TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Jenni Ranta

Polynomirenkaista ja euklidisista alueista

Matematiikan, tilastotieteen ja filosofian laitos
Matematiikka
Elokuu 2005

Tampereen yliopisto

Matematiikan, tilastotieteen ja filosofian laitos

RANTA, JENNI: Polynomirenkaista ja euklidisista alueista

Pro gradu -tutkielma, 42 s.

Matematiikka

Elokuu 2005

TIIVISTELMÄ

Tutkielman pääaiheina ovat polynomirenkaat ja euklidiset alueet. Tutkielma on jaettu kolmeen lukuun.

Ensimmäinen luku sisältää esitietoja, joita tarvitaan toisessa ja kolmannessa luvussa. Ensimmäisessä luvussa käsitellään tutkielman pääaiheiden käsittelyssä tarvittavia käsitteitä ja lauseita. Lisäksi ensimmäisessä luvussa käydään lyhyesti läpi muutama tutkielmassa usein esiintyvä merkintätapa.

Toinen luku keskittyy polynomirenkaiden käsittelyyn. Toisessa luvussa määritellään aluksi polynomin ja polynomirenkaan käsitteet. Lisäksi käydään läpi polynomeihin ja polynomirenkaisiin liittyvien käsitteiden määritelmiä ja merkintätapoja. Luvussa käsitellään myös polynomien jaollisuutta ja esitetään useita polynomirenkaita koskevia lauseita, joista mainittakoon lauseet jakoalgoritmi ja jäännöslause.

Kolmannessa luvussa käsitellään euklidisia alueita. Ensimmäiseksi luvussa käydään läpi euklidisen alueen määritelmä. Gaussin kokonaislukujen joukko määritellään luvussa kolme ja Gaussin kokonaislukuja käsitellään myös laajemmin. Luvussa esimerkiksi todistetaan, että Gaussin kokonaislukujen rengas on euklidinen alue. Kolmannessa luvussa käsitellään myös euklidisen alueen ihanteita, kommutatiivisen renkaan alkioiden jaollisuutta ja käydään läpi liittoalkion määritelmä sekä esitetään liittoalkioiden ominaisuuksia koskevat kaksi lausetta. Suurimman yhteisen tekijän käsitettä laajennetaan kolmannen luvun viidennessä alaluvussa määrittelemällä käsite kommutatiivisessa renkaassa. Alaluvussa todistetaan kahden alkion suurimman yhteisen tekijän olemassaoloa koskeva lause ja lause, jonka perusteella alkioiden kaksi suurinta yhteistä tekijää ovat toistensa liittoalkioita. Kolmannen luvun kuudennessa eli viimeisessä alaluvussa käydään läpi tärkeä Eukleideen algoritmi. Kyseistä algoritmia käytetään euklidisen alueen kahden alkion suurimman yhteisen tekijän löytämiseen ja siinä sovelletaan tärkeää jakoalgoritmia.

Tutkielman jokainen luku sisältää useita esimerkkejä. Tutkielman tärkein lähdeteos on Malikin, Mordesonin ja Senin kirja Fundamentals of Abstract Algebra.

Asiasanat: algebra, polynomirengas, euklidinen alue.

Sisältö

Johdanto

Tämän tutkielman pääaiheina ovat polynomirenkaat ja euklidiset alueet. Pääaiheita käsitellään luvuissa 2 ja 3. Luku 1 sisältää nimensä mukaisesti esitietoja.

Luvun 1 alaluvuissa 1.2 ja 1.3 käydään läpi pääaiheiden käsittelyssä tarvittavien käsitteiden määritelmiä ja esitetään muutamia hyödyllisiä lauseita. Lisäksi luvun 1 alaluvussa 1.1 käydään lyhyesti läpi muutama tutkielmassa usein esiintyvä merkintätapa.

Luvussa 2 käsitellään polynomirenkaita. Alaluvussa 2.1 määritellään polynomin ja polynomirenkaan käsitteet. Lisäksi käydään läpi polynomeihin ja polynomirenkaisiin liittyvien käsitteiden määritelmiä ja merkintätapoja. Alaluvussa 2.2 esitetään neljä polynomirenkaita koskevaa lausetta. Alaluvussa 2.3 käsitellään polynomien jaollisuutta lauseiden ja määritelmien avulla. Alaluvun tärkeimpinä lauseina voidaan pitää jakoalgoritmia ja jäännöslausetta.

Luvussa 3 käsitellään euklidisia alueita. Euklidisen alueen määritelmä käydään läpi alaluvussa 3.1. Gaussin kokonaislukujen joukko määritellään alaluvussa 3.2 ja alaluvussa todistetaan, että Gaussin kokonaislukujen rengas on euklidinen alue. Alaluvussa 3.3 käsitellään euklidisen alueen ihanteita. Alaluvussa 3.4 käsitellään hieman kommutatiivisen renkaan alkioiden jaollisuutta, käydään läpi liittoalkion määritelmä ja esitetään liittoalkioiden ominaisuuksia koskevat kaksi lausetta. Suurimman yhteisen tekijän käsitettä laajennetaan alaluvussa 3.5 määrittelemällä käsite kommutatiivisessa renkaassa. Alaluvussa todistetaan kahden alkion suurimman yhteisen tekijän olemassaoloa koskeva lause ja lause, jonka perusteella alkioiden kaksi suurinta yhteistä tekijää ovat toistensa liittoalkioita. Luvun 3 viimeisessä alaluvussa eli alaluvussa 3.6 käydään läpi tärkeä Eukleideen algoritmi. Kyseistä algoritmia käytetään euklidisen alueen kahden alkion suurimman yhteisen tekijän löytämiseen ja siinä sovelletaan tärkeää jakoalgoritmia.

Luvun 1 lauseet jätetään pääosin todistamatta, mutta lukujen 2 ja 3 kaikki lauseet ja seurauslauseet todistetaan. Lauseen 3.6 todistus on tekijän itse tekemä, mutta lause löytyy lähdekirjan [5] sivulta 353. Tutkielman jokainen luku sisältää useita esimerkkejä. Osa esimerkeistä on lähdekirjojen esimerkkejä ja osa esimerkeistä on lähdekirjojen harjoitustehtäviä, jotka tekijä on itse ratkaissut. Tutkielmassa on myös muutama esimerkki, jotka tekijä on kokonaan itse tehnyt. Esimerkkien tarkoituksena on havainnollistaa aihepiiriä ja helpottaa asioiden ymmärtämistä.

Lukijalta edellytetään algebran peruskurssin asioiden hallintaa (esimerkiksi lähdekirjan [3] sivut 1-63). Esimerkiksi renkaan määritelmä oletetaan tunnetuksi. Tutkielma on teoreettinen ja sen tärkein lähdeteos on Malikin, Mordesonin ja Senin kirja Fundamentals of Abstract Algebra [5]. Tutkielman rakenne on samankaltainen kuin lähdekirjan [5] ja tutkielmassa käytetään pääosin kyseisen lähdekirjan merkintätapoja.

1 Esitietoja

Tässä luvussa käydään luettelonomaisesti läpi tutkielmassa käytettävien käsitteiden määritelmiä ja niihin liittyviä lauseita. Lauseet jätetään pääosin todistamatta, mutta niihin annetaan kirjallisuusviittaukset. Lisäksi käydään läpi muutama esimerkki ja selitetään käytetyt merkintätavat.

1.1 Käytetyistä merkintätavoista

Tässä alaluvussa käydään lyhyesti läpi tutkielmassa usein esiintyvät merkinnät, joiden käyttötavasta ei muualla tekstissä mainita.

Olkoon $m \in \mathbb{Z}^+$. Kaikkien jäännösluokkien joukkoa (mod m) merkitään symbolilla $\mathbb{Z}_m$ ja siis $\mathbb{Z}_m = \{\,\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\,\}$ (vrt. [3, s. 40]).

Esimerkki 1.1. Joukon $\mathbb{Z}_5$ alkiot ovat $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ ja $\overline{4}$ eli $\mathbb{Z}_5 = \{\,\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\,\}$.

Tässä tutkielmassa käytetään usein kahden laskutoimituksen struktuurien eli esimerkiksi renkaiden, kokonaisalueiden ja kuntien merkitsemiseen lyhyesti vain joukon kirjainta, merkitsemättä näkyviin kahta laskutoimitusta.

Esimerkki 1.2. Rengasta $(R, +, \cdot)$ merkitään lyhyesti vain renkaana R.

Huomautus. Merkinnät $(R, +, \cdot)$ ja R kuvaavat siis tutkielmassa samaa kahden laskutoimituksen struktuuria.

1.2 Tarvittavien käsitteiden määritelmiä ja tarvittavia lauseita

Tässä alaluvussa käydään läpi tarvittavien käsitteiden määritelmiä (vrt. [1, s. 168], [3, s. 58], [5, s. 273] ja [6, s. 200 ja 203]). Lisäksi esitetään muutamia jatkossa tarvittavia lauseita ja käydään läpi muutama niihin liittyvä esimerkki.

Määritelmä 1.1. Kolmikko $(S, +, \cdot)$ on renkaan $(R, +, \cdot)$ *alirengas* (engl. subring), jos joukko S on joukon R ei-tyhjä osajoukko ja $(S, +, \cdot)$ on itsessään rengas.

Huomautus. Määritelmässä 1.1 alirenkaan $(S, +, \cdot)$ laskutoimitukset $+$ ja $\cdot$ ovat samat kuin renkaan $(R, +, \cdot)$ laskutoimitukset (vrt. [6, s. 196]).

Lause 1.1. (Alirengaskriteeri) *Olkoon R rengas ja S joukon R ei-tyhjä osajoukko. Silloin $(S, +, \cdot)$ on renkaan R alirengas, jos ja vain jos*

(i) $a - b \in S$,

(ii) $ab \in S$

aina, kun $a, b \in S$.

Todistus. Ks. [5, s. 289–290] ja [6, s. 196].

Käydään seuraavaksi läpi esimerkki, joka havainnollistaa lauseen 1.1 eli alirengaskriteerin käyttömahdollisuutta.

Esimerkki 1.3. ([6, s. 196–197, Esim. 6.1.16]) Joukko $\mathbb{Q}(\sqrt{2}) = \{\, a + b\sqrt{2} \mid a, b \in \mathbb{Q} \,\}$ muodostaa renkaan varustettuna tavallisella yhteen- ja kertolaskulla. Käytetään rengasta $\mathbb{R}$ ja alirengaskriteeriä tämän todistamiseen. Alirengaskriteeriä voidaan käyttää, koska selvästi $\mathbb{R}$ on rengas ja $\emptyset \neq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. Valitaan sitten mielivaltaisesti sellaiset alkiot $x, y \in \mathbb{Q}(\sqrt{2})$, että $x = a + b\sqrt{2}$ ja $y = c + d\sqrt{2}$, missä $a, b, c, d \in \mathbb{Q}$. Silloin

$$x - y = (a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2}$$

ja

$$xy = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

Koska $a - c, b - d, ac + 2bd, ad + bc \in \mathbb{Q}$, niin $x - y \in \mathbb{Q}(\sqrt{2})$ ja $xy \in \mathbb{Q}(\sqrt{2})$. Näin ollen alirengaskriteerin perusteella kolmikko $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ on renkaan $\mathbb{R}$ alirengas, jolloin määritelmän 1.1 mukaan $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ on itsessään rengas. Näin on saatu haluttu tulos todistettua alirengaskriteerin avulla.

Määritelmä 1.2. Kolmikko $(S, +, \cdot)$ on kokonaisalueen $(D, +, \cdot)$ *alialue* (engl. subdomain), jos joukko S on joukon D ei-tyhjä osajoukko ja $(S, +, \cdot)$ on itsessään kokonaisalue.

Huomautus. Määritelmässä 1.2 alialueen $(S, +, \cdot)$ laskutoimitukset $+$ ja $\cdot$ ovat samat kuin kokonaisalueen $(D, +, \cdot)$ laskutoimitukset (vrt. [6, s. 200]).

Lause 1.2. (Alialuekriteeri) (vrt. [6, s. 201]) *Olkoon D kokonaisalue ja S joukon D ei-tyhjä osajoukko. Silloin kolmikko $(S, +, \cdot)$ on kokonaisalueen D alialue, jos ja vain jos*

(i) *kolmikko $(S, +, \cdot)$ on renkaan D alirengas,*

(ii) $1 \in S$,

missä alkio 1 *on kokonaisalueen D ykkösalkio.*

Todistus. Lauseen 1.2 todistus seuraa määritelmistä 1.1 ja 1.2 sekä lauseesta 1.1 ja kokonaisalueen määritelmästä.

Käydään seuraavaksi läpi lauseen 1.2 eli alialuekriteerin käyttömahdollisuutta havainnollistava esimerkki.

Esimerkki 1.4. ([6, s. 201, Esim. 6.2.13]) Joukko $\mathbb{Q}(\sqrt{2}) = \{\, a + b\sqrt{2} \mid a, b \in \mathbb{Q} \,\}$ muodostaa kokonaisalueen varustettuna tavallisella yhteen- ja kertolaskulla. Käytetään kokonaisaluetta $\mathbb{R}$ ja alirengaskriteeriä tämän todistamiseen. Selvästi $\mathbb{R}$ on kokonaisalue ja joukko $\mathbb{Q}(\sqrt{2})$ on joukon $\mathbb{R}$ ei-tyhjä osajoukko, joten alialuekriteeriä voidaan käyttää. Esimerkin 1.3 mukaan kolmikko $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ on renkaan $\mathbb{R}$ alirengas ja joukon $\mathbb{Q}(\sqrt{2})$ alkioiden määrittelyn perusteella selvästi alkio $1 \in \mathbb{Q}(\sqrt{2})$. Näin ollen alialuekriteerin perusteella kolmikko $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ on kokonaisalueen $\mathbb{R}$ alialue, jolloin määritelmän 1.2 mukaan $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ on itsessään kokonaisalue. Näin on saatu haluttu tulos todistettua alialuekriteerin avulla.

Määritelmä 1.3. Olkoon R rengas, joka sisältää ykkösalkion. Silloin alkio $u \in R$ on renkaan R *yksikkö* (engl. unit), jos alkiolla u on käänteisalkio (kertolaskun suhteen) renkaassa R eli jos on olemassa sellainen alkio $v \in R$, että $uv = 1 = vu$.

Huomautus. Jos alkion $u \in R$ käänteisalkio (kertolaskun suhteen) on olemassa, niin se on yksikäsitteinen ja sitä merkitään kirjallisuudessa usein symbolilla u^{-1} (vrt. [6, s. 203]). Tällöin siis $u^{-1} \in R$ ja $uu^{-1} = 1 = u^{-1}u$.

Lause 1.3. *Olkoon R rengas, joka sisältää ykkösalkion. Jos alkio $u \in R$ on yksikkö, niin u ei ole nollanjakaja.*

Todistus. Ks. [6, s. 203].

Huomautus. Koska kunnan jokaisella nollasta eroavalla alkiolla on käänteisalkio, niin määritelmän 1.3 ja lauseen 1.3 perusteella kunnan jokainen nollasta eroava alkio on yksikkö.

1.3 Renkaan ihanteista

Tässä alaluvussa käydään läpi renkaan ihanteisiin liittyviä määritelmiä (vrt. [3, s. 81] ja [5, s. 295–298]), joita käytetään luvussa 3. Lisäksi käydään läpi tärkeitä renkaan ihanteisiin liittyviä lauseita.

Määritelmä 1.4. Olkoon R rengas. Joukon R ei-tyhjä osajoukko I on renkaan R *vasen ihanne* (engl. left ideal), jos

$$a - b \in I, \quad ra \in I$$

aina, kun $a, b \in I$ ja $r \in R$.

Määritelmä 1.5. Olkoon R rengas. Joukon R ei-tyhjä osajoukko I on renkaan R *oikea ihanne* (engl. right ideal), jos

$$a - b \in I, \quad ar \in I$$

aina, kun $a, b \in I$ ja $r \in R$.

Määritelmä 1.6. Olkoon R rengas. Joukon R ei-tyhjä osajoukko I on renkaan R *ihanne* (engl. ideal), jos I on renkaan R vasen ja oikea ihanne.

Määritelmistä 1.4 ja 1.5 seuraa, että jos I on renkaan R vasen tai oikea ihanne, niin silloin I on renkaan R alirengas (vrt. [5, s. 295]). Lisäksi jos R on kommutatiivinen rengas, niin silloin selvästi jokainen vasen ihanne on myös oikea ihanne ja jokainen oikea ihanne on myös vasen ihanne. Näin ollen määritelmän 1.6 mukaan kommutatiivisessa renkaassa R jokainen vasen tai oikea ihanne on kommutatiivisen renkaan R ihanne. (Vrt. [5, s. 296].)

Lause 1.4. (Ihannekriteeri) (vrt. [3, s. 80]) *Joukon R ei-tyhjä osajoukko I muodostaa renkaan R ihanteen, jos ja vain jos*

(i) $a - b \in I$ *aina, kun* $a, b \in I$,

(ii) $ra, ar \in I$ *aina, kun* $r \in R$ *ja* $a \in I$.

Todistus. Lauseen 1.4 todistus seuraa suoraan määritelmistä 1.4 ja 1.5.

Esimerkki 1.5. ([5, s. 296, Esim. 11.2.2]) Olkoon R rengas. Joukon R osajoukot $\{0\}$ ja R ovat renkaan R ihanteet, joita sanotaan renkaan R *triviaaleiksi ihanteiksi* (engl. trivial ideals).

Lause 1.5. *Olkoon R rengas, joka sisältää ykkösalkion. Olkoon I renkaan R ihanne, joka sisältää kääntyvän alkion. Silloin $I = R$.*

Todistus. Ks. [3, s. 81].

Lause 1.6. *Olkoon R rengas ja $\{ I_\alpha \mid \alpha \in \Lambda \}$ ei-tyhjä joukko renkaan R vasempia (oikeita) ihanteita. Silloin $\cap_{\alpha\in\Lambda} I_\alpha$ on renkaan R vasen (oikea) ihanne.*

Todistus. Ks. [5, s. 297].

Määritelmä 1.7. Olkoon R rengas ja S joukon R ei-tyhjä osajoukko. Silloin ihanne $\langle S \rangle$ on kaikkien joukon S sisältävien ihanteiden leikkaus. Ihannetta $\langle S \rangle$ sanotaan joukon S *virittämäksi ihanteeksi* (engl. the ideal generated by S).

Huomautus. Ihanne $\langle S \rangle$ on suppein ihanne, joka sisältää joukon S (vrt. [3, s. 81] ja [5, s. 297]).

Lause 1.7. *Olkoon R kommutatiivinen ykkösrengas ja S joukon R ei-tyhjä osajoukko. Silloin*

$$\langle S \rangle = \{ \sum_{i=1}^{k} r_i s_i \mid r_i \in R, s_i \in S, 1 \leq i \leq k, k \in \mathbb{N} \}.$$

Todistus. Lauseen 1.7 todistuksessa sovelletaan kommutatiivisuutta ja lähdekirjan [5] sivun 298 todistusta.

