Eisensteinin kriteeri

LuK-tutkielma
Niilo Paavola
Matematiikan tutkinto-ohjelma
Oulun yliopisto
Kevät 2019

Sisältö

Johdanto

Tämän LuK-tutkielman aiheena on Eisensteinin kriteeri. Eisensteinin kriteerin avulla voidaan helposti osoittaa sopiva kokonaislukukertoiminen polynomi jaottomaksi polynomirenkaassa $\mathbb{Q}[x]$. Lähdeteosta [3] hyödynnetään tutkielman ensimmäisessä luvussa. Toisessa ja neljännessä luvussa käytetään teosta [2], johon pohjaa myös tutkielman aiheen eli Eisensteinin kriteerin todistaminen. Lähdeteosta [1] hyödynnetään läpi koko tutkielman.

Luvussa 1 määritellään lukuteorian peruskäsitteitä sekä kunta, jota tarvitsemme, jotta pystymme määrittelemään polynomirenkaan luvun 2 alussa. Luvussa 2 todistetaan kaksi tärkeää lausetta, joita tarvitsemme Eisensteinin kriteerin todistamiseen. Näitä todistuksia varten määritellään lisäksi termit yhteinen kerroin, alkeispolynomi ja aste.

Kolmas luku käsittelee polynomien jaollisuutta. Tässä luvussa määritellään mitä tarkoittaa polynomin nollakohta, polynomin jaottomuus ja polynomin jaollisuus. Lisäksi esitetään neljä lausetta, joista ensimmäisen todistaminen on sivuutettu tässä LuK-tutkielmassa. Näistä lauseista ensimmäistä hyödynnetään kolmannen lauseen todistamisessa ja vastaavasti toista ja kolmatta lausetta käytetään apuna neljännen lauseen todistamisessa. Näitä lauseita ei kuitenkaan tarvita Eisensteinin kriteerin todistamiseen, joten yhden todistuksen sivuuttaminen on perusteltua. Sivuutettu todistus löytyy lähdeteoksesta [1].

Neljännessä luvussa tutkitaan polynomien jaottomuutta polynomirenkaassa $\mathbb{Q}[x]$. Luvun alussa määritellään johtava kerroin, minkä jälkeen todistetaan kaksi polynomien jaottomuuteen liittyvää lausetta, joista jälkimmäinen on Eisensteinin kriteeri. Lisäksi tässä luvussa esitetään esimerkkejä kyseisistä lauseista.

1 Perusteita

Tässä luvussa määritellään lukuteorian peruskäsitteitä. Lisäksi määritellään kunta, jolla on kaksi binääristä operaatioita $(+)$ ja $(\cdot)$. Kommutatiivinen rengas $(K, +, \cdot)$ on kunta, mikäli $(K \setminus \{\mathbf{0}\}, \cdot)$ on Abelin ryhmä.

Määritelmä 1.1. Olkoon $p \in \mathbb{Z}$ ja $p > 1$. Jos luvulla p ei ole muita positiivisia tekijöitä lukujen 1 ja p lisäksi, niin lukua p kutsutaan *alkuluvuksi*.

Määritelmä 1.2. Olkoon $a, b \in \mathbb{Z}$ ja ainakin toinen luvuista a ja b nollasta poikkeava. Mikäli $t \in \mathbb{Z}_+$ toteuttaa ehdot

1. $t \mid a$ ja $t \mid b$;
2. jos $c \mid a$ ja $c \mid b$, niin $c \mid t$,

niin lukua t sanotaan lukujen a ja b *suurimmaksi yhteiseksi tekijäksi* ja sitä merkitään

$$t = syt(a, b).$$

Määritelmä 1.3. Olkoon $a, b \in \mathbb{Z}$. Mikäli $t \in \mathbb{Z}_+$ toteuttaa ehdot

1. $a \mid t$ ja $b \mid t$;
2. jos $a \mid c$ ja $b \mid c$, niin $t \mid c$,

niin lukua t sanotaan lukujen a ja b *pienimmäksi yhteiseksi jaettavaksi* ja sitä merkitään

$$t = pyj(a, b).$$

Määritelmä 1.4. Olkoon $K \neq \emptyset$. Tällöin $(K, +, \cdot)$ on *kunta*, jos se toteuttaa seuraavat ehdot:

1. $(K, +)$ on Abelin ryhmä:
   - $a + b \in K$ kaikilla $a, b \in K$,
   - $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in K$,
   - on olemassa *nolla-alkio* $\mathbf{0} \in K$, jolle $\mathbf{0} + a = a + \mathbf{0} = a$ kaikilla $a \in K$,
   - jokaiselle $a \in K$ on olemassa *vasta-alkio* $-a \in K$, jolle pätee $a + (-a) = -a + a = \mathbf{0}$,
   - $a + b = b + a$ kaikilla $a, b \in K$.
2. Operaatiolle $(\cdot)$ pätevät ehdot:

