Viidennen asteen yhtälön ratkaisukaavan olemassaolon mahdottomuus Galois'n teorian pohjalta

Teppo Lahti

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kevät 2014

Tiivistelmä Teppo Lahti, *Viidennen asteen yhtälön ratkaisukaavan olemassaolon mahdottomuus Galois'n teorian pohjalta.* matematiikan pro gradu -tutkielma, 78 sivua, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, kevät 2014.

Tässä tutkielmassa on tarkoituksena todistaa, ettei viidennen asteen yhtälölle ole olemassa ratkaisukaavaa. Todistus tehdään Galois'n teorian pohjalta. Keskeisenä käsitteenä Galois'n teoriassa on kuntalaajennus, joka määritellään kahden kunnan välisenä monomorfismina. Kuntalaajennuksia voidaan luokitella useilla eri tavoilla, joista keskeisimmät ovat yksinkertainen, algebrallinen ja normaali kuntalaajennus. Lineaarialgebran avulla voidaan kuntalaajennukselle määritellä myös aste.

Sanotaan, että renkaan $K[x]$ polynomi p hajoaa kunnassa L, jos p voidaan kirjoittaa muodossa $p = k(x - \alpha_1) \cdots (x - \alpha_n)$, missä $k, \alpha_1, \ldots, \alpha_n \in L$. Pienintä mahdollista kuntaa, jossa p hajoaa, kutsutaan polynomin p hajotuskunnaksi.

Galois'n teoriassa keskeinen rooli on Galois'n ryhmillä. Luonnollisen kuntalaajennuksen $K \hookrightarrow L$ Galois'n ryhmä $\Gamma(K, L)$ määrittellään ryhmäksi automorfismeja $f : L \to L$, joille pätee $f(k) = k$ kaikilla $k \in K$. Jokaiselle Galois'n ryhmän $\Gamma(K, L)$ aliryhmälle H voidaan määritellä kiintopistekunta: se on kunta, jonka muodostavat ne kunnan L alkiot x, joille pätee $h(x) = x$ kaikilla $h \in H$.

Käyttäen apuna lineaarialgebraa voidaan todistaa Galois'n ryhmiä ja kiintopistekuntia koskevat viisi Galois'n lausetta. Näistä tärkeimpiä on ensimmäinen Galois'n lause, jonka mukaan Galois'n ryhmän $\Gamma(K, L)$ alkioiden lukumäärä on sama kuin kuntalaajennuksen $K \hookrightarrow L$ aste.

Tutkielman lopussa määritellään juurin ratkeavuus juurilaajennusten avulla. Galois'n viidettä lausetta käyttämällä voidaan osoittaa, että rationaalikertoiminen polynomi $p \in \mathbb{Q}[x]$, jonka hajotuskunta on Σ, on ratkaistavissa juurin, vain jos Galois'n ryhmä $\Gamma(\mathbb{Q}, \Sigma)$ on ratkeava.

Koska symmetrinen ryhmä $\mathbb{S}_5$ ei ole ratkeva, täytyy löytää polynomi, jonka Galois'n ryhmä on isomorfinen ryhmän $\mathbb{S}_5$ kanssa. Ensimmäisen Galois'n lauseen avulla voidaan todistaa, että jos rationaalikertoimisella polynomilla q, jonka aste p on alkuluku, on täsmälleen $p - 2$ reaalista nollakohtaa, niin sen Galois'n ryhmä on isomorfinen symmetrisen ryhmän $\mathbb{S}_p$ kanssa. Tämän lemman avulla on helppo löytää polynomeja, jotka eivät ole ratkaistavissa juurin.

Avainsanat: Galois'n teoria, Galois'n ryhmä, kuntalaajennus, polynomi, ratkaisukaava.

Johdanto 1

Luku 1. Polynomit 4
1.1. Polynomit 4
1.2. Polynomin tekijät 6
1.3. Polynomin nollakohdat 11

Luku 2. Kuntalaajennukset 13
2.1. Kuntalaajennukset 13
2.2. Minimaalipolynomit 16
2.3. Yksinkertaiset algebralliset kuntalaajennukset 18
2.4. Kuntalaajennuksen aste 23

Luku 3. Polynomien hajoaminen 27
3.1. Hajotuskunnat 27
3.2. Normaalit kuntalaajennukset 29
3.3. Separoituvat polynomit 31

Luku 4. Galois'n ryhmät 34
4.1. Galois'n ryhmät ja kiintopistekunnat 34
4.2. Lineaarialgebraa 35
4.3. K-monomorfismit 40
4.4. Normaalisulkeumat 40
4.5. Galois'n lauseet 46

Luku 5. Ryhmäteoriaa 50
5.1. Symmetriset ja alternoivat ryhmät 50
5.2. Ratkeavat ryhmät 53
5.3. Yksinkertaiset ryhmät 58
5.4. Cauchyn Lause 62

Luku 6. Viidennen asteen yhtälön ratkaisukaava 68
6.1. Juurilaajennukset 68
6.2. Viidennen asteen yhtälö 75

Kirjallisuutta 78

Sisältö

Johdanto

Toisen asteen yhtälölle on tunnnettu ratkaisukaava jo vähintään 3 600 vuotta [**12**, s. xviii]. Muinaiset babylonialaiset tarvitsivat ratkaisukaavaa pinta-alaan liittyvissä käytännön ongelmissa. Heille kuitenkin riitti, että kaava toimi käytännössä; mitään matemaattisia perusteluja kaavalle ei tuolta ajalta ole löydetty. Babylonialaiset osasivat ratkaista myös joitakin käytännön ongelmissa esiintyviä kolmannen asteen yhtälöitä palauttamalla niitä toisen asteen yhtälöiksi. [**2**, s. 62- 66]

Keskiajalla arabit ja persialaiset pitivät polynomiyhtälöitä tärkeinä monien käytännön ongelmien ratkaisemisessa, kuten perinnön jakamisessa, oikeudenkäynnissä, kaupankäynnissä ja maanmittauksessa [**2**, s. 328]. Arabimatemaatikko al-Kashi osasikin 1400-luvulla ratkaista riittävällä tarkkuudella kaikki käytännön ongelmista kumpuavat kolmannen asteen yhtälöt [**2**, s. 407]. Se ei silti hillinnyt antiikin kreikkalaista eksaktia matematiikkaa ihailevia renesanssiajan matemaatikoita. Monet italialaiset tiedemiehet etsivät 1500-luvulla korkeamman asteen yhtälöille samantapaista ratkaisukaavaa kuin toisen asteen yhtälöille.

Ensimmäisenä kolmannen asteen yhtälön ratkaisukaavan keksi luultavasti Bolognan yliopiston matematiikan professori Scipione del Ferro. Hieman myöhemmin ratkaisukaavan keksi itsenäisesti myös Niccolo Fontana, joka tunnetaan paremmin nimellä Tartaglia (suomeksi "Änkyttäjä"). Tartaglia paljasti salaisuutensa lääkäri Gerolamo Cardanolle, joka ensimmäisenä julkaisi sen 1545 kirjassaan *Ars Magna*. Teos sisälsi myös neljännen asteen yhtälön ratkaisukaavan, jonka oli keksinyt Cardanon oppilas Lodovico Ferrari. [**2**, s. 399-402]

Kolmannen ja neljännen asteen yhtälöiden ratkaisukaavojen keksimisen jälkeen seuraava askel oli luonnollisesti korkeamman asteen yhtälöiden ratkaisukaavojen keksiminen. Matemaatikot löivätkin viidennen asteen yhtälön kanssa päätänsä seinään yli kahdensadan vuoden ajan. Viidennen asteen yhtälön ratkaisukaavasta tuli niin merkittävä ongelma, että se voidaan rinnastaa antiikin Kreikan klassisiin ongelmiin. Kuten kreikkalaisten klassiset ongelmat, myös viidennen asteen yhtälön ratkaisuyritykset veivät epäonnistumisistaan huolimatta matematiikkaa eteenpäin. [**12**, s. xx-xxi]

Epäilykset koko ratkaisukaavan olemassaolosta heräsivät viimeistään 1770-luvulla. Silloin ranskalainen Joseph-Louis Lagrange osoitti, että tietyin varsin yleisin metodein − joilla kolmannen ja neljännen asteen yhtälö saadaan ratkaistuksi − ei viidennen asteen yhtälö ainakaan ratkea. Työssään Lagrange tutki yhtälöiden ratkeavuutta niiden juurten permutaatioiden avulla. [**12**, s. xxi]

Italialainen Paolo Ruffini uskoi vuonna 1799 todistaneensa viimein, ettei viidennen asteen yhtälölle ollut olemassa ratkaisukaavaa. Ruffinin todistus oli kuitenkin niin

pitkä ja monimutkainen, ettei kukaan pystynyt tarkastamaan sen pätevyyttä ennen Ruffinin kuolemaa. Myöhemmin selvisi, että todistuksessa oli todella aukko: Ruffini ei ollut todistanut väitettään siitä, että jokaisen polynomin ratkaisukaavassa esiintyvä juurilauseke voidaan ilmaista rationaalifunktiona polynomin nollakohtien avulla. [**12**, s. xxi]

Nuori norjalainen Niels Henrik Abel ajatteli 1820-luvulla myös ratkaisseensa viidennen asteen yhtälön ongelman. Hän kuvitteli ensin löytäneensä viimeinkin ratkaisukaavan, kunnes ymmärsi asian olevankin päinvastoin: Abel todisti 1824 ensimmäisenä, ettei viidennen asteen yhtälölle ole olemassa ratkaisukaavaa. Abel ei tuntenut Ruffinin työtä, mutta hänen todistuksessaan oli paljon yhtäläisyyksiä Ruffinin todistukseen. Abel onnistui myös todistamaan väitteen, jota Ruffini ei huomannut todistaa. [**2**, s. 732]

Vaikka Abelin todistus olikin yhtä pientä virhettä lukuun ottamatta pätevä, siinä oli yksi suuri heikkous: Abelin todistus kertoi vain, ettei ole olemassa yhtä ratkaisukaavaa, jolla kaikki viidennen asteen yhtälöt saataisiin ratkaistua. Sen avulla ei voitu päätellä, oliko jollain tietyllä viidennen asteen yhtälöllä ratkaisukaava. Itse asiassa Abelin todistuksesta huolimatta jokaiselle viidennen asteen yhtälölle saattoi edelleen olla olemassa oma erityinen ratkaisukaavansa. [**12**, s. xxiii]

Nuori ranskalainen Évariste Galois (syntynyt 1811) oli erittäin kiinnostunut sekä Abelin että Lagrangen ratkaisukaavoja käsittelevistä töistä. Niiden innoittamina Galois laati omaperäisen ja kekseliään teorian, joka elegantilla tavalla kiersi Ruffinin ja Abelin todistusten ongelmat. Galois'n teorian avulla voitiin viimein löytää konkreettisia viidennen asteen yhtälöitä, joilla ei ole ratkaisukaavaa. Tästä huolimatta hän ei saanut elämänsä aikana minkäänlaista tunnustusta työstään. Galois kyllä lähetti työnsä Pariisin Akatemiaan kahdesti. Toisella kerralla kyse oli matematiikkakilpailusta. Tuomaristo − todennäköisesti kilpailun aikana kuollut Adrien-Marie Legendre − hukkasi hänen työnsä eikä sitä koskaan löydetty. [**12**, s. xxiii-xxvii]

Galois'n elämä oli muutenkin täynnä vaikeuksia. Hänen isänsä teki itsemurhan 1828. Samana vuonna hän pyrki opiskelemaan École Polytechniqueen, jossa monet tuon ajan kuuluisista matemaatikoista olivat opiskelleet. Matemaattisista lahjoistaan huolimatta Galois ei saanut opiskelupaikkaa. Todennäköisesti hänen matemaattinen tietämyksensä oli liian suppeaa. Galois oli myös aktiivinen Ranskan monarkian vastustaja ja joutui poliittisen toimintansa vuoksi vankilaan. [**12**, s. xxiii-xvi]

Galois menehtyi vuonna 1832 vain 20-vuotiaana kaksintaistelussa. Tragedian syistä käydään yhä keskustelua. Galois'n kirjoittamien kirjeiden mukaan siihen liittyi ainakin pettymys rakkaudessa. [**11**]

Tämän tutkielman tarkoituksena on esittää ratkaisu yhteen matematiikan historian innoittavimmista ongelmista. Tarkoituksena on Galois'n teoriaa käyttäen osoittaa, ettei viidennen tai sitä korkeamman asteen yhtälöille ole olemassa ratkaisukaavaa. Tutkielman ymmärtämiseksi lukijan tulee hallita perusteet algebrasta (esimerkiksi [**4**], [**8**] tai [**9**]) sekä lineaarialgebrasta (esimerkiksi [**7**] tai [**10**]). Myös analyysistä ja kompleksianalyysistä saatavia tietoja esiintyy tässä tutkielmassa muutama.