Jos S on äärellinen joukko $S = \{a_1, a_2, \ldots, a_n\}$, niin ihanteen $\langle S \rangle$ sanotaan olevan *äärellisesti viritetty* (engl. finitely generated). Tällöin merkitään $\langle S \rangle = \langle a_1, a_2, \ldots, a_n \rangle$. (Vrt. [5, s. 298].)

Määritelmä 1.8. Olkoon R rengas ja S joukon R ei-tyhjä osajoukko. Jos $S = \{a\}$, niin merkitään $\langle S \rangle = \langle a \rangle$ ja sanotaan, että $\langle a \rangle$ on alkion a virittämä ihanne. Yhden alkion virittämää ihannetta sanotaan *pääihanteeksi* (engl. principal ideal).

Lause 1.8. *Olkoon R kommutatiivinen rengas ja $a \in R$. Silloin*

$$\langle a \rangle = \{\, ra + na \mid r \in R, n \in \mathbb{Z} \,\}.$$

Todistus. Ks. [3, s. 81].

Seuraus. Olkoon R kommutatiivinen ykkösrengas ja $a \in R$. Silloin

$$\langle a \rangle = \{\, ra \mid r \in R \,\}.$$

Todistus. Ks. [3, s. 82].

2 Polynomirenkaat

Polynomien opiskelu ja tutkiminen on saanut alkunsa noin 1650 eKr., jolloin egyptiläiset ratkaisivat tietynlaisia lineaarisia polynomiyhtälöitä. Vuonna 600 eKr. hindut olivat oppineet ratkaisemaan toisen asteen yhtälöitä. Nykyisellä merkintätavalla kirjoitetut polynomit tulivat kuitenkin käyttöön vasta noin 1700 jKr. Noin vuonna 400 jKr. alkoi Intiassa ja Arabiassa esiintymään symbolisen algebran käyttöä. Jotkut pitävät symbolien käyttöä algebrassa abstraktin matematiikan ensimmäisenä tasona.

Niin sanottu polynomirenkaiden luokka on yksi tärkeä renkaiden luokka. Polynomit ovat lähes kaikille tuttuja ja yleisesti saatetaan ajatella polynomia muodon $a_0 + a_1 x + \cdots + a_n x^n$ ilmaisuna tai funktiona $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Tämän luvun tarkoituksena on selvittää, miten polynomit määritellään algebrassa ja miksi kaksi polynomia $a_0 + a_1 x + \cdots + a_n x^n$ ja $b_0 + b_1 x + \cdots + b_m x^m$ ovat samat, jos ja vain jos $n = m$ ja $a_i = b_i$ aina, kun $i = 0, 1, 2, \ldots, n$ sekä käsitellä joitakin polynomien ja polynomirenkaiden perusominaisuuksia.

2.1 Peruskäsitteiden määritelmiä

Tässä alaluvussa käydään läpi polynomeihin ja polynomirenkaisiin liittyvien peruskäsitteiden määritelmiä ja merkintätapoja (vrt. [5, s. 335–337] ja [6, s. 233]). Lisäksi käydään läpi muutama esimerkki.

Määritelmä 2.1. Olkoon R rengas. Renkaan R *polynomi* (engl. polynomial) on ääretön jono $(a_0, a_1, a_2, \ldots)$, missä $a_i \in R$, kun $i = 0, 1, 2, \ldots$, ja on olemassa sellainen ei-negatiivinen kokonaisluku n (riippuvainen jonosta $(a_0, a_1, a_2, \ldots)$), että $a_k = 0$, kun $k > n$.

Merkintä. Merkitään renkaan R kaikkien polynomien joukkoa symbolilla $R[x]$.

Määritelmä 2.2. Määritellään joukossa $R[x]$ *polynomien yhteenlasku ja kertolasku* seuraavasti:

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots) \tag{2.1}$$

ja

$$(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots), \tag{2.2}$$

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

Havainnollistetaan määritelmää 2.2 esimerkin avulla.

Esimerkki 2.1. ([2, s. 318, Harj. 3]) Olkoot polynomit $f(x) = \overline{2}x^2 + \overline{3}x + \overline{4}$ ja $g(x) = \overline{3}x^2 + \overline{2}x + \overline{3}$ joukon $\mathbb{Z}_6[x]$ alkioita. Silloin kaavan (2.1) perusteella saadaan, että

$$\begin{aligned} f(x) + g(x) &= (\overline{2}x^2 + \overline{3}x + \overline{4}) + (\overline{3}x^2 + \overline{2}x + \overline{3}) \\ &= \overline{5}x^2 + \overline{5}x + \overline{7} = \overline{5}x^2 + \overline{5}x + \overline{1}, \end{aligned}$$

ja kaavan (2.2) perusteella saadaan, että

$$\begin{aligned} f(x)g(x) &= (\overline{2}x^2 + \overline{3}x + \overline{4})(\overline{3}x^2 + \overline{2}x + \overline{3}) \\ &= \overline{6}x^4 + \overline{4}x^3 + \overline{6}x^2 + \overline{9}x^3 + \overline{6}x^2 + \overline{9}x + \overline{12}x^2 + \overline{8}x + \overline{12} \\ &= \overline{13}x^3 + \overline{17}x = x^3 + \overline{5}x. \end{aligned}$$

Tyydytään toteamaan ilman tarkkaa todistusta, että kolmikko $(R[x], +, \cdot)$ on rengas. Todetaan, että polynomi $(0, 0, 0, \ldots)$ on renkaan $R[x]$ nolla-alkio eli neutraalialkio yhteenlaskun suhteen ja polynomin $(a_0, a_1, a_2, \ldots)$ vasta-alkio yhteenlaskun suhteen on polynomi $(-a_0, -a_1, -a_2, \ldots)$. Määritelmän 2.2 kaavan (2.2) perusteella on selvää, että rengas $R[x]$ on kommutatiivinen silloin, kun rengas R on kommutatiivinen. Jos renkaassa R on ykkösalkio, niin silloin polynomi $(1, 0, 0, \ldots)$ on renkaan $R[x]$ ykkösalkio eli neutraalialkio kertolaskun suhteen.

Huomautus. Rengasta $R[x]$ sanotaan *polynomirenkaaksi* (engl. polynomial ring).

Muutetaan seuraavaksi polynomien merkintätapa yleisesti tunnetumpaan muotoon.

Merkintä. Merkitään polynomeja seuraavalla tavalla:

$$\begin{aligned} a &= ax^0 = (a, 0, 0, \ldots), \\ ax &= ax^1 = (0, a, 0, 0, \ldots), \\ ax^2 &= (0, 0, a, 0, 0, \ldots) \end{aligned}$$

ja niin edelleen. Tällöin saadaan, että $(a_0, a_1, \ldots, a_n, 0, \ldots) = (a_0, 0, 0, \ldots) + (0, a_1, 0, 0, \ldots) + \cdots + (0, \ldots, 0, a_n, 0, \ldots) = \sum_{k=0}^{\infty} a_k x^k = a_0 + a_1 x + \cdots + a_n x^n$.

Esimerkki 2.2. Joukossa $\mathbb{Z}[x]$ saadaan uuden merkintätavan perusteella, että

$$(2, 1, 0, 1, 0, 0, \ldots) = 2 + x + x^3$$

ja

$$(0, 3, 1, 0, 0, \ldots) = 3x + x^2.$$

Määritelmä 2.3. Joukon R alkioita $a_0, a_1, \ldots, a_n$ sanotaan polynomin $a_0 + a_1 x + \cdots + a_n x^n$ *kertoimiksi* (engl. coefficients). *Muuttujan* x (engl. indeterminate) potenssit x^k ilmaisevat kertoimensa a_k paikan jonossa $(a_0, a_1, a_2, \ldots)$.

Syy, miksi kaksi polynomia $a_0 + a_1 x + \cdots + a_n x^n$ ja $b_0 + b_1 x + \cdots + b_m x^m$ ovat samat, jos ja vain jos $n = m$ ja $a_i = b_i$ aina, kun $i = 0, 1, 2, \ldots, n$, on se, että kaksi jonoa $(a_0, a_1, a_2, \ldots)$ ja $(b_0, b_1, b_2, \ldots)$ ovat samat, jos ja vain jos $a_i = b_i$ aina, kun $i = 0, 1, 2, \ldots$

Määritelmä 2.4. Jos polynomin $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ kaikki kertoimet $a_0, a_1, \ldots, a_n$ ovat nollia, niin polynomia sanotaan *nollapolynomiksi* (engl. zero polynomial).

Huomautus. Nollapolynomi on siis sama kuin polynomi $(0, 0, 0, \ldots)$, jonka todettiin olevan polynomirenkaan $R[x]$ nolla-alkio.

Merkintä. Jos polynomi $f(x)$ on nollapolynomi, niin merkitään $f(x) = 0$. Jos polynomi $f(x)$ on nollapolynomista eroava, niin merkitään $f(x) \neq 0$.

Määritelmä 2.5. Olkoon R rengas. Jos $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, missä $a_n \neq 0$ ja $f(x) \in R[x]$, niin polynomin $f(x)$ *aste* (engl. degree) on n. Silloin merkitään $\deg f(x) = n$. Kerrointa a_n sanotaan tällöin polynomin $f(x)$ *johtavaksi kertoimeksi* (engl. leading coefficient). Jos $a_n = 1$, niin polynomia $f(x)$ sanotaan *pääpolynomiksi* (engl. monic polynomial).

Määritelmä 2.6. Joukon $R[x]$ astetta 0 olevat polynomit ovat joukon $R \setminus \{0\}$ alkiot. Polynomin $0 \in R[x]$ astetta ei ole määritelty. Joukon R alkioita sanotaan *skalaareiksi* (engl. scalar) tai *vakiopolynomeiksi* (engl. constant polynomials).

2.2 Neljä polynomirenkaita koskevaa lausetta

Tässä alaluvussa esitetään neljä polynomirenkaita koskevaa lausetta. Ne todistetaan ja niitä tullaan käyttämään jatkossa. Lisäksi käydään läpi muutama esimerkki.

Lause 2.1. *Jos R on kommutatiivinen ykkösrengas, niin $R[x]$ on kommutatiivinen ykkösrengas.*

Todistus (vrt. [5, s. 337]). Oletetaan, että R on kommutatiivinen ykkösrengas.

Todistetaan ensin, että rengas $R[x]$ on kommutatiivinen. Olkoot polynomit $f(x) = a_0 + a_1x + \cdots + a_nx^n$ ja $g(x) = b_0 + b_1x + \cdots + b_mx^m$ joukon $R[x]$ alkioita. Olkoot tällöin $f(x)g(x) = c_0 + c_1x + \cdots + c_tx^t$ ja $g(x)f(x) = d_0 + d_1x + \cdots + d_sx^s$. Tällöin määritelmän 2.2 mukaan $c_j = \sum_{i=0}^{j} a_ib_{j-i}$ ja $d_j = \sum_{i=0}^{j} b_ia_{j-i}$, kun $j = 0, 1, 2, \ldots$ Koska oletuksen mukaan rengas R on kommutatiivinen, niin

$$\begin{aligned} c_j &= a_0b_j + a_1b_{j-1} + \cdots + a_{j-1}b_1 + a_jb_0 \\ &= b_0a_j + b_1a_{j-1} + \cdots + b_{j-1}a_1 + b_ja_0 \\ &= d_j \end{aligned}$$

aina, kun $j = 0, 1, 2, \ldots$ Näin on saatu todistettua, että $f(x)g(x) = g(x)f(x)$, joten rengas $R[x]$ on kommutatiivinen.

Todistetaan vielä, että renkaassa $R[x]$ on ykkösalkio. Oletuksen mukaan renkaassa R on ykkösalkio, joten $1 \in R$. Tällöin polynomi $(1, 0, 0, \ldots) = 1$ on renkaan $R[x]$ ykkösalkio, koska $1 \in R[x]$ ja kaavan (2.2) mukaan $1 \cdot f(x) = f(x) \cdot 1 = (a_0, a_1, \ldots, a_n) \cdot (1, 0, \ldots, 0) = (a_0 \cdot 1, a_0 \cdot 0 + a_1 \cdot 1, \ldots, a_0 \cdot 0 + a_1 \cdot 0 + \cdots + a_n \cdot 1) = (a_0, a_1, \ldots, a_n) = f(x)$ aina, kun $f(x) \in R[x]$. Täten renkaassa $R[x]$ on ykkösalkio.

Näin on saatu, että $R[x]$ on kommutatiivinen ykkösrengas, joten lause on todistettu.

Lause 2.2. *Jos R on kokonaisalue, niin $R[x]$ on kokonaisalue.*

Todistus (vrt. [5, s. 337]). Oletetaan, että R on kokonaisalue. Tällöin kokonaisalueen määritelmän mukaan R on kommutatiivinen ykkösrengas ja edelleen lauseen 2.1 perusteella $R[x]$ on kommutatiivinen ykkösrengas. Täten riittää todistaa, että renkaassa $R[x]$ ei ole nollanjakajia. Olkoot polynomit $f(x) = a_0 + a_1x + \cdots + a_nx^n$ ja $g(x) = b_0 + b_1x + \cdots + b_mx^m$ nollapolynomista eroavia joukon $R[x]$ alkioita. Silloin on olemassa sellaiset $a_i \neq 0$ ja $b_j \neq 0$, että $a_{i+t} = 0$ ja $b_{j+t} = 0$ aina, kun $t \geq 1$. Olkoon $f(x)g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$, missä nyt $c_{i+j} = a_0b_{i+j} + a_1b_{i+j-1} + \cdots + a_ib_j + \cdots + a_{i+j}b_0 = a_ib_j$. Kokonaisalueen määritelmän mukaan renkaassa R ei ole nollanjakajia, joten $a_ib_j \neq 0$. Näin ollen vähintään yksi polynomin $f(x)g(x)$ kertoimista on nollasta eroava, joten $f(x)g(x) \neq 0$. Täten renkaassa $R[x]$ ei ole nollanjakajia. Näin on saatu, että $R[x]$ on kokonaisalue, joten lause on todistettu.

Lause 2.3. *Olkoon $R[x]$ polynomirengas. Olkoot polynomit $f(x) \neq 0$ ja $g(x) \neq 0$ joukon $R[x]$ alkioita. Silloin polynomien summan ja tulon asteille ovat voimassa seuraavat ominaisuudet.*

(i) *Jos $f(x)g(x) \neq 0$, niin* $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$.

(ii) *Jos $f(x) + g(x) \neq 0$, niin* $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$.

Todistus (vrt. [5, s. 337]). Todistetaan ensin lauseen kohta (i). Jos $f(x) = a_0 + a_1x + \cdots + a_nx^n$ ja $g(x) = b_0 + b_1x + \cdots + b_mx^m$, niin silloin kaavan (2.2) mukaan $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m}$. Jos $f(x)g(x) \neq 0$, niin vähintään yksi polynomin $f(x)g(x)$ kertoimista on nollasta eroava. Nyt on kaksi eri mahdollisuutta, jotka käydään erikseen läpi. Jos polynomin $f(x)g(x)$ kerroin $a_nb_m \neq 0$, niin silloin

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

Jos kerroin $a_nb_m = 0$, mikä on mahdollista silloin, kun renkaassa R on nollanjakajia, niin silloin

$$\deg(f(x)g(x)) < n + m = \deg f(x) + \deg g(x).$$

Näin on saatu todistettua, että jos $f(x)g(x) \neq 0$, niin silloin $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$.

Todistetaan seuraavaksi kohta (ii) käymällä erikseen läpi kolme eri mahdollisuutta. Jos $\deg f(x) > \deg g(x)$, niin silloin

$$\deg(f(x) + g(x)) = \deg f(x) = \max\{\deg f(x), \deg g(x)\}.$$

Jos $\deg g(x) > \deg f(x)$, niin silloin

$$\deg(f(x) + g(x)) = \deg g(x) = \max\{\deg f(x), \deg g(x)\}.$$

Jos $\deg f(x) = \deg g(x)$, niin silloin on kolme mahdollisuutta:

$$\begin{aligned} f(x) + g(x) &= 0, \\ \deg(f(x) + g(x)) &= \deg f(x) = \deg g(x) = \max\{\deg f(x), \deg g(x)\}, \\ \deg(f(x) + g(x)) &< \deg f(x) = \deg g(x) = \max\{\deg f(x), \deg g(x)\}. \end{aligned}$$

Näin on saatu todistettua, että jos $f(x) + g(x) \neq 0$, niin silloin $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$.

Huomautus. Lauseen 2.3 kohdan (i) todistuksesta seuraa suoraan, että jos renkaassa R ei ole nollanjakajia eli jos R on kokonaisalue, niin lauseen 2.3 kohdassa (i) on voimassa yhtäsuuruus (ks. [6, s. 235, Lauseen 8.1.12 todistus]).

Käydään läpi lausetta 2.3 havainnollistava esimerkki.

Esimerkki 2.3. ([5, s. 338, Esim. 14.1.5]) Olkoot polynomit $f(x) = \overline{1} + \overline{2}x^2$ ja $g(x) = \overline{1} + \overline{3}x$ joukon $\mathbb{Z}_6[x]$ alkioita. Silloin $f(x)g(x) = \overline{1} + \overline{3}x + \overline{2}x^2 + \overline{6}x^3 = \overline{1} + \overline{3}x + \overline{2}x^2$. Täten $\deg(f(x)g(x)) = 2 < 3 = \deg f(x) + \deg g(x)$. Toisaalta $f(x) + g(x) = \overline{2} + \overline{3}x + \overline{2}x^2$. Täten $\deg(f(x) + g(x)) = 2 = \deg f(x) = \max\{\deg f(x), \deg g(x)\} = \max\{2, 1\}$. Olkoon polynomi $h(x) = \overline{5} + \overline{4}x^2$ myös joukon $\mathbb{Z}_6[x]$ alkio. Silloin $f(x) + h(x) = \overline{6} + \overline{6}x^2 = \overline{0}$ ja $\deg(f(x) + h(x))$ ei ole määritelty, koska nollapolynomin astetta ei ole määritelty.

Käydään seuraavaksi läpi esimerkki, jossa käytetään apuna lausetta 2.3.