- $a \cdot b \in K$ kaikilla $a, b \in K$,
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ kaikilla $a, b, c \in K$,
- on olemassa *ykkösalkio* $\mathbf{1} \in K$, jolle $\mathbf{1} \cdot a = a \cdot \mathbf{1} = a$ kaikilla $a \in K$,
- jokaiselle $a \in K \setminus \{\mathbf{0}\}$ on olemassa *käänteisalkio* $a^{-1} \in K \setminus \{\mathbf{0}\}$, jolla pätee $a \cdot a^{-1} = a^{-1} \cdot a = \mathbf{1}$,
- $a \cdot b = b \cdot a$ kaikilla $a, b \in K$.

3. Osittelulait pätevät:
   - $a \cdot (b + c) = a \cdot b + a \cdot c$ kaikilla $a, b, c, \in K$,
   - $(a + b) \cdot c = a \cdot c + b \cdot c$ kaikilla $a, b, c \in K$.

Esimerkki 1.5. $(\mathbb{Z}, +, \cdot)$ ei ole kunta, koska jokaista alkiota $a \in \mathbb{Z} \setminus \{0\}$ kohti ei ole olemassa alkiota $a^{-1} \in \mathbb{Z} \setminus \{0\}$. Esimerkiksi $(\mathbb{Q}, +, \cdot)$ on kunta.

Lause 1.6. *Jäännösluokkarengas $(\mathbb{Z}_p, +, \cdot)$ on kunta tarkalleen silloin, kun p on alkuluku.*

Todistus. Todistettu lähdeteoksesa [1]. □

2 Polynomirengas

Tässä luvussa siirrytään syvemmälle tutkielman aiheeseen ja määritellään polynomirengas kunnan jatkoksi sekä muita tärkeitä polynomeihin liittyviä termejä. Lisäksi todistetaan Gaussin lemma ja että, jos kokonaislukukertoiminen polynomi voidaan esittää rationaalilukukertoimisten polynomien tulona, niin se voidaan esittää kokonaislukukertoimisten polynomien tulona.

Määritelmä 2.1. Olkoon $(K, +, \cdot)$ kunta. Joukkoa

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

varustettuna polynomien yhteen- ja kertolaskulla kutsutaan *polynomirenkaaksi kunnan K suhteen* ja sitä merkitään $(K[x], +, \cdot)$ tai $K[x]$.

Huomautus 2.2. Koska $(\mathbb{Z}, +, \cdot)$ ei ole kunta, emme voi määritelmän 2.1 perusteella määrittää polynomirengasta $(\mathbb{Z}[x], +, \cdot)$. Kuitenkin $(\mathbb{Q}, +, \cdot)$ on kunta ja $\mathbb{Z} \subset \mathbb{Q}$. Lisäksi nyt polynomirengas $(\mathbb{Q}[x], +, \cdot)$ on olemassa.

Merkintä 2.3. Merkinnällä $\mathbb{Z}[x]$ tarkoitetaan jatkossa polynomirenkaan $\mathbb{Q}[x]$ kokonaislukukertoimisten alkioiden joukkoa

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

Määritelmä 2.4. Olkoon

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Polynomin $p(x)$ kertoimien suurin yhteinen tekijä eli

$$syt(a_n, a_{n-1}, \ldots, a_1, a_0)$$

on polynomin $p(x)$ *yhteinen kerroin.*

Määritelmä 2.5. Polynomi $p(x) \in \mathbb{Z}[x]$ on *alkeispolynomi*, jos ja vain jos sen yhteinen kerroin on 1.

Esimerkki 2.6. Polynomin

$$f(x) = 21x^3 + 3x^2 + 6x + 33$$

yhteinen kerroin on

$$syt(21, 3, 6, 33) = 3.$$

Polynomin

$$g(x) = 21x^3 + 3x^2 + 6x + 13$$

yhteinen kerroin on

$$syt(21, 3, 6, 13) = 1.$$

Näin ollen polynomi $g(x)$ on alkeispolynomi, mutta polynomi $f(x)$ ei ole alkeispolynomi.

Lause 2.7. *(Gaussin lemma). Alkeispolynomien $f(x), g(x) \in \mathbb{Z}[x]$ tulo*

$$h(x) = f(x)g(x)$$

on alkeispolynomi.