Tutkielma seuraa pääosin Ian Stewartin kirjaa *Galois Theory* [**12**]. Ensimmäisessä luvussa määritellään polynomit sekä perehdytään niiden tekijöihin ja nollakohtiin. Toisessa luvussa käsitellään kuntalaajennuksia, jotka määritellään monomorfismeiksi kunnalta kunnalle. Syy kuntalaajennusten esittelyyn liittyy polynomien nollakohtiin. Esimerkiksi rationaalikertoimisen polynomin x^2-2 nollakohdat eivät ole kunnassa $\mathbb{Q}$. Kunta $\mathbb{Q}$ voidaan kuitenkin laajentaa kuntalaajennuksella kunnaksi L, jossa kaikki nollakohdat ovat. Sanotaan, että tällöin polynomi x^2-2 hajoaa kunnassa L. Polynomien hajoamista käsitellään luvussa 3. Siinä myös todistetaan, ettei jaottomilla polynomeilla ole moninkertaisia nollakohtia kompleksilukujen joukossa.

Vasta neljännessä luvussa päästään käsittelemään Galois'n keksimää merkittävää ja omalaatuista ideaa, Galois'n ryhmää. Galois itse määritteli ryhmän polynomin nollakohtien tiettyinä permutaatioina. Tässä tutkielmassa sama asia määritellään kuitenkin modernin matematiikan kielellä: jokaista kuntalaajennusta vastaa ryhmä automorfismeja, jotka kiinnittävät lähtökunnan alkiot. Tämä ryhmän ominaisuudet kertovat myös, miksei kaikille polynomeille ole olemassa ratkaisukaavaa. Neljännen luvun merkittävimmät tulokset ovat viisi Galois'n lausetta. Niiden todistamiseksi tarvitaan jonkin verran lineaarialgebraa.

Galois'n ryhmien ominaisuuksien selvittämiseksi viidennessä luvussa käsitellään ryhmäteoriaa. Keskeisiä käsitteitä luvussa ovat permutaatiot ja symmetriset ryhmät sekä normaalit aliryhmät. Kun tämä kaikki on käyty läpi, voidaan kuudennessa luvussa viimein määritellä ratkaisukaava ja todistaa, ettei viidennen asteen yhtälölle sellaista ole.

LUKU 1

Polynomit

1.1. Polynomit

Tämä tutkielma käsittelee kunnan $\mathbb{C}$ alikuntia. Jokainen tämän tutkielman kunta sisältää tällöin rationaalilukujen kunnan $\mathbb{Q}$ alikuntanaan.

MÄÄRITELMÄ 1.1. Renkaan R *polynomi* p on jono $(a_n)_{n\in\mathbb{N}}$, missä $a_n \in R$ kaikille n sekä $a_n \neq 0$ vain äärellisen monelle alkiolle a_n. Tällöin äärettömän pitkä nollaketju voidaan jättää polynomin lopusta kirjoittamatta, jolloin päädytään muotoon $p = (a_0, a_1, \ldots, a_m)$ ja $a_n = 0$, kun $n > m$. Polynomista käytetään myös merkintöjä

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$

sekä

$$p(x) = \sum_{k=0}^{n} a_k x^k.$$

Jos $p = (a_0), a_0 \neq 0$, niin sanotaan, että p on *vakiopolynomi*.

MÄÄRITELMÄ 1.2. Renkaan R Polynomille määritellään *yhteenlasku* asettamalla

$$\sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{m} b_k x^k = \sum_{k=0}^{max\{m,n\}} (a_k + b_k) x^k \tag{1.1}$$

ja *kertolasku* asettamalla

$$\sum_{k=0}^{n} a_k x^k \cdot \sum_{k=0}^{m} b_k x^k = \sum_{k=0}^{n+m} \Big(\sum_{i+j=k} a_i \cdot b_j \Big) x^k, \tag{1.2}$$

kun $a_0, \ldots, a_n \in R$ ja $b_0, \ldots, b_m \in R$.

Kun renkaan R polynomit varustetaan niiden yhteenlaskulla ja kertolaskulla saadaan rengas, jota kutsutaan *polynomirenkaaksi* ja merkitään $R[X]$. Renkaan nolla-alkio on nollapolynomi (0) ja ykkösalkio vakiopolynomi (1).

Kun $a \in R$, niin kuvaus $f : R \to R[x], a \mapsto (a_0)$ on monomorfismi. Tällöin rengas R on isomorfinen polynomirenkaan $R[x]$ vakiopolynomeista koostuvan alirenkaan kanssa. Tämän isomorfisuuden ansiosta voidaan tulkita rengas R renkaan $R[x]$ alirenkaaksi eli $R \subset R[x]$. Näin voidaan tulkita jokainen $a \in R$ renkaan $R[x]$ vakiopolynomiksi.

MÄÄRITELMÄ 1.3. Olkoon R rengas ja $a_k \in R$ kaikilla $k \in \mathbb{N}$. Olkoon lisäksi $p \in R[x]$, $p = a_0 + \cdots + a_n X^n$. Polynomin p *asteesta* käytetään merkintää ∂p ja se määritellään nollasta eroaville polynomeille seuraavasti:

$$\partial p = \max\{k : a_k \neq 0\}.$$

Jos $p = 0$, niin asetetaan $\partial p = -\infty$.

HUOMAUTUS 1.4. Suoraan määritelmästä 1.3 sekä määritelmän 1.2 kohdasta (1.1) nähdään, että kun $p, q \in R[x]$, niin pätee

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

Yhtäsuuruus ei tässä todellakaan ole välttämätön, sillä polynomit p ja q voivat sopivasti kumota toistensa alkioita. Samoin yhtä suoraviivaisesti määritelmästä 1.3 ja määritelmän 1.2 kohdasta (1.2) nähdään, että

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

Määritelmässä 1.1 polynomi määriteltiin jonoksi alkioita. Sen merkinnöissä esiintyvä + ei siis ole yhteenlaskun symboli. Määritelmässä 1.2 polynomien yhteen- ja kertolasku kuitenkin määriteltiin sellaisiksi, että polynomi käyttäytyy kuten tavallinen yhteenlasku. Tämä selventää sitä, minkä vuoksi + esiintyy polynomin merkinnässä.

Ei kuitenkaan pidä ajatella, että polynomin merkinnässä esiintyvä x olisi jokin muuttuja tai x^k tarkoittaisi potenssia, jossa k toimii eksponenttina. Sen sijaan k ilmaisee, missä kohdalla jonoa alkio sijaitsee. Esimerkiksi merkintä ax^2 tarkoittaa polynomin tapauksessa vain sitä, että polynomijonon kolmas alkio on a. Näin ollen polynomi ei ole myöskään kuvaus, vaan pelkkä jono. Jokaiselle polynomille voidaan kuitenkin määritellä sen merkintää vastaava kuvaus seuraavasti.

MÄÄRITELMÄ 1.5. Olkoon R rengas ja $p \in R[x]$ polynomi. Tällöin polynomia $p = (a_0, \ldots, a_n)$ vastaava *polynomikuvaus* on kuvaus $\bar{p} : R \to R$, jolle

$$\bar{p} = \sum_{k=0}^{n} a_k x^k$$

kaikilla $x \in R$.

HUOMAUTUS 1.6. Jokaisella polynomilla on selvästi yksikäsitteinen polynomikuvaus. Käänteinen ei kuitenkaan välttämättä päde. Voi siis olla polynomit p ja q, joille $p \neq q$, mutta $\bar{p} = \bar{q}$. Tämän vuoksi yleisessä tapauksessa on tärkeää erotella polynomi ja sitä vastaava polynomikuvaus toisistaan. Tietyssä erikoistapauksessa nämä voidaan kuitenkin samaistaa. Tämän sanoo kuitenkin vasta lause 1.23.

MÄÄRITELMÄ 1.7. Jos $K \subset \mathbb{C}$ on kunta ja $p(x) \in K[x]$ sen polynomi, niin polynomin $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$, *johtava kerroin*, on luku a_n. Sanotaan, että polynomi p on *perusmuotoinen*, jos sen johtava kerroin $a_n = 1$.

1.2. Polynomin tekijät

Polynomille määritellään tekijät vastaavalla tavalla kuin kokonaisluvuillekin: annetun polynomin p tekijät ovat ne polynomit, joita kertomalla saadaan polynomi p. Kun puhutaan jaollisesta polynomista, tarkoitetaan kuitenkin sellaista polynomia, jonka tekijät eivät ole vakiopolynomeja.

MÄÄRITELMÄ 1.8. Olkoon R rengas ja $p, q \in R[x]$ nollasta eroavia polynomeja. Jos $p = q \cdot r$ jollekin polynomille nollasta eroavalle polynomille $r \in R[x]$, niin q on polynomin p *tekijä renkaassa* $R[x]$ eli q *jakaa* polynomin p *renkaassa* $R[x]$. Tästä käytetään myös merkintää $q \mid p$. Mikäli q ei jaa polynomia p, voidaan käyttää merkintää $q \nmid p$.

MÄÄRITELMÄ 1.9. Olkoon R rengas. Sen nollasta eroava polynomi $p \in R[x]$ on *jaollinen renkaassa* $R[x]$, jos se voidaan ilmaista muodossa

$$p = qr,$$

missä $q, r \in R[x]$ ovat polynomeja, joille pätee $1 \leq \partial q < p$ ja $1 \leq \partial r < p$. Jos polynomia p ei voida ilmaista tässä muodossa, sanotaan, että se on *jaoton*.

