TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Jukka Vilen

Polynomirenkaista

Informaatiotieteiden tiedekunta
Matematiikan, tilastotieteen ja filosofian laitos
Matematiikka
Kesäkuu 2005

Tampereen yliopisto
Matematiikan, tilastotieteen ja filosofian laitos

VILEN, JUKKA: Polynomirenkaista
Pro gradu -tutkielma, 35s
Matematiikka
Kesäkuu 2005

Tiivistelmä

Polynomit ja niiden nollakohdat ovat olleet jo varhainen kohde matematiikan historiassa. Tämän työn tarkoituksena on tutkia polynomien muodostamaa joukkoa, tämän joukon ominaisuuksia ja koota yhteen teoreettinen perusta niillekin tiedoille polynomeista, jotka lukiossa on vain otettu käyttöön ilman tarkempaa käsittelyä vaativien todistusten vuoksi.

Työssä tutkitaan kaikkien polynomien muodostamaa rengasta ja sen ominaisuuksia, polynomien nollakohtia, jaollisuutta ja suurimpia yhteisiä tekijöitä sekä rationaalilukuja, reaalilukuja ja kompleksilukuja polynomirenkaiden kerroinrenkaina.

Polynomien tekijöihinjako, jaollisuus yleensä ja polynomit eri kerroin renkailla sisältävät mielenkiintoisia tuloksia. Esimerkiksi jokainen reaalilukukertoiminen polynomi voidaan jakaa ensimmäisen ja toisen asteen tekijöihin riippumatta siitä, onko polynomilla reaaliluku vai kompleksilukunollakohtia. Lukijalta vaaditaan lukion perustiedot sekä muutaman todistuksen osalta perustietoja algebrasta, kompleksilukulaskennasta ja lukuteoriasta.

Sisältö

Johdanto

Polynomien historiaa

Polynomilaskennalla on pitkä historia. Egyptiläisten tiedetään ratkoneen polynomiyhtälöitä jo 1650 eKr. Vuonna 600 eKr. hindut olivat oppineet ratkaisemaan neljännen asteen yhtälöitä. Kuitenkin polynomien nykyinen kirjoitusasu tuli tutuksi vasta 1700-luvulla. Likimain vuonna 400 jKr. Intiassa ja Arabimaissa algebran symbolit alkoivat esiintyä tuon ajan matemaattisissa kirjoituksissa. [2, s. 335]

Työstä

Monilla matematiikan osa-alueilla polynomit ovat tärkeässä roolissa. Tämän työn tarkoituksena on esittää polynomilaskennan ominaisuuksia laajemmassa mittakaavassa. Tutumman analyyttisen polynomien merkintätavan $2x^3 - 3x + 5$ ohella tässä työssä käytetään myös algebrallisen lähdekirjallisuuden suosimaa merkintää $(5, 3, 0, 2, 0, 0, \ldots)$. Merkintätavassa $2x^3 - 3x + 5$ merkki x ei ole analyyttiseen tapaan muuttujan roolissa, vaan merkin x eri potenssit merkataan selvittämään kertoimen sijaintia polynomissa. Myös monet lukiomatematiikan parissa opitut menetelmät ja tiedot polynomien nollakohtien etsimisestä ja ratkaisemisesta voidaan perustella algebran avulla.

Algebran kannalta polynomien joukko on monessa suhteessa hyvä esimerkki, esimerkiksi reaalilukukertoimisten polynomien joukko tekijöihinjaon vuoksi.

Työ noudattaa pääasiassa lähdekirjallisuudesta teoksen [1] järjestystä ja mittavaa sisältöä polynomirenkaiden läpikäynnissä, minkä lisäksi muusta kirjallisuudesta on lisätty todistuksia ja selkeitä perustietoja.

Työssä merkintöjen kannalta on tärkeä nähdä merkintöjen R ja $\mathbb{R}$ ero. Merkinnöistä R tarkoittaa yleistä lukujoukkoa, kun $\mathbb{R}$ tarkoittaa erityisesti reaalilukujen joukkoa. Vastaavasti kokonais-, rationaali- ja kompleksilukujen joukoille käytetään merkintöjä $\mathbb{Z}$, $\mathbb{Q}$ ja $\mathbb{C}$. Samaan tapaan merkitään myös luonnollisten lukujen joukkoa $\mathbb{N}$, johon kuuluu myös nolla. Tämä siksi, että työssä ei tarvita erikseen luonnollisten lukujen joukkoa, mihin nolla ei kuulu ja lisäksi tällöin voitaisiin käyttää positiivisten kokonaislukujen joukkoa $\mathbb{Z}_+$.

Lukijalta vaaditaan lukion perustiedot sekä muutaman todistuksen osalta perustietoja algebrasta, kompleksilukulaskennasta ja lukuteoriasta.

Tampereella, kesäkuussa 2005
Jukka Vilen

Luku 1

Esitiedot

1.1 Renkaat ja niiden ominaisuuksia

Määritelmä 1.1.1 *Rengas on epätyhjän joukon R ja kahden laskutoimituksen $+$ ja $\cdot$ muodostama järjestetty kolmikko $(R, +, \cdot)$, joka toteuttaa seuraavat aksioomat:*

(R1) $(a + b) + c = a + (b + c)$ $\forall$ a, b, $c \in R$.

(R2) $a + b = b + a$ $\forall$ a, $b \in R$.

(R3) Joukossa R on olemassa alkio 0 siten, että $a + 0 = a$ $\forall$ $a \in R$.

(R4) Kaikille alkioille $a \in R$ on olemassa vasta-alkio $-a \in R$ siten, että

$$a + (-a) = 0.$$

(R5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall$ a, b, $c \in R$.

(R6) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ $\forall$ a, b, $c \in R$.

(R7) $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ $\forall$ a, b, $c \in R$.

[2, s. 270]

Yleisimmin tunnettuja renkaita ovat $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$.

Määritelmä 1.1.2 *Rengas R on kommutatiivinen, jos $ab = ba \ \forall \ a, b \in R$. [2, s. 270]*

Määritelmä 1.1.3 *Olkoon R ykkösalkion sisältävä kommutatiivinen rengas. Jos renkaalla R ei ole nollanjakajia, niin R on kokonaisalue.*

Renkaan R alkiota $a \neq 0$ kutsutaan nollajakajaksi, jos on olemassa sellainen renkaan R alkio $b \neq 0$, että joko $ab = 0$ tai $ba = 0$.

Määritelmä 1.1.4 *Kunta on ykkösalkion sisältävä kommutatiivinen rengas, jossa kaikilla nolla-alkiosta poikkeavalla alkiolla käänteisalkio. [2, s. 274]*

1.2 Kompleksilukulaskentaa

Määritelmä 1.2.1 *Kun kompleksiluku $c = a + bi$, niin luvun c konjugaatti määritellään $\overline{z} = a - bi$. Tällöin ovat voimassa muun muassa seuraavat laskusäännöt:*

1. $\overline{z + w} = \overline{z} + \overline{w}$
2. $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.

Liouvillen lause 1.2.2 *Olkoon funktio f holomorfinen ja rajoitettu kompleksitasossa $\mathbb{C}$. Tällöin f on vakio.*

Todistus. Ks. [3, s. 65]

Luku 2

Polynomirengas

2.1 Kaikkien polynomien joukko $R[x]$

Määritelmä 2.1.1 *Renkaan R alkioiden jonoa $(a_0, a_1, a_2, \ldots)$ voidaan pitää polynomina, jos on olemassa ei-negatiivinen kokonaisluku n siten, että $a_k = 0$ kaikilla $k > n$. Kokonaisluku n ei ole vakio, vaan sen arvo riippuu polynomista. Kaikkien tällaisten polynomien joukkoa merkitään $R[x]$. Polynomin $(a_0, a_1, a_2, \ldots)$ jokaista kerrointa a_k $(k \geq 0)$ kutsutaan polynomin k:nneksi kertoimeksi. Kaksi polynomia $(a_0, a_1, a_2, \ldots)$ ja $(b_0, b_1, b_2, \ldots)$ ovat yhtä suuret, jos kaikilla kertoimen k arvoilla $a_k = b_k$.*

Lause 2.1.2 *Joukko $R[x]$ on ykkösalkion sisältävä kommutatiivinen rengas, jolla on renkaan R kanssa isomorfinen alirengas.*

Todistus. [1, s. 279] Valitaan joukosta $R[x]$ polynomit (a_k), (b_k) ja (c_k). Yhteenlasku on suljettu, sillä $(a_k) + (b_k) = (a_k + b_k)$ on selvästi joukon $R[x]$ polynomi. Yhteenlasku on hyvinmääritelty laskuoperaatio joukossa $R[x]$, koska summa on hyvinmääritelty renkaassa R. Yhteenlasku on assosiatiivinen, sillä

$$\begin{aligned}(a_k) + [(b_k) + (c_k)] &= (a_k) + (b_k + c_k) \\ &= (a_k + [b_k + c_k]) \\ &= ([a_k + b_k] + c_k)\end{aligned}$$

$$
\begin{aligned}
&= (a_k + b_k) + (c_k) \\
&= [(a_k) + (b_k)] + (c_k).
\end{aligned}
$$

Yhteenlaskun neutraalialkio on nollapolynomi $(0) = (0, 0, 0, \ldots)$ ja alkio (a_k) vasta-alkio on $(-a_k)$. Koska yhteenlasku on selvästi kommutatiivinen, niin $R[x]$ on yhteenlaskun suhteen Abelin ryhmä. Voidaan osoittaa, että polynomien kertolasku on joukossa $R[x]$ hyvinmääritelty laskutoimitus, joten joukon $R[x]$ todistamiseksi renkaaksi tarvitsee osoittaa, että polynomien kertolasku on assosiatiivinen ja distributiivinen polynomien yhteenlaskun suhteen. Polynomien kertolaskun assosiatiivisuuden osoittamiseksi tutkitaan tuloa $(a_k)[(b_k)(c_k)]$. Tulon $(b_k)(c_k)$ m:nnen kertoimen selvittämiseksi lasketaan yhteen kaikki mahdolliset tulot $b_j c_k$, missä $j + k = m$. Tällöin tulon $(b_k)(c_k)$ m:s kerroin saadaan muotoon

$$\sum_{j+k=m} b_j c_k.$$

Puolestaan tulon $(a_k)[(b_k)(c_k)]$ n:nnen kertoimen selvittämiseksi lasketaan nyt yhteen kaikki muotoa $a_i \left(\sum_{j+k=m} b_j c_k \right)$ olevat tulot, missä $i + m = n$. Näin n:s kerroin saadaan muotoon

$$\sum_{i+m=n} \left[a_i \left(\sum_{j+k=m} b_j c_k \right) \right].$$

Toisaalta $j+k = m$, jolloin $i+j+k = n$. Lisäksi renkaan R distributiivisuutta käyttämällä tulo $\sum_{i+m=n} \left[a_i \left(\sum_{j+k=m} b_j c_k \right) \right]$ saadaan muotoon

$$\sum_{i+j+k=n} a_i (b_j c_k).$$

Tulon $(a_k)[(b_k)(c_k)]$ n:s kerroin on siis muodoltaan summa kaikista mahdollisista tuloista $a_i(b_j c_k)$, missä $i+j+k = n$. Vastaavasti tulon $[(a_k)(b_k)](c_k)$ n:s kerroin on summa kaikista mahdollisista tuloista $(a_i b_j)c_k$, missä $i+j+k = n$. Siis n:s kerroin on muotoa

$$\sum_{i+j+k=n} (a_i b_j) c_k.$$

Kertolaskun assosiatiivisuus renkaassa R voidaan kirjoittaa myös lausekkeen muotoon: $a_i(b_j c_k) = (a_i b_j)c_k$. Näin ollen polynomien kertolasku on assosiatiivinen, sillä $(a_k)[(b_k)(c_k)] = [(a_k)(b_k)](c_k)$.