Todistus. Olkoon

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

ja

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]$$

alkeispolynomeja. Olkoon $h(x) = f(x)g(x)$ ja olkoon $p \in \mathbb{Z}$ mikä tahansa alkuluku. Koska $f(x)$ on alkeispolynomi, löydetään sellainen kerroin a_{i_0}, että $p \nmid a_{i_0}$ mutta $p \mid a_n, \ldots, a_{i_0+1}$. Vastaavasti löydetään sellainen kerroin b_{j_0} niin, että $p \nmid b_{j_0}$ mutta $p \mid b_m, \ldots, b_{j_0+1}$. Olkoon $k = i_0 + j_0$. Nyt

$$\begin{aligned} h(x) &= f(x)g(x) \\ &= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) \cdot (b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0) \\ &= a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1}b_m)x^{n+m-1} + \cdots + \\ &\quad (a_k b_0 + a_{k-1}b_1 + \cdots + a_{i_0}b_{j_0} + \cdots + a_1 b_{k-1} + a_0 b_k)x^k + \cdots + \\ &\quad (a_1 b_0 + a_0 b_1)x + a_0 b_0. \end{aligned}$$

Tarkastellaan nyt polynomin $h(x)$ termiä

$$(a_k b_0 + a_{k-1}b_1 + \cdots + a_{i_0}b_{j_0} + \cdots + a_1 b_{k-1} + a_0 b_k)x^k.$$

Merkitään termin kerrointa

$$\begin{aligned} c_k &= a_k b_0 + a_{k-1}b_1 + \cdots + a_{i_0}b_{j_0} + \cdots + a_1 b_{k-1} + a_0 b_k \\ &= (a_k b_0 + a_{k-1}b_1 + \cdots + a_{i_0+1}b_{j_0-1}) + a_{i_0}b_{j_0} + \\ &\quad (a_{i_0-1}b_{j_0+1} + \cdots + a_1 b_{k-1} + a_0 b_k). \end{aligned}$$

Koska

$$p \mid a_n, \ldots, a_{i_0+1},$$

niin

$$p \mid (a_k b_0 + a_{k-1}b_1 + \cdots + a_{i_0+1}b_{j_0-1}),$$

ja koska

$$p \mid b_m, \ldots, b_{j_0+1},$$

niin

$$p \mid (a_{i_0-1}b_{j_0+1} + \cdots + a_1 b_{k-1} + a_0 b_k).$$

Jos nyt $p \mid a_{i_0}b_{j_0}$, niin $p \mid c_k$. Tiedetään kuitenkin, että $p \nmid a_{i_0}$ ja $p \nmid b_{j_0}$, joten $p \nmid a_{i_0}b_{j_0}$. Näin ollen $p \nmid c_k$.

Koska jokaista alkulukua p kohden on olemassa polynomin $h(x)$ jonkin termin kerroin c_k siten, että $p \nmid c_k$, niin polynomin $h(x)$ yhteinen kerroin on 1. Tällöin $h(x)$ on alkeispolynomi. □

Määritelmä 2.8. Olkoon $(K, +, \cdot)$ kunta ja

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x].$$

Suurinta lukua $i \in \{n, n-1, \ldots, 1, 0\}$, jolla $a_i \neq \mathbf{0}$, kutsutaan polynomin $f(x)$ *asteeksi*. Määritellään lisäksi, että nollapolynomin $f(x) = \mathbf{0}$ aste on $-\infty$. Jos polynomin $f(x)$ aste on n, sitä merkitään $deg\, f(x) = n$.

Lause 2.9. *Olkoon $f(x) \in \mathbb{Z}[x]$ ja $p(x), q(x) \in \mathbb{Q}[x]$. Jos polynomi $f(x)$ voidaan esittää muodossa $f(x) = p(x)q(x)$, niin on olemassa sellaiset polynomit $p_1(x), q_1(x) \in \mathbb{Z}[x]$, että $f(x) = p_1(x)q_1(x)$ ja lisäksi $deg\, p(x) = deg\, p_1(x)$ ja $deg\, q(x) = deg\, q_1(x)$.*

