# Polynomiyhtälöiden ratkeavuus juurilausekkeilla

Ville Uusivuori

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

| Tiedekunta/Osasto — Fakultet/Sektion — Faculty | Laitos — Institution — Department |
|---|---|
| Matemaattis-luonnontieteellinen | Matematiikan ja tilastotieteen laitos |

Tekijä — Författare — Author
Ville Uusivuori

Työn nimi — Arbetets titel — Title

Polynomiyhtälöiden ratkeavuus juurilausekkein

| Oppiaine — Läroämne — Subject | | |
|---|---|---|
| Matematiikka | | |
| Työn laji — Arbetets art — Level | Aika — Datum — Month and year | Sivumäärä — Sidoantal — Number of pages |
| Pro gradu -tutkielma | Tammikuu 2014 | 54 s. |

Tiivistelmä — Referat — Abstract

Työssä esitetään todistus sille, että kaikki polynomiyhtälöt joiden kertoimet ovat rationaalilukujen kunnassa ovat juurilausekkein ratkeavia kun niiden aste enintään 4. Tämä osoitetaan todistamalla, että yhtälön Galoisryhmän ratkeavuus on riittävä ja välttämatön ehto sen ratkeavuudelle juurilausekkein, jonka jälkeen tarkastelaan millaisia ovat polynomiyhtälöiden Galoisryhmät. Lisäksi annetaan esimerkki 5. asteen polynomiyhtälöstä, joka ei ole juurilausekkein ratkeava.

Johadantoluvussa esitellään tutkielman keskeinen tulos. Lisäksi tehdään katsaus siihen matematiikan historian osaan, jonka päätepisteenä tämän työn keskiössä oleva tulos oli.

Luvuissa kaksi ja kolme käydään läpi niitä työkaluja, joita käytetään keskeisimmissä todistuksissa. Luvussa kaksi esitellään tutkielman kannalta tärkeitä määritelmiä kuten juurilaajennos, ryhmän rakeavuus sekä polynomiyhtälön ratkeavuus juurilausekkein. Luvussa kolme määritellään niitä apuvalineitä, joita tarvitaan tutkielman keskeisissä todistuksissa sekä todistetaan joukko niiden hyödyllisiä ominaisuuksia. Näitä ovat symmetriset alkeispolynomit, ykkösenjuuret, Galoisryhmän ja Galoisresolventtin käsitteet sekä alkion $u$ minimipolynomin $\pi(x)$ määritelmä.

Luvut neljä ja viisi muodostavat tämän työn keskeisimmän sisällön. Luku neljä sisältää tutkielman keskeisimmän tuloksen, riittävän ja välttämättömän ehdon polynomiyhtälön ratkaevuudelle juurilausekkein. Käytetty todistus seuraa pitkälti Èvariste Galois'n alkuperäistä todistusta 1800-luvun alusta, joskin modernia notaatiota ja paikoitellen myöhempää teoriaa hyödynätäen. Luvussa viisi osoitetaan polynomiyhtälöiden Galoisryhmien olevan symmetrisiä ryhmiä tai niiden aliryhmiä. Tämän jälkeen tarkastellaan symmetristen ryhmien ratkeavuutta ja lopuksi yhdistetään lukujen neljä ja viisi tulokset, jolloin saadaan alussa esitetty tulos.

Avainsanat — Nyckelord — Keywords
polynomit, ratkeavuus, Galoisteoria

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — Övriga uppgifter — Additional information

# Sisältö

# Luku 1

# Johdanto

Tämän tutkielma tarkoituksena on esitellä todistus sille, että kaikki polynomiyhtälöt joiden asteluku on enintään neljä ovat juurilausekkein ratkeavia ja että on olemassa viidennen asteen polynomeja, jotka eivät ole juurilausekkein ratkeavia. Tämä tehdään osoittamalla, että ehto juurilausekkein ratkeavuudelle on olemassa ja sitten tarkastelemalla polynomiyhtälöiden Galoisryhmiä riittävässä määrin, jotta niiden ratkeavuus selviää. Tutkielmassa esitellään lyhyesti myös tämän todistuksen tarvitsemia apuvälineitä kuten symmetriset alkeispolynomit, ykkösenjuuret, Galoisresolventti $V$ ja alkion $u$ minimipolynomi $\pi(x)$.

Tutkielman tulos on lopullinen vastaus matemaatikkoja aivan varhaisimmista ajoista aina 1800-luvulle asti kiinnostaneeseen ongelmaan. Matemaatikoiden kiinnostus polynomiyhtälöiden ratkaisujen ongelmiin näkyy varhaisimmistakinmistakin löydetyistä teksteistä. Tämä on varsin ymmärrettävää, sillä varhaisimmat yhtälöt liittyvät ymmärrettävästi lukumääriin, pituuksiin, pinta-aloihin ja tilavuuksiin. Nykymatematiikan kielellä ne kuuluvat polynomiyhtälöiden luokkaan. Helposti nähdään, että tällaisten ongelmien mahdollisimman yleisille ratkaisuille on paljon käytännön sovelluksia. Matemaatikkoja kiinnosti löytää mahdollisimman yleispäteviä ratkaisumenetelmiä, ja niitä löydettiinkin aina neljänteen asteeseen saakka (1400-luvulla) kunnes 1800-luvun alussa ensin Niels Abel osoitti, ettei viidennenasteen polynomiyhtälöille enää löytynyt yleistä ratkaisua. Pian tämäm jälkeen Edvarté Galois vei etsinnän päätökseen osoittamalla, ettei tätä korkeammillekaan asteille enää löydy yleistä ratkaisukaavaa.

## 1.1 Historiallista taustaa

Varhaisimmat säilyneet matemaattiset kirjoitukset ovat muinaisesta Egyptistä, jossa selvästi laskettiin matematiikkaa huvinkin vuoksi. Niistä löytyy ratkaisutekniikka ensimmäisen asteen yhtälöille. Egyptiläiset kutsuivat tuntematonta suuretta kasaksi ja ratkaisivat niihin liittyvät ongelmat niin sanotulla väärän sijoituksen tekniikalla. Tekniikan ideana on arvata tuntemattoman suureen koko ja sitten katsoa, paljonko arvaus meni pieleen. Toisen asteen ongelmien ratkomisesta ei ole säilynyt näyttöä ja muutenkin muinaisen Egyptin matematiikka oli etenkin algebran osalta melko alkeellista.

Myös babylonialaisilta on säilynyt paljon matemaattisia kirjoituksia. Syynä lienee, että siellä kirjoitettiin savitauluille eikä hauraalle papyrukselle. Babylonialaisten käyttämä 60-järjestelmä, josta jäänteitä näkyy edelleen muun muassa siinä, että tunnissa on 60 minuuttia, oli hyvin toimiva. Siinä oli paikkajärjestelmä, joka sisälsi myös "alkeisnollan". Babylonialaisten huomattavan abstraktista otteesta kertovat säilyneet tekstit, joissa neliön alasta saatettiin vähentää sen sivu suuremmitta ongelmitta, mikä viittaa sanojen takana olevaa yleisempiin käsiteisiin. Tehtäviä myös ratkottiin usein muuttujan vaihdoksella. Algebran ja erityisesti polynomiyhtälöiden ratkaisemisessa babylonialaiset olivat sangen edistyneitä ja he osasivatkin ratkoa osaa toisen, kolmannen ja jopa muutamia neljännen asteen polynomiyhtälöitä. Toisen asteen yhtälöt babylonialaiset ratkoivat käyttäen neliöön korottamista. Muotoa $x^3 = a$ olevia yksinkertaisimpia kolmannen asteen yhtälöitä ratkottiin suoraan kuutio-kuutiojuuritaulukoiden avulla. Monimutkaisemmissa tilanteissa yhtälö käännettiin muuttujan vaihdoksella babylonialaisten standardimuotoon $n^3 + n^2 = a$, jonka ratkaisut oli saatavilla taulukoituna. Babylonialaisten käytössä olevilla keinoilla olisi ollut mahdollista ratkoa jopa osa neliitermisistä kolmannen asteen yhtälöistä, mutta niistä ei ole jäänyt todisteita. Toisaalta babylonialaiset eivät pystyneet ratkaisemaan monia meille helppoja yhtälöitä kuten $x^2 + 12x = 6$, jonka molemmat juuret ovat negatiivisia, koska he eivät tunteneet negatiivisia tai imaginaarisiä lukuja. Tosin ei niitä tunnettu muuallakaan kuin Babyloniassa ennen uuden ajan alkua.

Johtuen pitkälti polynomiyhtälöiden käytännöllisyydestä niiden ratkaisemiseksi kehitettiinkin myös monia numeerisia ratkaisuja. Keskiajan lopussa Samarkandissa vaikuttanut arabimatemaatikko al-Kashi osasi ratkaista halutulla tarkkuudella kaikki käytännön ongelmista nousevat toisen ja kolmannen asteen yhtälöt eli sellaiset, joiden juuret ovat positiivisia reaalilukuja.

Vuonna 1545 Geronimo Cardano (1501-1576) julkaisi teoksen Ars magna, jota monet pitävät modernin matematiikan syntyhetkenä. Teoksessa hän esittelee ratkaisukaavat kolmannen ja neljännen asteen polynomiyhtälöille. Kumpaakaan kaavaa Cardano ei ota omiin nimiinsä, vaan kertoo kolmannen

asteen ratkaisun olevan Niccolo Tartaglian (n. 1500-1557) keksimä, joskin ilmeisesti on ollut olemassa jo tätä aikaisempi julkaisematon osittainen ratkaisu. Kunnian neljännen asteen ratkaisusta saa Cardanon sihteeri ja oppilas Ludovico Ferrari (1522-1565). Vaikka modernin notaation hallitseva lukija näkeekin kaavoista heti, että ne kuvaavat kaikki samoja tilanteita, niin Cardanon käyttämän matematiikan alkeellisuudesta johtuen on tarvinnut käydä läpi kaikki kertoimien merkkien mahdolliset kombinaatiot.

Cardanon ja Galois'n väliin mahtuneiden vuosisatojen aikana myös matemaattinen notaatio kehittyi paljon. Descartes poisti viimeisetkin yhteismitattomuuteen liittyvät omantunnon pistokset matemaatikoilta. Saksalaiset + ja − merkit korvasivat italialaiset $\bar{p}$ ja $\bar{m}$ merkit, ja eksponenttimerkinnät korvasivat vanhat *cubus* ja *quadratus* merkinnät.

Vaikka nykylukijalle selvästi tutuin ratkaisukaava on toisenasteen polynomiyhtälön $ax^2 + bx + c = 0$ ratkaisukaava

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

se tuli eurooppalaisten matemaatikkojen tietoisuuteen vasta Cardanon julkaisun jälkeen. Eurooppalaisen matematiikan kaanonin sen toi ensimmäisenä hollantilainen Simon Stevin vuonna 1585. Vaikka lopullisen kaavan olisikin voinut löytää ratkottaessa yhtälöitä neliöön täydentämällä ja huomaamalla säännönmukaisuuden, kuten intialainen 600-luvulla elänyt Brahmagupta, niin ei kuitenkaan käynyt. Osansa saattoi olla sillä, ettei neliöön täydentäminen ole kohtuuttoman työläs ratkaisualgoritmi. Toisaalta osasyy, miksi tämä keksintö antoi odottaa itseään, on, ettei (yleisten)kertoimien ja tuntemattomien käsitteitä vielä ollut kunnolla eroteltu toisistaan. Sen teki lopulta Francois Viéte, joka vuonna 1591 kirjassaan erotti tuntemattomat ja tunnetut suureet toisistaan käyttämällä ensimmäisille merkkeinä vokaaleja ja jälkimmäisille konsonantteja.

Cardanon esittämät ratkaisut antoivat lähtölaukauksen paitsi polynomiyhtälöiden ratkaisukaavojen etsimiselle ja monen muunkin algebran osa-alueiden tutkimukselle. Hänen ratkaisunsa nostivat kiistatta esille myös sen, että imaginaariluvuilla on oltava säännöt sillä niitä nousi esiin laskujen välivaiheissa, vaikka olisikin rajoituttu vain reaalisten juurien etsintään. Imaginaariset (ja negatiivisetkin) juuret hyväksyi ensimmäisenä Girard 1620-luvulla tehdessään tärkeän havainnon, että kaikki polynomit voidaan rakentaa juuriensa avulla ensimmäisen asteen polynomien tulona. Kesti aina 1830-luvulle, ennen kuin Gaussin esittelemä kompleksitaso, jonka oli ensimmäisenä julkaissut Caspar Wessel vuonna 1797, teki imaginaariluvuista salonkikelpoisia matemaatikoiden valtavirran keskuudessa.

Ratkaisukaavojen etsinnän veivät päätöspisteen kaksi nuorena traagisesti kuollutta neroa 1800-luvun alkupuoliskolla. Norjalainen Niels Abel (1802-1829) kuoli tuberkuloosiin juuri, kun hänen saavutuksensa olivat nousemassa laajempaan tietoisuuteen. Kirje hänelle myönnetystä matematiikan professuurista Berliinin yliopistolla saapui vain päiviä hänen kuolemansa jälkeen. Ranskalainen Edvarté Galois (1812-1832), joka turhautui lukuisiin vastoinkäymisiinsä, muun muassa tarkastajat hukkasivat hänen kirjoittamiaan artikkeleita. Hän kuoli lopulta kaksintaistelussa saamiinsa vammoihin.

Viidennenasteen polynomiyhtälöiden yleisen ratkaisukaavan etsiminen osoittautui kuitenkin ympyrän neliöimisen kaltaiseksi mahdottomaksi tehtäväksi, kun Abel vuonna 1824 julkaisi tutkielman "Yhtälöiden algebrallisesta ratkaisemisesta" jossa hän osoitti, ettei viidennen asteen polynomiyhtälöille ole yleistä ratkaisua. Saman tuloksen oli jo 1799 saanut Paolo Ruffini, mutta hänen todistuksensa oli vähemmän tyydyttävä ja jäi vähälle huomiolle. Nykyisin tämä tulos kulkee kuitenkin nimellä Abelin-Ruffinin lause.

Galois ei ehtinyt eläessään saada tunnustusta saavutuksistaan, sillä ne vähät artikkelit, joita hän sai julkaistua olivat liian pieniä sirpaleita hänen päässään olleesta kokonaisuudesta. Lisäksi ne olivat usein luonnoksenomaisia, joten arvioijat lähettivät niitä takaisin täydennettäväksi. Koska Galois kuoli nuorena nämä täydennykset jäivät palauttamatta ja hänen ajatuksensa pääsivät leviämään vasta vuonna 1846, kun Joseph Liouville sai julkaistuksi laajemman kokoelman Galois'n tekstejä omine selventävine täydennyksineen. Vaikka Galois veikin päätökseen matemaatikoita kiinnostaneen etsinnän osoittamalla, ettei mitään löydettävää ole, niin tapa, jolla hän sen teki oli varsin hedelmällinen. Se avasi monia uusia suuntia algebran tutkimukselle.

Galois oli ensimmäinen matemaatikko, joka käytti sanaa ryhmä kuvamaan sellaista oliota, jota nykyään kutsutaan algebrassa ryhmäksi. Lisäksi hän loi normaalin aliryhmän käsitteen ja aurasi tietä modernille ryhmäteorialle.

Galois'n tulos käyttää oleellisesti algebrallisten kuntien ominaisuuksia, vaikka koko kunnan käsitettä ei ollut vielä keksitty ja hän kuvailee nämä ominaisuudet määrittelemällä sen, mitä hän tarkoittaa rationaalifunktioilla esitettävissä olevilla joukon alkioilla. Nykylukija pystyy näkemään, että kuvailtu olio on selvästi kunta. Tämän käsitteen viimeistelyn tekivät saksalaiset matemaatikot vasta 1800-luvun lopulla.

Galois'n tärkein tienavaus jälkipolville on idea siitä, että kuntien ominaisuuksia voidaan tutkia tiettyjen ryhmien ominaisuuksien avulla. Hän käytti tätä yhtälöiden tutkimiseen, mutta häntä myöhemmät matemaatikot ovat käyttäneet tätä nykyään Galois-teorian nimellä kulkevaa työkalua hedelmällisesti monilla muillakin matematiikan osa-alueilla.

# Luku 2

# Perusmääritelmiä

**Määritelmä 2.1.** Olkoot $K$ ja $L$ kuntia siten, että $K$ on kunnan $L$ alikunta. Sanotaan, että kunta $L$ on kunnan $K$ kuntalaajennos. Merkinnällä $K(a_1, \ldots, a_n)$ tarkoitetaan pienintä kunnan $K$ kuntalaajennosta, joka sisältää alkiot $\{a_1, \ldots, a_n\}$ $\in L$ kun $K \subset L$.

**Määritelmä 2.2.** Olkoon $K$ kunta, ja olkoon $f(x)$ polynomi, jonka kertoimet löytyvät kunnasta $K$. Sanomme, että polynomiyhtälö $f(x) = 0$ on ratkeava juurilausekkeilla kunnassa $K$, jos $f(x)$ hajoaa ensimmäisen asteen polynomien tuloksi kunnan $K$ laajennuksessa $K(a_1, a_2, \ldots, a_n)$ ja on olemassa kokonaisluvut $k_1, \ldots, k_n$ siten, että $a_1^{k_1} \in K$ ja $a_i^{k_i} \in K(a_1, a_2, \ldots, a_{i-1})$ kun $i = 2, \ldots, n$.

**Määritelmä 2.3.** Kunnan $K$ kuntalaajennos $L$ on juurilaajennos, jos on olemassa äärellinen ketju kuntia $K = L_0 \subset L_1 \subset \cdots \subset L_n = L$ siten, että $L_i = L_{i-1}(a_i)$ missä $a_i^{p_i} \in L_{i-1}$ jollekin alkuluvulle $p_i$.

Juurilaajennosta $L$ kutsutaan kunnan $K$ $n$. asteen juurilaajennokseksi, jos ketjun $K = L_0 \subset L_1 \subset \cdots \subset L_n = L$ pituus on $n + 1$. Voidaan myöskin sanoa, että jokainen kunta $K$ on 0-asteen juurilaajennos itsestään.

**Esimerkki 2.4.** Kunta $\mathbb{Q}(\sqrt{5})$ on pienin rationaalilukujen kuntalaajennos, joka sisältää yhtälön $x^2 - 5 = 0$ juuret. Kyseessä on 1.asteen juurilaajennos sillä löytyy alkuluku $p_1 = 2$ jolle $(\sqrt{5})^2 = 5 \in \mathbb{Q}$. $\mathbb{Q}(\sqrt[6]{5})$ on vuorostaan 2. asteen juurilaajennos kunnalle $\mathbb{Q}$, sillä se on vuorostaan 1. asteen juurilaajennos kunnasta $\mathbb{Q}(\sqrt{5})$. Löydetään alkuluku $p_2 = 3$ siten, että $(\sqrt[6]{5})^3 = \sqrt{5} \in \mathbb{Q}(\sqrt{5})$, joten saadaan ketju $\mathbb{Q} = L_0 \subset L_1 = \mathbb{Q}(\sqrt{5}) \subset L_2 = \mathbb{Q}(\sqrt[6]{5})$.

Jos kunta $K$ sisältää $n$. ykkösenjuuren (ks. määritelmä 3.11), juurilaajennosten määritelmästä seuraavaa vaatimusta alkulukueksponenteille voidaan löyhentää tavalla, joka osoittautuu myöhemmin käteväksi.

**Lause 2.5.** *Olkoon $L$ kunnan $K$ kuntalaajennos. Jos $L$ on muotoa $K(u)$ jollakin $u$ jolle $u^n \in K$ jollekin kokonaisluvulla $n$ ja jos kunta $K$ sisältää $n$. alkeisykkösenjuuren, niin $L$ on kunnan $K$ juurilaajennos.*

Tämä lause poistaa eksponentin $n$ tarpeen olla alkuluku ja sekä vaatimuksen, ettei alkio $u^a$ olisi jonkin alkion $b \in K$, $n$. potenssi, kunhan $K$ sisältää $n$. alkeisykkösenjuuren.

*Todistus.* Todistetaan induktiolla eksponentin $n$ suhteen. Jos $n = 1$ niin $u \in K$ joten $L = K$ joka on 0-asteen juurilaajennos itsestään. Joten voidaan olettaa induktio-oletuksena, että kun $n \geq 2$ niin väite pitää kun alkion $u$ eksponentti on enintään $n - 1$.

Jos $n$ ei ole alkuluku, olkoon $n = rs$ joillekin kokonaisluvuille $r, s < n$. Induktio-oletuksen nojalla, $K(u)$ on juurilaajennos kunnille $K(u^r)$ ja $K(u^s)$ jotka ovat itsekin juurilaajennoksia kunnalle $K$, koska $(u^r)^s \in K$. Näin ollen $K(u)$ on kunnan $K$ juurilaajennos, koska määritelmästä seuraa, että laajennosten ketju $K \subset M \subset N$, jossa $N$ on kunnan $M$ juurilaajennos, joka vuorostaan on kunnan $K$ juurilaajennos, niin täytyy kunnan $N$ olla myös kunnan $K$ juurilaajennos.