Polynomien kertolaskun distributiivisuuden osoittamiseksi tarkastellaan puolestaan lauseketta $(a_k)[(b_k) + (c_k)]$. Summa $(b_k) + (c_k)$ voidaan kirjoittaa yksinkertaisemmin $(b_k + c_k)$, jolloin sen m:s kerroin on $(b_m + c_m)$. Kun selvitetään tulon $(a_k)(b_k + c_k)$ n:s kerroin, lasketaan yhteen kaikki mahdolliset tulot $(a_i)(b_m + c_m)$, missä $i + m = n$. Tällöin lausekkeen $(a_k)[(b_k) + (c_k)]$ n:s kerroin saadaan muotoon

$$\sum_{i+m=n} a_i(b_m + c_m).$$

Lausekkeen $[(a_k)(b_k)]+[(a_k)(c_k)]$ n:s kerroin saadaan laskemalla tulojen $(a_k)(b_k)$ ja $(a_k)(c_k)$ n:sien kertoimien summa

$$\sum_{i+m=n} (a_i b_m) + \sum_{i+m=n} (a_i c_m)$$

samaan tapaan kuin edellä. Koska yhteenlasku on osoitettu jo aiemmin assosiatiiviseksi, saadaan lausekkeen $[(a_k)(b_k)] + [(a_k)(c_k)]$ n:s kerroin muotoon

$$\sum_{i+m=n} a_i b_m + a_i c_m.$$

Renkaan R kertolaskun distributiivisuus voidaan kirjoittaa lausekkeena $a_i(b_m + c_m) = a_i b_m + a_i c_m$. Näin ollen polynomien kertolasku on distributiivinen, sillä $(a_k)[(b_k) + (c_k)] = [(a_k)(b_k)] + [(a_k)(c_k)]$. Polynomien kertolasku voidaan vastaavalla menettelyllä osoittaa kommutatiiviseksi laskutoimitukseksi, mikä kuitenkin sivuutetaan.

Koska polynomien kertolasku on havaittu assosiatiiviseksi, distributiiviseksi ja kommutatiiviseksi, on $R[x]$ kommutatiivinen rengas. Olkoon nyt $(a_0, a_1, \ldots) = (e, 0, 0, \ldots)$, missä e on renkaan R 1-alkio kertolaskun suhteen. Tulon $(a_k)(b_k)$ k:s kerroin on nyt $c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \cdots + a_k b_0$. Koska $a_i = 0$ kaikilla

$i = 1, 2, \ldots, k$, on summan c_k ainoa nollasta poikkeava tulo $a_0 b_k = e b_k = b_k$. Siis $c_k = b_k$ kaikilla $k \geq 0$, joten $(a_k)(b_k) = (b_k)$. Joukon $R[x]$ 1-alkio kertolaskun suhteen on siis $(e, 0, 0, \ldots)$.

Helposti voidaan vielä osoittaa, että $R' = \{(a, 0, 0, \ldots) \mid a \in R\}$, joka on erityisesti vakiopolynomien joukko, on joukon $R[x]$ alirengas ja että kuvaus $\phi : R \longrightarrow R'$, missä $\phi(a) = (a, 0, 0, \ldots)$ on isomorfismi. Siis $R \simeq R'$, joten $R[x]$ sisältää renkaan R kanssa isomorfisen alirenkaan. ■

2.2 Polynomien asteesta

Apulause 2.2.1 *Olkoot $f(x)$ ja $g(x)$ renkaan $R[x]$ polynomeja.*

1. *Jos $f(x)g(x) \neq 0$, niin $\deg(f(x)g(x)) \leq \deg(f(x)) + \deg(g(x))$. Yhtäsuuruus on voimassa, jos polynomien $f(x)$ ja $g(x)$ korkeinta astetta olevien termien kertoimien tulo ei ole nolla.*

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

Todistus. [1, s. 285] Olkoon $\deg(f(x)) = n$ ja $\deg(g(x)) = m$.

1. Jos $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ ja $g(x) = b_0 + b_1 x + \cdots + b_n x^m$, niin $f(x)g(x) = a_0 b_0 + (a_0 b_1 + (a_1 b_0)x + \cdots + a_n b_m x^{m+n})$. Koska $f(x)g(x) \neq 0$, niin ainakin yksi polynomin $f(x)g(x)$ kertoimista on oltava nollasta poikkeava. Jos $a_n b_m \neq 0$, niin

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

   Jos $a_n b_m = 0$, niin polynomin $f(x)g(x)$ asteen määrää polynomin $f(x)g(x)$ nollasta poikkeava, suurimman eksponentin omaava termi. Tällöin

   $$\deg(f(x)g(x)) < \deg(f(x)) + \deg(g(x)).$$

2. Kokonaislukujen perusominaisuuksiin kuuluu, että vain joko $m > n$, $m = n$ tai $m < n$ voi olla kerralla voimassa. Jos $m < n$, niin $f(x) +$

$g(x) = (a_0 + b_0) + (a_1 + b_1 x + \cdots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_n x^n$ ja

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

Vastaavasti käsitellään tilanne $m > n$. Jos $m = n$, niin $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_m)x^n$. Koska $f(x) + g(x) \neq 0$ polynomin $f(x) + g(x)$ termien kertoimista on nollasta poikkeava. Jos $a_n + b_n \neq 0$, niin

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

Jos $a_n + b_n = 0$, niin polynomin $f(x) + g(x)$ asteen määrää polynomin $f(x) + g(x)$ nollasta poikkeava, suurimman eksponentin omaava termi. Tällöin

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

Renkaan $R[x]$ erotuksen määritelmästä seuraa suoraan epäyhtälö $\deg(f(x) - g(x)) \leq \max\{\deg(f(x)), \deg(g(x))\}$. Koska $f(x) - g(x) = f(x) + [-g(x)]$ ja $\deg(-g(x)) = \deg(g(x))$, niin polynomien yhteenlaskun mukaisesti

$$\begin{aligned} \deg(f(x) - g(x)) &= \deg(f(x) + [-g(x)]) \\ &\leq \max\{\deg(f(x)), \deg(-g(x))\} \\ &= \max\{\deg(f(x)), \deg(g(x))\}. \blacksquare \end{aligned}$$

Lause 2.2.2 *Rengas R on kokonaisalue, jos ja vain jos $R[x]$ on kokonaisalue. Erityisesti, kun R on kokonaisalue, niin* $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$ *kaikille nollasta poikkeaville polynomeille $f(x)$, $g(x) \in R[x]$.*

Todistus. [1, s. 286] Oletetaan, että R on kokonaisalue ja polynomit $f(x)$, $g(x) \in R[x]$ ovat nollasta poikkeavia. Jos $\deg(f(x)) = n$ ja $\deg(g(x)) = m$, niin polynomien $f(x)$ ja $g(x)$ johtavat kertoimet $a_n$ja b_m ovat kumpikin nollasta poikkeavia renkaan R alkioita. Näin ollen $a_n b_m \neq 0$, koska R on kokonaisalue. Nyt $a_n b_m$ on polynomin $f(x)g(x)$ termin x^{m+n} kerroin, joten

$f(x) \neq 0$. Siis renkaan $R[x]$ nollasta poikkeavien polynomien tulo on nollasta poikkeava ja näin ollen $R[x]$ on kokonaisalue. Apulauseen 2.2.1 mukaan

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

Käänteisesti jos $R[x]$ on kokonaisalue ja a, $b \in R$ ovat nollasta poikkeavia, niin a ja b voidaan tulkita vakiopolynomeiksi renkaassa $R[x]$. Nyt $ab \neq 0$ kokonaisalueessa $R[x]$, joten $ab \neq 0$ renkaassa R. Täten R on kokonaisalue. ■

2.3 Polynomien jakolasku

Lause 2.3.1 *Jos $f(x)$, $g(x) \in R[x]$ ja polynomin $g(x)$ johtavalla kertoimella on käänteisluku renkaassa R, niin on olemassa sellaiset yksikäsitteiset polynomit $q(x)$ ja $r(x)$ renkaassa $R[x]$, että $f(x) = g(x)q(x) + r(x)$, missä $r(x) = 0$ tai $\deg(r(x)) < \deg(g(x))$.*