Esimerkki 2.4. ([6, s. 238, Harj. 19.(c)]) Etsitään polynomirenkaan $\mathbb{Z}_5[x]$ kaikki yksiköt. Olkoon polynomi $f(x) \neq 0$ joukon $\mathbb{Z}_5[x]$ alkio ja oletetaan, että se on polynomirenkaan $\mathbb{Z}_5[x]$ yksikkö. Tällöin yksikön määritelmän mukaan on olemassa sellainen joukon $\mathbb{Z}_5[x]$ alkio $g(x)$, että $f(x)g(x) = \overline{1} \in \mathbb{Z}_5[x]$. Koska polynomirenkaassa $\mathbb{Z}_5$ ei ole nollanjakajia, niin lauseen 2.3 kohdan (i) ja siihen liittyvän huomautuksen perusteella $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$. Toisaalta on saatu, että $f(x)g(x) = \overline{1}$, jolloin $\deg(f(x)g(x)) = \deg(\overline{1}) = 0$. Näin on saatu, että $\deg f(x) + \deg g(x) = 0$. Koska $\deg f(x) \geq 0$ ja $\deg g(x) \geq 0$, niin selvästi $\deg f(x) = 0$. Tällöin $f(x)$ on määritelmän 2.6 mukaan nollapolynomista eroava vakiopolynomi. Näin ollen joukon $\mathbb{Z}_5$ alkiot $\overline{1}$, $\overline{2}$, $\overline{3}$ ja $\overline{4}$ ovat polynomirenkaan $\mathbb{Z}_5[x]$ yksiköt.

Lause 2.4. *Olkoon R kokonaisalue. Silloin kokonaisalueen $R[x]$ yksiköt ovat täsmälleen samat kuin kokonaisalueen R yksiköt.*

Todistus (vrt. [6, s. 235]). Todistetaan lause kahteen eri suuntaan.

Oletetaan ensin, että alkio $c \in R$ on yksikkö kokonaisalueessa R ja että alkio $d \in R$ on sen käänteisalkio (kertolaskun suhteen). Alkiot c ja d ovat määritelmän 2.6 mukaan vakiopolynomeja, joten selvästi $c, d \in R[x]$. Tällöin määritelmän 1.3 mukaan $cd = 1$ kokonaisalueessa R ja koska vakiopolynomit $c, d \in R[x]$, niin $cd = 1$ myös kokonaisalueessa $R[x]$. Näin ollen määritelmän 1.3 mukaan alkio c on yksikkö myös kokonaisalueessa $R[x]$ ja alkio d on sen käänteisalkio (kertolaskun suhteen). Näin on saatu todistettua, että kokonaisalueen R yksiköt ovat myös kokonaisalueen $R[x]$ yksiköitä.

Oletetaan sitten, että polynomi $f(x) \in R[x]$ on yksikkö kokonaisalueessa $R[x]$ ja että polynomi $g(x) \in R[x]$ on sen käänteisalkio (kertolaskun suhteen). Tällöin määritelmän 1.3 mukaan $f(x)g(x) = 1$, joten $\deg(f(x)g(x)) = 0$. Koska lauseen oletuksen mukaan R on kokonaisalue, niin lauseen 2.3 kohdan (i) ja siihen liittyvän huomautuksen perusteella $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$. Edellä on saatu, että $\deg(f(x)g(x)) = 0$, joten $\deg f(x) + \deg g(x) = 0$. Koska polynomin aste on aina ≥ 0, niin selvästi nyt $\deg f(x) = 0$ ja $\deg g(x) = 0$. Tällöin määritelmän 2.6 mukaan polynomit $f(x)$ ja $g(x)$ ovat vakiopolynomeja ja näin ollen molemmat ovat joukon R alkioita. Merkitään $f(x) = c_0$ ja $g(x) = d_0$, jolloin siis $c_0, d_0 \in R$. Koska $c_0 d_0 = f(x)g(x) = 1$, niin määritelmän 1.3 mukaan c_0 on yksikkö kokonaisalueessa R ja d_0 on sen

käänteisalkio (kertolaskun suhteen). Näin on saatu todistettua, että kokonaisalueen $R[x]$ yksiköt ovat myös kokonaisalueen R yksiköitä.

Näin ollen lause 2.4 on saatu todistettua.

2.3 Polynomien jaollisuudesta

Tässä alaluvussa esitetään kaksi polynomien jaollisuuteen liittyvää lausetta; jakoalgoritmi ja jäännöslause. Lisäksi esitetään jäännöslauseeseen liittyvä seurauslause ja viimeiseksi astetta n olevan polynomin nollakohtien lukumäärää koskeva lause. Kaikki lauseet todistetaan ja niitä käytetään jatkossa. Lisäksi käydään läpi muutamien polynomien jaollisuuteen liittyvien käsitteiden määritelmiä (vrt. [5, s. 339]) sekä lauseisiin ja määritelmiin liittyviä ja niitä havainnollistavia esimerkkejä.

Lause 2.5. (Jakoalgoritmi) *Olkoon R kommutatiivinen ykkösrengas. Olkoot $f(x), g(x) \in R[x]$ sellaiset polynomit, että polynomin $g(x)$ johtava kerroin on yksikkö renkaassa R. Silloin on olemassa sellaiset yksikäsitteiset polynomit $q(x), r(x) \in R[x]$, että*

$$f(x) = q(x)g(x) + r(x),$$

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

Todistus (vrt. [5, s. 338-339] ja [6, s. 240-241]). Todistetaan lause kahdessa osassa.

Todistetaan ensin polynomien $q(x)$ ja $r(x)$ olemassaolo. Jos $f(x) = 0$ tai $\deg f(x) < \deg g(x)$, niin valitaan $q(x) = 0$ ja $r(x) = f(x)$. Oletetaan, että $\deg f(x) \geq \deg g(x)$ ja todistetaan polynomien $q(x)$ ja $r(x)$ olemassaolo induktiolla polynomin $f(x)$ asteen suhteen. Olkoon $\deg f(x) = n$ ja $\deg g(x) = m$. Jos $n = m = 0$, niin polynomit $f(x)$ ja $g(x)$ ovat vakiopolynomeja. Merkitään $f(x) = a_0$ ja $g(x) = b_0 \neq 0$, missä $a_0, b_0 \in R$. Koska $b_0 \neq 0$ on nyt polynomin $g(x)$ johtava kerroin, niin lauseen oletuksen mukaan b_0 on yksikkö renkaassa R, jolloin b_0^{-1} on olemassa yksikön määritelmän nojalla. Tällöin $a_0 b_0^{-1} \in R$ ja $f(x) = a_0 b_0^{-1} g(x) + 0$, joten $q(x) = f(x)g(x)^{-1}$ ja $r(x) = 0$. Tehdään seuraavaksi induktio-oletus, jonka mukaan polynomit $q(x)$ ja $r(x)$ ovat olemassa kaikilla polynomeilla, joiden aste on $< n$. Olkoot $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ ja $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ sellaiset polynomit, että $n \geq m$. Koska nyt $b_m \neq 0$ on polynomin $g(x)$ johtava kerroin, niin jälleen lauseen oletuksen mukaan b_m on yksikkö renkaassa R, jolloin b_m^{-1} on olemassa yksikön määritelmän nojalla. Polynomin

$$f_1(x) = f(x) - (a_n b_m^{-1}) x^{n-m} g(x) \tag{2.3}$$

aste on $< n$, koska muuttujan x^n kerroin on $a_n - (a_n b_m^{-1}) b_m = 0$. Tällöin induktio-oletuksen mukaan on olemassa sellaiset polynomit $q_1(x), r_1(x) \in R[x]$, että

$$f_1(x) = q_1(x)g(x) + r_1(x), \tag{2.4}$$

missä $r_1(x) = 0$ tai $\deg r_1(x) < \deg g(x)$. Kun nyt sijoitetaan yhtälöön (2.3) yhtälön (2.4) oikea puoli, niin saadaan yhtälö

$$q_1(x)g(x) + r_1(x) = f(x) - (a_n b_m^{-1})x^{n-m}g(x). \tag{2.5}$$

Ratkaistaan yhtälöstä (2.5) polynomi $f(x)$, jolloin saadaan

$$\begin{aligned} f(x) &= q_1(x)g(x) + r_1(x) + (a_n b_m^{-1})x^{n-m}g(x) \\ &= (q_1(x) + a_n b_m^{-1}x^{n-m})g(x) + r_1(x) \\ &= q(x)g(x) + r(x), \end{aligned}$$

missä $q(x) = q_1(x) + a_n b_m^{-1}x^{n-m}$ ja $r(x) = r_1(x)$. Näin on saatu polynomi $f(x)$, jonka aste on n, haluttuun muotoon ja polynomien $q(x)$ ja $r(x)$ olemassaolo on saatu todistettua.

Todistetaan vielä polynomien $q(x)$ ja $r(x)$ yksikäsitteisyys. Oletetaan, että on olemassa sellaiset polynomit $q(x), r(x), q'(x), r'(x) \in R[x]$, että

$$f(x) = q(x)g(x) + r(x)$$

ja

$$f(x) = q'(x)g(x) + r'(x),$$

missä $r(x) = 0$ tai $\deg r(x) < \deg g(x)$ ja $r'(x) = 0$ tai $\deg r'(x) < \deg g(x)$. Tällöin

$$q(x)g(x) + r(x) = q'(x)g(x) + r'(x),$$

josta saadaan yhtälö

$$r(x) - r'(x) = (q'(x) - q(x))g(x). \tag{2.6}$$

Oletetaan nyt, että $r(x) - r'(x) \neq 0$. Koska polynomin $g(x)$ johtava kerroin on lauseen oletuksen mukaan yksikkö renkaassa R, jolloin se ei voi olla nollanjakaja, niin lauseen 2.3 kohdan (i) perusteella

$$\deg((q'(x) - q(x))g(x)) = \deg(q'(x) - q(x)) + \deg g(x) \geq \deg g(x).$$

Tästä seuraa yhtälön (2.6) perusteella, että

$$\deg(r(x) - r'(x)) \geq \deg g(x),$$

mikä on mahdotonta, koska $\deg r(x), \deg r'(x) < \deg g(x)$. Näin ollen edellä tehty oletus on väärin ja yhtälö $r(x) - r'(x) = 0$ eli $r(x) = r'(x)$ on voimassa. Tällöin yhtälön (2.6) perusteella

$$0 = (q'(x) - q(x))g(x). \tag{2.7}$$

Koska b_m on yksikkö, niin $\deg(((q'(x) - q(x))g(x)) \geq 0$ aina, kun $q'(x) - q(x) \neq 0$. Yhtälön (2.7) perusteella $\deg(q'(x) - q(x))g(x)$ ei ole määritelty, koska $(q'(x) - q(x))g(x)$ on nollapolynomi. Näin ollen tulee olla, että $q'(x) - q(x) = 0$ eli $q'(x) = q(x)$. Näin on saatu todistettua polynomien $q(x)$ ja $r(x)$ yksikäsitteisyys.

Näin ollen lause 2.5 on siis saatu todistettua.

Määritelmä 2.7. Lauseessa 2.5 esiintyvä polynomi $q(x)$ on nimeltään *osamäärä* (engl. quotient) ja $r(x)$ on *jakojäännös* (engl. remainder), kun jaetaan polynomia $f(x)$ polynomilla $g(x)$.

Käydään läpi lauseeseen 2.5 ja määritelmään 2.7 liittyvä esimerkki.

Esimerkki 2.5. ([4, s. 151, Harj. 9]) Olkoot polynomit $f(x) = 7x^4 + 2x^3 + 9x^2 + 5$ ja $g(x) = x^3 + x + 1$ joukon $\mathbb{Z}[x]$ alkioita. Etsitään lauseen 2.5 mukaiset polynomit $q(x)$ ja $r(x)$. Kun jaetaan polynomi $f(x)$ polynomilla $g(x)$ jakokulmassa, niin saadaan, että osamäärä on $7x + 2$ ja jakojäännös on $2x^2 - 9x + 3$. Näin ollen määritelmän 2.7 mukaan $q(x) = 7x + 2$ ja $r(x) = 2x^2 - 9x + 3$. Tällöin $q(x)g(x) + r(x) = (7x+2)(x^3+x+1) + (2x^2 - 9x + 3) = 7x^4 + 7x^2 + 7x + 2x^3 + 2x + 2 + 2x^2 - 9x + 3 = 7x^4 + 2x^3 + 9x^2 + 5 = f(x)$, joten halutut polynomit $q(x)$ ja $r(x)$ ollaan löydetty.

Määritelmä 2.8. Olkoon R kommutatiivinen ykkösrengas ja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. Määritellään $f(r) = a_0 + a_1r + \cdots + a_nr^n$ aina, kun $r \in R$. Jos $f(r) = 0$, sanotaan alkiota $r \in R$ polynomin $f(x)$ *nollakohdaksi* (engl. zero) tai *juureksi* (engl. root).

Havainnollistetaan määritelmää 2.8 seuraavien esimerkkien avulla.

Esimerkki 2.6. ([2, s. 318, Harj. 13]) Etsitään polynomin $f(x) = x^3 + \overline{2}x + \overline{2} \in \mathbb{Z}_7[x]$ kaikki nollakohdat. Käydään läpi kaikki seitsemän mahdollisuutta. Laskemalla saadaan

$$\begin{aligned}
f(\overline{0}) &= \overline{2} \neq \overline{0},\\
f(\overline{1}) &= \overline{5} \neq \overline{0},\\
f(\overline{2}) &= \overline{14} = \overline{0},\\
f(\overline{3}) &= \overline{35} = \overline{0},\\
f(\overline{4}) &= \overline{74} = \overline{4} \neq \overline{0},\\
f(\overline{5}) &= \overline{137} = \overline{4} \neq \overline{0},\\
f(\overline{6}) &= \overline{230} = \overline{6} \neq \overline{0}.
\end{aligned}$$

Näin on saatu, että polynomin $f(x) = x^3 + \overline{2}x + \overline{2} \in \mathbb{Z}_7[x]$ ainoat nollakohdat ovat joukon $\mathbb{Z}_7$ alkiot $\overline{2}$ ja $\overline{3}$.

Esimerkki 2.7. Etsitään polynomin $g(x) = x^2 + \overline{1} \in \mathbb{Z}_3[x]$ kaikki nollakohdat. Käydään läpi kaikki kolme mahdollisuutta. Laskemalla saadaan

$$\begin{aligned}
g(\overline{0}) &= \overline{1} \neq \overline{0},\\
g(\overline{1}) &= \overline{2} \neq \overline{0},\\
g(\overline{2}) &= \overline{5} = \overline{2} \neq \overline{0}.
\end{aligned}$$

Näin on saatu, että polynomilla $g(x) = x^2 + \overline{1} \in \mathbb{Z}_3[x]$ ei ole yhtään nollakohtaa.

Määritelmä 2.9. Olkoon R kommutatiivinen ykkösrengas ja olkoot polynomit $f(x)$ ja $g(x) \neq 0$ joukon $R[x]$ alkioita. Jos on olemassa sellainen polynomi $q(x) \in R[x]$, että

$$f(x) = q(x)g(x),$$

niin sanotaan, että polynomi $g(x)$ *jakaa* (engl. divides) polynomin $f(x)$ tai että polynomi $g(x)$ on polynomin $f(x)$ *tekijä* (engl. factor). Tällöin merkitään

$$g(x) \mid f(x).$$

Havainnollistetaan seuraavalla esimerkillä määritelmää 2.9.

Esimerkki 2.8. Tarkastellaan kommutatiivista ykkösrengasta $\mathbb{Z}_6[x]$ ja siellä polynomeja $f(x) = \overline{2}+x^2$, $g(x) = \overline{2}+x$ ja $q(x) = \overline{4}+x$. Laskemalla saadaan, että $q(x)g(x) = (\overline{4}+x)(\overline{2}+x) = \overline{8}+\overline{4}x+\overline{2}x+x^2 = \overline{2}+\overline{6}x+x^2 = \overline{2}+x^2 = f(x)$, joten määritelmän 2.9 mukaan

$$\overline{2} + x \mid \overline{2} + x^2.$$

Laskemalla saadaan myös, että $g(x)q(x) = (\overline{2}+x)(\overline{4}+x) = \overline{8}+\overline{2}x+\overline{4}x+x^2 = \overline{2} + x^2 = f(x)$, joten määritelmän 2.9 mukaan

$$\overline{4} + x \mid \overline{2} + x^2.$$

Lause 2.6. (Jäännöslause) *Olkoon R kommutatiivinen ykkösrengas. Kun $f(x) \in R[x]$ ja $a \in R$, niin silloin on olemassa sellainen polynomi $q(x) \in R[x]$, että*

$$f(x) = (x - a)q(x) + f(a).$$

Todistus (vrt. [5, s. 340]). Lauseen todistamisessa voidaan käyttää jakoalgoritmia ja polynomia $g(x) = x-a$, koska jakoalgoritmin oletukset ovat voimassa. Tällöin jakoalgoritmin perusteella on olemassa sellaiset yksikäsitteiset polynomit $q(x), r(x) \in R[x]$, että $f(x) = (x-a)q(x)+r(x)$, missä joko $r(x) = 0$ tai $\deg r(x) < \deg g(x) = 1$. Tällöin määritelmän 2.6 mukaan $r(x)$ on vakiopolynomi, merkitään $r(x) = d$. Näin ollen yhtälö $f(x) = (x-a)q(x)+d$ on voimassa ja sijoittamalla siinä muuttujan x paikalle alkio $a \in R$, saadaan yhtälö $f(a) = (a-a)q(a)+d = d$. Näin on saatu, että yhtälö $f(x) = (x-a)q(x)+f(a)$ on voimassa, kun $f(x) \in R[x]$ ja $a \in R$, joten lause on todistettu.

Seuraus. Olkoon R kommutatiivinen ykkösrengas, $f(x) \in R[x]$ ja $a \in R$. Silloin polynomi $x - a$ jakaa polynomin $f(x)$, jos ja vain jos alkio a on polynomin $f(x)$ nollakohta.

Todistus (vrt. [5, s. 340]). Todistetaan seurauslause kahteen eri suuntaan.

Oletetaan ensin, että polynomi $x - a$ jakaa polynomin $f(x)$ eli että $x - a \mid f(x)$. Silloin määritelmän 2.9 mukaan on olemassa sellainen polynomi $q(x) \in R[x]$, että yhtälö $f(x) = (x - a)q(x)$ on voimassa. Tällöin $f(a) =$

$(a-a)q(a)=0$, joten alkio a on polynomin $f(x)$ nollakohta. Näin on saatu todistettua, että jos $x-a \mid f(x)$, niin $f(a)=0$.

Oletetaan sitten, että alkio a on polynomin $f(x)$ nollakohta eli että $f(a)=0$. Silloin jäännöslauseen perusteella saadaan, että yhtälö $f(x)=(x-a)q(x)+0=(x-a)q(x)$ on voimassa, joten määritelmän 2.9 mukaan polynomi $x-a$ jakaa polynomin $f(x)$. Näin on saatu todistettua, että jos $f(a)=0$, niin $x-a \mid f(x)$.

Näin on kaikkiaan saatu todistettua, että polynomi $x-a$ jakaa polynomin $f(x)$, jos ja vain jos alkio a on polynomin $f(x)$ nollakohta.

Käydään seuraavaksi läpi jäännöslauseen seurauslausetta havainnollistava esimerkki.

Esimerkki 2.9. Yllä olevan seurauslauseen ja esimerkin 2.6 perusteella renkaassa $\mathbb{Z}_7[x]$ polynomit $x-\overline{2}$ ja $x-\overline{3}$ jakavat polynomin $f(x)=x^3+\overline{2}x+\overline{2}$.

