

Henni Kiiskinen

Polynomien jaollisuus

Tiivistelmä

Henni Kiiskinen: Polynomien jaollisuus

Kandidaattitutkielma

Tampereen yliopisto

Matematiikan ja tilastotieteen kandidaatintutkinto

Kesäkuu 2024

Tässä tutkielmassa tutkitaan polynomien jaollisuutta ja hieman polynomien jakoalgoritmia. Ensiksi tutustutaan jaollisuuden ymmärtämistä varten vaadittaviin esitietoihin, jonka jälkeen käsitellään polynomirenkaita ja lopuksi polynomien jaollisuutta. Aiheita käsitellään pääasiassa lauseiden ja määritelmien avulla, mutta tärkeimpien lauseiden todistukset on myös esitetty ja niistä on annettu esimerkit.

Luvussa 2 käsitellään polynomien jaollisuutta varten tarvittavia esitietoja. Tässä tutkielmassa käsitellään muutamia renkaisiin liittyviä oleellisia lauseita ja määritelmiä, jotka sisältävät renkaiden ominaisuuksia. Lopuksi käsitellään myös lyhyesti kokonaisalue ja faktoriaalinen kokonaisalue sekä määritellään jaottomien alkioiden edustajisto.

Luvussa 3 käsitellään polynomien jaollisuutta. Ensiksi käsitellään polynomi ja sen ominaisuuksia, jonka jälkeen tutustutaan polynomirenkaisiin. Alaluvussa 3.3 aletaan käsittelemään tarkemmin polynomien jaollisuutta määrittelemällä polynomien jakoalgoritmi ja siitä seuraavia sovelluksia. Luvussa käsitellään myös Eukleideen algoritmi polynomeille ja esitetään algoritmin käyttöä esimerkin avulla.

Seuraavassa alaluvussa 3.4 todistetaan aritmetiikan peruslausetta vastaava tulos polynomeille. Lisäksi tutustutaan polynomien jaottomuuteen ja siihen, miten voidaan selvittää, onko polynomi jaollinen vai jaoton jonkin kunnan yli muodostetun polynomirenkaan alkiona. Luvussa käsitellään polynomien tekijöihin jakoa eri tavoin, sekä sen merkitystä polynomien jaollisuudelle. Monissa luvun lauseissa ja määritelmissä käsitellään primitiivisiä polynomeja, joten niistä on esitetty myös useampi esimerkki tutkielmassa. Luvussa käydään myös läpi Gaussin lemma ja Eisensteinin kriteeri jaottomuudelle sekä esitetään todistus Gaussin lemmalle. Lopussa käydään läpi vielä haastavampi esimerkki polynomien tekijöihin jakamisesta kahdessa eri renkaassa.

Avainsanat: polynomi, polynomirengas, Gaussin lemma, Eisensteinin kriteeri,
jaollisuus, jaottomuus

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -ohjelmalla.

Sisällys

1	Johdanto	5
2	Esitietoja	6
2.1	Renkaat	6
2.2	Faktoriaalinen kokonaisalue	7
3	Polynomien jaollisuus	10
3.1	Polynomi	10
3.2	Polynomirengas	12
3.3	Jakoalgoritmi ja sen sovellukset	13
3.4	Jaottomuus ja polynomien tekijöihin jako	18
	Lähteet	24

1 Johdanto

Tässä tutkielmassa perehdymme polynomien jaollisuuteen sekä lyhyesti polynomien jakoalgoritmiin, jonka avulla polynomeja voidaan jakaa keskenään. Tutkielmassa käsittelemme myös polynomien jaottomuutta.

Luvussa 2 käsitellään polynomien jaollisuutta varten vaadittavat esitiedot. Alaluvussa 2.1 käsitellään renkaan määritelmä sekä renkaiden ominaisuuksia. Seuraavassa alaluvussa 2.2 kerrataan lyhyesti kokonaisalueen määritelmä, minkä jälkeen perehdytään faktoriaalisen kokonaisalueen käsitteeseen.

Luvussa 3 perehdymme polynomeihin. Alaluvut 3.1 ja 3.2 käsittelevät polynomin ja polynomirenkaan määritelmiä sekä niitä koskevia lauseita ja niiden ominaisuuksia.

Alaluvussa 3.3 käsittelemme jakoalgoritmin polynomeille sekä Euklidisen algoritmin polynomeille. Näiden pohjalta käsittelemme myös lyhyen esimerkin osamäärän, jakojäännöksen ja suurimman yhteisen tekijän määrittämisestä. Luvussa perehdymme myös polynomien keskenäisiin operaatioihin tietyssä polynomirenkaassa.

Seuraavassa alaluvussa 3.4 perehdymme tarkemmin polynomien jaottomuuteen. Luvussa esitämme aritmetiikan peruslauseita vastaavan tuloksen polynomeille sekä esitämme muutamia esimerkkejä jaottomista polynomeista. Käsittelemme luvussa myös Gaussin lemmän sekä Eisensteinin kriteerin jaottomuudelle, jotka ovat keskeisiä lauseita polynomien jaollisuuden käsittelyssä.

Tutkielman lukijan oletamme hallitsevan polynomin määritelmän ja polynomien laskusäännöt jaollisuutta lukuunottamatta sekä kurssin Algebra perusteet. Tutkielman päälähteenä käytämme Reisin kirjaa *Abstract Algebra: An Introduction to Groups, Rings and Fields* [1]. Käytämme lähteenä myös Nicodemin, Sutherlandin ja Towsleyn kirjaa *An Introduction to Abstract Algebra with Notes to the Future Teacher* [2] sekä Nicholsonin kirjaa *Introduction to Abstract Algebra* [3].

2 Esitietoja

Luvussa 2 käsitellään polynomien jaollisuuden tarkastelua varten tarvittavia esitietoja. Lukua käsitellään teoksen *Abstract Algebra: An Introduction to Groups, Rings and Fields* luvun 8 mukaisesti. [1]

2.1 Renkaat

Renkas on matemaattinen joukko, jossa on kaksi kaksipaikkaista laskutoimitusta; summa ja tulo. Laskutoimituksilta edellytetään tiettyjen laskusääntöjen noudattamista, jotka esitellään tarkemmin määritelmässä 2.1. Kokonaislukujen, reaalisten polynomien ja jatkuvien funktioiden joukot ovat kaikki renkaita, sillä niiden alkioille on määritelty summa ja tulo.