Todistus. Todistetaan ensin, että lause 2.9 pätee alkeispolynomien tapauksessa. Olkoon $f(x) \in \mathbb{Z}[x]$ alkeispolynomi ja olkoon polynomit

$$p(x) = \frac{a_n}{b_n}x^n + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + \cdots + \frac{a_0}{b_0}, q(x) = \frac{c_m}{d_m}x^m + \frac{c_{m-1}}{d_{m-1}}x^{m-1} + \cdots + \frac{c_0}{d_0} \in \mathbb{Q}[x]$$

sellaiset, että

$$f(x) = p(x)q(x).$$

Olkoon

$$s = pyj(b_n, b_{n-1}, \ldots, b_0) \in \mathbb{Z}_+$$

polynomin $p(x)$ kertoimien nimittäjien pienin yhteinen jaettava, ja olkoon

$$t = pyj(d_m, d_{m-1}, \ldots, d_0) \in \mathbb{Z}_+$$

polynomin $q(x)$ kertoimien nimittäjien pienin yhteinen jaettava. Tällöin polynomien $sp(x)$ ja $tq(x)$ kertoimet ovat kokonaislukuja, joten

$$sp(x), tq(x) \in \mathbb{Z}[x].$$

Koska $f(x) \in \mathbb{Z}[x]$ ja $s, t \in \mathbb{Z}_+$, myös $stf(x) \in \mathbb{Z}[x]$. Olkoon polynomin $sp(x)$ yhteinen kerroin c_p ja olkoon polynomin $tq(x)$ yhteinen kerroin c_q. Koska c_p jakaa kaikki polynomin $sp(x)$ kertoimet, niin on olemassa sellainen polynomi $p_1(x) \in \mathbb{Z}[x]$, että $sp(x) = c_p p_1(x)$. Vastaavasti saadaan, että $tq(x) = c_q q_1(x)$,

missä $q_1(x) \in \mathbb{Z}[x]$. Koska c_p ja c_q ovat polynomien $sp(x)$ ja $tq(x)$ yhteiset kertoimet, niin selvästi $p_1(x)$ ja $q_1(x)$ ovat alkeispolynomeja. Lisäksi koska

$$s, c_p, t, c_q \in \mathbb{Z},$$

niin $deg\, p(x) = deg\, p_1(x)$ ja $deg\, q(x) = deg\, q_1(x)$. Nyt

$$stf(x) = stp(x)q(x) = c_p c_q p_1(x) q_1(x). \tag{1}$$

Koska $f(x)$ on alkeispolynomi, st on yhtälön (1) vasemman puolen yhteinen kerroin. Koska $p_1(x)$ ja $q_1(x)$ ovat alkeispolynomeja, niin Gaussin lemman 2.7 perusteella myös niiden tulo $p_1(x)q_1(x)$ on alkeispolynomi. Niinpä $c_p c_q$ on yhtälön (1) oikean puolen yhteinen kerroin ja saadaan

$$st = c_p c_q.$$

Näin ollen, koska

$$stf(x) = c_p c_q p_1(x) q_1(x),$$

niin

$$f(x) = p_1(x) q_1(x).$$

Löydettiin siis polynomit $p_1(x)$ ja $q_1(x)$, jotka toteuttavat lauseen 2.9 alkeispolynomin $f(x)$ tapauksessa. Osoitetaan vielä, että lause pätee yleisesti.

Olkoon polynomi $g(x) \in \mathbb{Z}[x]$ ja olkoon polynomit $h(x), i(x) \in \mathbb{Q}[x]$ sellaiset, että

$$g(x) = h(x)i(x).$$

Olkoon c polynomin $g(x)$ yhteinen kerroin. Nyt voidaan muodostaa alkeispolynomi $g_1(x) = \frac{g(x)}{c} \in \mathbb{Z}[x]$. Tällöin $g_1(x)$ voidaan esittää myös muodossa

$$g_1(x) = \frac{g(x)}{c} = \frac{h(x)i(x)}{c} = \left(\frac{1}{c}h(x)\right) i(x),$$

missä $\frac{1}{c}h(x), i(x) \in \mathbb{Q}[x]$. Olemme jo osoittaneet, että lause 2.9 pätee alkeispolynomeille, joten löydetään sellaiset $h_1(x)$ ja $i_1(x) \in \mathbb{Z}[x]$, että

$$g_1(x) = h_1(x) i_1(x).$$

Lisäksi $deg\, \frac{1}{c}h(x) = deg\, h_1(x)$ ja $deg\, i(x) = deg\, i_1(x)$. Nyt saadaan

$$g(x) = c g_1(x) = c(h_1(x) i_1(x)) = (c h_1(x)) i_1(x),$$

missä $ch_1(x), i_1(x) \in \mathbb{Z}[x]$. Selvästi myös

$$deg\, h(x) = deg\, \frac{1}{c}h(x) = deg\, h_1(x) = deg\, ch_1(x)$$

ja

$$deg\, i(x) = deg\, i_1(x).$$

□

3 Polynomin jaollisuus

Polynomien jaollisuus ja jaottomuus on tämän luvun aiheena. Luvussa määritellään termit jaoton ja jaollinen sekä todistetaan niihin liittyviä lauseita.