Todistus. [1, s. 289] Koska polynomin $g(x)$ korkeinta astetta olevan termin kertoimella on käänteisluku, niin $g(x) \neq 0$. Alkuun on osoitettava, että polynomit $q(x)$ ja $r(x)$ ovat olemassa. Tutkittavana on kolme eri vaihtoehtoa: joko (1) $f(x) = 0$, (2) $f(x) \neq 0$ ja $\deg(g(x)) > \deg(f(x))$ tai (3) $f(x) \neq 0$ ja $\deg(g(x)) \leq \deg(f(x))$. Jos $f(x) = 0$ tai $\deg(g(x)) > \deg(f(x))$, valitaan $q(x) = 0$ ja $r(x) = f(x)$. [Muokkaus: Numerointi.] Näistä tapaukset (1) ja (2) voidaan merkata lausekkeena $f(x) = 0 \cdot g(x) + r(x)$, joten kiinnostavin tapauksista on tapaus (3). Tämän todistetaan induktiolla polynomin $f(x)$ asteen suhteen. Oletetaan nyt $f(x) \neq 0$ ja $\deg(g(x)) \leq \deg(f(x))$. Jos $\deg(f(x)) = 0$, niin polynomi $f(x)$ on vakiopolynomi. Oletetaan, että $f(x) = a$ ja $g(x) = b$. Nyt vakiolla b on käänteisalkio renkaassa R. Tällöin voidaan polynomi $f(x)$ merkata lausekkeena $f(x) = b(ab^{-1}) + 0$, missä $q(x) = ab^{-1}$ ja $r(x) = 0$. Näin voidaan havaita polynomien $q(x)$ ja $r(x)$ olevan olemassa, kun $\deg(f(x)) = 0$. Tehdään seuraavaksi induktio-oletus, että voidaan löytää polynomit $q(x)$ ja $r(x)$ kaikille nollapolynomista poikkeaville polynomeille, joiden aste on pienempi kuin n, kun $n \geq 0$. Olkoot $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ ja

$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$, missä $m \leq n$. Määritellään nyt polynomi $f_1(x)$ kaavalla

$$f_1(x) = f(x) - g(x)(a_nb_m^{-1})x^{n-m}. \; (*)$$

Polynomin $f_1(x)$ kuvaava lauseke on muotoiltu kumoamaan polynomin $f(x)$ suurinta astetta olevan termin. Seuraavassa tarkastellaan termin kumoutumista laskennallisesti:

$$\begin{aligned} f(x) &= f(x) - g(x)(a_nb_m^{-1})x^{n-m} \\ &= (a_0 + \cdots + a_nx^n) - (a_nb_m^{-1})x^{n-m}(b_0 + \cdots + b_mx^m) \\ &= a_0 + \cdots + a_nx^n - (a_nb_m^{-1})x^{n-m}b_0 - \cdots - (a_nb_m^{-1})x^{n-m}b_mx^m \\ &= a_0 + \cdots + a_nx^n - (a_nb_m^{-1}b_0)x^{n-m} - \cdots - (a_nb_m^{-1}b_{m-1})x^{n-1} - a_nx^n \\ &= a_0 + \cdots + a_{n-1}x^{n-1} - (a_nb_m^{-1}b_0)x^{n-m} - \cdots - (a_nb_m^{-1}b_{m-1})x^{n-1}. \end{aligned}$$

Nyt $\deg(f_1(x)) < n$ tai $f_1(x) = 0$. Toisaalta polynomi $f_1(x)$ saadaan myös jakokulmassa suoritetun laskun

$$\begin{array}{rl} & a_nb_m^{-1}x^{n-m} \\ g(x) = b_mx^m + \cdots + b_1x + b_0 \quad & \overline{\big|\; a_nx^n + \cdots + a_1x + a_0 = f(x)} \\ & \underline{a_nx^n + a_nb_m^{-1}b_{m-1}x^{n-1} + \cdots} \\ f_1(x) = & \quad f(x) - g(x)(a_nb_m^{-1})x^{n-m} \end{array}$$

ensimmäisen vaiheen jakojäännöksenä. Jos $f_1(x) = 0$, niin $f(x) = g(x)q(x) + r(x)$, missä $q(x) = (a_nb_m^{-1})x^{n-m}$ ja $r(x) = 0$. Jos puolestaan $f_1(x) \neq 0$, niin $\deg(f_1(x)) > 0$ ja induktio-oletuksen mukaan on olemassa renkaan $R[x]$ polynomit $q_1(x)$ ja $r(x)$, missä $r(x) = 0$ tai $\deg(r(x)) < \deg(g(x))$. Näin voidaan havaita, että

$$\begin{aligned} f(x) &= f_1(x) + g(x)(a_nb_m^{-1})x^{n-m} \\ &= g(x)q_1(x) + r(x) + (a_nb_m^{-1})x^{n-m}g(x) \\ &= g(x)[q_1(x) + (a_nb_m^{-1})x^{n-m}] + r(x) \\ &= g(x)q(x) + r(x), \end{aligned}$$

missä $q(x) = q_1(x) + (a_nb_m^{-1})x^{n-m}$. Näin polynomi $f(x)$ on ilmaistu tavoitellussa muodossa, kun $\deg(f(x)) = n$. Niinpä induktioperiaatteen mukaisesti

on osoitettu, että kaikkia polynomeja $f(x)$ ja $g(x)$ kohti on olemassa polynomit $q(x)$ ja $r(x)$ olettaen, että polynomin $g(x)$ suurinta astetta olevan termin kertoimella on käänteisalkio renkaassa R.

Lopuksi tulee vielä osoittaa, että polynomit $q(x)$ ja $r(x)$ ovat yksikäsitteisiä. Oletetaan nyt, että on olemassa polynomit $q(x)$, $q'(x)$, $r(x)$ ja $r'(x) \in R[x]$ siten, että

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

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

$$r(x) - r'(x) = (q'(x) - q(x))g(x). \; (**)$$

Jos $q'(x) \neq q(x)$ ja c on polynomin $q'(x) - q(x)$ suurimman asteen termin kerroin, niin $c \neq 0$. Koska polynomin $g(x)$ suurimman asteen termin kertoimella b_m on renkaassa R käänteisalkio, niin $b_m \neq 0$ ja edelleen $cb_m \neq 0$. Nyt $(q'(x) - q(x))g(x) \neq 0$. Yhtälön $(**)$ ja apulauseen 2.2.1 mukaan

$$\begin{aligned} \deg(r(x) - r'(x)) &= \deg((q'(x) - q(x))g(x)) \\ &= \deg(q'(x) - q(x)) + \deg(g(x)) \\ &\geq \deg(g(x)). \end{aligned}$$

Tämä on kuitenkin mahdotonta, sillä $\deg(r(x)) < \deg(g(x))$ ja $\deg(r'(x)) < \deg(g(x))$, jolloin apulauseen 2.2.1 mukaan

$$\deg(r(x) - r'(x)) \leq \max\{deg(r(x), \deg(-r'(x)))\} < \deg(g(x)).$$

Koska oletus $q'(x) \neq q(x)$ johtaa ristiriitaan, on voimassa $q'(x) = q(x)$, mistä puolestaan seuraa $r(x) = r'(x)$. Siis polynomit $q(x)$ ja $r(x)$ on osoitettu yksikäsitteisiksi. ■

Esimerkki 2.3.2 *Jaetaan polynomi* $f(x) = x^5 + 5x^4 - 2x^3 + x^2 - 8x + 1$ *polynomilla* $g(x) = x^2 + x + 2$ *jakokulmassa.*

$$
\begin{array}{rl}
 & x^3 + 4x^2 - 8x + 1 \\
x^2 + x + 2 & \overline{\big| \; x^5 + 5x^4 - 2x^3 + x^2 - 8x + 1} \\
 & \underline{-x^5 - x^4 - 2x^3} \\
 & \quad 4x^4 - 4x^3 \\
 & \quad \underline{-4^4 - 4x^3 - 8x^2} \\
 & \qquad -8x^3 - 7x^2 \\
 & \qquad \underline{+8x^3 + 8x^2 + 16x} \\
 & \qquad\quad +x^2 + 8x \\
 & \qquad\quad \underline{-x^2 - x - 2} \\
 & \qquad\qquad 7x - 1
\end{array}
$$

Nyt polynomi voidaan kirjoittaa myös muotoon $x^5+5x^4-2x^3+x^2-8x+1 = (x^2 + x + 2)(x^3 + 4x^2 - 8x + 1) + 7x - 1$

Seuraus 2.3.3 *Jos* F *on kunta,* $f(x)$, $g(x) \in F[x]$ *ja* $g(x) \neq 0$, *niin on olemassa yksikäsitteiset* $q(x)$, $r(x) \in F[x]$ *siten, että* $f(x) = g(x)q(x) + r(x)$, *missä* $r(x) = 0$ *tai* $\deg(r(x)) < \deg(g(x))$.

Todistus. [1, s. 291] Jos $g(x) \neq 0$, polynomin $g(x)$ johtava kerroin on kunnan F nollasta poikkeava alkio. Koska F on erityisesti kunta, kertoimella on käänteisalkio kunnassa F. ■

Luku 3

Nollakohdat, jaollisuus ja suurin yhteinen tekijä

3.1 Polynomin nollakohdat

Määritelmä 3.1.1 *Olkoot $f(x)$ ja $g(x)$ renkaan $R[x]$ polynomeja, joista $g(x) \neq 0$. Jos on olemassa sellainen polynomi $h(x)$, että $f(x) = g(x)h(x)$, niin polynomi $g(x)$ jakaa polynomin $f(x)$ tai polynomi $g(x)$ on polynomin $f(x)$ tekijä. Merkintä $g(x) \mid f(x)$ tarkoittaa, että polynomi $g(x)$ jakaa polynomin $f(x)$ ja vastaavasti $g(x) \nmid f(x)$ tarkoittaa, ettei polynomi $g(x)$ jaa polynomia $f(x)$. Jos $f(x) \in R[x]$, $c \in R$ ja $f(x) = a_0 + a_1x + \cdots + a_nx^n$, niin $f(c)$ on renkaan R alkio $a_0 + a_1c + \cdots + a_nc^n$. Jos $f(c) = 0$, niin luku c on polynomin f(x) nollakohta.*

Lause 3.1.2 *Jos polynomin $f(x) \in R[x]$ aste on positiivinen ja $c \in R$, niin jaettaessa polynomi $f(x)$ polynomilla $x - c$ jää jakojäännökseksi $f(c)$.*

Todistus. [1, s. 296] Koska polynomin $x - c$ johtava kerroin on ykkösalkio ja ykkösalkiolla on kertolaskun suhteen käänteisalkio renkaassa R, niin lauseen 2.3.1 mukaan on olemassa sellaiset polynomit $q(x)$, $r(x) \in R[x]$, että $f(x) = (x - c)q(x) + r(x)$, missä $r(x) = 0$ tai $\deg(r(x)) < \deg(x - c) = 1$. Siis $r(x) = 0$ tai $\deg(r(x)) = 0$, joten polynomi $r(x)$ on vakio, jota voidaan

merkata yksinkertaisesti r. Näin ollen $f(x) = (x - c)q(x) + r$, josta saadaan $f(c) = (c - c)q(c) + r = r$. ■

3.2 Polynomin jako tekijöihin

Tekijälause 3.2.1 *Jos $f(x) \in R[x]$ on positiivista astetta oleva polynomi, niin $c \in R$ on polynomin $f(x)$ nollakohta, jos ja vain jos $x - c$ on polynomin $f(x)$ tekijä.*

Todistus. [1, s. 296] Lauseen 2.3.1 mukaan $f(x) = (x - c)q(x) + r$, missä $r \in R$. Tällöin $f(c) = 0$, jos ja vain jos $r = 0$, jos ja vain jos $f(x) = (x-c)q(x)$. Nyt $c \in R$ on polynomin $f(x)$ nollakohta, jos ja vain jos $f(x) = (x - c)q(x)$. Näin ollen c on polynomin $f(x)$ nollakohta, jos ja vain jos $x-c$ on polynomin $f(x)$ tekijä. ■

Seuraavan lauseen todistuksessa polynomin kerroinrengas F on kunta.

