Tampereen yliopisto

Jesse Nieminen

KUNTALAAJENNUKSIA JA GALOIS'N TEORIAA

Tekniikan ja luonnontieteiden tiedekunta
Kandidaatintyö
Helmikuu 2021

TIIVISTELMÄ

Jesse Nieminen: Kuntalaajennuksia ja Galois'n teoriaa
Kandidaatintyö
Tampereen yliopisto
Tekniikka ja luonnontieteet, TkK
Helmikuu 2021

Tässä tutkielmassa rakennetaan pohjaa Galois'n teorialle ja tutustutaan sen alkeisiin. Galois'n teoria on abstraktin algebran osa-alue, joka käsittelee kuntateorian ja ryhmäteorian välistä yhteyttä. Sen avulla monia kuntateoriaan liittyviä ongelmia voidaan ratkaista ryhmäteorian avulla. Esimerkiksi polynomin termien kerrointen tarkastelun sijaan voidaan tarkastella saman polynomin juurten permutaatiokuvausten muodostamaa ryhmää. Tämän ryhmän ominaisuuksien perusteella voidaan päätellä esimerkiksi, että voidaanko kyseisen polynomin juuret esittää äärellisinä yhteen-, vähennys-, kerto- ja jakolaskuista ja juurenotoista koostuvina lausekkeina.

Galois'n teoriaan ei voida kuitenkaan hypätä suoraan pelkän kandidaatintutkinnon aineopintoihin kuuluvan algebran kurssin pohjalta. Nykyaikainen Galois'n teoria perustuu kuntalaajennusten teoriaan, johon matematiikkaa opiskeleva henkilö törmää yleensä aikaisintaan maisteritason opinnoissa. Kuntalaajennus muodostuu kahdesta kunnasta, joista ensimmäistä kutsutaan lähtökunnaksi ja toista laajennuskunnaksi. Kaikki lähtökunnan alkiot sisältyvät laajennuskuntaan, jossa on yleensä myös lähtökuntaan kuulumattomia alkioita. Voidaan siis ajatella, että lähtökuntaa on laajennettu liittämällä sinne uusia alkioita.

Tämän tutkielman alussa määritellään perusteellisesti polynomi ja esitellään muita siihen liittyviä käsitteitä ja lauseita. Erityisesti jaollisuuden käsite on tärkeä. Tämän jälkeen määritellään kuntalaajennus ja käsitellään sen teoriaa polynomien pohjalta, jonka jälkeen rakennetaan Galois'n teorian perusteet kuntalaajennusten pohjalta. Lopuksi todistetaan, että polynomin juurten permutaatiokuvausten muodostaman ryhmän koko on sama kuin sellaisen kuntalaajennuksen aste, jossa kyseisen polynomin kerroinkuntaa on laajennettu liittämällä siihen sen juuret.

Työn tarkoituksena on jatkaa kandidaatintutkintoon kuuluvalla abstraktin algebran kurssilla käsiteltyjen asioiden pohjalta ja esitellä Galois'n teorian alkeiden ymmärtämiseen vaadittavat käsitteet ja todistukset mahdollisimman täsmällisesti ja aukottomasti. Kokonaisuudessaan tämä tutkielma antaa lukijalleen hyvän pohjan kuntalaajennuksista ja Galois'n teorian alkeista, josta on hyvä jatkaa esimerkiksi Galois'n teorian ja muun abstraktin algebran opiskelua.

Avainsanat: abstrakti algebra, moderni algebra, polynomi, kuntalaajennus, Galois'n teoria

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

$\mathbb{N} = \{0, 1, 2, \ldots\}$	luonnolliset luvut
$(a_n) = (a_0, a_1, a_2, \ldots)$	ääretön jono
$R[x]$	renkaan R polynomit
$K[x]$	kunnan K polynomit
p_n	polynomin p astetta n olevan termin kerroin
$\max\{\mathrm{a}, \mathrm{b}\}$	suurempi luvuista
$\deg(p)$	polynomin aste
$\mathrm{syt}(p, q)$	perusmuotoinen suurin yhteinen tekijä
$\tilde{p}$	polynomia p vastaava polynomikuvaus
L/K	kuntalaajennus, missä K on lähtökunta ja L laajennuskunta
$K(A)$	joukon A virittämä kunta
$K(\alpha)$	alkion α virittämä kunta
m_α	alkion α minimaalipolynomi
$[L : K]$	kuntalaajennuksen aste
$\mathrm{Aut}(L/K)$	Automorfismien muodostama ryhmä
$\mathrm{Gal}(L/K)$	Galois'n ryhmä
$\lvert\mathrm{Gal}(L/K)\rvert$	Galois'n ryhmän koko

1 JOHDANTO

Galois'n teoria on yksi modernin algebran helmistä. Se luo kuntateorian ja ryhmäteorian välille yhteyden, jonka avulla voidaan selittää esimerkiksi miksi toisen, kolmannen ja neljännen asteen polynomiyhtälön ratkaisukaava on tiettyä muotoa ja miksi sellaista ei ole olemassa viidennen tai sitä korkeamman asteen polynomiyhtälölle. Myös jotkin klassisen geometrian ongelmat voidaan osoittaa mahdottomiksi ratkaista. Pelkkää harppia ja viivainta, jossa ei ole merkintöjä pituuksille, käyttämällä on mahdotonta jakaa mielivaltainen kulma kolmeen yhtä suureen osaan tai piirtää kuution pohjalta uusi kuutio, jonka tilavuus on kaksinkertainen alkuperäiseen nähden.

Ensimmäisessä luvussa määritellään polynomit ja todistetaan niitä koskevia tärkeitä lauseita. Polynomit määritellään sellaisella tavalla, joka toimii yleisen renkaan tapauksessa, jolloin polynomin kerrointen ei välttämättä täydy olla esimerkiksi reaalilukuja. Sitten käsitellään polynomin astetta ja jaollisuutta, joita tarvitaan jakoyhtälön määrittelemiseksi. Lopuksi tarkastellaan polynomin nollakohtia.

Toisessa luvussa käsitellään kuntalaajennusten teoriaa. Määritellään kuntalaajennus ja algebrallisuuden käsite, jonka jälkeen siirrytään käsittelemään minimaalipolynomeja. Kuntalaajennukselle määritellään myös aste sen muodostaman vektoriavaruuden avulla, jonka jälkeen lopetetaan hajotuskuntiin ja separoituvuuteen.

Kolmannessa luvussa tarkastellaan itse Galois'n teoriaa määrittelemällä Galois'n ryhmän käsite. Normaalisulkeumien kautta siirrytään kohti Galois'n teorian päälauseesta, josta lopuksi todistetaan heikennetty versio aikaisemmin rakennetun teorian pohjalta.

Työn tarkoituksena on esitellä kuntalaajennusten teoriaa ja Galois'n teorian alkeita. Lukijalta oletetaan hyvää tuntemusta modernin algebran perusteista esimerkiksi teoksen [2] pohjalta. Tutkielman rakenne ja sisältö pohjautuu teokseen [3].

2 POLYNOMIT

Tässä luvussa tarkastellaan polynomia ja siihen liittyviä käsitteitä modernin algebran näkökulmasta. Esitetty teoria perustuu teokseen [2].

2.1 Polynomirengas

Määritellään polynomin ja polynomirenkaan käsitteet yleisen renkaan tapauksessa. Renkaan määritelmä on esitetty lähteessä [2, s. 163]. Lisäksi tässä tutkielmassa kaikki renkaat ovat vaihdannaisia ja ne sisältävät neutraalialkion kertolaskun suhteen. Myös kunta toteuttaa lähteessä annetun määritelmän [2, s. 178].

Polynomit ajatellaan usein lausekkeina, jotka koostuvat muuttujan x potenssien ja vakioiden tuloista ja summista. Niiden tarkastelu modernin algebran kannalta vaatii kuitenkin täsmällisemmän määritelmän, joka esitetään seuraavaksi.

Määritelmä 2.1 (Polynomi)**.** Olkoon $p = (p_0, p_1, \ldots) = (p_n)$ ääretön jono renkaan R alkioita. Jos on olemassa sellainen indeksi m, että $p_n = 0$, kun $n > m$, niin jonoa p sanotaan renkaan R *polynomiksi*. Kaikkien renkaan R polynomien joukkoa merkitään $R[x]$.

Toisin sanoen, polynomit määriteltiin äärettöminä jonoina, joissa on vain äärellinen määrä nollasta poikkeavia alkioita. Seuraavaksi määritellään näille jonoille yhteen- ja kertolasku.

