geometrinen tulkinta lähteessä [1, s. 107].

2.2. **Eisensteinin kokonaisluvut.** Eisensteinin luvut ovat kompleksilukuja, jotka on nimetty saksalaisen matemaatikon Gotthold Eisensteinin mukaan. Luvut ovat muotoa

$$z = a + b\zeta_3, \text{ missä } a, b \in \mathbb{Z} \quad \text{ja} \quad \zeta_3 = \frac{-1+\sqrt{-3}}{2} = \frac{-1+i\sqrt{3}}{2} = e^{\frac{2\pi i}{3}}.$$

Eisensteinen kokonaisluvun $z = a + b\zeta_3$ **konjugaatti** on $\bar{z} = a + b\bar{\zeta_3}$. Eisensteinin kokonaisluvut muodostavat kompleksitasoon kolmiohilan (kuva 2) toisin kuin Gaussin kokonaisluvut muodostavat neliöhilan (kuva 1).



KUVA 2. Eisensteinin kokonaisluvut kompleksitasossa. Kuvassa $\omega = \zeta_3$.

Eisensteinin kokonaisluvuille voidaan määritellä **normi**

$$N(a + b\zeta_3) = a^2 - ab + b^2. \tag{4}$$

Todetaan, että luvulle $z = a + b\zeta_3$ on voimassa $|z|^2 = N(z)$:

$$\begin{aligned}
|z|^2 &= (a + b\zeta_3)(\overline{a + b\zeta_3}) \\
&= (a + b\zeta_3)(\bar{a} + \bar{b}\bar{\zeta_3}) \\
&= (a + b\zeta_3)(a + b\bar{\zeta_3}) \\
&= a^2 + ab(\zeta_3 + \bar{\zeta_3}) + b^2\zeta_3\bar{\zeta_3} \\
&= a^2 + ab \cdot \frac{-1+i\sqrt{3}-1-i\sqrt{3}}{2} + b^2 \cdot \frac{-1+i\sqrt{3}}{2} \cdot \frac{-1-i\sqrt{3}}{2} \\
&= a^2 - ab + b^2.
\end{aligned}$$

Huomataan, että

$$a^2 - ab + b^2 = \frac{1}{4}((2a-b)^2 + 3b^2) > 0,$$

joten normi on positiivinen kokonaisluku kaikilla nollasta poikkeavilla kokonaisluvuilla a ja b.

Jos $N(a + b\zeta_3) = \pm 1$, niin luku $a + b\zeta_3$ on **yksikkö**. Joukon $\mathbb{Z}[\zeta_3]$ yksiköt ovat $\pm 1, \pm\zeta_3, \pm{\zeta_3}^2$. Yksiköiden kärkipisteet muodostavat kuusikulmion nolla ympärille (katso kuva 2). Huomaa, että

$$\begin{aligned}
\pm\zeta_3^2 &= \pm\Big(\frac{-1+i\sqrt{3}}{2}\Big)^2 = \pm\frac{1-2i\sqrt{3}-3}{4} = \pm\frac{(-2)(1+i\sqrt{3})}{4}) = \pm\frac{-(1+i\sqrt{3})}{2} \\
&= \pm\frac{1-i\sqrt{3}}{2} - 1 = \pm(-\zeta_3 - 1).
\end{aligned}$$

Lemma 26. *Eisensteinin kokonaisluvut ovat algebrallisia lukuja.*

Todistus. Luku ζ_3 on algebrallinen kokonaisluku, koska se toteuttaa yhtälön $x^3-1=0$. De Moivren kaavan perusteella:

$$\zeta_3^3 - 1 = e^2\pi i - 1 = 1 - 1 = 0.$$

□

Renkaan määritelmä esitetään luvussa 4.1. Eisensteinin kokonaislukujen muodostamalle renkaalle

$$\mathbb{Z}[\zeta_3] = \{a + b\zeta_3 : a, b \in \mathbb{Z}\}$$

voidaan osoittaa olevan yksikäsitteinen tekijöihinjako ja se esitetään luvussa 4.

2.3. **Ryhmistä.** Todistuksissa esiintyvät myös käsitteet **ryhmä** ja **syklinen ryhmä**, joten esitellään ne vielä ennen Pellin yhtälön ratkaisemista. Ryhmäksi sanotaan epätyhjää joukkoa, jolle on määritelty laskutoimitus ja tietyt perusehdot. Syklisellä aliryhmällä tarkoitetaan yhden alkion virittämää ryhmää, joka koostuu annetun alkion kaikista kokonaislukupotensseista.

Määritelmä 27. Epätyhjä joukko G varustettuna laskutoimituksella $\star$ on ryhmä, jos kaikille $a, b, c \in G$ on voimassa seuraavat ominaisuudet:

(1) Vaihdannaisuus: $a \star (b \star c) = (a \star b) \star c$.
(2) Laskutoimituksella on neutraalialkio 0: $a \star 0 = a$.
(3) Jokaisella $a \in G$ on vasta-alkio $-a$: $a \star (-a) = 0$.

Määritelmä 28. Olkoon G ryhmä, ja $a \in G$. Tällöin merkitään

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} \subset G,$$

ja sanotaan, että se on alkion a virittämä syklinen aliryhmä. Jos $G = \langle a \rangle$, jollain $a \in G$ sanotaan, että G on syklinen ryhmä.

3. Pellin yhtälö

Pellin yhtälö on yksi vanhimmista ja kuuluisimmista Diofantoksen yhtälöistä, ja sen juuret sijoittuvat Pythagoralaisten aikaan 500-luvulle eaa. Yhtälö on nimetty harhaanjohtavasti englantilaisen matemaatikon John Pellin mukaan. Pell ei ole ratkaissut yhtälöä, vaan sen oikea löytäjä on toinen englantilainen matemaatikko William Brouncker. Euler erehtyi luulemaan Brounckerin ratkaisutapaa Pellin tekemäksi, ja tämän jälkeen yhtälöä alettiin kutsua Pellin yhtälöksi. Lagrangen ratkaisutapa ketjumurtolukuja hyödyntäen on peräisin 1700-luvulta.

Algebrallisten lukujen käyttäytymisessä on paljon yhteistä perinteisten kokonaislukujen kanssa. Pellin yhtälö on hyvä esimerkki siitä, miten algebrallisia lukuja ja ominaisuuksia hyödyntämällä voidaan löytää tapa tuottaa uusia kokonaislukuratkaisuja yhtälöille. Tässä luvussa esitellään tapa, jossa pienimmän kokonaislukuratkaisun avulla Pellin yhtälölle voidaan tuottaa äärettömän paljon uusia ratkaisuja. Pellin yhtälön tarkastelussa käytetyt tavat käsitellä algebrallisia kokonaislukuja toimii johdantona seuraaville luvuille, joissa siirrytään syvemmälle algebrallisen lukuteorian maailmaan. Tässä luvussa päälähteinä on käytetty lähteitä [1] ja [2]. Ketjumurtolukuja koskevat tulokset ovat lähteestä [4].

Määritelmä 29. Olkoot $x, y, n \in \mathbb{Z}$ siten, että n ei ole neliöluku. Pellin yhtälö on

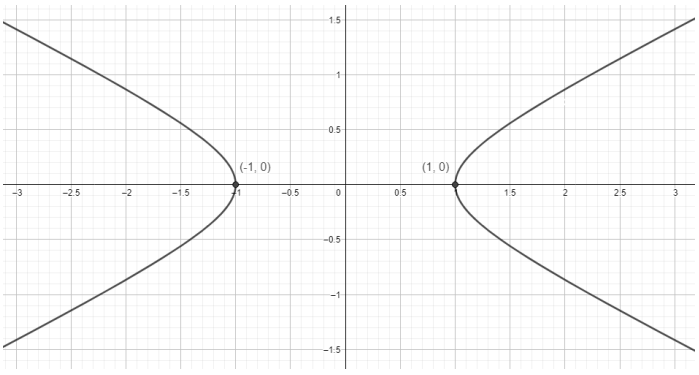
$$x^2 - ny^2 = 1.$$

Neliöluvulla tarkoitetaan kokonaislukua, joka on jonkin kokonaisluvun neliö.

Tarkastellaan tilannetta, jossa n on neliöluku. Olkoon $n = m^2$ ja $x^2 - ny^2 = 1$. Tällöin

$$x^2 - ny^2 = 1 \Rightarrow x^2 - m^2y^2 = 1 \Rightarrow (x + my)(x - my) = 1 \Rightarrow \begin{cases} x + my = \pm 1 \\ x - my = \pm 1. \end{cases}$$

Tällöin luvut $x = \pm 1$ ja $y = 0$ ovat ainoat luvut, jotka toteuttavat yhtälöt. Toisin sanoen: jos n on neliöluku, niin Pellin yhtälölle löydetään vain triviaalit ratkaisut $(1, 0)$ ja $(-1, 0)$. On siis järkevää vaatia, että n ei ole neliöluku.



Kuva 3. Yhtälölle $x^2 - 4y^2 = 1$ löydetään vain ratkaisut $(1, 0)$ ja $(-1, 0)$.

Tässä luvussa pienimmällä positiivisella kokonaislukuratkaisulla tarkoitetaan sellaista paria (x_0, y_0), missä $x_0 > 0$, $y_0 > 0$ ja

$$x_0 + y_0\sqrt{n} = \min\{x + y\sqrt{n} : x > 0, y > 0, x^2 - ny^2 = 1\}.$$

3.1. **Yksinkertaisin esimerkki Pellin yhtälöstä: $x^2 - 2y^2 = 1$.** Pythagoralaiset käyttivät yksinkertaista esimerkkiä Pellin yhtälöstä apuna ymmärtääkseen luvun $\sqrt{2}$ irrationaalisuuden. Esitellään tämä tapa ennen kaikkien ratkaisujen etsimistä.

3.1.1. ***Approksimaatiota sivu- ja diagonaalilukujen avulla.*** Muinaiset kreikkalaiset matemaatikot huomasivat, että jakolaskun $\frac{x_i}{y_i}$ avulla saadaan approksimaatio luvulle $\sqrt{2}$. Jos luku y_i on neliön sivu, niin silloin luku x_i approksimoi diagonaalia.

Olkoon $x^2 - 2y^2 = 1$, silloin

$$\frac{x_i^2}{y_i^2} = 2 + \frac{1}{y_i^2} \to 2, \text{ kun } \ y_i \to \infty.$$

Kreikkalaiset löysivät ratkaisun (x_i, y_i), jonka he määrittelivät seuraavasti. Yhtälöistä

$$d_1^2 - 2s_1^2 = 1,$$
$$d_{i+1}^2 - 2s(i+1)^2 = -(d_i^2 - 2s_i^2)$$

saadaan määriteltyä

$$d_1 = 3,$$
$$s_1 = 2,$$
$$d_{i+1} = d_i + 2s_i,$$
$$s_{i+1} = d_1 + s_i.$$

Parit $(d_1, s_1), (d_3, s_3)...$, joissa indeksi i on pariton, toteuttavat yhtälön $x^2 - 2y^2 = 1$ ja puolestaan parit $(d_2, s_2), (d_4, s_4)...$, joissa indeksi i on parillinen, toteuttavat yhtälön $x^2 - 2y^2 = -1$. Kun indeksi i on pariton, parit toteuttavat Pellin yhtälön.

3.1.2. ***Ratkaisujen joukko.*** Pienimmän positiivisen kokonaislukuratkaisun avulla voidaan tuottaa uusia ratkaisuja. Yhtälön $x^2 - 2y^2 = 1$ pienin positiivinen kokonaislukuratkaisu on $(3, 2)$. Uusia ratkaisuja voidaan löytää seuraavan säännön avulla.

Lause 30. *Jos (x_1, y_1) ja (x_2, y_2) ovat yhtälön $x^2 - 2y^2 = 1$ ratkaisuja, niin silloin myös (x_3, y_3) on ratkaisu, joka määritellään kaavalla*

$$(x_1 + y_1\sqrt{2})(x_2 + y_2\sqrt{2}) = x_3 + y_3\sqrt{2}.$$

Todistus. Muokataan yhtälöä ja eritellään kokonais- ja irrationaaliosat:

$$x_3 = x_1x_2 + 2y_1y_2, \quad y_3 = x_1y_2 + y_1x_2.$$

Laskemalla voidaan osoittaa, että (x_3, y_3) todella toteuttaa yhtälön $x_3^2 - 2y_3^2 = 1$.

$$\begin{aligned} x_3^2 - 2y_3^2 &= (x_1x_2 + 2y_1y_2)^2 - 2(x_1y_2 + y_1x_2)^2 \\ &= (x_1x_2)^2 + 4x_1x_2y_1y_2 + (2y_1y_2)^2 - 2(x_1y_2)^2 - 4x_1y_2y_1x_2 - 2(y_1x_2)^2 \\ &= (x_1^2 - 2y_1^2)(x_2^2 - 2y_2^2) \\ &= 1 \cdot 1 = 1. \end{aligned}$$

□

Tämän säännön avulla voidaan tuottaa uusia kokonaislukuratkaisuja Pellin yhtälölle, mutta se ei vielä todista, että kaikki kokonaislukuratkaisut oltaisiin löydetty. Olisi mahdollista osoittaa, että kokonaislukuratkaisut (x, y) muodostavat yhdessä ryhmän, sillä vaatimukset neutraali- ja vasta-alkiosta ovat voimassa sekä laskutoimituksen voidaan osoittaa olevan kommutatiivinen ja assosiatiivinen. Pellin yhtälön ratkaisut muodostavat ryhmän, jonka neutraalialkio on $(1, 0)$ ja vasta-alkio $(x, -y)$. Kommutatiivisuus on helppo havaita lauseen 30 kertolaskukaavasta. Assosiatiivisuuden tutkiminen johtaisi pitkään laskutoimitukseen, joten se sivuutetaan.

Lause 31. *Positiiviset luvut $x + y\sqrt{2}$ muodostavat ryhmän, jossa (x, y) on yhtälön $x^2 - 2y^2 = 1$ positiivinen kokonaislukuratkaisu. Ratkaisut muodostavat äärettömän syklisen ryhmän, jonka alkiot ovat luvun $3 + 2\sqrt{2}$ potensseja.*

Todistus. Olkoot luvut muotoa $x + y\sqrt{2}$, missä luvut x ja y ovat positiivisia kokonaislukuja siten, että lukupari (x, y) on yhtälön $x^2 - 2y^2 = 1$ ratkaisu. Sovelletaan logaritmifunktiota $\log(ab) = \log a + \log b$, jonka avulla ryhmän laskutoimitus saadaan muutettua tulosta yhteenlaskuksi. Tämän tiedon nojalla voidaan todeta, että luvut $\log(x + y\sqrt{2})$ muodostavat yhteenlaskulla varustetun ryhmän G.

Olkoon $m = \log(3 + 2\sqrt{2})$ ryhmän G pienin positiivinen luku. Luku m on todella pienin, sillä luku $3 + 2\sqrt{2}$ on pienin muotoa $x + y\sqrt{2}$ $(x, y > 0)$ oleva luku, joka on yhtälön $x^2 - 2y^2 = 1$ ratkaisu. Ratkaisu $(x, -y)$ on ratkaisun (x, y) vasta-alkio. Luvut $x - y\sqrt{2} < 1$, joten myös niiden logaritmit ovat pienempää kuin 0.

Olkoon k mikä tahansa ryhmän G alkio. Jaetaan jokin reaaliakselin väli luvun m pituisiin osaväleihin. Jos $k \neq mn$ kaikille $n \in \mathbb{Z}$, niin jollekin $n \in \mathbb{Z}$ on

$$mn < k < m(n + 1).$$

Tällöin myös $k - mn$ kuuluu ryhmään G, sillä ryhmä on varustettu yhteenlaskulla. Tällöin pätee

$$0 < k - mn < m.$$

Päädytään ristiriitaan, sillä m on joukon pienin alkio. Täytyy olla $k = mn$. Käyttämällä logaritmin laskusääntöjä saadaan

$$mn = n\log(3 + 2\sqrt{2}) = \log(3 + 2\sqrt{2})^n.$$

□

On osoitettu, että kaikki yhtälön $x^2 - 2y^2 = 1$ ratkaisut (x, y), joissa $x + y\sqrt{2} > 0$, vastaavat luvun $3+2\sqrt{2}$ potensseja. Kaikki ratkaisut ovat siis positiivisia ja ovat joko muotoa $x + y\sqrt{2}$ tai $-x - y\sqrt{2}$. Jäljelle jääneet ratkaisut (x, y) ovat negatiivisia, ja nekin saadaan luvun $3 + 2\sqrt{2}$ potensseista.

3.2. **Yleinen Pellin yhtälö.** Yleistä Pellin yhtälöä $x^2 - ny^2 = 1$ käsiteltäessä käytetään apuna lukuja, jotka ovat muotoa $x + y\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, aivan kuten ylempänä käytettiin lukuja $x + y\sqrt{2}$ yksinkertaisen Pellin yhtälön ratkaisussa.

Määritelmä 32. Olkoon $a + b\sqrt{n} \in \mathbb{R}$. Sanotaan, että a on luvun kokonaisosa ja b irrationaaliosa.

Lause 33. *Olkoon $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ ja olkoon $\sqrt{n}$ irrationaaliluku. Jos*

$$a_1 + b_1\sqrt{n} = a_2 + b_2\sqrt{n},$$

niin $a_1 = a_2$ ja $b_1 = b_2$.

Todistus. Tehdään vastaväite ja oletetaan, että $b_1 \neq b_2$. Muokkaamalla yhtälöä niin, että vasemmalla puolella ovat kokonaisosat ja oikealla puolella irrationaaliosat, saadaan yhtälö muotoon

$$a_1 - a_2 = (b_2 - b_1)\sqrt{n}.$$

Nyt oletuksesta $b_2 - b_1 \neq 0$ seuraa, että

$$\sqrt{n} = \frac{a_1 - a_2}{b_2 - b_1}.$$

Tästä seuraa ristiriita luvun $\sqrt{n}$ irrationaalisuuden kanssa. Täytyy olla $b_1 = b_2$ ja täten myös $a_1 = a_2$.

□

Määritelmä 34. Olkoon n kokonaisluku, joka ei ole neliöluku. Merkitään

$$\mathbb{Z}[\sqrt{n}] = \{x + y\sqrt{n} : x, y \in \mathbb{Z}\}.$$

Määritellään **normi** seuraavasti

$$N(x + y\sqrt{n}) = (x - y\sqrt{n})(x + y\sqrt{n}) = x^2 - ny^2.$$

Lukua $x - y\sqrt{n}$ kutsutaan luvun $x + y\sqrt{n}$ **konjugaattiksi** joukossa $\mathbb{Z}[\sqrt{n}]$.

Algebrallisten lukujen käyttö pelkkien kokonaislukujen sijasta on ollut merkittävä oivallus algebran historiassa. Silloin kun normi on yksi, Pellin yhtälön ratkaisemiseksi riittää renkaan $\mathbb{Z}[\sqrt{n}]$ alkutekijöiden selvittäminen. Rengas on tuttu käsite algebran kursseilta, ja sen määritelmä löytyy tutkielman luvusta 4.1.