Jos $n$ on alkuluku, tarkastellaan kahta tapausta, riippuen siitä onko $u^n$ jonkin kunnan $K$ alkion $n$. potenssi. Jos se ei ole, niin $L$ on määritelmän nojalla kunnan $K$ juurilaajennos. Mutta jos se kuitenkin on jonkin alkion $n$. potenssi niin olkoon

$$u^n = b^n$$

jollekin $b \in K$. Jos $b = 0$ niin myös $u = 0$ ja taas $L = K$ ja väite on tältä osin todistettu. Jos kuitenkin $b \neq 0$, niin edellisestä yhtälöstä saadaan

$$(\frac{u}{b})^n = 1,$$

eli $u/b$ on $n$. ykkösenjuuri, jotka kaikki ovat kunnassa $K$. Tästä seuraa, että $u/b \in K$, josta edelleen seuraa, että $u \in K$, joten $K = L$. Ja näin todistus on valmis. □

**Määritelmä 2.6.** Polynomin $f(x)$, jonkakertoimet ovat kunnassa $\mathbb{Q}$, juurikunnaksi kutsutaan pienintä kompleksilukujen alikuntaa $K$, jossa se voidaan pilkkoa ensimmäisen asteen polynomien tuloksi.

**Määritelmä 2.7.** Luonnollinen surjektio on kuvaus $\varphi_N : H \mapsto H/N : \varphi_N(x) = xN$, missä $H$ on ryhmä, $N$ sen normaali aliryhmä ja $H/N$ niiden muodostama tekijäryhmä.

**Määritelmä 2.8.** Olkoon $L$ kunta ja $f : L \mapsto L$ sen isomorfismi. Jos jollekin kunnan $L$ alikunnalle $K$ pätee $f(k) = k$ kaikille $k \in K$ niin isomorfismia $f$ kutsutaan $K$-automorfismiksi.

**Määritelmä 2.9.** Olkoon ryhmät $G$ ja $H$ siten, että $H \subset G$. Aliryhmän $H$ indeksiksi ryhmässä $G$ kutsutaan sen (vasempien) sivuluokkien $xH$ lukumäärää, missä $x \in G$. Indeksiä merkitään $(G : H)$. Se on samalla myös tekijäryhmän $G/H$ mahtavuus.

**Määritelmä 2.10.** Ryhmä $G$ on ratkeava, jos ja vain jos sille voidaan löytää ketju normaaleja aliryhmiä $\{e\} = H_1 \lhd H_2 \lhd \ldots \lhd H_{n-1} \lhd H_n = G$ siten, että tekijäryhmät $H_2/H_1, \ldots, H_n/H_{n-1}$ ovat vaihdannaisia tai $G = \{e\}$. Näiden normaalien aliryhmien ketjua kutsutaan myöhemmin ryhmän $G$ ratkeavaksi ketjuksi.

Ratkeavuudelle on äärellisten ryhmien tapauksessa myös ekvivalentti ja hyödyllinen määritelmä.

**Määritelmä 2.11.** Äärellinen ryhmä $G$ on ratkeava, jos ja vain jos sille voidaan löytää ketju normaaleja aliryhmiä $\{e\} = H_1 \lhd H_2 \lhd \ldots \lhd H_{n-1} \lhd H_n = G$ siten, että aliryhmän $H_i$ indeksi ryhmässä $H_{i+1}$ on alkuluku.

**Lause 2.12.** *Määritelmät 2.10 ja 2.11 ovat ekvivalentteja äärellisille ryhmille.*

*Todistus. Määritelmä 2.11 $\Rightarrow$ määritelmä 2.10:* Väite seuraa suoraan siitä, että tekijäryhmien $H_{i+1}/H_i$ mahtavuudet ovat alkulukuja, joten ne ovat syklisiä ryhmiä, jotka ovat tunnetusti vaihdannaisia.

*Määritelmä 2.10 $\Rightarrow$ määritelmä 2.11:* Aloitetaan osoittamalla, että jokainen tekijäryhmä $H_{i+1}/H_i$ sisältää ketjun normaaleja aliryhmiä

$$H_{i+1}/H_i \supset K_{i1} \supset \cdots \supset K_{ir_i} = \{1\},$$

missä jokaisen aliryhmän indeksi edeltäjässään on jokin alkuluku. Koska vaihdannaisen ryhmän kaikki aliryhmät ovat normaaleja, riittää osoittaa, että niiden indeksi edeltäjässään on jokin alkuluku. Tämä onnistuu osoittamalla, että jos $K$ on vaihdannaisen ryhmän $H$ aito äärellinen osajoukko, niin löytyy $H_1 \subset H$, jonka indeksi ryhmässä $H$ on alkuluku ja johon sisältyy joukko $K$. Todistetaan induktiolla yli indeksin $(H : K)$. Jos indeksi $(H : K)$ on 2, 3 tai jokin muu alkuluku, niin voimme valita $H_1 = K$. Oletetaan sitten ettei $(H : K)$ ole alkuluku. Valitaan $x \in H$ joka ei kuuluu joukkoon $K$ ja tarkastellaan pienintä eksponenttia $e > 0$ jolle $x^e \in K$. Olkoon alkuluku

$p$ jokin eksponentin $e$ tekijä ja $y = x^{e/p}$. Nyt eksponentin $e$ valinnan vuoksi $y \notin K$ ja $y^p \in K$. Tarkastellaan ryhmää

$$K' = \{x^i z \mid i = 1, \ldots, p-1;\ z \in K\}.$$

On selvää että $K \subset K' \subset H$ ryhmän $K$ sivuluokat ryhmässä $k'$ ovat

$$K', xK', x^2K', \ldots, x^{p-1}K',$$

joten indeksi

$$(K' \ : \ K) = p.$$

Näin ollen, $K' \neq H$ koska oletuksen mukaan $(H \ : \ K)$ ei ollut alkuluku ja

$$(H \ : \ K') < (H \ : \ K).$$

Induktio-oletuksen nojalla ryhmän $H$ sisältää aliryhmän $H_1$, jonka indeksi ryhmässä $H$ on alkuluku, joka sisältää ryhmän $K'$ ja samalla ryhmän $K$.

Nyt käyttämällä luonnollisen surjektion $\pi$ käänteiskuvausta näihin tekijäryhmiin $H_{i+1}/H_i$ ketju

$$H_{i+1} \supset \pi^{-1}H_{i1} \supset \cdots \supset H_i\pi^{-1}K_{ir_i} \supset H_i,$$

jossa aliryhmien indeksit edeltäjissään ovat alkulukuja. Nyt nämä ketjut voidaan laittaa täydentämään määritelmän 2.10 mukainen ketju määritelmän 2.11 vaatimaan muotoon. □

**Määritelmä 2.13.** Symmetrinen ryhmä $S_n$ on kaikkien joukon $\{1, \ldots, n\}$ permutaatioiden joukko laskutoimituksenaan kuvausten yhdistäminen $\circ$. Sen neutraalialkio on identiteettikuvaus $Id$. Sen aliryhmistä käytetään laajempaa nimitystä permutaatioryhmä.

**Määritelmä 2.14.** Vuorotteleva ryhmä $A_n$ on kaikkien parillisten permutaatioiden, eli sellaisten permutaatioiden, jotka saadaan yhdistämällä parillinen määrä transpositioita, muodostama ryhmä.

Tutkielmassa turvaudutaan toistuvasti algebran peruslauseeseen.

**Lause 2.15.** ***Algebran peruslause:*** *Jokaisella yhden muuttujan polynomilla $P(x)$, jonka kertoimet ovat kunnassa $K \subset \mathbb{C}$ ja jonka aste on $n \geq 1$ on ainakin yksi juuri kunnassa $\mathbb{C}$.*

*Todistus.* Lause oletetaan tunnetuksi. □

# Luku 3

# Tärkeitä työkaluja

## 3.1 Symmetriset alkeispolynomit

**Määritelmä 3.1.** Symmetrisiksi alkeispolynomeiksi $s_1, \ldots, s_n$ kutsutaan polynomeja, jotka rakennetaan muuttujista $x_1, \ldots, x_n$ seuraavasti:

$$\begin{aligned}
s_1 &= \sum_{i=1}^{n} x_i &&= x_1 + \cdots + x_n \\
s_2 &= \sum_{i,j=1,\, i<j}^{n} x_i x_j &&= x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n \\
&&&\cdots \\
s_{n-1} &= \sum_{i=1}^{n} \frac{x_1x_2\cdots x_n}{x_i}* &&= x_2\cdots x_n + x_1x_3\cdots x_n + \cdots + x_1\cdots x_{n-1} \\
s_n &= \sum_{i=1}^{1} x_i x_{i+1}\cdots x_n &&= x_1\cdots x_n
\end{aligned}$$

** Tässä syyllistyn hiukan notaation väärinkäyttöön, sillä supistan $\frac{x_i}{x_i} = 1$, vaikka en kielläkään mitään muuttujista $x_i$ olemasta nolla.*

Näiden polynomien kutsuminen symmetrisiksi perustuu siihen, että ne pysyvät samoina, vaikka muuttujat $x_1, \ldots, x_n$ järjestettäisiin uudelleen jollakin permutaatiolla, ja niiden kutsuminen alkeispolynomeiksi johtuu siitä, että muut symmetriset polynomit voidaan esittää niiden avulla, kuten osoitamme lauseessa 3.2.

**Lause 3.2.** *Polynomi, jossa on $n$ muuttujaa $x_1, \ldots, x_n$ ja jonka kertoimet ovat kunnassa $K$, voidaan esittää polynomina käyttäen symmetrisiä alkeispolynomeja $s_1, \ldots, s_n$ jos ja vain jos se itse on symmetrinen.*

Todistuksessa käytetään Waringin metodia määrittää $n$ muuttujan polynomin aste. Tällaisen (ei nolla-) polynomin asteeksi tulee $n$-jono $(i_1, \ldots, i_n)$. Määritellään $n$-jonojen suuruusjärjestys seuraavasti: $(i_1, \ldots, i_n) \geq (j_1, \ldots, j_n)$, jos ensimmäinen nollasta poikkeava erotus jonossa $i_1 - j_1, \ldots, i_n - j_n$ on positiivinen. Nyt määritellään, että (ei nolla-) polynomin $p(x_1, \ldots, x_n)$ aste $\deg p(x_1, \ldots, x_n)$ on suurin $n$-jono $(i_1, \ldots, i_n)$, jolle termin $x_1^1 \cdots x_n^n$ kerroin on nollasta poikkeava. Kun lisäksi sovitaan, että nollapolynomille $\deg 0 = -\infty$ niin saadaan toimimaan seuraavat yhdenmuuttujan polynomeilta tutut suhteet

$$\deg(p+q) \leq \max(\deg p, \deg q), \tag{3.3}$$

$$\deg(pq) = \deg p + \deg q. \tag{3.4}$$

Todistuksen kannalta oleellisimpia ovat symmetristen alkeispolynomien asteet, jotka ovat

$$\begin{aligned} \deg s_1 &= (1,0,0,\ldots,0) \\ \deg s_2 &= (1,1,0,\ldots,0) \\ &\cdots \\ \deg s_{n-1} &= (1,1,1,\ldots,1,0) \\ \deg s_n &= (1,1,\ldots,1,1). \end{aligned} \tag{3.5}$$

*Todistus.* Olkoon $f(x_1, \ldots, x_n)$ symmetrinen polynomi. Todistuksen ideana on löytää symmetrisistä alkeispolynomeista $s_1, \ldots, s_n$ rakennettu polynomi $g(s_1, \ldots, s_n)$, jonka asteluku on sama kuin polynomilla $f(x_1, \ldots, x_n)$. Säätämällä polynomin $g(s_1, \ldots, s_n)$ ensimmäistä kerrointa saadaan

$$\deg(f(x_1, \ldots, x_n) - g(s_1, \ldots, s_n)) < \deg f(x_1, \ldots, x_n),$$

josta todistus viedään loppuun induktiolla asteen suhteen.

Olkoon $f(x_1, \ldots, x_n)$ symmetrinen polynomi, jolla on nollasta poikkeavia kertoimia ja olkoon

$$\deg(f(x_1, \ldots, x_n)) = (i_1, i_2, \ldots, i_n) \in \mathbb{N}^n.$$

Ensiksi huomataan, että $i_1 \geq i_2 \geq \cdots \geq i_n$. Jos löydämme polynomin $f(x_1, \ldots, x_n)$ termin, joka on muotoa $a x_1^{i_1} \cdots x_n^{i_n}$, missä $a \neq 0$, niin löydetään kaikki ne termit, jotka saadaan permutoimalla muuttujat $x_1, \ldots, x_n$, sillä polynomi $f(x_1, \ldots, x_n)$ on symmetrinen. Näiden termien asteluvut ovat $n$-jono, jotka saadaan permutoimalla $i_1, \ldots, i_n$ ja niistä suurin on se $n$-jono, jonka jäsenille $i_1 \geq i_2 \geq \cdots \geq i_n$.

Nyt asetetaan

$$g(s_1, \ldots, s_n) = s_1^{i_1 - i_2} s_2^{i_2 - i_3} \cdots s_{n-1}^{i_{n-1} - i_n} s_n^{i_n}.$$

Kaavojen (3.4) ja (3.5) nojalla saadaan

$$\begin{aligned} \deg g(s_1, \ldots, s_n) &= (i_1 - i_2)\deg(s_1) + (i_2 - i_3)\deg(s_2) + \cdots + i_n \deg(s_n) \\ &= (i_1 - i_2, 0, \ldots, 0) + (i_2 - i_3, i_2 - i_3, 0, \ldots, 0) + \cdots (i_n, \ldots i_n) \\ &= (i_1, i_2 \ldots, i_n). \end{aligned}$$

Lisäksi huomataan, että polynomin $g(s_1, \ldots, s_n)$ ensimmäisen termin kerroin on 1. Joten

$$g(s_1, \ldots, s_n) = x_1^{i_1} \cdots x_n^{i_n} + (\textit{alemman asteen termit}).$$

Näin ollen, jos $a \in K$ on polynomin $f(x_1, \ldots, x_n)$ ensimmäisen termin kerroin, siten että

$$f(x_1, \ldots, x_n) = a x_1^{i_1} \cdots x_n^{i_n} + (\textit{alemman asteen termit}),$$

nyt olkoon $f_1(x_1, \ldots, x_n) = f(x_1, \ldots, x_n - a g(s_1, \ldots, s_n)$, josta nähdään, että $\deg f_1(x_1, \ldots, x_n) < f(x_1, \ldots, x_n)$. Lisäksi $f_1(x_1, \ldots, x_n)$ on symmetrinen, joten voimme toistaa sille saman prosessin ja etsiä polynomin $g_1(s_1, \ldots, s_n)$ ja niin edelleen. Nyt riittää osoittaa, että prosessi päättyy äärellisen monessa askeleessa. Tämä seuraa suoraan seuraavasta lemmasta. □

**Lemma 3.6.** $\mathbb{N}^n$ *ei sisällä päättymättömiä aidosti laskevia jonojen ketjuja.*

*Todistus.* Lemma pätee selvästi, kun $n = 1$, joten todistetaan väite induktiolla jonojen pituuden $n$ suhteen olettamalla, että kun $n \geq 2$ väite pätee kun jonot ovat pituudeltaan $n - 1$. Jos

$$(i_{11}, i_{12}, \ldots, i_{1n}) > (i_{21}, i_{22}, \ldots, i_{2n}) > \cdots > (i_{m1}, i_{m2}, \ldots, i_{mn}) > \cdots \tag{3.7}$$

on päättymätön laskeva ketju jonoja, niin jonojen ensimmäiset termit eivät muodosta kasvavaa ketjua, joten

$$i_{11} \geq i_{21} \geq \cdots \geq i_{m1} \geq \cdots$$

Näin ollen ketju muuttuu ennemmin tai myöhemmin vakioksi, on siis olemassa indeksi $M$, jolle

$$i_{m1} = i_{M1} \quad \textit{kaikille } m \geq M.$$

Kun poistetaan ensimmäiset $(M-1)$ ketjun (3.7) jäsentä ja keskitytään jäljelle jääneiden jäsenten $(n-1)$ viimeiseen jäseneen, saadaan seuraava päättymätön ketju:

$$(i_{M2}, i_{M3}, \ldots i_{Mn}) > (i_{(M+1)2}, i_{(M+1)3}, \ldots i_{(M+1)n}) > \cdots$$

joka on päättymätön ketju $(n-1)$-pituisia ketjua, joka on ristiriidassa induktio-oletuksemme kanssa. □

**Lause 3.8.** *Olkoon $g(x_1, \ldots, x_n)$ polynomi, jossa on $n$ muuttujaa ja jonka kertoimet ovat kunnassa $K$. Jos $g(x_1, \ldots, x_n)$ on invariantti kaikissa muuttujien $x_1, \ldots, x_n$ permutaatioissa, niin se voidaan esittää polynomina käyttäen muuttujaa $x_1$ ja symmetrisiä alkeispolynomeja $s_1, \ldots, s_{n-1}$ joissa muuttujina ovat $x_2, \ldots, x_n$.*

*Todistus.* Tarkastellaan polynomia $g(x_1, \ldots, x_n)$ polynomina, jonka muuttujat ovat $x_2, \ldots, x_n$ ja sen kertoimet ovat kunnassa $K(x_1)$, joka on kunnan $K$ laajennos, joka sisältää kaikki murtolausekkeet, jotka saadaan muodostettua muuttujasta $x_1$ käyttäen kertoimina kunnan $K$ alkioita. Lauseesta 3.2 seuraa, että $g$ voidaan kirjoittaa polynomina käyttäen symmetrisiä alkeispolynomeja $s'_1, \ldots, s'_{n-1}$, joissa muuttujina ovat $x_2, \ldots, x_n$ ja kertoimet ovat kunnassa $K(x_1)$. Näin ollen on olemassa polynomi $g'(x_1, \ldots, x_n)$ jolle

$$g(x_1, \ldots, x_n) = g'(x_1, s'_1, \ldots, s'_n), \tag{3.9}$$

jossa

$$s'_1 = x_2 + \cdots + x_n, \quad s'_2 = x_2x_3 + \cdots + x_{n-1}x_n, \quad \cdots, \quad s'_{n-1} = x_2x_3 \cdots x_n.$$

Todistuksen viemiseksi loppuun riittää osoittaa, että polynomien, jotka on rakennettu muuttujasta $x_1$ ja symmetrisistä alkeispolynomeista $s_1, \ldots, s_{n-1}$, tilalle voidaan sijoittaa polynomit $s'_1, \ldots, s'_n$. Helppo tapa saada riittävän konkreettiset kaavat polynomeille $s'_1, \ldots, s'_{n-1}$ on jakaa binomilla $X - x_1$ yleinen polynomi

$$(X - x_1) \cdots (X - x_n) = X^n - s_1X^{n-1} + \cdots + (-1)^n s_n$$

ja samastaa tulos seuraavasti

$$(X - x_2) \cdots (X - x_n) = X^{n-1} - s'_1X^{n-2} + \cdots + (-1)^{n-1} s'_{n-1}.$$

Tästä saadaan

$$\begin{aligned} s'_1 &= s_1 - x_1 \\ s'_2 &= s_2 - s_1x_1^2 - x_1^2 \\ s'_3 &= s_3 - s_2x_1 + s_1x_1^3 - x_1^3 \\ &\cdots \\ s'_{n-1} &= s_{n-1} - s_{n-2}x_1 + \cdots + (-1)^{n-1}x_1^{n-1}, \end{aligned} \tag{3.10}$$

josta, sijoittamalla $s'_1, \ldots, s'_{n-1}$ yhtälöön 3.9, saadaan

$$g(x_1, \ldots, x_n) = g'(x_1, s_1 - x_1, \ldots, s_{n-1} - s_{n-2}x_1 + \cdots + (-1)^{n-1}x_1^{n-1}),$$

jonka oikea puoli on polynomi, joka on rakennettu muuttujasta $x_1$ ja symmetrisistä alkeispolynomeista $s_1, \ldots, s_{n-1}$. □

## 3.2 Ykkösenjuuret

**Määritelmä 3.11.** Ykkösenjuureksi kutsutaan sellaista kunnan $K \subset \mathbb{C}$ alkiota $a$, jolle pätee , $a^n = 1$, jollakin $n$. Ykkösenjuurta, jolle $k$ on pienin kokonaisluku siten, että $a^k = 1$, kutsutaan $k$. alkeisykkösenjuureksi. Ykkösenjuurten joukkoa, jonka jäsenille pätee $a^n = 1$ merkitään $\mu_n$.

**Lause 3.12.** *Jos $\zeta$ on $p$. alkeisykkösenjuuri, niin $p$. ykkösenjuuret ovat muotoa*

$$\zeta, \zeta^2, \ldots, \zeta^{p-1}, \zeta^p = 1.$$

*Todistus.* Halutaan osoittaa, että $S = \{\zeta^n \mid n \in 1, \ldots, p\} = \mu_p$, sillä jos $a > p$ niin

$$\zeta^a = \zeta^{kp+b} = \zeta^{kp}\zeta^b = \zeta^b$$

missä $k \in \mathbb{Z}_+$ ja $b \in \{0, \ldots, p-1\}$.