Lause 3.1. *(Jakoalgoritmi polynomeille). Mikäli $f(x), g(x) \in K[x]$ ja $g(x) \neq \mathbf{0}$, niin on olemassa sellaiset yksikäsitteiset polynomit $q(x), r(x) \in K[x]$, että*

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

missä $\deg r(x) < \deg g(x)$.

Todistus. Ohitetaan tässä LuK-tutkielmassa. Todistus löydettävissä Myllylän, Niemenmaan ja Törmän (2018) esittämänä Algebralliset rakenteet luentorungosta [1]. □

Määritelmä 3.2. Olkoon

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$$

ja $a \in K$. Jos $f(a) = \mathbf{0}$, niin a on polynomin $f(x)$ *nollakohta* eli yhtälön $f(x) = \mathbf{0}$ *juuri.*

Lause 3.3. *Polynomirenkaan $K[x]$ 1. asteen polynomilla on aina nollakohta kunnassa K.*

Todistus. Olkoon $f(x) = ax + b \in K[x]$, missä $a, b \in K$ ja $a \neq \mathbf{0}$. Asetetaan nyt

$$f(x) = \mathbf{0}$$

eli

$$ax + b = \mathbf{0}.$$

Koska K on kunta, $b \in K$ ja $a \in K \setminus \{\mathbf{0}\}$, niin on olemassa alkiot $-b, a^{-1} \in K$. Lisäämällä äskeiseen yhtälöön puolittain termi $-b$ saadaan

$$\begin{aligned} & (ax + b) - b = \mathbf{0} - b \\ \iff & ax + (b - b) = -b \\ \iff & ax + \mathbf{0} = -b \\ \iff & ax = -b. \end{aligned}$$

Kertomalla nyt yhtälö puolittain vasemmalta alkiolla a^{-1} saadaan

$$\begin{aligned} & a^{-1}(ax) = a^{-1}(-b) \\ \iff & (a^{-1}a)x = a^{-1}(-b) \\ \iff & \mathbf{1} \cdot x = a^{-1}(-b) \\ \iff & x = a^{-1}(-b). \end{aligned}$$

Koska $a^{-1}, -b \in K$, niin $x = a^{-1}(-b) \in K$. Näin ollen 1. asteen polynomilla on aina nollakohta kunnassa K. □

Määritelmä 3.4. Olkoon $f(x), g(x) \in K[x]$. Jos $f(x) = g(x)q(x)$ eräällä $q(x) \in K[x]$, niin sanotaan, että polynomi $g(x)$ *jakaa* polynomin $f(x)$ ja sitä merkitään $g(x) \mid f(x)$.

Lause 3.5. *Olkoot $f(x) \in K[x]$ ja $a \in K$. Tällöin*

$$f(a) = \boldsymbol{0} \iff (x - a) \mid f(x).$$

Todistus. Olkoon $f(x) \in K[x]$ ja $a \in K$.
1° Oletetaan, että $(x - a) \mid f(x)$. Tällöin on olemassa sellainen polynomi $g(x) \in K[x]$, että

$$f(x) = (x - a) \cdot g(x).$$

Tällöin

$$f(a) = (a - a) \cdot g(a) = \mathbf{0} \cdot g(a) = \mathbf{0}.$$

2° Oletetaan, että $f(a) = \mathbf{0}$. Nyt lauseen 3.1 perusteella on olemassa sellaiset $q(x), r(x) \in K[x]$, että

$$f(x) = q(x) \cdot (x - a) + r(x)$$

ja

$$deg\, r(x) < deg\, (x - a) = 1.$$

Tästä seuraa, että $deg\, r(x) = 0$ tai $deg\, r(x) = -\infty$, eli $r(x)$ on vakiopolynomi. Merkitään nyt, $r(x) = C$, missä $C \in K$. Näin ollen

$$f(x) = q(x) \cdot (x - a) + C$$

ja

$$\begin{aligned} \mathbf{0} &= f(a) \\ &= q(a) \cdot (a - a) + C \\ &= q(a) \cdot \mathbf{0} + C \\ &= C. \end{aligned}$$

Nyt siis

$$f(x) = q(x) \cdot (x - a)$$

eli

$$(x - a) \mid f(x).$$

□

Määritelmä 3.6. Olkoon polynomi $f(x) \in K[x]$. Polynomi $f(x)$ on *jaoton* polynomirenkaassa $K[x]$, jos $deg\, f(x) \geq 1$ ja jos ei ole olemassa polynomeja $g(x), h(x) \in K[x]$ niin, että $deg\, g(x) \geq 1, deg\, h(x) \geq 1$ ja $f(x) = g(x)h(x)$. Jos polynomi ei ole jaoton, sanotaan, että se on *jaollinen.*