Intialainen matemaatikko Brahmagupta löysi 600-luvulla tavan tuottaa uusia ratkaisuja Pellin yhtälölle. Laskemalla voidaan osoittaa, että kyseinen multiplikatiivisuusominaisuus pääte sekä kokonaislukukertoimiselle että rationaalilukukertoimiselle Pellin yhtälölle.

Lause 35. ***Brahmaguptan multiplikatiivisuusominaisuus.*** *Jos parit* (x_1, y_1) *ja* (x_2, y_2) *ovat Pellin yhtälön* $x^2 - ny^2 = 1$ *ratkaisuja ja kun*

$$(x_3, y_3) = (x_1x_2 + ny_1y_2, x_1y_2 + y_1x_2),$$

niin (x_3, y_3) *on myös ratkaisu.*

Todistus. (x_1, y_1) ja (x_2, y_2) ovat ratkaisuja. Silloin

$$x_1^2 - ny_1^2 = 1 = x_2^2 - ny_2^2$$

Siksi

$$\begin{aligned}
1 &= (x_1^2 - ny_1^2)(x_2^2 - ny_2^2) \\
&= (x_1 - y_1\sqrt{n})(x_1 + y_1\sqrt{n})(x_2 - y_2\sqrt{n})(x_2 + y_2\sqrt{n}) \\
&= (x_1 - y_1\sqrt{n})(x_2 - y_2\sqrt{n})(x_1 + y_1\sqrt{n})(x_2 + y_2\sqrt{n}) \\
&= [x_1x_2 + ny_1y_2 - (x_1x_2 + y_1x_2)\sqrt{n}]x[x_1x_2 + ny_1y_2 + (x_1y_2 + y_1x_2)\sqrt{n}] \\
&= (x_1x_2 + ny_1y_2)^2 - n(x_1y_2 + y_1x_2)^2 \\
&= x_3^2 - ny_3^2
\end{aligned}$$

□

Esimerkki 36. Etsitään yhtälölle $x^2 - 5y^2 = 1$ uusia ratkaisuja.

Kokeilemalla huomataan, että pienin positiivinen kokonaislukuratkaisu on $(9, 4)$. Kertomalla (9,4) itsellään saadaan toinenkin ratkaisu. Jatkamalla tällä tavoin saadaan tuotettua lisää ratkaisuja yhtälölle $x^2 - 5y^2 = 1$.

$$(9 \cdot 9 + 5 \cdot 4 \cdot 4, 9 \cdot 4 + 4 \cdot 9) = (161, 72)$$
$$(9 \cdot 161 + 5 \cdot 4 \cdot 72, 9 \cdot 72 + 4 \cdot 161) = (2889, 1292)$$

Nämä ratkaisut vastaavat $9 + 4\sqrt{5}$ potensseja.

Brahmaguptan multiplikatiivisuusominaisuus pätee myös rationaalikertoimisille luvuille, jotka määritellään seuraavasti

$$\mathbb{Q}[\sqrt{n}] = \{x + y\sqrt{n} : x, y \in \mathbb{Q}\}, \text{ ja normi } N(x + y\sqrt{n}) = x^2 - ny^2.$$

Lause 37. *Olkoot* α *ja* β *renkaan* $\mathbb{Q}[\sqrt{n}]$ *alkioita. Tällöin*

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

Todistus. Olkoot $\alpha = x_1 + y_1\sqrt{n}$ ja $\beta = x_2 + y_2\sqrt{n}$. Silloin

$$\begin{aligned}
N(\alpha)N(\beta) &= (x_1^2 - ny_1^2)(x_2^2 - ny_2^2) \\
&= (x_1x_2 + ny_1y_2)^2 - n(x_1y_2 + y_1x_2)^2 \\
&= N(\alpha\beta).
\end{aligned}$$

□

Normin multiplikatiivisuusominaisuus voidaan ilmaista myös toisella tavalla. Jos (x_1, y_1) ja (x_2, y_2) täyttävät ehdot $x_1^2 - ny_1^2 = k_1$ ja $x_2^2 - ny_2^2 = k_2$, niin $(x_1x_2 + ny_1y_2, x_1y_2 + y_1x_2)$ on yhtälön $x^2 - ny^2 = k_1k_2$ ratkaisu.

Kolmikoiden (x_1, y_1, k_1) ja (x_2, y_2, k_2) avulla saadaan muodostettua uusi kolmikko $(x_1x_2 + ny_1y_2, x_1y_2 + x_2y_1, k_1k_2)$. Tämä on varsin käyttökelpoinen tapa, silloin kun Pellin yhtälölle on olemassa ilmeinen ratkaisu $x^2 - ny^2 = 1$.

Esimerkki 38. Etsitään kokonaislukuratkaisu yhtälölle $x^2 - 92y^2 = 1$.

Sijoittamalla $x = 10$ ja $y = 1$ saadaan, että $10^2 - 92 \cdot 1^2 = 8$. Muodostuu kolmikko $(10, 1, 8)$, joka kerrottuna itsellään muodostaa toisen kolmikon. Lasketaan:

$$(10 \cdot 10 + 92 \cdot 1 \cdot 1, 10 \cdot 1 + 1 \cdot 10, 8 \cdot 8) = (192, 20, 84),$$

mikä tarkoittaa

$$192^2 - 92 \cdot 20^2 = 8^2.$$

Kun jaetaan puolittain luvulla 8^2, jäljelle jää

$$24^2 - 92 \cdot \left(\frac{5}{2}\right)^2 = 1,$$

joka muodostaa kolmikon $(24, \frac{5}{2}, 1)$. Se on lähes kokonaisluvuista muodostuva kolmikko, joten kerrotaan se vielä kertaalleen itsellään, jolloin saadaan ainoastaan kokonaisluvuista koostuva kolmikko

$$(24^2 + 92 \cdot \left(\frac{5}{2}\right)^2, 24 \cdot \frac{5}{2} + \frac{5}{2} \cdot 24, 1) = (1151, 120, 1).$$

Kun $x = 1151$ ja $y = 120$, yhtälölle löytyy kokonaislukuratkaisu $x^2 - 92y^2 = 1$.

Tämä on Brahmaguptan ensimmäinen esimerkki, josta hän on sanonut seuraavasti: ”Henkilö, joka ratkaisee tämän ongelman vuodessa on matemaatikko.”

Esimerkeistä huomataan, että luvuista tulee nopeasti niin isoja, että niiden laskeminen käsin tuntuu työläältä. Tietokoneella uusien vastauksien tuottaminen on helppoa. Seuraavassa esimerkissä on käytetty wxMaximaa apuna uusien tulosten generoimisessa. Esimerkin kahdessa ensimmäisessä vaiheessa tallennetaan Pellin yhtälö kahdella eri tavalla.

```
(% i1)  pell_p[n](xy):=xy[1]^2-n*xy[2]^2=1;
```

(% o1) $$pell_{p_n}(xy) := xy_1^2 - n\,xy_2^2 = 1$$

```
(% i2)  pell_m[n](xy1, xy2):=
        [xy1[1]*xy2[1]+n*xy1[2]*xy2[2], xy1[1]*xy2[2]+xy1[2]*xy2[1]];
```

(% o2) $$pell_{mn}(xy1, xy2) := [xy1_1\,xy2_1 + n\,xy1_2\,xy2_2, xy1_1\,xy2_2 + xy1_2\,xy2_1]$$

Nyt ollaan muodostettu kaksi hieman erilaista funktiota. Paikalle [n] sijoitetaan Pellin yhtälön termin y^2 kerroin. Seuraavassa vaiheessa käytetään for-silmukkaa uusien vastausten tuottamisessa. Käytetään jälkimmäistä muotoa Pellin yhtälöstä ja sijoitetaan muuttujien paikalle lukupari $(3, 2)$. Vastaukseksi tulostuu seitsemän uutta ratkaisua.

```
(% i3)  (xy0:[3,2],
        for j:1 thru 7 do (
        xy0:pell_m[2](xy0, [3,2]),
        print(xy0)
        )
        );
```

$$[17, 12]$$
$$[99, 70]$$
$$[577, 408]$$
$$[3363, 2378]$$
$$[19601, 13860]$$
$$[114243, 80782]$$
$$[665857, 470832]$$

(% o3) *done*

Seuraavissa vaiheissa luvut alkavat olla jo niin isoja, että niitä olisi kovin työlästä laskea käsin. Käytetään jälleen for-silmukkaa, mutta tarkistetaan kuitenkin ennen silmukan muodostamista, että sijoitettavat alkuarvot todella toteuttavat Pellin yhtälön.

```
(% i4)  pell_p[26]([51,10]);
```

(% o4) $1 = 1$

Huomataan, että luvut toteuttavat Pellin yhtälön. Yläpuolella oleva lasku on siis sama kuin $51^2 - 26 \cdot 10^2 = 1$. Käytetään jälleen for-silmukkaa.

```
(% i5)  (xy0:[51,10],
        for j:1 thru 4 do (
        xy0:pell_m[26](xy0, [51,10]),
        print(xy0)
        )
        );
```

$$[5201, 1020]$$
$$[530451, 104030]$$
$$[54100801, 10610040]$$
$$[5517751251, 1082120050]$$

(% o5) *done*

```
(% i6)  pell_p[73]([2281249,267000]);
```

(% o6) $1 = 1$

```
(% i7)  (xy0:[2281249,267000],
        for j:1 thru 3 do (
        xy0:pell_m[73](xy0, [2281249, 267000]),
        print(xy0)
        )
        );
```

$$[10408194000001, 1218186966000]$$

$$[47487364308614281249, 5557975596000801000]$$

$$[216661004683313632776000001, 25358252540801244373932000]$$

(% o7) *done*

3.3. **Pellin yhtälön ei-triviaalit ratkaisut.** Pienimmän kokonaislukuratkaisun löytäminen ei ole helppoa, eikä sille ole yksinkertaista kaavaa. Itseasiassa pienimmän kokonaislukuratkaisun olemassaolon todistaminen on helpompaa kuin sen löytäminen. Todistuksen ideana on etsiä äärettömän monta vaihtoehtoa pienimmäksi kokonaislukuratkaisuksi ja osoitetaan, että yksi niistä on oikea.

On useita tapoja todistaa Pellin yhtälön ratkaisujen olemassaolo. Tässä luvussa esitetään todistus kuten Dirichlet sen teki 1840-luvulla käyttäen kyyhkyslakkaperiaatetta. Tämä kyyhkyslakkaperiaate on saanut nimensä ajatuksesta: jos $n+1$ kyyhkystä laitetaan n laatikkoon, vähintään yhdessä laatikossa täytyy olla vähintään kaksi kyyhkystä. Kyyhkyslakkaperiaattesta on myös toinen muoto: jos ääretön määrä kyyhkysiä laitetaan äärelliseen määrään laatikoita, silloin vähintään yhdessä laatikossa on ääretön määrä kyyhkysiä.

Lause 39. ***Dirichleen approksimointilause.*** *Olkoon $\sqrt{n}$ irrationaaliluku ja $B > 0$ kokonaisluku. Tällöin on olemassa $a, b \in \mathbb{Z}$ siten, että $0 < b < B$ ja*

$$|a - b\sqrt{n}| < \frac{1}{B}.$$

Todistus. Olkoon $B > 0$ kokonaisluku. Tarkastellaan lukuja $\sqrt{n}$, $2\sqrt{n}$, $3\sqrt{n}$, ... , $(B-1)\sqrt{n}$ eli toisin sanoen tarkastellaan irrationaalilukuja $k\sqrt{n}$, joissa $k = 1, 2, ..., B-1$. Jokaiselle kertojalle k voidaan valita kokonaisluku A_k, jolle pätee

$$0 < A_k - k\sqrt{n} < 1.$$

Koska $\sqrt{n}$ on irrationaaliluku, luvut $A_k - k\sqrt{n}$ ovat kaikki lukujen 0 ja 1 välissä. Lukuja

$$0, A_1 - \sqrt{n}, ..., A_{B-1} - (B-1)\sqrt{n}, 1$$

on yhteensä $B+1$ kappaletta välillä $[0, 1]$.

Jaetaan väli [0,1] osaväleihin, joiden pituus on $\frac{1}{B}$. Tällöin osavälejä on yhteensä B kappaletta ja lukuja on yhteensä $B+1$ kappaletta, niin kyyhkyslakkaperiaatteesta

seuraa, että vähintään kaksi lukua sisältyy yhteen pienempään väliin. Olkoon näiden kahden luvun erotus muotoa $a - b\sqrt{n}$, joillain $a, b \in \mathbb{Z}$. Luku on irrationaalinen ja sille saadaan esitys

$$0 < a - b\sqrt{n} < \frac{1}{B}.$$

Toisin sanoen lukujen etäisyys toisistaan on alle $\frac{1}{B}$. Myös $b < B$, sillä luku b on kahden lukua B pienemmän positiivisen kokonaisluvun välissä.

□

Koska Dirichleen approksimointilause pätee kaikille $B > 0$, voidaan valita luvut $a = a_B$ ja $b = b_B$ siten, että löydetään aina uusi lukupari (a, b), jolle pätee $|a - b\sqrt{n}| < \frac{1}{B}$. Jos $0 < b < B$, niin

$$|a - b\sqrt{n}| < \frac{1}{b}. \tag{5}$$

Voidaan todeta, että lukupareja (a, b) on äärettömän monta.

Kyyhkyslakkaperiaatteen äärettömästä muodosta seuraa ajatus: jos ääretön määrä lukuja laitetaan äärelliseen määrään osavälejä, niin vähintään yhdessä osavälissä on ääretön määrä lukuja. Tämän tiedon nojalla saadaan seuraukset:

Seuraus 40. *Yhtälön 5 nojalla voidaan tehdä päättely*

$$a + b\sqrt{n} \leq a - b\sqrt{n} + 2b\sqrt{n} < \frac{1}{b} + 2b\sqrt{n} \leq 3b\sqrt{n},$$

ja edelleen

$$a^2 - nb^2 \leq \frac{1}{b} \cdot 3b\sqrt{n} = 3\sqrt{n}.$$

Tällöin on olemassa äärettömän monta kahden luvun erotusta $a - b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, jolle voidaan laskea normi, joka on pienempää kuin $3\sqrt{n}$.

Todistus. Voidaan valita äärettömän monta lukuparia (a, b), joille pätee $|a - b\sqrt{n}| < \frac{1}{b}$. Tämä osoittaa myös sen, että on olemassa ääretön määrä lukuja $a - b\sqrt{n}$, joiden normi on pienempää kuin $3\sqrt{n}$.

□

Seuraus 41. *Olkoon $\alpha = a_1 - b_1\sqrt{n}$ ja $\beta = a_2 - b_2\sqrt{n}$ positiivisia lukuja. Tällöin kyyhkyslakkaperiaatteen nojalla*

(1) *on olemassa luvut α ja β, joilla on yhteinen normi N,*
(2) $a_1 \equiv a_2 \pmod{N}$,
(3) $b_1 \equiv b_2 \pmod{N}$.

Jos on olemassa äärettömän monta lukua $a - b\sqrt{n}$, niin on olemassa myös äärettömän monta sellaista lukua, joilla on sama normi. Tällöin on olemassa myös äärettömän monta lukua a, joilla on sama kongruenssiluokka $\pmod{N}$ ja äärettömän monta lukua b, joilla on sama kongruenssiluokka $\pmod{N}$.

Lause 42. *Olkoon n on positiivinen kokonaisluku, joka ei ole neliöluku. Tällöin Pellin yhtälöllä $x^2 - ny^2 = 1$ on kokonaislukuratkaisu $(a, b) \neq (\pm 1, 0)$.*

Todistus. Olkoon $a-b\sqrt{n} = \frac{a_1-b_1\sqrt{n}}{a_2-b_2\sqrt{n}}$, jossa luvut $a_1-b_1\sqrt{n}$ ja $a_2-b_2\sqrt{n}$ ovat erisuuria ja positiivisia lukuja. Tällöin

$$\begin{aligned} a - b\sqrt{n} &= \frac{a_1 - b_1\sqrt{n}}{a_2 - b_2\sqrt{n}} \\ &= \frac{(a_1 - b_1\sqrt{n})(a_2 + b_2\sqrt{n})}{a_2^2 - nb_2^2} \\ &= \frac{a_1a_2 + a_1b_2\sqrt{n} - b_1a_2\sqrt{n} - b_1b_2n}{a_2^2 - b_2^2} \\ &= \frac{a_1a_2 - nb_1b_2}{a_2^2 - nb_2^2} + \frac{a_1b_2 - b_1a_2}{a_2^2 - nb_1^2}\sqrt{n}. \end{aligned}$$

Aiemmin todistetusta Dirichleen approksimointilauseesta seuraa, että luvuilla $a_1 - b_1\sqrt{n}$ ja $a_2 - b_2\sqrt{n}$ on yhteinen normi. Merkitään $N = a_2^2 - nb_2^2$, jolloin saatu yhtälö $\frac{a_1a_2-nb_1b_2}{a_2^2-nb_2^2} + \frac{a_1b_2-b_1a_2}{a_2^2-nb_1^2}\sqrt{n}$ voidaan kirjoittaa muodossa

$$\frac{a_1a_2 - nb_1b_2}{N} + \frac{a_1b_2 - b_1a_2}{N}\sqrt{n}.$$

Koska luvuilla $a_1 - b_1\sqrt{n}$ ja $a_2 - b_2\sqrt{n}$ on yhteinen normi, tällöin myös lukujen osamäärällä $a - b\sqrt{n}$ on normi 1. Tämä on seurausta normin multiplikatiivisuusominaisuudesta (lause 37). Luvut $a_1 - b_1\sqrt{n}$ ja $a_2 - b_2\sqrt{n}$ ovat erisuuria ja positiivisia, joten osamäärä $a - b\sqrt{n} \neq \pm 1$.

Vielä täytyisi osoittaa, että luvut a ja b ovat kokonaislukuja. Osoitetaan, että

$$N \mid a_1a_2 - nb_1b_2 \quad \text{ja} \quad N \mid a_1b_2 - b_1a_2$$

eli

$$a_1a_2 - nb_1b_2 \equiv a_1b_2 - b_1a_2 \equiv 0 \pmod{N}. \tag{6}$$

Ensimmäinen kongruenssi $a_1a_2 - nb_1b_2 \equiv a_1b_2 - b_1a_2 \pmod{N}$ pätee, koska $N = a_1^2 - nb_1^2$. Merkitään

$$0 \equiv a_1^2 - nb_1^2 \pmod{N}.$$

Korvataan a_1 ja b_1 niitä vastaavilla arvoilla, jotka saadaan kongruensseista $a_1 \equiv a_2 \pmod{N}$ ja $b_1 \equiv b_2 \pmod{N}$. Kongruenssi voidaan kirjoittaa muodossa

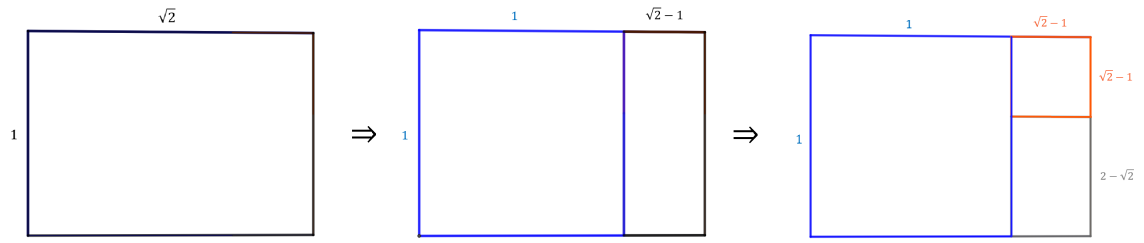
$$a_1a_1 - nb_1b_1 \equiv a_1a_2 - nb_1b_2 \pmod{N}.$$

Kongruenssin (6) toinen osa $a_1b_2 - b_1a_2 \equiv 0 \pmod{N}$ seuraa tiedosta, että $a_1 \equiv a_2 \pmod{N}$ ja $b_2 \equiv b_1 \pmod{N}$. Kongruenssin laskusäännöistä saadaan, että $a_1b_2 \equiv b_1a_2 \pmod{N}$, joka tarkoittaa samaa kuin $a_1b_2 - b_1a_2 \equiv 0 \pmod{N}$.