Määritelmä 2.2 (Summa ja tulo)**.** Olkoot p ja q joukon $R[x]$ alkioita. Määritellään yhteenlasku sellaiseksi, että

$$p + q = (p_0 + q_0, p_1 + q_1, \ldots) = (p_n + q_n)$$

ja kertolasku sellaiseksi, että

$$pq = (p_0 q_0, p_0 q_1 + p_1 q_0, \ldots) = \left(\sum_{i=0}^{n} p_i q_{n-i} \right).$$

Renkaan R polynomien joukko $R[x]$ muodostaa renkaan edellä määriteltyjen yhteen- ja kertolaskun suhteen. Todistus on suoraviivainen ja löytyy lähteestä [2, s. 285]. Tästä lähtien joukkoa $R[x]$ kutsutaan polynomirenkaaksi.

Vaikka polynomi on määritelty äärettömänä jonona, voidaan se silti esittää summana muuttujan x potenssien avulla. Ensin pitää kuitenkin määritellä, että mikä tämä muuttuja x on.

Määritelmä 2.3 (Nolla- ja vakiopolynomi)**.** Olkoon $p = (p_0, p_1, p_2, \ldots)$ polynomirenkaan $R[x]$ alkio. Polynomia p sanotaan *vakiopolynomiksi*, jos $p_n = 0$, kun $n = 1, 2, 3, \ldots$ Jos lisäksi $p_0 = 0$, polynomia p sanotaan *nollapolynomiksi*. Jos polynomi ei ole vakiopolynomi, niin sitä sanotaan *vakiosta eroavaksi*. Vastaavasti, jos polynomi ei ole nollapolynomi, niin sitä sanotaan *nollasta eroavaksi*.

Huomataan, että jokaista polynomirenkaan $R[x]$ vakiopolynomia p vastaa yksikäsitteinen renkaan R alkio p_0, missä p_0 jonon p ensimmäinen alkio. Vakiopolynomi p voidaankin siis samaistaa alkion p_0 kanssa.

Huomautus 2.4. Polynomirenkaan $R[x]$ vakiopolynomia $p = (p_0, 0, 0, \ldots)$ voidaan merkitä lyhyesti renkaan R alkiolla p_0, jolloin merkitään $p = p_0$.

Esimerkki 2.5. Jos $p = (2, 0, 0, \ldots)$ niin voidaan merkitä lyhyesti, että $p = 2$.

Polynomit esitetään usein tuntemattoman alkion x avulla. Määritellään seuraavaksi tämä alkio x polynomina.

Määritelmä 2.6. Polynomirenkaan $R[x]$ alkiota $(0, 1, 0, \ldots)$, jossa kaikki paitsi toinen alkio ovat nollia, merkitään symbolilla x.

Apulause 2.7. *Olkoon n luonnollinen luku. Määritellään, että x^n tarkoittaa tuloa, jossa polynomi 1 kerrotaan polynomilla x täsmälleen n kertaa. Tällöin x^n on polynomi, jonka jonoesityksen kaikki alkiot ovat nollia paitsi $x_n^n = 1$.*

Todistus. Väite on selvästi tosi tapauksissa $n = 0$ ja $n = 1$ vakiopolynomin ja polynomin x määritelmän nojalla. Lisäksi jos väite on tosi kun $n \leq k$, missä k on luonnollinen luku, joka on suurempi kuin 1, niin väite on tosi myös tapauksessa $n = k + 1$, koska polynomien tulon määritelmän nojalla polynomin $x^{k+1} = x^k \cdot x$ jonoesityksen ainoa jollasta eroava kerroin on $x_{k+1}^{k+1} = x_k^k \cdot x_1 = 1$. Väite on siis tosi kun n on mikä tahansa luonnollinen luku matemaattisen induktioperiaatteen nojalla. □

Lause 2.8. *Olkoon $p = (p_0, p_1, p_2, \ldots)$ polynomirenkaan $R[x]$ alkio. Tällöin polynomi p voidaan esittää äärettömänä summana*

$$\sum_{n=0}^{\infty} p_n x^n.$$

Todistus. Jos p_n on nollapolynomi niin $p_n x^n = 0$. Muussa tapauksessa polynomin $p_n x^n$ jonoesityksen ainoa nollasta eroava alkio on polynomia p_n vastaava vakio. Tällöin polynomien summan määritelmän nojalla polynomin

$$\sum_{n=0}^{\infty} p_n x^n$$

se kerroin jonka indeksi on n, on polynomia p_n vastaava renkaan R alkio, jolloin

$$p = \sum_{n=0}^{\infty} p_n x^n.$$

□

Esimerkki 2.9. Polynomi $(2, 3, 0, 1, \ldots)$, jossa on täsmälleen kolme nollasta eroavaa alkiota, voidaan esittää muodossa $x^3 + 3x + 2$.

2.2 Polynomin aste

Yksi tärkeimmistä polynomeihin liittyvistä käsitteistä on jaollisuus ja se tullaan määrittelemään polynomeille melko samanlaiseen tapaan kuin kokonaisluvuille. Ennen tätä täytyy kuitenkin määritellä polynomeille astefunktio.

Määritelmä 2.10 (Johtava kerroin)**.** Olkoon p polynomirenkaan $R[x]$ alkio ja olkoon n suurin sellainen luonnollinen luku, että $p_n \neq 0$. Tällöin kerrointa p_n sanotaan polynomin p *johtavaksi kertoimeksi*. Polynomia p sanotaan *perusmuotoiseksi*, jos sen johtava kerroin on 1.

Määritelmä 2.11 (Polynomin aste)**.** Olkoon p polynomirenkaan $R[x]$ nollasta eroava alkio. Tällöin on olemassa suurin sellainen kokonaisluku n, että $p_n \neq 0$, jolloin määritellään $\deg(p) = n$. Nollapolynomin tapauksessa johtavaa kerrointa ei ole, joten nollapolynomille ei määritellä astetta.

Polynomin asteelle on voimassa intuitiivisia, mutta hyödyllisiä ominaisuuksia. Kahden polynomin summan aste on korkeintaan suurempi summattavien polynomien asteista ja kahden polynomin tulon aste on korkeintaan tulon tekijöiden asteiden summa. Nämä eivät ole yhtälöitä, koska summattavien polynomien johtavat kertoimet voivat kumota toisensa summassa ja myöskin tulon tekijöiden johtavien kerrointen tulo voi olla nolla yleisen renkaan tapauksessa.

Lause 2.12. *Olkoot p ja q polynomirenkaan $R[x]$ nollasta eroavia alkioita. Tällöin on voimassa epäyhtälö*

$$\deg(p+q) \leq \max\{\deg(p), \deg(q)\}.$$

Todistus. Merkitään polynomin $p+q$ astetta symbolilla n. Jos n on suurempi kuin polynomin p aste, niin $p_n = 0$ ja vastaavasti jos n on suurempi kuin polynomin q aste, niin $q_n = 0$. Polynomin $p+q$ johtava kerroin $p_n + q_n$ ei kuitenkaan saa olla nolla, joten varmasti $p_n \neq 0$ tai $q_n \neq 0$. Tällöin on oltava $n \leq \deg(p)$ tai $n \leq \deg(q)$, jolloin alkuperäinen epäyhtälö on tosi. □

Lause 2.13. *Olkoot p ja q polynomirenkaan $R[x]$ nollasta eroavia alkioita. Oletetaan myös, että pq ei ole nollapolynomi. Tällöin on voimassa epäyhtälö*

$$\deg(pq) \leq \deg(p) + \deg(q).$$

Todistus. Merkitään $\deg(p) = n$ ja $\deg(q) = m$. Tarkastellaan polynomin pq astetta $k > n + m$ olevaa kerrointa. Polynomien kertolaskun määritelmän mukaan tämä kerroin on

$$\sum_{i=0}^{k} p_i q_{k-i}.$$

Tämä summan jokainen yhteenlaskettava on kuitenkin nolla, koska kun $i < n$, niin $q_{k-i} = 0$ ja kun taas $i \geq n$, niin $p_i = 0$. Polynomin pq aste on siis korkeintaan $n + m$. □

2.3 Polynomien jaollisuus

Polynomin aste ja sen tärkeimmät ominaisuudet on nyt käsitelty. Määrittellään seuraavaksi polynomien jaollisuus, joka mahdollistaa myös osamäärän ja jakojäännöksen määrittelyn samaan tapaan kuin kokonaisluvuille. Jaollisuuden määrittely myös vaatii sen, että polynomin kertoimet muodostavat renkaan sijasta kunnan, jolloin jokaiselle nollasta eroavalle kertoimelle löytyy käänteisalkio kertolaskun suhteen. Jatkossa kun puhutaan polynomirenkaasta $K[x]$ oletetaan, että rengas K on lisäksi kunta. Tämä polynomirengas ei kuitenkaan ole itsessään kunta, koska esimerkiksi polynomilla x ei ole siinä käänteisalkiota.