Helposti nähdään, että $\zeta^n$ on $p$. ykkösenjuuri, sillä

$$(\zeta^n)^p = \zeta^{np} = (\zeta^p)^n = 1^n = 1$$

Nyt riittää osoittaa, ettei joukossa $\mu_p$ ole muita jäseniä. Tähän riittää osoittaa, että $\zeta^i \neq \zeta^k$ kun $i \neq j$, $i, j \in \{1, \ldots, n\}$.

Vastaoletuksena oletetaan $\zeta^i = \zeta^j$ joillekin $1 \leq i < j \leq n$. Nyt $\zeta^{j-i} = 1$, jolloin $j - i = kn$, mikä ei ole mahdollista sillä $0 < j - i < n$ joka on todistaa alkuperäisen väitteen. □

**Lause 3.13.** *Mille tahansa kokonaisluvulle $n$ ja mille tahansa kunnalle $K \subset \mathbb{C}$, $n$. ykkösenjuuri on kunnan $K$ juurilaajennoksessa.*

Todistuksessa tarvitaan Lagrangen resolventtiä.

**Määritelmä 3.14.** Todistuksessa Lagrangen resolventtilla $t(\omega)$ tarkoitetaan kompleksilukua joka määritellään

$$t(\omega) = \zeta_0 + \omega\zeta_1 + \cdots + \omega^{n-2}\zeta_{n-2},$$

missä $\zeta_i$ ovat epätriviaalit $n$. ykkösenjuuret siten $\zeta_0$ on alkeisykkösenjuuri ja $\zeta_i = \zeta_0^{n-1}$ ja missä $\omega$ on jokin $(n-1)$. ykkösenjuuri.

*Todistus.* Riittää osoittaa, että $n$. alkeisykkösenjuuri $\zeta$ on kunnan $K$ juurilaajennoksessa $L$, sillä muut ykkösenjuuret ovat sen potensseja ja ovat siksi kunnassa $L$.

Tämä todistetaan induktiolla luvun $n$ suhteen. Jos $n = 1$ niin $\zeta = 1$ ja selvästi kuuluu kuntaan $K$, joka on itsensä 0. asteen juurilaajennos. Voidaan siis olettaa induktio-oletuksena, että kun $n \geq 2$ väite pätee ykkösenjuurille $\zeta^k = 1$ joille $k < n$.

Jos $n$ ei ole alkuluku löytyy kokonaisluvut $r$ ja $s$ siten, että $n = rs$ ja $0 < r, s < n$. Nyt $\zeta^r$ on $s$. ykkösenjuuri. Induktio-oletuksen nojalla löytyy kunnan $K$ juurilaajennos $R_1$, johon $\zeta^r$ kuuluu. Nyt edelleen induktio-oletuksen nojalla löydetään kunnan $R_1$ juurilaajennos $R_2$, joka sisältää $r$. alkeisykkösjuuren. Nyt koska $\zeta^r \in R_2$ niin $R_2(\zeta)$ on kunnan $R_2$, sekä myös kunnan $K$, juurilaajennos, joten lause on tältä osin todistettu.

Jos $n$ on alkuluku, niin aloitamme etsimällä kunnan $K$ juurilaajennoksen $R_1$ joka sisältää ykkösenjuuren $\omega^{n-1} = 1$. Tämä onnistuu induktio-oletuksen avulla, kuten edellä osoitettiin. Nyt otetaan käyttöön Lagrangen resolventti $t(\omega)$. Nyt lemman 3.15 nojalla saadaan

$$t(\omega)^{n-1} \in R_1$$

kaikille $\omega$, jotka ovat $(n-1)$. ykkösenjuuria. Nyt $R_1(t(\omega))$ on kunnan $R_1$ juurilaajennos. Kun liitetään kaikki Lagrangen resolventit $t(\omega)$ kuntaan $R_1$, niin saadaan juurilaajennos $R_2$, joka on samalla myös kunnan $K$ juurilaajennos. Nyt $R_2$ sisältää kaikki resolventit $t(\omega) \in \mu_{n-1}$. Lagrangen kaavasta seuraa, että $\zeta$ voidaan rakentaa rationaalilausekkein Lagrangen resolventeista, joten $\zeta \in R_2$, ja näin ollen todistus on valmis. □

**Lemma 3.15.** *Jokaiselle $k$. ykkösenjuurelle $\eta$ on olemassa $t(\eta)^k$, joka voidaan esittää rationaalilausekkeena ykkösenjuuren $\eta$ ja $g$ mittaisten jaksojen avulla.*

**Määritelmä 3.16.** Tämän todistuksen yhteydessä käytetään Gaussin jaksoksi nimeämää kompleksilukujoukkoa. Olkoon $e, f$ positiivisia kokonaislukuja, joille $ef = p-1$, missä $p$ on alkuluku. Näin määrittyy $e$ kappaletta lukuja

$$\begin{aligned}
\eta_0 &= \zeta_0 + \zeta_e + \zeta_{2e} + \cdots + \zeta_{e(f-1)} \\
\eta_1 &= \zeta_1 + \zeta_{e+1} + \zeta_{2e+1} + \cdots + \zeta_{e(f-1)+1} \\
\eta_2 &= \zeta_2 + \zeta_{e+2} + \zeta_{2e+2} + \cdots + \zeta_{e(f-1)+2} \\
&\cdots \\
\eta_{e-1} &= \zeta_{e-1} + \zeta_{2e-1} + \zeta_{3e-1} + \cdots + \zeta_{p-2}
\end{aligned}$$

joita Gauss kutsui $f$ mittaisiksi jaksoiksi.

Erityisesti on huomattava, että 1 mittaiset jaksot ovat ykkösenjuuret $\zeta_0, \zeta_1, \ldots, \zeta_{p-2}$ ja $p-1$ mittainen jakso on summa kaikista epätriviaaleista ($\zeta_i \neq 1$) ykkösenjuurista.

Lisäksi on tärkeää huomata, että mikä tahansa $f$ mittainen jakso saadaan rakennettua murtolausekkein mistä tahansa toisesta $f$ mittaisesta jaksosta.

*Todistus.* Lemman 3.19 nojalla tiedetään että kahden $f$ mittaisen jakson tulo voidaan esittää $f$ mittaisten jaksojen lineaarikombinaationa. Näin voimme siis esittää ensimmäisen asteen polynomeina kaikki jaksojen potenssit. Erityisesti

$$\begin{aligned} t(\omega)^k &= (\eta_0 + \omega\eta_h + \cdots \omega^{k-1}\eta_{h(k-1)})^k \\ &= a_0\eta_0 + \cdots + a_{h-1}\eta_{h-1} \\ &\quad + a_h\eta_h + \cdots + a_{2h-1}\eta_{2h-1} \\ &\quad + \cdots \\ &\quad + a_{h(k-1)}\eta_{h(k-1)} + \cdots + a_{e-1}\eta_{e-1} \end{aligned} \tag{3.17}$$

missä kertoimet $a_0, \ldots, a_{e-1}$ ovat rationaalisia kunnassa $\mathbb{Q}(\omega)$.

Olkoon $\sigma^h$ kuten lemmassa 3.19. Koska jaksojen $\eta_0, \ldots, \eta_{e-1}$ väliset suhteet säilyvät kuvauksessa $\sigma^h$, voidaan korvata $\eta_0$ sen kuvalla $\sigma^h(\eta_0) = \eta_h$ ja vastavaasti $\eta_1 \mapsto \sigma^h(\eta_1) = \eta_{h+1}$ ja niin edelleen, laskettaessa $t(\omega)^k$. Tästä saadaan

$$\begin{aligned} (\eta_h + \omega\eta_{2h} + \cdots + \omega^{k-1}\eta_0)^k &= a_0\eta_h + \cdots + a_{h-1}\eta_{2h-1} \\ &\quad + a_h\eta_{2h} + \cdots + a_{2h-1}\eta_{3h-1} \\ &\quad + \cdots \\ &\quad + a_{h(k-1)}\eta_0 + \cdots + a_{e-1}\eta_{n-1}. \end{aligned} \tag{3.18}$$

Tästä saadaan $(\sigma^h(t(\omega)))^k$ esitys. Kuitenkin, koska

$$(\sigma^h(t(\omega)) = \omega^{-1}t(\omega),$$

saadaan

$$(\sigma^h(t(\omega)))^k = t(\omega)^k,$$

joten sekä (3.17) ja (3.18) ovat molemmat $t(\omega)^k$ esityksiä. Nyt korvataan alkuperäisestä $t(\omega)^k$ kaavasta jakso $\eta_i$ jaksolla $\sigma^{2h}(\eta_i)$, seuraavat jaksoilla $\sigma^{4h}(\eta_i), \ldots, \sigma^{k-1}(\eta_i)$ kun $i \in \{1, \ldots, e-1\}$ löydetään vielä $k-2$ kappaletta $t(\omega)^k$ esityksiä. Huomataan, että jakson $\eta_i$ kertoimet näissä esityksissä ovat

$a_{i+h}, a_{i+2h}, \ldots, a_{a+h(k-1)}$ Niinpä laskemalla nämä esitykset yhteen saadaan

$$\begin{aligned} kt(\omega)^k &= (a_0 + \ldots + a_{h(k-1)})(\eta_0 + \ldots + \eta_{h(k-1)}) \\ &= (a_1 + \ldots + a_{h(k-1)+1})(\eta_1 + \ldots + \eta_{h(k-1)+1}) \\ &\quad + \cdots \\ &= (a_{h-1} + \ldots + a_{e-1})(\eta_{h-1} + \ldots + \eta_{e-1}) \end{aligned}$$

Koska $\eta_i + \eta_{h+i} + \cdots + \eta_{h(k-1)+i} = \xi_i$ kun $i = 0, \ldots, h-1$ niin seuraa, että $t(\omega)^k$ voidaan esittää murtolausekkeina käyttäen jaksoja $\omega$ ja $\xi_0, \ldots, \xi_{h-1}$, eksplisiittisemmin

$$t(\omega)^k = \frac{1}{k}((a_0 + \cdots + a_{h(k-1)})\xi_0 + \cdots + (a_{h-1} + \cdots + a_{h(e-1)})\xi_{h-1}).$$

□

**Lemma 3.19.** *Olkoon $\sigma^e$ $\mathbb{Q}$-automorfismi joka kuvaa kunnan $\mathbb{Q}(\mu_p)$ itselleen ja $K_f$ kunnan $\mathbb{Q}(\mu_p)$ alikunta, jonka jäsenet ovat invariantteja kuvauksen*

$$\sigma^e(x) = \begin{cases} x & x \in \mathbb{Q} \\ \zeta_{i+e} & x = \zeta_i, i \in \{0, 1, \ldots, p-e\} \\ \zeta_0 & x = \zeta_{(p-e)+1} \\ \zeta_{(i-e)+1} & x = \zeta_i, i \in \{(p-e)+2, \ldots, p-2\} \end{cases}$$

*suhteen kun $ef = p-1$. Kaikilla kunnan $K_f$ jäsenillä on yksikäsitteinen esitys $f$ pituisten jaksojen lineaarikombinaatioina, joita on $e$ kappaletta ja käyttäen vain rationaalisia kertoimia.*

*Todistus.* Olkoon $a$ mielivaltainen kunnan $\mathbb{Q}(\mu_p)$ jäsen, joka kirjoitetaan seuraavasti:

$$\begin{aligned} a &= a_0\zeta_0 + a_1\zeta_1 + \cdots a_{e-1}\zeta_{e-1} \\ &\quad + a_e\zeta_e + a_{e+1}\zeta_{e+1} + \cdots + a_{2e-1}\zeta_{2e-1} \\ &\quad + \cdots \\ &\quad + a_{e(f-1)}\zeta_{e(f-1)} + a_{e(f-1)+1}\zeta_{e(f-1)+1} + \cdots a_{p-2}\zeta_{p-2}. \end{aligned}$$

Nyt permutaation $\sigma^e$ määritelmästä seuraa

$$\begin{aligned} \sigma^e(a) &= a_0\zeta_e + a_1\zeta_{e+1} + \cdots a_{e-1}\zeta_{2e-1} \\ &\quad + a_e\zeta_{2e} + a_{e+1}\zeta_{2e+1} + \cdots + a_{2e-1}\zeta_{3e-1} \\ &\quad + \cdots \\ &\quad + a_{e(f-1)}\zeta_0 + a_{e(f-1)+1}\zeta_1 + \cdots a_{p-2}\zeta_{e-1}. \end{aligned}$$

Jos $\sigma^e(a) = a$ niin lemman 3.20 nojalla ykkösenjuurten $\zeta_i$ kertoimet ovat samat yllä olevissa esityksissä, kun $i = 0, \ldots, p-2$, joten

$$\begin{array}{ccccccccc} a_0 & = & a_e & = & a_{2e} & = & \cdots & = & a_{e(f-1)}, \\ a_1 & = & a_{e+1} & = & a_{2e+1} & = & \cdots & = & a_{e(f-1)+1}, \\ & & & & \cdots & & & & \\ a_{e-1} & = & a_{2e-1} & = & a_{3e-1} & = & \cdots & = & a_{p-2}, \end{array}$$

Näin ollen jokainen $a \in K_f$ voidaan kirjoittaa

$$\begin{aligned} a \;=\; & a_0(\zeta_0 + \zeta_e + \cdots + \zeta_{e(f-1)}) \\ & + a_1(\zeta_1 + \zeta_{e+1} + \cdots + \zeta_{e(f-1)+1}) \\ & \cdots \\ & a_{e-1}(\zeta_{e-1} + \zeta_{2e-1} + \cdots + \zeta_{p-2}). \end{aligned}$$

Nyt on osoitettu, että $a$ on jaksojen lineaarikombinaatio, sillä sulkujen sisällä olevat lausekkeet ovat $f$ mittaisia jaksoja.

Ilmaisun yksikäsitteisyys seuraa suoraan lemmasta 3.20, jonka nojalla kaikki kunnan $\mathbb{Q}(\mu_p)$ voidaan kirjoittaa vain yhdellä tavalla ykkösenjuurten $\zeta_0, \ldots, \zeta_p$ lineaarikombinaationa. □

**Lemma 3.20.** *Jokaiselle kunnan $\mathbb{Q}(\mu_p)$ jäsenelle on olemassa vain yksi esitys epätriviaalien $p$. ykkösenjuurten rationaalikertoimien lineaarikombinaationa.*

$$a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1} \quad (a_i \in \mathbb{Q}).$$

*Todistus.* Lauseesta 3.12 seuraa, että $\mathbb{Q}(\mu_p) = \mathbb{Q}(\zeta)$. Koska $\zeta$ on polynomin $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ juuri ja koska $\Phi_p(x)$ on jaoton sekä asteeltaan $p-1$, saadaan lemman 3.34 avulla, että kaikki kunnan $\mathbb{Q}(\mu_p)$ alkiot voidaan yksikäsitteisesti esittää muodossa

$$a = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2} \tag{3.21}$$

joillekin $a_i \in \mathbb{Q}$. Jotta saadaan haluttu muoto, riittää käyttää tietoa

$$\Phi_p(\zeta) = 1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0. \tag{3.22}$$

Tästä yhtälöstä huomataan

$$a_0 = -a_0(\zeta + \zeta^2 + \cdots + \zeta^{p-1}),$$

jonka sijoittaminen yhtälöön (3.21) saadaan

$$a = (a_1 - a_0)\zeta + (a_2 - a_0)\zeta^2 + \cdots + (a_{p-2} - a_0)\zeta^{p-2} - a_0\zeta^{p-1}.$$

Tämän yksikäsitteisyys seuraa esityksen (3.21) yksikäsitteisyydestä, sillä jos

$$a_1\zeta + \cdots + a_{p-1}\zeta^{p-1} = b_1\zeta + \cdots + b_{p-1}\zeta^{p-1},$$

ja käytämme yhtälöä (3.22) eliminoimaan termin $\zeta^{p-1}$, niin saadaan

$$\begin{aligned} -a_{p-1} + (a_1 - a_{p-1})\zeta + \cdots + (a_{p-2} - a_{p-1})\zeta^{p-2} = \\ -b_{p-1} + (b_1 - b_{p-1})\zeta + \cdots + (b_{p-2} - b_{p-1})\zeta^{p-2}. \end{aligned}$$

Yhtälön (3.21) yksikäsitteisyydestä seuraa, että kertoimet termeille $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$ ovat samat molemmille puolille, joten

$$a_{p-1} = b_{p-1}, \quad a_1 = b_1, \quad \ldots, \quad a_{p-2} = b_{p-2}.$$

□

## 3.3 Galoisryhmä $G_K(f)$ ja Galoisresolventti $V$

Galois'n todistuksessa tärkeää osaa näyttelevät polynomin $f(x)$ juurten permutaatioiden muodostama ryhmä, joka onkin nimetty Galoisryhmäksi.

**Määritelmä 3.23.** Olkoon $f(x) = 0$ polynomiyhtälö, jonka kertoimet ovat äärettömässä kunnassa $K = \mathbb{Q}$ ja olkoot $r_1, \ldots, r_n \in \mathbb{C}$ sen juuret. Olkoon $K(r_1, r_2, \ldots, r_n)$ kunnan $K$ juurilaajennos, joka sisältää kaikki polynomiyhtälön $f(x) = 0$ juuret. Galoisryhmä $G_K(f)$ on polynomiyhtälön $f(x) = 0$ juurten permutaatioiden joukko, jonka tuottavat sellaiset kunnan $K(r_1, r_2, \ldots, r_n)$ automorfismit, jotka kiinnittävät alikunnan $K$ eli, joille $\sigma(a) = a$ jos $a \in K$. Sitä kutsutaan polynomiyhtälön $f(x) = 0$ Galoisryhmäksi kunnan $K$ suhteen.

*Huomautus* 3.24. Merkintää $\sigma$ käytetään sekä edellä esitettyjen kuvausten että niiden tuottamien permutaatioiden kohdalla.

Polynomiyhtälön $f(x) = 0$ Galoisryhmillä kuntien $K$ ja $L$ suhteen on seuraavaa hyödyllinen ominaisuus:

**Lause 3.25.** *Jos $L$ on kunnan $K$ kuntalaajennos niin $G_L(f)$ on Galoisryhmän $G_K(f)$ aliryhmä.*

*Todistus.* Koska sekä $G_K(f)$ että $G_L(f)$ ovat Galoisryhmiä, niin riittää osoittaa, ettei $G_L(f)$ voi sisältää sellaisia permutaatioita, jotka eivät kuuluu ryhmään $G_K(f)$. Polynomilla $f(x)$ on $n$ juurta $\{r_1, \ldots, r_n\}$. Nyt meillä on kaksi tapausta:

*Tapaus 1* $\{r_1, \ldots, r_n\} \cap L = \{r_1, \ldots, r_n\} \cap K$. Tästä seuraa, että $G_L(f) = G_K(f)$.

*Tapaus 2* $\{r_1, \ldots, r_n\} \cap L \neq \{r_1, \ldots, r_n\} \cap K$. Triviaalisti, jos $\{r_1, \ldots, r_n\} \subset L$ niin $G_L(f) = \{Id\} \in G_K(f)$. Koska $K \subset L$ niin $G_L(f) \subset G_K(f)$, sillä jos jokin alkio on kiinnitetty $L$-automorfismeissa niin se on kiinnitetty myös $K$-automorfismeissa. □

Toinen Galois'n tärkeä työkalu on hänen nimeään kantava resolventti $V$, jonka avulla voidaan kaikki yhtälön $f(x) = 0$ juuret sisältävä kuntalaajennos esittää kätevämmin.

**Määritelmä 3.26.** Polynomiyhtälön $f(x) = 0$ jonka kertoimet ovat ääretömässä kunnassa $K$, jonka juuret ovat $r_1, \ldots, r_n$, Galoisresolventiksi kunnan $K$ suhteen kutsutaan sellaista kunnan $K(r_1, \ldots, r_n)$ alkiota $V$, jolle pätee

$$r_i \in K(V) \quad \textit{kaikille } i = 1, \ldots, n.$$

Toisin sanoen kaikki polynomiyhtälön juuret voidaan esittää Galoisresolventin $V$ avulla murtolausekkein.

**Lause 3.27.** *On olemassa yhtälön $f(x) = 0$ Galoisresolventti $V \in K(r_1, \ldots, r_n)$ jolle*

$$r_i \in K(V) \quad \textit{kaikille } i = 1, \ldots n.$$

*Todistus.* Todistetaan kahdessa vaiheessa

*Vaihe 1* Olkoon $f(x) = 0$ polynomiyhtälö, jonka juuret ovat $r_1, \ldots, r_n$. Osoitetaan, että on olemassa polynomi $g(x_1, \ldots, x_n)$ siten, että ne kunnan $K(r_1, \ldots, r_n)$ alkiot, jotka saadaan sijoittamalla polynomin $g(x_1, \ldots, x_n)$ muuttujien paikalle $r_1, \ldots, r_n$ kaikilla $n!$ tavoilla, ovat kaikki eri alkioita.