Määritelmä 2.1. Epätyhjä joukko R on rengas binääristen operaatioiden summa + ja tulo \cdot suhteen (merkitään $(R, +, \cdot)$), jos se toteuttaa seuraavat ehdot:

- (i) $(R, +)$ on Abelin ryhmä;
- (ii) (R, \cdot) on puoliryhmä;
- (iii) jokaisella $a, b, c \in S$ on voimassa $a(b + c) = ab + ac$ ja $(b + c)a = ba + ca$. Näitä kutsutaan vasemmaksi ja oikeaksi osittelulaiksi.

Huomautus.

- (i) Ei ole todettu, että renkaalla on välttämättä neutraalialkio kertolaskun suhteen. Kun näin on, identiteettiä merkitään symbolilla 1 , missä $1 \neq 0$. Rengasta R kutsutaan tällöin ykköselliseksi renkaaksi. Jotta neutraalialkio kertolaskun suhteen voidaan erottaa neutraalialkiosta yhteenlaskun suhteen, kutsutaan sitä renkaan ykkösalkioksi.
- (ii) Rengasta $R = \{0\}$ laskutoimituksilla $0 + 0 = 0 \cdot 0 = 0$ kutsutaan triviaaliksi renkaaksi tai nollarenkaaksi.
- (iii) Kun tulo on vaihdannainen, kutsutaan rengasta vaihdannaiseksi renkaaksi.

Tarkastellaan seuraavaksi renkaiden ominaisuuksia.

Lause 2.1. [1, s. 190] *Renkaalle R pätee seuraavat ominaisuudet:*

- (i) *Jokaisella $a \in R$, $a \cdot 0 = 0 \cdot a = 0$;*
- (ii) *Jokaisella $a, b \in R$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$;*
- (iii) *$-(-a) = a$;*
- (iv) *Jokaisella $a, b \in R$, $(-a)(-b) = ab$.*

Renkailla voi olla myös osajoukkoja, joita kutsutaan alirenkaiksi. Alirenkaassa tulee toteutua samat renkaiden laskusäännöt kuin siinä renkaassa, jonka osajoukko se on.

Määritelmä 2.2. Renkaan R osajoukkoa T kutsutaan renkaan R alirenkaaksi, jos $(T, +, \cdot)$ on rengas määriteltynä samojen laskutoimitusten suhteen kuin R .

Lause 2.2. [1, s. 191] *Renkaan R osajoukko T on renkaan R alirengas, jos ja vain jos*

- (i) *$T \neq \emptyset$;*
- (ii) *jos $a, b \in T$, niin $a - b \in T$;*
- (iii) *jos $a, b \in T$, niin $ab \in T$.*

Määritelmä 2.3.

- (i) *Olkoon $(R, +, \cdot)$ ykkösellinen rengas. Renkaan R alkio a on yksikkö, jos sillä on käänteisalkio a^{-1} kertolaskun suhteen renkaassa R , eli $a \cdot a^{-1} = a^{-1} \cdot a = 1$.*
- (ii) *Kommutatiivisen renkaan R alkio s on nollatekijä ja $s \neq 0$, jos on olemassa nollosteroava alkio t , jolla $st = 0$.*

2.2 Faktoriaalinen kokonaisalue

Jotta voidaan tutkia polynomien jaollisuutta, on ensin ymmärrettävä jaollisuuden käsite yleisesti renkaissa. Tässä luvussa perehdytään kokonaisalueisiin, joissa voidaan kertolaskujärjestystä vailla yksikäsitteisesti esittää mikä tahansa renkaan alkio jaottomien alkioiden tulona.

Määritellään ensiksi kokonaisalue. Kokonaisalueella tarkoitetaan kommutatiivista, ykkösellistä rengasta, jolla ei ole nollatekijää ja jolle pätevät seuraavat ehdot (ks. [3]):

1. jos $ab = 0$, niin joko $a = 0$ tai $b = 0$ jokaisella $a, b \in R$
2. jos $ab = ac$ ja $a \neq 0$, niin $b = c$ jokaisella $a, b, c \in R$
3. jos $ba = ca$ ja $a \neq 0$, niin $b = c$ jokaisella $a, b, c \in R$.

Määritellään seuraavaksi renkaan R alkioiden joukossa eräänlainen kongruenssirelaatio, minkä jälkeen osoitetaan sen olevan ekvivalenssirelaatio.

Määritelmä 2.4. Kaksi alkioita $a, b \in S$ ovat keskenään kongruentit täsmälleen silloin, kun on olemassa sellainen kääntyvä renkaan alkio $u \in R$, jolla $a = ub$. Alkioiden u joukkoa kutsutaan ekvivalenssiluokaksi ja kongruenssirelaatio on ekvivalenssirelaatio joukossa R .

Määritelmän 2.4 kongruenssirelaatio on ekvivalenssirelaatio joukossa R . Todistetaan tämä seuraavaksi.

Todistus. Osoitetaan relaation olevan ekvivalenssirelaatio.

1. Refleksiivisyys: Kongruenssin refleksiivisyys seuraa siitä, että kokonaisalueessa R on ykkösalkio 1 ja mikä tahansa alkio a kokonaisalueessa R voidaan kirjoittaa muodossa $a \cdot 1 = 1 \cdot a = a$.
2. Symmetrisyys: Olkoon a kongruentti alkion b kanssa eli $a = ub$, missä u on jokin kääntyvä alkio. Saadaan $b = u^{-1}a$, jolloin symmetrisyys on voimassa.
3. Transitivisuus: Oletetaan, että a on kongruentti alkion b kanssa ja b on kongruentti alkion c kanssa. Saadaan siis yhtälöt $a = db$ ja $b = d'c$, missä d ja d' ovat kääntyviä alkioita. Sijoitetaan nyt ensimmäiseen yhtälöön $b = d'c$, jolloin saadaan $a = (dd')c$, josta transitivisuus seuraa.

□

Nyt valitsemalla yksi alkio jokaisesta ekvivalenssiluokasta, muodostuu joukon S osajoukko C . Osajoukolla C on seuraavat ominaisuudet:

1. jokainen jaoton alkio alueella R on kongruentti jonkun osajoukon C alkion kanssa;
2. osajoukkoon C kuuluvat alkioit eivät ole milloinkaan keskenään kongruentteja.