Toisaalta yllä olevan seurauslauseen ja esimerkin 2.7 perusteella renkaassa $\mathbb{Z}_3[x]$ mikään 1.asteen polynomi ei jaa polynomia $g(x)=x^2+\overline{1}$.

Lause 2.7. *Olkoon R kokonaisalue ja $f(x) \in R[x]$ astetta n oleva nollapolynomista eroava polynomi. Silloin polynomilla $f(x)$ on enintään n nollakohtaa kokonaisalueessa R.*

Todistus (vrt. [5, s. 340]). Jos $\deg f(x)=0$, niin silloin $f(x)$ on nollapolynomista eroava vakiopolynomi. Merkitään $f(x)=c\neq 0$. Tällöin polynomilla $f(x)$ ei ole yhtään nollakohtaa kokonaisalueessa R, joten lauseen väitös on tosi. Tehdään seuraavaksi induktio-oletus, että lauseen väitös on tosi kaikilla polynomeilla, joiden aste on $<n$. Induktioväitteenä on tällöin, että lauseen väitös on tosi polynomeilla, joiden aste on n. Oletetaan, että $\deg f(x)=n$. Jos polynomilla $f(x)$ ei ole yhtään nollakohtaa kokonaisalueessa R, on lauseen väitös selvästi tosi. Oletetaan nyt, että alkio $r \in R$ on polynomin $f(x)$ nollakohta eli että $f(r)=0$. Silloin jäännöslauseen seurauslauseen perusteella polynomi $x-r$ jakaa polynomin $f(x)$, jolloin määritelmän 2.9 mukaan on olemassa sellainen polynomi $q(x) \in R[x]$, että yhtälö

$$f(x)=(x-r)q(x) \tag{2.8}$$

on voimassa. Yhtälössä (2.8) $\deg q(x)=n-1$, koska oletuksen mukaan $\deg f(x)=n$ ja selvästi $\deg(x-r)=1$. Perusteena polynomin $q(x)$ asteelle on lisäksi oletus siitä, että R on kokonaisalue ja lauseen 2.3 kohtaan (i) liittyvä huomautus, joiden perusteella yhtälö $\deg f(x)=\deg((x-r)q(x))=\deg(x-r)+\deg q(x)=n$ on voimassa. Jos alkio $r' \in R$ on polynomin $f(x)$ jokin toinen nollakohta, niin silloin $f(r')=(r'-r)q(r')=0$. Koska R on kokonaisalue, niin lauseen 2.2 perusteella $R[x]$ on kokonaisalue. Koska $r' \neq r$, niin $r'-r\neq 0$. Näin ollen $q(r')=0$, koska kokonaisalueessa ei ole nollanjakajia. Tällöin siis r' on polynomin $q(x)$ nollakohta. Näin ollen mikä tahansa polynomin $f(x)$ nollakohdasta r eroava nollakohta r' on myös polynomin $q(x)$

nollakohta. Koska $f(x) = (x-r)q(x)$, niin mikä tahansa polynomin $q(x)$ nollakohta on myös polynomin $f(x)$ nollakohta. Koska $\deg q(x) = n-1 < n$, niin induktio-oletuksen mukaan polynomilla $q(x)$ on enintään $n-1$ nollakohtaa r'. Täten polynomilla $f(x)$ on enintään $n-1$ nollakohtaa r' ja lisäksi nollakohta r, joten polynomilla $f(x)$ on kaikkiaan enintään n nollakohtaa kokonaisalueessa R. Näin on saatu induktioväite todistettua ja samalla induktioperiaatteen nojalla lauseen väitös on todistettu.

3 Euklidiset alueet

Tämän luvun yhtenä tarkoituksena on saattaa jo tutuksi tullut jakoalgoritmin käsite abstraktimpaan muotoon. Tämä on mielekästä jakoalgoritmin tärkeyden vuoksi. Luvun alaluvut ovat todella paljon yhteydessä toisiinsa ja tämän vuoksi alaluvuissa esiintyvät esimerkit liittyvät usein useampaan kuin yhteen alalukuun.

3.1 Euklidisen alueen määritelmä

Tässä alaluvussa käydään läpi euklidisen alueen määritelmä (vrt. [5, s. 345] ja [6, s. 280]) ja muutama siihen liittyvä huomautus. Lisäksi käydään läpi muutama määritelmään liittyvä esimerkki. Alaluvussa esitetään myös yksi lause, joka osoittaa polynomirenkaiden ja euklidisten alueiden yhteyden.

Määritelmä 3.1. Kokonaisalue $(E, +, \cdot)$ ja sellainen funktio $v\colon (E \setminus \{0\}) \to (\mathbb{Z}^+ \cup \{0\})$, että

(i) jokaisia joukon E alkioita a ja $b \neq 0$ kohti on olemassa sellaiset alkiot $q, r \in E$, että $a = qb + r$, missä joko $r = 0$ tai $v(r) < v(b)$ ja

(ii) $v(a) \leq v(ab)$ aina, kun $a, b \in E \setminus \{0\}$,

muodostavat *euklidisen alueen* (engl. Euclidean domain) $(E, +, \cdot, v)$.

Määritelmässä 3.1 esiintyvää alkiota q sanotaan *osamääräksi* (engl. quotient) ja alkiota r sanotaan *jakojäännökseksi* (engl. remainder). (Vrt. [6, s. 280].)

Huomautus. Euklidisen alueen määritelmässä eli määritelmässä 3.1 ei vaadita osamäärän q eikä jakojäännöksen r yksikäsitteisyyttä. (Vrt. [6, s. 281].)

Huomautus. Määritelmässä 3.1 määriteltyä funktiota v sanotaan *euklidiseksi valuaatioksi* (engl. Euclidean valuation) ja se siis kuvaa joukon E nollasta eroavat alkiot ei-negatiivisiksi kokonaisluvuiksi.

Seuraava esimerkki ja lause osoittavat, että rengas $\mathbb{Z}$ ja polynomirengas $F[x]$, missä F on kunta, ovat euklidisia alueita.

Esimerkki 3.1. ([5, s. 345, Esim. 15.1.2]) Kokonaisalue $(\mathbb{Z}, +, \cdot)$ ja funktio $v\colon (\mathbb{Z} \setminus \{0\}) \to (\mathbb{Z}^+ \cup \{0\})$, missä $v(a) = |a|$ aina, kun $a \neq 0$, muodostavat euklidisen alueen. Määritelmän 3.1 kohta (i) on voimassa joukon $\mathbb{Z}$ jakoalgoritmin perusteella. Määritelmän 3.1 kohta (ii) on voimassa, koska yhtälö $v(a) = |a| \leq |a||b| = |ab| = v(ab)$ pätee aina, kun $a, b \in \mathbb{Z} \setminus \{0\}$.

Lause 3.1. *Jos F on kunta, niin polynomirengas $F[x]$ on euklidinen alue.*

Todistus (vrt. [5, s. 345–346]). Oletetaan, että F on kunta, jolloin F on myös kokonaisalue. Silloin lauseen 2.2 perusteella myös polynomirengas $F[x]$ on kokonaisalue. Olkoon funktio $v\colon (F[x] \setminus \{0\}) \to (\mathbb{Z}^+ \cup \{0\})$ sellainen, että $v(f(x)) = \deg f(x)$ aina, kun $f(x) \in F[x] \setminus \{0\}$. Koska $\deg f(x) \in \mathbb{Z}^+ \cup \{0\}$ aina, kun $f(x) \in F[x] \setminus \{0\}$, niin $v(f(x)) \in \mathbb{Z}^+ \cup \{0\}$. Todistetaan nyt määritelmän 3.1 kohdat (i) ja (ii) erikseen.

Todistetaan ensin kohta (i). Olkoot polynomit $f(x)$ ja $g(x) \neq 0$ joukon $F[x]$ alkioita. Silloin lauseen 2.5 perusteella on olemassa sellaiset polynomit $q(x), r(x) \in F[x]$, että

$$f(x) = q(x)g(x) + r(x),$$

missä joko $r(x) = 0$ tai $\deg r(x) < \deg g(x)$. Koska $\deg f(x) = v(f(x))$, niin saadaan, että

$$f(x) = q(x)g(x) + r(x),$$

missä joko $r(x) = 0$ tai $v(r(x)) < v(g(x))$. Näin on saatu todistettua määritelmän 3.1 kohta (i).

Todistetaan sitten kohta (ii). Olkoot $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x] \setminus \{0\}$ ja $g(x) = b_0 + b_1x + \cdots + b_mx^m \in F[x] \setminus \{0\}$ sellaiset polynomit, että $a_n \neq 0$ ja $b_m \neq 0$. Silloin $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m}$. Oletuksen mukaan F on kunta ja kunnassa ei ole nollanjakajia, joten $a_nb_m \neq 0$. Tällöin $\deg(f(x)g(x)) = n + m$, jolloin saadaan, että $v(f(x)) = \deg f(x) = n \leq n + m = \deg(f(x)g(x)) = v(f(x)g(x))$. Näin on saatu todistettua määritelmän 3.1 kohta (ii).

Näin on saatu todistettua, että jos F on kunta, niin polynomirengas $F[x]$ on euklidinen alue.

Käydään seuraavaksi läpi kaksi esimerkkiä, jotka liittyvät olennaisesti määritelmään 3.1.

Esimerkki 3.2. ([5, s. 349, Harj. 1.(ii)]) Olkoon $(E, +, \cdot, v)$ euklidinen alue.

Osoitetaan ensin, että epäyhtälö $v(a) \geq v(1)$ on voimassa aina, kun $a \in E \setminus \{0\}$. Olkoon $a \in E \setminus \{0\}$. Silloin määritelmän 3.1 kohdan (ii) mukaan $v(1) \leq v(1 \cdot a)$, koska $1 \in E \setminus \{0\}$. Koska $v(1 \cdot a) = v(a)$, niin on saatu osoitettua, että epäyhtälö $v(a) \geq v(1)$ on voimassa aina, kun $a \in E \setminus \{0\}$.

Osoitetaan vielä, että epäyhtälössä $v(a) \geq v(1)$ on voimassa yhtäsuuruus, jos ja vain jos alkio $a \in E \setminus \{0\}$ on yksikkö renkaassa E. Oletetaan ensin, että

$a \in E \setminus \{0\}$ on yksikkö renkaassa E. Silloin yksikön määritelmän mukaan on olemassa sellainen alkio $c \in E$, että $ac = 1$. Tällöin $v(1) = v(ac)$ ja edelleen määritelmän 3.1 kohdan (ii) mukaan $v(ac) \geq v(a)$. Näin on saatu, että $v(1) \geq v(a)$. Koska edellä on osoitettu, että epäyhtälö $v(a) \geq v(1)$ on voimassa, niin nyt on saatu osoitettua, että $v(a) = v(1)$. Oletetaan nyt, että $v(a) = v(1)$. Koska oletusten mukaan $a \neq 0$ ja $(E, +, \cdot, v)$ on euklidinen alue, niin määritelmän 3.1 kohdan (i) mukaan on olemassa sellaiset alkiot $q, r \in E$, että $1 = qa + r$, missä joko $r = 0$ tai $v(r) < v(a) = v(1)$. Koska edellä on osoitettu, että epäyhtälö $v(a) \geq v(1)$ on voimassa, niin epäyhtälö $v(r) < v(1)$ ei voi olla voimassa. Näin ollen yhtälö $r = 0$ on voimassa, jolloin siis yhtälö $1 = qa$ on voimassa. Tällöin yksikön määritelmän mukaan alkio $a \in E \setminus \{0\}$ on yksikkö renkaassa E. Näin ollen on saatu todistettua, että $v(a) = v(1)$, jos ja vain jos alkio $a \in E \setminus \{0\}$ on yksikkö renkaassa E.

Esimerkki 3.3. ([5, s. 349, Harj. 1.(iii)]) Olkoon $(E, +, \cdot, v)$ euklidinen alue ja n sellainen kokonaisluku, että $v(1) + n \geq 0$. Osoitetaan, että funktio

$$v_n \colon (E \setminus \{0\}) \to (\mathbb{Z}^+ \cup \{0\}),$$

missä $v_n(a) = v(a) + n$ aina, kun $a \in E \setminus \{0\}$, on euklidinen valuaatio. Olkoon $a \in E \setminus \{0\}$. Silloin oletuksen ja esimerkin 3.2 perusteella $v_n(a) = v(a) + n \geq v(1) + n \geq 0$, joten $v_n(a) \in \mathbb{Z}^+ \cup \{0\}$. Oletetaan, että $a, b \in E$ ja $b \neq 0$. Koska $(E, +, \cdot, v)$ on euklidinen alue, niin määritelmän 3.1 kohdan (i) mukaan on olemassa sellaiset alkiot $q, r \in E$, että $a = qb + r$, missä joko $r = 0$ tai $v(r) < v(b)$. Jos $v(r) < v(b)$, niin silloin $v(r) + n < v(b) + n$, joten $v_n(r) < v_n(b)$. Oletetaan nyt, että $a, b \in E \setminus \{0\}$. Koska $(E, +, \cdot, v)$ on euklidinen alue, niin määritelmän 3.1 kohdan (ii) mukaan $v(a) \leq v(ab)$. Tällöin $v_n(a) = v(a) + n \leq v(ab) + n = v_n(ab)$. Näin on saatu osoitettua, että funktio v_n on euklidinen valuaatio.

Käydään vielä läpi muutama aihepiiriin liittyvä esimerkki.

Esimerkki 3.4. ([5, s. 349–350, Harj. 2]) Olkoon n ($n \neq 0, 1$) neliövapaa kokonaisluku eli luvulla n ei ole tekijänä mitään kokonaisluvun neliötä m^2, missä $m > 1$. Olkoon $\mathbb{Z}[\sqrt{n}] = \{\, a + b\sqrt{n} \mid a, b \in \mathbb{Z} \,\}$. Kolmikko $(\mathbb{Z}[\sqrt{n}], +, \cdot)$ on kokonaisalue lähdekirjan [5] sivun 275 perusteella. Määritellään funktio $N \colon \mathbb{Z}[\sqrt{n}] \to (\mathbb{Z}^+ \cup \{0\})$ seuraavasti:

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

Olkoot $x = a + b\sqrt{n}$ ja $y = c + d\sqrt{n}$ joukon $\mathbb{Z}[\sqrt{n}]$ alkioita. Tällöin

$$xy = (a + b\sqrt{n})(c + d\sqrt{n}) = (ac + nbd) + (ad + bc)\sqrt{n}.$$

Koska $a, b, c, d \in \mathbb{Z}$, niin selvästi $xy \in \mathbb{Z}[\sqrt{n}]$. Joukon $\mathbb{Z}[\sqrt{n}]$ määrittelyn mukaan $0 = 0 + 0\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$. Todistetaan nyt kaksi funktioon N liittyvää ominaisuutta kohdilla (i) ja (ii).

Kohta (i): Todistetaan, että $N(x) = 0$, jos ja vain jos $x = 0$. Olkoon $x = a + b\sqrt{n}$ joukon $\mathbb{Z}[\sqrt{n}]$ alkio. Silloin $N(x) = N(a + b\sqrt{n}) = a^2 - nb^2$. Todistetaan kohta kahdessa osassa. Oletetaan ensin, että $N(x) = 0$. Jos $b = 0$, niin silloin selvästi myös $a = 0$. Jos $b \neq 0$, niin silloin $nb^2 = a^2$ eli $n = \frac{a^2}{b^2} = (\frac{a}{b})^2$. Tämä on ristiriita, koska oletuksen mukaan n on neliövapaa kokonaisluku. Näin ollen $a = 0$ ja $b = 0$, joten $x = 0$. Oletetaan sitten, että $x = 0$. Silloin $N(x) = N(0 + 0\sqrt{n}) = 0$. Näin on saatu kohta (i) todistettua.

Kohta (ii): Todistetaan, että $N(xy) = N(x)N(y)$ aina, kun $x, y \in \mathbb{Z}[\sqrt{n}]$. Olkoot $x = a + b\sqrt{n}$ ja $y = c + d\sqrt{n}$ joukon $\mathbb{Z}[\sqrt{n}]$ alkioita. Tällöin

$$\begin{aligned} N(xy) &= N((ac + nbd) + (ad + bc)\sqrt{n}) \\ &= [(ac + nbd) + (ad + bc)\sqrt{n}][(ac + nbd) - (ad + bc)\sqrt{n}] \\ &= (ac + nbd)^2 - (ad + bc)^2 n \\ &= a^2c^2 + n^2b^2d^2 - a^2d^2n - b^2c^2n \\ &= (a^2 - nb^2)(c^2 - nd^2) \\ &= N(x)N(y). \end{aligned}$$

Näin on saatu kohta (ii) todistettua.

Esimerkki 3.5. ([5, s. 350, Harj. 3]) Osoitetaan, että $(\mathbb{Z}[\sqrt{n}], +, \cdot, v)$ on euklidinen alue, kun $n = -2, -1, 2, 3$. Esimerkin 3.4 mukaan $(\mathbb{Z}[\sqrt{n}], +, \cdot)$ on kokonaisalue. Määritellään funktio $v\colon (\mathbb{Z}[\sqrt{n}]\setminus\{0\}) \to (\mathbb{Z}^+ \cup \{0\})$ seuraavasti:

$$v(a + b\sqrt{n}) = |N(a + b\sqrt{n})|,$$

missä funktio N on määritelty kuten esimerkissä 3.4.

Osoitetaan ensin, että määritelmän 3.1 kohta (ii) on voimassa. Olkoot $a + b\sqrt{n}, c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}] \setminus \{0\}$. Tällöin funktion v määrittelyn ja esimerkin 3.4 kohdan (ii) perusteella

$$\begin{aligned} v((a + b\sqrt{n})(c + d\sqrt{n})) &= |N((a + b\sqrt{n})(c + d\sqrt{n}))| \\ &= |(a^2 - nb^2)(c^2 - nd^2)| \\ &\geq |(a^2 - nb^2)| \\ &= |N(a + b\sqrt{n})| \\ &= v(a + b\sqrt{n}). \end{aligned}$$

Näin on saatu osoitettua, että määritelmän 3.1 kohta (ii) on voimassa.