Olkoon $h(x_1, \ldots, x_n) = A_1x_1 + \cdots + A_nx_n$, missä $A_1, \ldots, A_n$ ovat muuttujia. Yhtäsuuruus kahden polynomin $h(x_1, \ldots, x_n)$ arvon, jotka on saatu sijoittamalla $x_1, \ldots, x_n$ paikalle $r_1, \ldots, r_n$ jollain tavalla, välillä muodostaa yksinkertaisia ensimmäisen asteen yhtälöitä muuttujien $A_1, \ldots, A_n$ välillä, joiden kertoimet ovat kunnassa $K(r_1, \ldots, r_n)$. Kun kirjoitetaan auki kaikki mahdolliset yhtäsuuruudet, joita on äärellinen määrä, saadaan äärellinen määrä yhtälöitä muotoa $rA_i = sA_j$ jotka ovat epätriviaaleja $(r, s \neq 0)$, sillä $r_1, \ldots, r_n$ ovat eri alkioita. Nyt jokaisen tällaisen yhtälön toteuttavat $n$-jonot muodostavat oman aidon aliavaruuden vektoriavaruudessa $K^n$. Kaikki $n$-jonot, jotka toteuttavat yhdenkin näistä yhtälöistä muodostavat äärellisen yhdisteen aidoista vektoriavaruuden $K^n$ aliavaruuksista. Koska kunta $K$ on ääretön, niin vektoriavaruus $K^n$ ei voi olla aitojen aliavaruuksien äärellinen

yhdiste, joten löydetään $n$-jono $(\alpha_1, \ldots, \alpha_n) \in F^n$, jolle mikään yhtälöistä $A_1, \ldots, A_n$ välillä ei pidä. Saadaan polynomi

$$g(x_1, \ldots, x_n) = \alpha_1 x_1 + \cdots + \alpha_n x_n$$

joka toteuttaa annetun ehdon.

*Vaihe 2* Olkoon $g(x_1, \ldots, x_n)$ kuten vaiheessa 1 ja olkoon

$$V = g(r_1, \ldots, r_n) \in K(r_1, \ldots, r_n).$$

Osoitetaan, että $r_1, \ldots, r_n$ kuuluvat kuntaan $K(V)$. Tätä varten riittää osoittaa, että yksi näistä juurista, vaikkapa $r_1$, kuuluu tähän kuntaan, sillä sama todistus puree niihin kaikkiin, vain numerointia pitää muuttaa.

Tarkastellaan polynomia

$$l(x_1, \ldots, x_n) = \prod_{\sigma} (V - g(x_1, \sigma(x_2), \ldots, \sigma(x_n))$$

jonka kertoimet ovat kunnassa $K(V)$ ja missä $\sigma$ käy läpi kaikki alkioiden $x_2, \ldots, x_n$ permutaatiot. Koska $l(x_1, \ldots, x_n)$ on symmetrinen polynomi muuttujien $x_2, \ldots, x_n$ suhteen, lause 3.8 sanoo, että se voidaan kirjoittaa polynomilausekkeena käyttäen muuttujaa $x_1$ ja symmetrisiä alkeispolynomeja $s_1, \ldots, s_{n-1}$, joissa muuttujina ovat $x_2, \ldots, x_n$. Olkoon

$$l(x_1, x_2, \ldots, x_n) = k(x_1, s_1, \ldots, s_{n-1})$$

jollekin polynomille $k(x_1, \ldots, x_n)$, jonka kertoimet ovat kunnassa $K(V)$. Kun sijoitetaan muuttujiksi $x_1, \ldots, x_n$ eri tavoin juuret $r_1, \ldots, r_n$ , mikä on sama asia kuin polynomien $s_1, \ldots, s_{n-1}$ korvaaminen eräillä kunnan $K$ alkioilla $a_1, \ldots, a_{n-1}$, saadaan

$$l(r_1, \ldots, r_n) = k(r_1, a_1, \ldots, a_{n-1}) \tag{3.28}$$

ja

$$g(r_i, r_1, r_2, \ldots, r_{i-1}, r_{i+1}, \ldots, r_n) = k(r_i, a_1, \ldots, a_{n-1}). \tag{3.29}$$

Nyt, koska polynomilla $g(x_1, \ldots, x_n)$ on vaiheessa 1 osoitettu ominaisuus ja koska $V = g(r_1, \ldots, r_n)$ saadaan

$$V \neq g(r_i, \sigma(r_1), \sigma(r_2), \ldots, \sigma(r_{i-1}), \sigma(r_{i+1}), \ldots, \sigma(r_n))$$

kun $i \neq 1$ ja mille tahansa joukon $\{r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_n\}$ permutaatiolle $\sigma$. Näin ollen

$$l(r_i, r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_n) \neq 0 \quad \textit{kun } i \neq 1.$$

Toisaalta tavasta, jolla $h(x_1, \ldots, x_n)$ ja $V$ on määritelty seuraa että

$$l(r_1, \ldots, r_n) = 0.$$

Kun otetaan huomioon yhtälöt (3.28) ja (3.29), huomataan, että polynomi $k(x, a_1, \ldots, a_{n-1})$, jonka kertoimet ovat kunnassa $K(V)$, saa arvon 0, kun $x = r_1$, mutta ei kun $x = r_i$ jos $i \neq 1$. Näin ollen polynomi $k(x, a_1, \ldots, a_{n-1})$ on jaollinen binomilla $x - r_i$ vain kun $i = 1$.

Olkoon polynomi $j(x)$, jonka kertoimet ovat kunnassa $K(V)$, polynomien $f(x)$ ja $k(x, a_1, \ldots, a_{n-1})$ suurin yhteinen jakaja, jonka ensimmäisen termin kerroin on 1. Koska kunta $K(r_1, \ldots, r_n)$ on polynomin $f(x)$ juurikunta, niin

$$f(x) = (x - r_1) \cdots (x - r_n),$$

josta seuraa edelleen, että $K(r_1, \ldots, r_n)$ on myös polynomin $j(x)$ juurikunta. Koska binomi $x - r_1$ jakaa polynomit $f(x)$ ja $k(x, a_1, \ldots, a_{n-1})$, se jakaa myös polynomin $j(x)$. Toisaalta koska $k(x, a_1, \ldots, a_{n-1})$ ei ole jaollinen binomilla $x - r_i$ kun $i \neq 1$, polynomilla $j(x)$ ei ole muita tekijöitä kuin $x - r_1$. Näin ollen $j(x) = x - r_1$, josta seuraa $r_1 \in K(V)$, koska polynomin $x - r_1$ kertoimet ja siten myös $r_1$ kuuluvat kuntaan $K(V)$. □

## 3.4 Alkion $u$ minimipolynomit

**Määritelmä 3.30.** Olkoon $u$ jokin kunnan $K$ laajennoksen $K(r_1, \ldots, r_n)$ alkio. Alkion $u$ minimipolynomi kunnan $K$ suhteen $\pi(x)$ on sellainen (kunnassa $K$) jaoton polynomi, jolle

- sen kertoimet ovat kunnassa $K$,
- sen korkeimman asteen termin kerroin on 1,
- $\pi(u) = 0$,
- kunta $K(r_1, \ldots, r_n)$ on sen juurikunta.

**Lause 3.31.** *Jokaiselle kunnan $K(r_1, \ldots, r_n)$ alkiolle $u$ on olemassa yksikäsitteinen määritelmän 3.30 mukainen polynomi $\pi(x)$.*

*Todistus.* Todistetaan lause kahdessa vaiheessa. Ensiksi vaiheessa 1 osoitetaan väite sellaisille $u \in K(r_1, \ldots, r_n)$ jotka voidaan esittää polynomilausekkeella käyttäen alkioita $r_1, \ldots, r_n$ ja kertoimina kunnan $K$ alkioita. Sitten vaiheessa 2 osoitetaan, että kaikki $u \in K(r_1, \ldots, r_n)$ voidaan esittää tällaisillä polynomilausekkeilla.

*Vaihe 1.* Olkoon $u \in K(r_1, \ldots, r_n)$ esitettävissä polynomin $\varphi(r_1, \ldots, r_n)$ avulla eli

$$u = \varphi(r_1, \ldots, r_n)$$

missä $\varphi(r_1, \ldots, r_n)$ on $n$ muuttujan polynomi, jonka kertoimet ovat kunnassa $K$ ja jonka muuttujien paikalle on sijoitettu alkiot $r_1, \ldots, r_n$.

Jos $u$ on jonkin polynomin $f(x)$ juuri, on se myös jonkin jaottoman polynomin $f_1(x)$, jonka korkeimman asteen termin kerroin on 1, juuri. Tämä seuraa suoraan polynomin $f(x)$ jakamisesta tekijöihin:

$$f(x) = c \cdot f_1(x) f_2(x) \cdots f_n(x).$$

Seuraavaksi todistetaan polynomin $f_1(x)$ yksiskäsitteisyys. Oletetaan, että meillä on olemassa polynomi $g_1(x)$, jolla olisi nämä samat ominaisuudet kuin polynomilla $f_1(x)$. Koska niillä on yhteinen juuri $u$, niin lemman 3.33 nojalla polynomi $g_1(x)$ jakaa polynomin $f_1(x)$ ja päin vastoin. Koska kummallakaan ei ole edessä vakiokerrointa niin $f_1(x) = g_1(x)$.

Nyt osoitetaan, että $u$ on sellaisen polynomin juuri, jonka kertoimet ovat kunnassa $K$ ja jonka juurikunta on $K(r_1, \ldots, r_n)$. Olkoon

$$\theta(y, x_1, \ldots, x_n) = \prod_{\sigma} (y - \varphi(\sigma(x_1), \ldots, \sigma(x_n)))$$

missä $\sigma$ käy läpi kaikki muuttujien $x_1, \ldots, x_n$ permutaatiot. Koska $\theta$ on selvästi symmetrinen, niin se voidaan lauseen 3.2 nojalla esittää polymina $\psi$ symmetristen alkeispolynomien $s_1, \ldots, s_n$ avulla. Olkoon

$$\theta(y, x_1, \ldots, x_n) = \psi(y, s_1, \ldots, s_n)$$

missä polynomin $\psi$ kertoimet ovat kunnassa $K$. Kun sijoitetaan muuttujien $x_1, \ldots, x_n$ paikalle juuret $r_1, \ldots, r_n$, saadaan

$$\theta(y, r_1, \ldots, r_n) = \psi(y, a_1, \ldots, a_n),$$

missä polynomin $\psi(y, a_1, \ldots, a_n)$ kertoimet löytyvät kunnasta $K$. Tavasta jolla $\theta$ on määritelty, seuraa,

$$\theta(u, r_1, \ldots, r_n) = 0,$$

joten $u$ on myös polynomin $\psi(u, a_1, \ldots, a_n)$ juuri. Lisäksi koska $\theta(y, r_1, \ldots, r_n)$ on ensimmäisten asteen termien tulo, niin myös $\psi(y, a_1, \ldots, a_n)$ on hajoitettavissa ensimmäisen asteen polynomien tuloksi kunnassa $K(r_1, \ldots, r_n)$, joten sen on polynomin $\psi(y, a_1, \ldots, a_n)$ juurikunta.

*Vaihe 2.* Todistetaan, että kaikille $u \in K(r_1, \ldots, r_n)$ on olemassa polynomiesitys käyttäen alkioita $r_1, \ldots, r_n$ ja kertoimina kunnan $K$ alkiota.

Olkoon $V \in K(r_1, \ldots, r_n)$ Galoisresolventti (Määritelmä 3.26). Koska $r_1, \ldots, r_n$ ovat esitettävissää murtolausekkeina Galoisresolventin $V$ avulla, on myös $u$ esitettävissä sen avulla, joten $u \in K(V)$. Koska $V$ voidaan esittää polynomilausekkeilla käyttäen alkioita $r_1, \ldots, r_n$ eli

$$V = f(r_1, \ldots, r_n), \tag{3.32}$$

niin voidaan kohdan 1 ja lemman 3.34 nojalla löytää polynomi $q(x)$, jonka kertoimet ovat kunnassa $K$ ja jolle

$$u = q(V).$$

Nyt sijoitetaan tulos (3.32) edellä olevaan kaavaan niin saadaan

$$u = q(f(r_1, \ldots, r_n))$$

ja tämä on polynomiesitys käyttäen alkioita $r_1, \ldots, r_n$ ja kertoimina kunnan $K$ alkiota, koska $f$ ja $q$ ovat polynomeja. □

**Lemma 3.33.** *Olkoot $f(x)$ ja $g(x)$ polynomeja, joiden kertoimet ovat kunnassa $K$ ja lisäksi olkoon $f(x)$ jaoton kunnassa $K$. Jos polynomeilla $f(x)$ ja $g(x)$ on yhteinen juuri jossakin kunnan $K$ laajennoksessa $L$, niin $f(x)$ jakaa polynomin $g(x)$.*

*Todistus.* Jos $f(x)$ ei jaa polynomia $g(x)$, niin $syt(f(x), g(x)) = 1$ ja näin ollen on olemassa polynomit $p(x)$ ja $q(x)$, joiden kertoimet ovat kunnassa $K$, siten, että

$$f(x)p(x) + g(x)q(x) = 1.$$

Kun sijoitetaan muuttujan $x$ paikalle polynomien $f(x)$ ja $g(x)$ yhteinen juuri $u$, saadaan

$$f(u)p(u) + g(u)q(u) = 1 \quad \text{kunnassa } L,$$

mutta koska $f(u) = g(u) = 0$ antaa yllä oleva kaava $0 = 1$ kunnassa $L$ ja tämä ristiriita osoittaa, että $f(x)$ jakaa polynomin $g(x)$. □

**Lemma 3.34.** *Olkoon $f(x)$ jaoton $d$. asteen polynomi kunnassa $K$ ja olkoon kunta $L$ kunnan $K$ laajennos. Jos polynomin $f(x)$ juuri $u \in L$, niin kaikki kunnan $K(u)$ alkiot voidaan esittää yksikäsitteisesti muodossa*

$$a_0 + a_1 u + a_2 u^2 + \cdots + a_{d-1} u^{d-1} \quad \textit{missä } a_i \in K.$$

*Todistus.* Olkoon $g(u)/h(u)$ mielivaltainen kunnan $K(u)$ alkio. Koska $h(u) \neq 0$, polynomi $h(x)$ ei ole jaettavissa polynomilla $f(x)$ joka on jaoton, joten polynomi $h(x)$ ei vuorostaaan jaa polynomia $f(x)$. Koska näin ollen polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä on 1, on olemassa polynomit $p(x)$ ja $q(x)$, joiden kertoimet ovat kunnassa $K$ siten, että

$$g(x)p(x) + f(x)q(x) = 1.$$

Kun sijoitetaan muuttujan $x$ paikalle $u$ ja muistamalla, että $f(u) = 0$ saadaan

$$g(u)p(u) = 1 \quad \text{kunnassa L.}$$

Tästä seuraa, että $g(u)/h(u)$ voidaan kirjoittaa murtolausekkeen sijasta polynomina alkion $u$ avulla.

$$\frac{g(u)}{h(u)} = g(u)p(u) \quad \text{kunnassa L.}$$

Nyt olkoon $r(x)$ jakojäännös kun polynomi $f(x)$ jakaa polynomin $g(x)p(x)$ joten,

$$g(x)p(x) = f(x)s(x) + r(x) \quad \deg r(x) \leq d - 1.$$

Koska $f(u) = 0$ saadaan

$$g(u)p(u) = r(u) \quad \text{kunnassa L,}$$

ja koska polynomin $r(x)$ kertoimet ovat kunnassa $K$ ja sen aste on enintään $d-1$, olemme saaneet mielivaltaisen kunnan $K(u)$ alkion $g(u)/h(u)$ esitettyä polynomina

$$a_0 + a_1u + \cdots + a_{d-1}u^{d-1}$$

missä $a_i \in K$.

Osoittaaksemme polynomiesityksen yksikäsitteisyyden oletetaan, että

$$a_0 + a_1u + \cdots + a_{d-1}x^{d-1} = b_0 + b_1u + \cdots + b_{d-1}x^{d-1}$$

keräämällä kaikki termit vasemmalle puolelle puolelle huomataan, että $u$ on polynomin $v(x)$ juuri kun

$$v(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{d-1} - b_{d-1})x^{d-1}$$

Koska polynomeilla $f(x)$ ja $v(x)$ on yhteinen juuri ja $f(x)$ on jaoton kunnassa $K$ lemman 3.33 nojalla $f(x)$ jakaa polynomin $v(x)$, mutta koska $\deg v(x) < \deg f(x)$ tämä on mahdollista vain, jos $v(x) = 0$, joten

$$a_0 - b_0 = a_1 - b_1 = \cdots = a_{d-1} - b_{d-1} = 0.$$

□

Galoisresolventin $V$ minimipolynomilla on monta hyödyllistä ominaisuutta, jotka osoitamme seuraavaksi.

**Korollaari 3.35.** *Olkoon $V$ jokin polynomiyhtälön $f(x) = 0$ Galoisresolventti kunnan $K$ suhteen, ja olkoon $V_1, \ldots, V_m$ sen minimipolynomin (kunnassa $K$) juuret. Nyt*

$$K(r_1, \ldots, r_n) = K(V) = K(V_1, \ldots, V_n).$$

*Todistus.* Koska $r_1, \ldots, r_n$ saadaan Galoisresolventin määritelmän mukaan esitettyä murtolausekkeilla käyttäen resolventtiä $V$ niin seuraa

$$K(r_1, \ldots, r_n) \subset K(V).$$

Toisaalta edeltävän lauseen nojalla minimipolynomin juuret $V_1, \ldots, V_m$ ovat kunnassa $K(r_1, \ldots, r_n)$, joten

$$K(V_1, \ldots, V_m) \subset K(r_1, \ldots, r_n).$$

Koska $V$ on yksi juurista $V_1, \ldots, V_m$, niin

$$K(V) \subset K(V_1, \ldots, V_m).$$

Nämä relaatiot toteutuvat vain kun

$$K(r_1, \ldots, r_n) = K(V) = K(V_1, \ldots, V_n).$$

□

**Lause 3.36.** *Olkoon $V$ polynomiyhtälön $f(x) = 0$ Galoisresolventti kunnan $K$ suhteen ja $V_1, \ldots, V_M$ sen minimipolynomin juuret. Lisäksi olkoot $q_i(x)$ murtolausekkeita siten, että alkiot $q_i(V) = r_i$ ovat polynomiyhtälön $f(x) = 0$ juuria $r_1, \ldots, r_n$, kun $i = 1, \ldots, n$. Tällöin kaikille $i = 1, \ldots, n$ ja kaikille $j = 1, \ldots, M$ alkiot $q_i(V_j)$ ovat polynomiyhtälön $f(x) = 0$ juuria. Lisäksi mille tahansa $j = 1, \ldots, m$ juuret $q_1(V_j), \ldots, q_n(V_j)$ ovat erillisiä siten, että*

$$\{q_1(V_j), \ldots, q_n(V_j)\} = \{r_1, \ldots, r_n\}.$$

*Todistus.* Voidaan valita $V = V_1$ joten $q_i(V_1) = r_i$ kun $i = 1, \ldots n$ ja näin ollen $f(q_i(V_1)) = 0$. Nyt sovelletaan lemmaa 3.38 murtolausekkeeseen $f(q_i(V_1))$ ja saadaan

$$f(q_i(V_j)) = 0 \quad kun\ j = 1, \ldots m.$$

Samalla huomataan, että $q_i(V_j)$ on määritelty kaikilla $i = 1, \dots n$, $j = 1, \dots m$.

Lisäksi, jos joillekin $i, k = 1 \dots n$ ja jollekin $j = 1, \dots m$ pätee

$$q_i(V_j) = q_k(V_j),$$

niin $V_j$ on murtolausekkeen $q_i(x) - q_k(x)$ juuri, josta taas lemman 3.38 avulla saadaan

$$q_i(V_1) = q_k(V_1).$$

Tämä osoittaa, että $r_i = r_k$, joten $i = k$ sillä juuret $r_1, \dots, r_n$ on oletettu erillisiksi. □

**Korollaari 3.37.** *Olkoon $V$ polynomiyhtälön $f(x) = 0$ Galoisresolventti ja $\pi(x)$ sen minimipolynomi, molemmat kunnan $K$ suhteen. Näin ollen minipolynomin $\pi(x)$ aste*

$$\deg \pi(x) = |G_K(f)|.$$

*Todistus.* Edellinen lause osoitti, että kaikille $j = 1, \dots, m$ kuvaukset

$$\sigma_j : r_i = q_i(V_1) \mapsto q_i(V_j) \quad kun\ i = 1, \dots, n$$

ovat juurten $r_1, \dots, r_n$ permutaatioita, ja selvästi nähdään, että ne muodostavat permutaatioryhmän. Nyt osoitetaan, että $\{\sigma_1, \dots, \sigma_m\} = G_K(f)$.

Laajennetaan permutaatio $\sigma \in \{\sigma_1, \dots, \sigma_m\}$ kunnan $K(r_1, \dots, r_n)$ automorfismiksi, joka kuvaa kunnan $K$ alkiot itselleen, määrittelemällä

$$\sigma(q(r_1, \dots, r_n)) = q(\sigma(r_1), \dots, \sigma(r_n))$$

kaikille murtolausekkeille $q(x_1, \dots, x_n)$, joille $q(r_1, \dots, r_n)$ on määritelty.