Lause 3.2.2 *Olkoon $f(x) \in F[x]$ mikä tahansa positiivista aste n oleva polynomi. Jos polynomilla $f(x)$ on erisuuret nollakohdat c_1, c_2, ..., $c_n \in F$, niin $f(x)$ voidaan kirjoittaa muotoon $f(x) = a(x - c_1)(x - c_2) \cdots (x - c_n)$, missä a on polynomin $f(x)$ korkeinta astetta olevan termin kerroin.*

Todistus. [1, s. 297] Lause todistetaan induktiolla polynomin $f(x) \in F[x]$ asteen suhteen. Jos $\deg(f(x)) = 1$, niin polynomi voidaan kirjoittaa muotoon $f(x) = ax + b$, missä a, $b \in F$. Jos $c_1 \in F$ on polynomin $f(x)$ nollakohta, niin $0 = f(c_1) = ac_1 + b$. Ratkaisemalla tästä b, saadaan $b = -ac_1$. Näin ollen $f(x) = ax - ac_1 = a(x - c_1)$, joten polynomin asteen ollessa 1 lause on voimassa. Oletetaan nyt, että jokainen asteen k polynomi $g(x) \in F[x]$, jolla on erisuuret nollakohdat c_1, c_2, ..., $c_k \in F$ ja johtava kerroin a, voidaan kirjoittaa muotoon $a(x - c_1)(x - c_2) \cdots (x - c_n)$. Jos polynomi $f(x)$ on astetta $k + 1$, niin lauseen 3.2.1 mukaan on olemassa $g(x) \in F[x]$, että $f(x) = (x - c_1)g(x)$. Nyt puolestaan lauseen 2.2.2 mukaan $k + 1 = \deg(f(x)) = \deg(x - c_1) + \deg(g(x)) = 1 + \deg(g(x))$, joten

$\deg(g(x)) = k$. Edelleen $0 = f(c_i) = (c_i - c_1)g(c_i) \in F$, kun $i = 2, 3, \ldots, k+1$. Koska polynomin nollakohdat ovat erisuuria, $c_i - c_1 \neq 0$ ja kunnassa ei ole nollanjakajia, niin $g(i) = 0$, kun $i = 2, 3, \ldots, k+1$. Koska lisäksi polynomin $g(x)$ suurimman asteen termin kerroin on a ja polynomi $g(x)$ voidaan kirjoittaa muotoon $g(x) = a(x - c_2)(x - c_3)\cdots(x - c_{k+1})$, niin selvästi $f(x) = a(x-c_1)(x-c_2)(x-c_3)\cdots(x-c_{k+1})$. Siis induktioperiaatteen mukaan erisuuret nollakohdat $c_1, c_2, \ldots, c_n \in F$ omaava polynomi voidaan asteesta riippumatta kirjoittaa muotoon $f(x) = a(x - c_1)(x - c_2)\cdots(x - c_n)$. ■

Lauseen 3.2.2 seurauksena 3.2.3 havaitaan polynomin asteen rajoittavan nollakohtien määrää.

Seuraus 3.2.3 *Jos polynomin $f(x) \in F[x]$ aste on $n \geq 0$, niin polynomilla $f(x)$ voi olla enintään n erisuurta nollakohtaa.*

Todistus. [1, s. 297] Jos polynomin $f(x)$ aste $n \geq 0$, niin $f(x) \neq 0$, koska nollapolynomille astetta ei ole määritelty. Jos $n = 0$, niin polynomi $f(x)$ on nollasta poikkeava vakiopolynomi, jolla ei ole nollakohtia. Siis lause pätee, kun $n = 0$. Oletetaan nyt, että $n \geq 0$. Jos polynomilla $f(x)$ on vähemmän erisuuria nollakohtia kuin n kappaletta, mitään todistettavaa ei ole. Oletetaan, että polynomilla $f(x)$ on täsmälleen n erisuurta nollakohtaa kunnassa F, ja osoitetaan, ettei nollakohtia voi olla enempää. Jos c_1, $c_2, \ldots, c_n \in F$ ovat polynomin $f(x)$ nollakohdat, niin lauseen 3.2.2 mukaan $f(x) = a(x - c_1)(x - c_2)\cdots(x - c_n)$, missä a on polynomin $f(x)$ suurimman asteen termin kerroin. Jos $c \in F$ on polynomin $f(x)$ nollakohta ja erisuuri kuin jo mainitut nollakohdat, niin $0 = f(c) = a(c - c_1)(c - c_2)\cdots(c - c_n)$. Koska kaikki nollakodat ovat erisuuria, niin $c \neq c_k$ kaikilla $k = 1, 2, \ldots, n$, joten kaikki tulon tekijät ovat nollasta poikkeavia. Näin ollen ainakin yhden tulon tekijöistä on oltava nollajakaja, mikä on kuitenkin ristiriita, sillä F on kunta. Polynomilla $f(x)$ ei voi olla ylimääräistä nollakohtaa. ■

Seuraus 3.2.4 *Olkoot sellaiset polynomit $f(x)$, $g(x) \in F[x]$, että $f(c) = g(c)$ kaikilla $c \in F$. Jos kunnan F alkioiden lukumäärä on suurempi kuin kummankaan polynomin $f(x)$ tai $g(x)$ aste, niin $f(x) = g(x)$.*

Todistus. [1, s. 298] Joko $f(x) = g(x)$ tai $f(x) \neq g(x)$. Jos $f(x) \neq g(x)$, olkoon $h(x) = f(x) - g(x)$. Tällöin $h(x)$ on renkaan $F[x]$ nollasta poikkeava polynomi ja koska $f(c) = g(c)$, niin $h(c) = f(c) - g(c) = 0$ kaikille $c \in F$. Nyt $\deg(h(x)) = \deg(f(x) - g(x)) \leq \max\{\deg(f(x)), \deg(g(x))\} <$ kunnan F alkioiden lukumäärä lauseen 2.2.1 perusteella. Siis polynomin $h(x)$ nollakohtien lukumäärä on suurempi kuin polynomin $h(x)$ aste, mikä on kuitenkin ristiriidassa lauseen 3.2.3 kanssa. Näin ollen $f(x) \neq g(x)$ ei ole mahdollista, joten $f(x) = g(x)$. ■

3.3 Polynomien suurin yhteinen tekijä

Määritelmä 3.3.1 *Polynomia $f(x) \in F[x]$ kutsutaan pääpolynomiksi, jos polynomin $f(x)$ suurinta astetta olevan termin kerroin on kunnan F ykkösalkio. Jos $f(x)$ ja $g(x)$ ovat renkaan $F[x]$ polynomeja, joista vähintään yksi on nollasta poikkeava, niin pääpolynomi $d(x) \in F[x]$ on polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä seuraavin ehdoin:*

(i) $d(x) \mid f(x)$ *ja* $d(x) \mid g(x)$

(ii) Jos $h(x) \in F[x]$, $h(x) \mid f(x)$ *ja* $h(x) \mid g(x)$, *niin* $h(x) \mid d(x)$.

Polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä merkitään $\text{syt}(f(x), g(x))$. *Jos* $\text{syt}(f(x), g(x)) = e$, *niin polynomit $f(x)$ ja $g(x)$ ovat keskenään jaottomat.*

Lause 3.3.2 *Olkoot $f(x)$ ja $g(x)$ renkaan $F[x]$ polynomeja. Kun polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä on olemassa, se on yksikäsitteinen.*

Todistus. [1, s. 300] Tehdään vastaoletus, että polynomien $f(x)$ ja $g(x)$ suurimmat yhteiset tekijät ovat polynomit $d_1(x)$ ja $d_2(x)$. Tällöin suurimman yhteisen tekijän määritelmän mukaan $d_1(x) \mid d_2(x)$ ja $d_2(x) \mid d_1(x)$. Nyt on olemassa polynomit $k_1(x)$ ja $k_2 \in F[x]$ siten, että $d_2(x) = k_1(x)d_1(x)$ ja $d_1(x) = k_2(x)d_2(x)$. Näin ollen $d_1(x) = k_1(x)k_2(x)d_1(x)$, jolloin $e = k_1(x)k_2(x)$, sillä

$F[x]$ on kokonaisalue. Siis

$$\begin{aligned} 0 &= \deg(e) = \deg(k_1(x)k_2(x)) \\ &= \deg(k_1(x)) + \deg(k_2(x)). \end{aligned}$$

Koska polynomin aste on aina ≥ 0, niin $\deg(k_1(x)) = \deg(k_2(x)) = 0$. Siis $k_1(x)$ ja $k_2(x)$ ovat nollasta poikkeavia vakiopolynomeja. Koska polynomit $d_1(x)$ ja $d_2(x)$ ovat pääpolynomeja, $k_1(x) = k_2(x) = e$. Edelleen $d_1(x) = d_2(x)$, joten polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä on yksikäsitteinen. ■

Lause 3.3.3 *Olkoot $f(x)$, $g(x) \neq 0$ renkaan $F[x]$ polynomeja. Tällöin $d(x) = \text{syt}(f(x), g(x))$ on sekä olemassa että yksikäsitteinen. Lisäksi on olemassa polynomit $a(x)$, $b(x) \in F[x]$, että $d(x) = a(x)f(x) + b(x)g(x)$. Edelleen $d(x)$ on pienin astetta oleva pääpolynomi, joka voidaan kirjoittaa muotoon $a(x)f(x) + b(x)g(x)$.*

Todistus. [1, s. 301] Olkoon joukko $S = \{a(x)f(x) + b(x)g(x) \mid a(x), b(x) \in F[x]\}$. Nyt $f(x)$, $g(x) \in S$, sillä $f(x) = ef(x) + 0g(x)$ ja $g(x) = 0f(x) + eg(x)$. Olkoon nyt $d(x)$ joukon S pääpolynomi, joka on pienintä astetta. Tällainen polynomi voidaan valita, kun muodostetaan joukko D joukon S polynomien asteista. Tällöin D on epätyhjä järjestetyn luonnollisten lukujen joukon $\mathbb{N}$ osajoukko, jolla on pienin alkio. Voidaan olettaa, että $d(x)$ on pääpolynomi. Jos $d(x)$ ei ole pääpolynomi ja suurimman asteen termin kerroin on a, voimme korvata polynomin $d(x)$ pääpolynomilla $a^{-1}d(x)$. Koska $d(x) \in S$, niin myös $a^{-1}d(x) \in S$.