Määritelmissä 1.8 ja 1.9 on oleellista, missä renkaassa polynomin p oletetaan olevan jaollinen. Esimerkiksi polynomi $p = x^2 + 1$ ei ole jaollinen renkaassa $\mathbb{Q}[x]$. Tästä huolimatta se on jaollinen renkaassa $\mathbb{C}[x]$, sillä $p = (x+i) \cdot (x-i)$, missä $x + i \in \mathbb{C}[x]$ ja $x - i \in \mathbb{C}[x]$.

MÄÄRITELMÄ 1.10. Olkoon K kunta ja olkoot $p, q \in K[x]$ polynomeja. Polynomien p ja q *suurin yhteinen tekijä* on polynomi $r \in K[x]$, jolle pätee $r \mid p$ ja $r \mid q$ sekä $s \mid r$ kaikille polynomeille $s \in K[x]$, joille $s \mid p$ ja $s \mid q$.

HUOMAUTUS 1.11. Suurin yhteinen tekijä ei nimestään huolimatta ole yksikäsitteinen. Jos nimittäin $d \in K[x]$ on polynomien p ja q suurin yhteinen tekijä, niin myös polynomi kd kaikilla $k \in K \setminus 0$ on polynomien p ja q suurin yhteinen tekijä. Ei ole myöskään selvää, että kaikilla polynomeilla olisi suurin yhteinen tekijä. Tämä saadaan todistettua etsimällä suurin yhteinen tekijä polynomien Eukleideen algoritmilla (ks. [**6**, Theorem 4.1]).
Seuraava lause sanoo, että kuten kokonaisluvutkin, jokainen nollasta eroava polynomi voidaan jakaa jaottomiin tekijöihin.

LAUSE 1.12. *Olkoon K kunta. Tällöin sen jokainen polynomi $p \in K[x]$ voidaan ilmaista tulona*

$$p = kq_1q_2 \cdots q_n,$$

missä $k \in K$ on vakio ja $q_1, \ldots, q_n \in K[x], n \in \mathbb{N}$, ovat renkaassa $K[x]$ jaottomia polynomeja, joille pätee $\partial q_i \geq 1$ kaikilla $i = 1, \ldots, n$.

TODISTUS. Todistetaan väite induktiolla polynomin p asteen suhteen. Jos $\partial p = 0$, niin $p = k$, jolloin väite pätee, kun $n = 0$. Oletetaan siis, että väite pätee jollain $\partial p = l \geq 1$. Tarkastellaan ensiksi tapausta $\partial p = m > l$, kun p on jaoton. Tällöin voidaan valita $k = 1$ ja $q_1 = p$, jolloin väite pätee. Tarkastellaan sitten tapausta $\partial p = m > l$, kun p on jaollinen. Tällöin p on muotoa $p = r_1r_2$ jollain polynomeilla

$r_1, r_2 \in K[x]$, joille pätee $1 \leq \partial r_1 < m$ ja $1 \leq \partial r_2 < m$. Nyt voidaan käyttää induktio-oletusta. Sen mukaan $r_1 = k_1$ sekä $r_2 = k_2 q_2$, missä $k_1, k_2 \in K$ ja $q_1, q_2 \in K[x]$ ovat jaottomia ei-vakioita polynomeja. Tällöin p on muotoa $p = k_1 k_2 q_1 q_2 q$. □

Lisäksi lauseen 1.12 mukainen esitys on jokaisella nollasta eroavalla polynomilla yksikäsitteinen. Ennen tämän todistamista tarvitaan kuitenkin vielä yksi lemma.

LEMMA 1.13. *Olkoon K kunta, $p \in K[x]$ renkaassa $K[x]$ jaoton polynomi ja olkoot $q, r \in K[x]$ polynomeja. Jos p jakaa polynomin $q \cdot r$, niin p jakaa polynomin q tai p jakaa polynomin r.*

TODISTUS. Jos p jakaa polynomin q, niin väite pätee. Oletetaan siis, että p ei jaa polynomia q. Olkoon $d \in K[x]$ polynomien p ja q suurin yhteinen tekijä. Tällöin $d \mid p$, mutta koska p on jaoton, täytyy olla $d = k$ tai $d = kp$ jollain $k \in K \setminus \{0\}$.

Oletetaan ensin, että $d = kp$. Koska $d \mid q$, niin $kp \mid q$, jolloin myös $p|q$. Tämä on kuitenkin vastoin oletusta.

Oletetaan siis, että $d = k$. Koska d on polynomien p ja q suurin yhteinen tekijä, niin huomautuksen 1.14 perusteella myös $k'd, k' \in K \setminus \{0\}$ on polynomien p ja q suurin yhteinen tekijä. Tällöin polynomien suurin yhteinen tekijä on myös $k^{-1}d = k^{-1}k = 1$. Nyt voidaan käyttää Bézout'n lausetta (katso todistus kokonaisluvuille esimerkiksi kirjasta [**1**, Chapter 2] − todistus polynomeille etenee vastaavasti). Sen mukaan on olemassa polynomit $t, u \in K[x]$ siten, että

$$tp + uq = 1. \tag{1.3}$$

Kertomalla yhtälö (1.3) polynomilla r saadaan

$$rtp + ruq = r. \tag{1.4}$$

Oletuksen nojalla p jakaa polynomin rq, jolloin on olemassa polynomi $v \in K[x]$, jolle pätee

$$pv = rq. \tag{1.5}$$

Sijoittamalla yhtälö (1.5) yhtälöön (1.4) saadaan

$$rtp + upv = r$$

eli

$$p(rt + uv) = r,$$

jolloin $p|r$. □

LAUSE 1.14. *Olkoon K kunta ja $p \in K[x]$ polynomi, jolle pätee $\partial p \geq 1$. Tällöin polynomi p on muotoa*

$$p = kq_1 q_2 \cdots q_n,$$

missä $k \in K$ on yksikäsitteinen ja $q_1, \ldots, q_n \in K[x]$ ovat järjestystä vaille yksikäsitteiset renkaassa $K[x]$ jaottomat ja perusmuotoiset polynomit, joille pätee $\partial q_i \geq 1$, $i = 1, \ldots, n$.

TODISTUS. Polynomin jaottomien tekijöiden olemassaolo on jo todistettu, joten jäljelle jää yksikäsitteisyyden todistaminen. Täytyy siis osoittaa, että jos

$$p = kq_1q_2 \dots q_n \tag{1.6}$$

ja

$$p = k'r_1r_2 \dots r_m, \tag{1.7}$$

niin $k = k'$, $n = m$ ja polynomit $q_i, i = 1, \dots, n$, ovat samat kuin polynomit r_j, $j = 1, \dots, m$. Todistetaan väite induktiolla luvun n suhteen. Jos $n = 1$, niin

$$p = kq_1 = k'r_1 \dots r_m. \tag{1.8}$$

Yhtälöstä (1.8) ja polynomin tekijän määritelmästä 1.8 seuraa, että $kq_1 \mid k'r_1 \dots r_m$. Tulkitaan vakio k' vakiopolynomiksi, jolloin soveltamalla lemmaa 1.13 m kertaa peräkkäin saadaan selville, että $kq_1 \mid k'$ tai $kq_1 \mid r_i$ jollain $i = 1, \dots m$. Koska q ei ole vakio, niin tapaus $kq_1 \mid k'$ on mahdoton. Siten $kq_1 \mid r_i$. Tekijöiden järjestyksen ei tarvitse olla yksikäsitteinen, joten koska r_i on jaoton, niin järjestystä tarvittaessa vaihtamalla voidaan olettaa, että $kq_1 = k'r_1$ jollain $k' \in K[x]$. Silloin $q_1 = k^{-1}k'r_1$. Toisaalta r_1 ja q_1 ovat perusmuotoisia, joten on oltava $k^{-1}k' = 1$. Tällöin pätee $k = k'$, jolloin $m = 1$ ja edelleen yhtälön (1.8) perusteella $q_1 = r_1$. Alkuaskel siis pätee.

Tarkastellaan edelleen muotoa (1.7) olevaa polynomia. Oletetaan seuraavaksi, että $s \in \mathbb{N}, s > 1$ ja jollain s pätee $s = m$ ja $k = k'$. Oletetaan lisäksi, että polynomit q_i, $i = 1, \dots, s$, ovat samat kuin polynomit $q_i = r_j, j = 1, \dots, m$. Tarkastellaan seuraavaksi tilannetta

$$p = kq_1 \dots q_sq_{s+1} = k'r_1 \dots r_{m+1}. \tag{1.9}$$

Yhtälöstä (1.9) seuraa, että

$$q_{s+1} \mid r_1 \cdots r_{m+1},$$

jolloin soveltamalla jälleen lemmaa 1.13 saadaan

$$q_{s+1} \mid r_i$$

jollain $i = 1, \dots, m + 1$. Tarvittaessa merkintöjä vaihtamalla voidaan olettaa, että $q_{s+1} \mid r_{m+1}$. Koska kaikki polynomit r_i ja q_i ovat jaottomia, niin

$$q_{s+1} = hr_{m+1} \tag{1.10}$$

jollain $h \in K \setminus \{0\}$. Yhdistämällä yhtälöt (1.10) ja (1.9) saadaan

$$p = kq_1 \cdots q_sq_{s+1} = h^{-1}k'r_1 \cdots r_mq_{s+1} \cdots r_{m+1}. \tag{1.11}$$

Induktio-oletuksen nojalla jokaista polynomia $q_i, i = 1, \dots, s$, ovat samat kuin polynomit $r_j, j = 1, \dots, m$ ja $s = m$. Yhtälöistä (1.11) ja (1.10) nähdään, että myös $r_{s+1} = q_{s+1}$. Koska yksikään polynomi r_i ei ole vakio, niin täytyy olla $k = h^{-1}k'$ ja $s + 1 = m + 1$, joten väite on todistettu. □

Nyt on osoitettu, että jokaisella polynomilla on yksikäsitteinen tekijäesitys. Seuraava askel on etsiä välineitä, joilla saadaan selville, onko annettu polynomi jaoton vai jaollinen. Keinoja on useita, mutta tässä tutkielmassa esitellään Eisensteinin ehto. Siihen tarvitaan kuitenkin vielä kaksi lemmaa.