Osoitetaan vielä, että määritelmän 3.1 kohta (i) on voimassa. Olkoot nyt $a + b\sqrt{n}, c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, missä $c + d\sqrt{n} \neq 0$. Seuraavaksi on tarkoituksena osoittaa, että on olemassa sellaiset alkiot $q_0 + q_1\sqrt{n}, r_0 + r_1\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, että

$$a + b\sqrt{n} = (c + d\sqrt{n})(q_0 + q_1\sqrt{n}) + (r_0 + r_1\sqrt{n}),$$

missä joko $r_0 + r_1\sqrt{n} = 0$ tai $v(r_0 + r_1\sqrt{n}) < v(c + d\sqrt{n})$. Tutkitaan nyt, miten alkio $q_0 + q_1\sqrt{n}$ on valittava, jos se on olemassa. Jos alkio $q_0 + q_1\sqrt{n}$ on olemassa, niin silloin joukossa $\mathbb{Q}[\sqrt{n}]$ on voimassa yhtälö

$$\begin{aligned} r_0 + r_1\sqrt{n} &= (a + b\sqrt{n}) - (c + d\sqrt{n})(q_0 + q_1\sqrt{n}) \\ &= (c + d\sqrt{n})[(a + b\sqrt{n})(c + d\sqrt{n})^{-1} - (q_0 + q_1\sqrt{n})]. \end{aligned}$$

Olkoon $(a+b\sqrt{n})(c+d\sqrt{n})^{-1} = u+v\sqrt{n}$, missä u ja v ovat rationaalilukuja. Silloin

$$\begin{aligned} r_0 + r_1\sqrt{n} &= (c + d\sqrt{n})[(u + v\sqrt{n}) - (q_0 + q_1\sqrt{n})] \\ &= (c + d\sqrt{n})[(u - q_0) + (v - q_1)\sqrt{n}] \\ &= [c(u - q_0) + d(v - q_1)n] + [c(v - q_1) + d(u - q_0)]\sqrt{n}. \end{aligned}$$

Tällöin

$$\begin{aligned} v(r_0 + r_1\sqrt{n}) &= |[c(u - q_0) + d(v - q_1)n]^2 - [c(v - q_1) + d(u - q_0)]^2 n| \\ &= |(c^2 - nd^2)[(u - q_0)^2 - n(v - q_1)^2]| \\ &= |(c^2 - nd^2)||(u - q_0)^2 - n(v - q_1)^2| \\ &< |(c^2 - nd^2)| \\ &= v(c + d\sqrt{n}), \end{aligned}$$

jos $|(u-q_0)^2-n(v-q_1)^2| < 1$. Nyt löydetään sellainen alkio $q_0+q_1\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, että $|(u-q_0)^2-n(v-q_1)^2| < 1$. Valitaan sellaiset kokonaisluvut q_0 ja q_1, että $(u-q_0)^2 \leq \frac{1}{4}$ ja $(v-q_1)^2 \leq \frac{1}{4}$. Kun $n = -2, -1$, niin silloin

$$|(u - q_0)^2 - n(v - q_1)^2| \leq \frac{1}{4} + (-n)\frac{1}{4} < 1.$$

Kun $n = 2, 3$, niin silloin

$$-\frac{n}{4} \leq (u - q_0)^2 - n(v - q_1)^2 \leq \frac{1}{4}.$$

Näin ollen $|(u - q_0)^2 - n(v - q_1)^2| < 1$, kun $n = -2, -1, 2, 3$. Näin on saatu, että on olemassa sellaiset alkiot $q_0 + q_1\sqrt{n}, r_0 + r_1\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, että

$$a + b\sqrt{n} = (c + d\sqrt{n})(q_0 + q_1\sqrt{n}) + (r_0 + r_1\sqrt{n}),$$

missä joko $r_0 + r_1\sqrt{n} = 0$ tai $v(r_0 + r_1\sqrt{n}) < v(c + d\sqrt{n})$. Näin on saatu osoitettua, että määritelmän 3.1 kohta (i) on voimassa.

Näin ollen tehtävän osoitus on saatu valmiiksi.

3.2 Gaussin kokonaisluvut

Tässä alaluvussa käydään läpi Gaussin kokonaislukujen joukon määritelmä (vrt. [5, s. 346]) ja esitetään kaksi aiheeseen liittyvää lausetta, jotka myös todistetaan. Lisäksi käydään läpi aiheeseen liittyviä esimerkkejä.

Määritelmä 3.2. Kompleksilukujen osajoukkoa $\mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \}$ sanotaan *Gaussin kokonaislukujen* (engl. Gaussian integers) joukoksi.

Seuraavassa lauseessa todistetaan, että kolmikko $(\mathbb{Z}[i], +, \cdot)$, missä laskutoimitukset $+$ ja $\cdot$ ovat perinteiset kompleksilukujen yhteen- ja kertolasku, on renkaan $\mathbb{C}$ alirengas.

Lause 3.2. *Kolmikko* $(\mathbb{Z}[i], +, \cdot)$ *on renkaan* $\mathbb{C}$ *alirengas.*

Todistus (vrt. [6, s. 196, Esim. 6.1.15]). Määritelmän 3.2 nojalla $\mathbb{Z}[i] \neq \emptyset$ ja $\mathbb{Z}[i] \subseteq \mathbb{C}$, joten alirengaskriteeriä voidaan käyttää. Valitaan mielivaltaisesti sellaiset luvut $x, y \in \mathbb{Z}[i]$, että $x = a + bi$ ja $y = c + di$, missä $a, b, c, d \in \mathbb{Z}$. Silloin

$$x - y = (a + bi) - (c + di) = a + bi - c - di = (a - c) + (b - d)i$$

ja

$$xy = (a + bi)(c + di) = ac + adi + bci - bd = (ac - bd) + (ad + bc)i.$$

Koska $a - c, b - d, ac - bd, ad - bc \in \mathbb{Z}$, niin $x - y \in \mathbb{Z}[i]$ ja $xy \in \mathbb{Z}[i]$. Tällöin alirengaskriteerin perusteella kolmikko $(\mathbb{Z}[i], +, \cdot)$ on renkaan $\mathbb{C}$ alirengas ja lause on näin todistettu.

Huomautus. Lauseen 3.2 ja määritelmän 1.1 perusteella kolmikko $(\mathbb{Z}[i], +, \cdot)$ on itsessään rengas. Merkitään tämän vuoksi jatkossa kolmikkoa $(\mathbb{Z}[i], +, \cdot)$ renkaana $\mathbb{Z}[i]$.

Saksalainen matemaatikko Carl Friedrich Gauss (1777-1855) oli ensimmäinen, joka tutki määritelmässä 3.2 määriteltyä joukkoa $\mathbb{Z}[i]$ ja siksi hänen kunniakseen rengasta $\mathbb{Z}[i]$ sanotaan *Gaussin kokonaislukujen renkaaksi* (engl. the ring of Gaussian integers). (Ks. [5, s. 56].)

Seuraavassa esimerkissä etsitään Gaussin kokonaislukujen renkaan kaikki yksiköt.

Esimerkki 3.6. ([5, s. 346, Lause 15.1.6]) Etsitään renkaan $\mathbb{Z}[i]$ kaikki yksiköt. Koska $\mathbb{C}$ on kunta, niin se on myös kokonaisalue. Koska lauseen 3.2 perusteella $\mathbb{Z}[i]$ on renkaan $\mathbb{C}$ alirengas ja selvästi määritelmän 3.2 mukaan $1 \in \mathbb{Z}[i]$, niin tällöin lauseen 1.2 ja määritelmän 1.2 perusteella $\mathbb{Z}[i]$ on kokonaisalue (ks. [6, s. 201, Esim. 6.2.12]). Oletetaan, että alkio $a + bi \in \mathbb{Z}[i]$ on renkaan $\mathbb{Z}[i]$ yksikkö. Tällöin yksikön määritelmän mukaan on olemassa sellainen alkio $c + di \in \mathbb{Z}[i]$, että $(a + bi)(c + di) = 1$. Nyt kompleksilukujen ominaisuuksien ja laskusääntöjen nojalla saadaan, että $1 = \overline{1} =$

$\overline{(a+bi)(c+di)} = \overline{(a+bi)}\ \overline{(c+di)} = (a-bi)(c-di)$, missä viiva luvun yläpuolella tarkoittaa kompleksikonjugaattia. Näin on saatu, että $1 = 1 \cdot 1 = (a+bi)(c+di)(a-bi)(c-di) = ((a+bi)(a-bi))((c+di)(c-di)) = (a^2+b^2)(c^2+d^2)$ ja tämän perusteella $a^2 + b^2 = 1$, koska $a, b, c, d \in \mathbb{Z}$. Näin ollen $a = \pm 1$ ja $b = 0$ tai $a = 0$ ja $b = \pm 1$, joten joukon $\mathbb{Z}[i]$ alkiot $1, -1, i$ ja $-i$ ovat renkaan $\mathbb{Z}[i]$ yksiköt.

Seuraavassa esimerkissä etsitään tietyn kokonaisalueen kaikki yksiköt.

Esimerkki 3.7. ([5, s. 359, Harj. 2]) Olkoon $\mathbb{Z}[i\sqrt{3}] = \{\, a+bi\sqrt{3} \mid a, b \in \mathbb{Z} \,\}$. Etsitään kokonaisalueen $\mathbb{Z}[i\sqrt{3}]$ kaikki yksiköt. Olkoon $a + bi\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$ ja oletetaan, että se on yksikkö kokonaisalueessa $\mathbb{Z}[i\sqrt{3}]$. Tällöin yksikön määritelmän mukaan on olemassa sellainen alkio $c + di\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$, että $(a + bi\sqrt{3})(c + di\sqrt{3}) = 1$. Näin ollen kompleksilukujen laskusääntöjen ja ominaisuuksien nojalla $1 = \overline{1} = \overline{(a + bi\sqrt{3})(c + di\sqrt{3})} = \overline{(a + bi\sqrt{3})}\ \overline{(c + di\sqrt{3})} = (a-bi\sqrt{3})(c-di\sqrt{3})$. Näin on saatu, että $1 = 1 \cdot 1 = (a+bi\sqrt{3})(c+di\sqrt{3})(a-bi\sqrt{3})(c-di\sqrt{3}) = (a^2+3b^2)(c^2+3d^2)$. Tämän perusteella $a^2+3b^2 = 1$, koska $a, b, c, d \in \mathbb{Z}$. Näin ollen $a = \pm 1$ ja $b = 0$, joten joukon $\mathbb{Z}[i\sqrt{3}]$ alkiot 1 ja -1 ovat kokonaisalueen $\mathbb{Z}[i\sqrt{3}]$ kaikki yksiköt.

Seuraava lause osoittaa, että Gaussin kokonaislukujen rengas on euklidinen alue.

Lause 3.3. *Gaussin kokonaislukujen rengas $\mathbb{Z}[i]$ ja funktio $N\colon (\mathbb{Z}[i] \setminus \{0\}) \to (\mathbb{Z}^+ \cup \{0\})$, missä $N(a+bi) = (a+bi)(a-bi) = a^2 + b^2$ aina, kun $a, b \in \mathbb{Z}$, muodostavat euklidisen alueen.*

Todistus (vrt. [5, s. 347]). Todistetaan erikseen, että määritelmän 3.1 kohdat (i) ja (ii) ovat voimassa. Esimerkin 3.6 mukaan Gaussin kokonaislukujen rengas $\mathbb{Z}[i]$ on kokonaisalue.

Todistetaan ensin, että kohta (ii) on voimassa. Jos alkio $a+bi \in \mathbb{Z}[i] \setminus \{0\}$, niin $N(a+bi)$ on positiivinen kokonaisluku, koska $a, b \in \mathbb{Z}$ ja $N(a+bi) = a^2 + b^2$. Olkoot $a+bi, c+di \in \mathbb{Z}[i] \setminus \{0\}$. Tällöin kompleksilukujen laskusääntöjen ja funktion N määrittelyn perusteella

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

Näin ollen saadaan, että

$$N(a+bi) \leq N(a+bi)N(c+di) = N((a+bi)(c+di)),$$

koska $N(c+di) \geq 1$. Näin on saatu todistettua, että määritelmän 3.1 kohta (ii) on voimassa.

Todistetaan vielä, että kohta (i) on voimassa. Olkoot $a+bi, c+di \in \mathbb{Z}[i]$, missä $c+di \neq 0$. Todistetaan nyt, että tällöin on olemassa sellaiset alkiot $q_0+q_1i, r_0+r_1i \in \mathbb{Z}[i]$, että

$$a+bi = (q_0+q_1i)(c+di) + (r_0+r_1i),$$

missä joko $r_0+r_1i = 0$ tai $N(r_0+r_1i) < N(c+di)$. Tutkitaan seuraavaksi, miten alkio q_0+q_1i on valittava, jos se on olemassa. Jos alkio q_0+q_1i on olemassa, niin silloin joukossa $\mathbb{C}$ on voimassa yhtälö

$$\begin{aligned} r_0+r_1i &= (a+bi) - (c+di)(q_0+q_1i) \\ &= (c+di)[(a+bi)(c+di)^{-1} - (q_0+q_1i)]. \end{aligned}$$

Olkoon $(a+bi)(c+di)^{-1} = u+vi$, missä u ja v ovat rationaalilukuja. Silloin

$$\begin{aligned} r_0+r_1i &= (c+di)[(u+vi) - (q_0+q_1i)] \\ &= (c+di)[(u-q_0) + (v-q_1)i] \\ &= (cu - cq_0 - dv + dq_1) + (ud - q_0d + cv - cq_1)i \\ &= [c(u-q_0) - d(v-q_1)] + [c(v-q_1) + d(u-q_0)]i. \end{aligned}$$

Tällöin

$$\begin{aligned} N(r_0+r_1i) &= [c(u-q_0) - d(v-q_1)]^2 + [c(v-q_1) + d(u-q_0)]^2 \\ &= (c^2+d^2)[(u-q_0)^2 + (v-q_1)^2]. \end{aligned}$$

Jos nyt $(u-q_0)^2 + (v-q_1)^2 < 1$, niin $N(r_0+r_1i) < N(c+di)$. Nyt löydetään sellainen alkio $q_0+q_1i \in \mathbb{Z}[i]$, että viimeksi mainittu epäyhtälö on voimassa. Valitaan sellaiset kokonaisluvut q_0 ja q_1, että $(u-q_0)^2 \leq \frac{1}{4}$ ja $(v-q_1)^2 \leq \frac{1}{4}$, jolloin $(u-q_0)^2+(v-q_1)^2 < 1$. Olkoon nyt $r_0+r_1i = (a+bi)-(c+di)(q_0+q_1i)$. Tällöin $a+bi = (c+di)(q_0+q_1i) + (r_0+r_1i)$, missä joko $r_0+r_1i = 0$ tai $N(r_0+r_1i) < N(c+di)$, kuten edellä on saatu. Näin on saatu todistettua, että määritelmän 3.1 kohta (i) on voimassa.

Näin ollen kaikkiaan on saatu todistettua, että rengas $\mathbb{Z}[i]$ ja lauseessa 3.3 määritelty funktio N muodostavat euklidisen alueen.

Käydään seuraavaksi läpi muutama määritelmään 3.1 ja lauseeseen 3.3 liittyvä esimerkki.

Esimerkki 3.8. ([6, s. 284, Harj. 4]) Olkoon $(\mathbb{Z}[i], +, \cdot, N)$ euklidinen alue, missä funktio N on määritelty kuten lauseessa 3.3. Olkoot $a = 5+3i$ ja $b = 2+i$ joukon $\mathbb{Z}[i]$ alkioita. Etsitään sellaiset alkiot $q, r \in \mathbb{Z}[i]$, että $a = qb+r$, missä joko $r = 0$ tai $N(r) < N(b)$. Jakamalla alkio a jakokulmassa alkiolla b saadaan, että osamäärä $q = 2$ ja jakojäännös $r = 1+i$. Tällöin selvästi $q, r \in \mathbb{Z}[i]$ ja $qb+r = 2(2+i)+(1+i) = 4+2i+1+i = 5+3i = a$. Lisäksi $N(r) = N(1+i) = 2$ ja $N(b) = N(2+i) = 5$, joten $N(r) < N(b)$. Näin on löydetty sopivat alkiot $q, r \in \mathbb{Z}[i]$.

Esimerkki 3.9. ([6, s. 284, Harj. 5]) Olkoon $(\mathbb{Z}[i], +, \cdot, N)$ euklidinen alue, missä funktio N on määritelty kuten lauseessa 3.3. Olkoot $a = 3 + 4i$ ja $b = 4 - 3i$ joukon $\mathbb{Z}[i]$ alkioita. Etsitään sellaiset alkiot $q, r \in \mathbb{Z}[i]$, että $a = qb + r$, missä joko $r = 0$ tai $N(r) < N(b)$. Huomaamalla alkioiden a ja b samankaltaisuus saadaan helposti, että $q = i$ ja $r = 0$. Tällöin $q, r \in \mathbb{Z}[i]$, $qb + r = i(4 - 3i) + 0 = 4i - 3i^2 = 3 + 4i = a$ ja $r = 0$. Näin on siis löydetty sopivat alkiot $q, r \in \mathbb{Z}[i]$.

3.3 Euklidisen alueen ihanteista

Tässä alaluvussa käsitellään euklidisen alueen ihanteita. Aluksi käydään läpi kaksi määritelmää (vrt. [5, s. 347]) ja sen jälkeen esitetään kaksi lausetta todistuksineen. Lisäksi käsitellään toiseen lauseeseen liittyvä seurauslause.

Palautetaan tässä kohtaa mieleen, että kommutatiivisen ykkösrenkaan R ihannetta I sanotaan pääihanteeksi, jos $I = \langle a \rangle$ jollakin alkiolla $a \in R$ (vrt. määritelmä 1.8 ja [2, s. 358]).

Määritelmä 3.3. Olkoon R kommutatiivinen ykkösrengas. Jos renkaan R jokainen ihanne on pääihanne, niin silloin rengasta R sanotaan *pääihannerenkaaksi* (engl. principal ideal ring).

Määritelmä 3.4. Olkoon D kokonaisalue. Jos kokonaisalue D on pääihannerengas, niin silloin kokonaisaluetta D sanotaan *pääihannealueeksi* (engl. principal ideal domain).

Lause 3.4. *Jokainen euklidinen alue on pääihannealue.*

Todistus (vrt. [5, s. 348] ja [6, s. 281]). Olkoon E kokonaisalue ja funktio v euklidinen valuaatio, jotka muodostavat euklidisen alueen. Tehtävänä on todistaa, että kokonaisalueen E jokainen ihanne on pääihanne. Olkoon I kokonaisalueen E mielivaltainen ihanne. Jos $I = \{0\}$, niin silloin $I = \langle 0 \rangle$ ja $0 \in E$, joten pääihanteen määritelmän mukaan ihanne I on tällöin pääihanne. Oletetaan nyt, että $I \neq \{0\}$. Olkoon $0 \neq a \in E$ sellainen ihanteen I alkio, että $v(a) \leq v(x)$ aina, kun $0 \neq x \in I$. Todistetaan nyt kahdessa osassa, että $I = \langle a \rangle$ eli että I on pääihanne.

