JYVÄSKYLÄN YLIOPISTO
MATEMATIIKAN JA TILASTO-
TIETEEN LAITOS

Pro gradu-tutkielma

Transkendenttiluvut

Mia Viitala

5. kesäkuuta 2024

Tekijä
Mia Viitala

Otsikko
Transkendenttiluvut (engl. Transcendental numbers)

Tutkinto-ohjelma
Matematiikan aineenopettajan maisteriohjelma

Päivämäärä	**Sivumäärä**
5. kesäkuuta 2024	44

Tiivistelmä

Tämän pro gradu -tutkielman tarkoituksena on perehtyä transkendenttilukuihin sekä algebrallisiin lukuihin. Algebrallinen luku on jonkin rationaalilukukertoimisen polynomin juuri. Jos luku ei ole algebrallinen niin se on transkendentti. Tutkielmassa aihetta lähestytään kuntien, kuntalaajennosten sekä symmetristen polynomien kautta. Tutkielman tarkoituksena on antaa tiivis yleiskuvaus aiheesta.

Ensin tutkielmassa perehdytään pohjatietona rationaali- ja irrationaalilukuihin sekä erityisesti esitetään todistukset lukujen π ja e irrationaalisuudesta luvussa 1. Pohjatietojen käsittelyn jälkeen annetaan määritelmä transkendenttiluvulle ja algebralliselle luvulle. Tästä siirrytään tarkastelemaan tutkielmassa myöhemmin tarvittavaa perusalgebraa luvussa 2. Luvussa 3 perehdytään polynomirenkaisiin sekä symmetrisiin polynomeihin. Samassa luvussa todistetaan symmetristen polynomien peruslause 3.19, jolla on oleellinen osa tutkielman päätuloksien todistuksissa.

Luvussa 4 tutustaan kuntalaajennoksiin ja erilaisiin niitä koskeviin tuloksiin. Luvussa 5 käsitellään algebrallisten lukujen ominaisuuksia ja osoitetaan, että algebralliset luvut muodostavat kunnan. Tutkielman päätuloksina luvussa 6 esitetään todistukset lukujen π ja e transkendenttiudesta. Tutkielman lopuksi luvussa 6 esitellään vielä, miten luvun π transkendenttius liittyy antiikin konstruktio-ongelmaan ympyrän neliöinnistä ja samassa luvussa esitellään myös kuution kahdentamiseen liittyvä konstruktio-ongelma. Tämän lisäksi otetaan pieni katsaus siihen millaisiin transkendenttilukuihin liittyviin ratkaisemattomiin ongelmiin nykypäivän matemaatikot yrittävät löytää ratkaisuja.

Sisällys

Johdanto

Tutustumme tutkielmassa transkendenttilukuihin sekä algebrallisiin lukuihin ja niiden ominaisuuksiin. Algebrallinen luku on jonkin rationaalilukukertoimisen polynomin juuri. Luvut, jotka eivät ole algebrallisia, ovat transkendenttejä. Tunnetuimmat transkendenttiluvut ovat ympyrän kehän ja halkaisijan suhdetta kuvaava luku π ja Neperin luku e.

Transkendenttilukuja on tutkittu matematiikan historian saatossa useamman sadan vuoden ajan. Jo 1700-luvun lopussa matemaatikko Johann Lambert esitti väitteen lukujen π ja e transkendenttiudesta julkaisussaan, jossa hän esitti todistuksen luvun π irrationaalisuudesta. Kuitenkin vasta 1800-luvun loppupuolella ensimmäiset luvut onnistuttiin todistamaan transkendenteiksi. Tätä pitkää väliä väitteiden ja niiden todistusten välillä selittää se, että transkendenttilukujen todistuksiin liittyy teknisiä haasteita eikä yleistä menetelmää luvun transkendentiksi todistamiselle tunneta.

Ensimmäisen todistuksen Neperin luvun e transkendenttiudesta esitti ranskalainen matemaatikko Charles Hermite vuonna 1873. Tässä tutkielmassa toinen luvussa 6 esitetyistä päätuloksista on luvun e transkendenttiuden osoittaminen niin, että todistus mukailee Hermiten alkuperäistä todistusta. Yhdeksän vuotta Hermiten todistuksen jälkeen vuonna 1882 saksalainen matemaatikko Ferninand von Lindemann julkaisi todistuksen, jossa hän osoitti luvun π olevan transkendenttiluku kun ensimmäinen todistus luvun π irrationaalisuudesta oli esitetty jo yli sata vuotta aiemmin. Lindemanin esitystä mukaileva todistus luvun π transkendenttiudesta esitellään luvussa 6.

Osoittaessaan luvun π olevan transkendentti Lindemann tuli samalla ratkaisseeksi yhden antiikin kolmesta suuresta konstruktio-ongelmasta. Luvulle π ei Lindemannin todistuksen mukaisesti voida löytää rationaalilukukertoimista polynomia, jonka juuri se olisi ja tästä seuraa se, että annetulle ympyrälle ei voida konstruoida pinta-alaltaan yhtä suurta neliötä. Luvussa 6 tutkielman lopussa esitellään ympyrän neliöinnin konstruktio-ongelma tarkemmin ja tutustutaan myös kuution kahdentamiseen.

Ennen kuin tutkielmassa päästään käsiksi sen päätuloksiin, esitellään pohjatietoja, jotka johdattelevat lukijan aiheeseen tutumpien matemaattisten tulosten kautta. Ensimmäisessä luvussa 1 annetaan määritelmät rationaali- ja irrationaaliluvuille ja käydään läpi useampi todistus eri lukujen irrationaalisuudesta. Tutkielman aihetta lähestytään aluksi irrationaalilukujen kautta, koska jokainen transkendenttiluku on myös irrationaaliluku. Toiseen suuntaan väite ei ole totta eli jokainen irrationaaliluku ei ole transkendentti. Esimerkki tällaisesta luvusta on $\sqrt{2}$, jonka irrationaalisuus on todistettu luvussa 1. Luku $\sqrt{2}$ on siis irrationaaliluku, mutta se ei ole transkendentti, koska se on polynomin $P(x) = x^2 - 2$ juuri.

Irrationaalilukujen tarkastelun jälkeen tutkielmassa määritellään algebrallinen luku ja transkendenttiluku. Tämän jälkeen siirrytään perusalgebraan ja tutkielman päätavoitteen kannalta olennaisiin määritelmiin ja tuloksiin renkaisiin, kuntiin ja vektoriavaruuksiin liittyen luvussa 2.

Luvussa 3 käsitellään polynomirenkaita ja symmetrisiä polynomeja. Polynomi on symmetrinen silloin, kun sen muuttujien järjestystä vaihtamalla itse polynomi ei muutu. Lukijalle esitellään Eisensteinin kriteeri polynomien jaottomuudesta ja polynomien jakoalgoritmi. Samassa luvussa käydään läpi myös symmetristen polynomien peruslause 3.19, jota tarvitsemme tutkielman loppupuolella usean eri tuloksen todistuksissa. Lauseen mukaan mikä tahansa polynomirenkaan $R[x_1, \ldots, x_n]$ symmetrinen polynomi voidaan esittää alkeispolynomien polynomina siten, että polynomin kertoimet ovat renkaassa R. Erityisesti algebrallisten lukujen ominaisuuksia tutkittaessa luvussa 5 kyseinen lause pääsee käyttöön. Tässä tutkielmassa on haluttu nostaa symmetriset polynomit ja erityisesti symmetristen polynomien peruslause 3.19 esiin, koska niiden hyödyntäminen lauseiden 5.4 ja 5.5 todistuksissa on harvinaisempi lähestymistapa.

Luvussa 4 hyödynnetään tutkielmassa aiemmin esiteltyjä määritelmiä sekä tuloksia ja tutustaan kuntalaajennoksiin. Algebrallisista luvuista tiedetään transkendenttilukuja enemmän, joten luvussa 5 keskitytään algebrallisten lukujen ominaisuuksiin. Algebralliset luvut muodostavat kunnan ja tämän osoittaminen on luvun 5 pääsisältö.

Viimeisessä luvussa 6 esitellään tutkielman päätulokset lukujen π ja e transkendenttiudesta ja perehdytään kahteen antiikin aikaiseen konstruktioongelmaan ja osoitetaan ne mahdottomiksi. Transkendenttilukuihin liittyy edelleen avoimia kysymyksiä, joihin nykyiset sekä tulevat matemaatikot koittavat löytää vastauksia. Kiinnostavaan transkendenttilukuihin liittyvään ratkaisemattomaan ongelmaan tutustutaan lyhyesti tutkielman lopussa ja samalla pohditaan transkendenttilukujen tutkimisen tulevaisuutta.

Tämän tutkielman pääasiallisena lähteenä on käytetty Ian Stewartin kirjaa Galois theory [10]. Stewartin kirjaa on tarpeen tullen täydennetty muilla lähteillä kuten Langin kirjalla [7] ja Kahanpään luentomonisteella [4]. Historiallisina lähteinä luvussa 1 on käytetty Stainvillen kirjaa [2] ja Jeffreysin kirjaa [3], joissa on julkaistu todistukset lukujen e ja π irrationaalisuudesta ja täydentävänä lähteenä on käytetty Roegelin artikkelia [9]. Lineaarialgebran määritelmien ja tulosten lähteinä luvussa 2 on käytetty Petersenin kirjaa [8] ja Äkkisen luentomonistetta [11]. Luvussa 3 symmetrisiä polynomeja käsiteltäessä on käytetty lähteenä Daoubin julkaisua [1].

1 Irrationaaliluvut

1.1 Rationaaliluvut ja irrationaaliluvut

Ennen kuin ryhdymme tarkastelemaan tutkielman pääaihetta eli transkendenttilukuja, niin pohjustetaan aihetta käsittelemällä irrationaalilukuja sekä niiden ominaisuuksia. Aloitetaan antamalla rationaali- ja irrationaaliluvulle määritelmät.

Määritelmä 1.1. Luku $q \in \mathbb{R}$ on rationaaliluku, jos on olemassa luvut $a \in \mathbb{Z}$ ja $b \in \mathbb{N}$ siten, että

$$q = \frac{a}{b}.$$

Luku $r \in \mathbb{R}$ on irrationaaliluku, jos se ei ole rationaaliluku.

Merkitään rationaalilukujen joukkoa kirjaimella $\mathbb{Q}$ ja olkoon irrationaalilukujen joukon merkintä $\mathbb{R} \setminus \mathbb{Q}$. Yksittäisen luvun irrationaalisuuden osoittaminen ei ole aina helppoa eikä ole olemassa tiettyä menetelmää, joka toimisi kaikissa reaalilukujen tapauksissa. Tarkastellaan seuraavaksi muutamaa erilaista reaalililukua ja kuinka niiden irrationaalisuus voidaan osoittaa.

Lause 1.2. *Luku $\sqrt{2}$ on irrationaaliluku.*

Todistus. Todistetaan väite epäsuoran todistuksen avulla eli muodostetaan vastaoletus: Luku $\sqrt{2}$ on rationaaliluku. Rationaaliluvun määritelmän mukaisesti on olemassa luvut $a \in \mathbb{Z}$ ja $b \in \mathbb{N}$ siten, että

$$\sqrt{2} = \frac{a}{b}.$$

Oletetaan, että lukujen a ja b suurin yhteinen tekijä on 1, koska jos näin ei ole, lukuja voitaisiin supistaa kunnes on löydetty uudet luvut a ja b, joille pätee $\text{syt}(a, b) = 1$.

Olkoon

$$\begin{aligned} & \sqrt{2} = \frac{a}{b} \\ \Leftrightarrow \quad & \left(\sqrt{2}\right)^2 = \left(\frac{a}{b}\right)^2 \\ \Leftrightarrow \quad & 2 = \frac{a^2}{b^2} \\ \Leftrightarrow \quad & a^2 = 2b^2. \end{aligned}$$

Koska $b \in \mathbb{N}$, niin myös $b^2 \in \mathbb{N}$, jolloin a^2 on parillinen luku. Näin ollen myös a on parillinen luku. Voidaan siis merkitä $a = 2k$, jollain $k \in \mathbb{Z}$. Nyt

$$\begin{aligned} & 2b^2 = a^2 = (2k)^2 = 4k^2 \\ \Leftrightarrow \quad & b^2 = 2k^2. \end{aligned}$$

Täten luku b^2 on parillinen, koska $k^2 \in \mathbb{Z}$. Myös luku b on parillinen, jolloin on olemassa $l \in \mathbb{Z}$ niin, että $b = 2l$. Joten pätee

$$\sqrt{2} = \frac{a}{b} = \frac{2k}{2l}.$$

Tämä on ristiriidassa vastaoletuksen kanssa, koska osamäärää voi edelleen supistaa. Näin ollen ei löydy lukuja $a \in \mathbb{Z}$ ja $b \in \mathbb{N}$ siten, että

$$\sqrt{2} = \frac{a}{b}.$$

Antiteesin kumoutuminen todistaa alkuperäisen väitteen eli $\sqrt{2}$ on irrationaaliluku. □

Edellinen lause voidaan yleistää korvaamalla luku 2 millä tahansa alkuluvulla. Oletusta, että p on alkuluku tarvitaan tässä todistuksessa.

Lause 1.3. *Luku $\sqrt{p}$ on irrationaaliluku, kun p on alkuluku.*

Todistus. Todistetaan väite epäsuoralla todistuksella. Oletetaan siis, että luku $\sqrt{p}$ on rationaaliluku. Näin ollen on olemassa luvut $a \in \mathbb{Z}$ ja $b \in \mathbb{N}$ siten, että

$$\sqrt{p} = \frac{a}{b}.$$

Oletetaan vastaavasti kuin lauseen 1.2 todistuksessa, että lukujen a ja b osamäärää ei voida supistaa. Nyt

$$\begin{aligned} & \sqrt{p} = \frac{a}{b} \\ \Leftrightarrow \quad & p = \frac{a^2}{b^2} \\ \Leftrightarrow \quad & b^2 p = a^2, \end{aligned} \tag{1.1}$$

jolloin p on luvun a^2 tekijä eli a^2 on luvun p monikerta. Kaikki lukua yksi suuremmat kokonaisluvut voidaan esittää yksikäsitteisesti alkulukujen tulona. Eli $a = m_1 \cdot m_2 \cdot \ldots \cdot m_n$, missä $m_1, .., m_n$ ovat alkulukuja, jolloin $a^2 = (m_1 \cdot m_2 \cdot \ldots \cdot m_n)(m_1 \cdot m_2 \cdot \ldots \cdot m_n) = m_1 \cdot m_1 \cdot \ldots \cdot m_n \cdot m_n$. Nyt p

on jokin luvun a^2 alkulukutekijöistä $m_1, ..., m_n$ ja tällöin myös luvun a alkulukutekijöistä. Näin ollen luku a on luvun p monikerta eli se voidaan esittää muodossa $a = kp$, missä $k \in \mathbb{Z}$. Tällöin yhtälö 1.1 saadaan muotoon

$$b^2 p = (kp)^2$$
$$b^2 = k^2 p$$

eli b^2 on luvun p monikerta ja vastaavalla päättelyllä kuin aiemmin myös b on luvun p monikerta. Tästä aiheutuu ristiriita vastaoletuksen kanssa, koska luvuilla a ja b ei pitänyt olla muita yhteisiä tekijöitä kuin luku 1. Antiteesin kumoutuminen todistaa alkuperäisen väitteen, joten luku $\sqrt{p}$ on irrationaaliluku, kun p on alkuluku. □

1.2 Lukujen π ja e irrationaalisuus

Tutkielman päätuloksia ovat lauseet lukujen e ja π transkendenttiudesta, mutta tutkitaan ensin kyseisten lukujen irrationaalisuutta. Erilaisia todistuksia Neperin luvun, toiselta nimeltään Eulerin luvun, irrationaalisuudelle on useita, mutta tähän tutkielmaan on valittu kenties kaikista tunnetuin versio. Kyseinen todistus on julkaistu vuonna 1815 kirjassa *Mélanges d'analyse algébrique et de géométrie* [2]. Suomennettuna kirjan nimi tarkoittaa *Sekoitus algebrallista analyysia ja geometriaa*. Kirjan julkaisi Janot de Stainville, mutta kirjassa mainitaan luvun e irrationaalisuustodistuksen olevan peräisin tunnetulta matemaatikolta Joseph Fourierilta. Seuraavaksi esitettävä todistus mukailee lähteen [2] alkuperäistä versiota todistuksesta, mutta selkeyden vuoksi joitakin välivaiheita on täsmennetty. Todistuksessa hyödynnetään Neperin luvun e sarjakehitelmää, joten määritellään se ensin.