Määritelmä 2.14 (Jaollisuus)**.** Olkoot p ja $d \neq 0$ polynomirenkaan $K[x]$ polynomeja. Sanotaan, että polynomi d *jakaa* polynomin p, jos on olemassa sellainen polynomirenkaan $K[x]$ alkio q, että $p = qd$.

Kokonaislukujen jaollisuuteen liittyy läheisesti alkuluvun käsite. Polynomirenkaan tapauksessa tätä käsitettä vastaa jaoton polynomi, joka määritellään seuraavaksi.

Määritelmä 2.15 (Jaoton polynomi)**.** Olkoon p polynomirenkaan $K[x]$ alkio. Polynomia p sanotaan jaottomaksi, jos sitä ei voida esittää kahden vakiosta eroavan polynomin tulona.

Todistetaan seuraavaksi jakoyhtälö, joka takaa yksikäsitteisen osamäärän ja jakojäännöksen löytymisen silloin kun polynomi jaetaan nollasta eroavalla polynomilla.

Lause 2.16 (Jakoyhtälö)**.** *Olkoot p ja $d \neq 0$ polynomirenkaan $K[x]$ alkioita. Tällöin on olemassa sellaiset yksikäsitteiset polynomirenkaan $K[x]$ alkiot q ja r, että*

$$p = qd + r,$$

missä joko r on nollapolynomi tai $\deg(r) < \deg(d)$.

Todistus. Jos polynomi d jakaa polynomin p, niin väite seuraa suoraan jaollisuuden määritelmästä. Muulloin määritellään joukko

$$A = \{p - td \mid t \in K[x]\}.$$

Polynomien asteet ovat aina ei-negatiivisia kokonaislukuja, joten hyvän järjestyksen periaatteen nojalla joukossa A on polynomi s, jonka aste on pienin mahdollinen. Merkitään $\deg(s) = n$ ja $\deg(d) = m$. Tarkastellaan tilannetta, jossa $n \geq m$. Tällöin polynomi

$$s - s_n d_m^{-1} d\, x^{n-m}$$

on joukossa A ja sen aste on pienempi kuin polynomin s aste. On siis oltava $n < m$. Koska s on joukossa A, on olemassa sellainen polynomi t, että $p - td = s$. Nyt valinnat $q = t$ ja $r = s$ toteuttavat jakoyhtälön.

Olkoot parit (q, r) ja (q', r') kaksi ratkaisua jakoyhtälöön. Tällöin $(q - q')d = r' - r$. Polynomi d siis jakaa polynomin $r' - r$. Tämä on kuitenkin mahdollista vain kun $r' - r = 0$, koska muuten olisi voimassa epäyhtälö

$$\deg(d) \leq \deg((q - q')d) = \deg(r' - r) \leq \max\{\deg(r'), \deg(r)\} < \deg(d).$$

Tulon nollasäännön nojalla tällöin on oltava myös $q - q' = 0$. Jakoyhtälön ratkaisu on siis yksikäsitteinen. □

2.4 Polynomin juuret

Jokaista polynomia kohti on olemassa polynomikuvaus. Polynomikuvauksen avulla voidaan määritellä polynomin juuret sitä vastaavan polynomikuvauksen nollakohtina.

Määritelmä 2.17 (Polynomikuvaus)**.** Olkoon $p = (p_0, p_1, p_2, \ldots)$ polynomirenkaan $R[x]$ alkio. Määritellään *polynomikuvaus*

$$\tilde{p} : R \to R$$

sellaiseksi, että renkaan R alkio α kuvautuu renkaan R alkioksi

$$\sum_{n=0}^{\infty} p_n \alpha^n.$$

Määritelmä 2.18 (Juuret)**.** Olkoon p polynomirenkaan $R[x]$ alkio ja α renkaan R alkio. Tällöin α on polynomin p juuri, jos $\tilde{p}(\alpha) = 0$.

Polynomit jaetaan usein tekijöihin juurtensa avulla. Seuraava lause todistaa, että jos polynomilla on jokin juuri, niin kyseinen polynomi voidaan jakaa perusmuotoisella ensimmäisen asteen polynomilla, jonka ainoa juuri kyseinen juuri on.

Lause 2.19 (Juurten ja tekijöiden yhteys)**.** *Olkoon p polynomirenkaan $K[x]$ alkio. Kunnan K alkio α on polynomin p nollakohta, jos ja vain jos polynomi $x - \alpha$ jakaa polynomin p renkaassa $K[x]$.*

Todistus. Jos polynomi $x - \alpha$ jakaa polynomin p, niin on olemassa sellainen kunnan K polynomi q, että on voimassa $p = (x - \alpha)q$. Tällöin $\tilde{p}(\alpha) = (\alpha - \alpha)\tilde{q}(\alpha) = 0$.

Toisaalta jos α on polynomin p nollakohta, niin jakoyhtälön nojalla löytyy kunnan K polynomit q ja r jotka toteuttavat yhtälön

$$p = (x - \alpha)q + r,$$

jossa joko r on nollapolynomi tai

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

Tällöin r on vakiopolynomi. Koska $\tilde{p}(\alpha) = (\alpha - \alpha)\tilde{q}(\alpha) + \tilde{r}(\alpha) = \tilde{r}(\alpha) = 0$, niin r on nollapolynomi, jolloin polynomi $x - \alpha$ jakaa polynomin p. □

Samaan tapaan kuin kokonaisluvuilla, on myös polynomeilla yhteisiä tekijöitä. Kahden polynomin yhteinen tekijä jakaa ne molemmat. Lisäksi voidaan määritellä suurin yhteinen tekijä, joka on jaollinen kaikilla näiden polynomien yhteisillä tekijöillä.

Määritelmä 2.20 (Yhteinen tekijä)**.** Olkoot p ja q polynomirenkaan $K[x]$ alkioita. Polynomirenkaan $K[x]$ alkiota, joka jakaa sekä polynomin p että polynomin q, sanotaan niiden *yhteiseksi tekijäksi*.

Määritelmä 2.21 (Suurin yhteinen tekijä)**.** Olkoot p ja q polynomirenkaan $K[x]$ alkioita. Niiden yhteinen tekijä on suurin yhteinen tekijä, jos mielivaltainen polynomien p ja q yhteinen tekijä jakaa sen. Suurin yhteinen tekijä ei kuitenkaan ole nimestään huolimatta yksikäsitteinen. Nimittäin suurimman yhteisen tekijän kertominen millä tahansa polynomirenkaan $K[x]$ nollasta eroavalla vakiopolynomilla tuottaa toisen suurimman yhteisen tekijän. Polynomien p ja q perusmuotoista suurinta yhteistä tekijää merkitään $\mathrm{syt}\,(p, q)$.

Vaikka usein ajatellaan, että suurin yhteinen tekijä olisi yksikäsitteinen, niin näin ei kuitenkaan ole. Jo kokonaislukujenkin joukossa suurimman yhteisen tekijän vastaluku on myös suurin yhteinen tekijä. Perusmuotoinen suurin yhteinen tekijä on kuitenkin yksikäsitteinen.

Viimeisin suoraan polynomeihin liittyvä tulos on Bézout'n lemma, josta on hyötyä kun myöhemmin todistetaan, että yksinkertaisen kuntalaajennuksen mielivaltainen alkio on jonkin polynomifunktion arvo kyseisen kuntalaajennuksen virittävällä alkiolla.

Lause 2.22 (Bézout'n lemma)**.** *Olkoot a ja b polynomirenkaan $K[x]$ nollasta eroavia alkioita. Tällöin löytyy polynomirenkaan $K[x]$ alkiot p ja q, jotka toteuttavat yhtälön*

$$ap + bq = \mathrm{syt}\,(a, b)\,.$$

Todistus. Tarkastellaan joukkoa

$$S = \{ap + bq \mid p, q \in K\,[x]\}\,.$$

Joukko S ei ole tyhjä, koska valitsemalla $p = 1$ ja $q = 0$ voidaan todeta, että polynomi a on joukossa S. Hyvän järjestyksen periaatteen nojalla joukossa S on perusmuotoinen polynomi $d = as + bt$, jonka aste on pienin mahdollinen.

Polynomien jakoyhtälön nojalla on olemassa polynomit q ja r, jotka toteuttavat yhtälön

$$a = qd + r,$$

jossa joko r on nollapolynomi tai $\deg(r) < \deg(d)$. Tällöin polynomin

$$r = a - qd = a - qas - qbt = a(1 - qs) + b(-qt)$$

on oltava nollapolynomi, koska muuten polynomin d aste ei voisi olla pienin. Täten polynomi d jakaa polynomin a ja vastaavasti se jakaa myös polynomin b.