□

3.4. **Ketjumurtoluvut ja Pellin yhtälön ratkaisu niiden avulla.** Myöhemmin Euroopassa Pellin yhtälön todistustavat saivat rinnalleen yksinkertaisemman ja elegantimman todistuksen ketjumurtolukujen avulla. Eurooppalaiset matemaatikot, kuten esimerkiksi Brouncker, työskentelivät Pellin yhtälön parissa. Tässä luvussa jatketaan vielä siitä, mihin aiemmin jäätiin tarkasteltaessa Pythagoralaisten tapaa tutkia lukujen irrationaalisuutta jakoyhtälön avulla ja yhdistetään nämä ajatukset ketjumurtolukujen merkintätapaan. Tämän luvun lauseet ja määritelmät seuraavat lähteitä [2] ja [4].

3.4.1. ***Johdattelua ketjumurtolukuihin.*** Pythagoralaiset huomasivat luvun $\sqrt{2}$ irrationaalisuuden tutkimalla yhtälöä $x^2 - 2y^2 = 1$ (katso luku 3.1.1). He käyttivät apunaan Eukleideen algoritmia tutkiessaan jaksollisuutta. He käyttivät paria $(\sqrt{2}, 1)$, ja tekivät havainnon, että luku on irrationaalinen, jos jakoa pystytään jatkamaan loputtomiin (katso kuva 4). Koska $\sqrt{2}$ on irrationaalinen, voitaisiin pilkkomista jatkaa kuvan osoittamalla tavalla loputtomiin.



Kuva 4. Eukleiden algoritmi parilla ($\sqrt{2}$,1).

Eukleideen algoritmin yhtälöistä (luku 1.4) saadaan

$$\begin{aligned}
\frac{a}{b} = \frac{r_0}{r_1} &= q_1 + \frac{r_2}{r_1} = q_1 + \frac{1}{r_1/r_2} \\
\frac{r_1}{r_2} &= q_2 + \frac{1}{r_2/r_3} \\
&\vdots \\
\frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{1}{r_{n-1}/r_n} \\
\frac{r_{n-1}}{r_n} &= q_n.
\end{aligned}$$

Sijoittamalla saadaan

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + q_{n-1} + \cfrac{1}{q_n}}}}.$$

Ketjumurtolukua voidaan merkitä $\frac{a}{b} = [q_1; q_2, ..., q_n]$, joka on esitys **päättyvälle ketjumurtoluvulle**. Kaikki rationaaliluvut voidaan esittää käyttäen päättyviä ketjumurtolukuja.

Päättymättömän yksinkertaisen ketjumurtoluvun sanotaan olevan jaksollinen, jos on olemassa luvut N ja k siten, että

$$a_n = a_{n+k} \quad \text{kaikilla positiivisilla kokokonaisluvuilla } n \geq N.$$

Tällöin esityksessä esiintyvät luvut $a_0, a_1, ...$ muodostavat jonon, josta jaksollisuus voidaan huomata ja **jakson pituus** voidaan määrittää. Kun n ei ole neliöluku, luvun $\sqrt{n}$ jaksollinen ketjumurtolukuesitys on

$$\sqrt{n} = [a_0; \overline{a_1, a_2, ..., a_2, a_1, 2a_0}].$$

Esityksestä voidaan havaita **symmetrisyys**, kun viimeinen termi jätetään huomioimatta. Jakson viimeinen termi on kaksinkertainen jonon ensimmäiseen termiin verrattuna. Tällöin jakson pituus olisi jonon $a_1, a_2, ..., a_2, a_1, 2a_0$ termien lukumäärä. Todistus on esitetty lähteessä [4, s. 383-387].

Esimerkki 43.

(1) Luvun $\sqrt{2}$ ketjumurtolukuesitys:

$$\begin{aligned}
\sqrt{2} = 1 + (\sqrt{2} - 1) &= 1 + \frac{1}{1 + \sqrt{2}} \\
&= 1 + \frac{1}{1 + (1 + \frac{1}{1+\sqrt{2}})} \\
&= 1 + \frac{1}{2 + \frac{1}{1+\sqrt{2}}} \\
&= 1 + \frac{1}{2 + \frac{1}{1+(1+\frac{1}{1+\sqrt{2}})}} \\
&= 1 + \frac{1}{2 + \frac{1}{2+\frac{1}{1+\sqrt{2}}}} \\
&= \cdots \\
&= [1; 2, 2, 2...] \\
&= [1; \overline{2}].
\end{aligned}$$

Ketjumurtolukuesitys on päättymätön ja jaksollinen. Jakson pituus on 1.

(2) Luvun $\frac{57}{23}$ ketjumurtolukuesitys:

$$\frac{57}{23} = 2 + \frac{11}{23} = 2 + \frac{1}{\frac{23}{11}} = 2 + \frac{1}{2 + \frac{1}{11}} = [2, 2, 11].$$

Ketjumurtolukuesitys on päättyvä.

Kuten esimerkeistä huomataan, ketjumurtolukuja on sekä päättyviä että päättymättömiä. Voitaisiin osoittaa, että jokainen positiivinen rationaaliluku voidaan kirjoittaa päättyväksi ketjumurtoluvuksi ja puolestaan jokainen positiivinen irrationaaliluku voidaan esittää päättymättömänä ketjumurtolukuna. Pellin yhtälön ratkaisualgoritmissa käytetään yksinkertaisia päättymättömiä ketjumurtolukuja, joten keskitytään vain niiden määrittelyyn.

3.4.2. ***Pellin yhtälö ketjumurtolukujen avulla.*** Brahmagupta löysi valtavan määrän ratkaisuja Pellin yhtälölle, mutta hän ei kyennyt kuitenkaan yleistämään tulostaan kaikille luvun n arvoille, vaan sen teki intialainen matemaatikko ja tähtitietelijä Bhaskara II. Hänkään ei kuitenkaan kyennyt antamaan todistusta, joka todistaisi syklisen menetelmän toimivan aina. 1700-luvulla Lagrange kehitti tavan, jonka avulla Pellin yhtälölle löydetään ratkaisuja käyttäen ketjumurtolukuja.

Ketjumurtoluvut tarjoavat mielenkiintoisen tavan tarkastella Pellin yhtälön ratkaisuja, mutta tutkielman päätavoitteen kannalta tämä osio on sivuhaara, minkä vuoksi todistukset sivuutetaan. Tässä luvussa esitellään tuloksia, joiden avulla löydetään tapa generoida Pellin yhtälölle uusia ratkaisuja ketjumurtolukujen avulla. Lauseet ja määritelmät seuraavat lähdettä [4] ja niiden täsmälliset todistukset löytyvät [4, s. 405-406].

Lemma 44. *Olkoon n luku, joka ei ole neliöluku. Irrationaaliluku $\sqrt{n}$ voidaan esittää päättymättömänä ketjumurtolukuna*

$$[a_0; a_1, a_2 ...] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}. \tag{7}$$

Lause 45. *Olkoot n ja a kokonaislukuja siten, että $n > 0$ ja se ei ole neliöluku. Olkoon myös $|a| < \sqrt{n}$. Jos $x^2 - ny^2 = a$ niin $\frac{x}{y}$ on yksinkertaisen ketjumurtoluvun **konvergentti**. Yksinkertaisella ketjumurtoluvulla tarkoitetaan ketjumurtoluvua, jonka esityksessä osoittajat ovat ykkösiä.*

Konvergenttilla tarkoitetaan ketjumurtoluvun osaa. Kun k kuuluu indeksijoukoon, voidaan konvergenttia merkitä

$$C_k = [a_0; a_1, ..., a_k].$$

Tällöin sanotaan, että C_k on k. konvergentti.

Lause 46. *Olkoon $n \in \mathbb{N}$ siten, että se ei ole neliöluku. Määritellään rekursiivisesti*

$$a_k = \frac{P_k + \sqrt{n}}{Q_k}, \quad b_k = \lfloor a_k \rfloor^{(*}, \quad P_{k+1} = b_k Q_k - P_k, \quad \text{ja } Q_{k+1} = \frac{(n - P_{k+1}^2)}{Q_k},$$

kun $k = 0, 1, 2...$, $a_0 = \sqrt{n}$ ja P_k ja Q_k ovat kokonaislukuja. Olkoon $\frac{p_k}{q_k}$ luvun $\sqrt{n}$ yksinkertaisen ketjumurtoluvun k. konvergentti. Tällöin

$$p_k^2 - nq_k^2 = (-1)^{k-1} Q_{k+1}.$$

*) Merkinnällä $\lfloor a_k \rfloor$ (a_k on "lattia") tarkoitetaan suurinta kokonaislukua x, joka toteuttaa ehdon $x \leq a_k$. Esimerkiksi $\lfloor \sqrt{2} \rfloor = 1$.

Esimerkki 47. Määritetään luvun $\sqrt{2}$ ketjumurtolukuesitys käyttäen lausetta 46 Aloitetaan muodostamalla alkuarvot P_0, Q_0, n ja b_0, saadaan

$$P_0 = 0, \quad n = 2, \quad Q_0 = 1, \quad b_0 = \left\lfloor \frac{0+\sqrt{2}}{1} \right\rfloor = 1.$$

Alkuarvojen ja rekursioyhtälöiden avulla saadaan:

$$P_1 = 1 \cdot 1 - 0 = 1, \quad Q_1 = \frac{2-1^2}{1} = 1, \quad b_1 = \left\lfloor \frac{1+\sqrt{2}}{1} \right\rfloor = 2$$

$$P_2 = 2 \cdot 1 - 1 = 1, \quad Q_2 = \frac{2-1^2}{1} = 1, \quad b_2 = \left\lfloor \frac{1+\sqrt{2}}{1} \right\rfloor = 2$$

$$P_3 = 2 \cdot 1 - 1 = 1, \quad Q_3 = \frac{2-1^2}{1} = 1, \quad b_3 = \left\lfloor \frac{1+\sqrt{2}}{1} \right\rfloor = 2.$$

Huomataan, että $P_1 = P_2 = P_3$ ja $Q_1 = Q_2 = Q_3$ eli jakoalgoritmi alkaa toistua samanlaisena. Kun verrataan tätä esimerkkiin 43, huomataan esityksien olevan samat. Saadaan

$$\sqrt{2} = [1; \overline{2}].$$

Lause 48. *Olkoon n positiivinen kokonaisluku, joka ei ole neliöluku. Olkoon p_k/q_k luvun $\sqrt{n}$ yksinkertaisen ketjumurtolukuesityksen k. konvergentti, kun $k = 1, 2, ...$ Olkoon a jakson pituus ja $j = 1, 2, ...$*

(1) *Jos a on parillinen, niin yhtälöllä $x^2 - ny^2 = 1$ on positiiviset ratkaisut $x = p_{ja-1}$ ja y_{ja-1} ja yhtälöllä $x^2 - ny^2 = -1$ ei ole ratkaisuja.*
(2) *Jos a on pariton, niin yhtälöllä $x^2 - ny^2 = 1$ on positiiviset ratkaisut $x = p_{2ja-1}$ ja y_{2ja-1} ja yhtälöllä $x^2 - ny^2 = -1$ on ratkaisut $x = p_{(2j-1)-a-1}$ ja $y_{(2j-1)-a-1}$ $(j = 1, 2, ...)$*

Lause 49. *Olkoon (x_1, y_1) pienin positiivinen ratkaisu Pellin yhtälölle $x^2 - ny^2 = 1$, missä n on positiivinen kokonaisluku ja n ei ole neliöluku. Silloin kaikki positiiviset kokonaislukuratkaisut (x_k, y_k) ovat*

$$x_k + y_k\sqrt{n} = (x_1 + y_1\sqrt{n})^k, \text{ kun } k = 1, 2, 3...$$

Esimerkki 50. Tarkastellaan Pellin yhtälöä $x^2 - 26y^2 = 1$, joka esiintyi jo aiemmassa esimerkissä. Selvitetään luvun $\sqrt{26}$ ketjumurtolukuesitys.

$$\sqrt{26} = 5 + \cfrac{1}{10 + \cfrac{1}{10 + \cfrac{1}{10 + \cfrac{1}{\cdots}}}} = [5; \overline{10}].$$

Pienin positiivinen ratkaisu on $(x_1, y_1) = (51, 10)$. Nyt saadaan tuotettua uusia ratkaisuja lauseen 49 avulla seuraavasti

$$x_2 + y_2\sqrt{26} = (51 + 10\sqrt{26})^2 = 5201 + 1020\sqrt{26}.$$

Ja esimerkiksi

$$x_5 + y_5\sqrt{26} = (51 + 10\sqrt{26})^5 = 5517751251 + 1082120050\sqrt{26}.$$

4. Aritmetiikan peruslauseen yleistäminen tiettyjen algebrallisten kokonaislukujen muodostamiin renkaisiin

Aiemmassa kappaleessa esiteltiin tapa, jolla voitiin normin ja Eukleideen algoritmin avulla tuottaa Pellin yhtälölle uusia ratkaisuja. Seuraavaksi onkin mielenkiintoista lähteä tutkimaan algebrallisten kokonaislukujen muodostamia renkaita. Osalle algebrallisten kokonaislukujen muodostamille renkaille voidaan osoittaa olevan voimassa yksikäsitteinen alkutekijäesitys. Tämä onnistuu tarkastelemalla renkaiden algebrallisia ominaisuuksia. Pellin yhtälöä käsiteltäessä tutustuttiin jo renkaaseen $\mathbb{Z}[n]$, jolle voitiin määritellä normi

$$x^2 - ny^2 = (x + y\sqrt{n})(x - y\sqrt{n}).$$

Tässä luvussa osoitetaan, että yksikäsitteinen tekijöihinjako onnistuu renkaissa $\mathbb{Z}[\sqrt{-2}]$ ja $\mathbb{Z}[\zeta_3]$. Määritelmät ja todistukset seuraavat lähteitä [6] ja [7]. Geometristen todistusten ja ajatusten takana on lähde [1].

4.1. Algebrallisten kokonaislukujen muodostamat renkaat.

Vaikka käsitellään renkaita, käytetään silti samoja merkintöjä kuin perinteisillä kokonaisluvuilla laskettaessa. Olkoon R vaihdannainen rengas. Olkoot $a, b \in R$. Sanotaan, että luku b on luvun a **jakaja**, jos on olemassa $q \in R$ siten, että $a = qb$. Käytetään merkintää $b \mid a$. Voidaan sanoa myös, että luku a on luvun b **monikerta**.

Määritelmä 51. Rengas R on on epätyhjä joukko varustettuna kahdella laskutoimituksella ($+$ ja $\cdot$), jotka toteuttavat seuraavat ehdot kaikilla $a, b, c \in R$:

(1) $a + (b + c) = (a + b) + c$
(2) $a + b = b + a$
(3) on olemassa $0_R \in R$ siten, että $a + 0_R = a = 0_R + a$ kaikilla $a \in R$
(4) jokaisella $a \in R$ yhtälöllä $a + x = 0_R$ on ratkaisu $x \in R$
(5) $a(bc) = (ab)c$
(6) $a(b + c) = ab + ac$ ja $(a + b)c = ac + bc$
(7) on olemassa 1_R siten, että $a \cdot 1_R = a = 1_R \cdot a$ kaikilla $a \in R$.

Määritelmä 52. Rengas R on **vaihdannainen**, jos laskutoimitus $\cdot$ on vaihdannainen eli jos kaikilla $a, b \in R$

$$ab = ba.$$

Määritelmä 53. Olkoon R vaihdannainen rengas. Alkion $a \in R$ sanotaan olevan **kääntyvä**, jos on olemassa alkio $b \in R$ siten, että $ab = 1$. Tällöin alkiota a kutsutaan **yksiköksi** ja alkiota b (merkitään usein a^{-1}) kutsutaan alkion a **käänteisalkioksi**. **Nollanjakajaksi** sanotaan sellaista renkaan R nollasta poikkeavaa alkiota a, jolle on nollasta poikkeava $b \in R$ siten, että $ab = 0$. Alkioita 0_R ja 1_R kutsutaan laskutoimituksien $+$ ja $\cdot$ **neutraalialkioiksi.**

Määritelmä 54. Vaihdannainen rengas R, jossa $0_R \neq 1_R$, on **kokonaisalue**, jos kaikille $a, b \in R$

$$ab = 0_R, \text{ niin } a = 0_R \text{ tai } b = 0_R.$$

Kokonaisalue on siis vaihdannainen rengas, jolla ei ole nollanjakajia, mutta sillä on neutraalialkio.

Esimerkki 55. Osoitetaan, että rengas $\mathbb{Z}[\sqrt{-2}]$ on kokonaisalue.

Olkoot $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$. Oletetaan, että $\beta \neq 0$, joten halutaan osoittaa, että $\alpha = 0$. Merkitään

$$\alpha = a + b\sqrt{-2}.$$

Nyt

$$\alpha\beta = \beta(a + b\sqrt{-2}) = \beta a + \beta b\sqrt{-2} = 0,$$

ja edelleen

$$\beta a = \beta b = 0 \Rightarrow a = b = 0 \Rightarrow \alpha = 0.$$

Lisäksi huomataan, että

$$(\bar{\mu}\mu)\alpha = \bar{\mu}(\mu\alpha) = \bar{\mu}0 = 0,$$

kun $\mu \in \mathbb{Z}[\sqrt{-2}]$ ja $\mu\alpha = 0$. Tämä osoittaa, että renkaalla $\mathbb{Z}[\sqrt{-2}]$ ei ole nollanjakajia ja se on kokonaisalue.

Lemma 56. *Olkoon R vaihdannainen rengas ja $a, b, c \in R$.*

(1) *Jos $c \mid b$ ja $b \mid a$, niin $c \mid a$.*
(2) *Jos $c \mid a$, niin $c \mid ab$*
(3) *Jos $c \mid a$ ja $c \mid b$, niin $c \mid (ax + by)$ kaikilla $x, y \in R$.*

Todistus. Todistetaan jokainen kohta erikseen:

(1) Jos $b = cq_1$ ja $a = bq_2$, niin $a = c(q_1q_2)$.
(2) Jos $a = cq$, niin $ab = c(qb)$.
(3) Jos $a = cq_1$ ja $b = cq_2$, niin $ax + by = c(q_1x + q_2y)$.