Osajoukkoa C , jolle kyseiset ominaisuudet pätevät, voidaan myös kutsua täydelliseksi kokonaisalueen R jaottomien alkioiden edustajistoksi. On siis todistettu seuraava lause:

Lause 2.3. [1, s. 207] *Jokaisella kokonaisalueella on (mahdollisesti tyhjä) täydellinen joukko jaottomia alkioita.*

Kokonaisalue R on faktoriaalinen (unique factorization domain, UFD), jos sillä on olemassa sellainen täydellinen jaottomien alkioiden edustajisto C , että jokainen nollasta eroava alkio $a \in R$ voidaan kirjoittaa muodossa $a = up_1p_2\dots p_k$, missä u on yksikkö ja $p_i \in C$ jokaisella $i \in \{1, 2, \dots, k\}$. Esitys on myös kertolaskujärjestykselle yksikäsitteinen.

Yksi esimerkki tällaisesta kokonaisalueesta on kokonaislukujen joukko \mathbb{Z} , jossa joukoksi C voidaan valita alkulukujen joukko.

3 Polynomien jaollisuus

Luvussa 3 käsitellään polynomin määritelmää, polynomirengasta sekä polynomien jaollisuutta. Lukua käsitellään teoksen *Abstract Algebra: An Introduction to Groups, Rings and Fields* luvun 9 mukaisesti. [1]

3.1 Polynomi

Polynomi on lauseke, joka koostuu yhdestä tai useammasta termistä, kuten muuttujista ja vakioista. Useimmiten polynomi tunnetaan muodossa

$$(3.1) \quad a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n,$$

missä x on muuttuja ja kertoimet a_n , missä $n = 1, 2, 3, \dots, n-1, n$ ovat vakioita ja $a_n \neq 0$. Seuraavassa määritelmässä käydään läpi polynomin määritelmää sekä joitakin merkintätapoja.

Määritelmä 3.1. Olkoon R kommutatiivinen, ykkösellinen rengas.

(i) Muuttujan x R -kertoimista polynomia merkitään

$$(3.2) \quad a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

missä jokainen a_j on renkaan R alkio ja x on tuntematon muuttuja.

(ii) Alkiot a_j ovat polynomin kertoimia ja a_j on muuttujan x_j potenssin x^j kerroin.

(iii) Jos $a_n \neq 0$, termi a_nx^n on polynomin johtava termi ja kerroin a_n on sen johtava kerroin.

(iv) Polynomin $p(x)$ aste, merkitään $\deg p(x)$, on muuttujan x suurin potenssi, jolla on nollasta eroava kerroin. Jos kaikki polynomin kertoimet ovat nollia, sanotaan polynomin asteen olevan $-\infty$.

(v) Jos johtava kerroin on 1, polynomin sanotaan olevan pääpolynomi.

(vi) Muotoa ax^s olevaa polynomia kutsutaan monomiksi.

- (vii) Jos ei ole tärkeää tietää polynomin tarkkaa muotoa, voidaan sille käyttää merkintää $p(x)$ sekä merkintää $p(x)_j$ polynomin termin x^j kertoimelle. Polynomi $p(x)$ voidaan kirjoittaa myös muodossa

$$(3.3) \quad \sum_{j=0}^n a_j x^j = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

- (viii) Kaikkien R -kertoimisten muuttujan x polynomien joukosta käytetään merkintää $R[x]$.
- (ix) Kahden polynomin $p(x)$ ja $q(x)$ sanotaan olevan yhtä suuret, jos jokaisella j pätee $p(x)_j = q(x)_j$. Tällöin merkitään $p(x) = q(x)$.

Huomautus.

- (i) Symbolia x käytetään niin sanotusti paikkamerkkinä ja polynomin symbolit + eivät suoraan merkitse summaa. Polynomia $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ merkitään joissakin tapauksissa äärettömänä jonona renkaan R alkioita muodossa $(a_0, a_1, a_2, \dots, a_n, 0, 0, 0 \dots)$ jolloin symboleja x ja $+$ ei tarvita. Tällä merkintätavalla $(0, 1, 0, 0, 0 \dots)$ tarkoittaa polynomia $1x$, jonka merkintätapa on usein vain x .
- (ii) Mikäli haluttaisiin noudattaa täsmällisesti kohdassa (i) esitettyä merkintätapaa, tulisi polynomit kirjoittaa muodossa

$$(3.4) \quad a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + 0x^{n+1} + 0x^{n+2} + \cdots$$

sen sijaan, että ne kirjoitetaan muodossa $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, mutta nollakeroimet jätetään usein merkintätavasta pois.

- (iii) Kerroin a_0 on polynomin vakiotermi ja jokainen polynomi, jonka muut kertoimet kerrointa a_0 lukuunottamatta ovat nollia, on vakiopolynomi.
- (iv) Otetaan käyttöön seuraavanlaiset käytännöt koskien yhteenlaskuoperaatioita symbolin $-\infty$ kanssa: (äärellinen kokonaisluku) $+ -\infty = -\infty = -\infty +$ (äärellinen kokonaisluku); $-\infty + -\infty = -\infty$; $-\infty <$ mikä tahansa äärellinen kokonaisluku.

3.2 Polynomirengas

Tehdään joukosta $R[x]$ rengas määrittelemällä sille sopivat operaatiot. Polynomien joukosta muodostettua rengasta kutsutaan polynomirenkaaksi.

Määritelmä 3.2. Määritetään operaatiot $+$ ja \cdot polynomijoukolle $R[x]$ seuraavasti:

$$(3.5) \quad \sum_{j=0}^m a_j x^j + \sum_{j=0}^n b_j x^j = \sum_{j=0}^{\max(m,n)} (a_j + b_j) x^j;$$

$$(3.6) \quad \left(\sum_{j=0}^m a_j x^j \right) \left(\sum_{j=0}^n b_j x^j \right) = \sum_{j=0}^{m+n} c_j x^j, \text{ missä } c_j = \sum_{k+l=j} a_k b_l.$$

Lause 3.1. [1, s. 232] *Kolmikko $(R[x], +, \cdot)$ on kommutatiivinen rengas, jota kutsutaan polynomirenkaaksi muuttujan x suhteen renkaan R yli.*

Lause 3.2. [1, s. 233] *Jos D on kokonaisalue ja $p(x)$ sekä $q(x)$ ovat D -kertoimisia muuttujan x polynomeja, niin*

$$(3.7) \quad \deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)).$$

Todistus. (Vrt. [3], 4.1. Polynomials, Example 4)

Olkoon

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$$

ja

$$q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$$

polynomeja renkaassa D ja $a_m \neq 0$ sekä $b_n \neq 0$. Tällöin $\deg(p(x)) = m$ ja $\deg(q(x)) = n$. Nyt voidaan laskea tulo $p(x)q(x)$:

$$p(x)q(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + (a_mb_n)x^{m+n}.$$