Oletetaan ensin, että $b \in I$. Tällöin määritelmän 3.1 kohdan (i) mukaan on olemassa sellaiset alkiot $q, r \in E$, että $b = qa + r$, missä joko $r = 0$ tai $v(r) < v(a)$. Näin ollen $r = b - qa$, missä $a, b \in I$ ja $q \in E$. Koska I on oletuksen mukaan kokonaisalueen E ihanne, niin tällöin ihanteen määritelmän mukaan $qa \in I$. Näin on saatu, että ihannekriteerin perusteella $r = b - qa \in I$, koska $b \in I$ ja $qa \in I$. Epäyhtälö $v(r) < v(a)$ ei voi olla voimassa alkion a valinnan vuoksi, koska valinnan mukaan $v(a) \leq v(r)$, kun $0 \neq r \in I$. Näin ollen yhtälö $r = 0$ on voimassa, jolloin $b = qa$. Koska E on kokonaisalueena myös kommutatiivinen ykkösrengas ja $q \in E$, niin lauseen 1.8 seurauslauseen perusteella $b = qa \in \langle a \rangle$. Näin on saatu, että $b \in \langle a \rangle$ aina, kun $b \in I$, joten $I \subseteq \langle a \rangle$.

Oletetaan nyt, että $b \in \langle a \rangle$. Koska E on kokonaisalueena myös kommutatiivinen ykkösrengas, niin tällöin lauseen 1.8 seurauslauseen perusteella $b = qa$, missä $q \in E$ ja $a \in I$. Koska I on kokonaisalueen E ihanne, niin ihanteen määritelmän mukaan $qa = b \in I$. Näin on saatu, että $b \in I$ aina, kun $b \in \langle a \rangle$, joten $\langle a \rangle \subseteq I$.

Näin ollen on saatu todistettua, että $I = \langle a \rangle$ eli että ihanne I on pääihanne. Kaiken kaikkiaan on saatu todistettua, että euklidisen alueen jokainen ihanne on pääihanne. Näin ollen yllä olevan todistuksen ja määritelmän 3.4 mukaan jokainen euklidinen alue on pääihannealue, joten lause on saatu todistettua.

Lauseen 3.4 ja edellä olevien esimerkkien sekä lauseiden perusteella nähdään, että rengas $\mathbb{Z}$, polynomirengas $F[x]$, missä F on kunta, ja Gaussin kokonaislukujen rengas $\mathbb{Z}[i]$ ovat pääihannealueita.

Jos tehtävänä on tutkia, onko jokin kokonaisalue euklidinen alue vai eikö ole, niin usein on helpointa tutkia, onko kyseinen kokonaisalue pääihannealue vai eikö ole. Jos tutkittava kokonaisalue ei ole pääihannealue, niin silloin lauseen 3.4 perusteella kyseinen kokonaisalue ei ole euklidinen alue. (Vrt. [6, s. 281].) Jos tutkittava kokonaisalue on pääihannealue, niin silloin ei voida sanoa mitään, koska jokainen pääihannealue ei ole euklidinen alue. (Vrt. [2, s. 377].)

Lause 3.5. *Olkoon R kommutatiivinen ykkösrengas. Silloin seuraavat ehdot ovat yhtäpitäviä.*

(i) *R on kunta.*

(ii) *Polynomirengas $R[x]$ on euklidinen alue.*

(iii) *Polynomirengas $R[x]$ on pääihannealue.*

Todistus (vrt. [5, s. 348]). Todistetaan lause kolmessa eri osassa. Todistetaan ensin, että (i)⇒(ii). Oletetaan, että R on kunta. Silloin lauseen 3.1 perusteella polynomirengas $R[x]$ on euklidinen alue. Näin ollen on saatu todistettua, että kohdasta (i) seuraa kohta (ii).

Todistetaan sitten, että (ii)⇒(iii). Oletetaan, että polynomirengas $R[x]$ on euklidinen alue. Silloin lauseen 3.4 perusteella polynomirengas $R[x]$ on pääihannealue. Näin ollen on saatu todistettua, että kohdasta (ii) seuraa kohta (iii).

Todistetaan vielä, että (iii)⇒(i). Oletetaan, että polynomirengas $R[x]$ on pääihannealue. Olkoon $a \in R$ ja $a \neq 0$. Olkoon $I = \langle a, x \rangle$ polynomirenkaan $R[x]$ ihanne, joka on alkioiden a ja x virittämä. Koska polynomirengas $R[x]$ on oletuksen mukaan pääihannealue, niin polynomirenkaan $R[x]$ jokainen ihanne on pääihanne. Näin ollen pääihanteen määritelmän mukaan on olemassa sellainen alkio $f(x) \in R[x]$, että $I = \langle f(x) \rangle$. Tällöin $a, x \in \langle f(x) \rangle$. Siis on olemassa sellaiset alkiot $g(x), h(x) \in R[x]$, että $f(x)g(x) = a$ ja $f(x)h(x) = x$.

Tällöin $\deg(f(x)g(x)) = \deg(a) = 0$ ja toisaalta lauseen 2.3 kohtaan (i) liittyvän huomautuksen perusteella $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$, missä $\deg f(x), \deg g(x) \geq 0$ (kyseinen huomautus on voimassa, koska $R[x]$ on pääihannealueena myös kokonaisalue). Näin ollen $\deg f(x) = 0$, joten $0 \neq f(x) \in R$ eli $f(x)$ on vakiopolynomi määritelmän 2.6 mukaan. Merkitään $f(x) = b$. Tällöin $bh(x) = x$, jonka perusteella $bc = 1$ jollakin alkiolla $c \in R$. Siis alkio $b \in R$ on yksikkö ja $I = \langle b \rangle = R[x]$. Näin ollen $1 \in I$ ja silloin oletuksen $I = \langle a, x \rangle = \{\, af_1(x) + xf_2(x) \mid f_1(x), f_2(x) \in R[x] \,\}$ mukaan $1 = af_1(x) + xf_2(x)$ joillakin polynomeilla $f_1(x), f_2(x) \in R[x]$. Olkoot $f_1(x) = d_0 + d_1x + \cdots + d_nx^n \in R[x]$ ja $f_2(x) = e_0 + e_1x + \cdots + e_{n-1}x^{n-1} \in R[x]$. Tällöin $af_1(x) + xf_2(x) = ad_0 + ad_1x + \cdots + ad_nx^n + e_0x + e_1x^2 + \cdots + e_{n-1}x^n$. Toisaalta edellä on saatu, että $af_1(x) + xf_2(x) = 1$. Näin ollen $ad_0 = 1$ jollakin alkiolla $d_0 \in R$, joten alkio $a \in R$ on yksikkö. Näin on saatu todistettua, että joukon R jokaisella nollasta eroavalla alkiolla on käänteisalkio. Lisäksi lauseen 3.5 oletuksen mukaan R on kommutatiivinen ykkösrengas. Tällöin kunnan määritelmän mukaan R on kunta. Näin ollen on saatu todistettua, että kohdasta (iii) seuraa kohta (i).

Kaiken kaikkiaan on saatu todistettua, että lauseen 3.5 ehdot ovat yhtäpitäviä. Näin ollen lause on saatu todistettua.

Seuraus. Polynomirengas $\mathbb{Z}[x]$ ei ole pääihannealue.

Todistus (vrt. [5, s. 348]). Selvästi $\mathbb{Z}$ on kommutatiivinen ykkösrengas. Tällöin lauseen 3.5 oletukset ovat voimassa, joten sitä voidaan käyttää apuna. Koska $\mathbb{Z}$ ei ole kunta, niin lauseen 3.5 perusteella polynomirengas $\mathbb{Z}[x]$ ei ole pääihannealue. Näin seurauslause on saatu todistettua.

3.4 Jaollisuus ja liittoalkiot

Tässä alaluvussa käydään läpi yksi kommutatiivisen renkaan alkioiden jaollisuuteen liittyvä määritelmä (vrt. [5, s. 353]) ja esitetään yksi jaollisuuteen liittyvä lause todistettuna. Tämän jälkeen käydään läpi liittoalkion määritelmä (vrt. [5, s. 353]). Lisäksi käydään läpi havainnollistavia esimerkkejä. Alaluvun lopussa esitetään kaksi liittoalkioiden ominaisuuksia käsittelevää lausetta todistuksineen.

Määritelmä 3.5. Olkoon R kommutatiivinen rengas. Olkoot a, b joukon R sellaisia alkioita, että $a \neq 0$. Jos on olemassa sellainen alkio $c \in R$, että $b = ac$, niin silloin sanotaan, että alkio a *jakaa* (engl. divides) alkion b tai että alkio a on alkion b *tekijä* (engl. factor).

Merkintä. Jos alkio a jakaa alkion b eli jos alkio a on alkion b tekijä, niin silloin merkitään $a \mid b$. Merkintä $a \nmid b$ tarkoittaa, että alkio a ei jaa alkiota b eli että alkio a ei ole alkion b tekijä.

Lause 3.6. *Olkoon R kommutatiivinen ykkösrengas. Silloin seuraavat ominaisuudet ovat voimassa aina, kun $a, b, c \in R$.*

(i) $a \mid a$, $1 \mid a$ *ja* $a \mid 0$.

(ii) *Alkio a on renkaan R yksikkö, jos ja vain jos* $a \mid 1$.

(iii) *Jos* $a \mid b$ *ja* $b \mid c$, *niin* $a \mid c$.

Todistus. Todistetaan erikseen lauseen kohdat (i)–(iii).

Todistetaan ensin lauseen kohta (i). Kommutatiivisessa ykkösrenkaassa on ykkösalkio, joten $1 \in R$. Koska $a = a \cdot 1$, niin määritelmän 3.5 mukaan $a \mid a$. Oletuksen mukaan $a \in R$. Koska $a = 1 \cdot a$, niin määritelmän 3.5 mukaan $1 \mid a$. Kommutatiivisessa ykkösrenkaassa on myös nolla-alkio, joten $0 \in R$. Koska $0 = a \cdot 0$, niin määritelmän 3.5 mukaan $a \mid 0$. Näin on saatu todistettua lauseen kohta (i).

Todistetaan seuraavaksi lauseen kohta (ii). Oletetaan ensin, että alkio a on renkaan R yksikkö. Tällöin yksikön määritelmän mukaan on olemassa sellainen alkio $b \in R$, että $1 = ab$. Näin ollen määritelmän 3.5 mukaan $a \mid 1$. Oletetaan sitten, että $a \mid 1$. Tällöin määritelmän 3.5 mukaan on olemassa sellainen alkio $c \in R$, että $1 = ac$. Näin ollen yksikön määritelmän mukaan alkio a on renkaan R yksikkö. Näin on saatu todistettua lauseen kohta (ii).

Todistetaan vielä lauseen kohta (iii). Oletetaan, että $a \mid b$ ja $b \mid c$. Tällöin määritelmän 3.5 mukaan on olemassa sellaiset alkiot $d, e \in R$, että $b = ad$ ja $c = be$. Näin ollen saadaan, että $c = be = (ad)e = a(de)$, jolloin määritelmän 3.5 mukaan $a \mid c$. Näin on saatu todistettua lauseen kohta (iii).

Näin on saatu lause 3.6 todistettua.

Määritelmä 3.6. Olkoon R kommutatiivinen ykkösrengas. Nollasta eroavaa alkiota $a \in R$ sanotaan nollasta eroavan alkion $b \in R$ *liittoalkioksi* (engl. associate), jos $a = bu$ jollakin renkaan R yksiköllä u.

Käydään seuraavaksi läpi määritelmää 3.6 havainnollistava esimerkki.

Esimerkki 3.10. ([5, s. 353, Esim. 15.2.3]) Selvästi renkaan $\mathbb{Z}$ ainoat yksiköt ovat 1 ja -1. Näin ollen määritelmän 3.6 mukaan alkion $0 \neq a \in \mathbb{Z}$ liittoalkiot ovat a ja $-a$, koska $a \cdot 1 = a$ ja $a \cdot (-1) = -a$.

Esimerkin 3.6 mukaan renkaan $\mathbb{Z}[i]$ kaikki yksiköt ovat $1, -1, i$ ja $-i$. Näin ollen määritelmän 3.6 mukaan alkion $1 + i \in \mathbb{Z}[i]$ liittoalkiot ovat $1 + i, -1 - i, -1 + i$ ja $1 - i$, koska $(1 + i) \cdot 1 = 1 + i, (1 + i) \cdot (-1) = -1 - i, (1 + i) \cdot i = i - 1 = -1 + i$ ja $(1 + i) \cdot (-i) = -i + 1 = 1 - i$.

Käydään vielä lisäksi läpi kaksi esimerkkiä, jotka havainnollistavat hyvin määritelmää 3.6 sekä annetun alkion liittoalkioiden konkreettista laskemista.

Esimerkki 3.11. ([5, s. 359, Harj. 1.(i)]) Etsitään alkion $3 - 2i \in \mathbb{Z}[i]$ kaikki liittoalkiot. Esimerkin 3.6 mukaan renkaan $\mathbb{Z}[i]$ kaikki yksiköt ovat $1, -1, i$ ja

$-i$. Tällöin $(3-2i)\cdot 1 = 3-2i$, $(3-2i)\cdot(-1) = -3+2i$, $(3-2i)\cdot i = 2+3i$ ja $(3-2i)\cdot(-i) = -2-3i$. Näin ollen määritelmän 3.6 mukaan alkion $3-2i$ kaikki liittoalkiot renkaassa $\mathbb{Z}[i]$ ovat $3-2i$, $-3+2i$, $2+3i$ ja $-2-3i$.

Esimerkki 3.12. ([5, s. 359, Harj. 1.(iii)]) Etsitään alkion $\overline{6} \in \mathbb{Z}_{10}$ kaikki liittoalkiot. Etsitään ensin renkaan $\mathbb{Z}_{10}$ kaikki yksiköt. Laskemalla nähdään helposti, että $\overline{1}\cdot\overline{1} = \overline{1}$, $\overline{3}\cdot\overline{7} = \overline{21} = \overline{1}$ ja $\overline{9}\cdot\overline{9} = \overline{81} = \overline{1}$. Näin ollen yksikön määritelmän mukaan joukon $\mathbb{Z}_{10}$ alkiot $\overline{1}, \overline{3}, \overline{7}$ ja $\overline{9}$ ovat renkaan $\mathbb{Z}_{10}$ kaikki yksiköt. Tällöin $\overline{6}\cdot\overline{1} = \overline{6}$, $\overline{6}\cdot\overline{3} = \overline{18} = \overline{8}$, $\overline{6}\cdot\overline{7} = \overline{42} = \overline{2}$ ja $\overline{6}\cdot\overline{9} = \overline{54} = \overline{4}$. Näin ollen määritelmän 3.6 mukaan alkion $\overline{6}$ kaikki liittoalkiot renkaassa $\mathbb{Z}_{10}$ ovat $\overline{2}, \overline{4}, \overline{6}$ ja $\overline{8}$.

Käydään vielä seuraavaksi läpi kaksi esimerkkiä, jotka liittyvät määritelmiin 3.1, 3.5 ja 3.6.

Esimerkki 3.13. ([5, s. 359, Harj. 7]) Olkoon $(E, +, \cdot, v)$ euklidinen alue. Olkoot joukon E alkiot a ja b sellaisia, että ne ovat toistensa liittoalkiot. Todistetaan, että silloin $v(a) = v(b)$.

Koska oletuksen mukaan alkio a on alkion b liittoalkio, niin määritelmän 3.6 mukaan $a = bu$ jollakin yksiköllä $u \in E$. Tällöin määritelmän 3.1 kohdan (ii) perusteella saadaan, että $v(b) \leq v(bu) = v(a)$. Koska oletuksen mukaan alkio b on alkion a liittoalkio, niin määritelmän 3.6 mukaan $b = at$ jollakin yksiköllä $t \in E$. Tällöin määritelmän 3.1 kohdan (ii) perusteella saadaan, että $v(a) \leq v(at) = v(b)$.

Näin on saatu, että $v(b) \leq v(a)$ ja $v(a) \leq v(b)$, joten selvästi $v(a) = v(b)$. Näin on saatu todistus valmiiksi.

Esimerkki 3.14. ([5, s. 359, Harj. 8]) Olkoon $(E, +, \cdot, v)$ euklidinen alue ja olkoot $a, b \in E$. Todistetaan, että jos $a \mid b$ ja $v(a) = v(b)$, niin silloin alkiot a ja b ovat toistensa liittoalkiot.

Oletetaan siis, että $a \mid b$ ja $v(a) = v(b)$. Määritelmän 3.1 kohdan (i) perusteella on olemassa sellaiset alkiot $q, r \in E$, että

$$a = qb + r, \tag{3.1}$$

missä joko $v(r) < v(b)$ tai $r = 0$. Oletetaan nyt, että epäyhtälö $v(r) < v(b)$ on voimassa. Koska oletuksen mukaan $a \mid b$, niin määritelmän 3.5 mukaan on olemassa sellainen alkio $c \in E$, että

$$b = ac. \tag{3.2}$$

Tällöin yhtälö (3.1) saadaan muotoon $a = acq + r$, josta edelleen saadaan yhtälö

$$r = a - acq = a(1 - cq). \tag{3.3}$$

Yhtälöstä (3.3) nähdään, että $a \mid r$. Tällöin määritelmän 3.5 mukaan on olemassa sellainen alkio $u \in E$, että $r = au$. Tällöin saadaan oletusten ja määritelmän 3.1 kohdan (ii) perusteella, että

$$v(b) = v(a) \leq v(au) = v(r) < v(b),$$

mikä on selvästi ristiriita. Näin ollen oletus, että epäyhtälö $v(r) < v(b)$ on voimassa, on väärin. Tällöin yhtälö $r = 0$ on välttämättä voimassa. Näin ollen yhtälöstä (3.1) saadaan, että

$$a = bq. \tag{3.4}$$

Nyt yhtälöiden (3.2) ja (3.4) perusteella saadaan, että $b = ac = (bq)c = b(qc)$. Tällöin kokonaisalueessa voimassa olevien supistussääntöjen perusteella yhtälö $qc = 1$ on voimassa, jolloin yksikön määritelmän mukaan alkiot $q, c \in E$ ovat yksiköitä. Näin ollen yhtälöiden (3.2) ja (3.4) sekä määritelmän 3.6 perusteella alkiot a ja b ovat toistensa liittoalkiot.

Näin on saatu tehtävän todistus valmiiksi.

Kaksi seuraavaa lausetta käsittelevät liittoalkioiden ominaisuuksia.

Lause 3.7. *Olkoon R kommutatiivinen ykkösrengas ja olkoot $a, b, c \in R$. Silloin ovat voimassa seuraavat ominaisuudet.*

(i) *Jos alkio a on alkion b liittoalkio, niin silloin alkio b on alkion a liittoalkio.*

(ii) *Jos alkio a on alkion b liittoalkio ja alkio b on alkion c liittoalkio, niin silloin alkio a on alkion c liittoalkio.*

Todistus (vrt. [5, s. 353]). Todistetaan lauseen kohdat (i) ja (ii) erikseen.

Todistetaan ensin lauseen kohta (i). Oletetaan, että alkio a on alkion b liittoalkio. Silloin määritelmän 3.6 mukaan $a = bu$, jollakin yksiköllä $u \in R$. Koska $u \in R$ on yksikkö, niin yksikön määritelmän mukaan u^{-1} on olemassa ja se on renkaan R yksikön käänteisalkiona myös renkaan R yksikkö. Tällöin $buu^{-1} = au^{-1}$. Koska siis $uu^{-1} = 1$, niin nyt saadaan, että $b = au^{-1}$. Näin ollen määritelmän 3.6 mukaan alkio b on alkion a liittoalkio, joten lauseen kohta (i) on saatu todistettua.