□

Lause 57. *Olkoot $a \neq 0_R$ ja b kokonaisalueen R alkioita. Jos $a \mid b$ ja $b \mid a$, niin a ja b ovat* assosioituja.

Todistus. Jos $a = bq_1$ ja $b = aq_2$, niin $a = bq_1 = aq_2q_1$. Jaetaan puolittain alkiolla a. Näin voidaan tehdä, sillä R on kokonaisalue. Saadaan $1 = q_2q_1$. Tästä seuraa, että q_1 ja q_2 ovat yksiköitä sekä a ja b ovat assosioituja.

□

Määritelmä 58. Olkoon $a_1, ..., a_n$ vaihdannaisen renkaan R alkioita. Olkoon $d \in R$ nollasta poikkeava alkio, jota kutsutaan a_i:n **suurimmaksi yhteiseksi tekijäksi**, jos

(1) $d \mid a_i$ kun $1 \leq i \leq n$ ja
(2) jos $c \mid a_i$ kun $1 \leq i \leq n$, kun $c \in R$, silloin $c \mid d$.

Merkitään $d = \text{syt}(a_i, a_j)$.

Alkioita a_i kutsutaan suhteellisiksi alkutekijöiksi, jos niiden suurin yhteinen tekijä d on yksikkö.

Määritelmä 59. Olkoon D kokonaisalue ja $a \in D$.

(1) Alkiota $p \neq 0_D$ sanotaan **jaottomaksi**, jos se ei ole yksikkö ja ehdosta $p = ab$ seuraa, että joko a tai b on renkaan yksikkö.
(2) Alkiota $p \neq 0_D$ sanotaan **alkutekijäksi**, jos se ei ole yksikkö ja ehdosta $p \mid ab$ seuraa, että $p \mid a$ tai $p \mid b$.

Lemma 60. *Olkoon D kokonaisalue. Tällöin sen alkutekijät ovat jaottomia.*

Todistus. Olkoon $p \in D$ alkutekijä siten, että $ab = p$. Tällöin joko alkion a tai alkion b täytyisi olla alkion p monikerta. Oletetaan, että $p \mid a$. Merkitään $a = cp$ ja edelleen, että $cpb = p$. Tiedetään, että D on kokonaisalue ja p alkutekijä, joten täytyy olla $cb = 1$ ja b on yksikkö. Tämä osoittaa alkion p olevan jaoton.

□

Huomaa, että tämä osoittaa vain alkutekijöiden jaottomuuden kokonaisalueessa. Se ei kuitenkaan välttämättä päde toisinpäin.

Määritelmä 61. Olkoon D kokonaisalue. Se on **Eukleideen alue**, jos on olemassa funktio $N : D \setminus \{0\} \to \mathbb{N}$ siten, että

(1) $N(ab) \geq N(b)$ kaikilla nollasta poikkeavilla $a, b \in D$
(2) Mille tahansa nollasta poikkeaville $a, b \in D$ on olemassa q, r siten, että

$$a = bq + r \text{ ja } N(r) < N(b), \text{ tai } r = 0.$$

Lause 62. *Olkoon a Eukleideen alueen D alkio. Luku a on yksikkö jos ja vain jos*

$$N(a) = N(1).$$

Todistus. Olkoon $x \in D$ nollasta poikkeava alkio, jolle pätee $N(1) \leq N(1 \cdot x) = N(x)$. Jos $ab = 1$ ja a on yksikkö, niin $N(a) \leq N(ab) = N(1)$. Kun $N(a) = N(1)$ ja D on Eukleideen alue, voidaan merkitä $1 = aq + r$, jossa $r = 0$ tai $N(r) < N(a)$. Mutta koska $N(a) = N(1) \leq N(r)$, ainoa vaihtoehto on $r = 0$. Tämä osoittaa, että a on yksikkö jos ja vain jos $N(a) = N(1)$. □

Määritelmä 63. Olkoon D kokonaisalue. Se on **yksikäsitteisen tekijöihinjaon alue**, jos

(1) jokainen nollasta poikkeava alkio $a \in D$, joka ei ole yksikkö, voidaan esittää kokonaisalueen D jaottomien alkioiden tulona, ja
(2) kaksi tekijöihinjakoa $a = p_1 p_2 ... p_n = q_1 q_2 ... q_n$ ovat samat ja tekijät voidaan järjestää uudelleen siten, että alkiot q_i ja p_i ovat assosioituja, kun $p \leq i \leq n$.

Osoittamalla rengas Eukleideen alueeksi osoitetaan samalla sen olevan yksikäsitteisen tekijöihinjaon alue sekä pääideaalialue. Todistukset vaativat luvussa 5 esitettyjä tuloksia, joten tässä vaiheessa vain oletetaan kyseiset väitteet todeksi ja tutkitaan jakoyhtälöä sekä yksikäsitteistä tekijöihinjakoa algebrallisten kokonaislukujen muodostamissa renkaissa $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{-3}]$ ja $\mathbb{Z}[\zeta_3]$.

4.2. **Yksikäsitteinen tekijöihinjako renkaassa $\mathbb{Z}[\sqrt{-2}]$.** Yksikäsitteinen tekijöihinjako onnistuu renkaassa $\mathbb{Z}[\sqrt{-2}]$. Aloitetaan etsimällä kaikki kokonaislukuratkaisut Diofantoksen yhtälölle $y^3 = x^2 + 2$. Sekä Diofantos että Fermat olivat työskennelleet yhtälön parissa, mutta Euler todisti sen vuonna 1770.

Tässä luvussa esitellään kaksi erilaista lähestymistapaa tutkia renkaan $\mathbb{Z}[\sqrt{-2}]$ tekijöihinjakoa. Ensimmäisessä käytetään geometrista tulkintaa jakoyhtälölle ja osoitetaan, että renkaalle löydetään todella yksikäsitteinen tekijöihinjako. Toisessa tavassa käytetään tietoa, että Eukleideen alue on myös yksikäsitteisen tekijöihinjaon alue.

Esimerkki 64. Etsitään Diofantoksen yhtälön $y^3 = x^2 + 2$ kaikki kokonaislukuratkaisut.

Oletetaan, että yksikäsitteinen tekijöihinjako on olemassa renkaassa $\mathbb{Z}[\sqrt{-2}]$. Merkitään

$$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}.$$

Olkoot $x, y \in \mathbb{Z}$, jolloin yhtälö voidaan kirjoittaa muodossa

$$y^3 = x^2 + 2 = (x - \sqrt{-2})(x + \sqrt{-2}).$$

Lisäksi oletetaan, että (osoitetaan myöhemmin todeksi)

$$\text{syt}(x - \sqrt{-2}, x + \sqrt{-2}) = 1.$$

Tästä voidaan päätellä, että $x + \sqrt{-2}$ ja $x - \sqrt{-2}$ ovat kuutioita, koska niiden tulo on kuutio y^3. Kun oletetaan, että muotoa $a + b\sqrt{2}$ olevat luvut käyttäytyvät kuten tavalliset kokonaisluvut, voidaan tehdä päättely:

$$\begin{aligned} x + \sqrt{-2} &= (a + b\sqrt{-2})^3 \\ &= a^3 + 3a^2b\sqrt{-2} + 3ab^2(-2) + b^3(-2\sqrt{-2}) \\ &= a^3 - 6ab^2 + (3a^2b - 2b^3)\sqrt{-2}. \end{aligned}$$

Erottelemalla saadusta yhtälöstä reaali- ja imaginääriosan, saadaan yhtälöt

$$\begin{aligned} x &= a^3 - 6ab^2, \\ \sqrt{2} = (3a^2b - 2b^3)\sqrt{2} &\Rightarrow 1 = b(3a^2 - 2b^2). \end{aligned}$$

Huomataan, että ainoat kokonaisluvut, jotka toteuttavat jälkimmäisen yhtälön ovat 1 tai -1. Toisin sanoen kun $b = \pm 1$, täytyy olla myös $3a^2 - 2b^2 = \pm 1$, mistä seuraa $a = \pm 1$. Sijoittamalla $a = \pm b = \pm - 1$ ylempään yhtälöön saadaan $x = \pm 5$ ja $y = 3$. Ainut positiivinen kokonaislukuratkaisu saadaan, kun $a = -1$ ja $b = \pm 1$. Tällöin ratkaisu on $x = 5$ ja $y = 3$.

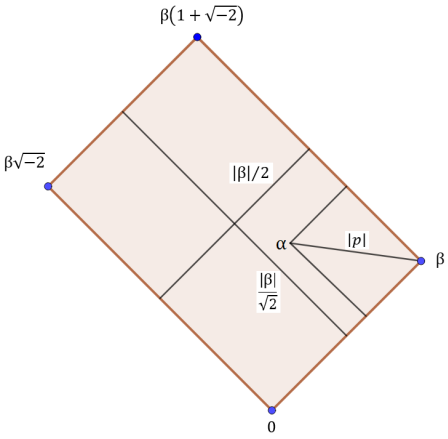
Jakoyhtälön geometrinen tulkinta

Yksikäsitteinen tekijöihinjako ja alkutekijähajotelma ovat seurausta Eukleideen algoritmin löytymisestä. Tutkitaan renkaan $\mathbb{Z}[\sqrt{-2}]$ jako-ominaisuutta ensin geometrisesti. (Vertaa jakoyhtälöön (2), jossa vastaava ominaisuus osoitettiin kokonaisluvuille.)

Lause 65. ***Jakoyhtälö renkaassa*** $\mathbb{Z}[\sqrt{-2}]$. *Olkoot* $\alpha, \beta \neq 0 \in \mathbb{Z}[\sqrt{-2}]$. *Tällöin on olemassa* ρ, $\mu \in \mathbb{Z}[\sqrt{-2}]$, *joille pätee*

$$\alpha = \mu\beta + \rho, \quad ja \quad 0 \leq |\rho| < |\beta|.$$

Todistus. Tarkastellaan kerrannaisia $\mu\beta$. Kuvassa 5 on ruudukko, jonka reunimmaiset pisteet ovat 0,β, $\beta\sqrt{-2}$ ja $\beta(1+\sqrt{-2})$.



KUVA 5. Jako-ominaisuutta renkaassa $\mathbb{Z}[\sqrt{-2}]$

Kuvaan 5 on merkitty piste $\alpha \in \mathbb{Z}[\sqrt{-2}]$, joka sijaitsee ruudukossa suorakaiteen sisäpuolella. Merkitään pisteen α etäisyyttä lähimmästä monikerrasta $\mu\beta$ merkinnällä $|\rho|$.

Pythagoraan teoreeman nojalla saadaan epäyhtälö

$$\begin{aligned} |\rho|^2 &\leq (\frac{|\beta|}{2})^2 + (\frac{|\beta|}{\sqrt{2}})^2 \\ &= \frac{|\beta|^2 + 2|\beta|^2}{4} \\ &= \frac{3}{4}|\beta|^2. \end{aligned}$$

Nyt $|\rho|^2 \leq \frac{3}{4}|\beta|^2$, joten $|\rho| < |\beta|$, mikä todistaa lauseen.

□

Renkaan $\mathbb{Z}[\sqrt{-2}]$ normi on

$$N(a + b\sqrt{-2}) = |a + b\sqrt{-2}|^2 = (a + b\sqrt{-2})(a - b\sqrt{-2}) = a^2 + 2b^2.$$

Olkoon $a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$. Yksiköt voidaan selvittää normin avulla seuraavasti

$$N(a + b\sqrt{-2}) = a^2 + 2b^2 = 1, \text{ jos ja vain jos } b = 0 \text{ ja } a = \pm 1.$$

Olkoon s ja $t \in \mathbb{Z}[\sqrt{-2}]$ renkaan alkutekijöitä. Oletetaan, että on olemassa tekijöihinjako:

$$y^3 = st.$$

Koska lukuja s ja t ei voida hajottaa enää pienempiin osiin, kuution y^3 molemmat alkutekijät voidaan ajatella kuutioiksi. Tekijät s ja t voivat olla ainoastaan 1 tai -1. Molemmat ovat kuutioita, joten voidaan todeta kuution suhteellisten alkutekijöiden olevan myös itse kuutioita.

Normin multiplikatiivisuusominaisuutta käytettiin jo tutkittaessa Gaussin kokonaislukuja ja ratkaistaessa Pellin yhtälöä. Voitaisiin osoittaa, että jos $\alpha \in \mathbb{Z}[\sqrt{-2}]$ ja $\beta \in \mathbb{Z}[\sqrt{-2}]$ niin

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

Tästä seuraisi, jos $\alpha \mid \beta$ silloin myös $N(\alpha) \mid N(\beta)$. Olkoon γ lukujen α ja β yhteinen tekijä, silloin $N(\gamma) \mid N(\alpha)$ ja $N(\gamma) \mid N(\beta)$.

Vielä täytyisi osoittaa, että syt $(x - \sqrt{-2}, x + \sqrt{-2}) = 1$.

Lause 66. *Olkoon $x, y \in \mathbb{Z}$ siten, että $y^3 = x^2 + 2$. Tällöin*

$$\text{syt}\,(x - y\sqrt{-2}, x + y\sqrt{-2}) = 1.$$

Todistus. Tutkitaan yhtälöä

$$y^3 = x^2 + 2 = (x - \sqrt{-2})(x + \sqrt{-2}).$$

Tutkitaan erikseen tilanteet, joissa x on parillinen ja pariton. Oletetaan ensin, että x on parillinen. Olkoon $k \in \mathbb{Z}$. Tällöin

$$x = 2k \Rightarrow x^2 + 2 = 4k^2 + 2 \equiv 2 \pmod 4.$$

Toisaalta

$$y = 4k + j, j \in \{0, 1, 2, 3\} \Rightarrow y^3 = 4(16k^3 + 12jk^2 + 3j^2k) + j^3 \equiv \begin{cases} 0 \\ 1 \\ 3 \end{cases} \pmod 4.$$

Yleisesti: Jos $s = \text{syt}(a, b)$, niin $s \mid a$ ja $s \mid b$, joten on olemassa k ja l siten, että $a = sk$ ja $b = sl$. Tällöin $a - b = s(k - l)$, joten $s \mid a - b$. Kahden alkion suurin yhteinen tekijä jakaa siis niiden erotuksen.

Olkoon

$$s = \text{syt}\,(x - \sqrt{-2}, x + \sqrt{-2}).$$

Tällöin $s \mid x + \sqrt{-2}$, joten

$$N(s) \mid N(x + \sqrt{-2}) = x^2 + 2.$$

Toisaalta $s \mid 2\sqrt{-2}$, joten

$$N(s) \mid N(2\sqrt{-2}) = 8.$$

Luku $N(s)$ jakaa siis parittoman luvun $x^2 + 2$ ja luvun 8. Siis $N(s) = 1$, ja s on yksikkö.

□

Nyt ollaan osoitettu, että yhtälön $y^3 = x^2 + 2$ ainoat ratkaisut luonnollisten lukujen joukossa ovat $x = 5$ ja $y = 3$. Ollaan myös saatu selville renkaan $\mathbb{Z}[\sqrt{-2}]$ yksiköt ja osoitettu, että kuutio y^3 voidaan jakaa yksikäsitteisen alkutekijähajotelman nojalla tekijöihin. Ja koska tiedetään, että yksiköt ovat myös kuutioita, voidaan merkitä

$$x - \sqrt{-2} = (a + b\sqrt{-2})^3.$$

Yksikäsitteinen alkutekijähajotelma seuraa renkaalla $\mathbb{Z}[\sqrt{-2}]$ samalla tavalla jakoominaisuudesta kuten kokonaisluvuilla. Seuraavaksi esitetään suoraviivainen todistus sille, että renkaalla $\mathbb{Z}[\sqrt{-2}]$ on yksikäsitteinen alkutekijähajotelma.

Yksikäsitteisen tekijöihinjaon todistaminen algebrallisesti

Esitellään nyt algebrallisempi tapa todistaa yksikäsitteisen alkutekijähajotelman olemassaolo osoittamalla, että rengas $\mathbb{Z}[\sqrt{-2}]$ on Eukleideen alue.

Olkoot $\alpha = a + b\sqrt{-2}$ ja $\beta = c + d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ nollasta poikkeavia, missä $a, b, c, d \in \mathbb{Z}$.

$$\begin{aligned}
N(\alpha\beta) &= N((a + b\sqrt{-2})(c + d\sqrt{-2})) \\
&= N(ac - 2bd + (ad + bc)\sqrt{-2}) \\
&= (ac - 2bd + (ad + bc)\sqrt{-2})(ac - 2bd - (ad + bc)\sqrt{-2}) \\
&= (a + b\sqrt{-2})(c + d\sqrt{-2})(a - b\sqrt{-2})(c - d\sqrt{-2}) \\
&= |a + b\sqrt{-2}|^2 |c + d\sqrt{-2}|^2 \\
&= N(\alpha)N(\beta) \geq N(\beta).
\end{aligned}$$

Olkoon

$$\frac{\alpha}{\beta} = e + f\sqrt{-2}, \text{ jossa } e, f \in \mathbb{Q}.$$

Luku $\frac{\alpha}{\beta} \in \mathbb{Q}[\sqrt{-2}]$, koska

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{|\beta|^2} = \frac{(a + b\sqrt{-2})(c - d\sqrt{-2})}{c^2 + 2d^2} = \frac{ac + 2bd}{c^2 + 2d^2} + \frac{bc - ad}{c^2 + 2d^2}\sqrt{-2} \in \mathbb{Q}[\sqrt{-2}].$$

Valitaan $u, v \in \mathbb{Z}$ siten, että $|e - u| \leq \frac{1}{2}$ ja $|f - v| \leq \frac{1}{2}$. Olkoon $q = u + v\sqrt{-2}$ ja olkoon $r = \alpha - \beta q$. Jos $r \neq 0$, niin

$$r = \alpha - \beta q = \beta(\frac{\alpha}{\beta} - q)$$

ja siten

$$\begin{aligned}
N(r) &= |\beta((e - u) + (f - v)\sqrt{-2}|^2 \\
&= |\beta|^2 |(e - u) + (f - v)\sqrt{-2}|^2 \\
&= |\beta|^2((e - u)^2 + 2(f - v)^2) \\
&\leq |\beta^2|(\frac{1}{4} + 2 \cdot \frac{1}{4}) \\
&= |\beta|^2 \frac{3}{4}.
\end{aligned}$$

Tällöin $N(r) \leq \frac{3}{4}N(\beta) < N(\beta)$, joten on osoitettu, että rengas $\mathbb{Z}[\sqrt{-2}]$ on Eukleideen alue.