LEMMA 1.15. *Olkoot $q(x), r(x) \in \mathbb{Z}[x]$ polynomeja. Olkoon lisäksi p alkuluku, joka jakaa tulon qr renkaassa $\mathbb{Z}[x]$. Tällöin p jakaa polynomin q tai polynomin r renkaassa $\mathbb{Z}[x]$.*

TODISTUS. Olkoon

$$q = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$$

ja

$$r = \beta_0 + \beta_1 x + \cdots + \beta_m x^m.$$

Tehdään vastaväite ja oletetaan, että p ei jaa polynomia q eikä polynomia r. Tällöin p ei jaa myöskään kaikkia polynomien q ja r kertoimia. Siten on olemassa pienimmät sellaiset luvut i ja j, joille pätee $p \nmid \alpha_i$ ja $p \nmid \beta_j$. Alkuluku p jakaa kuitenkin tulon qr ja silloin p jakaa myös kaikki tulon kertoimet. Erityisesti p jakaa termin x^{i+j} kertoimen eli luvun

$$\alpha_0\beta_{i+j} + \alpha_1\beta_{1+j-1} + \cdots + \alpha_j\beta_i + \cdots + \alpha_{i+j}\beta_0. \tag{1.12}$$

Nyt p jakaa esityksen 1.12 kaikki muut termit, mutta ei välttämättä termiä $\alpha_j\beta_i$. Tämä seuraa siitä, miten i ja j on valittu. Toisaalta p jakaa koko esityksen 1.12, joten täytyy päteä $p \mid \alpha_j\beta_i$. Aikaisemmin valittiin kuitenkin i ja j siten, että $p \nmid \alpha_i$ ja $p \nmid \beta_j$. Koska p on alkuluku, syntyy ristiriita. □

LEMMA 1.16 (Gaussin lemma). *Olkoon $q \in \mathbb{Z}[x]$ jaoton polynomi renkaassa $\mathbb{Z}[x]$. Tällöin q on myös jaoton renkaassa $\mathbb{Q}[x]$.*

TODISTUS. Tehdään vastaväite ja oletetaan, että q on jaoton renkaassa $\mathbb{Z}[x]$, mutta jaollinen renkaassa $\mathbb{Q}[x]$. Tällöin $q = rs$, missä $r, s \in \mathbb{Q}[x]$ sekä $0 < \partial r, s < \partial q$. Olkoon

$$r = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$$

ja

$$s = \beta_0 + \beta_1 x + \cdots + \beta_m x^m$$

joillain $n, m \in \mathbb{N}, m, n \geq 1$. Koska r ja s ovat rationaalikertoimisia, niin $\alpha_i = \frac{a_i}{b_i}$ joillain $a_i \in \mathbb{Z}$ ja $b_i \in \mathbb{Z} \setminus \{0\}$ sekä $\beta_i = \frac{c_i}{d_i}$ joillain $c_i \in \mathbb{Z}$ ja $d_i \in \mathbb{Z} \setminus \{0\}$. Jos polynomi r kerrotaan kokonaisluvulla $k_b = b_0 \cdots b_n$, saadaan kokonaislukukertoiminen polynomi. Samoin käy, jos s kerrotaan luvulla $k_d = d_0 \cdots d_m$. Kerrotaan siis polynomi p luvulla $k = k_b k_d$, jolloin saadaan

$$k \cdot q = r_2 s_2, \tag{1.13}$$

missä r_2 ja s_2 ovat kokonaislukukertoimisia polynomeja. Koska $\partial(k \cdot q) = \partial q$, $\partial r_2 = \partial r$ ja $\partial s_2 = \partial s$, niin pätee $0 < \partial r_2 < \partial(k \cdot q)$ ja $0 < \partial s_2 < \partial(k \cdot q)$. Siten $k \cdot q$ on jaollinen renkaassa $\mathbb{Z}[x]$. Nyt päädytään ristiriitaan, jos voidaan osoittaa, että $k \cdot q$ on jaoton polynomi renkaassa $\mathbb{Z}[x]$. Tämä ei ole kuitenkaan itsestään selvää, sillä $\mathbb{Z}$ ei ole kunta.

Osoitetaan seuraavaksi induktiolla, että $k \cdot q$ on jaoton polynomi renkaassa $\mathbb{Z}[x]$ eli yhtälö (1.13) ei voi päteä. Luvulla k on nyt alkulukuesitys $k = p_1 \cdots p_l$. Tehdään induktio alkulukujen lukumäärän l suhteen. Olkoon ensiksi $l = 1$, eli k on alkuluku. Nyt lemman 1.15 nojalla $k = p_1$ jakaa polynomin r_2 tai polynomin s_2 renkaassa $\mathbb{Z}[x]$. Tarvittaessa merkintöjä vaihtamalla voidaan olettaa, että p_1 jakaa polynomin r_2. Tällöin $p_1 q = p_1 r_3 s_2$ jollekin renkaan $\mathbb{Z}[x]$ polynomille r_3, jonka aste on sama

kuin polynomeilla r ja r_2. Siten $q = r_3 s_2$ eli q on jaollinen renkaassa $\mathbb{Z}[x]$. Tämä on kuitenkin vastoin oletusta.

Oletetaan sitten, että polynomi $p_1 \cdots p_l \cdot q$ on jaoton renkaassa $\mathbb{Z}[x]$. Osoitetaan, että tällöin $p_1 \cdots p_{l+1} \cdot q$ eli polynomi $p_{l+1} p_1 \cdots p_l \cdot q$ on jaoton renkaassa $\mathbb{Z}[x]$. Tämä seuraa kuitenkin välittömästi alkuaskeleesta, sillä p_{l+1} on alkuluku ja $p_1 \cdots p_l \cdot q$ induktio-oletuksen nojalla jaoton polynomi renkaassa $\mathbb{Z}[x]$. Näin on todistettu induktiolla, että $k \cdot q$ on jaoton renkaassa $\mathbb{Z}[x]$. Tämä on kuitenkin ristiriita yhtälön (1.13) kanssa, joten q on jaoton renkaassa $\mathbb{Q}[x]$. □

LAUSE 1.17 (Eisensteinin ehto). *Olkoon $p(x) \in \mathbb{Z}[x]$ polynomi muotoa*

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

missä $a_i \in \mathbb{Z}$ kaikilla $i = 1, \ldots, n$, sekä $n \in \mathbb{N}, n \geq 1$. Tällöin p on jaoton polynomi renkaassa $\mathbb{Q}[x]$, jos on olemassa alkuluku t, jolle pätee

(1) $t \nmid a_n$,

(2) $t \mid a_i, i = 0, \ldots, n-1$,

(3) $t^2 \nmid a_0$.

TODISTUS. Tehdään vastaväite ja oletetaan, että kun väitteen ehdot (1)-(3) pätevät, niin p on jaollinen polynomi renkaassa $\mathbb{Q}[x]$. Tällöin lemman 1.16 nojalla p on jaollinen renkaassa $\mathbb{Z}[x]$. Siten on olemassa polynomit $q, r \in \mathbb{Z}[x]$, joille pätee $p = qr$ ja $\partial q, \partial r \geq 1$. Olkoot polynomit muotoa

$$q = b_0 + \cdots + b_m x^m$$

ja

$$r = c_0 + \cdots + c_k x^k,$$

kun $b_i, c_j \in \mathbb{Z}$ kaikilla $i = 1, \ldots, m$ ja $j = 1, \ldots, k$. Nyt $k, m \geq 1$ ja $m + k = n$. Polynomien tulon määritelmän perusteella $a_0 = b_0 c_0$. Koska t on lisäksi alkuluku, niin ehdon (2) perusteella $t \mid b_0$ tai $t \mid c_0$. Jos $t \mid b_0$ ja $t \mid c_0$, niin jollain $l_1, l_2 \in \mathbb{Z} \setminus \{0\}$ pätee $b_0 = l_1 t$ ja $c_0 = l_2 t$, jolloin $a_0 = b_0 c_0 = t^2 l_1 l_2$. Tämä on puolestaan vastoin ehtoa (3). Tarvittaessa merkintöjä vaihtamalla voidaan olettaa, että $t \mid b_0$ ja $t \nmid c_0$. Jos $t \mid b_i$ kaikilla $i = 0, \ldots, m$, niin $t \mid (b_m c_k)$ eli $t \mid a_n$, mikä on vastoin ehtoa (1). Olkoon $s \in \mathbb{N}, 1 \leq s \leq m$, pienin luku, jolle pätee $t \nmid b_s$. Tarkastellaan nyt termiä a_s. Polynomin tulon määritelmän nojalla sille pätee

$$a_s = b_0 c_s + b_1 c_{s-1} + \cdots + b_s c_0. \tag{1.14}$$

Tässä on huomattava, että voi olla $c_j = 0$, jollekin $j = 1, \ldots, s$, jos pätee $s > k$. Koska $m + k = n$ ja $k \geq 1$, niin $m < n$. Tällöin myös $s < n$, jolloin ehdon (2) nojalla

$$t \mid a_s. \tag{1.15}$$

Koska s on pienin luku, jolle pätee $t \nmid b_i$, niin $t \mid b_i c_j$ kaikilla $i = 1, \ldots, s-1$ ja $j = 0, \ldots, s-1$. Tällöin ehdon (1.15) ja yhtälön (1.14) nojalla täytyy päteä $t \mid b_s c_0$. Koska $t \nmid b_s$, niin täytyy olla $t \mid c_0$, mikä on vastoin oletusta. □

1.3. Polynomin nollakohdat

MÄÄRITELMÄ 1.18. Olkoon R rengas ja $p(x) \in R[X]$ polynomi. Polynomin p nollakohta on alkio $\alpha \in R$, jolle pätee $\bar{p}(\alpha) = 0$.

LAUSE 1.19. *Olkoon $K \subset \mathbb{C}$ kunta. Luku $\alpha \in K$ on polynomin $p \in K[x]$ nollakohta, jos ja vain jos polynomi $(x - \alpha)$ jakaa polynomin p renkaassa $K[x]$.*

TODISTUS. Oletetaan ensiksi, että polynomi $x - \alpha$ jakaa polynomin p. Tällöin $p = (x - \alpha)q$ jollekin polynomille $q \in K[x]$. Tällöin

$$\bar{p}(\alpha) = (\alpha - \alpha)\bar{q}(\alpha) = 0.$$

Todistetaan sitten toinen suunta. Oletetaan, että $\bar{p}(\alpha) = 0$ jollekin polynomille $p \in K[x]$. Tällöin polynomien jakoyhtälön (ks. [**12**, Theorem 2.8]) perusteella on olemassa sellaiset polynomit $q, r \in K[x]$, joille pätee

$$p = (x - \alpha)q + r \tag{1.16}$$

ja $\partial r < \partial(x - \alpha) = 1$. Tällöin r on vakiopolynomi eli $r \in K$. Polynomikuvaukselle $\bar{p}$ saadaan nyt

$$\bar{p}(\alpha) = (\alpha - \alpha)\bar{q}(\alpha) + r = 0.$$

Tällöin täytyy olla $r = 0$, jolloin yhtälön (1.16) perusteella $(x - \alpha) \mid p$. □

Edellisen lauseen valossa määritellään polynomin moninkertaiset nollakohdat seuraavasti.

MÄÄRITELMÄ 1.20. Olkoon $K \subset \mathbb{C}$ kunta. Alkio $\alpha \in K$ on polynomin p *yksinkertainen nollakohta*, jos $(x - \alpha) \mid p$, mutta $(x - \alpha)^2 \nmid p$. Alkio α on polynomin $p \in K[x]$ *m-kertainen nollakohta*, jos $(x - \alpha)^m \mid p$, mutta $(x - \alpha)^{m+1} \nmid p$. Jos α on polynomin p m-kertainen nollakohta ja $m \geq 2$, sanotaan, että α on polynomin p *moninkertainen nollakohta*.

Vielä ei kuitenkaan tiedetä, voidaanko jokainen polynomi esittää tulona muotoa $(x - \alpha)$ olevista polynomeista, sillä ei tiedetä, onko jokaisella polynomilla nollakohtia. Tämän ongelman ratkaisee seuraavaksi esiteltävä algebran peruslause, jota tullaan käyttämään tässä tutkielmassa useaan otteeseen. Sitä ei kuitenkaan todisteta.