Nyt voidaan huomata, että

$$\deg(p(x)q(x)) = m + n = \deg(p(x)) + \deg(q(x))$$

eli on osoitettu, että $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$. □

Seuraus 3.1. *Jos D on kokonaisalue, samoin on myös $D[x]$.*

Todistus. (Vrt. [1, s. 234]) Olkoot $p(x)$ ja $q(x)$ nolasta poikkeavia D -kertoimisia polynomeja. Tällöin $\deg(p(x)) \neq -\infty$ ja $\deg(q(x)) \neq -\infty$. Lauseen 3.2 nojalla $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$, ja koska kumpikin yhteenlaskettava termi on äärellinen kokonaisluku, on myös niiden summa äärellinen kokonaisluku. Tästä seuraa, että $p(x)q(x) \neq 0$, joten polynomirenkaalla $D[x]$ ei ole nolletekijöitä, joten se on kokonaisalue. \square

Huomautus. Jos R on kommutatiivinen rengas, voidaan muodostaa polynomirengas kahden tai useamman tuntemattoman muuttujan suhteen. Voidaan esimerkiksi muodostaa polynomirengas $R[x]$ ja sen jälkeen polynomirengas $(R[x])[y]$, joka koostuu polynomeista muuttujan y suhteen ja kertoimista, jotka ovat renkaan $R[x]$ alkioita. Tyypillinen alkio tällaisessa renkaassa on muotoa $\sum a_{ij}x^i y^j$, missä summa on äärellinen ja $a_{ij} \in R$. Tällaista rengasta merkitään $R[x, y]$. Seurauksen (3.1) mukaan $R[x, y]$ on kokonaisalue, jos R on kokonaisalue.

3.3 Jakoalgoritmi ja sen sovellukset

Tässä luvussa käsitellään polynomien jakoalgoritmia ja sen sovelluksia. Tästä eteenpäin F on jokin mielivaltaisesti valittu kunta ja D jokin mielivaltaisesti valittu kokonaisalue.

Apulause 3.1. [1, s. 235] Olkoon F kunta ja $b(x)$ sekä $a(x)$ F -kertoimisia polynomeja, missä $b(x) \neq 0$. Jos $\deg(a(x)) \geq \deg(b(x))$, niin on olemassa $q(x) \in F[x]$, jolle pätee

$$(3.8) \quad \deg[a(x) - b(x)q(x)] < \deg(a(x)).$$

Apulauseen todistus jätetään väliin, mutta todistuksessa hyödynnetään käänteisalkion olemassaoloa. Esitetään seuraavaksi polynomien jakoalgoritmia koskeva lause.

Lause 3.3 (Jakoalgoritmi polynomeille). *Olkoon $F[x]$ polynomirengas kunnan F yli ja olkoon $a(x), b(x) \in F[x], b(x) \neq 0$. Tällöin on olemassa yksikäsitteiset polynomit $q(x), r(x) \in F[x]$, joille pätee*

- (i) $a(x) = b(x)q(x) + r(x)$;
- (ii) $\deg(r(x)) < \deg(b(x))$. *Polynomi $(q(x))$ on osamäärä ja polynomi $r(x)$ jakojäännös, kun polynomi $b(x)$ jaetaan polynomilla $a(x)$.*

Todistus. (Vrt. [1, s. 235-236]) Olkoon $T = \{a(x) - b(x)t(x) \mid t(x) \in F[x]\}$.

1. Jos $0 \in T$, niin on $a(x) = b(x)q(x)$ jollekin polynomille $q(x) \in F[x]$. Tällöin jakojäännös on 0, jolloin $\deg(r(x)) = -\infty$. Koska $-\infty$ on pienempi kuin mikä tahansa äärellinen kokonaisluku, saadaan

$$a(x) = b(x)q(x) + r(x),$$

missä $\deg(r(x)) = \deg(0) = -\infty < \deg(b(x))$.

2. Jos $0 \notin T$, niin joukon T polynomien asteiden joukko K on ei-negatiivisten kokonaislukujen osajoukko. Tällöin hyvinjärjestysperiaatteen mukaan joukolla K on pienin alkio v ja on olemassa sellainen polynomi $q(x) \in F[x]$, että polynomin $r(x) = a(x) - b(x)q(x)$ aste on v . Jos $v \geq n = \deg(b(x))$, niin apulauseen 3.1. mukaan on olemassa sellainen polynomi $w(x) \in F[x]$, että $\deg(r(x) - b(x)w(x)) < v = \deg(r(x))$. Jos merkitään $u(x) = r(x) - b(x)w(x)$, saadaan

$$\begin{aligned} u(x) &= r(x) - b(x)w(x) \\ &= a(x) - b(x)q(x) - b(x)w(x) \\ &= a(x) - b(x)[q(x) + w(x)]. \end{aligned}$$

Syntyy ristiriita polynomin $r(x)$ pienimmän mahdollisen asteen suhteen, sillä $u(x) \in T$ ja tämän vuoksi on olemassa osamäärä ja jakojäännös, joille pätevät annetut ominaisuudet.

Oletetaan nyt, että $a(x) = b(x)q(x) + r(x) = b(x)q_1(x) + r_1(x)$, missä $\deg(r(x)) < \deg(b(x))$ ja $\deg(r_1(x)) < \deg(b(x))$. Tällöin

$$b(x)[q(x) - q_1(x)] = r_1(x) - r(x),$$

ja

$$\deg(b(x)[q(x) - q_1(x)]) = \deg(b(x)) + \deg(q(x) - q_1(x)) = \deg(r_1(x) - r(x)).$$

Tästä saadaan $(q(x) - q_1(x)) = \deg(r_1(x) - r(x)) - \deg(b(x)) < 0$, sillä $\deg(r_1(x) - r(x)) < \deg(b(x))$. Tällöin siis $\deg(q(x) - q_1(x)) = -\infty$, josta seuraa $q_1(x) - q(x) = 0$, joten $q_1(x) = q(x)$. Kaavasta (3.9) voidaan päätellä, että $r_1(x) = r(x)$. Siis yksikäsitteisyys on osoitettu.

□

Esitetään seuraavaksi lause Eukleideen jakoalgoritmista polynomeille polynomi-
renkaassa $F[x]$.

Lause 3.4 (Eukleideen jakoalgoritmi polynomeille). [2, s. 121] *Olkoon $f(x)$ ja $g(x)$ nollasta eroavia polynomeja polynomirenkaassa $F[x]$. Hyödynnetään lauseen 3.3 jakoalgoritmia, kunnes jakojäännös on 0 tai jakoa ei voida enää jatkaa.*

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

Nyt siis $\text{syt}(f(x), g(x)) = r_n(x)$. Jakojäännös on $r(x) = 0$ ja osamäärä on $q(x) = q_{n+1}(x)$.