Lemma 67. *Luku p on renkaan $\mathbb{Z}[\sqrt{-2}]$ alkutekijä jos ja vain jos se on jaoton.*

Todistus.
"$\Rightarrow$": Osoitettu jo lemmassa 60.
"$\Leftarrow$": Oletetaan, että p on jaoton ja halutaan osoittaa, että p on alkutekijä. Olkoot $a, b \in \mathbb{Z}[\sqrt{-2}]$. Koska p on jaoton, tällöin se ei ole yksikkö ja ehdosta $p \mid ab$ seuraa, että joko a tai b on yksikkö. Oletetaan, että alkio $p \nmid a$. Tällöin riittää osoittaa, että b on yksikkö. Voidaan merkitä syt $(a, p) = 1$ tai syt $(a, p) = p$. Jos p on suurin yhteinen tekijä, niin luku p on alkutekijä. Nyt siis

$$\text{syt}\,(a, p) = 1.$$

Tällöin lauseen 75 on olemassa $q_1, q_2 \in \mathbb{Z}[\sqrt{-2}]$ siten, että

$$1 = aq_1 + pq_2 \Rightarrow b = (ab)q_1 + p(bq_2) = (aq_1 + pq_2)b.$$

Tiedosta $p \mid ab$ seuraa, että luvun b täytyy olla yksikkö.

□

Kokonaislukujen joukossa voitaisiin osoittaa, että jaoton alkio on alkualkio (Eukleideen lemman avulla). Renkaissa tämä ei kuitenkaan välttämättä päde. Yllä osoitettiin, että väite kuitenkin pätee renkaassa $\mathbb{Z}[\sqrt{-2}]$, mutta myöhemmin tullaan huomaamaan, että esimerkiksi renkaalle $\mathbb{Z}[\sqrt{-5}]$ löytyy jaottomat tekijät $2, 3, 1 + \sqrt{-5}$ ja $1 - \sqrt{-5}$, mille $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, mutta $2 \nmid (1 + \sqrt{-5})$ tai $2 \nmid (1 - \sqrt{-5})$. Tällöin jaoton alkio ei voi olla alkualkio joka tapauksessa.

Esimerkki 68. Tarkastellaan renkaan $\mathbb{Z}[\sqrt{-2}]$ alkutekijöitä.

Olkoon $\alpha = a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ alkutekijä. Tiedetään, että renkaalla on yksikäsitteinen tekijöihinjako, joten voidaan kirjoittaa

$$(a + b\sqrt{-2})(a - b\sqrt{-2}) = p_1 p_2 \cdots p_k,$$

missä p_i ovat alkulukuja kokonaislukujen joukossa. Jakamalla puolittain luvulla $\alpha \neq 0$ ja merkitsemällä $p_i = p$ saadaan $p = \alpha(c + d\sqrt{-2})$.

Jos

$$\alpha(c + d\sqrt{-2}) = p \quad (p \text{ on oikea alkuluku}),$$

niin

$$N(\alpha) = p \quad \text{tai} \quad N(\alpha) = p^2.$$

Jos alkuluku p ei ole jaoton renkaassa $\mathbb{Z}[\sqrt{-2}]$, ei kumpikaan tekijä ole yksikkö, joten $N(\alpha) > 1$ ja $N(c+d\sqrt{-2}) > 1$. Tällöin $N(\alpha) = p$ eli luku p on tällaisessa tapauksessa muotoa $p = a^2 + 2b^2$.

Nyt ollaan tutkittu renkaan $\mathbb{Z}[\sqrt{-2}]$ yksikäsitteistä alkutekijöihinjakoa sekä geometrisesti että algebrallisemmalla tavalla. Yksi tapa olisi voinut olla myös samanlainen kuin kokonaislukuja tarkasteltaessa; ensin oltaisiin voitu todeta, että rengas voidaan

esittää alkutekijöiden tulona ja sitten osoittaa alkutekijähajotelman yksikäsitteisyys onnistuneesti (katso lemma 10 ja lause 12). Tutkielman tarkoituksena ei ole niinkään tarjota yhtä suurta lausetta jota käyttämällä ratkaistaan kaikki esimerkit, vaan tarjota mahdollisimman monipuolinen ja havainnollinen kuva käsiteltävästä asia.

4.3. Yksikäsitteisen tekijöihinjaon onnistuminen renkaassa $\mathbb{Z}[\zeta_3]$ ja epäonnistuminen renkaassa $\mathbb{Z}[\sqrt{-3}]$.

Tutkitaan rengasta

$$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\},$$

jolle voidaan määritellä normi

$$N(a + b\sqrt{-3}) = |a + b\sqrt{-3}|^2 = a^2 + 3b^2.$$

Seuraavassa esimerkissä huomataan, että yksikäsitteinen tekijöihinjako ei onnistukaan renkaassa $\mathbb{Z}[\sqrt{-3}]$.

Esimerkki 69. Luku 4 voidaan jakaa alkutekijöihin seuraavasti:

$$4 = 2 \cdot 2 = (1 - \sqrt{-3})(1 + \sqrt{-3}),$$

jolloin $N(2) = 4$. Luku 4 ei ole jaollinen muotoa $a^2 + 3b^2$ olevilla luvuilla (lukuunottamatta ykköstä). Tämä osoittaa, että luku 2 on renkaan $\mathbb{Z}[\sqrt{-3}]$ alkutekijä lemman 67 nojalla, sillä luku 2 on jaollinen vain luvulla 1 ja itsellään. Kuitenkin

$$N(1 - \sqrt{-3}) = 1 + 3 = 4,$$

joten $1 - \sqrt{-3}$ on alkutekijä ja samoin myös $1 + \sqrt{-3}$. Tämä osoittaa, että luvulla 4 on kaksi erilaista tekijöihinjakoa renkaassa $\mathbb{Z}[\sqrt{-3}]$, joten yksikäsitteinen tekijöihinjako epäonnistuu.

Vaikka yksikäsitteinen tekijöihinjako ei onnistukaan renkaassa $[\sqrt{-3}]$, on mielenkiintoista lähteä tutkimaan rengasta

$$\mathbb{Z}[\zeta_3] = \{a + b\zeta_3 : a, b \ \in \mathbb{Z}\}, \text{ jossa } \zeta_3 = \frac{-1 + \sqrt{-3}}{2},$$

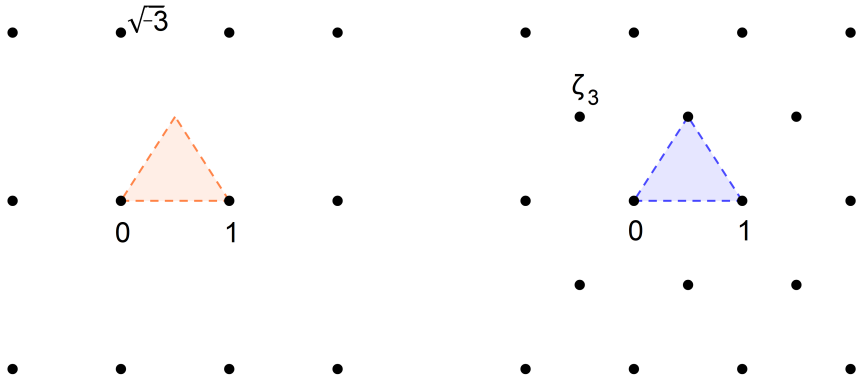
joka on ”laajennus” renkaasta $\mathbb{Z}[\sqrt{-3}]$ (katso kuva 6).

Luvussa 2.2 esiteltiin Eisensteinin kokonaisluvut. Korjauksen onnistuminen liittyy siihen, että alkion $\frac{-1+\sqrt{-3}}{2}$ voidaan osoittaa olevan algebrallinen kokonaisluku ja siten se käyttäytyy kuten kokonaisluku.

Tutkitaan ensin renkaan ominaisuuksia geometrisesti kuvaamalla rengas tasoon ja osoitetaan kuvan avulla, että sille löydetään jakoyhtälö. Tämän jälkeen esitetään algebrallisen todistuksen, joka osoittaa yksikäsitteisen alkutekijähajotelman olemassaolon.

Jakoyhtälön geometrinen tulkinta

Kuvasta 6 huomataan renkaiden $\mathbb{Z}[\sqrt{-3}]$ ja $\mathbb{Z}[\zeta_3]$ ero. Rengas $\mathbb{Z}[\sqrt{-3}]$ voidaan täydentää siten, että sille löydetään Eukleideen algoritmi ja yksikäsitteisen tekijöihinjako.

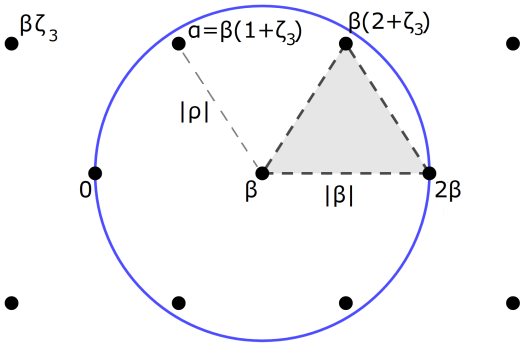


KUVA 6. Vasemmalla $\mathbb{Z}[\sqrt{-3}]$ ja oikealla $\mathbb{Z}[\zeta_3]$.

Lause 70. ***Jakoyhtälö renkaassa*** $\mathbb{Z}[\zeta_3]$. *Olkoon* $\alpha, \beta \neq 0 \in \mathbb{Z}[\zeta_3]$. *Silloin on olemassa* ρ, $\mu \in \mathbb{Z}[\sqrt{\zeta_3}]$ *siten, että*

$$\alpha = \mu\beta + \rho \quad ja \quad |\rho| < |\beta|.$$

Todistus. Kuvassa 6 on kuvattu $\mathbb{Z}[\zeta_3]$ tasossa. Voidaan olettaa, että jokainen tason piste sisältyy kolmioon ja silloin kolmion etäisyys lähimmästä kärjestä on vähemmän kuin kolmion sivun pituus. Itse asiassa sen etäisyys mistä tahansa ympäröivien kolmioiden kärjistä on vähemmän kuin sivun pituus. Tämä voidaan osoittaa piirtämällä ympyrä kolmion ympärille siten, että ympyrän keskipiste on kärjessä β.



KUVA 7. Jako-ominaisuus renkaassa $\mathbb{Z}[\zeta_3]$.

Etäisyys jollain alkiolla $\alpha \in \mathbb{Z}[\zeta_3]$ on

$$|\rho| = |\alpha - \mu\beta|.$$

Nyt kärjen α etäisyys lähimmästä kärjestä $\mu\beta$ on vähemmän kuin $|\beta|$. Tämä osoittaa, että renkaalla $\mathbb{Z}[\zeta_3]$ on jakoyhtälö. □

Yksikäsitteisen tekijöihinjaon todistaminen

Näytetään, että $\mathbb{Z}[\zeta_3]$ on Eukleideen alue ja silloin on voimassa yksikäsitteinen tekijöihinjako. Käytetään samaa oletusta, mitä käytettiin renkaan $\mathbb{Z}[\sqrt{-2}]$ käsittelyssä ja osoitetaan, että rengas $\mathbb{Z}[\zeta_3]$ on Eukleideen alue.

Olkoon

$$\mathbb{Z}[\zeta_3] = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}].$$

Luvussa 2.2 määriteltiin normi $N(a+b\zeta_3) = a^2 - ab + b^2$ renkaalle $\mathbb{Z}[\zeta_3]$. Luvussa 2.2 osoitettiin myös, että $N(\alpha) = |\alpha|^2 = \alpha\bar{\alpha}$.

Todistus. Olkoot $\alpha = a + b\zeta_3$, $\beta = c + d\zeta_3 \neq 0$ ja $\alpha, \beta \ \in \mathbb{Z}[\zeta_3]$.

$$\begin{aligned} N(\alpha\beta) &= N((a+b\zeta_3)(c+d\zeta_3)) \\ &= ((a+b\zeta_3)(c+d\zeta_3))((a+b\bar{\zeta_3})(c+d\bar{\zeta_3})) \\ &= (a+b\zeta_3)(a+b\bar{\zeta_3})(c+d\zeta_3)(c+d\bar{\zeta_3}) \\ &= N(\alpha)N(\beta). \end{aligned}$$

Nyt algebrallisessa kokonaisalueessa pätee:

$$\begin{aligned} \frac{\alpha}{\beta} &= \frac{a+b\zeta_3}{c+d\zeta_3} \\ &= \frac{(a+b\zeta_3)(c+d\bar{\zeta_3})}{(c+d\bar{\zeta_3})(c+d\bar{\zeta_3})} \\ &= \frac{ac+bc\zeta_3+ad\bar{\zeta_3}+bd\zeta_3\bar{\zeta_3}}{c^2+d^2-cd} \qquad (\zeta_3\bar{\zeta_3} = 1 \quad \text{ja} \quad \zeta_3+\bar{\zeta_3} = -1) \\ &= \frac{ac+bc\zeta_3+ad(-1-\zeta_3)+bd}{c^2+d^2-cd} \\ &= \frac{ac-ad+bd}{c^2+d^2-cd} + \frac{bc-ad}{c^2+d^2-cd}\zeta_3 \\ &= e + f\zeta_3, \end{aligned}$$

kun

$$e = \frac{ab+cd-ad}{c^2+d^2-cd} \quad \text{ja} \quad f = \frac{bc-ad}{c^2+d^2-cd}.$$

Valitaan $u, v \in \mathbb{Z}$ siten, että $|e-u| \leq \frac{1}{2}$ ja $|f-v| \leq \frac{1}{2}$. Olkoot $q = u+v\zeta_3$ ja $r = \alpha - \beta q$. Jos $r \neq 0$, niin

$$r = \alpha - \beta q = \beta(\frac{\alpha}{\beta} - q)$$

ja siten

$$\begin{aligned} N(r) &= |\beta((e-u)+(f-v)\zeta_3|^2 \\ &= |\beta|^2|(e-u)+(f-v)\zeta_3|^2 \\ &= |\beta|^2((e-u)^2+(f-v)^2-(e-u)(f-v)) \\ &\leq |\beta|^2(\frac{1}{4}+\frac{1}{4}+\frac{1}{4}) \\ &= |\beta|^2\frac{3}{4} \\ &= \frac{3}{4}N(\beta) < N(\beta). \end{aligned}$$

Tämä todistaa, että rengas $\mathbb{Z}[\zeta_3]$ on Eukleideen alue. Tulos on itseasiassa voimakkaampi kuin tässä tilanteessa oltaisiin tarvittu, mutta se todistaa yksikäsitteisen tekijöihinjaon onnistumisen renkaassa $\mathbb{Z}[\zeta_3]$. □

Yksikäsitteisen tekijöihinjaon onnistuminen renkaassa $\mathbb{Z}[\zeta_3]$ auttaisi Diofantoksen yhtälön $x^3+y^3=z^3$ ratkaisussa, sillä yhtälö voitaisiin muuttaa muotoon

$$x^3+y^3=(x+y)(x+\zeta_3 y)(x+\zeta_3^2 y).$$

Renkaan $\mathbb{Z}[\zeta_3]$ tekijöihinjakoa hyödyntämällä saataisiin todistettua, että yhtälöllä $x^3+y^3=z^3$ ei ole ratkaisuja luonnollisten lukujen joukossa. Tästä lisää lähteessä [1, s. 129-136].

Nyt ollaan osoitettu, että yksikäsitteinen tekijöihinjako onnistuu algebrallisten kokonaislukujen muodostamissa renkaissa $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-2}]$ ja $\mathbb{Z}[\zeta_3]$, sekä osoitettiin, että yksikäsitteinen tekijöihinjako ei ole voimassa renkaassa $\mathbb{Z}[\sqrt{-3}]$. Seuraavaksi tullaan huomaamaan, että yksikäsitteinen tekijöihinjako ei onnistu myöskään renkaassa $\mathbb{Z}[\sqrt{-5}]$. Tilannetta voidaan kuitenkin ”korjata” ideaalien avulla.

5. Ideaali-käsitteen käyttöönotto

Kuten jo aiemmista esimerkeistä huomattiin, aritmetiikan peruslausetta ei voida yleistää pätemään kaikille algebrallisten kokonaislukujen muodostamille renkaille. Renkaan $\mathbb{Z}[\sqrt{-3}]$ tilanteessa rengas "korjattiin" laajentamalla se renkaaksi $\mathbb{Z}[\zeta_3]$. Tässä luvussa otetaan käyttöön käsite *ideaali*, jonka avulla voidaan täsmentää ja täydentää aiemmin esitettyjä ajatuksia. Yksikäsitteinen tekijöihinjako epäonnistuu myös renkaassa $\mathbb{Z}[\sqrt{-5}]$, ja sitä ei voida laajentaa samalla tavalla kuin rengas $\mathbb{Z}[\sqrt{-3}]$. Richard Dedekind on merkittävä henkilö ideaalien teorian kehittämisessä. Hän huomasi, että sellaisille renkaille, joissa yksikäsitteinen tekijöihinjako epäonnistuu, voidaan kuitenkin mahdollisesti määrittää yksikäsitteinen tekijöihinjako alkuideaaleilla, jotka eivät kuitenkaan ole pääideaaleja. Luvun todistukset ja määritelmät seuraavat lähteitä [1], [6] ja [7]. Geometristen ideoiden taustalla on lähde [1].

Tässä luvussa sisältyvyydelle eli inkluusiolle käytetään symbolia $\subset$. Kun $A \subset B$, sanotaan joukon A olevan joukon B osajoukko. Jos $A \subset B$ ja $B \subset A$, niin $A = B$. Sisältyvyys ei kiellä mahdollisuutta, että joukot olisivat samoja. Toisin sanoen siis sisältyvyyden ei tarvitse olla aitoa.

5.1. **Ideaalin määritelmä ja ominaisuudet.**

Määritelmä 71. Ideaali I on renkaan R epätyhjä osajoukko siten, että

(1) $a \in I$ ja $b \in I \Rightarrow a + b \in I$
(2) $a \in I$ ja $r \in R \Rightarrow ar \in I$.

Ideaalille I on määritelty yhteen- ja kertolasku. Lisäksi sille voitaisiin määritellä myös vähennyslasku.

Lause 72. *Olkoon R vaihdannainen rengas ja $c_1, c_2, .., c_n \in R$ ja*

$$I = \{r_1c_1 + r_2c_2 + \cdots + r_nc_n : r_1, ..., r_n \in R, n \in \mathbb{Z}\}. \tag{8}$$

Tällöin I on renkaan R ideaali ja sanotaan, että I on alkioiden c_j virittämä ideaali.

Todistus. Olkoon

$$a = r_1c_1 + r_2c_2 + ... + r_nc_n \in I \text{ ja } b = s_1c_1 + s_2c_2 + ... + s_nc_n \in I.$$

Tällöin

$$a - b = (r_1 - s_1)c_1 + ... + (r_n - s_n)c_n \in I,$$

joten ensimmäinen ehto pätee.

Olkoon $u \in R$. Liitännäisyydestä seuraa, että

$$ua = au = (ur_1)c_1 + (ur_2)c_2 + ... + (ur_n)c_n \in I.$$

Tämä osoittaa, että I on renkaan ideaali. □

Määritelmä 73. Vaihdannaisen renkaan R ideaali I on **pääideaali**, jos se voidaan esittää muodossa

$$I = \{rc_1 : r \in R\}.$$

Merkitään

$$I = (c_1).$$

Jos renkaan kaikki ideaalit pääideaaleja, niin R on **pääideaalialue**.