Tutkitaan väitettä $d(x) = \text{syt}(f(x), g(x))$. Lauseen 2.3.1 mukaan nyt on olemassa polynomit $q(x)$, $r(x) \in F[x]$ siten, että $f(x) = d(x)q(x) + r(x)$. Koska $d(x) \in S$, niin joukon S määrittelyn mukaan $d(x) = a(x)f(x) + b(x)g(x)$, missä $a(x)$ ja $b(x)$ ovat renkaan $F[x]$ polynomeja. Näin ollen

$$\begin{aligned} r(x) &= f(x) - d(x)q(x) \\ &= f(x) - [a(x)f(x) + b(x)g(x)]q(x) \\ &= [e - a(x)q(x)]f(x) + [b(x)q(x)]g(x), \end{aligned}$$

joten polynomi $r(x) \in S$. Koska $\deg(r(x)) < \deg(d(x))$, niin $r(x) = 0$, sillä $d(x)$ on pienintä astetta oleva joukon S polynomi. Tällöin $f(x) = d(x)q(x)$ ja siis $d(x) \mid f(x)$. Vastaavasti myös $d(x) \mid g(x)$. Siis $d(x)$ on polynomien $f(x)$ ja $g(x)$ yhteinen jakaja. Oletetaan seuraavaksi, että on olemassa sellainen $c(x) \in F[x]$, että $c(x) \mid f(x)$ ja $c(x) \mid g(x)$. Tällöin on olemassa jotkin $a'(x)$, $b'(x) \in F[x]$, että $f(x) = a'(x)c(x)$ ja $g(x) = b'(x)c(x)$. Tällöin

$$\begin{aligned} d(x) &= a(x)f(x) - b(x)g(x) \\ &= a(x)a'(x)c(x) + b(x)b'(x)c(x) \\ &= [a(x)a'(x) + b(x)b'(x)]c(x). \end{aligned}$$

Tämän perusteella $c(x) \mid d(x)$, joten polynomi $d(x)$ toteuttaa määritelmän 3.3.1 ehdot (i) ja (ii). Siis määritelmän mukaan $d(x)$ on polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä.

Polynomin $d(x)$ yksikäsitteisyys osoitettiin lauseessa 3.3.2 ja polynomin $d(x)$ uudelleenmuotoilu

$$d(x) = [a(x) + g(x)]f(x) + [b(x) - f(x)]g(x)$$

osoittaa, että polynomit $a(x)$ ja $b(x)$ eivät ole yksikäsitteisiä. Koska jokainen joukon S polynomi voidaan kirjoittaa muodossa $a(x)f(x) + b(x)g(x)$, on selvää, että $d(x)$ on pienintä astetta olevan polynomi, joka voidaan myös kirjoittaa tässä muodossa. ■

Lause 3.3.4 *Olkoot renkaan $F[x]$ polynomit $f(x)$, $g(x)$ ja $h(x)$ sellaisia, että $f(x) \mid g(x)h(x)$. Jos $f(x)$ ja $g(x)$ ovat keskenään jaottomia, niin $f(x) \mid h(x)$.*

Todistus. [1, s. 302] Jos polynomit $f(x)$ ja $g(x)$ ovat keskenään jaottomia, niin on olemassa sellaiset polynomit $a(x)$, $b(x) \in F[x]$, että $e = a(x)f(x) + b(x)g(x)$. Tällöin

$$\begin{aligned} eh(x) &= [a(x)f(x) + b(x)g(x)]h(x) \\ h(x) &= a(x)f(x)h(x) + b(x)g(x)h(x). \end{aligned}$$

Koska $f(x) \mid g(x)h(x)$, niin on olemassa sellainen polynomi $c(x) \in F[x]$, että $g(x)h(x) = c(x)f(x)$. Polynomi $h(x)$ voidaan esittää muodossa

$$\begin{aligned} h(x) &= a(x)f(x)h(x) + b(x)c(x)f(x) \\ &= [a(x)h(x) + b(x)c(x)]f(x), \end{aligned}$$

joten $f(x) \mid h(x)$. ■

Lause 3.3.5 *Olkoot renkaan $F[x]$ polynomit $f(x)$, $g(x)$, $q(x)$ ja $r(x)$ sellaisia, että $f(x) = g(x)q(x) + r(x)$. Tällöin* $\text{syt}(f(x), g(x)) = \text{syt}(g(x), r(x))$.

Todistus. Vrt. [1, s. 39] Olkoon A polynomien $f(x)$ ja $g(x)$ kaikkien yhteisten tekijöiden joukko ja B puolestaan polynomien $g(x)$ ja $r(x)$ kaikkien yhteisten tekijöiden joukko. Jos $c(x) \in A$, niin $c(x) \mid f(x)$ ja $c(x) \mid g(x)$. Tällöin $f(x) = c(x)j_1(x)$ ja $g(x) = c(x)j_2(x)$, missä $j_1(x)$, $j_2 \in F[x]$. Koska $f(x) = g(x)q(x) + r(x)$, niin $r(x) = [j_1(x) - q(x)j_2(x)]c(x)$ ja siis $c(x) \mid r(x)$. Tällöin $c(x) \in B$, joten $A \subseteq B$. Kun vastaavasti $c(x) \in B$, niin $c(x) \mid g(x)$ ja $c(x) \mid r(x)$. Tällöin $g(x) = c(x)k_1(x)$ ja $r(x) = c(x)k_2(x)$, missä $k_1(x)$, $k_2 \in F[x]$. Koska $f(x) = g(x)q(x)+r(x)$, niin $f(x) = [q(x)k_1(x)+k_2(x)]c(x)$ ja siis $c(x) \mid f(x)$. Tällöin $c(x) \in A$, joten $B \subseteq A$. Koska $A \subseteq B$ ja $B \subseteq A$, niin $A = B$. Koska A on lisäksi kaikkien yhteisten tekijöiden joukko, niin erityisesti $\text{syt}(f(x), g(x)) \in A$ sekä $\text{syt}(g(x), r(x)) \in B$. Koska $A = B$, niin lisäksi $\text{syt}(f(x), g(x)) \in B$ ja $\text{syt}(g(x), r(x)) \in A$. Koska molemmat suurimmat yhteiset tekijät $\text{syt}(f(x), g(x))$ ja $\text{syt}(g(x), r(x))$ ovat polynomien $f(x)$ ja $g(x)$ yhteisiä tekijöitä, polynomien $g(x)$ ja $r(x)$ yhteisiä tekijöitä ja lauseen 3.3.3 mukaan suurin yhteinen tekijä on yksikäsitteinen, niin $\text{syt}(f(x), g(x)) = \text{syt}(g(x), r(x))$. ■

3.4 Eukleideen algoritmi polynomeille

Lause 3.4.1 *Olkoot renkaan $F[x]$ polynomit $f(x)$ ja $g(x)$ nollasta poikkeavia, joille* $\deg(g(x)) \leq \deg(f(x))$. *Jos* $g(x) \mid f(x)$, *niin* $\mathrm{syt}(f(x), g(x)) = a^{-1}g(x)$, *missä a on polynomin $g(x)$ suurimman asteen termin kerroin. Jos taas* $g(x) \nmid f(x)$, *niin lauseen 2.3.1 mukaisesti polynomien jakolaskua toistaen saadaan*

$$\begin{aligned}
f(x) &= g(x)q_0(x) + r_0(x), && \textit{missä} \quad \deg(r_0(x)) < \deg(g(x)) \\
g(x) &= r_0(x)q_1(x) + r_1(x), && \textit{missä} \quad \deg(r_1(x)) < \deg(r_0(x)) \\
r_0(x) &= r_1(x)q_2(x) + r_2(x), && \textit{missä} \quad \deg(r_2(x)) < \deg(r_1(x)) \\
r_1(x) &= r_2(x)q_3(x) + r_3(x), && \textit{missä} \quad \deg(r_3(x)) < \deg(r_2(x)) \\
r_2(x) &= r_3(x)q_4(x) + r_4(x), && \textit{missä} \quad \deg(r_4(x)) < \deg(r_3(x)) \\
&\vdots && \vdots
\end{aligned}$$

Koska ei-negatiiviset lukujen jono $\deg(r_0) > \deg(r_1) > \deg(r_2) > \cdots$ *on vähenevä, niin on olemassa sellainen positiivinen kokonaisluku k, jolle*

$$\begin{aligned}
&\vdots && \vdots \\
r_{k-2}(x) &= r_{k-1}(x)q_k(x) + r_k(x), && \textit{missä} \quad \deg(r_k(x) < \deg(r_{k-1}(x))) \\
r_{k-1}(x) &= r_k(x)q_{k+1}(x) + 0.
\end{aligned}$$

Erityisesti $\mathrm{syt}(f(x), g(x)) = a^{-1}r_k(x)$, *missä luku a on polynomin $r_k(x)$ johtava kerroin.*

Todistus. [1, s. 303] Apulauseen 3.3.5 mukaan $\mathrm{syt}(f(x), g(x)) = \mathrm{syt}(g(x), r_0(x)) = \mathrm{syt}(r_0(x), r_1(x)) = \mathrm{syt}(r_1(x), r_2(x)) = \cdots = \mathrm{syt}(r_{k-1}(x), r_k(x)) = \mathrm{syt}(r_k(x), 0) = a^{-1}r_k(x)$, missä luku a on polynomin $r_k(x)$ johtava kerroin. ■