Määritelmä 1.4. Neperin luku e voidaan ilmaista kaavalla

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + ...$$

Tätä kutsutaan e:n sarjakehitelmäksi.

Lause 1.5. *Luku $e \in \mathbb{R}$ on irrationaaliluku.*

Todistus. Todistetaan väite epäsuoran todistuksen avulla. Oletetaan siis, että e on rationaaliluku eli se voidaan esittää kokonaisluvun ja luonnollisen luvun osamääränä. Osoitetaan ensin, että e ei ole kokonaisluku. Selvästi nähdään, että

$$2 < \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + ...$$

eli $2 < e$, koska kahden ensimmäisen termin summa on 2. Kun tutkitaan loppuja termejä niin voidaan huomata, että

$$\frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + ... < \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + ...,$$

koska $n! = 1 \cdot 2 \cdot ... \cdot n > 2^{n-1}$. Geometrisen sarjan summakaavalla saadaan

$$\sum_{n=1}^{\infty} \left(\frac{1}{2}\right)^n = 1.$$

Eli $2 < e < 3$ ja täten e ei ole kokonaisluku. Oletetaan, että

$$e = \frac{a}{b} = \sum_{n=0}^{\infty} \frac{1}{n!},$$

missä kokonaisluvut a ja b ovat suurempia tai yhtä suuria kuin luku 2. Kerrotaan yhtälöä puolittain luvulla $b!$

$$\begin{aligned} \frac{a \cdot b!}{b} &= b! \left(\frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} ... + \frac{1}{b!} + \frac{1}{b!(b+1)} + ... \right) \\ \Leftrightarrow a \cdot (b-1)! &= \frac{b!}{0!} + \frac{b!}{1!} + \frac{b!}{2!} + \frac{b!}{3!} ... + \frac{b!}{b!} + \frac{b!}{b!(b+1)} + ... \\ &= \frac{b!}{0!} + \frac{b!}{1!} + \frac{b!}{2!} + \frac{b!}{3!} ... + 1 + \frac{1}{b+1} + ... \end{aligned} \tag{1.2}$$

Vasen puoli yhtälöstä 1.2 on selvästi kokonaisluku, koska $a \in \mathbb{Z}$ ja $b \in \mathbb{N}$. Näin ollen myös oikean puolen kuuluisi olla kokonaisluku. Jaetaan yhtälön oikean puolen tarkastelu kahteen osaan:

$$\frac{b!}{0!} + \frac{b!}{1!} + \frac{b!}{2!} + \frac{b!}{3!} + ... + 1 \tag{1.3}$$

ja

$$\frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + ... \tag{1.4}$$

Yhtälön 1.2 oikean puolen lausekkeen osa 1.3 on kokonaisluku, koska jokainen summattava on kokonaisluku osoittajien $b!$ kumotessa kaikki nimittäjät. Tarkastellaan seuraavaksi lausekkeen toista osaa 1.4 etsimällä sen arvolle sopiva ala- ja yläraja. Yksi sopiva alaraja lausekkeen 1.4 arvolle on 0 ja valitaan yläraja siten, että se on lukua 1 pienempi positiviinen luku.

$$
\begin{aligned}
&\frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \frac{1}{(b+1)(b+2)(b+3)} + ... \\
\leq &\frac{1}{b+1} + \frac{1}{(b+1)^2} + \frac{1}{(b+1)^3} + ... \\
\leq &\frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + ... = \frac{1}{2}
\end{aligned}
$$

Nyt siis lausekkeen toinen osa 1.4 ei voi olla kokonaisluku, koska sen arvoa rajoittavat luvut 0 ja $\frac{1}{2}$ eli

$$0 < \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + ... \leq \frac{1}{2}$$

eikä kyseisten lukujen välistä voi löytyä kokonaislukua. Näin ollen yhtälön 1.2 oikea puoli ei voi olla kokonaisluku, koska kun kokonaislukuun summataan muu kuin kokonaisluku, niin ei voida päätyä kokonaislukuratkaisuun. Tästä aiheutuu ristiriita yhtälön 1.2 vasemman puolen ollessa kokonaisluku ja vastaoletus kumoutuu. Täten luku e on irrationaaliluku. □

Ensimmäinen julkaistu todistus luvun π irrationaalisuudesta ajoittuu jo 1700-luvulle ja kunnia todistuksesta kuuluu Johann Heinrich Lambertille. Lambertin todistus ja lisää historiaa aiheesta löytyy lähteestä [9]. Tähän tutkielmaan on valittu alkuperäisestä todistusta yksinkertaisempi Mary Cartwrightin versio [3, s. 268].

Lause 1.6. *Luku $\pi \in \mathbb{R}$ on irrationaaliluku.*

Todistus. Tarkastellaan integraalia

$$I_n = \int_{-1}^{1} (1-x^2)^n \cos(\alpha x) dx.$$

Osittaisintegroidaan lauseketta:

$$
\begin{aligned}
&\int_{-1}^{1} \left(1-x^2\right)^n \cos\left(ax\right)\ dx \\
= &\int_{-1}^{1} \left(\left(1-x^2\right)^n \frac{1}{\alpha} \sin\left(\alpha x\right)\right) - \int_{-1}^{1} \left(-2nx\left(1-x^2\right)^{n-1} \frac{1}{\alpha} \sin\left(\alpha x\right)\right) dx \\
= &\int_{-1}^{1} 2nx\left(1-x^2\right)^{n-1} \frac{1}{\alpha} \sin\left(\alpha x\right) dx.
\end{aligned}
$$

Osittaisintegroidaan saatua lauseketta uudelleen:

$$\begin{aligned}
&\int_{-1}^{1} 2nx\left(1-x^2\right)^{n-1}\frac{1}{\alpha}\sin(\alpha x)\,dx \\
=&\Bigg|_{-1}^{1}\left(2nx\left(1-x^2\right)^{n-1}\left(-\frac{1}{\alpha^2}\right)\cos(\alpha x)\right) \\
&-\int_{-1}^{1}\left(2n\left(\left(1-x^2\right)^{n-1}-2x^2(n-1)\left(1-x^2\right)^{n-2}\right)\left(-\frac{1}{\alpha^2}\right)\cos(\alpha x)\right)dx \\
=&\frac{1}{\alpha^2}\int_{-1}^{1}\left(2n\left(\left(1-x^2\right)^{n-1}-2x^2(n-1)\left(1-x^2\right)^{n-2}\right)\cos(\alpha x)\right)dx.
\end{aligned}$$

Järjestelemällä lauseketta uudelleen päädytään haluttuun muotoon.

$$\begin{aligned}
&\frac{1}{\alpha^2}\int_{-1}^{1}\left(2n\left(\left(1-x^2\right)^{n-1}-2x^2(n-1)\left(1-x^2\right)^{n-2}\right)\cos(\alpha x)\right)dx \\
=&\frac{1}{\alpha^2}\int_{-1}^{1}\left(-2n\left(1-x^2\right)^{n-2}\left((2n-1)x^2-1\right)\cos(\alpha x)\right)dx \\
=&\frac{1}{\alpha^2}\int_{-1}^{1}2n\left(1-x^2\right)^{n-2}\cos(\alpha x)-2n(2n-1)x^2\left(1-x^2\right)^{n-2}\cos(\alpha x)\,dx \\
&\vdots \\
=&\frac{1}{\alpha^2}2n(2n-1)\int_{-1}^{1}\left(1-x^2\right)^{n-1}\cos(\alpha x)\,dx \\
&-\frac{1}{\alpha^2}4n(n-1)\int_{-1}^{1}\left(1-x^2\right)^{n-2}\cos(\alpha x)\,dx \\
=&\frac{1}{\alpha^2}2n(2n-1)I_{n-1}-\frac{1}{\alpha^2}4n(n-1)I_{n-2}
\end{aligned}$$

Täten saadaan

$$\begin{aligned}
&I_n=\frac{1}{\alpha^2}2n(2n-1)I_{n-1}-\frac{1}{\alpha^2}4n(n-1)I_{n-2} \\
\Leftrightarrow\quad &\alpha^2 I_n=2n(2n-1)I_{n-1}-4n(n-1)I_{n-2}, \qquad \text{kun } n\geq 2.
\end{aligned}$$

Olkoon $J_n=\alpha^{2n+1}I_n$, jolloin saadaan

$$J_n=2n(2n-1)J_{n-1}-4n(n-1)\alpha^2 J_{n-2}.$$

Nyt kun $n=0$, niin

$$\begin{aligned}
J_0=\alpha I_0&=\alpha\int_{-1}^{1}\cos(ax)\;\,dx=\alpha\cdot\frac{1}{\alpha}\Bigg|_{-1}^{1}(\sin(ax)) \\
&=\sin(\alpha)-\sin(-\alpha)=2\sin(\alpha)
\end{aligned}$$

ja kun $n = 1$, niin

$$\begin{aligned}
J_1 &= \alpha^3 I_1 = \alpha^3 \int_{-1}^{1} \left(1 - x^2\right) \cos(\alpha x)\, dx \\
&= \alpha^3 \left(\int_{-1}^{1} \cos(\alpha x)\, dx - \int_{-1}^{1} x^2 \cos(\alpha x)\, dx \right) \\
&= \alpha^3 \left(\Big/_{-1}^{1} \frac{1}{\alpha} \sin(\alpha x) \right) - \alpha^3 \int_{-1}^{1} x^2 \cos(ax)\, dx \\
&= 2\alpha^2 \sin(\alpha) - a^3 \left(\Big/_{-1}^{1} \left(x^2 \frac{1}{\alpha} \sin(\alpha x) \right) - \int_{-1}^{1} 2x \frac{1}{\alpha} \sin(\alpha x)\, dx \right) \\
&= 2\alpha^2 \sin(\alpha) - 2\alpha^2 \sin(\alpha) + 2\alpha^2 \left(\Big/_{-1}^{1} \left(-\frac{x}{\alpha} \cos(\alpha x) \right) + \frac{1}{\alpha} \int_{1}^{1} (\cos(\alpha x)\, dx) \right) \\
&= -4\alpha \cos(\alpha) + 2\alpha \Big/_{-1}^{1} \frac{1}{\alpha} \sin(\alpha x)\, dx \\
&= -4\alpha \cos(\alpha) + 4 \sin(\alpha).
\end{aligned}$$

Osoitetaan induktiotodistuksen avulla, että kaikilla $n \in \mathbb{Z}^+$ pätee

$$J_n = n!(P_n(\alpha) \sin(\alpha) + Q_n(\alpha) \cos(\alpha)),$$

missä $P_n(x)$ ja $Q_n(x)$ ovat kokonaislukukertoimisia polynomeja, joiden aste on pienempää tai yhtä suurta kuin $2n$. Kun $n = 0$, niin $J_0 = 2\sin(\alpha)$ eli $P_n(\alpha) = 2$ ja $Q_n(\alpha) = 0$. Kun $n = 1$, niin $J_1 = -4\alpha \cos(\alpha) + 4\sin(\alpha)$ eli $P_n(\alpha) = 4$ ja $Q_n(\alpha) = -4\alpha$. Oletetaan, että väite pätee kun $n = k$ eli

$$J_k = k!(P_k(\alpha) \sin(\alpha) + Q_k(\alpha) \cos(\alpha))$$

sekä kaikille lukua k pienemmille luonnollisille luvuille. Osoitetaan, että väite pätee kun $n = k + 1$.

$$\begin{aligned}
J_{k+1} &= 2(k+1)(2k+1)J_k - 4(k+1)k\alpha^2 J_{k-1} \\
&= 2(k+1)(2k+1)k!(P_k(\alpha) \sin(\alpha) + Q_k(\alpha) \cos(\alpha)) \\
&\quad - 4(k+1)k\alpha^2(k-1)!(P_{k-1}(\alpha) \sin(\alpha) + Q_{k-1}(\alpha) \cos(\alpha)) \\
&= (k+1)! \left((4k+2) P_k(\alpha) - 4\alpha^2 P_{k-1}(\alpha) \right) \sin(\alpha) \\
&\quad + (k+1)! \left((4k+2) Q_k(\alpha) - 4\alpha^2 Q_{k-1}(\alpha) \right) \cos(\alpha) \\
&= (k+1)!(P_{k+1}(\alpha) \sin(\alpha) + Q_{k+1}(\alpha) \cos(\alpha)),
\end{aligned}$$

missä

$$\begin{aligned}
P_{k+1}(\alpha) &= (4k+2) P_k(\alpha) - 4\alpha^2 P_{k-1}(\alpha) \quad \text{ja} \\
Q_{k+1}(\alpha) &= (4k+2) Q_k(\alpha) - 4\alpha^2 Q_{k-1}(\alpha)
\end{aligned}$$

ovat kokonaislukukertoimisia polynomeja siten, että niiden asteet ovat pienempiä tai yhtä suuria kuin $2k+1$. Induktioperiaatteen nojalla $J_n = n!(P_n(\alpha)\sin(\alpha) + Q_n(\alpha)\cos(\alpha))$ pätee kaikilla $n \in \mathbb{N}$.

Oletetaan, että π on rationaaliluku eli on olemassa luvut $m \in \mathbb{Z}$ ja $n \in \mathbb{N}$ niin, että $\pi = \frac{m}{n}$. Olkoon $\alpha = \frac{\pi}{2} = \frac{b}{a}$, missä $a \neq 0$ ja b ovat kokonaislukuja. Tällöin

$$\begin{aligned} & \frac{b^{2n+1}}{a^{2n+1}} I_n = n! \left(P_n\left(\frac{\pi}{2}\right) \sin\left(\frac{\pi}{2}\right) + Q_n\left(\frac{\pi}{2}\right) \cos\left(\frac{\pi}{2}\right) \right) \\ \Leftrightarrow \quad & \frac{b^{2n+1}}{n!} I_n = P_n\left(\frac{\pi}{2}\right) a^{2n+1}. \end{aligned} \tag{1.5}$$

Nyt oikea puoli yhtälöstä 1.5 on kokonaisluku, koska $a \in \mathbb{Z}$ ja polynomin $P_n(x)$ aste on pienempää tai yhtä suurta kuin $2n$. Mutta $0 < I_n < 2$, koska integroitava funktio saa arvoja väliltä $]0, 1[$ kun $-1 < x < 1$ ja välin $[-1, 1]$ pituus on 2, ja

$$\frac{b^{2n+1}}{n!} \to 0 \text{ kun } n \to \infty.$$

Täten kun n on riittävän suuri

$$0 < \frac{b^{2n+1}}{n!} I_n < 1$$

eli väliltä $]0, 1[$ löytyisi kokonaisluku. Tästä aiheutuu ristiriita, koska kyseisellä välillä ei ole kokonaislukua. Tämä todistaa sen, että $\frac{\pi}{2}$ ei ole rationaalinen ja näin ollen myöskään π ei voi olla rationaalinen. Luku π on siis irrationaalinen. □

2 Kunnat ja renkaat

Irrationaalilukuja voidaan jaotella useilla eri tavoilla, mutta yksi keino on jakaa ne kahteen luokkaan eli algebrallisiin lukuihin ja transkendenttilukuihin. Määritellään ensin mitä tarkoittaa algebrallinen luku ja sen kautta saamme määritelmän myös transkendenttiluvulle.