Esimerkki 74. Osoitetaan, että kaikki kokonaislukujen ideaalit ovat pääideaaleja.

Tapaus $I = (0)$ selvä, joten oletetaan, että $I \neq (0)$. Tällöin ideaali I on epätyhjä joukko, jolla on pienin positiivinen alkio a. Ideaalille on voimassa kertolasku ja I sisältää kaikki alkiot $ar, r \in \mathbb{Z}$. Täten

$$(a) \subset I.$$

Jos $b = 0$, niin selvästi $b = a0 \in (a)$. Olkoon $b \in I$ siten, että $b \neq 0$. Oletetaan, että $b > 0$. Tällöin jakoyhtälön nojalla on olemassa alkiot $q, r \in \mathbb{Z}$, jotka toteuttavat yhtälön

$$b = aq + r \quad \text{ja} \quad 0 \leq r < a.$$

Nyt $r = b - aq \in I$ $(a, b \in I)$, mikä seuraa määritelmästä 71. Oletuksesta $r < a$ ja tiedosta, että a on pienin alkio ideaalissa I, saadaan $r = 0$. Täten $b = aq \in (a)$ ja $I \subset (a)$, mikä osoittaa, että $I = (a)$.

Lause 75. *Olkoon R vaihdannainen rengas ja olkoot alkiot $a, b, d \in R$ ja $d \neq 0_R$. Jos*

$$dR = aR + bR = \{ar_1 + br_2 : r_1, r_2 \in R\},$$

silloin syt $(a, b) = d$.

Todistus. Olkoon $aR+bR$ on pienin ideaali, joka sisältää alkiot a ja b. Oletetaan, että $dR = aR+bR$ $(a, b \in dR)$. Tällöin $a \in aR \subset aR+bR = dR$ sekä $d \mid a$ ja $d \mid b$. Olkoot $a = sc$ ja $b = ct$. Ja koska tiedetään, että $d \in dR = aR + bR$, saadaan

$$d = ua + vb = usc + vct = (us + vt)c \Rightarrow c \mid d.$$

Tämä osoittaa, että syt $(a, b) = d$. □

Lemma 76. *Olkoon D pääideaalialue ja alkiot $a, b \in D$ siten, että $a, b \neq 0_D$. Tällöin on olemassa alkiot $s, t \in D$ siten, että*

$$\text{syt}\,(a, b) = as + bt.$$

Lisäksi alkioiden a ja b kaksi suurinta yhteistä tekijää ovat assosioituja.

Todistus. Olkoot $a, b \neq 0_D$. Koska D on pääideaalialue, voidaan valita ideaalin $aD + bD$ generoiva alkio $d \neq 0_D$. Aiemman lemman nojalla d on suurin yhteinen tekijä ja se voidaan esittää muodossa $as + bt$, kun $s, t \in R$. Jos d' on toinen suurin yhteinen tekijä, silloin $d' \mid d$ ja $d \mid d'$, mistä seuraa viimeinen väite. □

Lemma 77. *Olkoon R rengas ja alkiot $a, b \in R$. Tällöin $(a) \subset (b)$, jos ja vain jos $b \mid a$.*

Todistus.
"⇒": Oletetaan ensin $(a) \subset (b)$. Oletuksesta seuraa, että $a \in (a)$ ja edelleen $a \in (b)$. Tällöin on olemassa $k \in R$ siten, että $a = bk$, joten $b \mid a$.
"⇐": Oletetaan nyt, että $b \mid a$. Olkoon $ka \in (a)$. Oletuksesta seuraa, että on olemassa $n \in D$ siten, että $a = nb$. Tästä seuraa, että $ka = knb \in (b)$, mikä osoittaa $(a) \subset (b)$.
□

Voidaan siis sanoa, että inkluusio tarkoittaa pääideaaleille samaa kuin ideaalien virittävien alkioiden jaollisuus.

Esimerkki 78. Olkoon $p \in \mathbb{Z}$ alkuluku ja ideaali $(ab) \subset (p)$. Osoitetaan, että silloin myös $(a) \subset (p)$ tai $(b) \subset (p)$.

Esimerkissä 74 osoitettin, että kaikki kokonaislukujen ideaalit ovat pääideaaleja, joten olkoot $(a) = \{ar : r \in R\}$ ja $(b) = \{br : r \in R\}$. Oletetaan, että $(a) \not\subset (p)$, jolloin osoitettavaksi jää, että $(b) \subset (p)$. Lemman 77 nojalla tiedetään, että

$$(b) \subset (p) \Leftrightarrow p \mid a$$

ja tällöin $(a) \not\subset (p) \Rightarrow p \nmid a$. Tiedetään, että

$$\begin{aligned}(ab) &\subset (p)\\ &\Rightarrow p \mid ab\\ &\Rightarrow p \mid b\\ &\Rightarrow (b) \subset (p),\end{aligned}$$

joten väite on todistettu.

5.2. **Eukleideen alue on yksikäsitteisen tekijöihinjaon alue.** Jos tiedetään, että renkaalla on voimassa Eukleideen algorimi, voidaan sen osoittaa olevan Eukleideen alue. Tässä luvussa todistetaan, että jokainen Eukleideen alue on myös yksikäsitteisen tekijöihinjaon alue. Lisäksi huomataan, että jos rengas on Eukleideen alue, niin se on myös pääideaalialue. Tässä luvussa otetaan käyttöön käsite *alkuideaali*. Alkuideaalit ovat alkutekijöitä ideaalien joukossa kuten alkuluvut ovat kokonaislukujen joukossa.

Lause 79. *Olkoon p jaoton alkio pääideaalialueessa D. Jos $a, b \in D$ ja $p \mid ab$, niin $p \mid a$ tai $p \mid b$.*

Todistus. Oletetaan, että $p \mid ab$ ja $p \nmid a$. Silloin $\operatorname{syt}(p, a) = 1$. Tällöin on olemassa $q_1, q_2 \in D$, siten että

$$\begin{aligned}1 &= pq_1 + aq_2\\ b &= p(bq_1) + (ab)q_2.\end{aligned}$$

Ja koska $p \mid ab$, täytyy olla $p \mid b$. □

Määritelmä 80. Ideaalia I sanotaan renkaan R **aidoksi ideaaliksi**, jos $I \neq R$.

Määritelmä 81. Olkoon $I \neq (1)$ vaihdannaisen renkaan R aito ideaali. Jos ehdosta $ab \in I$ seuraa, että $a \in I$ tai $b \in I$ kaikilla $a, b \in R$, sanotaan ideaalin olevan renkaan R **alkuideaali.** Ideaalin I sanotaan olevan renkaan R **maksimaalinen ideaali**, jos kaikilla renkaan R ideaaleilla J ehdosta $I \subset J \subset R$ seuraa, että $J = I$ tai $J = R$. Jos ideaali $I = (1)$, käytetään ideaalille nimitystä **yksikköideaali**.

Lemma 82. *Olkoon D pääideaalialue ja $p \in D$ siten, että $p \neq 0_D$. Tällöin p on jaoton pääideaalialueessa D, jos ja vain jos pD on alkuideaali pääideaalialueessa D.*

Todistus.
"⇒": Oletetaan, että $p \in D$ on jaoton. Jos $ab \in D$, kun $a, b \in D$, niin lauseen 79 nojalla joko $a \in pD$ tai $b \in pD$. Täten pD on alkuideaali.
"⇐": Olkoon $pD \subset D$ alkuideaali. Jos p ei ole jaoton, silloin $p = ab$ joillain alkioilla $a, b \in D$, jotka eivät ole yksiköitä. Koska $ab \in pD$ oletuksesta seuraa, että $a \in pD$ tai $b \in pD$ ja edelleen joko $p \mid a$ tai $p \mid b$. Jos $p \mid a$, niin $a = pc$ jollain $c \in D$ ja siten $p = pcb$. Saadaan, että $cd = 1$. Seuraa ristiriita oletuksen kanssa, sillä b ei ole yksikkö. Jos $p \mid b$ niin päädytään samanlaiseen ristiriitaan. Tämä osoittaa, että pD on alkuideaali, $p \neq (1)$ ja se on silloin jaoton. □

Lemma 83. *Olkoon D pääideaalialue. Oletetaan, että $I_1 \subset I_2 \subset ...$ Tällöin $I_n = I_m$ kaikilla $n > m$.*

Todistus. Olkoon $I_1 \subset I_2 \subset ...$ mikä tahansa nouseva ideaalien ketju ja olkoon

$$I = \bigcup_{n=1}^{\infty} I_n.$$

Jos $a, b \in I$, niin $a \in I_j$ ja $b \in I_k$, jollain $j, k \in \mathbb{N}$. Oletetaan, että $j \geq k$ ja silloin $a + b \in I_j$. Saadaan $a + b \in I_j \subset I$. Jos $r \in D$, niin $ra \in I_j \subset I$. Nyt I on ideaali pääideaalialueessa D ja $I = cD$, jollain $c \in D$. Olkoon $c \in I_m$, jollain $m \in \mathbb{N}$. Siitä seuraa, että $I = cD \subset I_m$ ja

$$I_n = I = I_m \text{ kaikilla } n > m.$$

□

Lause 84. *Jokainen maksimaalinen ideaali on alkuideaali.*

Todistus. Oletetaan, että M on maksimaalinen ideaali siten, että $ab \in M$ ja $a \notin M$. Halutaan siis osoittaa, että $b \in M$. Merkitään

$$M[a] = \{ar + ms : r, s \in R, m \in M\}.$$

Ideaali $M[a]$ sisältää ideaalin M ja alkion a, sekä $M, a \in R$. Maksimaalisuuden takia pitää olla $M[a] = D$, joten $1 \in M[a]$. Tällöin saadaan osoitettua, että

$$\begin{aligned} 1 &= ar + ms \\ b &= (ab)r + m(bs) \\ &\Rightarrow b \in M, \text{ sillä } ab \in M \text{ ja } m \in M, \end{aligned}$$

mikä todistaa väitteen. □

Nyt ollaan osoitettu, että jokainen maksimaalinen ideaali on alkuideaali. Tämä ei kuitenkaan tarkoita, että alkuideaali olisi aina maksimaalinen. Esimerkissä 74 on osoitettu, että kaikki kokonaislukujen ideaalit ovat pääideaaleja. Kuitenkin huomataan, että (0) on alkuideaali, mutta se ei ole maksimaalinen. Tietyissä tilanteissa alkuideaali on maksimaalinen ja seuraavaksi esitetään kyseinen tulos. Tätä tietoa tullaan tarvitsemaan renkaan $\mathbb{Z}[\sqrt{-5}]$ yksikäsitteisen alkuideaalihajotelman todistuksessa.

Lause 85. *Jokainen nollasta poikkeava alkuideaali pääideaalialueessa on maksimaalinen.*

Todistus. Olkoon $P \neq (0)$ alkuideaali pääideaalialueessa D. Olkoon J ideaali, jolle pätee $P \subset J \subset D$. Sillä D on pääideaalialue, voidaan olettaa, että $P = Da$ ja $J = Db$, jollain $ab \in D$. Tällöin $a \in A$ ja saadaan, että $a \in J$. Tällöin on olemassa $d \in D$ siten, että $a = db$. Tästä seuraa, että $db \in P$ ja joko $b \in P$ tai $d \in P$. Nyt jos $b \in P$, niin $P = D$. Jos $d \in P$, niin $d = sa \quad (s \in D)$ ja siten P on alkion a virittämä alkuideaali. Tällöin

$$a = sab \Rightarrow 1 = sb,$$

mikä osoittaa, että $1 \in J$ ja siten $S = D$. □

Lause 86. *Jokainen Eukleideen alue on pääideaalialue.*

Todistus. Olkoon D Eukleideen alue ja ideaali $I \neq (0) \subset D$. Olkoon

$$J = \{N(d) \in \mathbb{N} : d \in I, d \neq 0\}.$$

Tällöin J on luonnollisten lukujen joukon epätyhjä osajoukko, joten joukossa J on pienin luku (lause 1) eli on olemassa $d \in I$, $d \neq 0$, jolle $N(d) \leq N(c)$ kaikille $c \in I$, $c \neq 0$. Osoitetaan, että

$$I = dD.$$

Tiedetään, että $d \in I$ ja tällöin myös $dD \subset I$, joten riittää osoittaa $I \subset dD$. Olkoon $a \in I$ ja merkitään $a = dq + r$, missä $r = 0$ tai $N(r) < N(d)$. Koska $N(d)$ on joukon pienin alkio, täytyy olla $r = 0$. Tällöin $a = dq \in dD$, mikä täydentää väitteen todistuksen ja ollaan osoitettu, että $I = dD$. □

Lause 87. *Jokainen pääideaalialue on yksikäsitteisen tekijöihinjaon alue.*

Todistus. Olkoon D pääideaalialue ja olkoon $d \in D$ siten, että d ei ole yksikkö ja se on nollasta poikkeava. Oletetaan, että alkiota d ei voi kirjoittaa jaottomien alkioiden tulona, joten d ei ole silloin jaoton. Koska d ei ole jaoton, merkitään $d = a_1 b_1$, missä pääideaalialueen alkiot a_1, b_1 eivät ole yksiköitä.

Oletetaan ensin, että alkiota a_1 ei voi kirjoittaa jaottomien alkioiden tulona. Oletuksesta seuraa, että b_1 ei ole yksikkö, joten saadaan $dD \subset a_1 D$. Jatketaan samaa prosessia ja otetaan alkiosta a_1 tekijä a_2, jota ei voida esittää jaottomien alkioiden tulona. Saadaan $a_1 D \subset a_2 D$. Jatkamalla näin saadaan

$$dD \subset a_1 D \subset a_2 D \subset ...$$

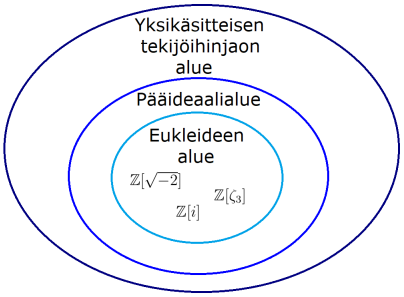
mikä on ristiriidassa lemman 83 kanssa.

Oletetaan nyt, että $d = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, missä $n \leq m$. Toisin sanoen oletetaan, että d voidaan kirjoittaa kahdella eri tavalla jaottomien alkioiden tulona. Koska p_1 on jaoton ja jakaa jonkin alkioista $q_1 q_2 \cdots q_m$. Voidaan sanoa, että $p_1 \mid q_i$, jollain $i = 1$. Tiedetään, että p_1 ja q_1 ovat jaottomia ja järjestystä vaihtamalla voidaan olettaa, että $p_1 \mid q_1$. Voidaan merkitä

$$p_2 \cdots p_n = u q_2 \cdots q_m, \text{ missä } u \text{ on yksikkö.}$$

Jatkamalla prosessia saadaan lopulta, että p_i ja q_i ovat jaottomia ja $p_i \mid q_i$. □

Seuraus 88. *Eukleideen alue on yksikäsitteisen tekijöihinjaon alue.*



KUVA 8. Eukleideen alue on pääideaalialue ja yksikäsitteisen tekijöihinjaon alue.

Täytyy kuitenkin muistaa, että jokainen Eukleideen alue on yksikäsitteisen tekijöihinjaon alue, mutta jokainen yksikäsitteisen tekijöihinjaonalue ei ole Eukleideen alue.

Esimerkki 89. Osoitetaan, että yksikäsitteinen tekijöihinjako epäonnistuu renkaassa $\mathbb{Z}[\sqrt{-5}]$.

Olkoon

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : \ a, b \ \in \ \mathbb{Z}\}.$$

Olkoon $r = a + b\sqrt{-5} \in R$, ja määritellään $N(r) = a^2 + 5b^2$. Jos a on kokonaisalueen R yksikkö, silloin $N(r)N(r^{-1}) = N(rr^{-1}) = 1$ ja täytyisi olla $N(r) = 1$. Tällöin ainoa mahdollisuus olisi, että $a = \pm 1$ ja $b = 0$ ja silloin kokonaisalueen R yksiköt olisivat ± 1.

Tutkimalla kokonaislukua 6, huomataan että sillä on kaksi erilaista tekijöihinjakoa

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Osoitetaan, että luvut $2, 3, 1 + \sqrt{-5}$ ja $1 - \sqrt{-5}$ ovat jaottomia kokonaisalueessa R, minkä avulla voidaan osoittaa ettei kokonaisalue R ei ole yksikäsitteisen tekijöihinjaon alue.

Aloitetaan sillä, että tutkitaan yhtälöitä $a^2 + 5b^2 = 2$ ja $a^2 + 5b^2 = 3$. Huomataan, että yhtälöillä ei ole kokonaislukuratkaisuja ja siten kokonaisalueella R ei ole alkioita, joiden normi olisi 2 tai 3. Jos $rs = 3$, jossa $r, s \in R$ ja r, s eivät ole yksiköitä, niin $N(r)N(s) = N(3) = 9$. Täytyy olla $N(r) > 1$ ja $N(s) > 1$. Näistä tiedoista voidaan päätellä, että $N(r) = 3$ ja $N(s) = 3$, mistä seuraa ristiriita. Samalla tavalla voitaisiin osoittaa, että 2 on jaoton kokonaisalueessa R.

Jos $rs = 1 + \sqrt{-5}$, missä luvut $r, s \in R$ eivät ole yksiköitä, seuraa $N(r)N(s) = N(1 + \sqrt{-5}) = 6$. Tämä on ristiriita, sillä $N(r) = 2$ tai $N(r) = 3$. Samalla tavalla osoitettaisiin myös $1 - \sqrt{-5}$ jaottomuus kokonaisalueessa R, joten on todistettu $\mathbb{Z}[\sqrt{-5}]$ ei ole yksikäsitteisen tekijöihinjaon alue.

5.3. **Tekijöihinjaon tutkimista renkaassa $\mathbb{Z}[\sqrt{-3}]$.** Esimerkissä 69 osoitettiin, että $\mathbb{Z}[\sqrt{-3}]$ ei ole yksikäsitteisen tekijöihinjaon alue. Lauseista 86 ja 87 seuraa, että se ei ole myöskään pääideaalialue. Renkaille $\mathbb{Z}[\sqrt{-3}]$ ja $\mathbb{Z}\sqrt{-5}$, joille yksikäsitteinen tekijöihinjako epäonnistuu, voidaan löytää kuitenkin tekijöihinjaot käyttäen ideaaleja, jotka eivät ole pääideaaleja. Lähdetään nyt tutkimaan jako-ominaisuutta tarkemmin renkaissa $\mathbb{Z}[\sqrt{-3}]$ ja $\mathbb{Z}[\sqrt{-5}]$, joissa yksikäsitteinen tekijöihinjako epäonnistuu.