Koska $\sigma$ on selvästi bijektio kunnassa $K(r_1, \dots, r_n)$, niin se on helppo todeta automorfismiksi määritelmän nojalla, sillä

$$q(\sigma(r_1), \dots, \sigma(r_n)) + s(\sigma(r_1), \dots, \sigma(r_n)) = (q + s)(\sigma(r_1), \dots, \sigma(r_n))$$

ja

$$q(\sigma(r_1), \dots, \sigma(r_n)) \cdot s(\sigma(r_1), \dots, \sigma(r_n)) = (qs)(\sigma(r_1), \dots, \sigma(r_n)).$$

Nyt pitää osoittaa, ettei alkio $\sigma(q(r_1, \dots, r_n))$ riipu siitä murtolausekkeesta $q$, joka sen esittämiseen on valittu, vaan ainostaan sen arvosta.

Oletetaan siis

$$q(r_1, \dots, r_n) = s(r_1, \dots, r_n)$$

joillekin murtolausekkeille, joissa on $n$ muuttujaa $x_1, \ldots, x_n$, ja joiden kertoimet löytyvät kunnasta $K$. Murtolauseke $q - s = 0$ kun $x_i = r_i$ ja $i = 1, \ldots, n$. Lemma 3.39 osoittaa, että kaikille $\sigma \in \{\sigma_1, \ldots, \sigma_m\}$ pätee

$$(q - s)(\sigma(r_1), \ldots, \sigma(r_n)) = (q - s)(r_1, \ldots, r_n) = 0$$

joten

$$q(\sigma(r_1), \ldots, \sigma(r_n)) = s(\sigma(r_1), \ldots, \sigma(r_n)).$$

Tästä seuraa, että murtolauseke $q(\sigma(r_1), \ldots, \sigma(r_n))$ riippuu vain alkiosta $q(\sigma(r_1), \ldots, \sigma(r_n)) \in K(r_1, \ldots, r_n)$, eikä sen esittämiseen valitusta murtolausekkeesta. Näin ollen, jos murtolauseke $q(r_1, \ldots, r_n)$ esittää kunnan $K$ alkiota, niin $\sigma$ kuvaa sen itselleen, sillä se on laajennos juurten $r_1, \ldots, r_n$ permutaatiosta $\sigma$.

Nyt siis $\{\sigma_1, \ldots, \sigma_m\} = G_K(f)$ joten

$$\deg \pi = m = |\{\sigma_1, \ldots \sigma_m\}| = |G_K(f)|.$$

□

**Lemma 3.38.** *Olkoon $q(x)$ yhden muuttujan rationaalilauseke, jonka kertoimet löytyvät kunnasta $K$ ja olkoon $V$ jonkin jaottoman polynomin $f(x)$, jonka kertoimet myös ovat kunnassa $K$, juuri. Jos $q(V) = 0$ niin $q(W) = 0$ kaikille polynomin $f(x)$ juurille $W$.*

*Todistus.* Olkoon $q(x) = g(x)/h(x)$ joillekin polynomeille $g(x)$ ja $h(x)$, joiden kertoimet ovat kunnassa $K$ siten, että $h(V) \neq 0$ ja $g(V) = 0$. Lemman 3.33 nojalla jälkimmäisestä yhtälöstä seuraa, että $f(x)$ on polynomin $g(x)$ tekijä, joten $g(W) = 0$. Jos $h(W) = 0$ jollain juurella $W$, niin sama päättely johtaisi siihen, että $h(V) = 0$, joka olisi ristiriidassa polynomin $h(x)$ määritelmän kanssa. Joten $g(W) = 0$ ja $h(W) \neq 0$ joten $q(W) = 0$. □

**Lemma 3.39.** *Olkoon $\{\sigma_1, \ldots \sigma_m\}$ ryhmä permutaatioita kuten korollaarin 3.37 todistuksessa ja olkoon $q(x_1, \ldots, x_n)$ murtolauseke, jossa on $n$ muuttujaa ja jonka kertoimet ovat kunnassa $K$. Tällöin*

$$q(r_1, \ldots, r_n) \in K$$

*jos ja vain jos*

$$q(\sigma(r_1), \ldots \sigma(r_n)) = q(r_1, \ldots, r_n)$$

*kaikilla $\sigma \in \{\sigma_1, \ldots \sigma_m\}$.*

*Todistus.* Korvataan alkiot $r_1, \ldots, r_n$ niiden murtolauseke-esityksillä $r_1 = q_1(V), \ldots, r_n = q_n(V)$ käyttäen Galoisresolventtiä $V$ ja murtolausekkeita $q_1(x), \ldots, q_n(x)$, joiden kertoimet ovat kunnassa $K$ joten saadaan

$$q(r_1, \ldots, r_n) = s(V)$$

missä $s(x)$ on murtolauseke,

$$s(x) = q(q_1(x), \ldots, q_n(x)),$$

jonka kertoimet ovat kunnassa $K$. Jos $q(r_1, \ldots, r_n) \in K$ niin

$$s(x) - q(r_1, \ldots, r_n)$$

on murtolauseke, jonka kertoimet löytyvät kunnasta $K$. Koska se saa arvon 0, kun $x = V$, niin lemman 3.38 nojalla,

$$s(x) - q(r_1, \ldots, r_n) = 0 \quad kun\ x = V_1, \ldots, V_m$$

ja näin ollen

$$s(V_j) = q(s_1(V_j), \ldots, s_n(V_j)) = q(r_1, \ldots, r_n) \quad kun\ j = 1, \ldots, m.$$

Käytetään edelliseen yhtälöön korollaarin 3.37 todistuksen alussa esiteltyä permutaatiota $\sigma_j$ ja saadaan

$$q(\sigma_j(r_1), \ldots, \sigma_j(r_n)) = q(r_1, \ldots, r_n), \quad kun\ j = 1, \ldots, m.$$

Vastaavasti, jos edellinen yhtälö pitää paikkansa, niin silloin

$$q(r_1, \ldots, r_n) = s(V_j), \quad kun\ j = 1, \ldots, m$$

jolloin

$$q(r_1, \ldots, r_n) = \frac{1}{m}(s(V_1) + \cdots + s(V_m)). \tag{3.40}$$

Koska murtolauseke $s(x_1) + \cdots + s(x_m)$ on selvästi symmetrinen muuttujien $x_1, \ldots, x_m$ permutaatioiden suhteen, niin se voidaan esittää murtolausekkeena käyttäen symmetrisiä alkeispolynomeja $s_1, \ldots, s_m$. Kun sijoitetaan muuttujien $x_1, \ldots, x_n$ paikalle polynomin $\pi(x)$ juuret $V_1, \ldots, V_m$, niin huomataan, että yhtälön (3.40) oikea puoli voidaan muodostaa polynomin $\pi$ kertoimista, jotka kuuluvat kuntaan $K$, eli

$$q(r_1, \ldots, r_n) \in K.$$

□

# Luku 4

# Ratkeavuusehdon olemassaolo

Aloitetaan todistamalla, että meillä on keino vastata tähän matemaatikkoja pitkään askarruttaneeseen ongelmaan.

**Lause 4.1.** *Olkoon $f(x)$ polynomi, jonka kertoimet ovat äärettömässä kunnassa $K = \mathbb{Q}$ ja polynomilla $f(x)$ vain yksöisjuuria. Polynomiyhtälö $f(x) = 0$ on juurilausekkeilla ratkeava kunnassa $K$, jos ja vain jos sen Galoisryhmä $G_K(f)$ on ratkeava.*

*Huomautus* 4.2. Rajoittuminen polynomeihin, joilla on vain yksöisjuuria ei ole ongelma, sillä voidaan osoittaa (Lause 4.21), että kunnassa $K$ jaottomilla polynomeilla on vain yksöisjuuria ja jaolliset polynomit saadaan pilkottua jaottomien polynomien tuloksi.

*Todistus.* Aloitetaan osoittamalla induktiolla yli Galoisryhmän $G_K(f)$ mahtavuuden, että, jos yhtälö $f(x) = 0$ on juurilausekkeilla ratkeava kunnassa $K$, niin $G_K(f)$ on ratkeava. Jos $|G_K(f)| = 1$ niin $G_K(f) = \{Id\}$, joka on triviaalisti ratkeava. Nyt voimme olettaa induktio-oletuksena, että niiden juurilausekkeilla ratkeavien yhtälöiden, joiden Galoisryhmät ovat pienempiä kuin polynomiyhtälön $f(x) = 0$, Galoisryhmät ovat myös ratkeavia. Olkoon kunnan $K$ juurilaajennos $R$, joka sisältää kaikki yhtälön $f(x) = 0$ juuret. Nyt kaikki yhtälön $f(x) = 0$ juuret ovat kunnassa $R$, joten $G_R(f) = \{Id\}$. On siis olemassa Kunnan $K$ juurilaajennos $L$, jolle

$$|G_L(f)| < |G_K(f)|.$$

Seuraavaksi etsitään pienin alkuluku $p$, jolle $p$. juuren ottaminen pienentää yhtälön $f(x) = 0$ Galoisryhmää. Tarkemmin, olkoon $p$ pienin alkuluku, jolle on olemassa kunnan $K$ juurilaajennos $M$, jolle pätee

$$G_M(f) = G_K(f)$$

ja

$$|G_{M(a^{(1/p)})}(f)| < |G_K(f)|$$

jollekin $a \in M$, jolle $a \neq b^p$ kaikilla $b \in M$.

Lauseen 3.13 nojalla on olemassa kunnan $M$ juurilaajennos, joka sisältää $p$. alkeisykkösenjuuren. Lauseen 3.13 todistuksesta huomataan, että on olemassa sellainen laajennos $R'$, joka saadaan kunnasta $M$ ottamalla $q$. juuri alkuluvuille $q < p$. Siksi tavasta jolla alkuluku $p$ on määritelty saadaan

$$G_{R'}(f) = G_M(f) = G_K(f).$$

Nyt lauseen 3.25 nojalla

$$G_{R'(a^{1/p})}(f) \subset G_{M(a^{1/p})}(f),$$

joten

$$|G_{R'(a^{1/p})}(f)| < |G_K(f)|.$$

Koska $R'$ sisältää $p$. alkeisykkösenjuuren, $G_{R'(a^{1/p})}(f)$ on korollaarin 4.7 nojalla Galoisryhmän $G_{R'}(f) = G_K(f)$ normaali aliryhmä jonka indeksi Galoisryhmässä $G_{R'}(f) = G_K(f)$ on p. Koska $f(x) = 0$ on juurilausekkeilla ratkeava kunnassa $K$, se on vastaavasti juurilausekkeilla ratkeava myös kunnassa $R'(a^{1/p})$. Näin ollen voimme induktio-oletuksen nojalla rakentaa aliryhmien ketjun

$$G_{R'(a^{1/p})}(f) \supset G_t \supset \ldots \supset G_1 = \{Id\}$$

siten, että jokainen aliryhmä on edeltäjänsä normaali ja niiden indeksi edeltäjässään on alkuluku. Saadaan siis rakennettua ketju

$$G_K(f) \supset G_{R'(a^{1/p})}(f) \supset G_t \supset \ldots \supset G_1 = \{Id\},$$

joka osoittaa, että $G_K(f)$ on ratkeava.

Seuraavaksi osoitetaan, että Galoisryhmän $G_K(f)$ ratkeavuudesta seuraa yhtälön $f(x) = 0$ ratkeavuus juurilausekkein. Tämä tehdään jälleen induktiolla yli Galoisryhmän $|G_K(f)|$ mahtavuuden.

Jos $|G_K(f)| = 1$, niin ainoa siihen kuuluva permutaatio on identiteettikuvaus, näin ollen kaikki yhtälön $f(x) = 0$ juuret kuuluvat kuntaan $K$, joka on itsensä 0-asteinen juurilaajennos.

Voidaan siis olettaa induktio-oletuksena, että yhtälöt, joiden Galoisryhmät ovat ratkeavia ja pienempiä kuin $G_K(f)$, ovat ratkaistavissa juurilausekkein. Koska $G_K(f)$ on ratkeava, löytyy sille normaali aliryhmä $N$, jolle $(G_K(f) : N) = p$, missä $p$ on alkuluku. Lauseen 3.13 nojalla on olemassa sellainen juurilaajennos $R$, joka sisältää kaikki $p$. ykkösenjuuret. Jos

$$|G_R(f)| < |G_K(f)|$$

voidaan turvautua induktiohypoteesiin, sillä lauseen 4.3 nojalla $G_R(f)$ on ratkeava ryhmä. Yhtälö $f(x) = 0$ on siis juurilausekkeilla ratkeava kunnassa $R$ ja näin ollen on olemassa sen juurilaajennos $R'$, joka sisältää kaikki yhtälön $f(x) = 0$ juuret. Koska $R'$ on myös kunnan $K$ juurilaajennos on todistus tältä osin valmis. Jos taas

$$G_R(f) = G_K(f)$$

joudutaan turvautumaan lemmaan 4.16, jonka mukaan on olemassa juurilaajennos $R''$ siten, että $G_{R''}(f)$ on edellä esitetty $N$. Nyt saadaan

$$|G_{R''}(f)| < |G_K(f)|,$$

josta viemme todistuksen loppuun induktiohypoteesilla samoin kuin edellä. □

**Lause 4.3.** *Ratkeavan ryhmän $G$ aliryhmä $H$ on ratkeava.*

*Todistus.* Olkoon ketju $(G_i)_{1\leq i\leq n}$ ryhmän $G$ ratkeava ketju (ks. määritelmä 2.10) ja olkoon $H_i = G_i \cap H$ kaikille $i \in \{1, \ldots, n\}$. Nyt $H_n = H$ ja $H_1 = e$. Lisäksi $H_i$ on $H_{i+1}$ normaali aliryhmä kaikilla $i \in \{1, \ldots, n-1\}$, sillä jos $x \in H_{i+1}$ niin,

$$xH_ix^{-1} = (xH_ix^{-1}) \cap H \subseteq (xG_ix^{-1}) \cap H \subseteq G_i \cap H = H_i.$$

Olkoon $f_i$ luonnollisen surjektion $G_{i+1} \mapsto G_{i+1}/G_i$ rajoittuma ryhmään $H_{i+1}$. Silloin $x$ kuuluu kuvauksen $f_i$ ytimeen jos ja vain jos

$$x \in H_{i+1} \cap G_i = H \cap G_{i+1} \cap G_i = H_i.$$

Näin ollen lemman 4.4 nojalla ryhmä $H_{i+1}/H_i$ on isomorfinen ryhmän $G_{i+1}/G_i$ aliryhmän kanssa, joten $H_{i+1}/H_i$ on vaihdannainen ja siten on osoitettu että $(H_i)_{1\leq i\leq n}$ on ryhmän $H$ ratkeava ketju ja $H$ näin ollen ratkeava. □

**Lemma 4.4.** *Olkoon $f$ epimorfismi, eli surjektiivinen homomorfismi, ryhmältä $(H, \oplus)$ ryhmälle $(H', \oplus')$. Kuvauksen $f$ ydin $K$ on ryhmän $H$ normaali aliryhmä ja on olemassa vain yksi isomorfismi $g : H/K \mapsto H'$, jolle $g \circ \varphi_K = f$. Epimorfismi $f$ on isomorfismi jos ja vain jos $K = \{e\}$.*

*Todistus.* Olkoon $R$ kuvauksen $f$ määrittämä ekvivalenssirelaatio, ja olkoon $e'$ ryhmän $H'$ neutraalialkio. Nyt siis $xRe$ jos ja vain jos $f(x) = f(e)$. Nyt siis $K$ on neutraalialkion $e$ ekvivalenssiluokka. Koska $R$ on yhteensopiva laskutoimituksen $\oplus$ kanssa, ja lisäksi koska $K$ on ryhmän $H$ normaali aliryhmä niin $R$ on aliryhmän $K$ määrittämän ekvivalenssirelaatio $(K)$. Näin ollen lemman 4.5 nojalla on olemassa yksiselitteinen isomorfismi $g : H/K \mapsto H'$, jolle $g \circ \varphi_K = f$.

Jos $f$ on isomorfismi, niin $K = \{e\}$, sillä $f$ on injektio. Vastaavasti jos $K = \{e\}$ ja $f(x) = f(y)$ niin $x(K)y$, koska $R = (K)$, joten $x \oplus y^{-1} \in K$ ja näin ollen $x \oplus y^{-1} = e$ eli $x = y$. □

**Lemma 4.5.** *Jos $f$ on surjektiivinen homomorfismi $f : (E, \oplus) \mapsto (F, \odot)$, niin sen määrittelemä ekvivalenssirelaatio $R$ on yhteensopiva laskutoimituksen $\oplus$ kanssa ja on olemassa isomorfismi $g : (E/R, \oplus_R) \mapsto (F, \odot)$, jolle pätee $g \circ \varphi_K = f$.*

*Todistus.* Jos $xRx'$ ja $yRy'$ niin $f(x) = f(x')$ ja $f(y) = f(y')$. Näin ollen

$$f(x \oplus y) = (f(x) \odot f(y)) = (f(x') \odot f(y')) = f(x' \oplus y'),$$

eli $f(x \oplus y)Rf(x' \oplus y')$, joten $R$ on yhteensopiva $\oplus$:n kanssa. Lemman 4.6 nojalla on olemassa bijektio $g : (E/R, \oplus_R) \mapsto (F, \odot)$, jolle pätee $g \circ \varphi_K = f$. Lisäksi, koska kaikille $x, y \in E$ pätee

$$g(\bar{x} \oplus_R \bar{y}) = g(x \bar{\oplus} y) = f(x \oplus y) = f(x) \odot f(y) = g(\bar{x}) \odot g(\bar{y})$$

ja näin ollen $g$ on isomorfismi. □

**Lemma 4.6.** *Olkoon $f : E \mapsto F$ surjektio. Olkoon relaatio $R$ ekvivalenssirelaatio joukossa $E$ siten, että kaikille $x \in E$ on ekvivalenssiluokka $[x] = \{y \in E : \ f(x) = f(y)\}$. On olemassa yksiselitteinen bijektio $g : E/R \mapsto F$ jolle pätee*

$$g \circ \varphi = f.$$

*Todistus.* Koska $R$ on ekvivalenssrelaatio $[x] = [y]$ jos ja vain jos $xRy$ ja koska $f$ on surjektio, niin kuvaus $g : \ [x] \mapsto f(x)$ on selvästi hyvin määritelty bijektio joukosta $E/R$ joukolle $F$. Selvästi $g \circ \varphi_R = f$ ja $g$ on ainoa funktio joka toteuttaa annetun ehdon. □

Korollaari 4.7 on seurausta yleisemmistä tuloksista, lauseista 4.8 ja 4.13. Se oli kuitenkin Galois'n alkuperäisessä kirjassa itsenäisenä lemmana lauseen 4.13 sijasta, luonnostellun todistuksen saattelemana, minkä vuoksi se esitetään tässä niiden edellä.

**Korollaari 4.7.** *Olkoon $L$ kunnan $K$ ensimmäisen asteen juurilaajennos,*

$$L = K(u) \text{ jossa } u^p = a$$

*jollekin alkuluvulle $p$ ja jollekin $a \in K$ joka ei itse ole $p$. potenssi kunnassa $K$. Jos $K$ sisältää $p$. alkeisykkösjuuren, niin $G_L(f)$ on ryhmän $G_K(f)$ normaali aliryhmä ja indeksi $(G_K(f) \ : \ G_L(f))$ on joko $1$ tai $p$.*

*Todistus.* Väite on korollaari lauseista 4.8 ja 4.13, joten sovelletaan niiden tuloksia jaottomaan polynomiin

$$t(x) = x^p - a.$$

Koska kunta $K$ sisältää $p$. alkeisykkösenjuuren $\zeta$, niin kun siihen lisätään $u$, joka on yhtälön $t(x) = 0$ juuri, on kuntaan itseasiassa lisätty kaikki yhtälön juuret, sillä loput niistä ovat muotoa $\zeta u, \zeta^2 u, \ldots, \zeta^{p-1} u$. Näin ollen

$$L = K(u) = K(u, \zeta u, \zeta^2 u, \ldots, \zeta^{p-1} u)$$

Ja siksi $G_L(f)$ on Galoisryhmän $G_K(f)$ aliryhmä ja lauseen 4.8 nojalla indeksi $(G_K(f) \ : \ G_L(f))$ on joko 1 tai $p$ ja lauseen 4.13 nojalla sen normaali aliryhmä. □

Lauseiden 4.8 ja 4.13 todistuksissa käytetään apupolynomia $g(x)$ ja sen juuria $u_1, \ldots, u_t$. Olkoon polynomi $g(x)$ jaoton kunnassa $K$ ja sen asteluku on $t$, joten sillä on erilliset juuret $u_1, \ldots, u_t$ eli joille $u_i \neq u_j$ kun $i \neq j$. Nyt tarkastellaan, mitä polynomiyhtälön $f(x) = 0$ Galoisryhmille tapahtuu kun ryhdytään lisäämään kuntaan $K$, jossa molempien kertoimet ovat, polynomin $g(x)$ juuria.