Olkoon c polynomien a ja b yhteinen tekijä, jolloin on olemassa polynomirenkaan $K[x]$ polynomit u ja v, jotka toteuttavat yhtälöt $a = cu$ ja $b = cv$.

Tällöin $d = as + bt = c(us + vw)$, joten polynomi c jakaa polynomin d, jolloin d on polynomien a ja b suurin yhteinen tekijä. Kun polynomit s, t ja d kerrotaan polynomin d johtavan kertoimen käänteisluvulla, saadaan uudet polynomit, jotka toteuttavat alkuperäisen yhtälön. □

3 KUNTALAAJENNUKSET

Kuntalaajennuksen idea on lisätä johonkin olemassa olevaan kuntaan uusia alkioita, jonka jälkeen saatua joukkoa täydennetään muilla alkioilla kunnes se on kunta. Esimerkiksi rationaalilukujen kuntaan voidaan lisätä $\sqrt{2}$. Jotta tästä joukosta saataisiin kunta, pitää lisätä kaikki reaaliluvut muotoa $a + b\sqrt{2}$, missä a ja b ovat rationaalilukuja. Tämän luvun teoria pohjautuu teokseen [4].

3.1 Kuntalaajennus

Aloitetaan kuntalaajennusten tarkastelu määrittelemällä kuntalaajennus ja joitakin sen tyyppejä.

Määritelmä 3.1. Olkoon kunta K kunnan L alikunta. Nämä kaksi kuntaa muodostavat yhdessä kuntalaajennuksen, jota merkitään L/K. Tässä yhteydessä kuntaa K kutsutaan *lähtökunnaksi* ja kuntaa L *laajennuskunnaksi*.

Esimerkki 3.2. Reaalilukujen kunta $\mathbb{R}$ on kompleksilukujen kunnan $\mathbb{C}$ alikunta, joten $\mathbb{C}/\mathbb{R}$ on kuntalaajennus, missä $\mathbb{R}$ on lähtökunta ja $\mathbb{C}$ on laajennuskunta.

Kuten jo aiemmin todettiin, kuntalaajennus muodostetaan usein lisäämällä johonkin lähtökuntaan uusia alkioita, jonka jälkeen saatu joukko täydennetään laajennuskunnaksi.

Määritelmä 3.3. Olkoon L/K kuntalaajennus ja A joukko kunnan L alkioita. Joukon A *virittämä* kunta, jota merkitään $K(A)$, on pienin kunnan L alikunta, joka sisältää joukon A. Joukkoa A kutsutaan *virittäjäjoukoksi*.

Koska kunta K on kunnan L alikunta, niin todetaan, että $K(A)$ on varmasti olemassa. Jos pienempää kaikki joukon A alkiot sisältävää kuntaa ei ole, niin päädytään uusia alkioita lisäämällä lopulta kuntaan L, joka sisältää jokaisen joukon A alkion.

Kuntalaajennuksen virittäjäjoukko A on usein äärellinen. Tällöin sen virittämää kuntaa voidaan merkitä $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, missä α_i ovat joukon A alkiot, kun $i = 1, 2, \ldots, n$. Erityisesti, jos joukossa A on vain yksi alkio α, niin sen virittämää kuntaa merkitään $K(\alpha)$. Yhden alkion virittämä kunta esiintyy niin usein, että siihen liittyvälle kuntalaajennukselle annetaan erikseen nimi.

Määritelmä 3.4 (Yksinkertainen kuntalaajennus)**.** Kuntalaajennusta L/K kutsutaan yksinkertaiseksi, jos on olemassa sellainen kunnan L alkio α, että $L = K(\alpha)$.

Esimerkki 3.5. Olkoon lähtökuntana rationaalilukujen kunta $\mathbb{Q}$. Tarkastellaan alkion $\sqrt{2}$ virittämää laajennuskuntaa $\mathbb{Q}(\sqrt{2})$. Tunnetusti alkio $\sqrt{2}$ ei ole rationaaliluku, joten kunta $\mathbb{Q}(\sqrt{2})$ sisältää rationaalilukujen lisäksi alkioita, jotka eivät ole rationaalilukuja. Mitkä kaikki alkiot kunta $\mathbb{Q}(\sqrt{2})$ sitten sisältää?

Kunnan on oltava suljettu siinä määritellyn yhteen- ja kertolaskun suhteen. Voidaankin siis todeta, että alkio $a + b\sqrt{2}$, missä a ja b ovat rationaalilukuja, löytyy kunnasta $\mathbb{Q}(\sqrt{2})$. Lisäksi jokaiselle alkioille on löydyttävä vasta-alkio yhteenlaskun suhteen ja jokaiselle nollasta eroavalle alkiolle käänteisalkio kertolaskun suhteen. Luvun $a + b\sqrt{2}$ vasta-alkio $-a - b\sqrt{2}$ on kuitenkin selvästi samaa muotoa. Myöskin jos molemmat luvuista a ja b eivät ole nollia, luvun $a + b\sqrt{2}$ käänteisluku

$$\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$

on myös tätä samaa muotoa. Tämä laajennuskunta voidaankin siis esittää muodossa

$$\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \right\}.$$

Todetaan vielä, että kuntalaajennus $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ on yksinkertainen, koska sen laajennuskunnan voi virittää yhdellä alkiolla sen lähtökunnasta.

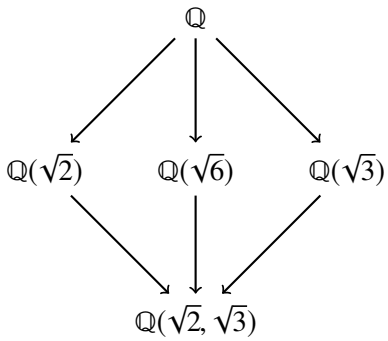
Lähtökunnan laajentamista ei tarvitse tehdä kerralla. Samaan tulokseen päästään kun laajennetaan ensin kunta K kunnaksi M ja sitten kunta M kunnaksi L. Itseasiassa jokainen kuntalaajennus voidaan esittää peräkkäisten yksinkertaisten kuntalaajennusten avulla. Tämä on erittäin hyödyllinen ominaisuus, koska se mahdollistaa todistusten rakentamisen matemaattisen induktioperiaatteen kautta.

Määritelmä 3.6. Olkoon L/K kuntalaajennus. Jos myös L/M ja M/L ovat kuntalaajennuksia, niin kuntaa M sanotaan kuntalaajennuksen L/K *välikunnaksi*.

Esimerkki 3.7. Valitaan lähtökunnaksi rationaalilukujen kunta $\mathbb{Q}$ ja tarkastellaan alkioiden $\sqrt{2}$ ja $\sqrt{3}$ virittämää laajennuskuntaa $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Yritetään esittää laajennuskunnan alkiot samaan tapaan kuin esimerkissä, jossa tarkasteltiin kuntaa $\mathbb{Q}(\sqrt{2})$. Ensimmäinen mieleen tuleva arvaus tälle esitykselle on $a + b\sqrt{2} + c\sqrt{3}$, missä alkiot a, b ja c ovat rationaalilukuja. Tämä ei kuitenkaan riitä, koska esimerkiksi lukua $\sqrt{2}\sqrt{3} = \sqrt{6}$ ei voida esittää tässä muodossa. Alkio $\sqrt{6}$ täytyy siis ottaa vielä tähän esitykseen mukaan.

Selvästi kaikki alkiot $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, missä alkiot a, b, c ja d ovat rationaalilukuja, sisältyvät tähän laajennuskuntaan ja itseasiassa muodostavat tämän laajennuskunnan kokonaan. Nämä kaikki alkiot voitaisiin kuitenkin esittää myös muodossa $(a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3}$.

Kunta $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ oltaisiin siis voitu muodostaa laajentamalla lähtökunta $\mathbb{Q}$ ensin kunnaksi $\mathbb{Q}(\sqrt{2})$ virittävän alkion $\sqrt{2}$ avulla ja sen jälkeen kunnaksi $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ virittävän alkion $\sqrt{3}$ avulla. Toisaalta oltaisiin voitu myös lähteä laajentamaan lähtökuntaa ensin alkiolla $\sqrt{3}$ tai $\sqrt{6}$. Havainnollistetaan näiden kuntalaajennusten välisiä suhteita seuraavalla kuvalla



Edellisestä kuvasta nähdään, että lähtiessä rakentamaan kuntaa $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ virittävä alkio kerrallaan, voidaan edetä kolmea eri reittiä pitkin ja päätyä silti samaan lopputulokseen. Vaikka virittäviä alkioita olivatkin vain $\sqrt{2}$ ja $\sqrt{3}$, on kuvaan silti otettu mukaan alkion $\sqrt{6}$ virittämä kunta. Tämä johtuu siitä, että kunnat $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{6})$ ja $\mathbb{Q}(\sqrt{3}, \sqrt{6})$ ovat kaikki itseasiassa täysin sama kunta. Kolmatta näistä alkioista ei tarvitse ottaa mukaan erikseen, koska se saadaan kertomalla kahden muun tulo sopivalla rationaaliluvulla.