Esimerkki 3.1. Olkoon $f(x) = x^2 + 6x - 5$ ja $g(x) = x^2 + 3x + 1$. Etsitään polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä käyttämällä Eukleideen algoritmia. Määritetään myös osamäärä $q(x)$ ja jakojäännös $r(x)$.

Lauseesta 3.3. seuraa, että on olemassa yksikäsitteiset polynomit $a(x), b(x)$, joille pätee $a(x) = b(x)q(x) + r(x)$, missä $q(x)$ on osamäärä ja $r(x)$ on jakojäännös. Eukleideen algoritmilla voidaan määrittää molemmat. Saadaan

$$\begin{aligned} x^2 + 6x - 5 &= 1 \cdot (x^2 + 3x + 1) + (3x - 6) \\ x^2 + 3x + 1 &= (3x - 6)\left(\frac{1}{3}x + 2\right) + 13. \end{aligned}$$

Koska jakoa ei voida enää jatkaa, niin polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä on polynomi $3x - 6$. Osamäärä on $q(x) = \frac{1}{3}x + 2$ ja jakojäännös on $r(x) = 13$.

Lause 3.5. *Polynomi $p(x)$ on polynomirenkaan $F[x]$ yksikkö, jos ja vain jos $p(x)$ on nollasta eroava vakiopolynomi.*

Todistus. (Vrt. [1, s. 236]) Jos $p(x)$ on yksikkö, niin on olemassa polynomi $q(x)$, jolle pätee $p(x)q(x) = 1$. Nyt lauseen 3.2 nojalla saadaan

$$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)) = \deg(1) = 0,$$

josta edelleen

$$\begin{aligned} \deg(p(x)) + \deg(q(x)) &= 0 \\ \deg(p(x)) &= -\deg(q(x)) \end{aligned}$$

Koska minkään polynomin aste ei voi olla negatiivinen kokonaisluku, niin ainoa vaihtoehto on, että $\deg(p(x)) = \deg(q(x)) = 0$, jolloin molemmat ovat nollasta eroavia vakiopolynomeja. Todistus on toiseen suuntaan triviaali, sillä jokainen nollasta eroava vakiopolynomi a on yksikkö, jonka käänteisalkio on a^{-1} . \square

Määritelmä 3.3. Polynomi $a(x) \neq 0$ jakaa polynomin $b(x)$ polynomirenkaassa $F[x]$, jos on olemassa sellainen polynomi $q(x) \in F[x]$, jolle $b(x) = a(x)q(x)$. Tätä merkitään $a(x)|b(x)$. Polynomia $a(x)$ sanotaan polynomin $b(x)$ jakajaksi.

Lause 3.6. *Olkoon $a(x)$, $b(x)$ ja $c(x)$ polynomeja joukossa $F[x]$. Tällöin*

- (i) jos $a(x)|b(x)$ ja $b(x)|a(x)$, niin $a(x) = ub(x)$, missä u on nollasta poikkeava alkio joukossa F ;
- (ii) 0 on ainoa polynomi, joka voidaan jakaa kaikilla nollasta poikkeavilla polynomeilla;
- (iii) jos $a(x)|b(x)$ ja $b(x)|c(x)$, niin $a(x)|c(x)$;
- (iv) jos $a(x)|b(x)$, niin $ua(x)|vb(x)$ kaikille yksiköille u ja v ;
- (v) jos $a(x)|b(x)$ ja $a(x)|c(x)$, niin $a(x)|(\pm b(x) \pm c(x))$;
- (vi) jos $a(x)|b(x)$ ja $a(x)|(\pm b(x) \pm c(x))$, niin $a(x)|c(x)$.

Todistus. (Vrt. [1, s. 237])

- (i) Olkoon $b(x) = a(x)q(x)$ ja $a(x) = b(x)s(x)$. Tällöin

$$b(x) = b(x)s(x)q(x).$$

Koska $b(x) \neq 0$ ja $F[x]$ on kokonaisalue, voidaan yhtälön molemmat puolet supistaa polynomilla $b(x)$, jolloin saadaan $s(x)q(x) = 1$. Tällöin sekä $s(x)$ että $q(x)$ ovat molemmat yksikköjä, esimerkiksi $s(x) = u$ ja $q(x) = v$, missä $u, v \in F$, joka seuraa lauseesta 3.5. Siis $a(x) = ub(x)$ eli polynomi $a(x)$ on polynomin $b(x)$ vakioterminen monikerta.

- (ii) Olkoon $a(x)$ jokin nollasta poikkeava polynomi. Tällöin $a|0 = 0$, joka seuraa yhtälöstä $0 = a(x) \cdot 0$ sekä jaollisuuden määritelmästä.
- (iii) Olkoon $b(x) = a(x)q(x)$ ja $b(x) = c(x)s(x)$. Saadaan $a(x)q(x) = c(x)s(x)$ ja edelleen $va(x) = uc(x)$ eli pätee myös $a(x)|c(x)$.

(iv) Koska $a(x)|b(x)$, pätee $b(x) = a(x)q(x)$ jollakin polynomilla $q(x) \in F[x]$ ja edelleen $vb(x) = ua(x)[u^{-1}vq(x)]$, mikä osoittaa, että $ua(x)|vb(x)$.

(v) Olkoon $b(x) = a(x)q(x)$ ja $c(x) = a(x)s(x)$ joillakin polynomeilla $q(x), s(x) \in F[x]$. Halutaan osoittaa, että $a(x)|(b(x) + c(x))$. Nyt saadaan

$$\begin{aligned} b(x) + c(x) &= a(x)q(x) + a(x)s(x) \\ &= a(x)(q(x) + s(x)) \end{aligned}$$

Huomataan, että $a(x)$ on polynomien summan $b(x) + c(x)$ tekijä, eli $a(x)|(b(x) + c(x))$. Vastaava todistus voidaan tehdä myös silloin, kun tarkastellaan relaatiota $a(x)|(-b(x) - c(x))$.