LAUSE 1.21 (Algebran peruslause). *Olkoon $p(x)$ renkaan $\mathbb{C}[x]$ mielivaltainen polynomi, jolle pätee $\partial p \geq 1$. Tällöin polynomilla p on vähintään yksi nollakohta $\alpha \in \mathbb{C}$.*

Algebran peruslauseen todisti ensimmäisenä onnistuneesti Carl Friedrich Gauss 1799 väitöskirjassaan. Myöhemmin Gauss paranteli vielä todistustaan vielä kolmeen otteeseen. [**12**, Chapter 2] Modernisoitu versio eräästä Gaussin tasotopologiaan perustuvasta todistuksesta on esitetty esimerkiksi kirjassa [**5**]. Algebran peruslauseen voi todistaa helposti myös kompleksianalyysin avulla (ks. esimerkiksi [**5**, Chapter 5]). Sekä Gaussin todistuksen että kompleksianalyysissä esitettävän todistuksen heikkoudet ovat siinä, etteivät ne ole puhtaan algebrallisia, vaan niihin tarvitaan paljon algebran ulkopuolista matematiikkaa, kuten kompleksianalyysiä. Toisaalta algebran peruslauseelle ei edes ole olemassa puhtaan algebrallista todistusta johtuen siitä, että

reaaliluvut määritellään topologisten käsitteiden avulla. Algebran peruslauseelle on kuitenkin olemassa todistus, jossa käytetään vain yksinkertaista reaalilukujen analyysiä sekä Galois'n teoriaa. Tällainen on esimerkiksi Stewartin kirjan lopussa esitetty todistus [**12**, Chapter 23].

HUOMAUTUS 1.22. Käyttämällä algebran peruslausetta sekä lausetta 1.19 saadaan selville polynomin nollakohtien täsmällinen lukumäärä: polynomilla on muotoa $(x-\alpha)$ olevia tekijöitä täsmälleen asteensa verran. Tässä on tosin huomioitava, että osa nollakohdista voi olla samoja eli polynomilla voi olla määritelmän 1.20 mukaisia moninkertaisia nollakohtia.

Tämän kappaleen lopuksi palataan vielä huomautuksessa 1.6 esitettyyn ongelmaan siitä, milloin jokaista polynomifunktiota vastaa yksikäsitteinen polynomi. Seuraava lause osoittaa, että näin on silloin, kun polynomi kuuluu kuntaan, jossa on äärettömän monta alkiota.

LAUSE 1.23. *Olkoon K ääretön kunta sekä $p, q \in K[x]$ polynomeja. Jos tällöin $\bar{p} = \bar{q}$, niin $p = q$.*

TODISTUS. Tehdään vastaväite ja oletetaan, että $p \neq q$. Määritellään sitten polynomi $r = p - q$. Nyt oletuksen mukaan $r \neq 0$. Olkoon $\partial r = n$. Koska $\bar{p} = \bar{q}$, niin $p(\alpha) - q(\alpha) = 0$ kaikilla $\alpha \in K$. Tällöin myös $r(\alpha) = 0$ kaikilla α ja siten polynomi $r_{\alpha_i} = (x-\alpha_i)$ on polynomin r tekijä kaikilla $\alpha_i \in K$. Koska K on ääretön kunta, siihen kuuluu alkiot $\alpha_0, \alpha_1, \ldots, \alpha_n$, joita on $n+1$ kappaletta. Tällöin polynomi r saadaan muotoon

$$r = (x - \alpha_0)(x - \alpha_1) \cdots (x - \alpha_n) \cdot s, \tag{1.17}$$

missä $s \in K[x]$ on nollasta eroava polynomi. Polynomin r aste riippuu nyt polynomin s asteesta, mutta käyttämällä huomautusta 1.5 ja yhtälöä (1.17) saadaan polynomin r asteesta tieto

$$\partial r \geq \partial(x - \alpha_0) \cdots \partial(x - \alpha_n) = n + 1.$$

Polynomin r aste on kuitenkin n, joten ajaudutaan ristiriitaan.

□

Koska tässä tutkielmassa jokainen kunta sisältää kunnan $\mathbb{Q}$, niin jokainen käytettävä kunta on ääretön. Tällöin lause 1.23 on aina voimassa. Niinpä kunnista puhuttaessa käytetään polynomikuvauksesta samaa merkintää p kuin sitä vastaavalle polynomille.

LUKU 2

Kuntalaajennukset

2.1. Kuntalaajennukset

MÄÄRITELMÄ 2.1. Olkoot K ja L kuntia. Näiden kuntien välinen *kuntalaajennus* on monomorfismi $i : K \to L$. Tällöin kunta K on *pienempi* kunta ja kunta L *suurempi*.

MÄÄRITELMÄ 2.2. Olkoon $i : K \to L$ kuntalaajennus. Jos $K \subset L$, niin kuvaus i on *luonnollinen kuntalaajennus*. Tällöin kuvauksesta i käytetään merkintää $K \hookrightarrow L$. Tässä tutkielmassa oletetaan, että $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, vaikka lukualueita konstruoidessa huomataaan, ettei kyse ole tarkalleen ottaen inkluusioista. Näin ollen tässä tutkielmassa kuntien $\mathbb{Q}, \mathbb{R}$ ja $\mathbb{C}$ väliset kuntalaajennukset ovat myös luonnollisia kuntalaajennuksia.

Tämä tutkielma rajoittuu käsittelemään lähinnä luonnollisia kuntalaajennuksia. Suurin osa tutkielmassa esiintyvistä tuloksista voidaan kuitenkin pienellä lisävaivalla yleistää koskemaan kaikkia kuntalaajennuksia.

MÄÄRITELMÄ 2.3. Olkoot K ja L kuntia sekä $f : K \to L$ monomorfismi. Määritellään kuvaus $\hat{f} : K[x] \to L[x]$ siten, että

$$\hat{f}(k_0 + k_1 x + \cdots + k_n x^n) = f(k_0) + f(k_1)x + \cdots + f(k_n)x^n$$

kun $k_0, k_1, \ldots, k_n \in K$.

Määritelmän 2.3 ideana on laajentaa kuntalaajennuksen käsite myös polynomirenkaille. Tarkoituksena siis on, että jokaista kuntalaajennusta f vastaa kuvaus $\hat{f}$, joka kuntalaajennuksen f pienempää ja suurempaa kuntaa vastaavien polynomirenkaiden välinen kuvaus. Tämän vuoksi on tärkeää, että kuvaus $\hat{f}$ käyttäytyy kuten kuntalaajennus, minkä sanoo seuraava lause.

LAUSE 2.4. *Kuvaus $\hat{f}$ on monomorfismi. Lisäksi jos f on isomorfismi, niin myös $\hat{f}$ on isomorfismi.*

TODISTUS. Todistetaan ensiksi, että $\hat{f}$ on homomorfismi. Kaikilla $b_0, \ldots, b_m \in K$ pätee

$$\begin{aligned}
&\hat{f}(a_0 + \cdots + a_n x^n + b_0 + \cdots + b_m x^m) \\
&= f(a_0) + \cdots + f(a_n)x^n + f(b_0) + \cdots + f(a_m)x^m \\
&= \hat{f}(a_0 + \cdots + a_n x^n) + \hat{f}(b_0 + \cdots + b_m x^m).
\end{aligned}$$

Toisaalta polynomien tulon määritelmän mukaan

$$\hat{f}\Big((\sum_{k=0}^{n} a_k x^k)(\sum_{k=0}^{m} b_k x^k) \Big) = \hat{f}\Big(\sum_{k=0}^{n+m} (\sum_{i+j=k} a_i b_j) x^k \Big). \tag{2.1}$$

Käytetään kuvauksen $\hat{f}$ määritelmää, jolloin saadaan

$$\hat{f}\Big(\sum_{k=0}^{n+m} (\sum_{i+j=k} a_i b_j) x^k \Big) = \sum_{k=0}^{n+m} f(\sum_{i+j=k} a_i b_j) x^k. \tag{2.2}$$

Koska f on homomorfismi, niin pätee

$$\sum_{k=0}^{n+m} f(\sum_{i+j=k} a_i b_j) x^k = \sum_{k=0}^{n+m} (\sum_{i+j=k} f(a_i) f(b_j)) x^k \tag{2.3}$$

Käyttämällä ensin polynomien tulon määritelmää ja seuraavaksi kuvauksen $\hat{f}$ määritelmää saadaan

$$\sum_{k=0}^{n+m} (\sum_{i+j=k} f(a_i) f(b_j)) x^k = \hat{f}\Big(\sum_{k=0}^{n} a_k x^k \Big) \hat{f}\Big(\sum_{k=0}^{m} b_k x^k \Big), \tag{2.4}$$

jolloin kohdista (2.1)-(2.4) seuraa, että $\hat{f}$ on homomorfismi. Monomorfismiksi osoittamiseen vaaditaan, että $\hat{f}$ on injektio. Olkoon siis $a'_0, \ldots, a'_m \in K$. Oletetaan, että

$$\hat{f}(a_0 + \cdots + a_n x^n) = \hat{f}(a'_0 + \cdots + a'_m x^m). \tag{2.5}$$

Tämä yhtäpitävää sen kanssa, että

$$f(a_0) + \cdots + f(a_n) x^n = f(a'_0) + \cdots + f(a'_m) x^m. \tag{2.6}$$

Tarvittaessa merkintöjä vaihtamalla voidaan olettaa, että $n \leq m$. Koska jokainen $x^i, i = 0, \ldots, n$ esiintyy kummallakin puolilla täsmälleen kerran, on oltava

$$f(a_i) = f(a'_i) \tag{2.7}$$

kaikilla $i = 0, \ldots, n$ sekä

$$a'_i = 0, \qquad \text{kun } i > m. \tag{2.8}$$

Yhtälöistä (2.6), (2.7) ja (2.8) seuraa, että

$$a_0 + \cdots + a_n x^n = a'_0 + \cdots + a'_m x^m \tag{2.9}$$

ja koska (2.9) on yhtäpitävää yhtälön (2.5) kanssa, niin $\hat{f}$ on injektio.

Oletetaan seuraavaksi, että f on isomorfismi. Tällöin f on surjektio eli $f(K) = L$. Tällöin jokainen $b \in L$ voidaan ilmoittaa muodossa

$$b = f(a_i), \tag{2.10}$$

missä $a_i \in K$. Olkoon seuraavaksi $p \in K[x]$ mielivaltainen polynomi. Se on muotoa

$$p = b_0 + \cdots + b_n x^n, \tag{2.11}$$

missä $b_i \in L$. Tällöin yhdistämällä yhtälöt (2.10) ja (2.11) saadaan

$$p = f(a_0) + \cdots + f(a_n) x^n, \tag{2.12}$$

missä $a_i \in K$. Nyt voidaan käyttää kuvauksen $\hat{f}$ määritelmää, jolloin yhtälö (2.12) on yhtäpitävää sen kanssa, että

$$p = \hat{f}(a_0 + \cdots + a_n x^n). \tag{2.13}$$

Koska yhtälöt (2.13) ja (2.11) ovat siis yhtäpitäviä, niin $L[x] \subset \hat{f}(K[x])$ ja koska selvästi $\hat{f}(K[x]) \subset L[x]$, niin $\hat{f}(K[x]) = L[x]$. Siten $\hat{f}$ on surjektio ja koska $\hat{f}$ on monomorfismi, niin se on bijektiivinen homomorfismi eli isomorfismi. □

Jatkossa merkintää $\hat{f}$ ei enää käytetä. Sen sijaan, koska myös $\hat{f}$ on monomorfismi, käytetään merkintää $\hat{f} = f$. Tällöin samaistetaan toisiinsa kuntalaajennus $f : K \to L$ sekä sitä vastaava polynomirenkaiden välinen monomorfismi $\hat{f} : K[x] \to L[x]$. Tämä ei aiheuta sekaannusta, sillä $\hat{f}(k) = f(k)$ kaikilla $k \in K$.