Polynomit ja kuntalaajennukset liittyvät läheisesti toisiinsa. Usein lähtökuntaan K halutaan lisätä, jonkin sen polynomirenkaan $K[x]$ alkion juuret. Määritellään seuraavaksi tähän liittyvä algebrallisuuden käsite.

Määritelmä 3.8. Olkoon α kunnan K alkio. Alkiota α sanotaan *algebralliseksi* kunnan K suhteen, jos on olemassa sellainen polynomirenkaan $K[x]$ nollasta eroava alkio p, jonka nollakohta α on.

Määritelmä 3.9. Kuntalaajennusta L/K sanotaan algebralliseksi, jos kaikki kunnan L alkiot ovat algebrallisia kunnan K suhteen.

Jokaiselle algebralliselle alkioille löytyy yksikäsitteinen pienintä mahdollista astetta oleva perusmuotoinen polynomi, jonka kertoimet ovat lähtökunnan alkioita ja jonka juuri kyseinen alkio on. Tätä polynomia kutsutaan kyseisen alkion minimaalipolynomiksi.

Määritelmä 3.10. Olkoon L/K kuntalaajennus ja olkoon kunnan L alkio α algebrallinen kunnan K suhteen. Alkion α minimaalipolynomi m_α on pienintä mahdollista astetta oleva perusmuotoinen kunnan K polynomi, jonka juuri α on.

Minimaalipolynomilla on monia ominaisuuksia. Yksi näistä on se, että se tietyn alkion minimaalipolynomi jakaa kaikki polynomit, joiden juuri kyseinen alkio on. Tämä todistetaan seuraavaksi.

Lause 3.11. *Olkoon L/K kuntalaajennus ja olkoon kunnan L alkio α algebrallinen kunnan K suhteen. Tällöin alkion α minimaalipolynomi m_α jakaa polynomin p, jos α on polynomin p nollakohta.*

Todistus. Polynomien jakoyhtälön nojalla on olemassa sellaiset polynomit q ja r, että

$$p = qm_\alpha + r,$$

jossa joko r on nollapolynomi tai $\deg(r) < \deg(m_\alpha)$. Tällöin jakoyhtälössä esiintyviä polynomeja vastaaville polynomikuvauksille on voimassa yhtälö

$$\tilde{p}(\alpha) = \tilde{q}(\alpha)\tilde{m}_\alpha(\alpha) + \tilde{r}(\alpha).$$

Koska α on minimaalipolynominsa nollakohta, niin $\tilde{r}(\alpha) = 0$. Jos r ei ole nollapolynomi, voidaan se kertoa johtavan terminsä käänteisluvulla, jolloin saatu polynomi on minimaalipolynomia m_α pienempiasteinen perusmuotoinen polynomi, jonka nollakohta α on. Täten siis r on nollapolynomi, jolloin m_α jakaa polynomin p. □

Todistetaan seuraavaksi, että tämä yksikäsitteinen minimaalipolynomi on todella olemassa.

Lause 3.12. *Olkoon L/K kuntalaajennus ja olkoon kunnan L alkio α algebrallinen kunnan K suhteen. Alkiolla α on yksikäsitteinen minimaalipolynomi.*

Todistus. Alkio α on algebrallinen kunnan K suhteen, joten se on polynomirenkaan $K[x]$ nollasta eroavan polynomin m nollakohta. Olkoon polynomin m johtava kerroin a. Tällöin $a^{-1}m$ on perusmuotoinen. Tällaisista perusmuotoisista polynomeista voidaan valita pienintä mahdollista astetta oleva, jolloin valittu polynomi on alkion α minimaalipolynomi.

Olkoot m ja n alkion α minimaalipolynomeja. Tällöin polynomien jaollisuuden ja lauseen 3.11 nojalla on olemassa sellaiset polynomit p ja q, että $m = pn$ ja $n = qm$. Edellisestä seuraa, että $m = pqm$, jolloin $(1 - pq)m = 0$. Minimaalipolynomi ei voi olla nollapolynomi, joten tulon nollasäännön nojalla $pq = 1$. Polynomit p ja q ovat siis vakiopolynomeja ja koska m ja n ovat minimaalipolynomeina perusmuotoisia, on oltava $p = q = 1$, jolloin $m = n$. Täten alkion minimaalipolynomi on yksikäsitteinen. □

Todistetaan seuraavaksi, että alkion α minimaalipolynomi m_α on ainoa perusmuotoinen jaoton polynomi, jonka juuri tämä kyseinen alkio on.

Lause 3.13. *Alkion α minimaalipolynomi m_α on jaoton.*

Todistus. Olkoot p ja q sellaisia polynomeja, että $m_\alpha = pq$. Tällöin tulon nollasäännön nojalla joko $\tilde{p}(\alpha) = 0$ tai $\tilde{q}(\alpha) = 0$. Symmetrian nojalla voidaan valita $\tilde{p}(\alpha) = 0$. Tällöin lauseen 3.11 nojalla on olemassa sellainen polynomi a, että $p = am_\alpha$. Nyt on voimassa $m_\alpha = m_\alpha aq$, jolloin polynomien a ja q on oltava vakiopolynomeja. Täten m_α on siis jaoton. □

Lause 3.14. *Olkoon L/K kuntalaajennus. Olkoon p polynomirenkaan $K[x]$ perusmuotoinen jaoton polynomi. Olkoon kunnan L alkio α on algebrallinen kunnan K suhteen ja olkoon α polynomin p nollakohta. Tällöin p on alkion α minimaalipolynomi.*

Todistus. Olkoon m_α alkion α minimaalipolynomi. Tällöin lauseen 3.11 nojalla on olemassa sellainen polynomi q, että $p = qm_\alpha$. Koska p on jaoton ja perusmuotoinen, on oltava $q = 1$, jolloin $p = m$. □

Seuraava apulause todistaa, että kun kuntaa laajennetaan jollakin alkiolla, niin kaikki laajennuskunnan alkiot voidaan esittää sijoittamalla tämä kyseinen alkio kahden alkuperäisen kunnan polynomifunktion osamäärään. Sen avulla todistetaan vielä vahvempi lause, jonka mukaan kaikki alkiot voidaan esittää sijoittamalla tämä virittävä alkio johonkin alkuperäisen kunnan polynomifunktioon.

Apulause 3.15. *Olkoon L/K kuntalaajennus ja α kunnan L alkio. Tällöin kunnan $K(\alpha)$ jokaista alkiota k kohti on olemassa sellaiset polynomirenkaan $K[x]$ polynomit p ja q, että $x = \tilde{p}(\alpha)\tilde{q}(\alpha)^{-1}$.*

Todistus. Olkoon M kunnan L osajoukko joka koostuu alkioista $\tilde{p}(\alpha)\tilde{q}(\alpha)^{-1}$. Voidaan valita $p = q = 1$, joten joukossa M on jokin muukin alkio kuin kunnan L nolla-alkio. Jos tulo $\tilde{p}(\alpha)\tilde{q}(\alpha)^{-1}$ ei ole nolla, niin sen käänteisalkio $\tilde{q}(\alpha)\tilde{p}(\alpha)^{-1}$ ei ole myöskään nolla, jolloin se on joukossa M eli jokaisella joukon M alkiolla on käänteisalkio. Valitaan joukon M alkiot

$$\tilde{p}(\alpha)\tilde{q}(\alpha)^{-1} \quad \text{ja} \quad \tilde{p'}(\alpha)\tilde{q'}(\alpha)^{-1}.$$

Selvästi niiden erotus ja tulo

$$\left(\tilde{p}(\alpha)\tilde{q'}(\alpha) - \tilde{p'}(\alpha)\tilde{q}(\alpha)\right)\tilde{q}(\alpha)^{-1}\tilde{q'}(\alpha)^{-1}, \quad \tilde{p}(\alpha)\tilde{p'}(\alpha)\tilde{q}(\alpha)^{-1}\tilde{q'}(\alpha)^{-1}$$

ovat myös joukon M alkioita.