Määritelmä 2.1. Luku $a \in \mathbb{R}$ on algebrallinen, jos on olemassa rationaalilukukertoiminen polynomi $P(x)$ siten, että a on kyseisen polynomin nollakohta eli $P(a) = 0$. Luku $t \in \mathbb{R}$ on transkendentti, jos se ei ole algebrallinen.

Määritelmän mukaisesti transkendenttiluku ei ole minkään rationaalilukukertoimisen polynomin juuri, joten osoittaaksemme luvun transkendentiksi, on todistettava että tällaista polynomia ei löydy. Vastaavasti kuin irrationaalilukujen tapauksessa, luvun transkendenttiuden osoittaminen on todettu

haastavaksi ja tästä johtuen tunnemme niistä vain muutamia erikoistapauksia. Palaamme tutkielmassa näihin erikoistapauksiin eli tunnettuihin transkendenttilukuihin myöhemmin luvussa 6, mutta algebrallisista luvuista on yksinkertaista antaa esimerkki.

Esimerkki 2.2. Luku $\sqrt{2}$ on algebrallinen, koska se on polynomin $P(x) = x^2 - 2$ juuri eli $P(\sqrt{2}) = (\sqrt{2})^2 - 2 = 2 - 2 = 0$.

Tutustuaksemme tarkemmin algebrallisiin ja transkendenttisiin lukuihin sekä niiden ominaisuuksiin, on määriteltävä joitakin olennaisia perusalgebran määritelmiä. Tämän luvun lähteinä on algebran osalta käytetty Langin kirjaa [7] ja Stewartin kirjaa [10]. Lineaarialgebran käsitteissä lähteinä on käytetty Petersenin kirjaa [8] ja Äkkisen luentomonistetta [11]. Määritellään ensin rengas ja annetaan sen avulla määritelmä kunnalle.

Määritelmä 2.3. Rengas R on joukko, jossa on määritelty operaatiot yhteen- ja kertolasku, ja se täyttää seuraavat ehdot.

1. Kaikilla $a, b \in R$ pätee $a + b = b + a$. *(summan vaihdantalaki)*
2. Kaikilla $a, b, c \in R$ pätee $(a + b) + c = a + (b + c)$. *(summan liitäntälaki)*
3. On olemassa $0 \in R$ siten, että $0 + a = a$ kaikilla $a \in R$. *(summan neutraalialkio)*
4. Jokaiselle $a \in R$ on olemassa $-a \in R$ siten, että $a + (-a) = 0$. *(vasta-alkio)*
5. Kaikilla $a, b, c \in R$ pätee $(ab)c = a(bc)$. *(tulon liitäntälaki)*
6. Kaikilla $a, b, c \in R$ pätee $a(b + c) = ab + ac$ ja $(b + c)a = ba + ca$. *(osittelulait)*

Rengas R on *ykkösellinen rengas* mikäli ehtojen 1.–6. lisäksi pätee myös seuraava.

- ❀ On olemassa $1 \in R$ ja $1 \neq 0$, siten, että $1a = a$ kaikilla $a \in R$. *(tulon neutraalialkio)*

Rengas R on *kommutatiivinen rengas* mikäli ehtojen 1.–6. lisäksi pätee seuraava ehto.

- ❀ Kaikilla $a, b \in R$ pätee $ab = ba$. *(tulon vaihdantalaki)*

Määritelmässä 2.3 sanomme joukossa R olevan määriteltyinä yhteen- ja kertolaskuoperaatiot. Tämä tarkoittaa sitä, että jos $a, b \in R$ niin myös $a+b \in R$ ja $ab \in R$. Tässä tutkielmassa jatkossa renkaista puhuttaessa kyseessä on ykkösellinen kommutatiivinen rengas, joka toteuttaa määritelmän 2.3 kaikki ehdot.

Esimerkki 2.4.

1. Kokonaislukujen joukko $\mathbb{Z}$, rationaalilukujen joukko $\mathbb{Q}$, reaalilukujen joukko $\mathbb{R}$ ja kompleksilukujen joukko $\mathbb{C}$ ovat renkaita.

2. Luonnollisten lukujen joukko $\mathbb{N}$ ei ole rengas, koska määritelmän 2.3 neljäs ehto vasta-alkiosta ei toteudu. Esimerkiksi $1 \in \mathbb{N}$, mutta ei ole olemassa $n \in \mathbb{N}$ siten, että $1 + n = 0$.

Lisäämällä määritelmään 2.3 vielä yhden ehdon joukolle, saamme määritelmän kunnalle.

Määritelmä 2.5. Kunta on ykkösellinen kommutatiivinen rengas K, joka toteuttaa myös seuraavan ehdon.

- ❀ Jokaiselle $a \in K$ on olemassa $a^{-1} \in K$ niin, että $aa^{-1} = 1$. *(tulon käänteisalkio)*

Esimerkki 2.6.

1. Rationaalilukujen joukko $\mathbb{Q}$, reaalilukujen joukko $\mathbb{R}$ ja kompleksilukujen joukko $\mathbb{C}$ ovat kuntia.

2. Kokonaislukujen joukko $\mathbb{Z}$ on rengas, mutta se ei ole kunta. Esimerkiksi $2 \in \mathbb{Z}$, mutta ei ole olemassa tulon käänteisalkiota $n \in \mathbb{Z}$ siten, että $2n = 1$, koska $2n$ on parillinen luku ja 1 on pariton luku.

Määritellään seuraavaksi alirengas ja alikunta.

Määritelmä 2.7.

1. Renkaan R alirengas on epätyhjä osajoukko $S \subset R$ siten, että jos $a, b \in S$, niin $a + b \in S$, $a - b \in S$ ja $ab \in S$.

2. Kunnan K alikunta on osajoukko $S \subset K$, joka sisältää alkiot 0 ja 1 ja jos $a, b \in S$, niin $a + b \in S$, $a - b \in S$ ja $ab \in S$ sekä jos $a \neq 0$ niin $a^{-1} \in S$.

Alirengas on siis renkaan epätyhjä osajoukko, joka sisältää alkioiden summat, erotukset ja tulot. *Alikunta* on kunnan alirengas, joka sisältää myös nollan, ykkösen sekä nollasta poikkeavien alkioiden käänteisalkiot. Osoitetaan seuraavan lemman avulla, että pienin kompleksilukujen joukon $\mathbb{C}$ alikunta on rationaalilukujen joukko $\mathbb{Q}$.

Lemma 2.8. *Jokainen joukon $\mathbb{C}$ alikunta sisältää joukon $\mathbb{Q}$.*

Todistus. Olkoon $K \subseteq \mathbb{C}$ alikunta. Tällöin $0, 1 \in K$ määritelmän 2.7 mukaan, joten $1+..+1 = n$ kuuluu joukkoon K kaikilla kokonaisluvuilla $n > 0$. Koska K on alikunta, niin myös $-n \in K$, joten $\mathbb{Z} \subseteq K$. Jos $p, q \in \mathbb{Z}$ ja $q \neq 0$, niin $pq^{-1} = \frac{p}{q} \in K$. Näin ollen $\mathbb{Q} \subseteq K$. □

Esimerkki 2.9. Olkoon K kaikkien niiden reaalilukujen joukko, jotka ovat muotoa $p + q\sqrt{2}$, missä $p, q \in \mathbb{Q}$. Osoittaaksemme, että K on joukon $\mathbb{C}$ alikunta, tulee meidän näyttää, että

1. K sisältää vähintään kaksi alkiota,
2. $a - b \in K$ kaikilla $a, b \in K$,
3. ja $ab^{-1} \in K$ kaikilla $a, b \in K, b \neq 0$.

Nämä ehdot muodostavat alikuntakriteerin. Käydään läpi jokainen kohta.

1. K sisältää vähintään kaksi alkiota, koska esimerkiksi $0, 1 \in K$.
2. Nyt $p + q\sqrt{2}, k + l\sqrt{2} \in K$ kun $p, q, k, l \in \mathbb{Q}$. Tällöin saadaan
$$p + q\sqrt{2} - (k + l\sqrt{2}) = (p - k) + (q - l)\sqrt{2} \in K.$$
3. Olkoon $p + q\sqrt{2}, k + l\sqrt{2} \in K$ ja $k, l \neq 0$. Nyt
$$(k + l\sqrt{2})^{-1} = \frac{1}{k + l\sqrt{2}} = \frac{(k - l\sqrt{2})}{k^2 - 2l^2} = \frac{k}{k^2 - 2l^2} - \frac{l}{k^2 - 2l^2}\sqrt{2} \in K,$$
jolloin
$$\begin{aligned}(p + q\sqrt{2})(k + l\sqrt{2})^{-1} &= \frac{p + q\sqrt{2}}{k + l\sqrt{2}} = \frac{(p + q\sqrt{2})(k - l\sqrt{2})}{k^2 - 2l^2} \\ &= \frac{pk + kq\sqrt{2} - pl\sqrt{2} - 2ql}{k^2 - 2l^2} \\ &= \frac{pk - 2ql}{k^2 - 2l^2} + \frac{kq - pl}{k^2 - 2l^2}\sqrt{2} \in K.\end{aligned}$$

Täten joukko K on joukon $\mathbb{C}$ alikunta.

Määritellään muutamia oleellisia lineaarialgebran määritelmiä, joita tarvitsemme myöhemmin tutkielmassa luvussa 4.

Määritelmä 2.10. Olkoon K kunta ja V joukko. Määritetään operaatiot

$$(\lambda, u) \to \lambda u \qquad (\lambda \in K, u \in V),$$
$$(u, v) \to u + v \qquad (u, v \in V).$$

Joukko V varustettuna edellä määritellyillä operaatioilla on vektoriavaruus kunnan K suhteen jos ja vain jos operaatiot toteuttavat seuraavat ehdot.

1. Kaikilla $u, v \in V$ pätee $u + v = v + u$.
2. Kaikilla $u, v, w \in V$ pätee $(u + v) + w = u + (v + w)$.
3. On olemassa $0 \in V$ siten, että $0 + u = u$ kaikilla $u \in V$.
4. Jokaiselle $u \in V$ on olemassa $-u \in V$ siten, että $u + (-u) = 0$.
5. Jos $\lambda \in K$ ja $u, v \in V$, niin $\lambda(u + v) = \lambda u + \lambda v$.
6. Jos $\lambda, \mu \in K$, niin $(\lambda + \mu)u = \lambda u + \mu u$ kaikilla $u \in V$.
7. Jos $\lambda, \mu \in K$, niin $\lambda(\mu u) = (\lambda\mu)u$ kaikilla $u \in V$.
8. Jos 1 on kunnan K neutraalialkio, niin $1u = u$ kaikilla $u \in V$.

Vektoriavaruuden V määritelmässä olevaa kuntaa K kutsutaan toisinaan vektoriavaruuden *skalaarikunnaksi.*

Määritelmä 2.11. Olkoon V vektoriavaruus kunnan K suhteen. Jos $c_1, ..., c_n \in K$ ja $v_1, ..., v_n \in V$ niin vektoreita

$$c_1v_1 + c_2v_2 + ... + c_nv_n$$

kutsutaan vektoreiden $v_1, v_2, ..., v_n$ *lineaarikombinaatioiksi.*

Määritelmä 2.12. Vektoriavaruuden V vektorit $v_1, ...v_n$ ovat lineaarisesti riippuvat, jos jokin vektoreista v_i voidaan esittää muiden lineaarikombinaationa. Muulloin kyseiset vektorit ovat lineaarisesti riippumattomat.

Lisäksi sovitaan, että yhden vektorin muodostama vektorijoukko v_1 on lineaarisesti riippumaton jos ja vain jos v_1 ei ole nollavektori.

Lause 2.13. *(a) Vektoriavaruuden V vektorit $v_1, ...v_n$ ovat lineaarisesti riippumattomia jos ja vain jos*

$$c_1v_1 + c_2v_2 + ... + c_nv_n = 0$$

pätee ainoastaan, kun $c_1 = c_2 = ... = c_n = 0$.

(b) *Vektoriavaruuden V vektorit $v_1, ...v_n$ ovat lineaarisesti riippuvia jos vain jos*

$$c_1v_1 + c_2v_2 + ... + c_nv_n = 0$$

pätee niin, että reaaliluvuista $c_1, c_2, \ldots, c_n$ ainakin yksi on nollasta poikkeava.

Todistus. Lauseen 2.13 todistus löytyy lähteestä [11, s. 44]. □

Määritelmä 2.14. Olkoon $\{v_1, \ldots, v_k\}$ vektoriavaruuden V äärellinen osajoukko. Vektorit $\{ v_1, \ldots, v_k \}$ muodostavat vektoriavaruuden V *kannan*, jos

1. $v_1, \ldots, v_k$ ovat lineaarisesti riippumattomia ja
2. jokainen vektoriavaruuden V vektori voidaan lausua vektoreiden $v_1, \ldots, v_k$ lineaarikombinaationa. Toisin sanoen vektorit $v_1, \ldots, v_k$ virittävät vektoriavaruuden V eli $\langle v_1, \ldots, v_k \rangle = V$.

Määritelmä 2.15. Vektoriavaruuden V dimensio eli ulottuvuus dim V on vektoriavaruuden V kannassa olevien vektoreiden lukumäärä.

Lisäksi sovitaan, että ainoastaan nollavektorista koostuvan vektorijoukon dimensio on 0.

3 Polynomirenkaat

Tutkielman transkendenttitodistuksia varten tarvitaan hieman pohjatietoa polynomeista, erityisesti symmetrisistä polynomeista, joten tutustaan niihin. Tämän luvun lähteenä on käytetty Stewartin kirjaa [10] ja symmetristen polynomien osalta täydentävänä lähteenä on käytetty Daoubin julkaisua [1].

3.1 Polynomit

Määritellään ensin polynomi, polynomin aste ja polynomirengas yhden muuttujan tilanteessa.

Määritelmä 3.1. Olkoon R rengas. Polynomi f, jonka muuttuja on x ja kertoimet $a_0, ..., a_n$ ovat renkaan R alkiota, on summa

$$f(x) = \sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + ... + a_n x^n.$$

Polynomin $f(x)$ aste on muuttujan x suurin eksponentti n siten, että kyseisen termin kerroin $a_n \neq 0$. Tällöin polynomin johtava termi on $a_n x^n$. Polynomin f asteesta käytetään merkintää $\partial f = n$.

Nollapolynomi on summa, jonka kaikki kertoimet $a_0, a_1, ..., a_n$ ovat nollia. Nollapolynomin asteen on sovittu olevan $\partial(0) = -\infty$.

Polynomit, joiden kertoimet ovat renkaan R alkioita, muodostavat polynomirenkaan $R[x]$. Määritellään vastaavasti myös monen muuttujan polynomit, jotka muodostavat polynomirenkaan.