3.5 Polynomien jaollisuus

Lause 3.5.1 *Jos D on kokonaisalue, niin renkaan $D[x]$ polynomeista käänteisalkio on olemassa ainoastaan nollasta poikkeavilla vakiopolynomeilla $f(x) = a$, sillä a on kokonaisalueen D alkio ja on kertolaskun suhteen käänteisalkio.*

Todistus. [1, s. 307] Jos polynomilla $g(x) \in D[x]$ on käänteispolynomi $f(x)$, niin lauseen 2.2.2 mukaan $0 = \deg(e) = \deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$. Koska $\deg(f(x)) \geq 0$ ja $\deg(g(x)) \geq 0$, niin tästä seuraa $\deg(f(x)) = \deg(g(x)) = 0$. Tällöin polynomien $f(x)$ ja $g(x)$ on oltava vakiopolynomeja. Jos $f(x) = a$ ja $g(x) = b$, niin $ab = e$, jolloin luvulla a on kertolaskun suhteen käänteisalkio kokonaisalueessa D. ■

Määritelmä 3.5.2 *Jos D on kokonaisalue, niin renkaan $D[x]$ vakiopolynomia u kutsutaan* **yksiköksi***, jos sillä on kertolaskun suhteen käänteisalkio renkaassa $D[x]$. Polynomeja $f(x)$, $g(x) \in D[x]$ kutsutaan puolestaan* **liittopolynomeiksi***, jos on olemassa sellainen yksikkö $u \in D[x]$, että $f(x) = ug(x)$. Polynomi $f(x) \in D[x]$, joka ei ole vakiopolynomi, on jaoton renkaassa $D[x]$, aina kun $f(x) = g(x)h(x)$, missä joko $g(x)$ tai $h(x)$ on yksikkö renkaassa $D[x]$. Renkaan $D(x)$ polynomia kutsutaan jaolliseksi, jos se ei ole jaoton renkaassa $D(x)$.*

Lause 3.5.3 *Olkoon renkaan $F[x]$ polynomi $f(x)$ positiivista astetta.*

1. *Tällöin renkaassa $F[x]$ on olemassa sellaiset jaottomat polynomit $f_1(x)$, $f_2(x)$, ..., $f_m(x)$, että $f(x) = f_1(x)f_2(x)\cdots f_m(x)$. Jos lisäksi polynomilla $f(x)$ on toinen tekijöihinjako $f(x) = g_1(x)g_2(x)\cdots g_n(x)$, missä $g_1(x)$, $g_2(x)$, ..., $g_n(x) \in F[x]$ ovat jaottomia, niin $m = n$ ja polynomien $g_i(x)$ sopivan uudelleenjärjestelyn jälkeen polynomit $f_i(x)$ ja $g_i(x)$ ovat liittopolynomeja kaikilla $i = 1, 2, \ldots, m$.*

2. *Jos a on polynomin $f(x)$ suurimman asteen termin kerroin, niin renkaassa $F[x]$ on olemassa sellaiset jaottomat pääpolynomit $h_1(x)$, $h_2(x)$, ..., $h_n(x)$, että $f(x) = ah_1(x)h_2(x)\cdots h_n(x)$. Lisäksi tämä tekijöihin jako on yksikäsitteinen lukuun ottamatta jaottomien moonisten tekijöiden järjestystä.*

Todistus. Sivuutetaan, vrt. [1, s. 43]

Luku 4

Renkaiden $\mathbb{Q}[x]$, $\mathbb{R}[x]$ ja $\mathbb{C}[x]$ polynomit

4.1 Polynomien nollakohdat renkaassa $\mathbb{C}[x]$

Tarkastellaan polynomirengasta $\mathbb{C}[x]$. Algebran peruslauseen todistamiseksi on oletettava kompleksianalyysin perusteet tunnetuiksi.

Algebran peruslause 4.1.1 *Olkoon $p(z) \in \mathbb{C}[x]$ polynomi, joka ei ole vakiopolynomi. Tällöin yhtälöllä $p(z) = 0$ on nollakohta renkaassa $\mathbb{C}[x]$.*

Todistus. [3, s. 66] Tehdään vastaoletus, että polynomi $p(z) \neq 0$ kaikilla $z \in \mathbb{C}$. Funktio $f(z) = \frac{1}{p(z)}$ on tällöin jatkuva renkaassa $\mathbb{C}$. Kun $|z| \to \infty$, niin $|p(z)| \to \infty$, joten $|f(z)| \to 0$. Nyt voidaan valita sellainen vakio $R > 0$, että $|f(z)| \leq 1$ aina, kun $|z| > R$. Koska origokeskeinen R-säteinen suljettu kiekko S on kompakti ja funktio f on jatkuva, niin funktio f on siellä rajoitettu. Täten on olemassa sellainen $m > 0$, että $|f(z)| \leq m$ aina, kun $|z| \leq R$. Olkoon $M = \max\{m, 1\}$. Tällöin $|f(z)| \leq M \ \forall z \in \mathbb{C}$, joten lauseen 1.2.2 mukaan funktio f on vakio, jolloin polynomi p on vakiopolynomi. Tämä on kuitenkin ristiriita alkuperäisen oletuksen kanssa, joten polynomilla p on ratkaisu. ■

Seuraus 4.1.2 *Jos polynomi $f(x) \in \mathbb{C}[x]$ on positiivista astetta n ja johtava kerron on a, niin polynomi $f(x)$ voidaan jakaa tekijöihin*

$$f(x) = a(x - c_1)(x - c_2) \cdots (x - c_n),$$

missä c_1, c_2, ..., $c_n \in \mathbb{C}$ ovat polynomin $f(x)$ nollakohdat. Nollakohdat eivät välttämättä ole aina toisistaan poikkeavia.

Todistus. [1, s. 317] Lause todistetaan induktiolla polynomin $f(x)$ asteen n suhteen. Jos polynomin aste on 1, niin polynomi on muotoa $f(x) = ax + b$, missä a,$b \in \mathbb{C}$ ja $a \neq 0$. Polynomi saadaan helposti muotoon $f(x) = a(x - (-\frac{b}{a}))$ ja selvästi polynomin $f(x)$ nollakohta joukossa $\mathbb{C}$ on $x = -\frac{b}{a}$. Tehdään induktio-oletus, että lause pitää paikkaansa kaikille renkaan $\mathbb{C}[x]$ polynomeille, jotka ovat positiivista astetta k. Olkoon nyt polynomi $g(x) \in \mathbb{C}[x]$ astetta $k+1$ ja olkoon polynomin johtava kerroin a. Algebran peruslauseen 4.1.1 mukaan polynomilla $g(x)$ on nollakohta joukossa $\mathbb{C}$. Olkoon $c \in \mathbb{C}$ polynomin $g(x)$ nollakohta. Lauseen 3.2.1 mukaan $x-c$ on polynomin $g(x)$ tekijä. Tällöin on olemassa polynomi $h(x) \in \mathbb{C}[x]$ siten, että $g(x) = (x - c)h(x)$. Selvästi kerroin a on myös polynomin $h(x)$ johtava kerroin. Polynomien asteille on voimassa $k + 1 = \deg(g(x)) = \deg(x - c) + \deg(h(x)) = 1 + \deg(h(x))$, mistä voidaan päätellä, että $\deg(h(x)) = k$. Induktio-oletuksen mukaan polynomi $h(x)$ voidaan jakaa tekijöihin $h(x) = a(x-c_1)(x-c_2)\cdots(x-c_k)$, missä c_1, c_2, ..., $c_k \in \mathbb{C}$ ovat polynomin $h(x)$ k nollakohtaa, jotka eivät välttämättä ole aina toisistaan poikkeavia. Nyt polynomi $g(x)$ voidaan kirjoittaa muotoon $g(x) = a(x - c)(x - c_1)(x - c_2) \cdots (x - c_k)$, missä c, c_1, c_2, ..., $c_k \in \mathbb{C}$ ovat polynomin $g(x)$ $k + 1$ nollakohtaa jotka eivät välttämättä ole aina toisistaan poikkeavia. Näin induktioperiaatteen perusteella positiivista astetta n oleva polynomi $f(x) \in \mathbb{C}[x]$, jonka johtava kerroin on a, voidaan jakaa tekijöihin

$$f(x) = a(x - c_1)(x - c_2) \cdots (x - c_n),$$

missä c_1, c_2, ..., $c_n \in \mathbb{C}$ ovat polynomin $f(x)$ nollakohdat. ■

Apulause 4.1.3 *Jos $f(x)$ on renkaan $\mathbb{C}[x]$ polynomi ja luku $z \in \mathbb{C}$ on polynomin $f(x)$ nollakohta, niin luvun z liittoluku $\overline{z}$ on polynomin $f(x)$ nollakohta.*

Todistus. [1, s. 318] Olkoon $f(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n \in \mathbb{R}[x]$. Jos $z \in \mathbb{C}$ on polynomin $f(x)$ nollakohta ja samalla myös reaaliluku, niin $z = \bar{z}$ eikä mitään todistettavaa ole. Oletetaan, että $z \in \mathbb{C}$ on polynomin $f(x)$ nollakohta ja $z \notin \mathbb{R}$. Koska indeksin j kaikilla arvoilla $\overline{a_j} = a_j$ ja vastaavasti $f(x) = 0$, $\overline{f(x)} = \overline{0} = 0$. Edelleen kompleksilukujen liittolukujen laskutoimitusten perusteella

$$\begin{aligned} 0 &= \overline{a_0 + a_1z + a_2z^2 + \cdots + a_nz^n} \\ &= \overline{a_0} + \overline{a_1z} + \overline{a_2z^2} + \cdots + \overline{a_nz^n} \\ &= \overline{a_0} + \overline{a_1z} + \overline{a_2}\,\overline{z^2} + \cdots + \overline{a_n}\,\overline{z^n} \\ &= a_0 + a_1\overline{z} + a_2\overline{z^2} + \cdots + a_n\overline{z^n} \\ &= a_0 + a_1\overline{z} + a_2\overline{z}^2 + \cdots + a_n\overline{z}^n \\ &= f(\overline{z}), \end{aligned}$$

joten on osoitettu $\overline{z}$ myös polynomin $f(x)$ nollakohdaksi. ■

Lause 4.1.4 *Jos kompleksiluku $z = a+bi$, $b \neq 0$, on polynomin $f(x) \in \mathbb{R}[x]$ nollakohta, niin $x^2 - 2ax + (a^2 + b^2)$ on polynomin $f(x)$ jaoton toisen asteen tekijä renkaassa $\mathbb{R}[x]$.*