**Lause 4.8.** *Olkoon $f(x)$ polynomi, jonka kertoimet ovat kunnassa $K$ ja jonka asteluku on $n$ ja jolla on $n$ juurta $r_1, \ldots, r_n$. Nyt*

$$t = k(G_K(f) \ : \ G_{K(u_1)}(f)) \quad \textit{missä } k \in \mathbb{N}_+,$$

*missä $t$ on edellä esitetyn apupolynomin $g(x)$ asteluku.*

*Todistus.* Olkoon $V$ yhtälön $f(x) = 0$ Galoisresolventti, kunnan $K$ suhteen. Se on myös yhtälön Galoisresoventti kunnan $K(u_1)$ suhteen. Olkoon $\theta$ sen minimipolynomi kunnan $K(u_1)$ suhteen ja vastaavasti $\pi$ kunnan $K$ suhteen. Nyt korollaarin 3.37 nojalla $\deg \pi = |G_K(f)|$ ja $\deg \theta = |G_{K(u_1)}(f)|$ joten nyt väite voidaan kirjoittaa muodossa

$$k \frac{\deg \pi(x)}{\deg \theta(x)} = t \quad \textit{missä } k \in \mathbb{N}_+.$$

Nyt lemman 3.33 nojalla tiedetään, että mimipolynomi $\theta(x)$ jakaa minimipolynomin $\pi(x)$. Olkoon

$$\pi(x) = \theta(x)\lambda(x) \tag{4.9}$$

jollekin polynomille $\lambda(x)$, jonka kertoimet ovat kunnassa $K(u_1)$. Olkoon myös

$$\theta(x) = x^r + b_{r-1}x^{r-1} + \cdots + b_1 x + b_0.$$

Koska $b_0, \ldots, b_{r-1} \in K(u_1)$, niin niille on polynomiesitys alkion $u_1$ avulla lemman 3.34 nojalla, joten olkoon

$$b_i = \theta_i(u_1) \quad kun\ i = 1, \ldots, r-1,$$

missä $\theta_i(y)$ on jokin polynomi, jonka kertoimet ovat kunnassa $K$. Määritetään kahden muuttujan polynomi $\Theta(x, y)$, jonka kertoimet ovat kunnassa $K$ seuraavasti

$$\Theta(x, y) = x^r + \theta_{r-1}(y)x^{r-1} + \cdots + \theta_1(y)x + \theta_0(y),$$

joten

$$\Theta(x, u_1) = \theta(x).$$

Vastaavasti rakennetaan polynomille $\lambda(x)$ kahden muuttujan polynomi $\Lambda(x, y)$, jolle

$$\Lambda(x, u_1) = \lambda(x)$$

Nyt yhtälö (4.9) voidaan kirjoittaa

$$\pi(x) = \Theta(x, u_1)\Lambda(x, u_1),$$

josta saadaan lemman 4.12 avulla

$$\pi(x) = \Theta(x, u_i)\Lambda(x, u_i), \quad kun\ i = 1, \ldots t.$$

tästä seuraa, että

$$\pi(x)^t = \Theta(x, u_1) \cdots \Theta(x, u_t)\Lambda(x, u_1) \cdots \Lambda(x, u_t) \tag{4.10}$$

joka on yhden muuttujan polynomi, jonka kertoimet löytyvät kunnasta $K(u_1, \ldots, u_t)$.

Itse asiassa kaavassa (4.10) esiintyvän tulon kertoimet löytyvät kaikki kunnasta $K$. Koska polynomi

$$\Theta(x, y_1) \cdots \Theta(x, y_t)$$

on selvästi symmetrinen muuttujien $y_1, \ldots, y_t$ suhteen, joten voidaan se esittää polynomina käyttäen muuttujina $x$ sekä symmetrisiä alkeispolynomeja muuttujille $y_1, \ldots, y_t$. Siksi kun sijoitamme juuret $u_1, \ldots, u_t$ muuttujien $y_1, \ldots, y_t$ paikalle niin saadaan polynomi, jonka kertoimet voidaan laskea apupolynomin $g(x) = 0$ kertoimista ja jonka juuret ovat $u_1, \ldots, u_t$. Koska polynomin $g(x)$ kertoimet ovat kunnassa $K$, niin sama pätee myös polynomille

$$\Theta(x, u_1) \cdots \Theta(x, u_t),$$

kuten väitimme.

Yhtälöstä (4.10) nähdään, että tämä tulo jakaa polynomin $\pi(x)^t$. Koska $\pi(x)$ on jaoton kunnassa $K$, seuraa siis

$$\Theta(x,u_1)\cdots\Theta(x,u_t) = \pi(x)^k \quad kun\ k \in \{1,\ldots,t\}. \tag{4.11}$$

Kun verrataan yhtälön puolten astelukuja niin saadaan $tr = k\deg\pi(x)$ ja koska $\deg\theta = r$

$$k\frac{\deg\pi(x)}{\deg\theta(x)} = t.$$

□

**Lemma 4.12.** *Olkoon $\pi(x)$ jaoton polynomi kunnassa $K$ ja olkoon $L$ kunnan $K$ laajennos, joka sisältää kaikki polynomin $\pi(x)$ juuret. Olkoot lisäksi $f(x,y)$,$g(x,y)$ ja $h(x,y)$ kahden muuttujan polynomeja, joiden kertoimet ovat kunnassa $K$. Jos jollekin polynomin $\pi(x)$ juurelle $V \in L$ pätee*

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

*niin kaikille polynomin $\pi(x)$ juurille $W$ pätee*

$$f(x,W) = g(x,W)h(x,W).$$

*Todistus.* Jos pidetään polynomeja $f(x,y)$ ,$g(x,y)$ ja $h(x,y)$ yhden muuttujan polynomeina joiden kertoimet ovat kunnassa $K(y)$, niin voidaan kirjoittaa

$$f(x,y) - g(x,y)h(x,y) = c_r(y)x^r + \cdots + c_0(y)$$

missä $c_r(y),\ldots,c_0(y)$ ovat yhden muuttujan polynomeja, joiden kertoimet ovat kunnassa $K$. Oletuksesta $f(x,V) = g(x,V)h(x,V)$ seuraa, että

$$c_i(V) = 0, \quad kun\ i = 1,\ldots,r,$$

joten lemman 3.38 mukaan

$$c_i(W) = 0, \quad kun\ i = 1,\ldots,r,$$

kaikille polynomin $\pi(x)$ juurille $W$, josta seuraa alkuperäinen väitteemme. □

Galois korvasi lemmana toimineen korollaarin 4.7 myöhemmässä käsikirjoituksessaan seuraavalla yleisemmällä tuloksella. Ilmeisesti kohtalokkaan kaksintaistelun aattona Galois kirjoitti lauseen kohdalle kommentin: ”Joku vielä löytää todistuksen”.

**Lause 4.13.** *Galoisryhmä $G_{K(u_1,\ldots,u_t)}(f)$ on Galoisryhmän $G_K(f)$ normaali aliryhmä, eli jos $\sigma \in G_K(f)$ ja $\tau \in G_{K(u_1,\ldots,u_t)}(f)$ niin*

$$\sigma \circ \tau \circ \sigma^{-1} \in G_{K(u_1,\ldots,u_t)}(f).$$

*Todistus.* Olkoon $V$ polynomiyhtälön $f(x) = 0$ Galoisresolventti kunnan $K$ suhteen ja samalla myös kunnan $K(u_1, \ldots, u_t)$ suhteen. Olkoon $\varphi(x)$ sen minimipolynomi kunnan $K(u_1, \ldots, u_n)$ suhteen ja vastaavasti $\pi(x)$ sen minimipolynomi kunnan $K$ suhteen. Lisäksi olkoot murtolausekkeet $q_1(x), \ldots, q_n(x)$, joiden kertoimet ovat kunnassa $K$ siten, että

$$r_i = q_i(V), \quad kun\ i = 1, \ldots, n.$$

Nyt kaikki permutaatiot $\tau \in G_{K(u_1,\ldots,u_t)}(f)$ ovat muotoa

$$\tau : \ r_i = q_i(V) \mapsto q_i(V'), \quad kun\ i = 1, \ldots, n, \tag{4.14}$$

missä $V'$ on polynomin $\varphi(x)$ juuri.

Määritelmän 3.23 perusteella permutaatio $\sigma \in G_K(f)$ voidaan laajentaa kunnan $K(r_1, \ldots, r_n)$ automorfismiksi, joka kuvaa kunnan $K$ alkiot itselleen. Kun käytämme automorfismia $\sigma$ yhtälön

$$\pi(V) = 0$$

molempiin puoliin, saamme

$$\pi(\sigma(V)) = 0.$$

Näin ollen $\sigma(V)$ on polynomin $\pi(x)$ juuri, ja lauseen 3.36 nojalla jokainen polynomin $f(x)$ juuri $r_1, \ldots, r_n$ voidaan esittää murtolausekkeena käyttäen alkiota $\sigma(V)$. Toisin sanoen myös $\sigma(V)$ on yhtälön $f(x) = 0$ Galoisresolventti kunnassa $K$ ja tietenkin samalla myös kunnan $K(u_1, \ldots, u_t)$ suhteen.

Tarkastellaan alkiota $\sigma(V)$ Galoisresolventtinä kunnassa $K(u_1, \ldots, u_t)$. Kaavasta (4.14) seuraa, että

$$\sigma \circ \tau \circ \sigma^{-1} : \ q_i(\sigma(V)) \mapsto q_i(\sigma(V')).$$

Osoittaaksemme, että $\sigma \circ \tau \circ \sigma^{-1} \in K(u_1, \ldots, u_t)$, riittää osoittaa, että $\sigma(V')$ on yksi alkion $\sigma(V)$ minimipolynomin (kunnassa $K(u_1, \ldots, u_t)$) juurista.

Olkoon $W$ polynomin $g(x) = 0$ Galoisresolventti ja olkoot $W_1, \ldots, W_s$ sen minimipolynomin kunnan $K$ suhteen juuret, joista $W$ on yksi. Korollaarin 3.35 perusteella

$$K(u_1, \ldots, u_t) = K(W) = K(W_1, \ldots, W_s).$$

Koska $W$ voi olla mikä tahansa juurista $W_1, \ldots, W_s$, niin saadaan

$$K(u_1, \ldots, u_t) = K(W_i), \quad \textit{kaikille } i = 1, \ldots, s.$$

Näin ollen kuntalaajennosta $K(u_1, \ldots, u_t)$ voidaan pitää kunnan $K$ laajennoksena, jossa siihen lisätään yksi olio $W_1$. Nyt toistaen lauseen 4.8 todistuksessa käytettyä menetelmää muodostetaan sellainen kahden muuttujan polynomi $\Phi(x, y)$, jonka kertoimet ovat kunnassa $K$, siten että

$$\varphi(x) = \Phi(x, W_1)$$

polynomin $\varphi(x)$ kertoimet ovat kunnassa $K(u_1, \ldots, u_t)$. Jatkettaessa lauseen 4.8 todistuksen mukailua saadaan yhtälön (4.14) kaltainen yhtälö, tarkemmin sanottuna

$$\Phi(x, W_1) \cdots \Phi(x, W_s) = \pi(x)^l$$

jollekin $l \in \{1, \ldots, s\}$. Koska $\sigma(V)$ on polynomin $\pi(x)$ juuri, niin tästä yhtälöstä huomataan, että $\sigma(V)$ on myös jonkin tekijän $\Phi(x, W_k)$ juuri.

Osoittaaksemme, että $\Phi(x, W_k)$ on alkion $\sigma(V)$ minimipolynomi kunnassa $K(u_1, \ldots, u_t)$, riittää osoittaa, että se on jaoton. Jos se hajoaa tekijöihin kunnassa $K(u_1, \ldots, u_t)$, niin koska $K(u_1, \ldots, u_t) = K(W_k)$, se voidaan kirjoittaa tekijöihin hajoitettuna

$$\Phi(x, W_k) = \Gamma(x, W_k)\Delta(x, W_k)$$

missä $\Gamma(x, y)$ ja $\Delta(x, y)$ ovat kahden muuttujan polynomeja, joiden kertoimet ovat kunnassa $K$. Nyt lemman 4.12 nojalla

$$\Phi(x, W_1) = \Gamma(x, W_1)\Delta(x, W_1).$$

Koska $\phi(x, W_1) = \varphi(x)$, niin se on jaoton ja edellinen tekijöihin jako on triviaali samoin kuin polynomin $\Phi(x, W_k)$ jako tekijöihin. Näin ollen polynomi $\Phi(x, W_k)$ on alkion $\sigma(V)$ minimipolynomi kunnassa $K(u_1, \ldots, u_t)$.

Nyt pitää enää osoittaa, että $\sigma(V')$ on polynomin $\Phi(x, W_k)$ juuri, kuten $\sigma(V)$, olettaen, että $V'$ on polynomin $\Phi(x, W_1)$ juuri kuten V.

Korollaarin 3.35 nojalla $K(r_1, \ldots, n_n) = K(V)$, joten saadaan

$$V' = s(V) \tag{4.15}$$

jollekin murtolausekkeelle $s(x)$, jonka kertoimet ovat kunnassa $K$. Lemman 3.34 perusteella voidaan valita $s(x)$ siten, että se on polynomi, jonka kertoimet ovat kunnassa $K$. Koska $\Phi(V', W_1) = 0$, saadaan

$$\Phi(s(V), W_1) = 0$$

joten $V$ on polynomin $\Phi(x, W_1)$ juuri. Lemman 3.33 nojalla polynomi $\Phi(x, W_1)$ jakaa polynomin $\Phi(s(x), W_1)$. Olkoon

$$\Phi(s(x), W_1) = \Phi(x, W_1)\Psi(x, W_1)$$

jollekin polynomille $\Psi(x, y)$ jonka kertoimet ovat kunnassa $K$. Lemma 4.12 puolestaan osoittaa meille, että koska

$$\Phi(s(x), W_k) = \Phi(x, W_k)\Psi(x, W_k)$$

ja koska $\sigma(V)$ on polynomin $\Phi(x, W_k)$ juuri, niin silloin

$$\Phi(s(\sigma(V)), W_k) = 0.$$

Nyt kun vielä käytetään kuvausta $\sigma$ yhtälön (4.15) molempiin puoliin, niin saadaan

$$\sigma(V') = s(\sigma(V)),$$

josta näemme, että $\sigma(V')$ on polynomin $\Phi(x, W_k)$ juuri, mikä pitikin osoittaa. □

**Lemma 4.16.** *Olkoon $N$ Galoisryhmän $G_K(f)$ aliryhmä siten, että $(G_K(f) : N) = p$ missä $p$ on alkuluku. Jos $K$ sisältää $p$. alkeisykkösenjuuren, niin on olemassa kunnan $K$ juurilaajennos $L \subset K(r_1, \ldots, r_n)$, joka on muotoa*

$$L = K(a^{1/p})$$

*jollekin $a \in K$ siten, että*

$$G_L(f) = N.$$

*Todistus.* Aloitetaan ottamalla permutaatio $\sigma \in G_K(f)$, joka ei kuulu aliryhmään $N$. Sitten edetään useammassa vaiheessa.

*Vaihe 1* Olkoon $x \in K(r_1 \ldots, r_n)$ siten, että $\upsilon(x) = x$ kaikilla $\upsilon \in N$. Väitetään että:

- Jos $\sigma(x) = x$, niin $x \in K$.
- Jos $\sigma(x) \neq x$, ja jos $\tau \in G_K(f)$ siten, että $\tau(x) = x$, niin $\tau \in N$.

Olkoon $X \subset G_K(f)$ niiden permutaatioiden joukko, joiden suhteen $x$ on invariantti, eli

$$X = \{\tau \in G_K(f) | \tau(x) = x\}.$$

Joukko $X$ muodostaa selvästi ryhmän, jolle oletuksen nojalla

$$G_K(f) \supset X \supset N$$

ja koska oletuksen nojalla $(G_K(f) \,:\, N) = p$, saadaan lemman 4.17 nojalla

$$X = N \qquad \text{tai} \qquad X = G_K(f).$$

Jos $\sigma(x) = x$, niin $\sigma \in X$ joten $X \neq N$ koska $\sigma \notin N$. Nyt siis $X = G_K(f)$, joten määritelmän 3.23 mukaan $x \in K$.

Jos $\sigma(x) \neq x$, niin $\sigma \notin X$ joten $X \neq G_K(f)$ ja näin ollen $X = N$ eli kaikki permutaatiot, joiden suhteen $x$ on invariantti, kuuluvat joukkoon $N$.

*Vaihe 2* On olemassa kunnan $K(r_1, \ldots, r_n)$ jäsen $v$, joka on invariantti kaikissa permutaatioissa $\rho \in N$, muttei kuulu kuntaan $K$.

Olkoon $p(x_1, \ldots, x_n)$ polynomi, jonka kertoimet ovat kunnassa $K$ ja jolla on seuraava ominaisuus: ne $n!$ kunnan $K(r_1, \ldots, r_n)$ jäsentä, jotka saadaan sijoittamalla $r_1, \ldots, r_n$ kaikilla mahdollisilla tavoilla polynomin $p(x_1, \ldots, x_n)$ muuttujien paikoille, ovat keskenään erillisiä. Olkoon $V = p(r_1, \ldots, r_n)$. Huomataan että $V$ on Galoisresolventti (määritelmä 3.26) polynomiyhtälölle $f(x) = 0$ kunnan $K$ suhteen, joten sen minipolynomin aste on korollaarin 3.37 mukaan yhtäsuuri kuin Galoisryhmän $G_K(f)$ mahtavuus. Katsotaan polynomia

$$\prod_{\rho \in N} (x - \rho(V)).$$

Tämän polynomin kertoimet ovat selvästi invariantteja permutaatiojoukossa $N$. Jos ne olisivat kaikki kunnassa $K$, niin $V$ olisi $|N|$-asteisen polynomin juuri kunnassa $K$. Tämä on mahdotonta, sillä minimipolynomi alkiolle $V$ on korkeampaa astetta kuin $|N|$. Näin ollen sillä täytyy olla ainakin yksi kerroin, joka on invariantti permutaatiojoukossa $N$ mutta joka ei kuuluu kuntaan $K$. Tämä kerroin voidaan valita edellä esitellyksi kunnan $K(r_1, \ldots, r_n)$ jäseneksi $v$.

Jokaiselle $p$. ykkösenjuurelle $\omega \in F$ määritellään Lagrangen-resolventti

$$t(\omega) = v + \omega\sigma(v) + \cdots + \omega^{p-1}\sigma^{p-1}(v).$$

*Vaihe 3* Osoitetaan, että $\sigma(t(\omega)) = \omega^{-1}t(\omega)$ ja $\rho(t(\omega)) = t(\omega)$ kaikilla $\rho \in N$.

Koska ykkösenjuuren $\omega$ potenssit ovat kunnassa $K$ ja siten määritelmän 3.23 perusteella invariantteja kaikissa $\sigma \in G_K(f)$, joten

$$\sigma(t(\omega)) = \sigma(v) + \omega\sigma^2(v) + \cdots + \omega^{p-1}\sigma^p(v)$$

joka voidaan esittää myös

$$\sigma(t(\omega)) = \omega^{-1}(\sigma^p(v) + \omega\sigma(v) + \cdots + \omega^{p-1}\sigma^{p-1}(v)),$$

ja

$$\rho(t(\omega)) = \rho(v) + \omega\rho\sigma(v) \cdots + \omega^{p-1}\rho\sigma^{p-1}(v),$$

kaikille $\rho \in N$.

Lauseen 4.18 nojalla $\sigma^p \in N$ joten $\sigma^p(v) = v$ josta seuraa suoraan

$$\sigma(t(\omega)) = \omega^{-1}t(\omega).$$

Toisaalta, koska $N$ on Galoisryhmän $G_K(f)$ normaali aliryhmä, saadaan

$$\sigma^{-i} \circ \rho \circ \sigma^i \in N \quad \textit{kaikille } \rho \in N \textit{ ja kaikille } i = 0, \ldots, p-1$$

josta saadaan

$$\sigma^{-i} \circ \rho \circ \sigma^i(v) = v \quad \textit{kaikille } \rho \in N \textit{ ja kaikille } i = 0, \ldots, p-1.$$

Nyt käytetään permutaatiota $\sigma^i$ yhtälön molempiin puoliin, niin saadaan

$$\rho \circ \sigma^i(v) = \sigma^i(v) \quad \textit{kaikille } \rho \in N \textit{ ja kaikille } i = 0, \ldots, p-1$$

joten

$$\rho(t(\omega)) = t(\omega) \quad \textit{kaikille } \rho \ \in N.$$

*Vaihe 4* Kaikille $p$. ykkösenjuurille $\omega$ pätee $t(\omega)^p \in K$ ja on $p$. ykkösenjuuri $\omega \neq 1$ siten, että $t(\omega) \neq 0$.

Vaiheesta 3 seuraa, että $t(\omega)^p$ on invariantti permutaation $\sigma$ suhteen ja kaikkien joukkoon $N$ kuuluvien permutaatioiden suhteen. Vaiheessa 1 osoitettiin, että tällöin $t(\omega)^p$ kuuluu kuntaan $K$.

Jos oletetaan, että $t(\omega) = 0$ kaikille $p$. ykkösenjuurille $\omega \neq 1$ niin Lagrangen kaavasta

$$v = \frac{1}{p}(\sum_{\omega} t(\omega))$$

saadaan

$$v = \frac{1}{p}t(1)$$

ja tästä yhtälöstä huomataan, vaiheen 3 nojalla, että $v$ on invariantti permutaation $\sigma$ suhteen. Koska se on invariantti myös joukon $N$ permutaatioiden suhteen, seuraa, vaiheen 1 nojalla, että $v$ kuuluu kuntaan $K$, mikä on ristiriita, sillä $v$ valitiin kunnan $K$ ulkopuolelta vaiheessa 2.