Määritelmä 3.2. Olkoon R rengas. Monen muuttujan polynomi, jonka muuttujia ovat $x_1, .., x_n$ ja kertoimet $a_{k_1}, ..., a_{k_n}$ ovat renkaan R alkiota, on summa

$$f(x_1, x_2, ..., x_n) = \sum_{k_1,...,k_n \in \mathbb{N} \cup \{0\}} a_{k_1,...,k_n} x_1^{k_1} \cdots x_n^{k_n}.$$

Polynomin $f(x_1, x_2, ..., x_n)$ termin aste on termin eri muuttujien eksponenttien summa ja kyseisen polynomin aste on suurin termien asteista.

Nämä useamman muuttujien polynomit, joiden kertoimet ovat renkaan R alkioita, muodostavat polynomirenkaan $R[x_1, ..., x_n]$.

Esimerkki 3.3. Olkoon $f(x_1, x_2) = x_1^2 x_2^3 + 3x_1^3 + 5x_2$, jolloin $\partial f = 2 + 3 = 5$.

Propositio 3.4. *Jos f ja g ovat polynomeja kunnan $\mathbb{C}$ suhteen, niin*

$$\partial(f + g) \leq \max(\partial f, \partial g) \quad ja \quad \partial(fg) = \partial f + \partial g.$$

Todistus. Todistus ohitetaan tässä tutkielmassa, mutta sen löytää lähteestä [7, s. 189-190]. □

Määritelmä 3.5. Polynomi $f(t) = a_n t^n + ... + a_1 t^1 + a_0$ alikunnan $K \subset \mathbb{C}$ suhteen on *mooninen* jos $a_n = 1$ eli johtavan termin kerroin on 1.

Polynomien jaollisuus on tärkeä käsite, jota tarvitaan kuntalaajennoksien yhteydessä kun käsitellään minimaalipolynomeja luvussa 4. Annetaan seuraavaksi yksinkertainen määritelmä polynomin jaollisuudesta ja tutkitaan sen jälkeen polynomin jaollisuuden tai jaottomuuden selvittämistä.

Määritelmä 3.6. Muu kuin vakiopolynomi on *jaollinen*, jos se on kahden pienempää astetta olevan polynomin tulo. Muussa tapauksessa se on *jaoton*.

Esimerkki 3.7. Olkoon $f(x) = x^2 - 4$. Polynomilauseke voidaan esittää muodossa

$$x^2 - 4 = x^2 - 2^2 = (x + 2)(x - 2).$$

Polynomi $f(x)$ voidaan esittää kahden pienempää astetta olevan polynomin tulona eli se on *jaollinen*.

Polynomin jaottomuuden tarkasteluun kunnassa $\mathbb{Q}$ voidaan käyttää esimerkiksi seuraavaa lausetta eli Eisensteinin kriteeriä.

Lause 3.8 (Eisensteinin kriteeri)**.** *Olkoon*

$$f(x) = a_0 + a_1 x + ... + a_n x^n$$

polynomi kunnan $\mathbb{Z}$ suhteen. Oletetaan, että on olemassa alkuluku q siten, että seuraavat ehdot pätevät.

1. $q \nmid a_n$
2. $q \mid a_i$, *missä* $i = 0, ..., n-1$
3. $q^2 \nmid a_0$

Tällöin polynomi f on jaoton kunnan $\mathbb{Q}$ suhteen.

Todistus. Lauseen todistus löytyy lähteestä [10, s. 55-56]. □

Esimerkki 3.9. Tutkitaan polynomin $p(x) = x^3 - 2$ jaottomuutta Eisensteinin kriteerin 3.8 avulla. Nyt löytyy alkuluku 2 siten, että se ei jaa polynomin johtavan termin kerrointa eli $2 \nmid 1$, mutta se jakaa polynomin toisen termin kertoimen eli $2 \mid -2$. Lisäksi pätee, että $2^2 \nmid -2$, joten Eisensteinin kriteerin 3.8 nojalla $x^3 - 2$ on jaoton.

Polynomien jakoalgoritmi on vastaavanlainen kuin kokonaislukujen jaollisuutta tutkiessa. Polynomien jakoalgoritmia tarvitaan tässä tutkielmassa erityisesti minimaalipolynomien tunnistamisessa sekä Lemman 4.12 ja Lauseen 4.13 todistuksissa.

Propositio 3.10 (Jakoalgoritmi)**.** *Olkoon p ja q polynomeja kunnan K suhteen siten, että p ei ole nollapolynomi. Tällöin on olemassa yksikäsitteiset polynomit r ja s yli kunnan K niin, että*

$$q = pr + s$$

ja polynomilla s on pienempi aste kuin polynomilla p.

Todistus. Hyödynnetään induktiotodistusta. Jos $\partial q = -\infty$, niin q on nollapolynomi ja voidaan valita $q = s = 0$. Jos $\partial q = 0$, niin $q = k$, missä k on kunnan K alkio. Jos myös $\partial p = 0$ niin p on kunnan K alkio ja voidaan valita $r = k/p$ ja $s = 0$.

Muissa tapauksissa $\partial p > 0$ ja voidaan valita $r = 0$ ja $s = q$. Oletetaan, että tulos pätee aina kun polynomin q aste on pienempi kuin n ja olkoon $\partial q = n > 0$. Jos $\partial p > \partial q$ voidaan valita $r = 0, s = q$. Muulloin

$$p = a_m t^m + ... + a_0$$

$$q = b_n t^n + ... + b_0,$$

missä $a_m \neq 0 \neq b_n$ ja $m \leq n$. Olkoon

$$q_1 = b_n a_m^{-1} t^{n-m} p - q.$$

Koska korkeinta astetta olevat termit kumoutuvat pois, saadaan $\partial q_1 < \partial q$. Tällöin induktio-oletuksen nojalla on olemassa polynomit r_1 ja s_1 yli kunnan K siten, että $q_1 = pr_1 + s_1$ ja $\partial s_1 < \partial p$. Olkoon

$$r = b_n a_m^{-1} t^{n-m} - r_1 \quad \text{ja} \quad s = -s_1.$$

Tällöin

$$pr + s = b_n a_m^{-1} t^{n-m} p - r_1 p - s_1 = q + q_1 - q_1 = q,$$

joten $q = pr + s$ ja selvästi $\partial s < \partial p$.

Osoitetaan vielä polynomien yksikäsitteisyys. Oletetaan, että

$$q = pr_1 + s_1 = pr_2 + s_2 \quad \text{missä} \quad \partial s_1, \partial s_2 < \partial p.$$

Näin ollen $p(r_1 - r_2) = s_2 - s_1$. Nyt yhtälön vasemmalla puolella olevalla polynomilla on suurempi aste kuin oikealla elleivät molemmat polynomeista ole nollapolynomeja. Nyt kuitenkin koska $p \neq 0$, niin täytyy päteä $r_1 = r_2$ ja $s_1 = s_2$. Jolloin siis r ja s ovat yksikäsitteisiä. □

Määritellään polynomien suurin yhteinen tekijä vastaavalla tavalla kuin se määritellään kokonaisluvuille.

Määritelmä 3.11. Olkoon f ja g polynomeja kunnan K suhteen. Mikäli polynomi d kunnan K suhteen toteuttaa ehdot

1. $d \mid f$ ja $d \mid g$
2. jos $e \mid f$ ja $e \mid g$, niin $e \mid d$

niin polynomia d sanotaan polynomien f ja g *suurimmaksi yhteiseksi tekijäksi* ja siitä käytetään merkintää $d = \text{syt}(f, g)$.

Kahdelle muulle kuin nollapolynomille voidaan löytää suurin yhteinen tekijä Eukleideen algoritmin avulla, jota tyypillisesti käytetään kokonaislukujen suurimman yhteisen tekijän laskemiseksi. Ohitamme Eukleideen algoritmin esittelyn tässä tutkielmassa, mutta siihen voi tutusta lähteestä [10, s. 50].

Lause 3.12. *Olkoon f ja g nollasta poikkeavia polynomeja kunnan K suhteen. Tällöin on olemassa polynomit a ja b kunnan K suhteen niin, että*

$$\text{syt}(f, g) = af + bg.$$

Todistus. Todistus ohitetaan. Se löytyy lähteestä [10, s. 50]. □

3.2 Symmetriset polynomit

Määritellään symmetrinen polynomi sekä symmetriset alkeispolynomit, jotta pääsemme käsittelemään tutkielman kannalta oleellista tulosta eli symmetristen polynomien peruslausetta.

Määritelmä 3.13 (Symmetrinen polynomi)**.** Polynomi f on symmetrinen jos

$$f(x_{\tau(1)}, x_{\tau(2)}, ..., x_{\tau(n)}) = f(x_1, x_2, ..., x_n)$$

kaikilla mahdollisilla kertoimien $x_1.x_2, ..., x_n$ permutaatioilla $x_{\tau(1)}, x_{\tau(2)}, ..., x_{\tau(n)}$.

Symmetrinen polynomi ei siis muutu kun sen muuttujia vaihdetaan keskenään eri järjestykseen. Annetaan ensin esimerkki symmetrisestä polynomista ja sen jälkeen polynomista, joka ei ole symmetrinen.

Esimerkki 3.14. Määritellään polynomi f niin, että

$$f(x_1, x_2, x_3) = 3x_1 \cdot x_2 \cdot x_3 + 3x_1 \cdot x_3 + 3x_1 \cdot x_2 + 3x_2 \cdot x_3.$$

Nyt koska voimme muuttaa muuttujien x_i järjestystä muuttamatta polynomia, niin polynomi f on symmetrinen.

Esimerkki 3.15. Olkoon polynomi $g(x_1, x_2) = x_1 \cdot x_2^2 + 2x_1 + 2x_2$ ja olkoon permutaatio $\tau = (21)$. Nyt

$$g(x_{\tau(1)}, x_{\tau(2)}) = x_2 \cdot x_1^2 + 2x_2 + 2x_1 \neq x_1 \cdot x_2^2 + 2x_1 + 2x_2$$

eli g ei ole symmetrinen polynomi.

Määritelmä 3.16. Symmetriset alkeispolynomit $\sigma_1, ..., \sigma_n$ muuttujille $x_1, x_2, ..., x_n$ ovat

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + ... + x_n, \\
\sigma_2 &= x_1x_2 + ... + x_1x_n + x_2x_3 + ... + x_2x_n + x_3x_4... + x_{n-1}x_n, \\
\sigma_3 &= x_1x_2x_3 + ... + x_1x_{n-1}x_n + ... + x_{n-2}x_{n-1}x_n \\
&\vdots \\
\sigma_n &= x_1x_2 \cdots x_n.
\end{aligned}$$

Esimerkki 3.17. Olkoon x_1, x_2 ja x_3 muuttujia kunnan K suhteen. Tällöin symmetriset alkeispolynomit ovat

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + x_3 \\
\sigma_2 &= x_1x_2 + x_1x_3 + x_2x_3
\end{aligned}$$

ja

$$\sigma_3 = x_1x_2x_3.$$

Määritelmä 3.18. [Leksikografinen järjestys] Olkoot $x_1^{a_1} \cdots x_n^{a_n}$ ja $x_1^{b_1} \cdots x_n^{b_n}$ monomeja polynomirenkaassa $K[x_1, ..., x_n]$. Tällöin

$$x_1^{a_1} \cdots x_n^{a_n} < x_1^{b_1} \cdots x_n^{b_n}$$

jos joko

$$a_1 + ... + a_n < b_1 + ... + b_n$$

tai

$$a_1 + ... + a_n = b_1 + ... + b_n.$$

ja jollekin $1 \leq j \leq n$, $a_i = b_i$ kaikille $1 \leq i < j$ ja $a_j < b_j$.

Seuraava lause, jota kutsutaan *symmetristen polynomien peruslauseeksi*, on tarpeellinen kun muodostamme todistuksen luvun π transkendenttiudesta luvussa 6 sekä kun tutkimme algebrallisten lukujen ominaisuuksia luvussa 5.

Lause 3.19. *[Fundamental theorem of symmetric polynomials] Jokainen polynomirenkaan $k[x_1, x_2, ..., x_n]$ symmetrinen polynomi voidaan lausua alkeispolynomien k-kertoimisena polynomina. Lisäksi alkeispolynomien avulla lausutun polynomin aste on pienempää tai yhtä suurta kuin alkuperäisen polynomin aste.*

Todistus. Olkoon $f \in k[x_1, ..., x_n]$ symmetrinen polynomi ja olkoot $\sigma_1, ..., \sigma_n$ symmetriset alkeispolynomit muuttujille $x_1, x_2, ..., x_n$. Olkoon polymonin f johtava termi $cx_1^{a_1} \cdots x_n^{a_n}$ ja valitaan toinen polynomi g siten, että

$$g = \sigma_1^{a_1 - a_2} \sigma_2^{a_2 - a_3} \cdots \sigma_n^{a_n},$$

missä $a_j \geq a_{j+1}$. Symmetrisen polynomin f johtavalla termillä on laskevat eksponentit, koska jos näin ei olisi, niin voisimme muuttaa muuttujien järjestystä sopivaksi muuttamatta itse polynomia. Nyt polynomin g johtavaksi termiksi saadaan

$$x_1^{a_1 - a_2}(x_1 x_2)^{a_2 - a_3} \cdots (x_1 \cdots x_n)^{a_n} = x_1^{a_1} \cdots x_n^{a_n}$$

Tästä huomataan, että polynomien f ja cg johtavat termit ovat samat. Määritetään polynomi $f_1 = f - cg$, jolla on pienempi aste kuin polynomilla f, koska johtavat termit kumoavat toisensa. Nyt koska molemmat polynomit f ja g ovat symmetrisiä niin myös niistä muodostuva polynomi f_1 on symmetrinen.

Samalla menetelmällä voidaan muodostaa symmetrinen polynomi $f_2 = f_1 - c_1 g_1$, jonka johtavan termin aste on pienempi kuin polynomilla f_1. Tämä voidaan kirjoittaa myös muodossa $f_2 = f_1 - c_1 g_1 = f - cg - c_1 g_1$. Jatkamalla samaa menetelmää saadaan polynomit

$$f, f_1 = f - cg, f_2 = f - cg - c_1 g_1, f_3 = f - cg - c_1 g_1 - c_2 g_2, \ldots$$

Menetelmää jatkamalla saatujen polynomien asteet pienenevät johtavien termien kumotessa toisensa, joten lopulta on olemassa jokin m siten, että $f_m = 0$. Kun $f_m = 0$, niin polynomilla ei enää ole johtavaa termiä eli menetelmä päättyy ja saadaan

$$f = cg + c_1 g_1 + c_2 g_2 + \cdots + c_{m-1} g_{m-1}.$$

Koska jokainen polynomi g_i on alkeispolynomien σ_j tulo, niin on saavutettu haluttu tulos eli polynomi f on saatu lausuttua alkeispolynomien avulla. Saadun polynomin $cg + c_1 g_1 + c_2 g_2 + \cdots + c_{m-1} g_{m-1}$ aste on selvästi pienempää tai yhtä suurta kuin alkuperäisen polynomin, koska alkuperäisen polynomin johtavan termin asteen perusteella $\partial f = a_1 + \cdots + a_n$ ja nyt $\partial g = (a_1 - a_2) + (a_2 - a_3) \cdots + a_n$. □

Edellisestä lauseesta on olemassa myös vahvempi versio, jossa osoitetaan alkeispolynomien avulla lausutun polynomin yksikäsitteisyys. Kyseisen vahvemman tuloksen todistuksen voi katsoa lähteestä [1, s. 58-59].