Todistus. [1, s. 319] Jos $z = a + bi$, $b \neq 0$, on polynomin $f(x)$ nollakohta, niin lauseen 4.1.3 mukaan myös $\overline{z} = a - bi$ on polynomin $f(x)$ nollakohta. Nollakohtia vastaavat polynomin $f(x)$ tekijät ovat $x - a - bi$ ja $x - a + bi$, joten

$$(x - a - bi)(x - a + bi) = x^2 - 2ax + (a^2 + b^2)$$

on myös polynomin $f(x)$ tekijä. Koska $a, b \in \mathbb{R}$ ja tekijän $x^2 - 2ax + (a^2 + b^2)$ molemmat nollakohdat eivät ole reaalilukuja, tekijällä $x^2 - 2ax + (a^2 + b^2)$ ei ole nollakohtia renkaassa $\mathbb{R}$. Täten $x^2 - 2ax + (a^2 + b^2)$ on jaoton renkaassa $\mathbb{R}[x]$. ■

Lause 4.1.5 *Jokainen renkaan $\mathbb{R}[x]$ polynomi voidaan jakaa johtavan kertoimen, renkaan $\mathbb{R}[x]$ ensimmäisen asteen ja jaottomien toisen asteen polynomien tuloksi.*

Todistus. [1, s. 320] Oletetaan, että $f(x) \in \mathbb{R}[x]$ on sellainen polynomi, jonka aste $\deg(f(x)) = n$ on pariton, ja olkoon a polynomin $f(x)$ johtava kerroin. Koska $\mathbb{R}[x] \subseteq \mathbb{C}[x]$, niin $f(x) \in \mathbb{C}[x]$. Lauseen 4.1.2 perusteella polynomi $f(x)$ voidaan jakaa tekijöihin

$$f(x) = a(x - c_1)(x - c_2) \cdots (x - c_n), (*)$$

missä c_1, c_2, ..., $c_n \in \mathbb{C}$ ovat polynomin $f(x)$ nollakohdat, jotka voivat olla yhtä suuria. Koska n on pariton, polynomilla $f(x)$ on ainakin yksi nollakohta joukossa $\mathbb{R}$. Jos kaikki polynomin $f(x)$ nollakohdat kuuluvat joukkoon $\mathbb{R}$, niin yhtälössä $(*)$ on tekijöihinjako suoritettu valmiiksi joukon $\mathbb{R}$ ensimmäisen asteen polynomien tuloksi. Jos yksi tai useampi nollakohdista, mutta eivät kuitenkaan kaikki, kuuluvat joukkoon $\mathbb{R}$, niin nollakohdat c_1, c_2, ..., c_n voidaan järjestää uudelleen siten, että nollakohdat c_1, c_2, ..., c_k ovat reaalilukuja ja c_{k+1}, c_{k+2}, ..., c_n ovat polynomin $f(x)$ nollakohdat joukossa $\mathbb{C}$. Lauseen 4.1.3 mukaan polynomin $f(x)$ nollakohdat esiintyvät aina joukossa $\mathbb{C}$ liittolukupareina, joten järjestetään polynomin $f(x)$ nollakohdat uudelleen siten, että $\overline{c_{k+1}} = c_{k+2}$, $\overline{c_{k+3}} = c_{k+4}$, ..., $\overline{c_{n-1}} = c_n$. Apulauseen 4.1.4 mukaan edellä ryhmiteltyjä kompleksilukuja vastaavat polynomin $f(x)$ tekijät voidaan kertoa pareittain tekijöihinjaosta

$$f(x) \;=\; a(x - c_1) \cdots (x - c_k)(x - c_{k+1})(x - c_{k+2}) \cdots (x - c_{n-1})(x - c_n),$$

missä tulo $(x - c_{k+1})(x - c_{k+2})$ on toisen asteen polynomi $x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$ ja sitä seuraavat ryhmitellyt tulot muodostavat samaan tapaan renkaan $\mathbb{R}[x]$ toisen asteen jaottomia polynomeja. Jos $\deg(f(x))$ on parillinen, niin polynomilla $f(x)$ ei välttämättä ole nollakohtia joukossa $\mathbb{R}$. Jos reaalilukunollakohtia on olemassa, niitä on oltava parillinen määrä. Polynomi $f(x)$ voidaan nyt jakaa johtavan kertoimen ja renkaan $\mathbb{R}[x]$ ensimmäisen asteen polynomien tuloksi tai johtavan kertoimen sekä renkaan $\mathbb{R}[x]$ ensimmäisen asteen polynomien ja jaottomien toisen asteen polynomien tuloksi. Jos polynomilla $f(x)$ ei ole reaalilukunollakohtia, niin polynomi voidaan esittää renkaan $\mathbb{R}[x]$ jaottomien toisen asteen polynomien tulona. ■

Esimerkki 4.1.6 *Polynomin* $f(x) = x^4-2x^3+6x^2-2x+5 \in \mathbb{R}$ *ensimmäisen asteen tekijät* $x+i$, $x-i$, $x-1+2i$ *ja* $x-1-2i$ *ovat kaikki renkaan* $\mathbb{C}$ *alkioita eli polynomilla* $f(x)$ *ei ole ensimmäisen asteen tekijöitä renkaassa* $\mathbb{R}$. *Kuitenkin havaitaan, että* $(x+i)(x-i) = x^2+1$ *ja* $(x-1+2i)(x-1-2i) = x^2-2x+5$, *joten polynomi* $f(x)$ *voidaan jakaa toisen asteen tekijöihin* $f(x) = (x^2+1)(x^2-2x+5)$

4.2 Polynomien nollakohdat renkaassa $\mathbb{Q}[x]$

Lause rationaalijuurista 4.2.1 *Olkoon* $f(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n$ *renkaan* $\mathbb{Z}[x]$ *polynomi ja olkoon lisäksi* $\frac{p}{q}$ *nollasta poikkeava rationaaliluku, joka on sievennetty supistetussa muodossa. Jos* $\frac{p}{q}$ *on funktion* $f(x)$ *nollakohta, niin tällöin* $p \mid a_0$ *ja* $q \mid a_n$.

Todistus. [1, s. 322] Olkoon $\frac{p}{q}$ polynomin $f(x)$ nollakohta, joka on supistetussa muodossa. Tällöin

$$a_0 + a_1\frac{p}{q} + a_2\left(\frac{p}{q}\right)^2 + \cdots + a_n\left(\frac{p}{q}\right)^n = 0.$$

Kerrottaessa yhtälön molemmat puolet termillä q^n saadaan

$$a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_np^n = 0$$

ja edelleen vähentämällä yhtälön molemmilta puolilta termi a_np^n saadaan

$$a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_{n-1}p^{n-1}q = -a_np^n.$$

Ottamalla q yhteiseksi tekijäksi yhtälön vasemmasta puolesta saadaan

$$q\left(a_0q^{n-1} + a_1pq^{n-2} + a_2p^2q^{n-3} + \cdots + a_{n-1}p^{n-1}\right) = -a_np^n.$$

Näin voidaan päätellä, että $q \mid a_np^n$. Koska $\frac{p}{q} \in Q$ ja on supistetussa muodossa, niin $q \nmid p$ ja tällöin $q \nmid p^n$. Koska $q \mid a_np^n$, niin tästä seuraa lukuteorian alkeiden mukaan, että $q \mid a_n$. Vastaavasti voidaan myös osoittaa, että $p \mid a_0$. ■

Lauseen 4.2.1 avulla kokonaislukukertoimisten polynomien rationaalilukunollakohtien etsiminen helpottuu huomattavasti, kun mahdollisia nollakohtia saadaan yksinkertaisesti selville tutkimalla kertoimien a_0 ja a_n tekijöiden eri osamääriä mahdollisina ratkaisuina. Mikäli tällä tavalla rationaalilukunollakohtia ei löydy, niin niitä ei ole. Lukiossa opetetaan tämän menetelmän avulla etsimään polynomien ratkaisuja, kun käsitellään kolmannen tai korkeamman asteen yhtälöitä. Taustalla oleva teoria jätetään yleensä käsittelemättä.

Apulause 4.2.2 *Olkoot $f(x)$, $g(x)$ ja $h(x) \in \mathbb{Z}[x]$ polynomeja, joille on voimassa $f(x) = g(x)h(x)$. Jos p on alkuluku, joka jakaa jokaisen polynomin $f(x)$ kertoimen, niin tällöin p jakaa jokaisen polynomin $g(x)$ kertoimen tai jokaisen polynomin $h(x)$ kertoimen.*

Todistus. [1, s. 324] Olkoon

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

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

$$h(x) = c_0 + c_1x + c_2x^2 + \cdots + c_sx^s$$

ja tehdään vastaoletus, että on olemassa polynomien $g(x)$ ja $h(x)$ kertoimia, joita alkuluku p ei jaa. Nyt p jakaa polynomin $f(x)$ jokaisen kertoimen. Polynomilla $g(x)$ on kerroin b_j sekä polynomilla $h(x)$ on kerroin c_k siten, että $p \nmid b_j$ ja $p \nmid c_k$. Oletetaan lisäksi, että kertoimien indeksit j ja k ovat pienimmät mahdolliset ei-negatiiviset kokonaisluvut. Polynomit $g(x)$ ja $h(x)$ keskenään kertomalla saadaan astetta $j + k$ olevan termin kertoimeksi $b_0c_{j+k}+\cdots+b_{j-1}c_{k+1}+b_jc_k+b_{j+1}c_{k-1}+\cdots+b_{j+k}c_0$. Toisaalta $f(x) = g(x)h(x)$, joten

$$a_{j+k} = b_0c_{j+k} + \cdots + b_{j-1}c_{k+1} + b_jc_k + b_{j+1}c_{k-1} + \cdots + b_{j+k}c_0.$$

Edelleen

$$b_jc_k = a_{j+k} - (b_0c_{j+k} + \cdots + b_{j-1}c_{k+1} + b_{j+1}c_{k-1} + \cdots + b_{j+k}c_0). \quad (**)$$

Koska j pienin sellainen ei-negatiivinen kokonaisluku, että $p \nmid b_j$ ja $p \mid b_0$, $p \mid b_1, \ldots, p \mid b_{j-1}$. Vastaavasti k on pienin sellainen ei-negatiivinen kokonaisluku, että $p \nmid c_k$ ja $p \mid c_0$, $p \mid c_1, \ldots, p \mid c_{k-1}$. Koska $p \mid a_{j+k}$ sekä $p \mid b_0c_{j+k}, \ldots, p \mid b_{j-1}c_{k+1}$, $p \mid b_{j+1}c_{k-1}, \ldots$ ja $p \mid b_{j+k}c_0$, niin p jakaa yhtälön $(**)$ oikean puolen, joten $p \mid b_jc_k$. Koska p on alkuluku, niin joko $p \mid b_j$ tai $p \mid c_k$, mikä on ristiriita tehdyn vastaoletuksen kanssa. Näin ollen alkuluku p jakaessa polynomin $f(x)$ jokaisen kertoimen, p jakaa joko polynomin $g(x)$ jokaisen kertoimen tai polynomin $h(x)$ jokaisen kertoimen. ■

Apulause 4.2.3 *Jos $f(x)$ on renkaan $\mathbb{Z}[x]$ polynomi, joka voidaan esittää tulona $f(x) = g(x)h(x)$ renkaassa $\mathbb{Q}[x]$, niin on olemassa sellaiset polynomit $g^*(x)$, $h^*(x) \in \mathbb{Z}[x]$, että $f(x) = g^*(x)h^*(x)$. Lisäksi* $\deg(g(x)) = \deg(g^*(x))$ *ja* $\deg(h(x)) = \deg(h^*(x))$.