Seuraavaksi on tarkoituksena luokitella kuntalaajennuksia niiden ominaisuuksien perusteella ottamalla käyttöön joukko määritelmiä.

MÄÄRITELMÄ 2.5. Olkoon $A \subset \mathbb{C}$ joukko. Joukon A *virittämä kunta* on leikkaus kaikista niistä kunnan $\mathbb{C}$ alikunnista, jotka sisältävät joukon A.

MÄÄRITELMÄ 2.6. Olkoot $K \subset L \subset \mathbb{C}$ kuntia, $K \hookrightarrow L$ kuntalaajennus ja $A \subset L$ joukko. Tällöin *liittämällä* joukko A kuntaan K saadaan kunta, jonka virittää joukko $K \cup A$. Liittämällä saadusta kunnasta käytetään merkintää $K(A)$. Jos $A = \{\alpha_1, \ldots, \alpha_n\}$, niin käytetään merkintää $K(A) = K(\alpha_1, \ldots, \alpha_n)$.

MÄÄRITELMÄ 2.7. Olkoot $K \subset L \subset \mathbb{C}$ kuntia. Kuntalaajennus $K \hookrightarrow L$ on *yksinkertainen*, jos $L = K(\alpha)$ jollekin $\alpha \in L$.

MÄÄRITELMÄ 2.8. Olkoon $K \subset \mathbb{C}$ kunta ja olkoon $\alpha \in \mathbb{C}$. Sanotaan, että luku α on *algebrallinen kunnan K suhteen*, jos on olemassa nollasta poikkeava polynomi $p(x) \in K[x]$, jolle pätee $p(\alpha) = 0$. Jos tällaista polynomia ei ole, α on *transkendentti kunnan K suhteen*. Jos $\alpha \in \mathbb{C}$ on algebrallinen kunnan $\mathbb{Q}$ suhteen, sanotaan lyhyesti, että α on algebrallinen.

MÄÄRITELMÄ 2.9. Olkoot $K \subset L \subset \mathbb{C}$ kuntia. Kuntalaajennus $K \hookrightarrow L$ on algebrallinen, jos jokainen kunnan L alkio on algebrallinen kunnan K suhteen. Jos kunnassa L on kunnan K suhteen transkendentti alkio, sanotaan, että kuntalaajennus $K \hookrightarrow L$ on transkendentti.

MÄÄRITELMÄ 2.10. Olkoot $f : K \to K'$ ja $g : L \to L'$ kuntalaajennuksia. Näiden *kuntalaajennusten välinen ismorfismi* on kuvauspari (ϕ, γ), missä $\phi : K \to L$ ja $\gamma : K' \to L'$ ovat isomorfismeja, joille pätee

$$g(\phi(k)) = \gamma(f(k))$$

kaikilla $k \in K$. Kuntalaajennukset g ja f *ovat isomorfiset*, jos on olemassa niiden välinen isomorfismi.

Määritelmää 2.10 voidaan kuvallisesti havainnollistaa seuraavalla kaaviolla:

$$\begin{array}{ccc} K & \xrightarrow{f} & K' \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\gamma} \\ L & \xrightarrow[g]{} & L' \end{array}$$

Jos kuntalaajennukset f ja g ovat isomorfiset, niin kaavio kommutoi. Toisin sanoen jos kuljetaan kunnasta K kuntaan L' kunnan L kautta, päädytään samaan kuvaukseen kuin kulkemalla kunnan K' kautta. Puhuttaessa luonnollisista kuntalaajennuksista voidaan samastaa kunta K sen kuvajoukkoon $f(K)$, jolloin $f(K) = K$ ja $g(L) = L$. Tällöin kuvaajan kommutoimiseksi riittää todeta, että $\gamma|_K = \phi$.

Määritelmä 2.10 herättää kysymyksen, milloin kaksi kuntalaajennusta ovat isomorfiset. Ovatko esimerkiksi yksinkertaiset kuntalaajennukset $K \hookrightarrow K(\alpha)$ ja $K \hookrightarrow K(\beta)$ aina isomorfiset? Jos α ja β ovat transkendentteja kunnan K suhteen, niin näin todellakin on, mutta algebrallisessa tapauksessa väite ei päde. Kuitenkin viidennen asteen yhtälön nollakohtien etsimisessä juuri algebralliset kuntalaajennukset ovat kiintoisia. Tarvitaan hieman lisäehtoja, jotta yksinkertaiset algebralliset kuntalaajennukset voidaan osoittaa isomorfisiksi. Sitä ennen on kuitenkin perehdyttävä tarkemmin yksinkertaisiin algebrallisiin kuntalaajennuksiin.

2.2. Minimaalipolynomit

Määritelmä 2.11. Olkoon $K \hookrightarrow L$ kuntalaajennus ja olkoon $\alpha \in L$ algebrallinen kunnan K suhteen. Alkion α *minimaalipolynomi* on pienintä mahdollista astetta oleva perusmuotoinen polynomi $m(x) \in K[x]$, jolle pätee $m(\alpha) = 0$.

Lause 2.12. *Olkoon $K \hookrightarrow L$ kuntalaajennus ja $\alpha \in L$ algebrallinen kunnan K suhteen. Luvulla α on minimaalipolynomi $p(x) \in K[x]$ ja se on yksikäsitteinen.*

Todistus. Osoitetaan ensiksi, että minimaalipolynomi on olemassa. Koska α on algebrallinen kunnan K suhteen, niin on olemassa polynomi $q(x) \in K[x] \setminus \{0\}$, jolle pätee $q(\alpha) = 0$. Olkoon polynomin q aste n ja sen johtava kerroin $a_n \in K$. Koska $q \neq 0$, niin $a_n \neq 0$. Tällöin on olemassa $a_n^{-1} \in K$. Nyt polynomi $r = a_n^{-1}q$ on perusmuotoinen ja sille pätee

$$r(\alpha) = a_n^{-1}q(\alpha) = 0.$$

On siis olemassa vähintään yksi polynomi, joka on perusmuotoinen ja jolle pätee $p(\alpha) = 0$. Siten näiden kaikkien polynomien joukosta voidaan valita myös pienintä astetta oleva tällainen polynomi.

Todistetaan seuravaaksi minimaalipolynomin yksikäsitteisyys. Olkoot p ja q alkion $\alpha \in L$ minimaalipolynomeja. Koska minimaalipoynomi on pienintä mahdollista astetta oleva polynomi m, jolle $m(\alpha) = 0$, niin $\partial p = \partial q$. Koska p ja q ovat perusmuotoisia, niin täytyy olla

$$\partial(p - q) < \partial p = \partial q. \tag{2.14}$$

Jos $p - q = 0$, niin $p = q$ ja väite on todistettu. Voidaan siis olettaa, että $p \neq q$ eli $p - q \neq 0$. Tällöin jos polynomi $p - q$ on astetta k, niin sillä on johtava kerroin $a_k \in K \setminus \{0\}$. Koska K on kunta, niin myös $a_k^{-1} \in K \setminus \{0\}$, jolloin on olemassa perusmuotoinen polynomi $r = a_k^{-1}(p-q)$. Sen asteelle pätee yhtälön (2.14) perusteella

$$\partial r = \partial(p - q) < \partial p = \partial q. \tag{2.15}$$

Lisäksi polynomille r pätee

$$r(\alpha) = a_k^{-1}(p(\alpha) - q(\alpha)) = a_k^{-1} \cdot 0 = 0. \tag{2.16}$$

Yhtälöiden (2.15) ja (2.16) nojalla polynomit p ja q eivät voi olla alkion α minimaalipolynomeja, mikä on ristiriidassa oletuksen kanssa. Näin ollen tapaus $p \neq q$ on mahdoton ja siten $p = q$. □

Lause 2.13. *Olkoon $K \subset \mathbb{C}$ kunta ja $\alpha \in \mathbb{C}$ algebrallinen kunnan K suhteen. Tällöin luvun α minimaalipolynomi $m(x) \in K[x]$ on jaoton polynomi renkaassa $K[x]$.*

Todistus. Tehdään vastaväite ja oletetaan, että luvun $\alpha \in K$ minimaalipolynomi m ei ole jaoton. Tällöin se on muotoa $m = pq$, missä $p, q \in K[x]$ ovat polynomeja. Polynomien asteille pätee $1 \leq \partial p < \partial m$ ja $1 \leq \partial q < \partial m$. Olkoon a polynomin p johtava kerroin ja b polynomin q johtava kerroin. Koska K on kunta, niin $a^{-1}, b^{-1} \in K$. Nyt pätee

$$a^{-1}p(\alpha)b^{-1}q(\alpha) = a^{-1}b^{-1}m(\alpha) = 0,$$

joten $a^{-1}p(\alpha) = 0$ tai $b^{-1}q(\alpha) = 0$. Nyt sekä $a^{-1}p$ että $b^{-1}q$ ovat perusmuotoisia polynomeja, joiden aste on pienempi kuin polynomin m aste. Tämä tarkoittaa kuitenkin sitä, ettei m voi olla luvun α minimaalipolynomi. Syntynyt ristiriita todistaa väitteen. □

Lemma 2.14. *Olkoon $K \subset \mathbb{C}$ kunta ja $\alpha \in \mathbb{C}$ algebrallinen kunnan K suhteen. Olkoon lisäksi $p(x) \in K[x]$ polynomi, jonka nollakohta on α. Tällöin luvun α minimaalipolynomi $m(x) \in K[x]$ jakaa polynomin p renkaassa $K[x]$.*

Todistus. Olkoon $p(x) \in K[x]$ polynomi, jolle $p(\alpha) = 0$. Polynomien jakoyhtälön mukaan on olemassa polynomit $q(x) \in K[x]$ ja $r(x) \in K[x]$ siten, että

$$p = mq + r \tag{2.17}$$

ja

$$\partial r < \partial m. \tag{2.18}$$

Jos $r = 0$, niin polynomi m jakaa polynomin p. Oletetaan siis, että $r \neq 0$. Olkoon polynomin r aste n ja $a_n \in K \setminus \{0\}$ polynomin r johtava kerroin. Nyt myös $a_n^{-1} \in K \setminus \{0\}$, joten polynomi $a_n^{-1}r \in K[x]$ ja on perusmuotoinen. Koska $p(\alpha) = 0$ ja $m(\alpha) = 0$, niin täytyy olla $r(\alpha) = 0$, yhtälön (2.17) mukaan. Kohdan (2.18) ja minimaalipolynomin määritelmän perusteella tästä seuraa, ettei m ei voi olla luvun α minimaalipolynomi. Ajaudutaan ristiriitaan, joten täytyy olla $r = 0$, jolloin väite pätee. □

Lause 2.15. *Olkoon $K \hookrightarrow L$ kuntalaajennus ja $L \subset \mathbb{C}$. Jos $\alpha \in L$ on algebrallinen kunnan K suhteen ja p perusmuotoinen ja renkaassa $K[x]$ jaoton polynomi, jolle pätee $p(\alpha) = 0$, niin p on luvun α minimaalipolynomi.*

TODISTUS. Olkoon m luvun α minimaalipolynomi. Tällöin lemmasta 2.14 seuraa, että m jakaa polynomin p. Koska m ei ole vakio ja p on jaoton, niin tämä tilanne on mahdollista vain, jos $p = mk$ jollain vakiolla $k \in K$. Sekä p että m ovat kuitenkin perusmuotoisia, joten on oltava $k = 1$, ja siten $p = m$. □

Lauseessa 2.12 todistettiin, että kaikilla algebrallisilla luvuilla on minimaalipolynomi. Seuraavaksi lauseessa 2.16 todistetaan, että myös käänteinen väite pätee: jokainen jaoton ja perusmuotoinen vakiosta poikkeava polynomi on jonkin luvun minimaalipolynomi.