Seuraavaa lausetta kutsutaan *algebran peruslauseeksi* ja sen mukaan jokaisella kunnan $\mathbb{C}$ polynomilla, joka ei ole vakiopolynomi, on ainakin yksi nollakohta.

Lause 3.20. *[Algebran peruslause] Jos $p(z)$ on positiiviasteinen polynomi kunnan $\mathbb{C}$ suhteen, niin on olemassa z_0 siten, että $p(z_0) = 0$.*

Todistus. Lauseen todistus löytyy lähteestä [10, s. 41-42]. □

Propositio 3.21. *Olkoon $p(t) \in \mathbb{C}[t]$ ja $\partial p = n \geq 1$. Polynomi $p(t)$ voidaan esittää muodossa*

$$p(t) = k(t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_n),$$

missä $c \neq 0 \in \mathbb{C}$ ja luvut $\alpha_1, ..., \alpha_n \in \mathbb{C}$ ovat polynomin $p(x)$ juuria.

Todistus. Todistus ohitetaan ja sen voi löytää lähteestä [10, s. 43]. □

Erityisesti edellisestä propositiosta seuraa, että α_j:t ovat polynomin $p(t)$ ainoat juuret kompleksilukujen joukossa, joten algebran peruslause 3.20 ja propositio 3.21 osoittavat, että jokaisella rationaalilukukertoimisella polynomilla p on n juurta kompleksilukujen joukossa, kun juurien mahdolliset toistot otetaan huomioon. Propositiossa 3.21 esitetyn muodon kautta polynomin p kertoimet saadaan ilmaistua symmetrisinä polynomeina juurista α_i. Yhdistetään seuraavalla lauseella algebran peruslause symmetrisiin polynomeihin.

Lause 3.22. *Jos f on rationaalilukukertoiminen symmetrinen polynomi, ja p on rationaalilukukertoiminen polynomi, jonka juuria ovat $\alpha_1, \ldots, \alpha_n$, niin tällöin $f(\alpha_1, \ldots, \alpha_n)$ on rationaaliluku.*

Todistus. Olkoon $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ nollasta poikkeava polynomi, jonka juuret ovat $\alpha_1, \ldots, \alpha_n$. Tarkastelemalla polynomia voidaan huomata, että

$$p(x) = a_n \prod_{i=1}^{n} (x - \alpha_i) = a_n x^n - a_n \sigma_1 x^{n-1} + a_n \sigma_2 x^{n-2} + \cdots + (-1)^n a_n \sigma_n,$$

missä σ_i:t ovat symmetrisiä alkeispolynomeja $\alpha_1, ..., \alpha_n$ suhteen.

Jos $f \in \mathbb{Q}[x]$ on symmetrinen alkeispolynomi σ_k, niin

$$\sigma_k(\alpha_1, \ldots, \alpha_n) = \frac{a_k}{a_n},$$

joten $f(\alpha_1, \ldots, \alpha_n)$ on rationaalinen. Muussa tapauksessa voidaan hyödyntää symmetristen polynomien peruslausetta 3.19, jolloin f voidaan lausua symmetristen alkeispolynomien avulla. □

4 Kuntalaajennokset

Pohjatietoja on käsitelty edellisessä kappaleissa, joten pääsemme vihdoin tutustumaan kuntalaajennoksiin. Annetaan kuntalaajennokselle ensin määritelmä.

Määritelmä 4.1. Jos K on kunta, joka sisältää alikunnan L, niin K on alikunnan L kuntalaajennos. Merkitään tätä $K : L$.

Esimerkki 4.2. Kunta $\mathbb{C}$ on alikunnan $\mathbb{Q}$ kuntalaajennos eli voidaan merkitä $\mathbb{C} : \mathbb{Q}$.

Määritelmä 4.3. Olkoon X osajoukko kompleksilukujen joukosta $\mathbb{C}$. Tällöin joukon X *virittämä* $\mathbb{C}$:n alikunta on leikkaus kaikista $\mathbb{C}$:n alikunnista, jotka sisältävät osajoukon X.

Joukon X virittämä alikunta siis pienin kompleksilukujen joukon $\mathbb{C}$ alikunta, joka sisältää joukon X.

Määritelmä 4.4. Jos $L : K$ on kuntalaajennos ja $A \subset L$ osajoukko, niin tällöin yhdisteen $K \cup A$ virittämää $\mathbb{C}$:n alikuntaa merkitään $K(A)$ ja se on saatu kunnasta K *lisäämällä* siihen joukko A.

Kun joukko $A = \{a_1, ..., a_n\}$ on äärellinen voidaan merkitä $K(A) = K(a_1, ..., a_n)$. Alikunta $K(A)$ on määritelmän mukaisesti pienin niistä kompleksilukujen joukon alikunnista, jotka sisältävät joukot K ja A. Tutustaan yksinkertaiseen kuntalaajennokseen, jossa kuntaan on lisätty yhden alkion joukko.

Määritelmä 4.5. Yksinkertainen laajennos on sellainen kuntalaajennos $L : K$, että $L = K(\alpha)$ jollakin $\alpha \in L$.

Esimerkki 4.6. Esimerkissä 2.9 osoitettiin joukon K, joka on kaikkien muotoa $p+q\sqrt{2}$ olevien lukujen joukko, missä $p, q \in \mathbb{Q}$, olevan joukon $\mathbb{C}$ alikunta. Nyt $\mathbb{Q}(\sqrt{2}) = \{p + q\sqrt{2} : p, q \in \mathbb{Q}\}$ eli kyseessä on yksinkertainen kuntalaajennos.

Tutkitaan kahdenlaisia yksinkertaisia kuntalaajennoksia. Jos uusi kuntaan K lisättävä alkio toteuttaa polynomiyhtälön kunnassa K, niin laajennos on algebrallinen. Muussa tapauksessa kyseessä on transkendentti laajennos.

Määritelmä 4.7. Olkoon K kompleksilukujen kunnan $\mathbb{C}$ alikunta ja $\alpha \in \mathbb{C}$. Luku α on algebrallinen kunnan K suhteen, jos on olemassa polynomi p, joka ei ole nollapolynomi, kunnan K yli siten, että $p(\alpha) = 0$. Muussa tapauksessa luku α on transkendentti yli kunnan K.

Esimerkki 4.8. 1. Luku $\alpha = \sqrt{\pi}$ on algebrallinen kunnan $\mathbb{Q}(\pi)$ suhteen, koska $\alpha^2 - \pi = 0$ pätee.

2. Luku $\alpha = \sqrt{\pi}$ on transkendentti kunnan $\mathbb{Q}$ suhteen. Tämä seuraa tutkielman toisesta päätuloksesta, joka todistetaan luvussa 6.

Jotta voimme ymmärtää paremmin yksinkertaisten algebrallisten laajennosten rakennetta, tarvitsemme määritelmän lisättyyn alkioon α liittyvälle polynomille. Kutsumme kyseistä polynomia minimaalipolynomiksi ja annetaan sille seuraavaksi määritelmä.

Määritelmä 4.9. Olkoon $L : K$ kuntalaajennos ja oletetaan, että $\alpha \in L$ on algebrallinen kunnan K suhteen. Tällöin luvun α *minimaalipolynomi* kunnan K suhteen on alinta mahdollista astetta oleva yksikäsitteinen mooninen polynomi m siten, että $m(\alpha) = 0$.

Luvun α minimaalipolynomi kunnan K suhteen on yksikäsitteinen, koska jos polynomit m ja p olisivat alinta mahdollista astetta olevia moonisia polynomeja siten, että $m(\alpha) = p(\alpha) = 0$, niin $p(\alpha) - m(\alpha) = 0$. Nyt jos $p \neq m$ niin jokin monikerta $p - q$ on mooninen polynomi, jonka juuri luku α olisi. Tämä on ristiriita määritelmän kanssa, joten minimaalipolynomi on yksikäsitteinen.

Määritellään kongruenssirelaatio polynomeille vastaavasti kuin kokonaisluvuille.

Määritelmä 4.10. Polynomit $a, b \in K[t]$ ovat kongruentteja modulo m, merkitään tätä

$$a \equiv b \pmod{m},$$

jos $a(t) - b(t)$ on jaollinen polynomilla $m(t)$ kunnan $K[t]$ suhteen.

Lemma 4.11. *Oletetaan, että* $a_1 \equiv a_2 \pmod{m}$ *ja* $b_1 \equiv b_2 \pmod{m}$. *Tällöin*

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$$

ja

$$a_1 b_1 \equiv a_2 b_2 \pmod{m}$$

Todistus. Lemman todistus löytyy lähteestä [10, s. 74] □

Lemma 4.12. *Jokainen polynomi $a \in K[t]$ on kongruentti modulo m jonkin yksikäsitteisen polynomin kanssa, jonka aste on pienempi kuin polymonin m aste.*

Todistus. Polynomit $a, b \in K[t]$ ovat kongruentteja modulo m jos $a(t) - b(t)$ on jaollinen polynomin $m(t)$ kanssa. ($a \equiv b \pmod{m}$)

Proposition 3.10 eli jakoalgoritmin nojalla on olemassa yksikäsitteiset polynomit $q, r \in K[t]$ siten, että $a = qm + r$ ja $\partial r < \partial m$. Nyt

$$\begin{aligned} a &= qm + r \\ a - r &= qm \\ a &\equiv r \pmod{m}. \end{aligned}$$

Osoitetaan vielä polynomin r yksikäsitteisyys. Olkoon $r, s \in K[t]$. Oletetaan, että $r \equiv s \pmod{m}$ ja $\partial r, \partial s < \partial m$. Eli $r - s = pm$, mutta

$$\partial(r - s) \leq \max(\partial r, \partial s) < \partial m$$

Täytyy siis olla $r - s = 0$ eli $r = s$. Näin ollen polynomi r on yksikäsitteinen. □

Käytetään merkintää $K[t]/\langle m \rangle$ polynomirenkaan $K[t]$ ekvivalenssiluokista modulo m.

Lause 4.13. *Olkoon $m \neq 0$ mielivaltainen polynomi. Tällöin jokaisella nollasta poikkeavalla tekijärenkaan $K[t]/\langle m \rangle$ alkiolla on käänteisalkio tekijärenkaassa $K[t]/\langle m \rangle$ jos ja vain jos polynomi m on jaoton polynomirenkaassa $K[t]$.*

Todistus. Jos polynomi m on jaollinen niin tällöin $m = ab$, missä $\partial a, \partial b < \partial m$. Nyt $[a][b] = [ab] = [m] = [0]$. Oletetaan, että ekvivalenssiluokalla $[a]$ on käänteisalkio $[c]$, jolloin $[a][c] = 1$. Nyt siis $[0] = [c][0] = [c][a][b] = [1][b] = [b]$, joten näin ollen m jakaa polynomin b. Koska tiedetään, että $\partial b < \partial m$, täytyy olla $b = 0$ ja siten myös $m = 0$. Tämä on ristiriita, koska nollapolynomeilla on samat asteet.

Jos m on jaoton, niin olkoon $a \in K[t]$ siten, että $[a] \neq [0]$. Nyt polynomien m ja a suurin yhteinen tekijä on 1. Lauseen 3.12 nojalla on olemassa $h, k \in K[t]$ niin, että $ha + km = 1$. Tällöin $[h][a] + [k][m] = [1]$, mutta $[m] = [0]$, joten $[1] = [h][a] + [k][m] = [h][a] + [k][0] = [h][a] + [0] = [h][a]$. Näin ollen $[h]$ on kysytty käänteisalkio. □

Lause 4.14. *Olkoon $K(\alpha) : K$ yksinkertainen algebrallinen kuntalaajennos ja olkoon luvun α minimaalipolymoni kunnan K suhteen m. Tällöin $K(\alpha) : K$ on isomorfinen $K[t]/\langle m \rangle : K$ kanssa. Isomorfismi $K[t]/\langle m \rangle \to K(\alpha)$ voidaan valita kuvaamaan t luvuksi α.*

Todistus. Isomorfismin määrittelee kuvaus $[p(t)] \to p(\alpha)$, missä $[p(t)]$ on polynomin $p(t)$ ekvivalenssiluokka modulo m. Nyt kun $m|p$ eli $p = a \cdot m$ ja oletuksen mukaan m on minimaalipolymoni eli $m(\alpha) = 0$, niin $p(\alpha) = 0$. Kun $p(\alpha) = 0$ niin selvästi $m|p$. Nyt siis kuvaus on hyvin määritelty, koska $p(\alpha) = 0$ jos ja vain jos $m|p$.

Kyseessä on selvästi kuntahomomorfismi, koska kuvaus säilyttää laskutoimitukset. Kuvaus on injektio, koska jokainen ekvivalenssiluokka $[p(t)]$ kuvautuu omaksi luvukseen $p(\alpha)$. Koska kyseessä on myös injektio, niin kuvaus on kuntamonomorfismi.

Osoitetaan vielä, että kuvaus on surjektiivinen. Kuvajoukko on alikunta, joten se sisältää kaikki $K(\alpha)$:n alkiot. Toisaalta määritelmän mukaisesti $K(\alpha)$ on kunta, joka sisältää sekä K:n, että α:n. Täten $p(\alpha) \in K(\alpha)$ kaikilla polynomeilla p. Näin ollen kuvajoukko sisältyy $K(\alpha)$:aan. Kuvajoukko on siis $K(\alpha)$ eli kuvaus on surjektio. Koska kuntahomomorfismi on bijektio niin se on isomorfismi. Kyseinen isomorfismi kuvaa polynomin muuttujan t luvuksi α.

□

Esimerkki 4.15. Olkoon $\alpha = \sqrt[3]{2}$ ja $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ yksinkertainen algebrallinen kuntalaajennos. Kuntalaajennos on algebrallinen, koska $\alpha = \sqrt[3]{2}$ toteuttaa polynomiyhtälön $x^3 - 2 = 0$ kunnassa $\mathbb{Q}$. Polynomi $x^3 - 2$ on luvun α minimaalipolynomi kunnan $\mathbb{Q}$ suhteen, koska se on jaoton Eisensteinin kriteerin nojalla 3.8. Muodostetaan polynomirenkaan $\mathbb{Q}[x]$ ekvivalenssiluokat modulo $x^3 - 2$ ja merkitään niitä $\mathbb{Q}[x]/\langle x^3 - 2\rangle$. Nyt siis

$$\mathbb{Q}[x]/\langle x^3 - 2\rangle = \{p \mid x^3 - 2\}, \text{missä } p \in \mathbb{Q}[x].$$

Jakoalgoritmin 3.10 nojalla kaikille ekvivalenssiluokkien $[p(x)] \in \mathbb{Q}[x]/\langle x^3 - 2\rangle$ edustajille $p(x)$ ja minimaalipolynomille $x^3 - 2$ on olemassa polynomit f ja r siten, että

$$p = f \cdot (x^3 - 2) + r,$$

missä polynomin r aste on pienempää tai yhtä suurta kuin 2. Koska $m \mid p - r$, niin $[p] = [r]$. Näin ollen

$$[a_0 + a_1 x + a_2 x^2 : a_0, a_1, a_2 \in \mathbb{Q}]$$

ovat kaikki ekvivalenssiluokat $\mathbb{Q}[x]/\langle x^3 - 2\rangle$. Nyt lauseen 4.14 nojalla

$$\mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1(\sqrt[3]{2}) + a_2(\sqrt[3]{2})^2 : a_0, a_1, a_2 \in \mathbb{Q}\}.$$

Lemma 4.16. *Olkoon $K(\alpha) : K$ yksinkertainen algebrallinen kuntalaajennos, m on luvun α minimaalipolynomi kunnan K suhteen ja minimaalipolynomin m aste n. Tällöin $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ on kunnan $K(\alpha)$ kanta kunnan K suhteen.*

Todistus. Todistus seuraa lemmasta 4.12. □

Tutustutaan seuraavaksi kuntalaajennoksen asteeseen, joka on karkea arvio kyseisen kuntalaajennoksen koosta. Kuntalaajennoksen asteen määritelmää varten tarvitsemme pohjatietoja vektoriavaruuksista luvusta 2.