Todistus. [1, s. 326] Oletetaan, että $f(x) = g(x)h(x)$, missä $g(x)$, $h(x) \in \mathbb{Q}[x]$. Jos a ja b ovat polynomien $g(x)$ ja $h(x)$ kertoimien nimittäjien pienimmät yhteiset monikerrat, niin tällöin polynomien $g'(x) = ag(x)$ ja $h'(x) = bh(x)$ kertoimet ovat kokonaislukuja. Nyt $abf(x) = abg(x)h(x) = [ag(x)][bh(x)] = g'(x)h'(x)$. Jos alkuluku p jakaa tulon ab, niin p jakaa polynomin $abf(x)$ jokaisen kertoimen. Apulauseen 4.2.2 mukaan p jakaa joko polynomin $g'(x)$ tai polynomin $h'(x)$ jokaisen kertoimen. Jos p jakaa polynomin $g'(x)$ jokaisen kertoimen ja luvulla p jaetaan polynomin $g'(x)$ jokainen termi, saadaan näin kokonaislukukertoiminen polynomi. Vastaavasti polynomin $h'(x)$ termit voidaan jakaa luvulla p, jos polynomin $h'(x)$ jokainen kerroin on jaollinen luvulla p. Koska tulolla ab on äärellinen määrä alkulukutekijöitä, voidaan toistuvasti jakaa yhtälön $abf(x) = g'(x)h'(x)$ molemmat puolet tulon ab alkulukutekijöillä. Äärellisen määrän vaiheita jälkeen saadaan yhtälö muotoon $f(x) = g^*(x)h^*(x)$, missä yhtälön oikean puolen polynomit $g^*(x)$ ja $h^*(x)$ ovat edelleen kokonaislukukertoimisia. On lisäksi selvää, etteivät polynomien $g(x)$ ja $h(x)$ asteluvut muutu, kun yhtälö jaetaan toistuvasti kokonaisluvuilla. Näin ollen $\deg(g(x)) = \deg(g^*(x))$ ja $\deg(h(x)) = \deg(h^*(x))$. ■

Ferdinaad Gotthold Eisenstein (1823-1852) oli saksalainen matemaatikko, joka tunnetaan parhaiten hänen nimeään kantavasta lauseesta polynomien jaottomuudelle.

Eisensteinin kriteeri jaottomuudelle 4.2.4 *Olkoon* $f(x) = a_0 + a_1x + \ldots + a_nx^n$ *polynomi renkaassa* $\mathbb{Z}[x]$. *Jos on olemassa sellainen alkuluku* p, *jolle*

(i) $p \mid a_i$, *kun* $i = 0, 1, 2, \ldots, n-1$,

(ii) $p \nmid a_n$,

(iii) $p^2 \nmid a_0$,

niin $f(x)$ *on jaoton renkaassa* $\mathbb{Q}[x]$.

Todistus. [1, s. 327] Jos $f(x)$ jaollinen renkaassa $\mathbb{Q}[x]$, niin on olemassa polynomit $g(x)$ ja $h(x) \in \mathbb{Q}[x]$ siten, että $f(x) = g(x)h(x)$. Lisäksi $n = s + t$, missä $1 \leq s, t \leq n$, $\deg(g(x)) = s$ ja $\deg(h(x)) = t$. Apulauseen 4.2.3 mukaan on olemassa sellaiset $g^*(x)$ ja $h^*(x) \in \mathbb{Z}[x]$, että $f(x) = g^*(x)h^*(x)$, $\deg(g(x)) = \deg(g^*(x))$ ja $\deg(h(x)) = \deg(h^*(x))$. Jos

$$\begin{aligned} g^*(x) &= b_0 + b_1x + \cdots + b_sx^s, \\ h^*(x) &= c_0 + c_1x + \cdots + c_tx^t, \end{aligned}$$

niin

$$a_0 + a_1x + \cdots + a_nx^n = (b_0 + b_1x + \cdots + b_sx^s)(c_0 + c_1x + \cdots + c_tx^t). \; (*)$$

Oletetaan nyt, että p on alkuluku, joka toteuttaa Eisensteinin kriteerin ehdot (i) – (iii). Olkoon $a_0 = b_0c_0$, ja koska p on alkuluku ja $p \mid a_0$, niin joko $p \mid b_0$ tai $p \mid c_0$. Tehdään vastaoletus, että molemmat $p \mid b_0$ ja $p \mid c_0$ ovat voimassa. Tällöin on olemassa sellaiset kokonaisluvut k_1 ja k_2, että $b_0 = pk_1$ ja $c_0 = pk_2$. Näin havaitaan, että $a_0 = b_0c_0 = p^2k_1k_2$, ja nyt $p^2 \mid a_0$. Tämä on kuitenkin ristiriidassa ehdon (iii) kanssa, joten ainoastaan toinen, $p \mid b_0$ tai $p \mid c_0$, voi olla voimassa. Oletetaan, että $p \mid b_0$ ja $p \nmid c_0$. Koska $a_n = b_sc_t$

ja ehdon (ii) mukaan $p \nmid a_n$, niin $p \nmid b_s$ ja $p \nmid c_t$. Olkoon k, $k \leq s < n$, pienin sellainen positiivinen kokonaisluku, että $p \nmid b_k$. Selvästi tällainen kokonaisluku on olemassa, sillä $p \nmid b_s$. Kun yhtälön $(*)$ molempien puolten termien x^k kertoimia verrataan keskenään, saadaan

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_kc_0,$$

ja näin ollen

$$b_kc_0 = a_k - (b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1). \, (**)$$

Koska $p \mid a_k$ ja k on pienin sellainen positiivinen kokonaisluku, että $p \nmid b_k$, niin kaikki yhtälön $(**)$ oikean puolen termit ovat jaollisia alkuluvulla p. Tästä seuraa, että $p \mid b_kc_0$, mikä on mahdotonta, sillä $p \nmid b_k$ ja $p \nmid c_0$. Vastaavasti voidaan käsitellä tapaus, jossa $p \nmid b_0$ ja $p \mid c_0$. Näin on saatu selville, että ehdot (i) – (iii) toteuttava polynomi $f(x)$ ei voi olla jaollinen renkaassa $\mathbb{Q}[x]$, joten polynomi $f(x)$ on jaoton renkaassa $\mathbb{Q}[x]$. ■

Edellisen todistuksen yhtälöön $(**)$ on korjattu lähdekirjallisuuden virhe lisäämällä puuttuneet sulkeet.

Määritelmä 4.2.5 *Jos polynomi* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$ *ja* p *on alkuluku, niin polynomia*

$$[f]_p(x) = [a_0] + [a_1]x + [a_2]x^2 + \cdots + [a_n]x^n \in \mathbb{Z}_p[x]$$

kutsutaan polynomia $f(x)$ *vastaavaksi renkaassa* $\mathbb{Z}_p[x]$ *polynomiksi.*

Lause 4.2.6 *Olkoon* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^n$ *renkaan* $\mathbb{Z}_p[x]$ *polynomi ja olkoon* p *sellainen alkuluku, jolle* $p \nmid a_n$. *Jos* $[f]_p(x)$ *on jaoton renkaan* $\mathbb{Z}_p[x]$, *niin* $f(x)$ *on jaoton renkaassa* $\mathbb{Q}[x]$.

Todistus. [1, s. 328] Jos $[f]_p(x)$ on jaoton renkaassa $\mathbb{Z}_p[x]$, niin $f(x)$ on joko jaoton renkaassa $\mathbb{Q}[x]$ tai se ei ole. Oletetaan, että $f(x)$ ei ole jaoton renkaassa $\mathbb{Q}[x]$. Nyt apulauseen 4.2.3 mukaan on olemassa sellaiset polynomit

$g(x)$, $h(x) \in \mathbb{Z}[x]$, jotka ovat positiivista astetta ja $f(x) = g(x)h(x)$. Koska a_n on polynomien $g(x)$ ja $h(x)$ johtavien kerrointen tulo ja $p \nmid a_n$, niin p ei voi jakaa polynomin $g(x)$ johtavaa kerrointa eikä polynomin $h(x)$ johtavaa kerrointa. Näin ollen

$$\deg([g]_p(x)) = \deg(g(x)) \quad \text{ja} \quad \deg([h]_p(x)) = \deg(h(x)),$$

eikä ole vaikea osoittaa, että $[f]_p(x) = [g]_p(x)[h]_p(x)$. Siis on löydetty positiivista astetta olevat polynomit $[g]_p(x)$, $[h]_p(x) \in \mathbb{Z}_p[x]$, jotka ovat polynomin $[f]_p(x)$ tekijät. Tämä on kuitenkin ristiriita, sillä $[f]_p(x)$ on jaoton renkaassa $\mathbb{Z}_p[x]$. Siis jos $[f]_p(x)$ on jaoton renkaassa $\mathbb{Z}_p[x]$, niin $f(x)$ on jaoton renkaassa $\mathbb{Q}[x]$. ■

Kirjallisuutta

[1] Bland, Paul E.: *The Basics of Abstract Algebra.*
W. H. Freeman and Company., 2001.

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

[3] Priestley, H.A.: *Introduction to Complex Analysis*
Oxford University Press Inc, 1985.