Joukko M on siis kunta. Jokainen kunnan K alkio k' on kunnassa M, koska voidaan valita $p = k'$ ja $q = 1$. Lisäksi myös α on kunnassa M, koska voidaan valita $p = k$ ja $q = 1$. Mutta L on pienin kunnan K laajennus joka sisältää alkion α, jolloin $M = L$. □

Lause 3.16. *Olkoon L/K kuntalaajennus ja α kunnan L alkio. Tällöin jokaista kunnan $K(\alpha)$ alkiota k kohti on olemassa yksikäsitteinen polynomirenkaan $K[x]$ polynomi p, jonka aste on pienempi kuin alkion α minimaalipolynomin aste ja jonka polynomikuvaus $\tilde{p}$ kuvaa alkioksi k eli $\tilde{p}(\alpha) = k$.*

Todistus. Olkoon S niiden kunnan $K(\alpha)$ alkioiden k joukko, jotka voidaan esittää muodossa

$$k = \tilde{p}(\alpha),$$

jossa p on nollapolynomi tai $\deg(p) < \deg(m_\alpha)$. Joukko S ei ole tyhjä, koska α ja kaikki kunnan K alkiot kuuluvat siihen. Olkoot $\tilde{p}(\alpha)$ ja $\tilde{q}(\alpha)$ joukon S alkioita. Jos $\tilde{p}(\alpha) = 0$ tai $\tilde{q}(\alpha) = 0$ niin alkiot $\tilde{p}(\alpha) - \tilde{q}(\alpha) = (\tilde{p} - \tilde{q})(\alpha)$ ja $\tilde{p}(\alpha)\tilde{q}(\alpha) = (\tilde{pq})(\alpha)$ ovat selvästi myös joukossa S. Muussa tapauksessa polynomin $p - q$ aste on pienempi kuin polynomin m_α aste, jolloin alkio $\tilde{p}(\alpha) - \tilde{q}(\alpha) = (\tilde{p} - \tilde{q})(\alpha)$ kuuluu myös joukkoon S. Polynomien jakoyhtälön nojalla on olemassa sellaiset polynomit a ja b, että

$$pq = m_\alpha b + a,$$

jossa joko a on nollapolynomi tai $\deg(a) < \deg(m_\alpha)$. Tällöin alkio $\tilde{p}(\alpha)\tilde{q}(\alpha) = (\tilde{pq})(\alpha) = \tilde{a}(\alpha)$ kuuluu myös joukkoon S. Lauseen 3.13 nojalla m_α on jaoton, joten $\mathrm{syt}(p, m_\alpha) = 1$, jolloin lauseen Bézout'n lemman nojalla on olemassa sellaiset kunnan K polynomit a ja b, että $pa + m_\alpha b = 1$. Tällöin

$\tilde{a}(\alpha) = \tilde{p}(\alpha)^{-1}$, joten alkion $\tilde{p}(\alpha)$ käänteisalkio on joukossa S. Joukko S on täten kunnan $K(\alpha)$ alikunta, mutta koska α kuuluu siihen, niin $S = K(\alpha)$. □

3.2 Kuntalaajennuksen aste

Määritellään seuraavaksi kuntalaajennukselle aste, jonka avulla voidaan arvioida kuinka suuri laajennettu kunta on suhteessa alkuperäiseen kuntaan. Lineaarialgebrassa vektoriavaruudelle on määritelty dimensio, joka on kyseisen vektoriavaruuden kantavektorien lukumäärä. Valitaan vektoriavaruuden vektorien joukoksi kuntalaajennuksen laajennuskunta ja skalaarien joukoksi sen lähtökunta. Tällöin kuntalaajennuksen virittävien alkioiden avulla voidaan muodostaa tälle vektoriavaruudelle kanta, jonka koko kertoo vektoriavaruuden dimension. Vektoriavaruuden määritelmä löytyy lähteestä [4, s. 159].

Määritelmä 3.17. Kuntalaajennuksen L/K aste on sama kuin K-vektoriavaruuden L dimensio ja sitä merkitään $[L : K]$. Kuntalaajennusta sanotaan äärelliseksi, jos sen aste on äärellinen.

Tässä tutkielmassa käsitellään vain äärellisiä kuntalaajennuksia. Kuntalaajennuksen aste voi kuitenkin myös olla ääretön ja Galois'n teoriaa voidaan rakentaa myös äärettömässäkin tapauksessa [1].

Lause 3.18. *Olkoot L/K, L/M ja M/K äärellisiä kuntalaajennuksia. Tällöin*

$$[L : K] = [L : M]\,[M : K]\,.$$

Todistus. Olkoon $A = \{a_1, a_2, \ldots, a_n\}$ K-vektoriavaruuden M kanta ja olkoon $B = \{b_1, b_2, \ldots, b_m\}$ M-vektoriavaruuden L kanta. Jokainen vektoriavaruuden L alkio x voidaan esittää muodossa

$$x = \sum_{i=1}^{m} \lambda_i b_i.$$

Toisaalta jokainen λ_i on vektoriavaruuden M alkio, joten se voidaan esittää muodossa

$$\lambda_i = \sum_{j=1}^{n} \mu_{ji} a_j.$$

Tällöin

$$x = \sum_{j=1}^{n} \sum_{i=1}^{m} \mu_{ji} a_j b_i,$$

joten K-vektoriavaruuden L alkiot voidaan esittää vektorien $a_j b_i$ lineaarikombinaationa, joten kyseiset vektorit virittävät vektoriavaruuden L. Koska B on kanta, yhtälö

$$\sum_{i=1}^{m} \lambda_i b_i = 0$$

on voimassa vain jos jokainen $\lambda_i = 0, \quad i = 1, 2, \ldots, m$. Toisaalta

$$\lambda_i = \sum_{j=1}^{n} \mu_{ji} a_j = 0$$

on voimassa vain jos $\mu_{ji} = 0, \quad j = 1, 2, \ldots, n$. Täten siis

$$\sum_{j=1}^{n} \sum_{i=1}^{m} \mu_{ji} a_j b_i = 0$$

vain jos $\mu_{ji} = 0, \quad j = 1, 2, \ldots, n, \quad i = 1, 2, \ldots, m$.

Vektoriavaruuden L virittäjävektorit $a_j b_i$ ovat siis lineaarisesti riippumattomia, joten ne muodostavat kannan, jolloin K-vektoriavaruuden L dimension on nm. □

Todistetaan vielä yksinkertaisen kuntalaajennuksen asteen ja sen virittävän alkion minimaalipolynomin asteen välinen yhteys. Nimittäin alkion minimaalipolynomin aste on sama kuin sen virittämän yksinkertaisen kuntalaajennuksen aste.

Lause 3.19. *Olkoon $K(\alpha)/K$ kuntalaajennus ja m_α alkion α minimaalipolynomi. Tällöin*

$$[K(\alpha) : K] = \deg(m_\alpha).$$

Todistus. Lauseen 3.16 nojalla jokaista kunnan $K(\alpha)$ alkiota k kohti on olemassa kunnan K polynomi p, joka toteuttaa yhtälön $k = \tilde{p}(\alpha)$, jossa joko p on nollapolynomi tai $\deg(p) < \deg(m_\alpha)$. Jokainen K-vektoriavaruuden $K(\alpha)$ alkio voidaan siis ilmaista sen alkioiden $1, \alpha, \alpha^2, \ldots, \alpha^n$ lineaarikombinaationa, missä $n = \deg(m_\alpha) - 1$. Toisaalta α voi olla polynomin p nollakohta vain jos p on nollapolynomi, joten nämä vektorit ovat lineaarisesti riippumattomia. □

Kun lähtökuntaa laajennetaan jonkin polynomin juurilla, voidaan rakennetusta laajennuskunnasta päätellä monia asioita pelkästään tämän polynomin pohjalta. Polynomin juuria ei siis välttämättä tarvitse tietää laajennuskunnan tarkastelemiseksi. Tämä on keskeinen idea seuraavassa luvussa. Lähteestä [4] löytyvä todistus viidennen asteen yhtälön ratkaisukaavan mahdottomuudelle perustuu juurikin siihen, että kaikilla juurilausekkeista koostuvilla virittäjäjoukoilla on tietty ominaisuus, jota jokaisen viidennen asteen polynomin juurten muodostamalla joukolla ei ole, jolloin päätellään, että kaikkien viidennen asteen polynomien juuria ei voida esittää juurilausekkeina.

4 GALOIS'N TEORIAA

Tarvittavat pohjatiedot polynomien ja kuntalaajennusten teoriasta esitettiin edeltävissä luvuissa ja nyt siirrytään itse Galois'n teoriaan. Polynomin määritelmä aivan luvun 2 alussa pohjautuu sen esitykseen jonona jonkin renkaan alkioita ja saman luvun lopussa todettiin polynomin nollakohtien yhteys siihen miten polynomi jakautuu tekijöiksi pienempi asteisten polynomien tulona. Galois'n teorian pääidea onkin, että polynomia voidaan tarkastella termiensä kertoimien sijaan myös sen juurien kautta. Tässä luvussa käytetään myös ryhmiä ja niiden perusominaisuuksia, kuten ryhmän kokoa, jotka löytyvät esimerkiksi lähteestä [2]. Itse Galois'n teoria pohjautuu teokseen [4].