Määritelmä 4.17. Olkoon K kunta, joka on kunnan L kuntalaajennos. Tällöin kuntaa K voidaan tarkastella vektoriavaruutena, jonka skalaarikuntana on L. Tämän vektoriavaruuden dimensio eli ulottuvuus on kuntalaajennoksen $K : L$ aste ja sitä merkitään $[K : L]$.

Esimerkki 4.18. Esimerkissä 4.6 määritellyn kuntalaajennoksen $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ aste on 2. Kun tarkastelemme vektoriavaruutta $\mathbb{Q}(\sqrt{2})$, niin huomaamme voivamme muodostaa sillee kannan $\{1, \sqrt{2}\}$. Tällöin vektoriavaruuden dimensio on 2, koska sen kanta muodostuu kahdesta vektorista ja näin ollen kuntalaajennoksen $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ aste on myös 2 määritelmän 4.17 mukaisesti.

Seuraava lause auttaa määrittämään kuntalaajennoksen astetta myös haastavammissa tapauksissa.

Lause 4.19. *Jos K, L ja M ovat kompleksilukujen kunnan $\mathbb{C}$ alikuntia ja pätee $K \subseteq L \subseteq M$, niin*

$$[M : K] = [M : L][L : K]$$

Todistus. Olkoon $(x_i)_{i\in I}$ kanta alikunnalle L vektoriavaruutena kunnan K suhteen ja olkoon vastaavasti $(y_j)_{j\in J}$ kanta alikunnalle M kunnan L suhteen. Nyt jokaiselle $i \in I$ ja $j \in J$ on olemassa $x_i \in L$ ja $y_j \in M$. Osoitetaan, että $(x_i y_j)_{i\in I, j\in J}$ on kanta vektoriavaruudelle M kunnan K suhteen.

Osoitetaan ensin lineaarinen riippumattomuus. Oletetaan, että jokin äärellinen lineaarikombinaatio oletetun kannan alkioista on nolla.

$$\sum_{i,j} k_{ij} x_i y_j = 0, \text{missä } k_{ij} \in K.$$

Järjestellään yhtälöä uudelleen

$$\sum_j \left(\sum_i k_{ij} x_i \right) y_j = 0.$$

Nyt koska tiedämme $(y_j)_{j\in J}$ olevan kanta, jonka kertoimet ovat kunnassa L, niin tässä tapauksessa siis kertoimet $k_{ij}x_i$ ovat kunnassa L. Kannan $(y_j)_{j\in J}$ alkiot ovat lineaarisesti riippumattomia kunnan L suhteen, joten

$$\sum_i k_{ij} x_i = 0.$$

Toistamalla sama päättely kunnan L sisällä saadaan $k_{ij} = 0$ kaikilla $i \in I$ ja $j \in J$. Näin ollen alkiot $x_i y_j$ ovat lineaarisesti riippumattomia kunnan K suhteen.

Osoitetaan vielä, että alkiot $x_i y_j$ virittävät vektoriavaruuden M kunnan K suhteen. Jokainen alkio $x \in M$ voidaan kirjoittaa muodossa

$$x = \sum_j \lambda_j x_i,$$

jollekin sopivalle valinnalle $\lambda_j \in L$, koska y_j virittää vektoriavaruuden M kannan L suhteen. Vastaavasti jokaiselle $j \in J$

$$\lambda_j = \sum_i \lambda_{ij} x_i,$$

missä $\lambda_{ij} \in K$. Kun yhdistetään nämä tiedot, niin saadaan

$$x = \sum_{i,j} \lambda_{ij} x_i y_j.$$

Tämä osoittaa halutun väitteen.

□

Seuraava propositio kertoo, että yksinkertaisista kuntalaajennoksista algebrallisilla on äärellinen aste ja transkendenteilla ääretön.

Propositio 4.20. *Olkoon $K(\alpha) : K$ yksinkertainen kuntalaajennos. Jos kuntalaajennos on transkendentti, niin $[K(\alpha) : K] = \infty$. Jos kuntalaajennos on algebrallinen, niin $[K(\alpha) : K] = \partial m$, missä m on luvun α minimaalipolynomi kunnan K suhteen.*

Todistus. Käsitellään ensin tapaus, jossa yksinkertainen kuntalaajennos on transkendentti. Riittää tarkastella, että alkiot $1, \alpha, \alpha^2, ..$ ovat lineaarisesti riippumattomia kunnan K suhteen. Jos $1, \alpha, \alpha^2, ..$ ovat lineaarisesti riippuvaisia, niin on olemassa jokin lineaarikombinaatio

$$\sum_{i=0}^{n} \lambda_i \alpha^i = 0, \text{ missä } \lambda_i \neq 0 \text{ joillain } i = 0, ..., n.$$

Tällöin on löydetty polynomi $p(x) = \sum_{i=0}^{n} \lambda_i x^i$ siten, että sen kertoimia ovat λ_i:t ja $p(\alpha) = 0$. Kuitenkin luku α on oletuksen mukaan transkendentti eikä se voi olla polynomin $p(x)$ juuri. Näin ollen alkioiden $1, \alpha, \alpha^2, ..$ tulee olla lineaarisesti riippumattomia ja transkendentin yksinkertaisen kuntalaajennoksen aste ei ole äärellinen.

Toinen tapaus eli kun yksinkertainen laajennos on algebrallinen seuraa suoraan Lemmasta 4.16.

□

Esimerkki 4.21. Esimerkiksi kompleksiluvut $\mathbb{C}$ ovat reaalilukujen kunnan yksinkertainen laajennos $\mathbb{R}$(i). Nyt luvun i minimaalipolynomi on $x^2 + 1$ kunnan $\mathbb{R}$ suhteen ja sen aste on 2 eli $[\mathbb{C} : \mathbb{R}] = 2$ Proposition 4.20 nojalla.

5 Algebralliset luvut

Tämän luvun tavoitteena on kuvailla algebrallisten lukujen joukkoa esittelemällä niiden ominaisuuksia. Algebrallisista luvuista osataan kertoa huomattavasti enemmän kuin transkendenttiluvuista, joten esitellään seuraavaksi neljä algebrallisia lukuja koskevaa lausetta.

Lause 5.1. *Jos luku $\alpha \in \mathbb{R}$ on algebrallinen niin myös $-\alpha$ on algebrallinen.*

Todistus. Oletetaan, että luku α toteuttaa yhtälön $f(x) = 0$, missä

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + ... + c_1 x + c_0,$$

missä $c_i \in \mathbb{Q}$ kaikilla i. Olkoon $f_1(x) = f(-x)$, jolloin

$$f_1(-\alpha) = f(\alpha) = 0$$

ja täten luku $-\alpha$ on algebrallinen. □

Lause 5.2. *Olkoon luku $\alpha \in \mathbb{R}$ algebrallinen. Tällöin myös luvun α käänteisluku α^{-1} on algebrallinen kun luku α on nollasta poikkeava.*

Todistus. Oletetaan, että

$$c_n \alpha^n + c_{n-1} \alpha^{n-1} + ... + c_1 \alpha + c_0 = 0,$$

missä $c_i \in \mathbb{Q}$ kaikilla i. Jakamalla yhtälöä puolittain luvulla α^n saadaan

$$c_n + c_{n-1} \frac{1}{\alpha} + ... + c_1 \frac{1}{\alpha^{n-1}} + c_0 \frac{1}{\alpha^n} = 0$$

eli

$$c_n + c_{n-1} \alpha^{-1} + ... + c_1 \alpha^{-(n-1)} + c_0 \alpha^{-n} = 0.$$

Näin ollen nollasta poikkeavan algebrallisen luvun α käänteisluku α^{-1} on myös algebrallinen.

□

Tutkitaan seuraavaksi tilannetta, jossa meillä on kaksi algebrallista lukua ja haluamme tietää ovatko niiden summa ja tulo myös algebrallisia lukuja. Tilannetta voi tutkia monella eri lähestymistavalla ja tähän tutkielmaan on valikoitunut tapa, joka hyödyntää symmetrisiä alkeispolynomeja ja symmetristen polynomien peruslausetta 3.19. Vaihtoehtoinen todistus kahden algebrallisen luvun summan ja tulon algebrallisuudesta esitetään videolla [5] ja vielä kolmas lähestymistapa esitellään lähteessä [4, s. 46].

Tarkastellaan ensin esimerkkiä, joka auttaa hahmottamaan seuraavien lauseiden todistukset paremmin.

Esimerkki 5.3. Olkoon $q(x), r(x) \in \mathbb{Q}[x]$ määritelty siten, että

$$q(x) = x^2 + a_1 x + a_0$$

ja

$$r(x) = x^2 + b_1 x + b_0,$$

ja olkoon α_1, α_2 polynomin $q(x)$ nollakohtia ja β_1, β_2 polynomin $r(x)$ nollakohtia. Tarkastellaan polynomin $p(x) = \prod_{i=1}^{2} \prod_{j=1}^{2} (x - (\alpha_i + \beta_j))$ kertoimia, missä polynomin $p(x)$ nollakohdat ovat summat $\alpha_1 + \beta_1, \alpha_1 + \beta_2, \alpha_2 + \beta_1$ ja $\alpha_2 + \beta_2$. Avaamalla tulomerkintöjä ja sulkeita sopivalla tavalla saadaan

$$\begin{aligned}
p(x) &= \prod_{i=1}^{2} \prod_{j=1}^{2} (x - (\alpha_i + \beta_j)) \\
&= \prod_{i=1}^{2} (x - (\alpha_i + \beta_1))\,(x - (\alpha_i + \beta_2)) \\
&= (x - (\alpha_1 + \beta_1))\,(x - (\alpha_1 + \beta_2))\,(x - (\alpha_2 + \beta_1))\,(x - (\alpha_2 + \beta_2)) \\
&= x^4 - ((\alpha_1 + \beta_1) + (\alpha_1 + \beta_2) + (\alpha_2 + \beta_1) + (\alpha_2 + \beta_2))\,x^3 \\
&+ ((\alpha_1 + \beta_1)(\alpha_1 + \beta_2) + (\alpha_1 + \beta_1)(\alpha_2 + \beta_1) + (\alpha_1 + \beta_1)(\alpha_2 + \beta_2) \\
&+ (\alpha_1 + \beta_2)(\alpha_2 + \beta_1) + (\alpha_1 + \beta_2)(\alpha_2 + \beta_2) + (\alpha_2 + \beta_1)(\alpha_2 + \beta_2))x^2 \\
&- ((\alpha_1 + \beta_1)(\alpha_1 + \beta_2)(\alpha_2 + \beta_1) + (\alpha_1 + \beta_1)(\alpha_1 + \beta_2)(\alpha_2 + \beta_2) \\
&+ (\alpha_1 + \beta_1)(\alpha_2 + \beta_1)(\alpha_2 + \beta_2) + (\alpha_1 + \beta_2)(\alpha_2 + \beta_1)(\alpha_2 + \beta_2))x \\
&+ (\alpha_1 + \beta_1)(\alpha_1 + \beta_2)(\alpha_2 + \beta_1)(\alpha_2 + \beta_2).
\end{aligned}$$

Nyt polynomin termien kertoimia tutkimalla voidaan huomata, että polynomin $p(x)$ kertoimet vastaavat symmetrisiä alkeispolynomeja muuttujille $(\alpha_1+\beta_1), (\alpha_1+\beta_2), (\alpha_2+\beta_1)$ ja $(\alpha_2+\beta_2)$. Esimerkiksi määritelmän 3.16 mukaisesti symmetrinen alkeispolynomi σ_1 muuttujille $(\alpha_1+\beta_1), (\alpha_1+\beta_2), (\alpha_2+\beta_1)$ ja $(\alpha_2 + \beta_2)$ on

$$\sigma_1(\alpha_i + \beta_j) = (\alpha_1 + \beta_1) + (\alpha_1 + \beta_2) + (\alpha_2 + \beta_1) + (\alpha_2 + \beta_2),$$

joka vastaa x^3:n kerrointa polynomissa $p(x)$. Näin ollen polynomi $p(x)$ voidaan kirjoittaa muodossa

$$p(x) = x^4 - \sigma_1(\alpha_i + \beta_j)x^3 + \sigma_2(\alpha_i + \beta_j)x^2 - \sigma_3(\alpha_i + \beta_j)x + \sigma_4(\alpha_i + \beta_j).$$

Polynomin $p(x)$ kertoimia eli alkeispolynomeja $\sigma_1(\alpha_i+\beta_j), ..., \sigma_4(\alpha_i+\beta_j)$, joiden muuttujia ovat $(\alpha_1+\beta_1), (\alpha_1+\beta_2), (\alpha_2+\beta_1)$ ja $(\alpha_2+\beta_2)$, voidaan tarkastella polynomeina muuttujinaan α_1, α_2 siten, että kyseisten polynomien kertoimet ovat polynomirenkaassa $\mathbb{Q}[\beta_1, \beta_2]$. Polynomin $p(x)$ termin x^3 kerrointa vastaava polynomi $p_1(\alpha_1, \alpha_2)$ voidaan ryhmitellä seuraavalla tavalla

$$p_1(\alpha_1, \alpha_2) = 2\alpha_1 + 2\alpha_2 + (2\beta_1 + 2\beta_2) \cdot 1,$$

missä kerroin 2 ja vakiotermin kerroin $2\beta_1 + 2\beta_2$ kuuluvat polynomirenkaaseen $\mathbb{Q}[\beta_1, \beta_2]$. Käsitellään näitä kertoimia polynomeina, jolloin koska ne ovat symmetrisiä β_1 ja β_2 suhteen, niin ne voidaan lauseen 3.19 nojalla lausua symmetristen alkeispolynomien $\sigma_1(\beta_j), \sigma_2(\beta_j)$ avulla. Tällöin koska oletuksen mukaan β_1 ja β_2 ovat rationaalilukukertoimisen polynomin $r(x)$ juuria, niin lauseen 3.22 nojalla kertoimet 2 ja $2\beta_1 + 2\beta_2$ ovat rationaalisia.

Nyt siis polynomi p_1 on rationaalilukukertoiminen ja symmetrinen muuttujien α_1 ja α_2 suhteen, joten symmetristen polynomien peruslauseen nojalla 3.19 se voidaan lausua alkeispolynomien $\sigma_1(\alpha_i)$ ja $\sigma_2(\alpha_i)$ polynomina. Myös α_1 ja α_2 ovat rationaalilukukertoimisen polynomin $q(x)$ juuria, joten lauseen 3.22 nojalla $p_1(\alpha_1, \alpha_2)$ on rationaaliluku.

Toistamalla sama tarkastelu myös muille alkeispolynomeille $\sigma_2(\alpha_i + \beta_j), \sigma_3(\alpha_i, \beta_j), \sigma_4(\alpha_i + \beta_j)$ voidaan todeta polynomin p kaikkien kertoimien olevan rationaalilukuja eli $p(x) \in \mathbb{Q}[x]$.

Yleistetään esimerkki seuraavan lauseen avulla, jonka todistus noudattaa vastaavaa periaatetta.