Lause 3.7. *Olkoon $f(x) \in K[x]$. Olkoon lisäksi $deg\, f(x) = 2$ tai $deg\, f(x) = 3$. Tällöin $f(x)$ on jaoton jos ja vain jos sillä ei ole nollakohtaa kunnassa K.*

Todistus. Olkoon $f(x) \in K[x]$.
1° Oletetaan, että $f(x)$ jaoton. Tehdään vastaoletus, että polynomilla $f(x)$ on nollakohta $a \in K$. Nyt lauseen 3.5 perusteella

$$(x - a) \mid f(x)$$

eli $f(x)$ ei ole jaoton. Tämä on ristiriita, joten polynomilla $f(x)$ ei ole nollakohtia.
2° Oletetaan, että polynomilla $f(x)$ ei ole nollakohtia. Tehdään vastaoletus, että $f(x)$ ei ole jaoton. Tällöin

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

missä $1 \leq deg\, q(x)$ ja $1 \leq deg\, g(x)$. Olkoon

$$\begin{aligned} f(x) &= a_n x^n + \cdots + a_1 x + a_0, \\ q(x) &= b_m x^m + \cdots + b_1 x + b_0, \\ g(x) &= c_k x^k + \cdots + c_1 x + c_0, \end{aligned}$$

missä $a_n, b_m, c_k \neq \mathbf{0}$. Tällöin $deg\, f(x) = n > 1$, deg $q(x) = m \geq 1$ ja $deg\, g(x) = k \geq 1$. Nyt

$$\begin{aligned} a_n x^n + \cdots + a_1 x + a_0 &= (b_m x^m + \cdots + b_1 x + b_0)(c_k x^k + \cdots + c_1 x + c_0) \\ &= b_m c_k x^{m+k} + \cdots + b_0 c_0. \end{aligned}$$

Koska $b_m, c_k \neq \mathbf{0}$, niin $b_m c_k \neq \mathbf{0}$, sillä kunnassa ei ole nollanjakajia. Näin ollen

$$n = m + k,$$

eli

$$deg\, f(x) = deg\, q(x) + deg\, g(x).$$

Jos $deg\, f(x) = 2$, niin $deg\, q(x) = 1 = deg\, g(x)$, sillä $deg\, q(x), deg\, g(x) \geq 1$. Jos $deg\, f(x) = 3$, niin polynomeista $q(x)$ ja $g(x)$ toisen polynomin aste on 1 ja toisen polynomin aste on 2, sillä $deg\, q(x), deg\, g(x) \geq 1$. Näin ollen, jos $deg\, f(x) = 2$ tai $deg\, f(x) = 3$, niin ainakin toinen polynomeista $q(x)$ ja $g(x)$ on 1. asteen polynomi. Koska astetta 1 olevalla polynomilla on aina nollakohta kunnassa K lauseen 3.3 perusteella, niin myös polynomilla $f(x)$ on nollakohta. Tämä on ristiriita, joten polynomi $f(x)$ on jaoton. □

4 Polynomin jaottomuus polynomirenkaassa $\mathbb{Q}[x]$

Tässä luvussa tutkitaan polynomien jaottomuutta polynomirenkaassa $\mathbb{Q}[x]$. Luvussa todistetaan kaksi tehokasta lausetta jaottomuuden tutkimiseen, joista ensimmäistä kutsutaan modulo p jaottomuustestiksi. Jälkimmäinen lause ja samalla tämän tutkielman viimeinen lause on Eisensteinin kriteeri. Lisäksi tässä luvussa esitetään esimerkkejä näiden lauseiden käytöstä.

Määritelmä 4.1. Olkoon

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$$

ja olkoon $a_n \neq \mathbf{0}$. Tällöin a_n on polynomin $f(x)$ *johtava kerroin.*

Lause 4.2. *Olkoon polynomi*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

ja olkoon p alkuluku. Olkoon

$$f_p(x) = [a_n]x^n + [a_{n-1}]x^{n-1} + \cdots + [a_1]x + [a_0] \in \mathbb{Z}_p[x].$$

Jos $deg\, f(x) = deg\, f_p(x)$ ja $f_p(x)$ on jaoton polynomirenkaassa $\mathbb{Z}_p[x]$, niin $f(x)$ on jaoton kokonaislukukertoimisten polynomien joukossa $\mathbb{Z}[x]$.