4.1 Automorfismit

Määritelmä 4.1 (K-automorfismi)**.** Olkoon L/K kuntalaajennus. Isomorfismi $f : L \to L$ on *K-automorfismi* kunnassa L, jos kunnan K alkiot k toteuttavat yhtälön

$$f(k) = k.$$

Näiden K-automorfismien muodostamaa ryhmää merkitään $\mathrm{Aut}\,(L/K)$. Isomorfismi f on siis K-automorfismi, jos se kiinnittää kunnan K alkiot.

Todistetaan seuraavaksi, että nämä automorfismit permutoivat minimaalipolynomin juuret eli kuvaavat polynomin juuren joksikin saman polynomin juureksi.

Lause 4.2. *Olkoon L/K algebrallinen kuntalaajennus ja α kunnan L alkio. Olkoon α' jokin alkion α minimaalipolynomin m_α juuri. Tällöin on olemassa yksikäsitteinen K-automorfismi*

$$\varphi : K(\alpha) \to K(\alpha'),$$

joka toteuttaa yhtälön $\varphi(\alpha) = \alpha'$.

Todistus. Olkoon φ homomorfismi, joka kiinnittää kunnan K alkiot ja joka toteuttaa yhtälön

$$\varphi(\alpha) = \alpha'.$$

Riittää osoittaa, että φ injektio, koska sen määrittely- ja maalijoukko ovat samat. Kuvaus φ on homomorfismi, joten kaikilla kunnan K polynomeilla p on voimassa $\varphi(\tilde{p}(\alpha)) = \tilde{p}(\alpha')$. Lauseen 3.16 nojalla jokaista kunnan $K(\alpha)$ alkiota β kohti löytyy yksikäsitteinen polynomi q, jonka aste on

pienempi kuin minimaalipolynomin m_α aste ja joka toteuttaa yhtälön $\tilde{q}(\alpha) = \beta$. Nyt jos on voimassa $\varphi(\beta_1) = \varphi(\beta_2)$, niin $\varphi(\beta_1 - \beta_2) = 0$. Tällöin löytyy kunnan K polynomi r joka toteuttaa yhtälön $\beta = \beta_1 - \beta_2 = \tilde{r}(\alpha)$ ja jonka aste on pienempi kuin alkion α minimaalipolynomin aste. On kuitenkin oltava $\varphi(\beta_1 - \beta_2) = \varphi(\tilde{r}(\alpha)) = \tilde{r}(\alpha') = 0$. Polynomin r on siis oltava nollapolynomi, jolloin $\beta_1 = \beta_2$. Annetut ehdot määrittelevät kuvauksen φ, joten se on myös yksikäsitteinen. □

4.2 Hajotuskunta

Lopuksi todistettavassa Galois'n teorian päälauseen heikennetyssä versiossa tarkastellaan kuntalaajennuksen automorfismien muodostaman ryhmän ja kuntalaajennuksen virittävien alkioiden peräkkäisten yksinkertaisten kuntalaajennuksen muodostaman rakenteen yhteyttä. Nämä virittävät alkiot ovat usein jonkin alkuperäisen kunnan polynomin juuret. Kun kaikki nämä juuret on lisätty kuntaan, jakautuu tämä polynomi tekijöihinsä kyseisessä kunnassa.

Määritelmä 4.3 (Polynomin hajoaminen)**.** Olkoon p polynomirenkaan $K[x]$ alkio. Sanotaan, että p *hajoaa* kunnassa K, jos se voidaan esittää muodossa

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

missä $\alpha_1, \ldots, \alpha_n$ ja k ovat kunnan K alkioita.

Määritelmä 4.4 (Hajotuskunta)**.** Olkoon p kunnan K polynomi. Pienintä kuntaa, jossa p hajoaa, sanotaan polynomin p *hajotuskunnaksi*.

Lause 4.5. *Olkoon $p = (p_0, p_1, p_2, \ldots)$ polynomirenkaan $K[x]$ alkio ja olkoon kunta L polynomin p hajotuskunta kunnan K suhteen. Olkoot lisäksi α jokin polynomin p juuri. Jos σ on K-automorfismi kunnassa L niin $\sigma(\alpha)$ on myös polynomin p juuri.*

Todistus. Olkoon α jokin polynomin p juurista. Tällöin

$$\tilde{p}(\alpha) = \sum_{k=0}^{\infty} p_k \alpha^k = 0.$$

Koska σ on K-automorfismi, niin

$$\sigma(\tilde{p}(\alpha)) = \sum_{k=0}^{\infty} p_k \sigma(\alpha)^k = 0.$$

Mutta tällöin alkio $\sigma(\alpha)$ on polynomin p juuri. □

Edellinen lause kertoo, että K-automorfismit polynomin hajotuskunnassa permutoivat sen juuret jollakin tavalla. Tätä ominaisuutta voidaan käyttää hyödyksi polynomin hajotuskunnan suhteen muodostetun kuntalaajennuksen Galois'n ryhmän selvittämisessä. Galois'n ryhmät esitellään seuraavaksi.

4.3 Galois'n ryhmät

Automorfismin määritelmässä esiintyvältä kuntalaajennukselta vaaditaan muutamia lisäominaisuuksia, jotta niiden muodostama ryhmä olisi Galois'n ryhmä.

Määritelmä 4.6 (Normaali laajennus)**.** Sanotaan, että kuntalaajennus L/K on *normaali*, jos jokainen kunnan K jaoton polynomi, jolla on nollakohta kunnassa L, hajoaa kunnassa L. Normaalin laajennuksen idea siis on, että polynomi jakautuu joko kokonaan tekijöihinsä tai ei ollenkaan.

Kuntaa ei haluta laajentaa useampaan kertaan samalla alkiolla, koska jo olemassa olevan alkion liittäminen kuntaan ei muuta sitä mitenkään ja on siksi aivan turhaa. Seuraavaksi määriteltävällä separoituvuudella taataan, että polynomilla ei ole samaa juurta kahdesti, jolloin virittäessä kuntalaajennusta polynomin juurten pohjalta ei tehdä ylimääräistä työtä.

Määritelmä 4.7 (Separoituvuus)**.** Olkoon p polynomirenkaan $K[x]$ jaoton polynomi ja olkoon Σ polynomin p hajotuskunta. Polynomia p sanotaan separoituvaksi, jos se voidaan esittää muodossa

$$p = k\,(x - \sigma_1) \cdots (x - \sigma_n),$$

missä k on kunnan K alkio ja $\sigma_1, \ldots, \sigma_n$ kunnan Σ eri alkioita.

Määritelmä 4.8 (Separoituva laajennus)**.** Algebrallista kuntalaajennusta L/K sanotaan separoituvaksi, jos kunnan K mielivaltaisen alkion α minimaalipolynomi m_α on separoituva.

Kootaan äärellisyys, normaalius ja separoituvuus yhden käsitteen alle Galois'n laajennukseksi. Galois'n laajennuksen automorfismien muodostamaa ryhmää kutsutaan Galois'n ryhmäksi. Näiden määritelmien avulla voidaan todistaa heikennetty versio Galois'n teorian päälauseesta joka esittää, että Galois'n laajennuksen aste on sama kuin sen Galois'n ryhmän koko.

Määritelmä 4.9 (Galois'n laajennus)**.** Jos kuntalaajennus on äärellinen, normaali ja separoituva sitä sanotaan Galois'n laajennukseksi.

Määritelmä 4.10 (Galois'n ryhmä)**.** Olkoon L/K Galois'n laajennus. Tällöin sen K-automorfismien muodostamaa ryhmää $\mathrm{Aut}\,(L/K)$ sanotaan *Galois'n ryhmäksi* ja sitä merkitään $\mathrm{Gal}\,(L/K)$.

Esimerkki 4.11. Olkoon L polynomin $x^2 - 2$ hajotuskunta. Määritetään kuntalaajennuksen $L/\mathbb{Q}$ Galois'n ryhmä.

Polynomin $x^2 - 2$ juuret ovat $\pm\sqrt{2}$, jolloin polynomin $x^2 - 2$ hajotuskunta on $\mathbb{Q}(\sqrt{2})$. Esimerkissä 3.5 todettiin, että kaikki kunnan $\mathbb{Q}(\sqrt{2})$ alkiot voidaan esittää muodossa $a + b\sqrt{2}$, missä a ja b ovat rationaalilukuja.