(vi) Oletetaan, että polynomi $a(x)$ jakaa polynomit $b(x)$ ja $b(x) + c(x)$. Tällöin $b(x) = q(x)a(x)$ ja $b(x) + c(x) = s(x)a(x)$ joillakin polynomeilla $q(x), s(x) \in F[x]$. Sijoitetaan nyt polynomi $b(x)$ jälkimmäiseen polynomiin.

$$\begin{aligned} b(x) + c(x) &= s(x)a(x) \\ q(x)a(x) + c(x) &= s(x)a(x) \\ c(x) &= s(x)a(x) - q(x)a(x) \\ &= a(x)(s(x) - q(x)) \end{aligned}$$

Huomataan, että $a(x)$ on polynomin $c(x)$ tekijä eli $a(x)|c(x)$. Vastaava todistus voidaan tehdä myös silloin, kun tarkastellaan relaatiota $a(x)|(-b(x) - c(x))$.

□

Seuraus 3.2. Jos $p(x)|q(x)$, $q(x)|p(x)$ ja molemmat $p(x)$ ja $q(x)$ ovat pääpolynomeja sekä molempien polynomien aste on vähintään 1, niin $p(x) = q(x)$.

Lause 3.7. [1, s. 238] Jos F on kunta, niin $F[x]$ on pääideaalirengas (principal ideal domain, PID). Sen lisäksi, jos I on renkaan $F[x]$ nollasta poikkeava ideaali, niin on olemassa yksikäsitteinen pääpolynomi $m(x)$, jolle pätee $I = \langle m(x) \rangle$.

Määritelmä 3.4. Olkoot $a(x)$ ja $b(x)$ sellaisia polynomeja yli kunnan F , että vähintään toinen niistä eroaa nollapolynomista. Pääpolynomi $d(x)$ on polynomien $a(x)$ ja $b(x)$ suurin yhteinen tekijä, jos

(i) $d(x)|a(x)$ ja $d(x)|b(x)$;

(ii) jos $s(x)|a(x)$ ja $s(x)|b(x)$, niin $s(x)|d(x)$.

Lause 3.8. [1, s. 239] Jos $a(x)$ ja $b(x)$ ovat sellaisia polynomeja yli kunnan F yli, että vähintään toinen niistä eroaa nollapolynomista, niin polynomien $a(x)$ ja $b(x)$ suurin yhteinen tekijä (syt) on olemassa ja se on yksikäsitteinen. Sen lisäksi yhtälö

$$(3.9) \quad \text{sy}(a(x), b(x)) = p(x)a(x) + q(x)b(x)$$

on voimassa joillakin polynomeilla $p(x)$ ja $q(x)$.

3.4 Jaottomuus ja polynomien tekijöihin jako

Tässä luvussa todistetaan aritmetiikan peruslausetta vastaava tulos polynomeille. Todistukset, jotka johtavat teoriaan polynomeille, ovat perusidealtaan lähes identtiset verrattuna kokonaisluvuille vastaaviin todistuksiin.

Määritelmä 3.5. Polynomien $p(x)$ kunnan F yli sanotaan olevan *jaoton* kunnan F yli, jos polynomien $p(x)$ aste on positiivinen ja sitä ei voida jakaa tekijöihin kahden F -kertoimisen polynomien, joiden kummankin aste on vähintään 1, avulla. Jos polynomien $p(x)$ aste on positiivinen ja se ei ole jaoton, sen sanotaan olevan jaollinen.

Määritelmä 3.6. Kahden polynomien $p(x)$ ja $q(x)$ sanotaan olevan keskenään jaottomia, jos niiden suurin yhteinen tekijä on 1.

Lause 3.9. [1, s. 242] Olkoon $a(x)$, $b(x)$, $c(x)$ F -kertoimisia polynomeja kunnan F yli. Jos $a(x)|b(x)c(x)$ ja $a(x)$ on keskenään jaoton polynomien $b(x)$ kanssa, niin $a(x)|c(x)$.

Seuraus 3.3. Jos $p(x)$ on jaoton kunnan F yli ja $p(x)|b(x)c(x)$, niin pätee joko $p(x)|b(x)$ tai $p(x)|c(x)$.

Todistus. (Vrt. [1, s. 74]) Oletetaan, että $p(x)$ on jaoton eli $p(x)$ ei jaa polynomeja $b(x)$. Olkoot $r(x)$ ja $s(x)$ sellaiset polynomit, että $b(x) = p(x)s(x) + r(x)$ ja $\deg(r(x)) < \deg(p(x))$. Voidaan olettaa, että $r(x) \neq 0$, sillä muussa tapauksessa polynomi $p(x)$ jakaa polynomien $b(x)$ ja väitteen implikaatio on tosi. Tällöin $d(x) = \text{sy}(p(x), b(x))$ on polynomien $p(x)$ jakaja ja $p(x)$ on jaoton, joten suurimman yhteisen tekijän on oltava joko 1 tai $p(x)$. Koska se ei voi olla $p(x)$, on sen oltava

1. Tällöin $p(x)$ ja $b(x)$ ovat keskenään jaottomia. Lauseen 3.8 nojalla on olemassa polynomit $h(x)$ ja $g(x)$, joille pätee

$$h(x)p(x) + g(x)b(x) = 1.$$

Toisaalta

$$h(x)p(x)c(x) + g(x)b(x)c(x) = c(x).$$

Saadaan $p(x)|g(x)p(x)c(x)$ ja $p(x)|g(x)b(x)c(x)$, sillä $p(x)|b(x)c(x)$, josta edelleen

$$c(x) = p(x)(h(x)c(x) + g(x)q(x)),$$

missä $q(x)$ on se osamäärä, joka saadaan, kun polynomi $b(x)c(x)$ jaetaan polynomilla $p(x)$. Tästä saadaan $p(x)|c(x)$. Vastaava todistus voidaan tehdä myös sille, että todistetaan $p(x)|b(x)$. \square

Lause 3.10. [1, s. 243] *Jokainen polynomi kunnan F yli, jonka aste on positiivinen, voidaan kirjoittaa yksikäsitteisesti jaottomien pääpolynomien tulona.*

Yleisesti ottaen on hankalaa selvittää, onko annettu polynomi jaoton mielivaltaisen kunnan yli vai ei. On kuitenkin olemassa helposti sovellettavissa oleva kriteeri, jos polynomin aste on 2 tai 3 ja on olemassa yksi tarvittava olosuhde sille, että polynomi on jaoton rationaalilukujen kunnan yli. Voidaan myös todistaa, että reaalilukujen kunnan yli kaikki jaottomat polynomit ovat astetta 1 tai 2. Vastaavasti kompleksilukujen kunnan yli kaikki jaottomat polynomit ovat astetta 1. Muissa tapauksissa jaottomuuden todistamiseksi on hyödynnettävä polynomien jakamiseen tarkoitettuja metodeja.