Esimerkistä 69 huomataan, että luvulle 4 voidaan löytää kaksi erilaista tekijöihinjakoa

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Tämä siis tarkoittaa, että tekijöihinjako ei ole yksikäsitteinen. Ottamalla mukaan ideaalit voidaan muodostaa ideaali $(2)+(1+\sqrt{-3})$, joka on summa lukujen 2 ja $1+\sqrt{-3}$ monikerroista.

Osoitetaan, että

$$(2) + (1 + \sqrt{-3}) = \{2m + (1 + \sqrt{-3})n : m, n \in \mathbb{Z}\}. \tag{9}$$

Valitaan jokin ideaalin $(2) + (1 + \sqrt{-3})$ mielivaltainen alkio. Merkitään sitä

$$2(a + b\sqrt{-3}) + (1 + \sqrt{-3})(c + d\sqrt{-3}) \qquad a, b, c, d \in \mathbb{Z}.$$

Järjestelemällä alkion termejä saadaan

$$2(a - b - 2d) + (1 + \sqrt{-3})(2b + c + d) = 2m + (1 + \sqrt{-3})n, \quad m, n \in \mathbb{Z}.$$

Tällöin siis

$$(2) + (1 + \sqrt{-3}) \subset \{2m + (1 + \sqrt{-3})n : m, n \in \mathbb{Z}\}.$$

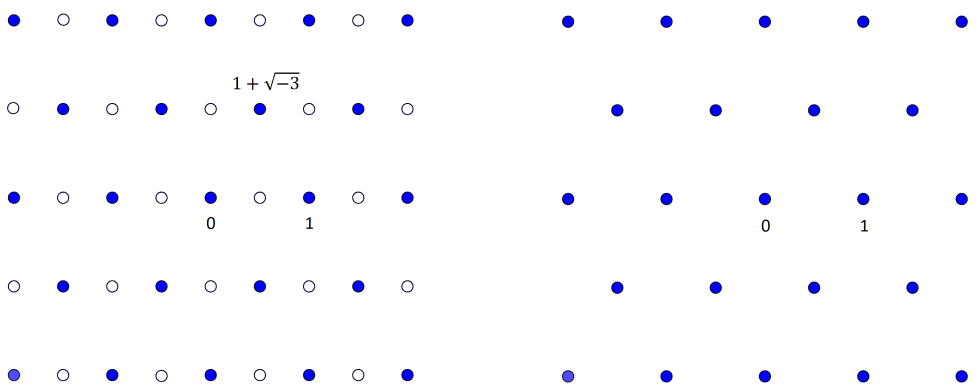
Lisäksi

$$\{2m + (1 + \sqrt{-3})n : m, n \in \mathbb{Z}\} \subset (2) + (1 + \sqrt{-3}),$$

mikä seuraa tiedosta, että ideaali $(2)+(1+\sqrt{-3})$ sisältää kaikki lukujen 2 ja $1+\sqrt{-3}$ monikertojen summat. Tämä osoittaa väitteen.

Kuvan 9 vasemmalla puolella on merkitty sinisellä ideaali $(2)+(1+\sqrt{-3})$. Vertaamalla oikeaan puoleen huomataan, että kuviot ovat täsmälleen samat: molemmissa kuvioissa tasoon muodostuu kolmiohila. Vertaamalla kuvaan 6, jossa on esitetty $\mathbb{Z}[\sqrt{-3}]$ tasossa, huomataan kuvion olevan erilainen.

Olkoon a renkaan $\mathbb{Z}[\sqrt{-3}]$ alkio. Jos ideaali $(2)+(1+\sqrt{-3})$ olisi pääideaali, niin kaikki renkaan $\mathbb{Z}[\sqrt{-3}]$ alkiot kuuluisivat ideaaliin. Täytyisi siis olla $(2) + (2 + \sqrt{-3}) = (a)$. Kuvasta huomataan, että näin ei ole, joten $(2) + (1 + \sqrt{-3})$ ei ole renkaan $\mathbb{Z}[\sqrt{-3}]$ pääideaali. Puolestaan jokainen renkaan $\mathbb{Z}[\zeta_3]$ alkio kuuluu ideaaliin $(\frac{1+\sqrt{-3}}{2})$, joten se on pääideaali. Kuvasta 9 nähdään, että ideaali $(2)+(1+\sqrt{-3})$ näyttää täsmälleen samalta tasossa kuin ideaali $(\frac{1+\sqrt{-3}}{2})$. Luvussa 4.3 näytettiin, että $\mathbb{Z}[\zeta_3]$ on Eukleideen alue, joten se on myös pääideaalialue. Tästä voidaan siis yhteenvetona sanoa, että $(2) + (1 + \sqrt{-3}) \subset \mathbb{Z}[\sqrt{-3}]$ ei ole pääideaali, mutta ottamalla mukaan niin sanotut ”ideaaliluvut” rengas $\mathbb{Z}[\sqrt{-3}]$ täydentyy renkaaksi $\mathbb{Z}[\zeta_3]$.



KUVA 9. Vasemmalla $(2)+(1+\sqrt{-3}) \in \mathbb{Z}[\sqrt{-3}]$ ja oikealla $(\frac{1+\sqrt{-3}}{2}) = \mathbb{Z}[\zeta_3]$

Luku $\frac{1+\sqrt{-3}}{2}$ jakaa luvut 2 ja $1+\sqrt{-3}$ renkaassa $\mathbb{Z}[\zeta_3]$ ja sen normi on 1. Tästä seuraa, että

$$\text{syt}\,(2, 1+\sqrt{-3}) = \frac{1+\sqrt{-3}}{2}.$$

Jatkamalla tarkastelua samoin kuin luvussa 4.3 voitaisiin tutkia tekijöihinjakoa ja osoittaa sen yksikäsitteisyys. Toisin sanoen renkaalla $\mathbb{Z}[\sqrt{-3}]$ voidaan määrittää yksikäsitteinen tekijöihinjako ideaalien avulla, mutta koska se tapahtuu ideaalilukujen avulla alkuperäisen renkaan ulkopuolella. Se ei kuitenkaan ole sama asia kuin yksikäsitteinen tekijöihinjako eli aritmetiikan peruslause.

5.4. **Tekijöihinjaon tutkimista renkaassa $\mathbb{Z}[\sqrt{-5}]$.** Renkaassa $\mathbb{Z}[\sqrt{-5}]$ ei voida suorittaa samanlaista korjaustoimenpidettä kuin tehtiin laajennettaessa $\mathbb{Z}[\sqrt{-3}]$ renkaaksi $\mathbb{Z}[\zeta_3]$. Tämä johtuu siitä, että $\mathbb{Z}[\sqrt{-5}]$ sisältää jo kaikki kokonaisluvut renkaasta $\mathbb{Q}[\sqrt{-5}]$.

Esimerkissä 89 osoitettiin, että luvulle 6 löydetään kaksi tekijöihinjakoa

$$2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Luvuille $2, 3, 1+\sqrt{-5}$ ja $1-\sqrt{-5}$ voidaan laskea normit $4, 9, 6, 6$. Huomataan, että ei ole olemassa sellaista lukua $a+b\sqrt{-5} \in \mathbb{Z}[-5]$, jonka normi a^2+5b^2 olisi 2 tai 3. Voidaan todeta, että luvut $2, 3, 1+\sqrt{-5}$ ja $1-\sqrt{-5}$ ovat alkutekijöitä renkaassa $\mathbb{Z}[\sqrt{-5}]$. Aloitetaan etsimällä ”suurin yhteinen tekijä”. Olkoon

$$(2)+(1+\sqrt{-5}),$$

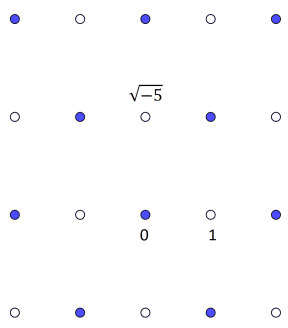
joka on summa luvun 2 monikerroista ja luvun $1+\sqrt{-5}$ monikerroista. Toteuttamalla samanlainen laskutoimitus kuin käsiteltäessä rengasta $\mathbb{Z}[\sqrt{-3}]$, saadaan

$$2(a+b\sqrt{-5})+(1+\sqrt{-5})(c+d\sqrt{-5}) \in (2)+(1+\sqrt{-5})$$

ja edelleen tulos

$$(2)+(1+\sqrt{-5}) = \{2m+(1+\sqrt{-5})n : m, n \in \mathbb{Z}\}.$$

Ideaali on esitetty kuvassa 10. Kuvasta huomataan selkeästi, että siniset pallot (kuuluvat ideaaliin) eivät ole kohtisuorassa, kuten pisteet olisivat renkaassa $\mathbb{Z}[\sqrt{-5}]$. Ylei-



KUVA 10. $(2) + (1 + \sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$.

semmin sanottuna renkaan $\mathbb{Z}[\sqrt{-5}]$ alkiot kerrottuna luvulla β muodostavat renkaan ideaalin (β). Tämä ideaali ei ole kuitenkaan pääideaali, joten rengas $\mathbb{Z}[\sqrt{-5}]$ ei ole pääideaalialue.

5.4.1. ***Tekijöihinjako ideaalien avulla.***

Määritelmä 90. Olkoon A ja B renkaan R ideaaleja. Silloin

$$AB = \{a_1b_1 + a_2b_2 + \cdots + a_kb_k : k \in \mathbb{Z}_+, a_i \in A, b_i \in B\}.$$

Määritelmä 91. Jokainen P on **alkuideaali**, jos

$$AB \subset P \Rightarrow A \subset P \text{ tai } B \subset P.$$

Lause 92. *Olkoon P alkuideaali. Seuraavat kohdat ovat ekvivalentit*

(1) $AB \subset P \Rightarrow A \subset P$ *tai* $B \subset P$.
(2) $ab \in P \Rightarrow a \in P$ *tai* $b \in P$.

Todistus. Osoitetaan ensin (1) $\Rightarrow$ (2):
Olkoon $ab \in P$, joten $(ab) \subset P$, mikä seuraa ideaalin ominaisuuksista. Tällöin myös $(a)(b) \subset P$. Oletuksen mukaan $(a) \subset P$ tai $(b) \subset P$ ja tällöin $a \in P$ tai $b \in P$, sillä tiedetään, että $a \in (a)$ ja $b \in (b)$.

Osoitetaan sitten (2) $\Rightarrow$ (1):
Oletetaan, että $AB \subset P$ ja $A \not\subset P$. Halutaan siis osoittaa, että $B \subset P$. Olkoon $a \in A$ siten, että $a \notin P$. Tällöin myös $ab \in P$. Oletuksesta (2) seuraa, että $a \in P$ tai $b \in P$. Koska oletuksen mukaan $a \notin P$, täytyy olla $b \in P$. Tästä seuraa, että $B \subset P$.

□

Laskujen lukemisen helpottamiseksi merkitään ideaaleja seuraavasti lukupareina (α, β). Esimerkiksi merkitään

$$(2) + (1 + \sqrt{-5}) = (2, 1 + \sqrt{5}).$$

Tämä kannattaa huomioida välttääkseen väärinkäsitykset seuraavassa esimerkissä.

Esimerkki 93. Osoitetaan seuraavat alkuideaalihajotelmat

a) $(2) = (2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5})$

Määritelmästä 90 saadaan, että

$$\begin{aligned} 4 = 2 \cdot 2 &\in (2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5}), \\ 2 + 2\sqrt{-5} = 2 \cdot (1 + \sqrt{-5}) &\in (2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5}), \\ -4 + 2\sqrt{-5} = (1 + \sqrt{-5})(1 + \sqrt{-5}) &\in (2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5}). \end{aligned}$$

Tiedetään, että

$$4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5} \in (2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5})$$

ja koska yhteen- ja vähennyslasku on voimassa, saadaan

$$2 \in (2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5}).$$

Kaikki luvun 2 monikerrat kuuluvat joukkoon $(2, 1+\sqrt{-5})(2, 1+\sqrt{-5})$, mistä seuraa että

$$(2) \subset (2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5}).$$

Vielä täytyy osoittaa toinen suunta. Jokainen alkio, joka kuuluu joukkoon $(2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5})$ koostuu termeistä $2m$ ja $(1 + \sqrt{-5})n$. Mikä tahansa tulo $2m$ on luvun 2 monikerta, joten myös jokainen alkio, joka kuuluu $(2, 1+\sqrt{-5})(2, 1+\sqrt{-5}) = 4 + 6 = 10$, mikä on luvun 2 monikerta. Tämä osoittaa, että

$$(2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5}) \subset (2).$$

b) $(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$

Käytetään jälleen määritelmää 90:

$$\begin{aligned} 9 = 3 \cdot 3 &\in (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}), \\ 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) &\in (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}). \end{aligned}$$

Ja kun tiedetään, että

$$9, 6 \in (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}),$$

niin siitä seuraa

$$3 \in (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

Koska renkaalle $\mathbb{Z}[\sqrt{-5}]$ on määritelty kertolasku saadaan, että kaikki luvun 3 monikerrat sisältyvät myös joukkoon $(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$. Tästä seuraa, että

$$(3) \subset (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

Osoitetaan, vielä toinen suunta:
Jokainen alkio, joka kuuluu joukkoon $(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$ on termien $3m$ ja $(1 \pm \sqrt{-5})n$ summa. Mikä tahansa tulo $3m$ on luvun 3 monikerta, joten jokainen sen alkio kuuluu myös joukkoon $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$. Tästä seuraa, että jokainen

alkio, joka kuuluu $(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$ on luvun 3 monikerta, ja tällöin ollaan osoitettu, että $(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) \subset (3)$.

Esimerkin nojalla luvun 6 tekijöihinjako voidaan esittää muiden tapojen lisäksi myös ideaalien avulla. Saadaan alkuideaalihajotelma

$$(6) = (2)(3) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}).$$

Toisaalta myös

$$(6) = (1+\sqrt{-5})(1-\sqrt{-5}),$$

koska voitaisiin osoittaa esimerkin tavoin myös, että

$$(1+\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})$$

$$(1-\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1-\sqrt{-5}).$$

Huomataan, että kaksi luvun 6 erilaista tekijöihinjakoa voidaan itseasiassa muodostaa samoista alkuideaaleista. Seuraavaksi lähdetään osoittamaan, että alkuideaalihajotelma todella on yksikäsitteinen.

5.5. **Alkuideaalihajotelman yksikäsitteisyys.** Kuten aiemmista esimerkeistä huomattiin, luvulle 6 löydetään kaksi alkutekijähajotelmaa, joilla on kuitenkin sama alkuideaalihajotelma renkaassa $\mathbb{Z}[\sqrt{-5}]$. Tämä ei vielä todista yksikäsitteisyyttä, mutta antaa vihjettä siihen suuntaan, että sellainen saatettaisiin löytää. Tullaan osoittamaan, että yksikäsitteinen alkuideaalihajotelma todella löytyy. Määritellään kuitenkin sitä ennen kongruenssit ideaaleilla.

5.5.1. ***Kongruenssi ideaaleilla.***

Määritelmä 94. Olkoon I renkaan R ideaali ja $a, b \in R$. Tällöin

$$a \equiv b \pmod{I} \Leftrightarrow a - b \in I.$$

Lause 95. *Olkoon $I \subset R$ renkaan R ideaali. Tällöin*

(1) $a \equiv a \pmod{I}$
(2) *Jos* $a \equiv b \pmod{I}$, *niinb* $\equiv a \pmod{I}$
(3) *Jos* $a \equiv b \pmod{I}$ *ja* $b \equiv c \pmod{I}$, *niina* $\equiv c \pmod{I}$

Todistus.

(1) $a - a = 0_R \in I$, mikä todistaa ensimmäisen väitteen.
(2) Jos $a-b \in I$, niin $b-a = -(a-b) = 0_R-(a-b)$. Koska $0_R \in I$ ja $(a-b) \in I$, niin ideaalin määritelmän nojalla väite todistettu.
(3) Jos $a-b \in I$ ja $b-c \in I$, niin $(a-c) = (a-b)-(b-c) \in I$, joten väite pätee.

□

Määritelmä 96. Olkoon I renkaan R ideaali. Joukkoa

$$I + a = \{i + a : i \in I\} = \{a + i : i \in I\} = a + I$$

sanotaan alkion a määräämäksi sivuluokaksi. Kaikkien sivuluokkien muodostamaa joukkoa merkitään R/I. Sivuluokkien joukko R/I on myös kongruenssiluokkien joukko $\pmod{I}$.

Määritelmä 97. Vaihdannainen rengas on **kunta**, jos se sisältää kaikkien alkioidensa $a \neq 0$ käänteisalkiot.

Lause 98. *Renkaan R ideaali I on* alkuideaali*, jos ja vain jos joukossa R/I ei ole nollanjakajaa. Nollanjakajat ovat (nollasta poikkeavia) kongruenssiluokkia $I + a$ ja $I + b$, joiden tulo $I + ab$ on ideaali I, jonka luokka on 0.*

Todistus.
"⇒": Oletetaan, että I on alkuideaali ja halutaan osoittaa, että sivuluokkien joukolla R/I ei ole nollanjakajia. Olkoon $I + ab = (0)$. Tällöin $ab \in I$, josta seuraa, että myös $I + a = (0)$ ja $I + b = (0)$. Tämä osoittaa, että joukolla R/I ei ole nollanjakajia.
"⇐": Oletetaan, että joukolla R/I ei ole nollanjakajia, ja halutaan osoittaa, että I on alkuideaali. Olkoon $ab \in I$, josta seuraa $I + ab = I$. Kongruenssiluokkien määritelmästä saadaan $(I + a)(I + b) = I$ ja oletuksesta, että joukolla R/I:llä ei ole nollanjakajia seuraa $I + a = I$ tai $I + b = I$. Siis $a \in I$ tai $b \in I$, mikä osoittaa, että I on alkuideaali. □

5.5.2. ***Alkuideaalihajotelman yksikäsitteisyyden todistaminen.*** Tässä luvussa esitetään loputkin tulokset, joiden avulla osoitetaan, että algebrallisten kokonaislukujen muodostamalle renkaalle $\mathbb{Z}[\sqrt{-5}]$ voidaan määrittää alkuideaalihajotelma yksikäsitteisesti.