Todistetaan seuraavaksi lauseen kohta (ii). Oletetaan, että alkio a on alkion b liittoalkio ja alkio b on alkion c liittoalkio. Silloin määritelmän 3.6 mukaan $a = bu_1$ ja $b = cu_2$, joillakin yksiköillä $u_1, u_2 \in R$. Tällöin saadaan, että $a = bu_1 = (cu_2)u_1 = c(u_2u_1)$. Koska $u_1, u_2 \in R$ ovat yksiköitä, niin u_2u_1 on renkaan R kahden yksikön tulona myös renkaan R yksikkö. Näin ollen määritelmän 3.6 mukaan alkio a on alkion c liittoalkio, joten lauseen kohta (ii) on saatu todistettua.

Näin on saatu lause 3.7 todistettua.

Lause 3.8. *Olkoon R kokonaisalue ja olkoot $a, b, c \in R$. Silloin ovat voimassa seuraavat ominaisuudet.*

(i) *Alkio a on alkion b liittoalkio, jos ja vain jos $a \mid b$ ja $b \mid a$.*

(ii) *Alkiot a ja b ovat toistensa liittoalkiot, jos ja vain jos $\langle a \rangle = \langle b \rangle$.*

Todistus (vrt. [5, s. 353–354] ja [2, s. 366]). Todistetaan lauseen kohdat (i) ja (ii) erikseen.

Todistetaan ensin lauseen kohta (i). Todistetaan kohta kahteen eri suuntaan. Oletetaan ensin, että alkio a on alkion b liittoalkio. Silloin määritelmän 3.6 mukaan $a = bu$, jollakin yksiköllä $u \in R$. Tällöin $b = au^{-1}$, kuten saatiin lauseen 3.7 kohdan (i) todistuksessa. Näin ollen määritelmän 3.5 mukaan $b \mid a$ ja $a \mid b$. Oletetaan sitten, että $b \mid a$ ja $a \mid b$. Silloin määritelmän 3.5 mukaan on olemassa sellaiset alkiot $q_1, q_2 \in R$, että $a = bq_1$ ja $b = aq_2$. Tällöin saadaan, että $b = aq_2 = (bq_1)q_2 = b(q_1q_2)$. Koska R on lauseen oletuksen mukaan kokonaisalue ja $a, b \neq 0$, niin kokonaisalueessa voimassa olevien supistussääntöjen perusteella tällöin saadaan, että $1 = q_1q_2$ (ks. [3, s. 60]). Tällöin yksikön määritelmän mukaan alkiot $q_1, q_2 \in R$ ovat yksiköitä. Näin ollen määritelmän 3.6 mukaan alkiot a ja b ovat toistensa liittoalkiot, jolloin erityisesti alkio a on alkion b liittoalkio. Näin on saatu todistettua lauseen kohta (i).

Todistetaan seuraavaksi lauseen kohta (ii).Todistetaan kohta kahteen eri suuntaan. Oletetaan ensin, että alkiot a ja b ovat toistensa liittoalkiot. Silloin lauseen 3.7 kohdan (i) ja lauseen 3.8 kohdan (i) perusteella $a \mid b$ ja $b \mid a$. Tällöin määritelmän 3.5 mukaan on olemassa sellaiset alkiot $q_1, q_2 \in R$, että $b = aq_2$ ja $a = bq_1$. Koska $\langle a \rangle = \{\, q_2a \mid q_2 \in R \,\}$ ja $\langle b \rangle = \{\, q_1b \mid q_1 \in R \,\}$, niin nyt selvästi $a \in \langle b \rangle$ ja $b \in \langle a \rangle$. Lauseen oletuksen mukaan R on kokonaisalue, jolloin se on kokonaisalueen määritelmän mukaan myös kommutatiivinen ykkösrengas, joten $1 \in R$. Näin ollen selvästi $a \in \langle a \rangle$ ja $b \in \langle b \rangle$. Näin ollen saadaan, että $\langle a \rangle \subseteq \langle b \rangle$ ja $\langle b \rangle \subseteq \langle a \rangle$. Tällöin $\langle a \rangle = \langle b \rangle$. Oletetaan sitten, että $\langle a \rangle = \langle b \rangle$. Silloin $a = bq_1$ ja $b = aq_2$, joillakin alkioilla $q_1, q_2 \in R$. Tällöin saadaan, että $a = bq_1 = (aq_2)q_1 = a(q_2q_1)$, josta edelleen kokonaisalueessa voimassa olevien supistussääntöjen perusteella saadaan, että $1 = q_2q_1$. Tällöin yksikön määritelmän mukaan alkiot $q_1, q_2 \in R$ ovat yksiköitä. Näin ollen määritelmän 3.6 mukaan alkiot a ja b ovat toistensa liittoalkiot. Näin on saatu todistettua lauseen kohta (ii).

Näin on saatu lause 3.8 todistettua.

3.5 Suurin yhteinen tekijä

Tässä alaluvussa käydään läpi käsitteen suurin yhteinen tekijä määritelmä kommutatiivisessa renkaassa (vrt. [5, s. 354]). Kyseinen määritelmä sisältää myös yhteisen tekijän määritelmän. Jo entuudestaan on tuttu määritelmä

kahden kokonaisluvun suurimmasta yhteisestä tekijästä (ks. [3, s. 5–6]), joten nyt on kyseessä käsitteen suurin yhteinen tekijä laajentaminen. Alaluvussa käydään myös läpi aihepiiriä havainnollistavia esimerkkejä. Lisäksi esitetään kaksi lausetta sekä toisen lauseen seurauslause todistuksineen. Alaluvun lopussa käydään vielä läpi käsitteen pienin yhteinen monikerta määritelmä kokonaisalueessa (vrt. [5, s. 359]).

Määritelmä 3.7. Olkoon R kommutatiivinen rengas ja olkoot $a_1, a_2, \ldots, a_n$ ($n \geq 2$) joukon R sellaisia alkioita, että ainakin yksi niistä on nollasta eroava. Nollasta eroavaa alkiota $d \in R$ sanotaan alkioiden $a_1, a_2, \ldots, a_n$ *yhteiseksi tekijäksi* (engl. common divisor), jos

$$d \mid a_i$$

aina, kun $i = 1, 2, \ldots, n$. Nollasta eroavaa alkiota $d \in R$ sanotaan alkioiden $a_1, a_2, \ldots, a_n$ *suurimmaksi yhteiseksi tekijäksi* (engl. greatest common divisor), jos

(i) alkio d on alkioiden $a_1, a_2, \ldots, a_n$ yhteinen tekijä ja

(ii) jos nollasta eroava alkio $c \in R$ on myös alkioiden $a_1, a_2, \ldots, a_n$ yhteinen tekijä, niin silloin $c \mid d$.

Huomautus. Suomeksi suurin yhteinen tekijä lyhennetään kirjainyhdistelmällä syt ja englanniksi lyhennys on gcd.

Merkintä. Alkioiden a_1 ja a_2 suurinta yhteistä tekijää merkitään symbolilla (a_1, a_2), $\text{syt}(a_1, a_2)$ tai $\gcd(a_1, a_2)$. Tässä tutkielmassa käytetään merkintää $\text{syt}(a_1, a_2)$.

Huomautus. Kommutatiivisessa renkaassa kahden alkion suurin yhteinen tekijä ei välttämättä ole yksikäsitteinen eikä sitä välttämättä ole edes olemassa (vrt. [5, s. 354]).

Käydään seuraavaksi läpi esimerkki, joka havainnollistaa määritelmiä 3.6 ja 3.7.

Esimerkki 3.15. ([5, s. 354, Esim. 15.2.7]) Tarkastellaan rengasta $\mathbb{Z}_{10}$. Silloin $\overline{4} \cdot \overline{6} = \overline{4 \cdot 6} = \overline{24} = \overline{4}$ ja $\overline{4} \cdot \overline{4} = \overline{4 \cdot 4} = \overline{16} = \overline{6}$. Tämä osoittaa, että alkiot $\overline{4}$ ja $\overline{6}$ ovat alkioiden $\overline{4}$ ja $\overline{6}$ yhteiset tekijät, koska $\overline{4} \cdot \overline{1} = \overline{4 \cdot 1} = \overline{4}$ ja $\overline{6} \cdot \overline{1} = \overline{6 \cdot 1} = \overline{6}$. Tällöin alkiot $\overline{4}$ ja $\overline{6}$ ovat alkioiden $\overline{4}$ ja $\overline{6}$ suurimmat yhteiset tekijät.

Koska renkaassa $\mathbb{Z}_{10}$ on yhtälö $\overline{9} \cdot \overline{9} = \overline{9 \cdot 9} = \overline{81} = \overline{1}$ voimassa, niin yksikön määritelmän mukaan alkio $\overline{9} \in \mathbb{Z}_{10}$ on renkaan $\mathbb{Z}_{10}$ yksikkö. Nyt koska $\overline{9} \cdot \overline{4} = \overline{9 \cdot 4} = \overline{36} = \overline{6}$ ja $\overline{9} \cdot \overline{6} = \overline{9 \cdot 6} = \overline{54} = \overline{4}$, niin määritelmän 3.6 mukaan alkiot $\overline{4}$ ja $\overline{6}$ ovat toistensa liittoalkiot.

Seuraava esimerkki liittyy määritelmiin 3.5 ja 3.7.

Esimerkki 3.16. ([5, s. 354, Esim. 15.2.8]) Merkitköön E kaikkien parillisten kokonaislukujen joukkoa. Tällöin kolmikko $(E, +, \cdot)$ on selvästi rengas. Renkaassa E alkiolla $2 \in E$ ei ole yhtään tekijää, koska millään nollasta eroavalla alkiolla $d \in E$ ei ole voimassa $d \mid 2$, koska yhtälö $2 = dc$ ei ole voimassa millään alkioilla $d, c \in E$. Tällöin määritelmän 3.7 mukaan alkiolla $2 \in E$ ei voi olla minkään joukon E alkion kanssa yhteistä tekijää.

Seuraava lause osoittaa, että pääihannerenkaassa jokaisella parilla, jossa ainakin toinen alkioista on nollasta eroava, on olemassa suurin yhteinen tekijä.

Lause 3.9. *Olkoon R pääihannerengas ja olkoot a, b joukon R sellaiset alkiot, että ainakin toinen niistä on nollasta eroava. Silloin on olemassa alkioiden a ja b suurin yhteinen tekijä $d \in R \setminus \{0\}$. Lisäksi jokaista alkioiden a ja b suurinta yhteistä tekijää d kohti on olemassa sellaiset alkiot $s, t \in R$, että $d = sa + tb$.*

Todistus (vrt. [5, s. 354] ja [6, s. 282]). Olkoon $I = \langle a, b \rangle = \{\, xa + yb \mid x, y \in R \,\}$ renkaan R ihanne, joka on alkioiden a ja b virittämä. Koska lauseen oletuksen mukaan R on pääihannerengas, niin määritelmän 3.3 mukaan renkaan R ihanne $\langle a, b \rangle$ on pääihanne. Pääihanteen määritelmän mukaan on olemassa sellainen alkio $d \in R$, että $I = \langle d \rangle$. Näin ollen on olemassa sellainen alkio $d \in R$, että $\langle a, b \rangle = \langle d \rangle$. Koska $d \in \langle a, b \rangle$, niin on olemassa sellaiset alkiot $s, t \in R$, että $d = sa + tb$. Koska $I = \langle d \rangle = \langle a, b \rangle$, niin on olemassa sellaiset alkiot $u, v \in R$, että $a = ud$ ja $b = vd$. Näin ollen määritelmän 3.5 mukaan $d \mid a$ ja $d \mid b$. Tällöin määritelmän 3.7 mukaan alkio d on alkioiden a ja b yhteinen tekijä. Oletetaan nyt, että nollasta eroava alkio $c \in R$ on alkioiden a ja b yhteinen tekijä. Silloin määritelmän 3.7 mukaan $c \mid a$ ja $c \mid b$. Tällöin määritelmän 3.5 mukaan on olemassa sellaiset alkiot $u', v' \in R$, että $a = u'c$ ja $b = v'c$. Tällöin $d = sa + tb = su'c + tv'c = (su' + tv')c$, joten $c \mid d$. Näin ollen määritelmän 3.7 mukaan d on alkioiden a ja b suurin yhteinen tekijä. Olkoon $d' \in R \setminus \{0\}$ alkioiden a ja b mikä tahansa suurin yhteinen tekijä. Silloin määritelmän 3.7 mukaan $d \mid d'$ ja $d' \mid d$, joten lauseiden 3.7 ja 3.8 perusteella $\langle d' \rangle = \langle d \rangle = \langle a, b \rangle$. Näin ollen on olemassa sellaiset alkiot $s', t' \in R$, että $d' = s'a + t'b$.

Näin on saatu todistettua, että alkioilla a ja b on olemassa suurin yhteinen tekijä $d \in R \setminus \{0\}$. Lisäksi on saatu todistettua, että jokaista suurinta yhteistä tekijää d kohti on olemassa sellaiset alkiot $s, t \in R$, että $d = sa + tb$. Näin ollen lause on saatu todistettua.

Seuraus. Olkoon R euklidinen alue ja olkoot a, b joukon R sellaiset alkiot, että ainakin toinen niistä on nollasta eroava. Silloin alkioilla a ja b on olemassa suurin yhteinen tekijä $d \in R \setminus \{0\}$. Jokaista alkioiden a ja b suurinta yhteistä tekijää d kohti on olemassa sellaiset alkiot $s, t \in R$, että $d = sa + tb$.

Todistus (vrt. [5, s. 355]). Koska jokainen euklidinen alue on lauseen 3.4 perusteella pääihannealue ja koska määritelmän 3.4 mukaan jokainen pääihannealue on pääihannerengas, niin tällöin jokainen euklidinen alue on pääihannerengas. Näin ollen seurauslauseen väitös seuraa suoraan lauseesta 3.9, joten seurauslause on saatu todistettua.

Huomautus. Lauseen 3.9 tulos on mahdollista todistaa myös mille tahansa äärelliselle joukolle pääihannerenkaan alkioita $a_1, a_2, \ldots, a_n$, joista ainakin yksi on nollasta eroava, menetellen kuten lauseen 3.9 todistuksessa. Tällaista todistusta ei kuitenkaan tässä tutkielmassa esitetä.

Käydään seuraavaksi läpi lause, joka osoittaa, että tiettyjen oletusten vallitessa alkioiden kaksi suurinta yhteistä tekijää ovat toistensa liittoalkioita.

Lause 3.10. *Olkoon R kokonaisalue ja olkoot $a_1, a_2, \ldots, a_n \in R$, missä $n \geq 2$. Jos joukon R alkiot d ja d' ovat alkioiden $a_1, a_2, \ldots, a_n$ kaksi suurinta yhteistä tekijää, niin silloin alkiot d ja d' ovat toistensa liittoalkioita.*

Todistus (vrt. [6, s. 283]). Oletetaan, että joukon R alkiot d ja d' ovat alkioiden $a_1, a_2, \ldots, a_n$ kaksi suurinta yhteistä tekijää. Silloin määritelmän 3.7 mukaan $d, d' \in R \setminus \{0\}$, $d' \mid d$ ja $d \mid d'$. Tällöin määritelmän 3.5 mukaan on olemassa sellaiset alkiot $u, v \in R$, että

$$d = ud' \quad \text{ja} \quad d' = vd. \tag{3.5}$$

Näin ollen $d = ud' = u(vd) = (uv)d$, jolloin yhtälö $d(1-uv) = 0$ on voimassa. Koska $d \neq 0$ ja R on kokonaisalue, jossa siis ei ole nollanjakajia, niin nyt saadaan, että $1 - uv = 0$ eli että $uv = 1$. Tällöin yksikön määritelmän mukaan alkiot u ja v ovat kokonaisalueen R yksiköitä. Näin ollen kohdan (3.5) yhtälöiden ja määritelmän 3.6 mukaan d on alkion d' liittoalkio ja d' on alkion d liittoalkio. Näin on saatu todistettua, että jos d ja d' ovat alkioiden $a_1, a_2, \ldots, a_n$ kaksi suurinta yhteistä tekijää, niin silloin alkiot d ja d' ovat toistensa liittoalkioita.

Huomautus. Jos d on alkioiden $a_1, a_2, \ldots, a_n$ suurin yhteinen tekijä, niin silloin alkion d mikä tahansa liittoalkio on myös alkioiden $a_1, a_2, \ldots, a_n$ suurin yhteinen tekijä. Lauseen 3.10 ja edellä mainitun perusteella voidaan sanoa, että kokonaisalueessa alkioiden $a_1, a_2, \ldots, a_n$ suurin yhteinen tekijä on yksikäsitteinen lauseen 3.10 mielessä eli se on liittoalkioita vaille yksikäsitteinen. (Vrt. [5, s. 355].)

Käydään seuraavaksi läpi esimerkki, joka osoittaa, että euklidisessa alueessa jaettavan ja jakajan syt on yhtäsuuri kuin jakajan ja jakojäännöksen syt.

Esimerkki 3.17. ([5, s. 356, Harj. 1]) Olkoon $(E, +, \cdot, v)$ euklidinen alue. Olkoot $a, b, q, r \in E$ sellaisia alkioita, että $b \neq 0$, $a = qb + r$ ja $r \neq 0$. Osoitetaan, että tällöin $\text{syt}(a, b) = \text{syt}(b, r)$.

Olkoon $\text{syt}(a,b) = d$ ja $\text{syt}(b,r) = d'$. Tällöin määritelmän 3.7 mukaan $d \mid a$ ja $d \mid b$. Oletuksen mukaan $r = a - qb$, joten $d \mid r$. Näin ollen määritelmän 3.7 mukaan alkio d on alkioiden b ja r yhteinen tekijä. Tällöin edellä tehdyn oletuksen ja määritelmän 3.7 mukaan $d \mid d'$. Lisäksi edellä tehdyn oletuksen ja määritelmän 3.7 mukaan $d' \mid b$ ja $d' \mid r$. Oletuksen mukaan $a = qb + r$, joten $d' \mid a$. Näin ollen määritelmän 3.7 mukaan alkio d' on alkioiden a ja b yhteinen tekijä. Tällöin edellä tehdyn oletuksen ja määritelmän 3.7 mukaan $d' \mid d$. Näin on saatu, että $d \mid d'$ ja $d' \mid d$. Tällöin lauseen 3.7 kohdan (i) ja lauseen 3.8 kohdan (i) perusteella alkiot d ja d' ovat toistensa liittoalkiot, joten lauseen 3.10 ja siihen liittyvän huomautuksen perusteella $\text{syt}(a,b) = \text{syt}(b,r)$.

Näin on saatu tehtävän osoitus valmiiksi.

Myös seuraava esimerkki osoittaa yhden suurimman yhteisen tekijän ominaisuuden.