Määritelmä 3.7. Kommutatiivisen renkaan R alkio b on polynomin $a(x) \in R[x]$ juuri renkaan R , yli jos $a(b) = 0$. Sanotaan myös, että b on polynomin $a(x)$ nollakohta.

Lause 3.11. [1, s. 245] *Jos $a(x)$ on polynomi kunnan F yli ja b on kunnan F alkio, niin jakojäännös, kun $a(x)$ jaetaan polynomilla $x - b$, on $a(b)$. Erityisesti b on polynomin $a(x)$ juuri, jos ja vain jos $x - b$ on polynomin $a(x)$ tekijä.*

Esimerkki 3.2. Olkoon $a(x) = x^2 + 3x - 4$ toisen asteen polynomi ja $b = 2$ ja $b = 7$ sen nollakohdat. Lauseen 3.11. nojalla polynomi $a(x)$ on jaollinen polynomeilla $x - 2$ ja $x - 7$.

Seuraus 3.4. Jos F -kertoimisella polynomilla, jonka aste on suurempaa kuin 1, on juuri kunnassa F , polynomi on jaollinen. Sen lisäksi polynomi, jonka aste on 2 tai 3, kunnan F yli on jaoton kunnan F yli, jos ja vain jos sillä ei ole juurta kunnassa F .

Todistus. (Vrt. [1, s. 246]) Oletetaan, että polynomien $p(x)$ aste on suurempi kuin 1 ja että sillä on olemassa juuri $b \in F$. Lauseen 3.11. mukaan $x - b$ on polynomien $p(x)$ tekijä. Koska $\deg(p(x)) > 1$, polynomien $p(x)$ toisen tekijän aste on oltava positiivinen, jolloin $p(x)$ on jaollinen.

Oletetaan nyt, että polynomi $p(x)$ on jaollinen ja sen aste on 2 tai 3. Merkitään $p(x) = s(x)t(x)$, missä $s(x)$ ja $t(x)$ ovat positiivista astetta olevia polynomeja. Tällöin $\deg(p(x)) = \deg(s(x)) + \deg(t(x))$, ja koska polynomien $p(x)$ aste on 2 tai 3, siitä seuraa, että joko polynomien $s(x)$ tai polynomien $t(x)$ aste on 1, esimerkiksi polynomien $s(x)$ on oltava muotoa $s(x) = cx + d$. Tällöin $-c^{-1}d$ on polynomien $p(x)$ juuri. \square

Seuraus 3.5. Jos $f(x)$ on polynomi kunnan F yli ja astetta $n \geq 0$, niin laskien mukaan monikerrat, polynomilla $f(x)$ on korkeintaan n juurta kunnassa F .

Määritelmä 3.8. Polynomien, jonka kertoimet kuuluvat kokonaislukujen joukkoon, sanotaan olevan primitiivinen, jos mikään alkuluvuista ei ole kaikkien sen kertoimien tekijä.

Huomautus. Jokainen \mathbb{Z} -kertoiminen polynomi voidaan kirjoittaa kokonaisluvun ja primitiivisen polynomien tulona ottamalla yhteiseksi tekijäksi kertoimien suurin yhteinen tekijä.

Esimerkki 3.3. Polynomi $2x^2 + 7x + 2$ on primitiivinen, sillä mikään alkuluvuista ei jaa kertoimia 2 ja 7. Polynomi $4x^2 + 14x + 4$ ei ole primitiivinen, sillä kertoimet 4 ja 14 voidaan jakaa jollain alkuluvulla, eli tässä tapauksessa alkuluvulla 2. Polynomi voidaan kuitenkin kirjoittaa muodossa $2(2x^2 + 7x + 2)$, missä $2x^2 + 7x + 2$ on primitiivinen polynomi.

Lause 3.12. [1, s. 249] Kahden primitiivisen polynomien tulo on myös primitiivinen polynomi.

Esimerkki 3.4. Tarkastellaan primitiivisiä polynomeja $a(x) = x^2 + 3x - 5$ ja $b(x) = 3x^2 - x + 7$. Polynomien tulo $c(x) = a(x)b(x) = (x^2 + 3x - 5)(3x^2 - x + 7) = 3x^4 + 8x^3 - 9x^2 + 26x - 35$ on myös primitiivinen polynomi, sillä mikään alkuluvuista ei jaa kaikkia kertoimia 3, 8, -9, 26 ja -35.

Apulause 3.2. [1, s. 249] Jos $p(x)$ ja $q(x)$ ovat primitiivisiä polynomeja ja $mp(x) = nq(x)$, missä m ja n ovat kokonaislukuja, niin $p(x) = \pm q(x)$.

Lause 3.13 (Gaussin lemma). Jos $a(x)$ on primitiivinen polynomi, jonka kertoimet ovat kokonaislukuja ja $a(x) = b(x)c(x)$, missä $b(x)$ ja $c(x)$ ovat \mathbb{Q} -kertoimisia polynomeja, niin on olemassa sellaiset kokonaislukukertoimiset polynomit $B(x)$ ja $C(x)$, että $a(x) = B(x)C(x)$. Sen lisäksi $B(x)$ ja $C(x)$ ovat vakiomoninkertoja polynomeille $b(x)$ ja $c(x)$ tässä järjestyksessä.

Todistus. (Vrt. [1, s. 249-250]) Voidaan olettaa, että $a(x)$ on primitiivinen polynomi. Olkoot h ja k kertoimien $b(x)$ ja $c(x)$ nimittäjien pienimpiä yhteisiä monikertoja eli jaettavia (pyj) tässä järjestyksessä. Tällöin

$$hb(x) = \hat{b}(x) \in \mathbb{Z}[x] \text{ ja } kc(x) = \hat{c}(x) \in \mathbb{Z}[x].$$

Määritelmän 3.8. jälkeisen huomautuksen perusteella voidaan kirjoittaa $\hat{b}(x) = mB(x)$ ja $\hat{c}(x) = nC(x)$, missä m ja n ovat kokonaislukuja ja $B(x)$ ja $C(x)$ ovat primitiivisiä polynomeja. Tällöin

$$a(x) = \frac{mn}{kh}B(x)C(x)$$

ja edelleen

$$kha(x) = mnB(x)C(x),$$

missä $B(x)C(x)$ on primitiivinen polynomi lauseen 3.12. mukaan ja polynomi $a(x)$ on primitiivinen alkuoletuksen mukaan.