Lemma 99. *Olkoon R vaihdannainen rengas $(1 \neq 0)$. Tällöin R on kunta jos ja vain jos sillä ei ole yhtään epätriviaalia ideaalia.*

Todistus.
"⇒": Oletetaan, että R on kunta. Olkoon I mikä tahansa renkaan R ideaali. Joko $I = (0)$ tai on olemassa alkio $a \in I$ siten, että $a \neq 0$. Tarkastellaan jälkimmäistä tapausta. Sillä R on kunta on olemassa käänteisalkio a^{-1} ja siten millä tahansa $r \in R$ pätee $r = r \cdot 1 = r(a^{-1})a = (ra^{-1}a)$. Ideaalien määritelmästä saadaan, että $r \in I$. Tämä osoittaa, että $I = (0)$ tai $I = R$.
"⇐": Oletetaan, että vaihdannaisella renkaalla R ei ole yhtään aitoa ideaalia. Olkoon $a \in R$ neutraalialkio. Halutaan osoittaa, että

$$I = \{x \in R : x = ra, \quad \text{jollain } r \in R\}.$$

Ideaali I on epätyhjä joukko, sillä $a = a \cdot 1 \in I$. Olkoot $ar_1, ar_2 \in I$. Tällöin $ar_1 \pm ar_2 = a(r_1 + r_2) \in I$. Vielä täytyy osoittaa, että jos $x = ar \in I$ ja $s \in R$, niin $a(sr) \in I$. Lasketaan $xs = ars = a(rs)$. Tämä osoittaa, että yllä mainittu joukko on ideaali. Tällöin täytyy olla $I = R$, siten $I \neq (0)$ ja $1 \in R$. Saadaan $1 = ra$, jollain $r \in R$. Tämä osoittaa, että r on kääntyvä ja siten R on kunta. □

Lemma 100. *Olkoon I vaihdannaisen renkaan R ideaali. Jokaisella ideaalilla $J \subset R/I$ määrittää ideaali $\pi^{-1}(J)$ renkaassa R ja jokaiselle ideaalille $J \subset R$, joka sisältää ideaalin I, voidaan määrittää ideaali $\pi(J)$ renkaassa R.*

Todistus. Olkoon $I \subset J$, tällöin

$$\pi(J) = \{a + I : a \in J\}.$$

Kaikilla alkioilla $r + I \in R/I$ ja $a + I \in \pi J$, saadaan $(r + I)(a + I) = ra + I \in \pi(J)$, kun $ra \in J$. Toisaalta jos $I \subset R/I$, niin

$$\pi^{-1}(J) = \{a \in R : a + I \in J\}.$$

Jos $r \in R$ ja $a \in \pi^{-1}(J)$, niin $ra \in \pi^{-1}(J)$, ja siten $ra + I = (r + I)(a + I) \in J$. □

Lause 101. *Olkoon I vaihdannaisen renkaan R aito ideaali.*

(a) *I on maksimaalinen ideaali, jos ja vain jos tekijärengas R/I on kunta.*
(b) *I on renkaan R alkuideaali, jos ja vain jos tekijärengas R/I on kokonaisalue.*

Todistus.

(a) Oletuksesta seuraa, etttä R on aito ideaali. Tällöin $(1) \not\subset I$ ja siten $1+I \neq 0+I$. Hyödyntämällä yläpuolella todistettuja lemmoja 99 ja 100 saadaan, että väite pätee ainoastaan silloin kuin ideaalien R ja I välillä ei ole aitoja ideaaleja. Voidaan todeta, että I on maksimaalinen ideaali.
(b) "⇐" Oletetaan että R/I on kokonaisalue ja olkoot $a, b \in R$ siten, että $ab \in I$. Tällöin kokonaisalueessa R/I on määritelty sivuluokkien kertolasku $(a+I)(b+I)$. Kaikkiin sivuluokkiin kuuluu neutraalialkio, joten on olemassa alkiot a, b siten, että $(a+I)(b+I) = (0)$. Tästä seuraa, että jommankumman sivuluokista $(a+I)$ tai $(b+I)$ täytyy olla nolla. Tällöin joko $a \in I$ tai $b \in I$, josta saadaan, että ideaalin I täytyy olla alkuideaali.
"⇒" Oletetaan, että I on alkuideaali. Jos $a, b \in R$ siten, että $(a + I)(b + I) = 0 + I \in R/I$, niin seuraa $ab \in I$ ja edelleen $a \in I$ tai $b \in I$. Tällöin joko $a + I = 0 + I$ tai $b + I = 0 + I$, mikä osoittaa, että R/I on kokonaisalue.

□

Jokainen kunta on siis kokonaisalue, mutta välttämättä jokainen kokonaisalue ei ole kunta. Esitellään vielä ennen alkuideaalihajotelman yksikäsitteisyyden todistamista tärkeä tulos kvadraattisille kokonaisluvuille. Kvadraattisilla kokonaisluvuilla tarkoitetaan muotoa

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$$

olevia lukuja, joissa d on neliövapaa. Luvun d sanotaan olevan neliöavapaa, jos ehdosta $a^2 \mid d, a \in \mathbb{Z}$ seuraa, että $a^2 = 1$. Joukolle $\mathbb{Q}[\sqrt{d}]$ on voimassa laskutoimitukset $+, -, \cdot, \div$.

Joukon $\mathbb{Q}[d]$ luvut eivät välttämättä ole kvadraattisia kokonaislukuja. Joukko $\mathbb{Q}[d]$ on eräs kvadraattisten lukujen muodostama kunta (katso määritelmä 21: algebralliset kokonaisluvut). Renkaan $\mathbb{Q}[d]$ kvadraattiset kokonaisluvut ovat kyseessä olevan renkaan algebralliset kokonaisluvut.

Lause 102. *Jos $d \not\equiv 1 \pmod 4$, niin joukon $\mathbb{Q}[\sqrt{d}]$ kokonaislukuja ovat $a+b\sqrt{d}, a, b \in \mathbb{Z}$. Jos $d \equiv 1 \pmod 4$, niin joukon $\mathbb{Q}[\sqrt{d}]$ kokonaislukuja ovat $a + b\sqrt{d}, a, b \in \mathbb{Z}$ tai $a + \frac{1}{2}, b + \frac{1}{2} \in \mathbb{Z}$.*

Todistus. Jos $a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ on algebrallinen kokonaisluku, silloin se toteuttaa yhtälön $x^2 + Ax + B = 0, A, B \in \mathbb{Z}$. Tästä seuraa, että on olemassa yhtälö, jonka toinen ratkaisu on $a - b\sqrt{d}$. Siten

$$x^2 + Ax + B = (x - (a + b\sqrt{d}))(x - (a - b\sqrt{d})) = x^2 - 2ax + (a^2 - db^2).$$

Saadaan

$$A = -2a \quad \text{ja} \quad B = a^2 - db^2,$$

mikä osoittaa niiden olevan kokonaislukuja.

Tarkastellaan erikseen tilanteet, joissa $2a$ on parillinen tai pariton.

Olkoot $2a$ parillinen ja $b = \frac{k}{m} \in \mathbb{Q}$. Nyt $\text{syt}(k, m) = 1$ ja myös $\text{syt}(k^2, m^2) = 1$. Tiedosta $a^2 - db^2 \in \mathbb{Z}$ saadaan, että myös $db \in \mathbb{Z}$. Voidaan tehdä päättely:

$$db^2 = l \in \mathbb{Z} \Rightarrow d\Big(\frac{k}{m}\Big)^2 = l \Rightarrow dk^2 = lm^2 \Rightarrow m^2 \mid dk^2 \Rightarrow m^2 \mid d.$$

Sillä $\text{syt}(k^2, m^2) = 1$, täytyy olla $m^2 = 1 \Rightarrow m = \pm 1$. Tämä osoittaa, että $b \in \mathbb{Z}$.

Olkoon nyt $a + \frac{1}{2} \in \mathbb{Z}$, kun $2a$ on pariton. Tällöin $(2a)^2 \equiv 1 \pmod 4$ ja siten $a^2 - ab^2 \in \mathbb{Z}$. Voidaan päätellä

$$(2a)^2 - d(2b)^2 \equiv 0 \pmod 4 \Rightarrow d(2a)^2 \equiv (2a)^2 \equiv 1 \pmod 4.$$

Sillä $(2b)^2 \equiv 3 \pmod 4$ on mahdotonta, saadaan

$$d \equiv 1 \pmod 4 \quad \text{ja} \quad (2b)^2 \equiv 1 \pmod 4.$$

Tästä seuraa, että $d \equiv 1 \pmod 4$ ja $2b \equiv 1 \pmod 2$. Täten siis $b + \frac{1}{2} \in \mathbb{Z}$. □

Lause 103. *Jos R on kokonaislukurengas imaginäärisessä kvadraattisessa kunnassa ja $A \subset R$ on ideaali, niin*

$$A\bar{A} = (k), \ \textit{jollain } k \in \mathbb{Z}.$$

Todistus. Olkoon $A = \{\alpha m + \beta n : m, n \in \mathbb{Z}\}$, kun $\alpha, \beta \in R$. Tällöin $\overline{A} = \{\bar{\alpha} m + \bar{\beta} n : m, n \in \mathbb{Z}\}$ ja määritelmästä 90 seuraa

$$A\bar{A} = \{s\alpha\bar{\alpha} + t\beta\bar{\beta} + u\bar{\alpha}\beta\alpha\bar{\beta} : s, t, u \in \mathbb{Z}\}.$$

Nyt $\alpha\bar{\alpha}, \beta\bar{\beta}$ ja $\bar{\alpha}\beta + \alpha\bar{\beta}$ ovat renkaan R kokonaislukuja ja siten

$$\alpha\bar{\alpha}, \beta\bar{\beta}, \bar{\alpha}\beta + \alpha\bar{\beta} \in \mathbb{Z}.$$

Tämän tiedon pohjalta voidaan tehdä seuraava päättely:

$$\text{syt}\left(|\alpha|^2, \beta\bar{\beta}, \bar{\alpha}\beta + \alpha\bar{\beta}\right) = k, \quad k \in \mathbb{Z}.$$

Eukleideen algoritmista saadaan:

$$k = p\alpha\bar{\alpha} + q\beta\bar{\beta} + r(\bar{\alpha}\beta + \alpha\bar{\beta}), \quad p, q, r \in \mathbb{Z}.$$

Nyt

$$k \in A\bar{A} \Rightarrow (k) \subset A\bar{A}.$$

Osoitetaan vielä toinen suunta. Halutaan näyttää, että $A\bar{A} \subset (k)$. Riittää näyttää, että luku k jakaa luvut $\alpha\bar{\alpha}, \beta\bar{\beta}, \bar{\alpha}\beta, \alpha\bar{\beta}$. Se jakaa selvästi luvut $\alpha\bar{\alpha}$ ja $\beta\bar{\beta}$. Tarkastellaan yhtälöä, jonka juuria luvut $\frac{\alpha\bar{\beta}}{k}$ ja $\frac{\bar{\alpha}\beta}{k}$ ovat. Saadaan

$$\Big(x - \frac{\alpha\bar{\beta}}{k}\Big)\Big(x - \frac{\bar{\alpha}\beta}{k}\Big) = x^2 - \frac{\alpha\bar{\beta} + \bar{\alpha}\beta}{k}x + \frac{\alpha\bar{\alpha}}{k} \cdot \frac{\beta\bar{\beta}}{k} = 0.$$

Yhtälön kertoimien tiedetään olevan kokonaislukuja, joten siten luvut $\frac{\alpha\bar{\beta}}{k}$ ja $\frac{\bar{\alpha}\beta}{k}$ ovat kvadraattisia kokonaislukuja ja renkaan R alkioita.

□

Lause 104. *Olkoon R kokonaislukurengas imaginäärisessä kvadraattisessa kunnassa. Jos A, B, C ovat (nollasta poikkeavia) renkaan R ideaaleja ja $AC \subset AB$, niin $C \subset B$.*

Todistus. Todistetaan lause hyödyntäen lemmaa 103. Oletetaan, että $AC \subset AB$. Kertomalla puolittain konjugaatilla $\bar{A}$ ja käyttämällä lemmaa 103 saadaan

$$(k)C \subset (k)B, \quad k \in \mathbb{Z}.$$

Ja koska tiedetään, että ideaaleille B ja C on voimassa kertolasku, seuraa $(k)B = kB$. Ideaalille C vastaavasti. Kertomalla yhtälö puolittain luvulla k^{-1} saadaan

$$(k)C \subset (k)B \Rightarrow kC \subset kB \Rightarrow C \subset B.$$

□

Lause 105. *Jos A ja B ovat renkaan R ideaaleja ja $A \subset B$, niin $B \mid A$ ja*

$$A = BC \text{ , kun } C \text{ jokin ideaali.}$$

Todistus. Tutkitaan ensin erityistilanne, missä $B = (\beta)$ on pääideaali. Nyt

$$\begin{aligned} A \subset B &\Rightarrow A \subset (\beta) \\ &\Rightarrow \beta \text{ jakaa kunkin A:n jäsenen} \\ &\Rightarrow A = (\beta)\{\alpha/\beta : \alpha \in A\} \\ &\Rightarrow A = BC. \end{aligned}$$

B on ideaali (β) ja myös $C = \{\alpha/\beta : a \in A\}$ on renkaan R ideaali. Jaollisuuden nojalla luku $\frac{\alpha}{\beta}$ on renkaan R alkio. Sillä renkaalle R on voimassa yhteen- ja kertolasku ja jokainen α on jaollinen luvulla β, joten väite on todistettu erityistilanteessa. Lähdetään tutkimaan vielä yleinen tilanne, kun $B = (\beta)$ ei ole pääideaali.

$$\begin{aligned} A \subset B &\Rightarrow A\bar{B} \subset B\bar{B} \\ &\Rightarrow A\bar{B} \subset (k) \\ &\Rightarrow A\bar{B} = (k)C \\ &\Rightarrow A\bar{B} = \bar{B}BC \\ &\Rightarrow A = BC. \end{aligned}$$

Päättely on seurausta lauseista 103 ja 104. □

Lause 106. *Olkoon R kokonaislukurengas imaginäärisessä kvadraattisessa kunnassa. Jokainen nollasta poikkeava ideaali $A \neq R$ voidaan esittää alkuideaalien tulona.*

Todistus. Olkoon A ideaali renkaassa R. Jos A ei ole alkuideaali, se ei ole myöskään maksimaalinen ideaali lauseen 84 nojalla. Siten on olemassa ideaali $A \subset B$, kun $B \neq R$. Tällöin lauseesta 105 seuraa

$$A = BC, \quad \text{jollain ideaalilla } C \subset R.$$

Olkoon nyt B ideaali renkaassa R. Tehdään vastaava päättely kuin ideaalille A. Saadaan

$$B = DE, \quad \text{joillain ideaaleilla } D, E \subset R.$$

Vastaavaa prosessia voitaisiin jatkaa, ja lopulta (äärellisen määrän jälkeen askelia) saataisiin selville alkutekijähajotelma. Jokainen laajennus pitää sisällään vähintään yhden aiemmista luokista. Nollasta poikkeavalla ideaalilla I on äärellinen määrä

kongruenssiluokkia $A + r$ ja tiedetään, että jokainen maksimaalinen ideaali on myös alkuideaali, mikä todistaa väitteen.

□

Aivan kuten aritmetiikan peruslauseessakin, yksikäsitteisyys seuraa alkutekijähajotelman olemassaolosta. Nyt käytössä on vain alkuideaalit alkulukujen sijasta. Yllä osoitettiin, että ideaalit voidaan esittää alkuideaalien tulona, joten jäljellä on enää todistaa, että alkuideaalihajotelma on yksikäsitteinen.

Lause 107. *Alkuideaalihajotelma, jossa ideaalit ovat nollasta poikkeavia, on tekijöiden järjestystä vaille yksikäsitteinen.*

Todistus. Yllä osoitetun lauseen nojalla jokainen ideaali voidaan esittää alkuideaalien tulona. Oletetaan, että

$$P_1 P_2 \cdots P_r = Q_1 Q_2 \cdots Q_s.$$

Tästä seuraa, että $Q_i \subset P_1$, jollain i. Järjestelemällä saadaan, että $Q_i \subset P_i$. Tällöin täytyy olla $P_1 = Q_1$, sillä jokainen alkuideaali on maksimaalinen. Jatketaan

$$P_2 \cdots P_r = Q_2 \cdots Q_s.$$

Tästä saadaan $Q_i \subset P_2$, ja järjestelemällä päädytään jälleen $P_2 = Q_2$. Jatkamalla prosessia saadaan, että $r = s$ ja $P_i = Q_i$ kaikilla i. Tämä osoittaa yksikäsitteisyyden.

□

Nyt ollaan osoitettu, että rengas $\mathbb{Z}[\sqrt{-5}]$ ei ole pääideaalialue ja tällöin sille ei voida löytää määritelmän mukaista alkutekijähajotelmaa, kuten esimerkiksi renkaille $\mathbb{Z}[\sqrt{-2}]$ ja $\mathbb{Z}[\zeta_3]$ löydettiin. Tutkimalla renkaan $\mathbb{Z}[\sqrt{-5}]$ ideaaleja huomataan, että renkaalle löydetään hajotelma ideaalien avulla, mutta kuitenkaan löydetyn hajotelman ideaalit eivät ole pääideaaleja. Osoittamalla ideaalit alkuideaaleiksi voidaan todeta renkaalle $\mathbb{Z}[\sqrt{-5}]$ löytyvän tekijöihinjako alkuideaalien avulla. Lause 107 viimeistelee todistuksen ja osoittaa, että algebrallisten kokonaislukujen muodostamalle renkaalle $\mathbb{Z}[\sqrt{-5}]$ löydetty alkuideaalihajotelma on yksikäsitteinen.

Mielenkiintoinen jatkotutkimuskohde voisi olla renkaan $\mathbb{Z}[\sqrt{-5}]$ ideaaliluokkien selvittäminen, sillä nyt ollaan päästy jo hyvään vaiheeseen renkaan $\mathbb{Z}[\sqrt{-5}]$ ja sen yksikäsitteisen alkuideaalihajotelman tarkastelussa. Ideaaliluokkien selvittämiseen tarvittaisiin kuitenkin enemmän tietoa renkaan $\mathbb{Z}[\sqrt{-5}]$ ideaaleista. Aiheesta löytyy lisää lähteestä [1, s. 231-233]. Renkaan $\mathbb{Z}[\sqrt{-5}]$ ideaaliluokkien tarkastelu mahdollistaa myös muotoa x^2+5y^2 olevien alkutekijöiden tarkastelun, mikä sai aikoinaan Fermatin ja Eulerin ymmälleen. Myös tästä löytyy lisää samaisesta lähteestä [1, s. 233-235].

Lähdeluettelo

[1] Stillwell, John. *Elements of Number Theory.* Undergraduate Texts in Mathematics. Springer, New York, 2003.

[2] Stillwell, John. *Mathematics and its History.* Third edition. Undergraduate Texts in Mathematics. Springer, New York, 2010.

[3] Hardy, Godfrey H. Wright, Edward M. *an Introduction to theory of numbers* Sixth edition. Principal and Vice-Chancellor Emeritus of the University of Aberdeen. Oxford University Press, Iso-Britannia, 2008.

[4] Rosen, Kenneth H. *Elementary number theory and its applications.* Fourth edition. AT&T Informotion Systems Laboratories (formerly part of Bell Laborotories). Addison Wesley Longman, Yhdysvallat, 2000.

[5] Stillwell, John. *Numbers and Geometry.* Undergraduate Texts in Mathematics. Reading in Mathematics. Springer, New York, 1998.

[6] Beachy, John A. Blair, William D. *Abstract Algebra.* Third edition. Northern Illinois University, Yhdysvallat, 2006.

[7] Koskela, Pekka. (Kai Rajalan luentojen pohjalta). *Algebra 1: Renkaat ja kunnat.* Luentomoniste. Jyväskylän yliopiston matematiikan laitos, Jyväskylä, 2017.

[8] Gathern, Joachim. Gerhard, Jürgen. *Modern Computer Algebra.* Second edition. Cambridge University Press, Cambridge, 2003.