Todistus. Olkoon $i : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ funktio, joka kuvaa polynomin kertoimet jäännösluokiksi $mod\, p$. Tällöin

$$\begin{aligned} i(f(x)) &= i(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) \\ &= [a_n]x^n + [a_{n-1}]x^{n-1} + \cdots + [a_1]x + [a_0] \\ &= f_p(x). \end{aligned}$$

Olkoon $f_p(x)$ jaoton polynomirenkaassa $\mathbb{Z}_p[x]$ ja tehdään vastaoletus, että polynomi $f(x)$ on jaollinen polynomirenkaassa $\mathbb{Z}[x]$. Tällöin on olemassa sellaiset polynomit

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0, h(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_0 \in \mathbb{Z}[x],$$

että $f(x) = g(x)h(x)$ ja $0 < deg\, g(x), deg\, h(x) < deg\, f(x)$. Olkoon p sellainen alkuluku, että $p \nmid a_n$ eli $[a_n] \neq [0]$, missä a_n on polynomin $f(x)$ johtava kerroin. Koska $a_n = b_m c_k$, niin $p \nmid b_m$ ja $p \nmid c_k$ eli p ei jaa polynomien $g(x)$ ja $h(x)$ johtavia kertoimia eli $[b_m] \neq [0]$ ja $[c_k] \neq [0]$. Olkoon $i(g(x)) = g_p(x)$

ja $i(h(x)) = h_p(x)$. Tällöin $deg\, f(x) = deg\, f_p(x)$, $deg\, g(x) = deg\, g_p(x)$ ja $deg\, h(x) = deg\, h_p(x)$. Nyt

$$\begin{aligned} f_p(x) &= [a_n]x^n + [a_{n-1}]x^{n-1} + \cdots + [a_1]x + [a_0] \\ &= [b_m c_k]x^n + ([b_m c_{k-1} + b_{m-1}c_k])x^{n-1} + \cdots + [b_0 c_0] \\ &= [b_m][c_k]x^n + ([b_m][c_{k-1}] + [b_{m-1}][c_k])x^{n-1} + \cdots + [b_0][c_0] \\ &= ([b_m]x^m + [b_{m-1}]x^{m-1} + \cdots + [b_0])([c_k]x^k + [c_{k-1}]x^{k-1} + \cdots + [c_0]) \\ &= g_p(x)h_p(x). \end{aligned}$$

Siis $f_p(x)$ on jaollinen polynomirenkaassa $\mathbb{Z}_p[x]$, koska

$$0 < deg\, g_p(x), deg\, h_p(x) < deg\, f_p(x).$$

Tämä on ristiriita oletuksen kanssa ja niinpä polynomin $f(x)$ täytyy olla jaoton joukossa $\mathbb{Z}[x]$. □

Esimerkki 4.3. Olkoon

$$f(x) = 17x^3 - x^2 - 4x + 5 \in \mathbb{Z}[x].$$

Tällöin

$$f_2(x) = x^3 + x^2 + [1] \in \mathbb{Z}_2[x]$$

ja selvästi 2 on alkuluku. Koska

$$f_2([1]) = [1]$$

ja

$$f_2([0]) = [1],$$

niin polynomilla $f_2(x)$ ei ole nollakohtaa. Koska $deg\, f_2(x) = 3$, niin lauseen 3.7 nojalla $f_2(x)$ on jaoton polynomirenkaassa $\mathbb{Z}_2[x]$. Koska $deg\, f_2(x) = deg\, f(x)$, niin $f(x)$ on jaoton joukossa $\mathbb{Z}[x]$.

Lause 4.4. *(Eisensteinin kriteeri) Olkoon polynomi*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Jos on olemassa sellainen alkuluku p, että

1. $p \nmid a_n$,
2. $p \mid a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ *ja*
3. $p^2 \nmid a_0$,

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

Todistus. Olkoon p alkuluku, joka toteuttaa Eisensteinin kriteerin ehdot polynomille

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Tällöin $p \nmid a_n$, $p \mid a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ ja $p^2 \nmid a_0$. Tehdään vastaoletus, että $f(x)$ olisi jaollinen polynomirenkaassa $\mathbb{Q}[x]$ eli $f(x) = g_1(x)h_1(x)$, missä $g_1(x), h_1(x) \in \mathbb{Q}[x]$. Tällöin $deg\, f(x) = n$ sekä $n > deg\, g_1(x) \geq 1$ ja $n > deg\, h_1(x) \geq 1$. Vastaavasti lauseen 2.9 nojalla on olemassa polynomit $g(x), h(x) \in \mathbb{Z}[x]$, joilla $f(x) = g(x)h(x)$. Lisäksi tällöin $deg\, g_1(x) = deg\, g(x)$ ja $deg\, h_1(x) = deg\, h(x)$. Olkoon