Nyt siis olkoon $\omega$ $p$. ykkösenjuuri siten, että $\omega \neq 1$ ja $t(\omega) \neq 0$, ja olkoon

$$L = K(t(\omega)).$$

Vaihe 4 ja lause 2.5 osoittavat, että $L$ on kunnan $K$ juurilaajennos, muotoa $K(a^{1/p})$. Nyt alkuperäisen väitteen todistamiseksi tarvitsee enää osoittaa, että $G_L(f) = N$.

*Vaihe 5* Osoitetaan, että $G_L(f) = N$. Koska $t(\omega) \neq 0$ ja $\omega \neq 1$, vaihe 3 osoittaa, ettei $t(\omega)$ ole invariantti permutaatiossa $\sigma$. Näin ollen $L \neq K$, joten se on ensimmäisen asteen juurilaajennos kunnasta $K$. Korollaarin 4.7 nojalla

$$\frac{|G_K(f)|}{|G_L(f)|} = p \Rightarrow |G_L(f)| = |N|.$$

Lisäksi, koska $\sigma(t(\omega)) \neq t(\omega)$, vaihe 1 osoittaa, että jokainen permutaatio Galoisryhmässä $G_K(f)$, jonka suhteen $t(\omega)$ on invariantti, kuuluu ryhmään $N$. Koska $t(\omega) \in L$, Galoisryhmän $G_L(f)$ permutaatiot jättävät alkion $t(\omega)$ invariantiksi, joten

$$G_L(f) \subseteq N.$$

Koska $N$ ja $L$ ovat saman kokoisia, saadaan että

$$G_L(f) = N.$$

□

**Lemma 4.17.** *Olkoon $G_1 \supset G_2 \supset G_3$ ketju aliryhmiä. Jos $G_1$ on äärellinen niin*

$$(G_1 \,:\, G_3) = (G_1 \,:\, G_2)(G_2 \,:\, G_3)$$

*Erityisesti , jos $(G_1 \,:\, G_3) = p$, missä $p$ on alkuluku, niin joko $G_1 = G_2$ tai $G_2 = G_3$.*

*Todistus.* Väite seuraa suoraan laskusta

$$\frac{|G_1|}{|G_3|} = \frac{|G_1|}{|G_2|} \cdot \frac{|G_2|}{|G_3|}.$$

□

**Lause 4.18.** *Olkoon $N$ äärellisen ryhmän $G$ normaali aliryhmä siten, että $|G|/|N| = p$, missä $p$ on alkuluku. Jos $\sigma \in G$ mutta $\sigma \notin N$, niin $\sigma^p \in N$.*

*Todistus.* Tarkastellaan sivuluokkia

$$N, \sigma N, \ldots, \sigma^p N,$$

joita on $p + 1$ kappaletta. Koska jokaisen sivuluokan koko on $|N|$ ja koska $(p+1) \cdot |N| > |G|$, täytyy löytyä kokonaisluvut $m$ ja $n$, joille $0 \leq m < n \leq p$ ja

$$\sigma^m N = \sigma^n N.$$

Lemman 4.19 nojalla saadaan

$$\sigma^{n-m} \in N.$$

Tarkastellaan pienintä kokonaislukua $k > 0$ jolle $\sigma^k \in N$. Edellä on osoitettu, että sille löytyy yläraja $k \leq p$. Nyt riittää osoittaa, että $k \geq p$. Tämä tehdään osoittamalla, että kaikki aliryhmän $N$ sivuluokat ryhmässä $G$ ovat jokin seuraavista:

$$N, \sigma N, \ldots, \sigma^{k-1} N.$$

Tästä nähdään, että $|G|/|N| = p \leq k$. Olkoon $H = \{\sigma^i | i \in \mathbb{Z}\}$. Tämä on selvästi ryhmän $G$ aliryhmä ja koska $\sigma \notin N$, seuraa, että $H \cdot N \neq N$. Lemmasta 4.20 seuraa, että $H \cdot N = G$ ja että jokainen ryhmän $N$ sivuluokka on muotoa $\sigma^i N$ jollekin $i \in \mathbb{Z}$. Euklideen jakoalgoritmillä saadaan $i = kq + r$ joillekin kokonaisluvuille $q$ ja $r$, missä $0 \leq r < k$. Nyt siis

$$\sigma^{i-r} = (\sigma^k)^q \in N,$$

Tästä taas lemman 4.19 avulla saadaan

$$\sigma^i N = \sigma^r N,$$

josta väitteemme seuraa, sillä $r$ oli välillä $0, \ldots, k-1$. □

**Lemma 4.19.** *$\sigma H = \tau H$ jos ja vain jos $\sigma^{-1}\tau \in H$.*

*Todistus.* Jos $\sigma H = \tau H$, niin $\tau \cdot 1 \in \sigma H$, joten $\tau = \sigma\xi$ jollekin $\xi \in H$ ja

$$\sigma^{-1}\tau = \xi \in H.$$

Toisaalta, jos $\sigma^{-1}\tau \in H$ niin yhtälö

$$\sigma\xi = \tau((\sigma^{-1}\tau)^{-1}\xi) \quad kun\ \xi \in H$$

osoittaa, että $\sigma H \subset \tau H$ ja vastaavasti yhtälö

$$\tau\xi = \sigma((\sigma^{-1}\tau)\xi) \quad kun\ \xi \in H$$

osoittaa, että $\tau H \subset \sigma H$. □

**Lemma 4.20.** *Olkoon ryhmät $H$ ja $N$ ryhmän $G$ aliryhmiä, ja määritellään ryhmän $G$ osajoukko $H \cdot N$ seuraavasti:*

$$H \cdot N = \{\xi\nu | \xi \in H, \nu \in N\}.$$

*Jos $N$ on ryhmän $G$ normaali aliryhmä, niin $H \cdot N$ aliryhmä ryhmälle $G$ ja $H \cap N$ on normaali aliryhmä ryhmälle $H$. Jos lisäksi $|G|/|N| = p$, missä $p$ on alkuluku, ja $G$ on äärellinen niin joko $H \cdot N = N$ tai $H \cdot N = G$.*

*Jos $H \cdot N = N$, niin $H \subset N$, joten $H \cap N = H$.*

*Jos $H \cdot N = G$, niin kaikki ryhmän $N$ sivuluokat ryhmässä $G$ ovat muotoa $\xi N$ jollekin $\xi \in H$.*

*Todistus.* Leikkauksen $H \cap N$ normaalius ryhmän $H$ aliryhmänä seuraa suoraan siitä, että $N$ on sen normaali aliryhmä. Samoin voidaan helposti tarkistaa, että $H \cdot N$ on aliryhmä ryhmälle $G$:

Sen neutraalialkio 1 kuuluu molempiin ryhmiin $H$ ja $N$, joten niiden tulo $1 \cdot 1 = 1 \in H \cdot N$.

Ryhmä $H \cdot N$ on suljettu laskutoimituksensa suhteen, koska alkioille $\xi_1, \xi_2 \in H$ ja $\nu_1, \nu_2 \in N$ pätee

$$(\xi_1\nu_1)(\xi_2\nu_2) = (\xi_1\xi_2)((\xi_2^{-1}\nu_1\xi_2)\nu_2),$$

missä $(\xi_2^{-1}\nu_1\xi_2) \in N$, sillä $N$ on ryhmän $G$ normaali aliryhmä.

Lopuksi tarkistetaan, että $H \cdot N$ sisältää kaikille alkioilleen vasta-alkiot. Nyt mielivaltaisille alkioille $\xi \in H$ ja $\nu \in N$,

$$(\xi\nu)^{-1} = \xi^{-1}(\xi\nu^{-1}\xi^{-1}) \in N.$$

Ollaan siis saatu ketju aliryhmiä

$$G \supset H \cdot N \supset N.$$

Jos $|G|/|N| = p$ niin lemman 4.17 nojalla joko $H \cdot N = N$ tai $H \cdot N = G$. Ensimmäisessä tapauksessa $H \subset N$, sillä $H$ sisältyy ryhmään $H \cdot N$. Jälkimmäisessä tapauksessa voidaan löytää jokaiselle alkiolle $\sigma \in G$, sellaiset alkiot $\xi \in H$ ja $\nu \in N$, että

$$\sigma = \xi\nu.$$

Nyt lemman 4.19 avulla saadaan

$$\sigma N = \xi N,$$

eli kaikki ryhmän $N$ sivuluokat ovat haluttua muotoa. □

Nyt lopuksi palataan huomautuksessa 4.2 mainittuun väitteeseen, ettei jaottomilla polynomeilla ole kuin yksöisjuuria.

**Lause 4.21.** *Jos polynomi $f(x)$ on jaoton kunnassa $K = \mathbb{Q}$ , niin sen juuret kaikissa kunnan $K$ kuntalaajennoksissa $L$ ovat yksöisjuuria.*

*Todistus.* Koska $f(x)$ on jaoton ja $\partial f(x)$ sen derivaatta (muutujan $x$ suhteen). Koska $f(x)$ on jaoton ja $\partial f(x)$ matalampaa astetta, niin $syt(f(x), \partial f(x)) = 1$, joten $f(x)$ on lemman 4.22 tarkoittama $f_s(x)$, jolla on vain yksöisjuuria. □

**Lemma 4.22.** *Olkoon $L$ kunnan $K$ mielivaltainen kuntalaajennos. Polynomi $f_s(x)$ määritellään seuraavasti $f_s(x) = \dfrac{f(x)}{g(x)}$ missä $g(x)$ on polynomin $f(x)$ ja sen derivaatan $\partial f(x)$ suurin yhteinen tekijä. Polynomin $f_s(x)$ juuret kunnassa $K$ ovat samat kuin polynomin $f(x)$ ja kaikki polynomin $f_s(x)$ juuret ovat yksöisjuuria.*

*Todistus.* Koska $f_s(x)$ on polynomin $f(x)$ tekijä, niin selvästi kaikki sen juuret ovat myös polynomin $f(x)$ juuria. Olkoon $a \in K$ jokin polynomin $f(x)$ juurista. Sanotaan että juuri $a$ on polynomin $f(x)$ $m$-kertainen juuri, kun $m$ on suurin kokonaisluku, jolle $(x-a)^m$ jakaa polynomin $f(x)$. Lemman 4.23 nojalla tiedetään, että $(x-a)^{m-1}$ on korkein binomin $(x-a)$ potenssi, joka jakaa polynomit $\partial f(x)$ ja $f(x)$. Näin ollen se on myös korkein binomin $(x-a)$ potenssi, joka jakaa polynomin $g(x)$. Nyt siis $(x-a)$ jakaa polynomin $f_s(x)$, mutta $(x-a)^2$ ei niin tee, joten $a$ on polynomin $f_s(x)$ yksöisjuuri. □

**Lemma 4.23.** *Olkoon $K = \mathbb{Q}$. Olkoon $f(x)$ polynomi, jonka kertoimet ovat kunnassa $K$ siten, että $f(x) \neq 0$ kaikilla $x \in K$ ja $a \notin K$ sen juuri. Olkoon $m$ suurin kokonaisluku, jolle $(x-a)^m$ jakaa polynomin $f(x)$. Nyt $m-1$ on korkein binomin $(x-a)$ potenssi, joka jakaa polynomin $f(x)$ derivaatan $\partial f(x)$.*

*Todistus.* Koska $(x-a)^m$ jakaa polynomin $f(x)$, voidaan se kirjoittaa muotoon $f(x) = (x-a)^m g(x)$, missä $g(x)$ on polynomi jonka kertoimet ovat kunnassa $K$, joka ei ole jaollinen binomilla $(x-a)$. Nyt derivointikaavoilla saadaan

$$\partial f(x) = (x-a)^{m-1}(m \cdot g(x) + (x-a)\partial g(x)),$$

nyt koska kunta $K = \mathbb{Q}$, niin ei ole kokonaislukua $m \neq 0$, jolle $m \cdot g(x) = 0$. Nyt, koska binomi $(x-a)$ ei jaa polynomia $g(x)$, huomataan, että $m-1$ on korkein binomin $(x-a)$ potenssi, joka jakaa derivaatan $\partial f(x)$. □

Kun Galois ja Abel sekä muut 1800-luvun alun matemaatikot painivat ratkeavuuden kanssa, ei heillä ollut työkaluna nykyiseen tapaan hyvin määriteltyjä reaalilukuja, vaan heille peruskuntana $K$ toimi rationaalilukujen kunta. Onneksi ei tarvitse kuitenkaan todistaa kaikkea tätä uudestaan esimerkiksi reaali- ja imaginääriluvuille, sillä seuraavan lauseen nojalla, jos $f(x) = 0$ on juurilausekkeilla ratkeava kunnassa $K$, on yhtälö sitä myös sen kuntalaajennoksessa $L$.

**Lause 4.24.** *Olkoon $f$ polynomi, jonka kertoimet ovat kunnassa $K \subset \mathbb{C}$. Jos $f(x) = 0$ on juurilausekkeilla ratkeava kunnassa $K$, niin se on juurilausekkeilla ratkeava kaikissa kunnissa $L$, jotka sisältävät kunnan $K$.*

*Todistus.* Olkoon $R$ kunnan $K$ juurilaajennos, joka sisältää polynomiyhtälön $f(x) = 0$ juuren $r$. Osoitetaan, että $R$ sisältyy johonkin kunnan $L$ juurilaajennokseen $S$.

Osoitetaan tämä induktiolla juurilaajennoksen $R$ korkeuden $h$ suhteen. Jos $h = 0$, niin $R = K$ ja voidaan valita $S = L$.

Jos $h = 1$, olkoon $R = K(u)$, missä $u^p = a$ jollekin $a \in K$, jolle $a \neq b^p$ millekään $b \in K$. Olkoon $M \subset \mathbb{C}$ polynomin $x^p - a$ juurikunta, joka sisältää kunnan $L$. Koska $u$ on polynomin $x^p - a$ juuri, niin $u \in M$ ja vielä lisäksi koska kaikki murtolausekkeet, jotka on rakennettu alkiosta $u$ ja kertoimista, jotka kuuluvat kuntaan $K$, eli siis juurilaajennos $R$, kuuluvat kuntaan $M$. Voidaan siis jatkossa olettaa, että $R$ on kunnan $M$ alikunta.

Jos $a \neq c^p$ millekään $c \in L$ niin $L(u)$ on kunnan $L$ juurilaajennos, jonka korkeus on 1, ja joka sisältää kunnan $R$, sillä se sisältää sekä alkion $u$ että kunnan $K$. Näin ollen se täyttää juurilaajennokselle $S$ asetetut ehdot.

Jos $a = c^p$ jollekin $c \in L$, niin koska $u^p = a = c^p$ saadaan

$$\left(\frac{u}{c}\right)^p = 1.$$

Näin ollen $u/c$ on $p$. ykkösenjuuri ja lauseen 3.13 nojalla löytyy kunnan $L$ juurilaajennos $S$ johon alkio $u/c$ kuuluu. Lisäksi koska $c \in L$, niin $u \in S$, josta edelleen saadaan $R \subset S$ ja näin ollen todistus on valmis tapauksessa $h = 1$.

Jos $h \geq 2$ seuraa väitteemme suoraan induktio-oletuksesta ja tapauksesta $h = 1$. Löydetään kunnan $R$ alikunta $R_1$, joka on $h-1$ korkuinen juurilaajennos kunnalle $K$ ja jolle $R$ on 1 korkuinen juurilaajennos. Induktio-oletuksen nojalla $R_1$ sisältyy kuntaan $S_1$, joka on kunnan $L$ juurilaajennos ja tapauksen $h = 1$ perusteella $R$ voidaan osoittaa kunnan $S$ alikunnaksi, joka vuorostaan on kunnan $S_1$ juurilaajennos. Näin ollen $S$ on kunnan $L$ juurilaajennos.

Näin ollen polynomiyhtälö $f(x) = 0$ on juurilausekkeilla ratkeava myös kunnassa $L$. □

# Luku 5

# Polynomiyhtälöiden Galoisryhmät

Kun on edellä osoitettu, että Galoisryhmien ratkeavuus kertoo meille sen, ovatko ne juurilausekkein ratkeavia, on tullut aika tarkastella, millaisia polynomiyhtälöiden Galoisryhmät itseasiassa ovat.

**Lause 5.1.** *Olkoon $f(x) = 0$ $n$. asteen polynomiyhtälö kunnassa $K$, silloin sen Galoisryhmä $G_K(f)$ on symmetrisen ryhmän $S_n$ aliryhmä.*

*Todistus.* Suoraan Galoisryhmän määritelmästä (määritelmä 3.23) huomataan, että $G_K(f) \subseteq S_n$. Samoin määritelmästä seuraa, että $G_K(f)$ on epätyhjä, sillä siihen kuuluu vähintään identiteettikuvaus $Id$. Laskutoimitusten suhteen se on suljettu, sillä juurten permutaatioiden yhdiste on juurten permutaatio. Käänteisalkioiden olemassa olo seuraa siitä, että jos juuret voidaan vaihtaa keskenään, niin ne voidaan vaihtaa molempiin suuntiin. □

Nyt kun on todettu polynomiyhtälöiden galoisryhmien olevan symmetristen ryhmien aliryhmiä, niin on aika katsoa milloin $G_K(f) = S_n$.

**Lause 5.2.** *Olkoon $K$ reaalilukujen alikunta. Jos $f(x)$ on $p$. asteen jaoton polynomi kunnassa $K$, jossa $p$ on alkuluku ja jos polynomilla $f(x)$ on tasan kaksi ei reaalista juurta kompleksitasossa, niin $G_K(f) = S_p$.*

*Todistus.* Olkoon $c_i \notin \mathbb{R}$ yksi polynomin $f(x)$ juurista. Koska polynomin $f(x)$ kertoimet ovat kaikki reaalisia, täytyy myös juuren $c_i$ kompleksikonjugaatin $\bar{c_i}$ olla polynomin $f(x)$ juuri ja siten $\bar{c_i} = c_j$ jollakin $j \in \{1, \ldots, p\}$ kun $j \neq i$. Olkoon $E$ polynomin $f(x)$ juurikunta, joka sisältyy kompleksitasoon. Otetaan kuvaus $\sigma$, joka kuvaa kompleksiluvut konjugaateilleen. Kuvaus $\sigma$ on selvästi $K$-automorfismi ja se kuvaa polynomin $f(x)$ juuret toisilleen seuraavasti $c_i \mapsto c_j$, $c_j \mapsto c_i$ ja $c_k \mapsto c_k$ kun $k \in \{1, \ldots, p\} \setminus \{i, j\}$. Toisin sanoen transpositio $(i, j)$ kuuluu yhtälön $f(x) = 0$ Galoisryhmään $G_K(f)$.

Koska $f(x)$ on jaoton kunnassa $K$, ovat kaikki sen juuret $c_n$, $n = 1, \ldots, p$ kunnan $K$ ulkopuolella. Löytyy $K$-automorfismi $\sigma_1 : K(c_i) \mapsto K(c_j)$ jolle $\sigma_1(c_i) = c_j$. Nyt tämä kuvaus $\sigma_1$ voidaan laajentaa $K$-automorfismiksi $\sigma : K(c_1, \ldots, c_p) \mapsto K(c_1, \ldots, c_p)$ ja tätä kuvausta $\sigma$ vastaava juurten permutaatio $\sigma_i \in G_K(f)$, jolle $\sigma_i(c_i) = c_j$.[1] Galoisryhmä $G_K(f)$ siis on niin sanottu transitiivinen permutaatioryhmä (Määritelmä 5.3).

Galoisryhmä $G_K(f)$ on siis transitiivinen permutaatioryhmä, jossa on ainakin yksi transpositio, joten lemman 5.4 nojalla $G_K(f) = S_p$. □

**Määritelmä 5.3.** Joukon $E$ permutaatioryhmää $H$ kutsutaan transitiiviseksi permutaatioryhmäksi jos kaikille $x, y \in E$ on olemassa $\sigma \in H$ jolle $\sigma(x) = y$.