Esimerkki 3.18. ([5, s. 359, Harj. 12]) Olkoon R kokonaisalue. Olkoot $a, b, c \in R \setminus \{0\}$ sellaisia alkioita, että $\text{syt}(a,b)$ ja $\text{syt}(ca,cb)$ ovat olemassa. Todistetaan, että $\text{syt}(ca,cb) = \text{syt}(a,b) \cdot c$.

Olkoon $\text{syt}(a,b) = d$ ja $\text{syt}(ca,cb) = e$. Tällöin määritelmän 3.7 mukaan $d \mid a$ ja $d \mid b$. Näin ollen myös $cd \mid ca$ ja $cd \mid cb$, joten määritelmän 3.7 mukaan $cd \mid e$. Tällöin määritelmän 3.5 mukaan on olemassa sellainen alkio $f \in R$, että

$$e = cdf. \tag{3.6}$$

Toisaalta määritelmän 3.7 mukaan $e \mid ca$ ja $e \mid cb$, jolloin määritelmän 3.5 mukaan on olemassa sellaiset alkiot $g, h \in R$, että $ca = eg$ ja $cb = eh$. Näin ollen yhtälön (3.6) perusteella saadaan, että $ca = eg = (cdf)g = c(dfg)$ ja $cb = eh = (cdf)h = c(dfh)$. Tällöin kokonaisalueessa voimassa olevien supistussääntöjen perusteella $a = dfg$ ja $b = dfh$. Näin ollen määritelmän 3.5 mukaan $df \mid a$ ja $df \mid b$, jolloin määritelmän 3.7 mukaan $df \mid d$. Tällöin määritelmän 3.5 mukaan on olemassa sellainen alkio $u \in R$, että $d = dfu$. Näin ollen kokonaisalueessa voimassa olevien supistussääntöjen perusteella $fu = 1$, jolloin yksikön määritelmän mukaan alkiot $f, u \in R$ ovat yksiköitä. Merkitään, että $df = v$, jolloin $v \in R$. Koska alkio $f \in R$ on yksikkö, niin määritelmän 3.6 mukaan alkio v on alkion d liittoalkio. Alussa tehdyn oletuksen mukaan $d = \text{syt}(a,b)$, joten lauseen 3.10 ja siihen liittyvän huomautuksen perusteella myös $v = \text{syt}(a,b)$.

Näin on saatu, että $\text{syt}(ca,cb) = e = cdf = cv = vc = \text{syt}(a,b) \cdot c$, joten todistus on saatu valmiiksi.

Käydään seuraavaksi läpi esimerkki, jossa tehtävän osoittamiseen käytetään apuna esimerkkiä 3.18.

Esimerkki 3.19. ([1, s. 215, Harj. 2]) Olkoon R sellainen kokonaisalue, että $\text{syt}(a, b)$ on olemassa aina, kun $a, b \in R$. Olkoot lisäksi $a, b, c \in R$. Osoitetaan nyt, että jos $\text{syt}(a, b) = 1$, $a \mid c$ ja $b \mid c$, niin silloin $ab \mid c$.

Oletetaan ensin, että $a \mid c$ ja $b \mid c$. Silloin määritelmän 3.5 mukaan on olemassa sellaiset alkiot $d, e \in R$, että

$$c = ad \quad \text{ja} \quad c = be. \tag{3.7}$$

Oletetaan vielä, että $\text{syt}(a, b) = 1$. Tällöin esimerkin 3.18 ja kohdan (3.7) yhtälöiden perusteella saadaan, että

$$\begin{aligned} c &= 1 \cdot c = \text{syt}(a, b) \cdot c \\ &= \text{syt}(ca, cb) = \text{syt}(bea, adb) \\ &= \text{syt}(abe, abd) = \text{syt}(e, d) \cdot ab. \end{aligned}$$

Näin ollen määritelmän 3.5 mukaan $ab \mid c$, joten tehtävän osoitus on saatu valmiiksi.

Seuraavassa esimerkissä käytetään määritelmiä 3.5 ja 3.7 sekä lausetta 3.9 apuna tehtävän osoittamiseen.

Esimerkki 3.20. ([5, s. 356, Harj. 2]) Olkoon R pääihannealue. Olkoot $a, b, c \in R \setminus \{0\}$. Osoitetaan, että tällöin on olemassa sellaiset alkiot $x, y \in R$, että $ax + by = c$, jos ja vain jos $\text{syt}(a, b) \mid c$.

Olkoon $\text{syt}(a, b) = d$. Tehdään osoitus kahdessa eri osassa. Oletetaan ensin, että on olemassa sellaiset alkiot $x, y \in R$, että $ax + by = c$. Koska oletuksen mukaan $\text{syt}(a, b) = d$, niin määritelmän 3.7 mukaan $d \mid a$ ja $d \mid b$. Näin ollen $d \mid c$ eli $\text{syt}(a, b) \mid c$.

Oletetaan sitten, että $\text{syt}(a, b) \mid c$ eli että $d \mid c$. Tällöin määritelmän 3.5 mukaan $c = dd'$, jollakin alkiolla $d' \in R$. Lisäksi lauseen 3.9 perusteella on olemassa sellaiset alkiot $x', y' \in R$, että $d = ax' + by'$. Tällöin saadaan, että $c = dd' = (ax' + by')d' = ax'd' + by'd'$. Valitaan nyt, että $x = x'd' \in R$ ja $y = y'd' \in R$. Tällöin saadaan, että on olemassa sellaiset alkiot $x, y \in R$, että $ax + by = c$.

Näin on saatu osoitettua, että on olemassa sellaiset alkiot $x, y \in R$, että $ax + by = c$, jos ja vain jos $\text{syt}(a, b) \mid c$, joten tehtävän osoitus on saatu valmiiksi.

Määritelmä 3.8. Olkoon R kokonaisalue ja olkoot $a_1, a_2, \ldots, a_n$ $(n \geq 2)$ joukon R nollasta eroavia alkioita. Silloin alkiota $d \in R$ sanotaan alkioiden $a_1, a_2, \ldots, a_n$ *pienimmäksi yhteiseksi monikerraksi* (engl. least common multiple), jos

(i) $a_i \mid d$ aina, kun $i = 1, 2, \ldots, n$ ja

(ii) jos $c \in R$ on sellainen alkio, että $a_i \mid c$ aina, kun $i = 1, 2, \ldots, n$, niin silloin $d \mid c$.

Huomautus. Suomeksi pienin yhteinen monikerta lyhennetään kirjainyhdistelmällä pym ja englanniksi lyhennys on lcm.

Merkintä. Alkioiden a_1 ja a_2 pienintä yhteistä monikertaa merkitään symbolilla $[a_1, a_2]$, $\text{pym}[a_1, a_2]$ tai $\text{lcm}[a_1, a_2]$.

3.6 Eukleideen algoritmi

Tässä alaluvussa käydään läpi euklidisessa alueessa käytettävä algoritmi, jonka avulla löydetään kahden alkion suurin yhteinen tekijä (vrt. [5, s. 355–356] ja [6, s. 282–283]). Kyseisessä algoritmissa sovelletaan jakoalgoritmia. Lisäksi esitetään tapa, jolla löydetään suurimman yhteisen tekijän lineaarikombinaatioesitys. Alaluvussa käydään myös läpi algoritmia ja lineaarikombinaatioesitystä havainnollistavat esimerkit.

Edellä lauseen 3.9 seurauslauseessa ollaan nähty, että euklidisessa alueessa $(E, +, \cdot, v)$ joukon E kahden alkion a, b (vähintään toinen alkioista nollasta eroava) suurin yhteinen tekijä on olemassa ja $\text{syt}(a, b) \in E \setminus \{0\}$.

Seuraavaksi käydään läpi algoritmi, jonka avulla löydetään euklidisessa alueessa $(E, +, \cdot, v)$ kahden alkion suurin yhteinen tekijä. Kyseinen algoritmi on samankaltainen kuin algoritmi, jonka avulla löydetään kahden kokonaisluvun suurin yhteinen tekijä (ks. [3, s. 7–8, Lause 1.3.4]).

Huomautus. Kahden alkion suurimman yhteisen tekijän löytämiseen käytettävää algoritmia sanotaan *Eukleideen algoritmiksi* (engl. Euclidean algorithm).

Käydään nyt läpi Eukleideen algoritmi, jonka avulla löydetään euklidisessa alueessa kahden alkion suurin yhteinen tekijä.

Olkoon $(E, +, \cdot, v)$ euklidinen alue ja olkoot $a, b \in E$ sellaisia alkioita, että $b \neq 0$.

Askel 1: Etsitään sellaiset alkiot $q_1, r_1 \in E$, että $a = q_1 b + r_1$, missä joko $r_1 = 0$ tai $v(r_1) < v(b)$.

Jos $r_1 = 0$, niin $a = q_1 b$ ja tällöin määritelmän 3.5 mukaan $b \mid a$. Määritelmän 3.5 mukaan selvästi myös $b \mid b$. Näin ollen määritelmän 3.7 mukaan $\text{syt}(a, b) = b$.

Jos $r_1 \neq 0$, niin silloin esimerkin 3.17 mukaan $\text{syt}(a, b) = \text{syt}(b, r_1)$. Näin ollen seuraavaksi tulee löytää $\text{syt}(b, r_1)$.

Askel 2: Etsitään sellaiset alkiot $q_2, r_2 \in E$, että $b = q_2 r_1 + r_2$, missä joko $r_2 = 0$ tai $v(r_2) < v(r_1)$.

Jos $r_2 = 0$, niin $b = q_2 r_1$ ja tällöin määritelmän 3.5 mukaan $r_1 \mid b$. Määritelmän 3.5 mukaan selvästi myös $r_1 \mid r_1$. Näin ollen määritelmän 3.7 mukaan $\text{syt}(a, b) = \text{syt}(b, r_1) = r_1$.

Jos $r_2 \neq 0$, niin silloin esimerkin 3.17 mukaan $\text{syt}(a, b) = \text{syt}(b, r_1) = \text{syt}(r_1, r_2)$. Näin ollen seuraavaksi tulee löytää $\text{syt}(r_1, r_2)$.

Koska $v(b) > v(r_1) > v(r_2) > \cdots \geq 0$ on aidosti vähenevä jono einegatiivisia kokonaislukuja, niin yllä oleva prosessi loppuu tietyn äärellisen askelmäärän jälkeen. Näin ollen on olemassa sellainen positiivinen kokonaisluku n, että askeleella n on olemassa sellaiset alkiot $q_n, r_n \in E$, että $r_{n-2} = q_n r_{n-1} + r_n$, missä $r_n = 0$. Tällöin siis

$$\begin{aligned}
a &= q_1 b + r_1, && v(r_1) < v(b),\\
b &= q_2 r_1 + r_2, && v(r_2) < v(r_1),\\
r_1 &= q_3 r_2 + r_3, && v(r_3) < v(r_2),\\
&\vdots && \vdots\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, && v(r_{n-1}) < v(r_{n-2}),\\
r_{n-2} &= q_n r_{n-1} + r_n, && r_n = 0.
\end{aligned}$$

Näin ollen esimerkin 3.17 nojalla

$$\begin{aligned}
\mathrm{syt}(a,b) &= \mathrm{syt}(b, r_1)\\
&= \mathrm{syt}(r_1, r_2)\\
&\vdots\\
&= \mathrm{syt}(r_{n-2}, r_{n-1})\\
&= \mathrm{syt}(r_{n-1}, 0)\\
&= r_{n-1}.
\end{aligned}$$

Näin on käyty läpi Eukleideen algoritmi, jonka avulla löydetään euklidisessa alueessa kahden alkion suurin yhteinen tekijä.

Käydään seuraavaksi läpi esimerkki, joka havainnollistaa edellä läpikäytyä Eukleideen algoritmia.

Esimerkki 3.21. ([5, s. 359, Harj. 13]) Etsitään $\mathrm{syt}(2-7i, 2+11i)$ euklidisessa alueessa $(\mathbb{Z}[i], +, \cdot, N)$. Lauseen 3.3 perusteella $(\mathbb{Z}[i], +, \cdot, N)$ on euklidinen alue, missä $N(a+bi) = (a+bi)(a-bi) = a^2+b^2$. Tällöin saadaan, että $N(2-7i) = 53$ ja $N(2+11i) = 125$. Käytetään nyt tehtävän ratkaisemiseen Eukleideen algoritmia.

Askel 1: Nyt

$$\begin{aligned}
\frac{2+11i}{2-7i} &= \frac{2+11i}{2-7i} \cdot \frac{2+7i}{2+7i} = \frac{-73+36i}{53} = \frac{-73}{53} + \frac{36i}{53}\\
&= (-1 - \frac{20}{53}) + (1 - \frac{17}{53})i = (-1+i) + \frac{-20-17i}{53}.
\end{aligned}$$

Näin ollen

$$\begin{aligned}
2+11i &= (-1+i)(2-7i) + (\frac{-20-17i}{53})(2-7i)\\
&= (-1+i)(2-7i) + \frac{-159+106i}{53}\\
&= (-1+i)(2-7i) + (-3+2i).
\end{aligned}$$

Tällöin $N(-3+2i) = 13 < 53 = N(2-7i)$.

Askel 2: Nyt

$$\begin{aligned}\frac{2-7i}{-3+2i} &= \frac{2-7i}{-3+2i}\cdot\frac{-3-2i}{-3-2i} = \frac{-20+17i}{13} = \frac{-20}{13}+\frac{17i}{13}\\ &= (-1-\frac{7}{13})+(1+\frac{4}{13})i = (-1+i)+\frac{-7+4i}{13}.\end{aligned}$$

Näin ollen

$$\begin{aligned}2-7i &= (-1+i)(-3+2i)+(\frac{-7+4i}{13})(-3+2i)\\ &= (-1+i)(-3+2i)+\frac{13-26i}{13}\\ &= (-1+i)(-3+2i)+(1-2i).\end{aligned}$$

Tällöin $N(1-2i) = 5 < 13 = N(-3+2i)$.

Askel 3: Nyt

$$\begin{aligned}\frac{-3+2i}{1-2i} &= \frac{-3+2i}{1-2i}\cdot\frac{1+2i}{1+2i} = \frac{-7-4i}{5} = \frac{-7}{5}-\frac{4i}{5}\\ &= (-1-\frac{2}{5})-(1-\frac{1}{5})i = (-1-i)+\frac{-2+i}{5}.\end{aligned}$$

Näin ollen

$$\begin{aligned}-3+2i &= (-1-i)(1-2i)+(\frac{-2+i}{5})(1-2i)\\ &= (-1-i)(1-2i)+\frac{5i}{5}\\ &= (-1-i)(1-2i)+i.\end{aligned}$$

Tällöin $N(i) = 1 < 5 = N(1-2i)$.

Askel 4: Nyt

$$\frac{1-2i}{i} = \frac{1-2i}{i}\cdot\frac{-i}{-i} = \frac{-i-2}{1} = -i-2.$$

Näin ollen

$$1-2i = (-i-2)\cdot i+0,$$

joten $r_4 = 0$.

Tällöin Eukleideen algoritmin perusteella $\mathrm{syt}(2-7i, 2+11i) = r_3 = i$. Näin on löydetty alkioiden $2-7i$ ja $2+11i$ suurin yhteinen tekijä euklidisessa alueessa $(\mathbb{Z}[i], +, \cdot, N)$, joten tehtävä on saatu ratkaistua.

Esitetään seuraavaksi tapa, jolla löydetään euklidisessa alueessa kahden alkion suurimman yhteisen tekijän lineaarikombinaatioesitys (vrt. [5, s. 356]).

Todetaan aluksi, että lauseen 3.9 seurauslauseen perusteella on olemassa sellaiset alkiot $x, y \in E$, että $\text{syt}(a, b) = ax + by$. Eukleideen algoritmin, jonka avulla löydetään euklidisessa alueessa kahden alkion suurin yhteinen tekijä, perusteella

$$\begin{aligned} r_{n-1} &= r_{n-3} - q_{n-1}r_{n-2} \\ &= r_{n-3} - q_{n-1}(r_{n-4} - q_{n-2}r_{n-3}) \\ &= r_{n-3}(1 + (-q_{n-1})(-q_{n-2})) + r_{n-4}(-q_{n-1}) \\ &\vdots \\ &= by + ax. \end{aligned}$$

Koska siis $r_{n-1} = \text{syt}(a, b)$, niin näin on saatu, että $\text{syt}(a, b) = ax + by$, joillakin alkioilla $x, y \in E$. Näin on siis saatu selville, miten suurimman yhteisen tekijän lineaarikombinaatioesitys löydetään.

Käydään seuraavaksi läpi yllä mainittua koskeva ja havainnollistava esimerkki, joka on samalla jatkoa esimerkille 3.21.

Esimerkki 3.22. ([5, s. 359, Harj. 13]) Etsitään sellaiset alkiot $x, y \in \mathbb{Z}[i]$, että $\text{syt}(2 - 7i, 2 + 11i) = (2 - 7i)x + (2 + 11i)y$. Esimerkin 3.21 ja yllä mainitun perusteella saadaan, että

$$\begin{aligned} i &= (-3 + 2i) - (-1 - i)(1 - 2i) \\ &= (-3 + 2i) + (1 + i)((2 - 7i) - (-1 + i)(-3 + 2i)) \\ &= (-3 + 2i) + (1 + i)(2 - 7i) + (1 + i)(1 - i)(-3 + 2i) \\ &= (2 + 11i) + (2 - 7i)((1 - i) + (1 + i)) + 2(2 + 11i) + 2(1 - i)(2 - 7i) \\ &= 3(2 + 11i) + (2 - 7i)((1 - i) + (1 + i) + 2(1 - i)) \\ &= 3(2 + 11i) + (4 - 2i)(2 - 7i). \end{aligned}$$

Näin on saatu, että $x = 4 - 2i$ ja $y = 3$. Näin on löydetty sopivat alkiot $x, y \in \mathbb{Z}[i]$, koska selvästi yhtälö $\text{syt}(2-7i, 2+11i) = i = (2-7i)(4-2i)+(2+11i)\cdot 3$ on voimassa. Näin on saatu tehtävä ratkaistua.

Viitteet

[1] Bhattacharya, P. B. & Jain, S. K. & Nagpaul, S. R. *Basic Abstract Algebra*, 2nd ed., Cambridge University Press, 1994.

[2] Fraleigh, John B. *A First Course in Abstract Algebra*, 5th ed., Addison-Wesley, 1997.

[3] Haukkanen, Pentti *Algebra*, Luentomoniste, Tampereen yliopisto, Kevät 2003.

[4] Mac Lane, S. & Birkhoff, G. *Algebra*, 1st ed., The Macmillan Company, 1967.

[5] Malik, D. S. & Mordeson, J. N. & Sen, M. K. *Fundamentals of Abstract Algebra*, WCB/McGraw-Hill, 1997.

[6] Papantonopoulou, Aigli *Algebra: Pure & Applied*, Prentice-Hall, 2002.