Apulauseen 3.2. mukaan $a(x) = \pm B(x)C(x)$, joka on joko $a(x) = B(x)C(x)$ tai $a(x) = -B(x)C(x)$. Jälkimmäisen tapauksessa voidaan merkitä $-B(x) = B'(x)$, jolloin saadaan $a(x) = B'(x)C(x)$ ja lause on todistettu. \square

Gaussin lemma voidaan esittää myös suppeammin seuraavassa muodossa: jos \mathbb{Z} -kertoiminen polynomi voidaan jakaa tekijöihin \mathbb{Q} -kertoimisten polynomien avulla, niin se voidaan jakaa myös tekijöihin \mathbb{Z} -kertoimisten polynomien avulla.

Lause 3.14 (Eisensteinin kriteeri jaottomuudelle). [1, s. 250] Olkoon $a(x) = \sum_{j=0}^n a_j x^j$ polynomi, missä $a_j \in \mathbb{Z}$ kaikilla $j = 0, 1, \dots, n-1, n$, jolla on seuraavat ominaisuudet:

- (i) On olemassa jokin alkuluku p , jolla $p|a_j$ kaikilla $j = 0, 1, \dots, n-1$, mutta alkuluku p ei ole kertoimen a_n tekijä.

(ii) p^2 ei ole kertoimen a_0 tekijä. (Siis $a_0 \neq 0$).

Tällöin polynomi $a(x)$ on jaoton \mathbb{Q} -kertoimisilla polynomeilla.

Esimerkki 3.5. Tutkitaan, mitkä seuraavista polynomeista ovat jaottomia \mathbb{Q} -kertoimisilla polynomeilla:

1. $3x^3 - 2x^2 + 4x - 2$,

2. $2x^3 + 3x^2 + 3x - 3$,

Tarkastellaan polynomeja Eisensteinin kriteerin avulla.

1. Eisensteinin kriteerin molemmat kohdat pätevät polynomille, sillä on olemassa alkuluku p , joka jakaa kertoimet a_0, a_1 ja a_2 , mutta ei jaa kerrointa a_3 , eli alkuluku 2. Luku $p^2 = 2^2 = 4$ ei myöskään ole kertoimen $a_0 = 2$ tekijä. Siis Eisensteinin kriteerin mukaan polynomi on jaoton \mathbb{Q} -kertoimisilla polynomeilla.
2. Eisensteinin kriteerin molemmat kohdat pätevät polynomille, sillä on olemassa alkuluku p , joka jakaa kertoimet a_0, a_1 ja a_2 , mutta ei jaa kerrointa a_3 , eli alkuluku 3. Luku $p^2 = 3^2 = 9$ ei myöskään ole kertoimen $a_0 = 3$ tekijä. Eisensteinin kriteerin mukaan polynomi on jaoton \mathbb{Q} -kertoimisilla polynomeilla.

Lause 3.15. [1, s. 254] Jos $a(x)$ on \mathbb{R} -kertoiminen polynomi siten, että se on jaoton reaalilukujen joukon \mathbb{R} yli, se on joko lineaarinen tai neliöllinen.

Lause 3.16. [1, s. 254] Reaalipolynomi $ax^2 + bx + c$ on jaoton reaalilukujen joukon \mathbb{R} yli, jos ja vain jos $b^2 - 4ac < 0$.

Lause 3.17. [1, s. 255] Jokainen positiivista astetta oleva reaalipolynomi voidaan yksikäsitteisesti kirjoittaa nollasta poikkeavan reaaliluvun ja lineaarisen pääpolynomin tai jaottoman neliöllisen polynomin tekijöiden tulona.

Esimerkki 3.6. Tutkitaan polynomeja $a(x) = x^3 - 1$ ja $b(x) = x^8 - 1$. Tutkitaan sitä, miten polynomit $a(x)$ ja $b(x)$ voitaisiin esittää jaottomien polynomien tulona renkaassa $\mathbb{R}[x]$ ja renkaassa $\mathbb{C}[x]$.

Tutkitaan ensin polynomia $a(x) = x^3 - 1$. Polynomi voidaan jakaa tekijöihin seuraavasti: $a(x) = x^3 - 1 = (x - 1)(x^2 + x + 1)$. Tällöin sen juuriksi saadaan $x = 1$,

$x = -\frac{1}{2} + \sqrt{3}\frac{1}{2}i$ ja $x = -\frac{1}{2} + \sqrt{3}(-\frac{1}{2}i)$. Siis renkaassa $\mathbb{R}[x]$ polynomi voidaan esittää jaottomien polynomien tulona muodossa

$$a(x) = (x - 1)(x^2 + x + 1)$$

ja renkaassa $\mathbb{C}[x]$ muodossa

$$a(x) = (x - 1)(x + (\frac{1}{2} + \sqrt{3}\frac{1}{2}i))(x + (\frac{1}{2} + \sqrt{3}(-\frac{1}{2}i))).$$

Polynomi $b(x) = x^8 - 1$ voidaan jakaa tekijöihin seuraavasti: $b(x) = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$. Tällöin sen juuriksi saadaan $x = 1$, $x = -1$, $x = i$, $x = -i$, $x = \sqrt{2}(-\frac{1}{2} - \frac{1}{2}i)$, $x = \sqrt{2}(-\frac{1}{2} + \frac{1}{2}i)$, $x = \sqrt{2}(\frac{1}{2} - \frac{1}{2}i)$ ja $x = \sqrt{2}(\frac{1}{2} + \frac{1}{2}i)$. Renkaassa $\mathbb{R}[x]$ polynomi voidaan siis esittää jaottomien polynomien tulona muodossa

$$b(x) = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$$

ja renkaassa $\mathbb{C}[x]$ se voidaan esittää muodossa

$$b(x) = (x - 1)(x + 1)(x - i)(x + i)(\sqrt{2}(-\frac{1}{2} - \frac{1}{2}i))(\sqrt{2}(-\frac{1}{2} + \frac{1}{2}i))(\sqrt{2}(\frac{1}{2} - \frac{1}{2}i))(\sqrt{2}(\frac{1}{2} + \frac{1}{2}i)).$$

Lähteet

- [1] Reis, C. *Abstract algebra: An introduction to Groups, Rings and Fields*. Singapore: World Scientific, 2011.
- [2] Nicodemi, O.E., Sutherland, M.A. ja Towsley, G.W. *An Introduction to Abstract Algebra with Notes to the Future Teacher* New Jersey, Pearson Education, Inc., 2007.
- [3] Nicholson, W. Keith. *Introduction to Abstract Algebra*. 4th ed. Calgary, Alberta, Canada: University of Calgary, 2012. Print.