$$g(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$$

ja olkoon

$$h(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0.$$

Tiedetään, että $p \mid a_0$ eli $p \mid b_0 c_0$. Jos $p \mid b_0$ ja $p \mid c_0$, niin $p^2 \mid b_0 c_0$. Tämä ei ole mahdollista oletuksen $p^2 \nmid a_0$ perusteella, ja tästä seuraa, että p jakaa tasan jomman kumman vakioista b_0 ja c_0. Oletetaan nyt, että $p \mid b_0$ mutta $p \nmid c_0$. Nyt polynomin $f(x)$ johtava kerroin on $a_n = b_k c_m$. Koska $p \nmid a_n$, niin $p \nmid b_k$ ja $p \nmid c_m$. Täten löytyy pienin mahdollinen indeksi i siten, että $p \nmid b_i$ mutta $p \mid b_{i-1}, \ldots, b_0$. Lisäksi selvästi $i \neq n$, $i \neq 0$ ja

$$a_i = b_i c_0 + b_{i-1}c_1 + \cdots + b_1 c_{i-1} + b_0 c_i.$$

Tästä saadaan

$$a_i - (b_{i-1}c_1 + \cdots + b_1 c_{i-1} + b_0 c_i) = b_i c_0.$$

Nyt $p \mid a_i$ oletuksen perusteella ja $p \mid b_{i-1}, \ldots, b_0$, joten $p \mid b_i c_0$. Tämä on ristiriita, koska p on alkuluku ja lisäksi $p \nmid b_i$ ja $p \nmid c_0$. Näin ollen polynomi $f(x)$, joka täyttää Eisensteinin kriteerin ehdot, todellakin on jaoton polynomirenkaassa $\mathbb{Q}[x]$. □

Esimerkki 4.5. Olkoon polynomi

$$p(x) = 20x^5 + 15x^4 + 3x^3 + 27x^2 + 75x + 6 \in \mathbb{Z}[x].$$

Tällöin löytyy alkuluku 3, joka ei jaa polynomin $p(x)$ johtavaa kerrointa 20 mutta jakaa polynomin $p(x)$ kaikki muut kertoimet. Koska lisäksi $3^2 \nmid 6$, niin polynomi $p(x)$ on Eisensteinin kriteerin perusteella jaoton polynomirenkaassa $\mathbb{Q}[x]$.

Esimerkki 4.6. Tutkitaan polynomin

$$f(x) = 453x^5 + 143x^4 - 242x^3 - 77x$$

jaollisuutta polynomirenkaassa $\mathbb{Q}[x]$. Huomataan aluksi, että

$$f(x) = x(453x^4 + 143x^3 - 242x^2 - 77)$$

ja merkitään nyt jälkimmäistä polynomia $g(x)$:llä, jolloin

$$f(x) = x \cdot g(x).$$

Etsitään nyt polynomin $g(x)$ kertoimien alkulukutekijähajotelmat:

$$\begin{aligned} 453 &= 3 \cdot 151, \\ 143 &= 11 \cdot 13, \\ 242 &= 2 \cdot 11 \cdot 11, \\ 77 &= 7 \cdot 11. \end{aligned}$$

Näin ollen

$$\begin{aligned} 11 &\nmid 453, \\ 11 &\mid 143, \\ 11 &\mid 242, \\ 11 &\mid 77, \\ 11^2 &\nmid 77. \end{aligned}$$

Koska 11 on alkuluku, niin Eisensteinin kriteerin perusteella $g(x)$ on jaoton polynomirenkaassa $\mathbb{Q}[x]$. Täten polynomin $f(x)$ tekijöihinjako polynomirenkaassa $\mathbb{Q}[x]$ on

$$f(x) = x(453x^4 + 143x^3 - 242x^2 - 77).$$

Lähdeluettelo

[1] Myllylä, K., Niemenmaa, M. & Törmä, T. (2018). *802355A Algebralliset rakenteet: Luentorunko*. Matemaattisten tieteiden tutkimusyksikkö. Oulun yliopisto.

[2] Nicodemi, O. E., Sutherland, M. A. & Towsley, G. W. (2007). *An introduction to abstract algebra: With notes to the future teacher*. Upper Saddle River (N.J.): Pearson /Prentice Hall.

[3] Niemenmaa, M., Myllylä, K. & Törmä, T. (2019). *802354A Algebran perusteet: Luentorunko*. Matemaattisten tieteiden tutkimusyksikkö. Oulun yliopisto.