LAUSE 2.16. *Olkoon $K \subset \mathbb{C}$ kunta ja $p(x) \in K[x]$ mikä tahansa vakiosta poikkeava, jaoton ja perusmuotoinen polynomi. Tällöin on olemassa kunnan K suhteen algebrallinen luku $\alpha \in \mathbb{C}$, jonka minimaalipolynomi p on.*

TODISTUS. Koska p ei ole vakiopolynomi, sillä on algebran peruslauseen nojalla vähintään yksi nollakohta $\alpha \in \mathbb{C}$. Tällöin luku $\alpha \in \mathbb{C}$ on algebrallinen kunnan K suhteen. Koska p on perusmuotoinen ja vakio, niin lauseesta 2.15 seuraa, että p on luvun α minimaalipolynomi. □

2.3. Yksinkertaiset algebralliset kuntalaajennukset

LEMMA 2.17. *Olkoon $K \subset \mathbb{C}$ kunta ja olkoon $\alpha \in \mathbb{C}$. Olkoon lisäksi $K \hookrightarrow K(\alpha)$ kuntalaajennus. Tällöin jokainen alkio $y \in K(\alpha)$ voidaan ilmoittaa muodossa*

$$y = q(\alpha) \cdot r(\alpha)^{-1},$$

missä $q, r \in K[x]$ ja $r(\alpha) \neq 0$.

TODISTUS. Olkoon

$$L = \{q(\alpha)r(\alpha)^{-1} : q, r \in K[x], r(\alpha) \neq 0\}.$$

Koska $q, r \in K[x]$, $K \subset K(\alpha)$ ja $\alpha \in K(\alpha)$, niin $L \subset K(\alpha)$.

Osoitetaan seuraavaksi, että L on kunta. Koska $L \subset K(\alpha)$, niin assosiatiivisuus, kommutatiivisuus ja distributiivisuus ovat selviä. Jos $q_1, q_2, r_1, r_2 \in L$, niin

$$\begin{aligned} &q_1(\alpha)r_1(\alpha)^{-1} + q_2(\alpha)r_2(\alpha)^{-1} \\ =&r_1(\alpha)^{-1}r_2(\alpha)^{-1}(q_1(\alpha)r_2(\alpha) + q_2(\alpha)r_1(\alpha)) \\ =&(q_1r_2 + q_2r_1)(\alpha)(r_1r_2(\alpha))^{-1} \in L, \end{aligned}$$

joten L on yhteenlaskun suhteen suljettu. Lisäksi

$$\begin{aligned} &q_1(\alpha)r_1(\alpha)^{-1} \cdot q_2(\alpha)r_2(\alpha)^{-1} \\ =&(q_1q_2)(\alpha)(r_1r_2(\alpha))^{-1} \in L, \end{aligned}$$

joten L on myös kertolaskun suhteen suljettu. Joukossa L jokaisella alkiolla on vastaalkio, sillä

$$-q(\alpha)r(\alpha)^{-1} = (-q)(\alpha)r(\alpha)^{-1} \in L.$$

Myös käänteisalkiot ovat joukossa L, sillä kun $q(\alpha) \neq 0$

$$(q(\alpha)r(\alpha)^{-1})^{-1} = r(\alpha)q(\alpha)^{-1}.$$

Näin ollen L on kunnan $K(\alpha)$ alikunta.

Jos $k \in K$ on mielivaltainen, niin valitsemalla $r = 1$ ja $q = k$ huomataan, että $k \in L$. Siten $K \subset L$. Toisaalta jos valitaan $r = 1$ ja $q = x$, niin saadaan $\alpha \in L$. Täytyy siis olla $K \cup \{\alpha\} \subset L$. Määritelmistä 2.6 ja 2.5 nähdään kuitenkin, että pienin mahdollinen kunta, joka sisältää joukon K ja alkion α on kunta $K(\alpha)$. Niinpä on oltava $K(\alpha) \subset L$ ja edelleen $K(\alpha) = L$, mikä todistaa väitteen. □

LEMMA 2.18. *Olkoon $K \subset \mathbb{C}$ kunta ja $K \hookrightarrow K(\alpha)$ yksinkertainen algebrallinen kuntalaajennus. Olkoon lisäksi m luvun $\alpha \in \mathbb{C}$ minimaalipolynomi kunnan K suhteen. Tällöin kaikille $y \in K(\alpha)$ on olemassa yksikäsitteinen polynomi $p(x) \in K[x]$, jolle $p(\alpha) = y$ ja $\partial p < \partial m$.*

TODISTUS. Lemman 2.17 mukaan

$$y = q(\alpha)r(\alpha)^{-1} \tag{2.19}$$

joillekin polynomeille $q, r \in K[x]$, missä $r(\alpha) \neq 0$. Koska $m(\alpha) = 0$ ja toisaalta $r(\alpha) \neq 0$, niin m ei voi jakaa polynomia r. Koska m on minimaalipolynomina lauseen 2.13 mukaan jaoton, niin polynomien m ja r suurin yhteinen tekijä on vakiopolynomi 1. Siten Bézout'n lauseen mukaan on olemassa polynomit $a, b \in K[x]$, joille pätee

$$am + br = 1. \tag{2.20}$$

Koska $m(\alpha) = 0$, niin yhtälöstä (2.20) seuraa, että

$$b(\alpha)r(\alpha) = 1.$$

Tämä on yhtäpitävää sen kanssa, että

$$r(\alpha)^{-1} = b(\alpha). \tag{2.21}$$

Nyt sijoittamalla yhtälö (2.21) yhtälöön (2.19) saadaan

$$y = q(\alpha)b(\alpha) = (qb)(\alpha). \tag{2.22}$$

Polynomien jakoyhtälön nojalla on olemassa sellaiset polynomit $c, p \in K[x]$, joille pätee

$$qb = cm + p. \tag{2.23}$$

ja

$$\partial p < \partial m. \tag{2.24}$$

Yhdistämällä yhtälöt (2.22) ja (2.23) saadaan

$$y = c(\alpha)m(\alpha) + p(\alpha),$$

ja koska $m(\alpha) = 0$, niin

$$y = p(\alpha). \tag{2.25}$$

Yhtälöiden (2.25) ja (2.24) nojalla etsitty polynomi p on löydetty. Osoitetaan vielä, että se on yksikäsitteinen. Olkoot polynomit $p_1, p_2 \in K[x]$, joille $y = p_1(\alpha) = p_2(\alpha)$ sekä $\partial p_1 < \partial m$ ja $\partial p_2 < \partial m$. Koska $p_1(\alpha) = p_2(\alpha)$, niin $p_1(\alpha) - p_2(\alpha) = 0$, jolloin $(p_1 - p_2)(\alpha) = 0$. Jos $p_1 - p_2 \neq 0$, niin tarvittaessa kertomalla polynomi $p_1 - p_2$ sen johtavan kertoimen käänteisluvulla voidaan olettaa sen olevan perusmuotoinen.

Koska $\partial(p_1 - p_2) < \partial m$, niin m ei voi olla tällöin luvun α minimaalipolynomi. On siis oltava $p_1 = p_2$. □

Nyt kyetään todistamaan tämän kappaleen päätulos, joka kertoo, milloin yksinkertaiset algebralliset kuntalaajennukset ovat isomorfiset.

LAUSE 2.19. *Olkoot $K \subset \mathbb{C}$ ja $L \subset \mathbb{C}$ kuntia ja $f : K \to L$ isomorfismi. Olkoot lisäksi $K \hookrightarrow K(\alpha)$ ja $L \hookrightarrow L(\beta)$ yksinkertaisia algebrallisia kuntalaajennuksia. Olkoot alkioiden α ja β minimaalipolynomit $m_\alpha \in K[x]$ ja $m_\beta \in L[x]$, joille pätee $m_\beta = f(m_\alpha)$. Tällöin on olemassa isomorfismi $g : K(\alpha) \to L(\beta)$, jolle pätee $g|_K = f$ ja $g(\alpha) = \beta$.*

TODISTUS. Lauseesta voidaan esittää seuraavanlainen kaavio:

$$\begin{array}{ccc} K & \longrightarrow & K(\alpha) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ L & \longrightarrow & L(\beta) \end{array}$$

Täytyy siis löytää kuvaus g ja saada kaavio kommutoimaan. Lemman 2.18 nojalla voidaan jokaiselle $y \in K(\alpha)$ valita yksikäsitteinen polynomi $p_y \in K[x]$. Sille pätee

$$y = p_y(\alpha) \tag{2.26}$$

ja $\partial p_y < \partial m_\alpha$. Määritellään kuvaus $g : K(\alpha) \to L(\beta)$ asettamalla kaikille $y \in K(\alpha)$

$$g(y) = f(p_y)(\beta) \in L(\beta). \tag{2.27}$$

Koska lemman 2.18 mukaan valittu polynomi p_y on yksikäsitteinen, g on todellakin kuvaus. Täytyy osoittaa, että se on isomorfismi. Aloitetaan tämä osoittamalla, että g on homomorfismi eli jos $a, b \in K(\alpha)$, niin

$$g(a + b) = g(a) + g(b) \tag{2.28}$$

ja

$$g(ab) = g(a)g(b). \tag{2.29}$$

Jos $a, b \in K(\alpha)$, niin yhtälön (2.26) mukaan pätee

$$a + b = p_a(\alpha) + p_b(\alpha) = (p_a + p_b)(\alpha). \tag{2.30}$$

Lisäksi koska $\partial p_y < \partial m_\alpha$ kaikilla $y \in K(\alpha)$, niin $\partial(p_a + p_b) < \partial m_\alpha$. Siten voidaan käyttää kuvauksen g määritelmää (2.27), jolloin yhtälöstä (2.30) saadaan

$$g(a + b) = f(p_a + p_b)(\beta). \tag{2.31}$$

Tällöin koska f on homomorfismi ja yhtälö (2.31) pätee, niin

$$g(a + b) = f(p_a + p_b)(\beta) = f(p_a)(\beta) + f(p_b)(\beta) = g(a) + g(b),$$

mikä toteuttaa vaatimuksen (2.28). Tarkastellaan seuraavaksi kertolaskua. Luvulla $ab \in K(\alpha)$ on esitys

$$ab = p_{ab}(\alpha).$$

Tällöin $g(ab)$ on muotoa

$$g(ab) = f(p_{ab})(\beta).$$

Täytyy siis osoittaa, että $g(ab) = g(a)g(b)$ eli

$$f(p_{ab})(\beta) = f(p_a)(\beta)f(p_b)(\beta). \tag{2.32}$$

Koska f on homomorfismi, niin väite (2.32) tulee muotoon

$$f(p_{ab})(\beta) = f(p_a p_b)(\beta). \tag{2.33}$$

Tarkastellaan seuraavaksi polynomia $p_a p_b - p_{ab}$. Sille pätee

$$p_a p_b(\alpha) - p_{ab}(\alpha) = p_a(\alpha)p_b(\alpha) - p_{ab}(\alpha) = ab - ab = 0.$$

Tällöin lemman 2.14 mukaan luvun α minimaalipolynomi m_α jakaa polynomin $p_a p_b - p_{ab}$. Toisin sanoen on olemassa polynomi $q \in K[x]$, jolle pätee

$$p_a p_b - p_{ab} = m_\alpha q. \tag{2.34}$$

Koska f on homomorfismi, saadaan yhtälö (2.34) muotoon

$$f(p_a p_b)(\beta) - f(p_{ab})(\beta) = f(m_\alpha)(\beta)f(q)(\beta). \tag{2.35}$$

Polynomi $f(m_\alpha)$ on oletuksen nojalla polynomin luvun β minimaalipolynomi, jolloin pätee $f(m_\alpha)(\beta) = 0$. Tällöin yhtälöstä (2.35) seuraa, että

$$f(p_a p_b)(\beta) - f(p_{ab})(\beta) = 0,$$

mikä on väite (2.29) uudelleen muotoiltuna. Siten g on homomorfismi.