Lause 5.4. *Olkoot $\alpha, \beta \in R$ algebrallisia lukuja. Tällöin myös luku $\alpha + \beta$ on algebrallinen.*

Todistus. Oletetaan, että $f(x), g(x) \in \mathbb{Q}[x]$ on määritetty siten, että

$$f(x) = x^m + a_1x^{m-1} + ... + a_m$$

ja

$$g(x) = x^n + b_1x^{n-1} + ... + b_n,$$

missä $a_i, b_j \in \mathbb{Q}$ kaikilla i, j. Oletetaan myös, että $f(\alpha) = 0$ sekä $g(\beta) = 0$.

Merkitään polynomin $f(x)$ nollakohtia $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n$ ja polynomin $g(x)$ nollakohtia $\beta_1 = \beta, \beta_2, ..., \beta_m$. Tarkastellaan polynomia

$$F(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - (\alpha_i + \beta_j)),$$

jonka nollakohtia ovat $\alpha_1 + \beta_1, \alpha_1 + \beta_2, ..., \alpha_n + \beta_m$. Nyt vastaavasti kuin esimerkissä 5.3 polynomin $F(x)$ kertoimet vastaavat symmetrisiä alkeispolynomeja muuttujissa $\alpha_i + \beta_j$. Alkeispolynomien $\sigma_1(\alpha_i + \beta_j), ..., \sigma_{nm}(\alpha_i + \beta_j)$ avulla polynomi $F(x)$ voidaan kirjoittaa uudelleen muodossa

$$\begin{aligned} F(x) &= \prod_{i=1}^{n} \prod_{j=1}^{m} (x - (\alpha_i + \beta_j)) \\ &= x^{nm} - \sigma_1(\alpha_i + \beta_j)x^{nm-1} + \sigma_2(\alpha_i + \beta_j)x^{nm-2} + ... + (-1)^{nm}\sigma_{nm}(\alpha_i + \beta_j). \end{aligned}$$

Polynomin $F(x) \in \mathbb{Q}[\alpha_i + \beta_j][x]$ muuttujana on x ja sen kertoimet kuuluvat kerroinrenkaaseen $\mathbb{Q}[\alpha_i + \beta_j]$. Tarkastellaan nyt polynomin $F(x)$ kertoimia polynomeina muuttujinaan $\alpha_1, ..., \alpha_n$, jolloin ne kuuluvat polynomirenkaaseen $\mathbb{Q}[\beta_j][\alpha_i]$. Kertoimet ovat siis polynomeja

$$\sigma_t = \sum_{j_1,...,j_n} q_{j_1,...,j_n}(\beta_1, \ldots, \beta_m)\alpha_1^{j_1} \cdots \alpha_n^{j_n},$$

missä $t = 1, \ldots, nm$, kertoimet $q_{j_1,...,j_n}(\beta_1, \ldots, \beta_m)$ ovat symmetrisiä β_j suhteen ja itse polynomi σ_i on symmetrinen muuttujissa α_i. Vastaavalla tavalla kuin esimerkissä 5.3, tarkastellaan ensin kertoimia $q_{j_1,...,j_n}(\beta_1, \ldots, \beta_m)$. Kertoimet ovat symmetrisiä eli ne voidaan lauseen 3.19 nojalla lausua symmetristen alkeispolynomien $\sigma_j(\beta_j)$ avulla. Määritelmän mukaisesti β_j kaikilla $j = 1, \ldots m$ on rationaalilukukertoimisen polynomin $g(x)$ juuri eli nollakohta. Nyt lauseen 3.22 nojalla kertoimet $q_{j_1,...,j_n}(\beta_1, \ldots, \beta_m)$ ovat rationaalilukuja.

Tästä seuraa, että kertoimet $\sigma_t = \sum_{j_1,...,j_n} q_{j_1,...,j_n}(\beta_1, \ldots, \beta_m)\alpha_1^{j_1} \cdots \alpha_n^{j_n}$ ovat rationaalilukukertoimisia symmetrisiä polynomeja siten, että α_i:t ovat polynomin $f(x) \in \mathbb{Q}[x]$ juuria, joten hyödyntämällä lauseita 3.19 ja 3.22 voidaan todeta kertoimien σ_t olevan rationaalilukuja. Nyt σ_t:t vastasivat polynomin $F(x)$ kertoimia eli näin ollen $F(x) \in \mathbb{Q}[x]$. Aiemmin asetettiin, että $\alpha_1 = \alpha$ ja $\beta_1 = \beta$ niin $\alpha_1 + \beta_1 = \alpha + \beta$, joten $\alpha + \beta$ on rationaalilukukertoimisen polynomin $F(x)$ juuri ja näin määritelmästä seuraa, että $\alpha + \beta$ on algebrallinen.

□

Lause 5.5. *Olkoot $\alpha, \beta \in R$ algebrallisia lukuja. Tällöin myös luku $\alpha\beta$ on algebrallinen.*

Todistus. Todistus on vastaavanlainen kuin edellisen lauseen todistus algebrallisten lukujen summasta. Tehdään siis alkuun samat oletukset eli oletetaan, että $f(x), g(x) \in \mathbb{Q}[x]$ on määritetty siten, että

$$f(x) = x^m + a_1 x^{m-1} + ... + a_m$$

ja

$$g(x) = x^n + b_1 x^{n-1} + ... + b_n,$$

missä $a_i, b_j \in \mathbb{Q}$ kaikilla i, j. Oletetaan myös, että $f(\alpha) = 0$ sekä $g(\beta) = 0$. Merkitään polynomin $f(x)$ nollakohtia $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n$ ja polynomin $g(x)$ nollakohtia $\beta_1 = \beta, \beta_2, ..., \beta_m$. Tarkastellaan kuitenkin tässä tapauksessa polynomia

$$F(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - \alpha_i \beta_j),$$

jonka nollakohtia ovat $\alpha_1\beta_1, \alpha_1\beta_2, ..., \alpha_n\beta_m$. Todistus etenee tästä eteenpäin vastaavalla tavalla kuin lauseen 5.4 todistus, jolloin nähdään, että polynomin $F(x)$ kertoimet ovat rationaalilukuja, joten $\alpha\beta$ on rationaalilukukertoimisen polynomin nollakohta ja täten algebrallinen luku. □

Edellisten lauseiden nojalla saadaan muodostettua seuraava tulos.

Seuraus 5.6. *Algebrallisten lukujen joukko on kunta.*

6 Transkendenttiluvut

Tässä luvussa esitellään todistukset tunnetuimmille transkendenttiluvuille sekä tutkielman lopuksi käsitellään kahta konstruktio-ongelmaa ja esitellään hieman millainen transkendenttilukujen tutkimisen tulevaisuus mahdollisesti on. Luvun päälähteenä on käytetty Stewartin kirjaa [10, s. 88-100, 288-291], jossa on esitelty lauseet lukujen π ja e transkendenttiudesta sekä perehdytty harppi-viivain-konstruktioihin. Tämän luvun lopussa alaluvussa 6.3 lähteenä on käytetty Lagariaksen artikkelia [6].

6.1 Lukujen π ja e transkendenttius

Lause 6.1. *Luku $\pi \in \mathbb{R}$ on transkendenttiluku.*

Todistus. Todistetaan väite epäsuoralla todistuksella. Oletetaan, että luku π on algebrallinen eli se on jonkin nollasta poikkeavan rationaalilukukertoimisen polynomin nollakohta. Tällöin myös $\mathrm{i}\pi$, missä $\mathrm{i} = \sqrt{-1}$, on jonkin rationaalilukukertoimisen polynomin nollakohta. Olkoon $\theta_1(x) \in \mathbb{Q}(x)$ polynomi, jonka nollakohtia ovat $\alpha_1 = \mathrm{i}\pi, \alpha_2, ..., \alpha_n$ eli

$$\theta_1(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Eulerin lauseen mukaisesti

$$e^{\mathrm{i}\pi} + 1 = 0,$$

joten

$$(e^{\alpha_1} + 1)(e^{\alpha_2} + 1)...(e^{\alpha_n} + 1) = 0 \tag{6.1}$$

tulon nollasäännön nojalla. Kun avataan yhtälöä 6.1 saadaan

$$1 + e^{\alpha_1} + e^{\alpha_2} + ... + e^{\alpha_n} + e^{\alpha_1+\alpha_2} + ... + e^{\alpha_1+\alpha_n} + ... + e^{\alpha_1+\alpha_2+...+\alpha_n} = 0. \tag{6.2}$$

Muodostetaan kokonaislukukertoiminen polynomi, jonka nollakohdat ovat luvun e eksponentit $\alpha_{i1} + ... + \alpha_{j_r}$, jotka esiintyvät yhtälössä 6.2. Olkoon θ_1 määritelty kuten edellä,

$$\theta_2 = a_2(x - (\alpha_1 + \alpha_2)) \cdots (x - (\alpha_1 - \alpha_n)) \cdots (x - (\alpha_{n-1} - \alpha_n)),$$

$$\vdots$$

ja

$$\theta_n = a_n(x - (\alpha_1 + \alpha_2 + \cdots + \alpha_{n-1} + \alpha_n)).$$

Vastaavalla tavalla kuin luvussa 5 lauseen 5.4 todistuksessa nähdään, että polynomit θ_i ovat rationaalilukukertoimisia symmetristen polynomien peruslauseen 3.19 nojalla. Näin ollen

$$\theta_1(x)\theta_2(x) \cdots \theta_n(x)$$

on polynomi, jonka nollakohdat ovat yhtälössä 6.2 esiintyvät luvun e eksponentit. Kun tämä polynomi jaetaan sopivalla muuttujan x potenssilla ja kerrotaan sopivalla kokonaisluvulla, niin saadaan polynomi $\theta(x) \in \mathbb{Z}[x]$, jonka nollakohdat ovat nollasta poikkeavat luvun e eksponentit yhtälöstä 6.2. Nyt yhtälö 6.2 voidaan kirjoittaa muodossa

$$e^{\beta_1} + ... + e^{\beta_r} + e^0 + ... + e^0 = 0$$

eli

$$e^{\beta_1} + ... + e^{\beta_r} + k = 0, \tag{6.3}$$

missä $k \in \mathbb{Z}$ ja $k > 0$, koska termi $1 \cdot 1 \cdots 1$ esiintyy yhtälössä 6.2. Oletetaan, että

$$\theta(x) = cx^r + c_1 x^{r-1} + ... + c_r,$$

koska luku 0 ei ole polynomin θ juuri, niin $c_r \neq 0$. Määritetään

$$f(x) = \frac{c^s x^{p-1} \left[\theta\left(x\right)\right]^p}{(p-1)!},$$

missä $s = rp - 1$ ja p on mikä tahansa alkuluku. Määritetään myös

$$F(x) = f(x) + f'(x) + ... + f^{(s+p+r-1)}(x)$$

ja huomioidaan, että $f^{(s+p+r)}(x) = 0$. Nyt

$$e^{-x}F(x) - F(0) = -\int_0^x e^{-y} f\left(y\right) dy,$$

koska

$$\frac{d}{dx}[e^{-x}F(x)] = -e^{-x}f(x).$$

Valitsemalla $y = \lambda x$ saadaan

$$F(x) - e^x F(0) = -e^x \int_0^1 e^{-\lambda x} f\left(\lambda x\right) d\lambda = -x \int_0^1 e^{(1-\lambda)x} f\left(\lambda x\right) d\lambda.$$

Muodostetaan summa siten, että muuttuja x käy läpi luvut $\beta_1, ..., \beta_r$. Yhtälön 6.3 nojalla $\sum_{i=1}^r e^{\beta_i} = -k$, joten

$$\sum_{i=1}^r F(\beta_i) + kF(0) = -\sum_{i=1}^r \beta_i \int_0^1 e^{(1-\lambda)\beta_i} f\left(\lambda\beta_i\right) d\lambda. \tag{6.4}$$

Osoitetaan, että kaikilla riittävän suurilla alkuluvuilla p yhtälön 6.4 vasen puoli on nollasta poikkeava kokonaisluku. Tutkitaan yhtälön 6.4 vasemman puolen ensimmäistä termiä eli summaa:

$$\sum_{i=1}^r F(\beta_i) = \sum_{i=1}^r \sum_{m=0}^{s+p+r-1} f^{(m)}(\beta_i).$$

Kun $0 \leq m < p$, niin

$$\sum_{i=1}^r f^{(m)}(\beta_i) = 0.$$

Kun taas $m \geq p$, niin jokaisella derivaatalla $f^{(m)}(\beta_i)$ on tekijänä p, koska $[\theta(x)]^p$ täytyy derivoida vähintään p kertaa, jotta saadaan nollasta poikkeava termi. Nyt jokaisella $m \geq p$

$$\sum_{i=1}^{r} f^{(m)}(\beta_i)$$

on symmetrinen polynomi $\beta_1, ..., \beta_r$ suhteen ja sen aste on $\leq s$. Nyt symmetristen polynomien peruslauseen 3.19 nojalla se voidaan lausua kokonaislukukertoimisena polynomina polynomin $\theta(x)/c$ kertoimista c_j/c, siten, että polynomin aste on $\leq s$. Luvulla c_s kertominen kun määriteltiin $f(x)$ tekee $\sum_{i=1}^{r} f^{(m)}(\beta_i)$:stä kokonaisluvun. Joten kun $m \geq p$, niin

$$\sum_{i=1}^{r} f^{(m)}(\beta_i) = pk_m$$

sopivalle $k_m \in \mathbb{Z}$ eli se on myös jaollinen luvulla p. Tutkitaan vielä mitä $F(0)$ on. Kun $0 \leq m \leq p-2$:

$$f(0) = 0, f'(0) = 0, ..., f^{(p-2)}(0) = 0 \quad \text{eli} \quad f^{(m)}(0) = 0.$$

Kun $m = p-1$ niin $f^{(m)}(0) = c^s(\theta(0))^p = c^s(c_r)^p$. Ja kun $m \geq p$ niin $f^{(m)}(0) = pl_m$ sopivalla kokonaisluvulla l_m. Nyt siis

$$kF(0) = k\left(0 + 0 + ... + 0 + c^s(c_r)^p + p\sum_{m=p}^{s+p+r-1} l_m\right).$$

Näin ollen yhtälön 6.4 vasen puoli on

$$\sum_{i=1}^{r} F(\beta_i) + kF(0) = tp + kc^s(c_r)^p$$

jollakin $t \in \mathbb{Z}$. Nyt $k \neq 0, c_r \neq 0$ ja $c \neq 0$. Jos valitaan p riittävän suureksi eli

$$p > \max(k, |c|, |c_r|),$$

niin vasen puoli yhtälöstä 6.4 on nollasta poikkeava kokonaisluku, joka ei ole jaollinen luvulla p. Arvioidaan vielä yhtälön 6.4 oikeaa puolta. Nyt kun $0 \leq \lambda \leq 1$, niin

$$\begin{aligned} |f(\lambda\beta_i)| &= \left|\frac{c^s\lambda^{p-1}\beta_i^{p-1}\theta(\lambda\beta_i)^p}{(p-1)!}\right| \\ &\leq \frac{|c^s||\beta_i|^{p-1}}{(p-1)!}\left[\sup_{0\leq\lambda\leq 1}|\theta(\lambda\beta_i)|\right]^p. \end{aligned}$$

Olkoon $m(i) = \sup_{0\leq\lambda\leq 1} |\theta(\lambda\beta_i)|$. Nyt siis

$$\left| -\sum_{i=1}^{r} \beta_i \int_0^1 e^{(1-\lambda)\beta_i} f\left(\lambda\beta_i\right) d\lambda \right| \leq \sum_{i=1}^{r} \frac{|c^s||\beta_i|^p |m(i)|^p}{(p-1)!} \max_{i=1,\ldots,r} \int_0^1 e^{(1-\lambda)\beta_i} d\lambda.$$