**Lemma 5.4.** *Jos $p$ on alkuluku ja $H \subset S_p$ on joukon $\{1, \ldots, p\}$ alkioiden transitiivinen permutaatiojoukko, joka sisältää transposition $(a, b)$, niin $H = S_p$.*

*Todistus.* Olkoon $a \in 1, \ldots, p$ ja $M = \{j \in \{1, \ldots, p\} \mid j = a \text{ tai } (a, j) \in H\}$ ja olkoon $\sigma \in H$. Osoitetaan, että jos $\sigma(M) \cap M \neq \emptyset$ niin $\sigma(M) = M$. Oletetaan siis, että on olemassa $i \in M$ siten, että $\sigma(i) \in M$. Osoitetaan ensiksi, että $\sigma(a) \in M$. Selvästi nähdään, että jos $a = i$ tai $\sigma(a) = a$, niin $\sigma(a) \in M$. Näin ollen oletetaan, ettei $\sigma(a)$ ole $\sigma(i)$ tai $a$. Nyt koska $(a, i)$ ja $(a, \sigma(i))$ kuuluvat joukkoon $H$, saadaan myös $\tau \circ (a, i) \circ \tau^{-1} \in H$, missä $\tau = (a, \sigma(i)) \circ \sigma$. Koska $(a, i)$ on transpositio, saadaan

$$\tau \circ (a, i) \circ \tau^{-1} = (\tau(a), \tau(i)) \circ \tau = (\sigma(a), a) = (a, \sigma(a))$$

ja näin ollen $\sigma(a) = M$. Nyt olkoon $j$ mielivaltainen joukon $M$ jäsen. Osoitetaan, että $\sigma(j)$ kuuluu joukkoon $M$. Jos $j = a$ tai $\sigma(j) = a$, niin $\sigma(j) \in M$ edellä osoitetun nojalla. Näin ollen oletamme, ettei $\sigma(j)$ ole $\sigma(a)$ tai $a$. Nyt, koska $(a, j) \in H$ saamme myös $\rho \circ (a, j) \circ \rho^{-1} \in H$, jossa $\rho = (a, \sigma(a)) \circ \sigma$ tai $\rho = \sigma$ riippuen siitä, onko $\sigma(a) = a$ vai $\sigma(a) \neq a$. Nyt voidaan edetä kuten edellä ja huomaamme, että

$$\rho \circ (a, j) \circ \rho^{-1} = \rho(a), \rho(j)) = (a, \sigma(j))$$

joten $\sigma(j) \in M$. Näin ollen $\sigma(M) \subseteq M$. Koska $M$ on äärellinen ja koska $\sigma$ on joukon $\{1, \ldots, p\}$ alkioiden permutaatio, niin saadaan $\sigma(M) = M$.

Koska jokaiselle $\sigma \in M$ pätee joko $\sigma(M) = M$ tai $\sigma(M) \cap M = \emptyset$, huomataan, että $\{\sigma(M) : \sigma \in H\}$ on joukon $\{1, \ldots, p\}$ ositus. Koska $H$ on

[1] kuvausten $\sigma_1$ ja $\sigma$ olemassaolon todistukset löytyvät teoksesta [3] korollaari 38.6 s.421 ja lause 49.5 s.542

transitiivinen, on jokaiselle $k \in \{1, \ldots, q\}$ olemassa $\sigma \in H$, jolle $\sigma(a) = k$ jolloin $k \in \sigma(M)$; lisäksi jos $j \in \tau(M) \cap \rho(m)$, missä $\tau, \rho \in H$, niin saadaan $\tau^{-1} \in M \cap \tau^{-1} \circ \rho(M)$. Näin ollen $M = \tau^{-1}(\rho(M))$ ja siten $\tau(M) = \rho(M)$ edellä osoitetun nojalla. Kaikilla osituksen osilla on selvästi yhtä monta alkiota, joten joukon $M$ alkioiden määrä $m$ jakaa alkuluvun $p$. Koska $a, b \in M$, niin $m \geq 2$ niin $m = p$ ja tämän vuoksi $M = \{1, \ldots, p\}$. Lisäksi $(a, s) \in H$ kaikilla $s \in \{1, \ldots, p\}$. Nyt huomattiin siis, että $H$ sisältää kaikki transpositiot alkioiden $1, \ldots, p$ kesken. Koska $H$ on ryhmä, se sisältää myös kaikki transpositioita yhdistelemällä saatavat syklit, joten helposti nähdään että $H = S_p$. □

**Esimerkki 5.5.** Polynomi $x^5 - 4x + 2$ on lauseessa 5.2 tarkoitetun kaltainen polynomi. Tutkimalla polynomifuktiota $f(x) = x^5 - 4x + 2$ huomataan, että $f(2) < 0$, $f(0) > 0$, $f(1) < 0$, $f(2) > 0$ joten sillä on ainakin 3 reaalista juurta. Toisaalta kun tarkastellaan funktion $f(x)$ kulkukaaviota huomataan, että sillä on enintään kolme reaalista juurta, joten sillä on kaksi juurta jotka eivät ole reaalilukuja.

Polynomin jaottomuuden voi tarkistaa Eisentseinin kriteerillä, jonka esittely jää tämän tutkielman ulkopuolelle.

Nyt kun ollaan havaittu, että kysymyksemme polynomiyhtälöiden ratkeavuudesta pelkistyy symmetristen ryhmien ratkeavuuteen, on tullut aika tarkastella niitä.

## 5.1 Symmetristen ryhmien ratkeavuus

**Lause 5.6.** *Symmetrinen ryhmä $S_n$ on ratkeava kun $1 \leq n \leq 4$.*

*Todistus.* Käydään tapaukset yksi kerrallaan läpi:

• $n = 1$: $S_1 = \{Id\}$, on triviaalisti ratkeava

• $n = 2$: $S_2 = \{Id, (12)\}$. Helposti nähdään, että $Id \lhd S_2$ ja että $S_2/Id = S_2$. Selvästi $S_2$ on vaihdannainen, sillä identiteettikuvaus on ryhmän neutraalialkio, joten $Id \circ (12) = (12) \circ Id$. Ryhmä $S_2$ on siis ratkeava.

• $n = 3$: $S_3 = \{Id, (12), (13), (23), (123), (132)\}$. Lemman 5.7 avulla $A_3 \lhd S_3$ ja koska $A_3 = \{Id, (123), (132)\}$, niin selvästi $Id \lhd A_3$. On siis saatu luotua normaalien aliryhmien ketju $Id \lhd A_3 \lhd S_3$.

Tekijäryhmä $A_3/Id = A_3$, jonka vaihdannaisuus on helppo todeta laskemalla: $(123) \circ (132) = Id = (132) \circ (123)$ sekä tietenkin $Id \circ (123) = (123) \circ Id$ ja $Id \circ (132) = (132) \circ Id$.

• $n = 4$: $S_4 = \{Id, (12), (13), (14), (23), (24), (34), (12)(34), (13)(24),$
$(14)(23), (123), (132), (134), (143), (124), (142), (234), (243), (1234), (1243),$

$(1324), (1342), (1423), (1432)\}$. Lemman 5.7 avulla saamme $A_4 \lhd S_4$. Löydetään ryhmälle $A_4$ normaali aliryhmä $V_4 = \{Id, (12)(34), (13)(24), (14)(23)\}$, niin sanottu Kleinin neliryhmä. Edelleen löydetään sille normaali aliryhmä $H = \{Id, (12)(34)\}$. Nyt ollaan saatu rakennettua normaaleista aliryhmistä ketju $Id \lhd H \lhd V_4 \lhd A_4 \lhd S_4$.

$H$ on syklinen ryhmä $C_2$ ja Kleinin neliryhmä on vaihdannainen joten $H/Id$ ja $V_4/H$ ovat vaihdannaiset. Tekijäryhmä $A_4/V_4$ on syklinen ryhmä $C_3$. Koska $(142) = (123) \circ (13)(24) = (134) \circ (12)(34) = (243) \circ (14)(23)$ niin saadaan luokaksi $a = \{(123), (142), (134), (243)\}$. Vastaavasti $a^2 = \{(132), (142), (143), (234)\}$ sillö $(234) = (132) \circ (13)(24) = (124) \circ (12)(34) = (143) \circ (14)(23)$. Ryhmän $V_4$ jäsenet muodostavat luokan $a^3 = e$. Viimeiseksi pitää osoittaa, että $S_4/A_4$ on vaihdannainen, mikä onnistuu lemman 5.8 avulla. □

**Lemma 5.7.** *Vuorotteleva ryhmä $A_n$ on symmetrisen ryhmän $S_n$ normaali aliryhmä.*

*Todistus.* Olkoon $p$ parillinen permutaatio, eli $p = p_1 p_2 \dots p_n$, missä $n$ on parillinen luku ja $p_i$ on transpositio. Nyt kaikille permutaatioille $q \in S_n$ pätee,

$$q^{-1}pq = q^{-1}(p_1 p_2 \dots p_n)p = (q^{-1}p_1 q)(q^{-1}p_2 q) \dots (q^{-1}p_n q)$$

jossa $(q^{-1}p_i q)$ on selvästi transpositio. Niinpä $q^{-1}pq$ on parillinen permutaatio ja vuorottelevan ryhmän $A_n$ määritelmän nojalla $q^{-1}A_n q \subseteq A_n$.

Kääntäen, kaikille parillisille permutaatioille $p'$, $qp'p^{-1} = (q^{-1})^{-1}p'q^{-1}$ on parillinen permutaatio. Näin ollen $p' = q^{-1}(qp'q^{-i})q \in q^{-1}A_n q$, josta seuraa $A_n \subseteq q^{-1}A_n q$.

Näin ollen $A_n = q^{-1}A_n q$, joka osoittaa, että $A_n$ on symmetrisen ryhmän $S_n$ normaali aliryhmä. □

**Lemma 5.8.** *Tekijäryhmä $S_n/A_n$ on isomorfinen syklisen ryhmän $C_2$ kanssa.*

*Todistus.* Koska kaikkien parillisten permutaatioiden käänteiskuvaus löytyy ryhmästä $A_n$, muodostaa niiden ekvivalenssiluokka neutraalialkion $e$ ja parittomat muodostavat alkion $a$. Parittomien permutaatioiden yhdiste on parillinen, samoin parillisten. Koska parillisten permutaatioiden luokan jäsenet ovat tässä tekijäryhmässä ekvivalentti identiteettikuvauksen kanssa, niin saamme seuraavat yhtälöt $a \circ a = e$, $e \circ e = e$ ja $a \circ e = e \circ a$, joten $S_n/A_n$ on isomorfinen syklisen ryhmän $C_2$ kanssa. □

**Lause 5.9.** *Symmetrinen ryhmä $S_n$ ei ole ratkeava kun, $n \geq 5$.*

*Todistus.* Aloitetaan todistamalla, ettei symmetrisellä ryhmällä $S_n$ ole muita normaaleja aliryhmiä kuin $S_n$, $A_n$ ja $Id$. Oletetaan että $H$ on symmetrisen

ryhmän $S_n$ normaali aliryhmä. Nyt $H \cap A_n$ on ryhmän $A_n$ normaali aliryhmä. Lemman 5.10 nojalla joko $H \cap A_n = A_n$ tai $H \cap A_n = \{Id\}$.

Jos $H \cap A_n = A_n$ niin $H \supseteq A_n$ jolloin joukon $H$ koko $m$ jakaa joukon $S_n$ mahtavuuden $n!$ ja on vuorottelevan ryhmän $A_n$ mahtavuuden $\frac{n!}{2}$ monikerta. Näin ollen pätee joko $m = n!$ jolloin $H = S_n$ tai $m = \frac{n!}{2}$ jolloin $H = A_n$.

Jos $H \cap A = \{Id\}$ niin $H = \{Id\}$, sillä ei ole ryhmän $S_n$ normaalia aliryhmää joka koostuisi vain parittomista permutaatioista ja identiteettikuvauksesta, jonka todistamme seuraavaksi:

Jos $H$ sisältää vähintään 2 paritonta permutaatiota $\sigma \neq \tau$ niin se sisältää myös permutaatiot $\sigma^2$ ja $\sigma\tau$ jotka ovat molemmat parillisia ja vain toinen on identiteettikuvaus. Toisaalta symmetrisellä ryhmällä $S_n$ ei ole aliryhmää $K$, jonka mahtavuus on 2 ja joka olisi normaali. Olkoon $K = \{Id, \sigma\}$, missä $\sigma$ on pariton permutaatio jolle $\sigma^2 = Id$(jotta $K$ täyttää ryhmän vaatimukset). Näin ollen löytyy $j \in 1, \ldots, n$ jolle $\sigma(j) \neq j$, ja koska $n \geq 5$ löytyy $k \in 1, \ldots, n$ jolle $\sigma(j) \neq k \neq j$. Nyt olkoon transpositio $(\sigma(j)k) = \rho \in S_n$). Nyt saadaan

$$(\rho\sigma\rho^{-1})(j) = \rho\sigma(j) = k$$

ja näin ollen $\rho\sigma\rho^{-1}$ ei kuulu ryhmään $K$ ja näin ollen $K$ ei ole ryhmän $S_n$ normaali aliryhmä.

Nyt siis jää ainoaksi tutkittavaksi ketjuksi $Id \lhd A_n \lhd S^n$.

Lemman 5.8 nojalla $S_n/A_n$ on vaihdannainen, joten riittää tutkia, onko $A_n/Id = A_n$ vaihdannainen. Helposti selvitämme vastaesimerkin

$$(123) \circ (234) = (13)(24) \neq (12)(34) = (234) \circ (123)$$

avulla, ettei $A_n$ ole vaihdannainen.

Näin ollen $S_n$ ei ole ratkeava kun $n \geq 5$. □

**Lemma 5.10.** *Vuorotteleva ryhmä $A_n$ on yksinkertainen, eli sen ainoat normaalit aliryhmät ovat $A_n$ ja $\{Id\}$ kun $n \geq 5$ tai $n = 3$.*

*Todistus.* Tapaus $n = 3$ on triviaali, sillä huomataan, että ryhmän $A_3$ ainoat aliryhmät ovat se itse ja $\{Id\}$, joista molemmat ovat triviaalisti sen normaaleja. Riittää siis tutkia tapaus $n \geq 5$.

Olkoon $H$ vuorottelevan ryhmän $A_n$ normaali aliryhmä, jossa on enemmän kuin yksi alkio ja olkoon $m$ suurin kokonaisluku $k$, jolle $H$ sisältää kahden erillisen permutaation yhdisteen, joista toinen on $k$-sykli. Koska erilliset permutaatiot ovat vaihdannaiset, löydetään permutaatio $p \in H$, jolle $p = (a_1 a_2 \ldots a_m)q$, jossa $q$ on identiteettikuvaus tai erillisten permutaatioiden yhdiste, jonka kaikki jäsenet ovat erillisiä permutaatiosta $(a_1 a_2 \ldots a_m)$.

*Tapaus 1*: $m > 3$ Permutaation $(a_1 a_2 a_3)$ käänteiskuvaus $(a_1 a_3 a_2)$ on myös erillinen permutaatiosta $q$, joten ryhmään $H$ kuuluu myös

$$\begin{aligned}[(a_1a_2a_3)p(a_1a_2a_3)^{-1}]q^{-1} &= (a_1a_2a_3)(a_1a_2\dots a_m)q(a_1a_2a_3)^{-1}q^{-1}\\ &= (a_1a_2a_3)(a_1a_2\dots a_m)(a_1a_2a_3)^{-1}qq^{-1}\\ &= (a_2a_3a_1\dots a_m)(a_1a_2\dots a_m)^{-1}\\ &= (a_1a_2a_4)\end{aligned}$$

nyt $H$ sisältää kolmisyklin ja lemman 5.11 perusteella $H = A_n$.

*Tapaus 2*: $m = 3$. Näin ollen jokainen permutaation $q$ tekijä on joko transpositio tai kolmisykli, mutta jos jokin sen tekijöistä olisi kolmisykli $(a_4a_5a_6)$ niin $q = (a_4a_5a_6)r$, missä $r$ on joko identiteettikuvaus tai yhdiste kuvauksista, jotka ovat erillisiä paitsi toisistaan, myös permutaatioista $(a_1a_2a_3)$ ja $(a_4a_5a_6)$. Nyt siis $(a_2a_4a_3) = (a_2a_3a_4)^{-1}$ on erillinen permutaatiosta $r$ ja ryhmään $H$ kuuluisi

$$\begin{aligned}&[(a_2a_3a_4)p(a_2a_3a_4)^{-1}]p\\ &= (a_2a_3a_4)(a_1a_2a_3)(a_4a_5a_6)r(a_2a_3a_4)^{-1}r^{-1}(a_4a_5a_6)^{-1}(a_1a_2a_3)^{-1}\\ &= (a_2a_3a_4)(a_1a_2a_3)(a_4a_5a_6)(a_2a_4a_3)rr^{-1}(a_4a_6a_5)(a_1a_3a_2)\\ &= (a_1a_4a_2a_3a_5),\end{aligned}$$

joka on ristiriidassa oletuksen $m = 3$ kanssa. Niinpä permutaation $q$ kaikkien tekijöiden täytyy olla transpositioita ja silloin $q^2 = Id$. Koska lisäksi $q$ on erillinen permutaatiosta $(a_1a_2a_3)$ voidaan kirjoittaa

$$p^2 = [(a_1a_2a_3)q][(a_1a_2a_3)q] = (a_1a_2a_3)^2q^2 = (a_1a_3a_2).$$

Tästä huomaamme että ryhmä $H$ sisältää myös myös alkion $p^2$. Ja saamme jälleen lemman 5.11 perusteella $H = A_n$.

*Tapaus 3*: $m = 2$. Tullaan huomaamaan, että oletuksesta $n > 4$ tulee seuraamaan, ettei tällaista tapausta pääse muodostumaan. Sillä jos $m = 2$, niin $p$ on parillisten permutaatioiden yhdiste, joten $p = (a_1a_2)(a_3a_4)r$, missä $r$ on joko identiteettikuvaus tai sellaisten toisistaan erillisten permutaatioiden yhdiste, jotka ovat erillisiä myös transpositioista $(a_1a_2)$ ja $(a_3a_4)$. Nyt $(a_2a_4a_3) = (a_2a_3a_4)^{-1}$ ja $(a_2a_3a_4)$ ovat permutaatiosta $r$ erilliset, joten $H$ sisältää

$$\begin{aligned}&[(a_2a_3a_4)p(a_2a_3a_4)^{-1}]p^{-1}\\ &= (a_2a_3a_4)(a_1a_2)(a_3a_4)r(a_2a_3a_4)^{-1}r^{-1}(a_1a_2)(a_3a_4)\\ &= (a_2a_3a_4)(a_1a_2)(a_3a_4)(a_2a_4a_3)rr^{-1}(a_1a_2)(a_3a_4)\\ &= (a_1a_4)(a_2a_3).\end{aligned}$$

Koska $n \geq 5$, on olemassa $a_5$, joka ei ole mikään $a_1, a_2, a_3, a_4$. Näin ollen $H$ sisältää

$$\begin{aligned}&[(a_2a_4a_5)[(a_1a_4)(a_2a_4)](a_1a_4a_5)^{-1}](a_1a_4)(a_2a_3)\\&= (a_1a_4a_5)(a_1a_4)(a_2a_3)(a_1a_5a_4)(a_1a_4)(a_2a_3)\\&= (a_1a_5a_4),\end{aligned}$$

mikä on ristiriidassa oletuksen $m = 2$ kanssa. □

**Lemma 5.11.** *Jos $H$ on vuorottelevan ryhmän $A_n$ normaali aliryhmä ja se sisältää kolmisyklin niin $H = A_n$.*

*Todistus.* Tapauksissa $A_3$ ja $A_4$ , helposti nähdään, että lemman väite pitää paikkansa, joten riittää keskittyä tilanteeseen $n \geq 5$. Olkoon $(abc) \in H$ ja $(xyz)$ mielivaltainen kolmisykli ryhmässä $A_n$. Selvästi on olemassa permutaatio $p_1$ siten, että $p_1 : a \mapsto x$ , $p_1 : b \mapsto y$ ja $p_1 : c \mapsto z$. Olkoon $p = p_1$, jos $p_1$ on parillinen ja olkoon $p = (ij)p_1$, missä $(ij)$ on syklistä $(xyz)$ erillinen transpositio, jos $p$ on pariton. Nyt $p$ on parillinen ja siksi

$$(xyz) = p(abc)p^{-1} \in H.$$

Näin ollen $H$ sisältää kaikki kolmisyklit ja niin lemman 5.12 nojalla pätee $H = A_n$. □

**Lemma 5.12.** *Jos $n \geq 3$ niin kaikki ryhmän $A_n$ jäsenet saadaan kolmisyklien yhdisteenä.*

*Todistus.* Koska kaikki kolmesyklit ovat parillisia permutaatioita kuuluvat kaikki ryhmän $S_n$ kolmisyklit aliryhmään $A_n$. Riittää osoittaa, että kaikki ryhmän $A_n$ jäsenet voidaan rakentaa kolmisykleistä. Koska $(12)(34) = (123)(143)$ ja $(12)(13) = (123)$ kaikki parilliset transpositioiden yhdisteet voidaan esittää kolmisyklien yhdisteenä, olivat ne sitten erillisiä tai eivät. □

Lauseiden 5.6 ja 4.3 perusteella siis kaikki polynomiyhtälöt $f(x) = 0$ ovat ratkeavia kun $\deg f(x) \leq 4$. Vuorostaan lauseista 5.9 ja 5.2 seuraa, että esimerkin 5.5 polynomista rakennettu yhtälö $x^5 - 4x + 2 = 0$ ei ole juurilausekkein ratkeava.

# Kirjallisuutta


[1] Metsänkylä, Tauno ja Näätänen, Marjatta: Algebra, 2. painos, Limes, Helsinki 2005

[2] Fang, J.: Abstract Algebra - Schaums outline of theory and problems of, Schaum Publishing Company, New York 1963

[3] Warner, Seth: Modern Algebra, Dover Publications Inc, New York 1990

[4] Fischer, Hanspeter: On the simplicity of alternating groups, www.cs.bsu.edu/homepages/fischer/math411/simple.pdf, noudettu 25.4.2013

[5] Tignol, Jean-Pierre: Galois Theory of Algebraic Equations, World Scientific Publishing Co. Pte. Ltd, Singapore 2001

[6] Boyer, Carl: Tieteiden kuningatar - Matematiikan historia osat I ja II, 3. painos, Art house, Juva 2000