Galois'n ryhmä koostuu $\mathbb{Q}$-automorfismeista, jotka lauseen 4.5 nojalla permutoivat polynomin $x^2 - 2$ juuret eli jos f on $\mathbb{Q}$-automorfismi niin $f(\sqrt{2}) = \sqrt{2}$ tai $f(\sqrt{2}) = -\sqrt{2}$. Koska automorfismit ovat homomorfismeja niin tapauksessa $f(\sqrt{2}) = \sqrt{2}$ kunnan $\mathbb{Q}(\sqrt{2})$ alkiolle $a + b\sqrt{2}$ on voimassa

$$f(a + b\sqrt{2}) = a + b\sqrt{2},$$

jolloin f siis on identiteettikuvaus. Jos taas $f(\sqrt{2}) = -\sqrt{2}$, niin

$$f(a + b\sqrt{2}) = a - b\sqrt{2}.$$

Molempia juurten permutaatiota vastaa siis yksikäsitteinen $\mathbb{Q}$-automorfismi, joten $\mathrm{Gal}(L/\mathbb{Q})$ on kahden alkion ryhmä.

Todistetaan lopuksi heikennetty versio Galois'n teorian päälauseesta, joka antaa pintaraapaisun Galois'n teorian luomasta yhteydestä kunta- ja ryhmäteorian välille.

Lause 4.12. *Olkoon L/K Galois'n laajennus. Tällöin sen aste $[L : K]$ on sama kuin sen Galois'n ryhmän $\mathrm{Gal}(L/K)$ koko.*

Todistus. Jos aste $[L : K] = 1$, niin $L = K$, jolloin on täsmälleen yksi K-automorfismi. Muulloin on olemassa kuntaan K kuulumaton kunnan L alkio α. Koska Galois'n laajennus L/K on algebrallinen, on alkiolla α minimaalipolynomi m_α. Minimaalipolynomin juuret α' eivät kuulu kuntaan K, joten separoituvuuden nojalla $\deg(m_\alpha) > 1$. Tällöin lauseiden 3.18 ja 3.19 nojalla

$$[L : K(\alpha')] = \frac{[L : K]}{[K(\alpha') : K]} < [L : K].$$

Kuntalaajennus $L/K(\alpha')$ toteuttaa edelleen Galois'n laajennuksen ehdot, joten siis

$$[L : K(\alpha')] = |\mathrm{Gal}(L/K(\alpha'))|.$$

Koska kuntalaajennus L/K on normaali ja separoituva, kunta $K(\alpha)$ on alkion α minimaalipolynomin hajotuskunta ja minimaalipolynomin juuret ovat erillisiä. Lauseen 4.2 nojalla jokaista minimaalipolynomin m_α juurta α' kohti on olemassa täsmälleen yksi K-automorfismi, joten niitä on vähintään $[K(\alpha') : K] = \deg(m_\alpha)$ kappaletta. Lauseen 4.5 nojalla jokainen K-automorfismi kuitenkin permutoi minimaalipolynomin juuret, joten niitä ei voi olla yhtään enempää. Siispä jokaista permutaatiota kohti on yksikäsitteinen K-automorfismi lauseen 4.2 mukaan.

Kaikki ryhmän $\mathrm{Gal}(L/K)$ alkiot voidaan muodostaa valitsemalla yksi automorfismi sekä ryhmästä $\mathrm{Gal}(L/K(\alpha'))$, että ryhmästä $\mathrm{Gal}(K(\alpha')/K)$. Siispä kuntalaajennuksen L/K Galois'n ryhmän koko voidaan esittää tulona

$$|\mathrm{Gal}(L/K)| = |\mathrm{Gal}(L/K(\alpha'))|\,|\mathrm{Gal}(K(\alpha')/K)|.$$

Koska kuntalaajennuksen $L/K(\alpha')$ aste ja kuntalaajennuksen $K(\alpha')/K$ aste ovat pienempiä kuin kuntalaajennuksen L/K aste, voidaan niiden Galois'n ryhmien koot esittää vastaavien vektoriavaruuksien dimensiona, jolloin

$$|\mathrm{Gal}(L/K)| = [L : K(\alpha')]\,[K(\alpha') : K].$$

Lopulta lauseen 3.18 nojalla seuraa, että

$$|\mathrm{Gal}\,(L/K)| = [L : K]\,.$$

□

Esimerkki 4.13. Esimerkin 4.11 Galois'n ryhmän koko voitaisiin laskea lauseen 4.12 avulla. Polynomi x^2-2, jonka aste on kaksi, on nimittäin alkion $\sqrt{2}$ minimaalipolynomi. Alkion minimaalipolynomin aste on sama kuin sen virittämän kuntalaajennuksen aste. Koska polynomi x^2-2 on separoituva ja hajoaa kunnassa $\mathbb{Q}(\sqrt{2})$, voidaan lauseen 4.12 nojalla todeta, että kyseisen kuntalaajennuksen Galois'n ryhmän koko on sama kuin kyseisen kuntalaajennuksen aste eli kaksi.

Lauseen 4.12 avulla huomataan, että tietyn tyyppisillä kuntalaajennuksilla (Galois'n laajennuksilla) on yhteys kuntaan lisättävien alkioiden muodostamiin polynomeihin ja edelleen näiden polynomien juurten permutaatioihin. Polynomia vastaavan Galois'n laajennuksen Galois'n ryhmän avulla voidaan saada hyödyllistä tietoa polynomin juurista. Esimerkiksi polynomin x^5-4x+2 juurten permutaatioiden muodostama ryhmä ei vastaa mitään algebrallisten lukujen virittämää kuntalaajennusta, joten viidennestä asteesta eteenpäin ei voi olla pelkästään niiden avulla muodostettua yleistä ratkaisukaavaa [4, s. 216]. Peruslaskutoimitukset ja juurilausekkeet eivät siis mahdollista yleistä ratkaisukaavaa.

Todellisuudessa Galois'n laajennuksen ja sen Galois'n ryhmän välinen yhteys on syvempi kuin mitä lause 4.12 antaa ilmi. Galois'n ryhmän kaikkien aliryhmien koot ovat myös samoja kuin niitä vastaavien Galois'n laajennusten virittävien alkioiden osajoukkojen virittämät laajennukset. Tämä tutkielma on vasta raapaissut pintaa Galois'n teoriasta todistamalla heikennetyn version Galois'n teorian päälauseesta, joka löytyy kaikessa loistossaan esimerkiksi teoksista [3] ja [4].

5 YHTEENVETO

Ensimmäisessä luvussa määriteltiin polynomiin liittyviä peruskäsitteitä yleisessä kunnassa ja määriteltiin ja todistettiin joitakin niiden ominaisuuksia, kuten polynomien yhteen- ja kertolasku, polynomin asteen käyttäytyminen näissä operaatioissa ja jakoyhtälö.

Kun tarvittava pohja oli luotu, päästiin esittelemään kuntalaajennukset. Kuntaa voidaan laajentaa lisäämällä siihen uusia alkiota. Usein kuntaa halutaan laajentaa lisäämällä siihen jonkin polynomin juuret, jolloin kyseessä on algebrallinen kuntalaajennus. Algebrallisille alkioille voidaan määritellä yksikäsitteinen minimaalipolynomi, joka on pienintä mahdollista astetta oleva perusmuotoinen polynomi, jonka juuri tämä alkio on. Lopuksi määriteltiin kuntalaajennuksen aste sitä vastaavan vektoriavaruuden dimension kautta ja huomattiin, että kaikki alkion virittämän laajennetun kunnan alkiot voidaan esittää alkuperäisen kunnan polynomifunktion arvoina, kun polynomifunktioon sijoitetaan tämä virittävä alkio.

Viimeisessä luvussa päästiin Galois'n teorian alkeisiin. Ensin määriteltiin kunnan automorfismit ja todistettiin, että alkion minimaalipolynomin eri juurten virittämät kunnat ovat keskenään isomorfisia ja että nämä automorfismit permutoivat polynomin juuret jollakin tavalla ja muodostavat siksi ryhmän. Sitten määriteltiin normaalit ja separoituvat kuntalaajennukset joiden avulla määriteltiin Galois'n laajennus. Viimeiseksi todistettu heikennetty versio Galois'n teorian päälauseesta kertoo Galois'n laajennuksen asteen ja sitä vastaavan Galois'n ryhmän koon olevan sama. Tätä yhteyttä voidaan soveltaa esimerkiksi viidennen asteen yhtälön ratkaisukaavan mahdottomuuden todistamisessa.

LÄHTEET

[1] J. Cruthirds. Infinite Galois theory for commutative rings. *Pacific Journal of Mathematics* 64 (1) (1976), 107–117. DOI: https://doi.org/10.2140/pjm.1976.64.107.

[2] J. Häsä ja J. Rämö. *Johdatus abstraktiin algebraan*. Gaudeamus Helsinki University Press, 2015.

[3] J. J. Rotman. *Galois Theory*. Springer-Verlag, 1998.

[4] J. J. Rotman. *Advanced Modern Algebra*. Prentice Hall, 2003.