Maksimi integraalista on äärellinen ja tiedetään, että pätee raja-arvo

$$\frac{h^p}{(p-1)!} \to 0,$$

kun $p \to \infty$. Näin ollen jokainen summan termi suppenee nollaan tasaisen suppenemisen nojalla, ja siispä yhtälön 6.4 oikean puolen lauseke suppenee nollaan. Tästä aiheutuu ristiriita yhtälön vasemman puolen ollessa nollasta poikkeava kokonaisluku, joten luku π ei ole algebrallinen vaan transkendentti. □

Lause 6.2. *Luku $e \in \mathbb{R}$ on transkendenttiluku.*

Todistus. Osoitetaan väite epäsuoran todistuksen avulla. Oletetaan siis, että luku $e \in \mathbb{R}$ ei ole transkendentti, jolloin se on algebrallinen. Näin ollen e on jonkin polynomin $P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ juuri eli

$$a_n e^n + a_{n-1}e^{n-1} + ... + a_1 e + a_0 = 0. \tag{6.5}$$

Oletetaan, että polynomin kertoimet $a_0, ..., a_n$ ovat kokonaislukuja ja $a_0 \neq 0$. Määritetään

$$f(x) = \frac{x^{p-1}(x-1)^p(x-2)^p...(x-n)^p}{(p-1)!},$$

missä p on mielivaltainen alkuluku. Nyt f on polynomi, jonka aste on $np + p - 1$. Asetetaan

$$F(x) = f(x) + f'(x) + ... + f^{(np+p-1)}(x)$$

ja huomataan, että $f^{(np+p)}(x) = 0$. Laskemalla saadaan

$$\begin{aligned}\frac{d}{dx}\left(e^{-x}F(x)\right) &= \frac{d}{dx}\left(e^{-x}\left(f(x) + f'(x) + ... + f^{(np+p-1)}\right)\right) \\ &= -e^{-x}f(x) + e^{-x}f'(x) - e^{-x}f'(x) + e^{-x}f''(x) - ... \\ &= -e^{-x}f(x).\end{aligned}$$

Näin ollen kaikille i pätee

$$a_i \int_0^i e^{-x} f\left(x\right) dx = a_i \left[-e^{-x}F\left(x\right)\right]_0^i = a_i F(0) - a_i e^{-i} F(i).$$

Kerrotaan tätä luvulla e^i ja summataan kun $i = 0, 1, ..., n$, jolloin

$$\sum_{i=0}^{n} \left(a_i e^i \int_0^i e^{-x} f(x)\, dx \right) = F(0) \sum_{i=0}^{n} a_i e^i - \sum_{i=0}^{n} a_i F(i)$$
$$\overset{(6.5)}{=} -\sum_{i=0}^{n} \sum_{j=0}^{np+p-1} a_i f^{(j)}(i). \tag{6.6}$$

Osoitetaan, että jokainen $f^{(j)}(i)$ on alkuluvulla p jaollinen kokonaisluku ellei $i = 0$ tai $j = p - 1$. Hyödynnetään Leibnizin sääntöä, jolloin ainoat nollasta poikkeavat termit kun $i \neq 0$ muodostuvat kun tekijää $(x - i)^p$ derivoidaan täsmälleen p kertaa. Koska $\frac{p!}{(p-1)!} = p$, niin kaikki nämä termit ovat kokonaislukuja, jotka ovat jaollisia luvulla p. Poikkeustapauksessa kun $i = 0$, ensimmäinen nollasta poikkeava termi esiintyy kun $j = p - 1$ ja tällöin

$$f^{(p-1)}(0) = (-1)^p \dots (-n)^p.$$

Peräkkäiset nollasta eriävät termit ovat kaikki luvun p monikertoja. Näin ollen yhtälön 6.6 arvo jollekin kokonaisluvulle K on

$$K_p + a_0(-1)^p ... (-n)^p.$$

Jos valitaan $p > \max(n, |a_0|)$, niin kokonaisluku $a_0(-1)^p ... (-n)^p$ ei ole jaollinen luvulla p. Näin ollen riittävän suurilla alkuluvuilla p yhtälön 6.6 arvo on luvulla p jaoton kokonaisluku ja täten se on nollasta poikkeava. Arvioidaan seuraavaksi integraalia. Kun $0 \leq x \leq n$, niin

$$|f(x)| \leq \frac{n^{np+p-1}}{(p-1)!},$$

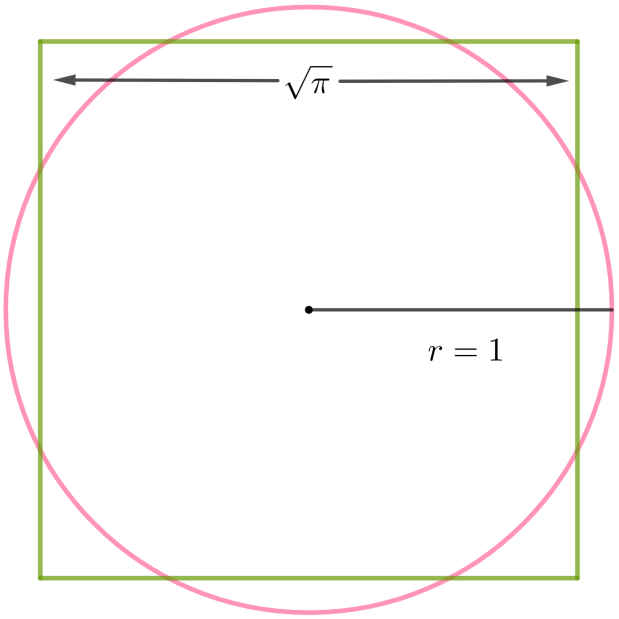
joten

$$\left| \sum_{i=0}^{n} a_i e^i \int_0^i e^{-x} f(x)\, dx \right| \leq \sum_{i=0}^{n} \left| a_i e^i \right| \int_0^i \frac{n^{np+p-1}}{(p-1)!} dx \leq \sum_{i=0}^{n} \left| a_i e^i \right| \, i \frac{n^{np+p-1}}{(p-1)!}$$

ja tämä lähestyy lukua 0 kun p lähestyy positiivista ääretöntä. Tämä on ristiriita sen kanssa, että yhtälön 6.6 arvon pitäisi olla nollasta poikkeava luvulla p jaoton kokonaisluku, kun p on riittävän suuri. Näin ollen luku e on transkendentti eikä algebrallinen. □

6.2 Konstruktio-ongelmat

Ympyrän kehän suhdetta sen halkaisijaan kuvaavan luvun π transkendenttiuden todistaminen ratkaisi yhden antiikin suurista konstruktio-ongelmista. Ympyrän neliöinnin konstruktio-ongelmassa tarkastellaan tilannetta, jossa harpin ja viivaimen avulla halutaan konstruoida annetun ympyrän pinta-alaa vastaava neliö. Haluttua tilannetta on havainnollistettu kuvassa 6.1, jossa ympyrän säde on 1 ja neliön sivun pituus on $\sqrt{\pi}$, jolloin molempien kappaleiden pinta-alat ovat π.



Kuva 6.1: Kuvan ympyrällä ja neliöllä on sama pinta-ala.

Osoitetaan seuraavaksi, että kuvan 6.1 mukaista neliötä ei pystytä konstruoimaan annetun ympyrän avulla.

Lause 6.3. *Annetun ympyrän kanssa pinta-alaltaan yhtä suurta neliötä ei ole mahdollista muodostaa käyttämällä harppi-viivain-konstruktioita.*

Todistus. Ympyrän neliöimisen ongelman tarkastelu voidaan rajata tilanteeseen, jossa ympyrän säde on 1 ja täten sen pinta-ala on π. Tässä tapauksessa

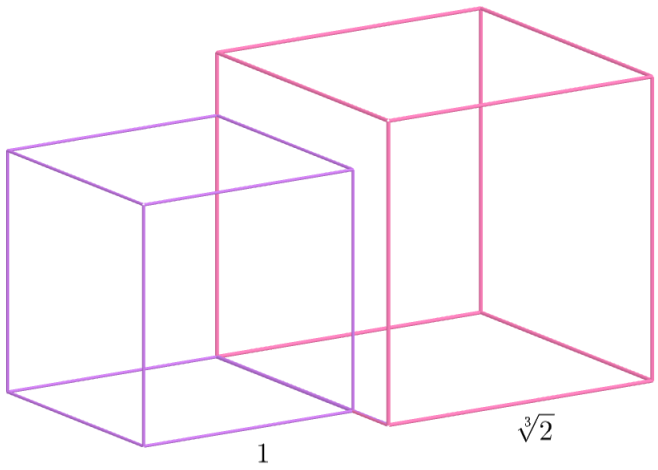
ympyrän pinta-alan suuruutta vastaavan neliön sivun pituus on $\sqrt{\pi}$. Onnistunut konstruktio tilanteesta vastaa sitä, että voitaisiin konstruoida jana, jonka pituus on $\sqrt{\pi}$.

Jos $\sqrt{\pi}$ on konstruoitava luku, niin tällöin on mahdollista konstruoida myös π. Kuitenkin Gaussin oppilas Pierre Wantzel osoitti vuonna 1837, että harppi-viivain-konstruktioiden avulla luotujen janojen pituuksien täytyy olla joidenkin rationaalikertoimisten polynomien juuria [10, s. 88, 98].

Näin ollen konstruoitavat janojen pituudet ovat algebrallisia lukuja. Tässä tapauksessa se tarkoittaa, että luvun π tulee olla algebrallinen, jotta ympyrän neliöinti olisi mahdollista vain harppia ja viivainta käyttämällä. Lauseen 6.1 nojalla luku π on transkendentti, joten ympyrän neliöinti ei ole mahdollista harppi-viivain-konstruktioilla.

□

Toinen kiinnostava antiikin aikainen konstruktio-ongelma liittyy kuution tilavuuden kaksinkertaistamiseen. Kyseistä ongelmaa kutsutaan myös kuution kahdentamiseksi. Haluttua konstruktiota on havainnollistettu kuvassa 6.2, jossa pienemmän kuution sivun pituus on 1 ja suuremman kuution sivun pituus on $\sqrt[3]{2}$ eli kuutioiden tilavuudet ovat 1 ja 2. Osoitetaan, että kuvan kaltaista suurempaa kuutiota ei voida konstruoida pienemmästä annetusta kuutiosta.



Kuva 6.2: Pienemmän kuution tilavuus on 1 ja suuremman tilavuus on 2.

Lause 6.4. *Annettua kuutiota ei voida kahdentaa käyttämällä harppi-viivain-konstruktioita.*

Todistus. Voimme rajoittaa tarkastelun tilanteeseen, jossa annetun kuution sivun pituus on 1 ja näin ollen kuution tilavuus on $1^3 = 1$. Kuution kärkien etäisyydet toisistaan ovat $1, \sqrt{2}$ tai $\sqrt{3}$. Jos voisimme kahdentaa kuution niin voisimme konstruoida janan, jonka pituus d toteuttaa yhtälön $d^3 = 2$. Tällöin lähteessä [10, 7.12, s. 98] esitetyn lauseen nojalla kuntalaajennoksen $[\mathbb{Q}(d) : \mathbb{Q}]$ asteen tulisi olla luvun 2 potenssi. Kuitenkin d on rationaalilukukertoimisen polynomin $t^3 - 2$ juuri ja Eisensteinin kriteerin 3.8 mukaisesti jaoton kunnan $\mathbb{Q}$ suhteen. Näin ollen $t^3 - 2$ on luvun d minimaalipolynomi ja proposition 4.20 mukaisesti $[\mathbb{Q}(d) : \mathbb{Q}] = 3$. Tämä on ristiriita, koska luku 3 ei ole luvun 2 potenssi. Näin ollen kuutiota ei voida kahdentaa harpin ja viivaimen avulla. □

6.3 Tulevaisuuden suuntia

Transkendenttilukujen saralla riittää edelleen tutkittavaa, vaikka useihin niitä koskeviin kysymyksiin onkin löydetty ratkaisut 1900-luvun alun jälkeen. Yksi merkittävistä edistysaskeleista transkendenttilukujen tutkimuksen saralla on vuonna 1935 esitetty ratkaisu Hilbertin seitsemänteen ongelmaan. Tuloksen mukaan luku a^b on aina transkendentti, jos $a \neq 0, 1$ on algebrallinen ja b on irrationaalinen algebrallinen luku.

Haasteena uusien transkendenttilukujen löytämisessä on yleisen menettelytavan puuttuminen, jolla voitaisiin testata onko luku algebrallinen vai transkendentti. Eulerin vakio, joka tunnetaan myös Eulerin-Mascheronin vakiona, määritellään harmonisen sarjan ja luonnollisen logaritmin erotuksen raja-arvona

$$\gamma = \lim_{n \to \infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \ln n \right).$$

Vakion likiarvo kymmenen desimaalin tarkkuudella on $0,5772156649$ ja se on yksi esimerkki luvusta, jota ei ole onnistuttu osoittamaan algebralliseksi tai transkendentiksi. Kyseinen luku on poikkeuksellinen sen takia, että myös sen irrationaalisuus on avoin ongelma edelleen.

Yleisen menettelytavan puuttumisen lisäksi transkendenttiustodistuksiin liittyy usein myös teknisiä haasteita. Näiden syiden takia tekoälyn kehittyminen voi avata uusia mahdollisuuksia lukujen algebrallisuuden ja transkendenttiuden tutkimiselle. Toivon mukaan transkendenttilukujen tutkimus ottaa seuraavien vuosikymmenien aikana edistysaskeleita ja yhä useampia transkendenttilukuja löydetään sekä niiden ominaisuuksista osataan kertoa enemmän.

Viitteet

[1] Hamza Elhadi S. Daoub: *The fundamental theorem of symmetric polynomials*. The teaching of mathematics, vol. XV (1):55–59, 2012.

[2] Janot de Stainville: *Mélanges d'analyse algébrique et de géométrie*. Veuve Courcier, 1815.

[3] Harold Jeffreys: *Scientific inference*. kolmas laitos, Cambridge: University Press, 1973.

[4] Lauri Kahanpää: *Algebra II, mahdollisuuksia ja mahdottomuuksia*. Jyväskylän yliopisto, 1991. http://users.jyu.fi/~laurikah/Algebrajatko.pdf. Luettu 15.5.2024.

[5] S. A. Katre: *Number Theory Lecture #34 Algebraic & Transcendental Numbers*. Youtube video, 1.4.2023. https://youtu.be/h7wJB0cYSFY?si=tpIEHVCe94oABcFr.

[6] Jeffrey C. Lagarias: *Euler's constant: Euler's work and modern developments*. Bulletin of the American Mathematical Society, vol. 50 (4):527–628, 2013.

[7] Serge Lang: *Algebra*. toinen laitos, Addison-Wesley, 1984.

[8] Peter Petersen: *Linear Algebra*. Springer New York, 2012.

[9] Denis Roegel: *Lambert's proof of the irrationality of Pi: Context and translation*. LORIA, 2020.

[10] Ian Stewart: *Galois Theory*. neljäs laitos, CRC Press, 2015.

[11] Tuomo Äkkinen: *Lineaarinen algebra ja geometria 1*. Jyväskylän yliopisto, 2019. https://tim.jyu.fi/files/202738/Linkku1uusi.pdf. Luettu 18.4.2024.