Osoitetaan seuraavaksi, että g on isomorfismi konstruoimalla sille käänteiskuvaus. Olkoon $z \in L(\beta)$. Lemman 2.18 mukaan alkiolla $z \in L(\beta)$ on esitys

$$z = p_z(\beta),\ \partial p_z < \partial m_\beta \tag{2.36}$$

Koska f on isomorfismi, sillä on käänteiskuvaus, jolloin voidaan määritellä kuvaus $h : L(\beta) \to K(\alpha)$ seuraavasti:

$$h(z) = f^{-1}(p_z)(\alpha). \tag{2.37}$$

Jotta saataisiin todistetuksi, että h todella on kuvauksen g käänteiskuvaus, niin täytyy osoittaa, että

$$h \circ g = I_{K(\alpha)} \tag{2.38}$$

ja

$$g \circ h = I_{L(\beta)}. \tag{2.39}$$

Jos $y \in K(\alpha)$, niin

$$g(y) = f(p_y)(\beta).$$

Kuvaukset h ja g voidaan yhdistää vain, jos $g(x)$ on muotoa (2.36). Täytyy siis osoittaa, että $\partial f(p_y) < \partial m_\beta$. Koska f homomorfismina säilyttää polynomin asteen, niin riittä osoittaa, että $\partial p_y < \partial m_\beta$. Koska $m_\beta = f(m_\alpha)$ ja f säilyttää asteen, niin $\partial m_\beta = \partial m_\alpha$. Toisaalta lemman 2.18 perusteella $\partial p_y < \partial m_\alpha$, joten $g(x)$ on muotoa (2.36). Näin ollen yhdistetty kuvaus saadan käyttämällä kuvauksen h määritelmää (2.37):

$$h((g(y)) = f^{-1}f(p_y)(\alpha) = p_y(\alpha).$$

Koska $y = p_y(\alpha)$, niin $h \circ g(y) = x$, mikä todistaa väitteen (2.38).

Väite (2.39) eli tapaus $g \circ h$ käsitellään täysin vastaavasti. Määritelmänsä mukaan

$$h(z) = f^{-1}(p_z)(\alpha)$$

ja se on muotoa (2.26), sillä $\partial p_z < \partial m_\alpha$. Siten

$$gh(z) = ff^{-1}(p_z)(\beta) = z,$$

mikä todistaa väitteen (2.39).

On siis osoitettu, että g on isomorfismi. Osoitetaan seuraavaksi, että $g(\alpha) = \beta$. Jos $\alpha \in K$, niin luvun α minimaalipolynomi on selvästi polynomi $x - \alpha \in K[x]$. Lemman 2.18 mukainen yksikäsitteinen esitys sille on $p_\alpha(\alpha)$, missä $p_\alpha = \alpha$ on vakiopolynomi. Tällöin saadaan

$$g(\alpha) = f(p_\alpha)(\beta) = f(\alpha). \tag{2.40}$$

Koska $f(m_\alpha)$ on luvun β minimaalipolynomi, niin β on polynomin $f(m_\alpha)$ nollakohta. Toisaalta koska $m_\alpha = x - \alpha$, niin

$$f(m_\alpha) = x - f(\alpha). \tag{2.41}$$

Tällä yhtälön (2.41) polynomilla voi olla vain yksi nollakohta. Koska $f(m_\alpha)$ on luvun β minimaalipolynomi, niin tämä nollakohta on β. Toisaalta myös $f(\alpha)$ on tämä ainoa nollakohta eli $f(\alpha) = \beta$. Tästä saadaan yhtälöä (2.40) käyttämällä

$$g(\alpha) = \beta.$$

Oletetaan sitten, että $\alpha \notin K$. Pätee $\partial m_\alpha \geq 1$, sillä m_α on minimaalipolynomi. Lisäksi jos olisi $\partial m_\alpha = 1$, niin pätisi $\alpha \in K$, mikä on mahdotonta. Voidaan siis olettaa, että $\partial m_\alpha \geq 2$. Tällöin luvulla $\alpha \in K(\alpha)$ on esitys $\alpha = p_\alpha(\alpha)$, missä $p_\alpha = x$ ja $\partial p_\alpha < \partial m_\alpha$.

Koska f on homomorfismi, sille pätee

$$f(x) = f(1 \cdot x + 0) = f(1) \cdot x + f(0) = 1 \cdot x + 0 = x. \tag{2.42}$$

Nyt voidaan käyttää kuvauksen g määritelmää (2.27) ja yhtälöä (2.42), jolloin saadaan

$$g(\alpha) = f(p_\alpha)(\beta) = f(x)(\beta) = x(\beta) = \beta,$$

joten myös tällöin väite pätee.

Jäljelle jää vielä osoittaa, että $g|_K = f$. On siis todistettava, että

$$g(k) = f(k) \tag{2.43}$$

kaikilla $k \in K$. Nyt luvulla $k \in K(\alpha)$ on lemman 2.18 mukaan esitys $k = p_k(\alpha)$. Vakiopolynomi $p_k = k$ toteuttaa tämän vaatimuksen. Lisäksi $\partial p_k = 0 < \partial m_\alpha$, joten $p_k = k$ on todella lemman 2.18 mukainen yksikäsitteinen esitys. Voidaan siis käyttää kuvauksen g määritelmää, jolloin saadaan

$$g(k) = f(p_k)(\beta) = f(k),$$

mikä todistaa väitteen (2.43). □

2.4. Kuntalaajennuksen aste

LAUSE 2.20. *Olkoot $K \subset L \subset \mathbb{C}$ kuntia ja olkoon $K \hookrightarrow L$ kuntalaajennus. Tällöin joukko L varustettuna operaatioilla*

$$(u, v) \mapsto u + v \qquad (u, v \in L),$$
$$(\lambda, u) \mapsto \lambda u \qquad (\lambda \in K, u \in L)$$

on K-vektoriavaruus.

TODISTUS. Koska $K \subset L \subset \mathbb{C}$ ja kompleksiluvut toteuttavat vektoriavaruudelle määrätyt aksioomat, on väite selvä. □

MÄÄRITELMÄ 2.21. Jos $K \hookrightarrow L$ on kuntalaajennus, niin *kuntalaajennuksen aste* $[K \hookrightarrow L]$ on K-vektoriavaruuden L dimensio. Jos K-vektoriavaruudella L on äärellinen kanta, sanotaan, että kuntalaajennus $K \hookrightarrow L$ on *äärellisasteinen*. Jos K-vektoriavaruudella L ei ole äärellistä kantaa, sanotaan, että se on *ääretönasteinen* ja merkitään $[K \hookrightarrow L] = \infty$.

LAUSE 2.22 (Ketjusääntö kuntalaajennuksen asteille). *Olkoot $K \subset L \subset M \subset \mathbb{C}$ kuntia. Jos kuntalaajennukset $K \hookrightarrow L$ ja $L \hookrightarrow M$ ovat äärellisasteisia, niin*

$$[K \hookrightarrow M] = [K \hookrightarrow L][L \hookrightarrow M].$$

TODISTUS. Olkoon $\{x_1, \ldots, x_n\} \subset L$ K-vektoriavaruuden L kanta. Olkoon lisäksi $\{y_1, \ldots, y_m\} \subset M$ L-vektoriavaruuden M kanta. Väitteen todistamiseksi riittää löytää K-vektoriavaruudelle M kanta, jossa on täsmälleen nm alkiota. Tällainen on kanta

$$A = \{x_i y_j : i = 1, \ldots, n,\ j = 1, \ldots, m\}.$$

Todistetaan ensiksi, että kanta A virittää K-vektoriavaruuden M. Olkoon tätä varten $z \in M$. Koska $\{y_1, \ldots, y_m\}$ on L-vektoriavaruuden M kanta, niin on olemassa sellaiset $\mu_j \in L, j = 1, \ldots, n$, joille pätee

$$z = \sum_{j=1}^{m} \mu_j y_j. \tag{2.44}$$

Toisaalta koska $\{x_1, \ldots, x_n\}$ on K-vektoriavaruuden L kanta, niin kaikille $\mu_j \in L$, $j = 1, \ldots, m$ on olemassa sellaiset $\lambda_{ij} \in K$, että

$$\mu_j = \sum_{i=1}^{n} \lambda_{ij} x_i. \tag{2.45}$$

Yhdistämällä yhtälöt (2.44) ja (2.45) saadaan

$$z = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{ij} x_i y_j,$$

mikä osoittaa, että A virittää K-vektoriavaruuden M. Täytyy vielä osoittaa, että kannan A alkiot ovat K-lineaarisesti riippumattomia. Oletetaan tätä varten, että

$k_{ij} \in K$ ja

$$\sum_{i=1}^{n}\sum_{j=1}^{m} k_{ij}x_i y_j = 0. \tag{2.46}$$

Järjestelemällä summaa (2.46) uudelleen saadaan

$$\sum_{j=1}^{m}\left(\sum_{i=1}^{n} k_{ij}x_i\right)y_j = 0. \tag{2.47}$$

Koska $\{y_1, \ldots, y_m\}$ on L-lineaarisesti riippumaton joukko ja $\sum_{i=1}^{n} k_{ij}x_i \in L$ kaikilla $j = 1, \ldots, m$, niin yhtälön (2.47) perusteella

$$\sum_{i=1}^{n} k_{ij}x_i = 0. \tag{2.48}$$

Toisaalta $\{x_1, \ldots, x_n\}$ on K-lineaarisesti riippumaton ja $k_{ij} \in K$ kaikilla $i = 1, \ldots, n$. Tällöin yhtälöstä (2.48) nähdään, että täytyy olla $k_{ij} = 0$ kaikilla $i = 1, \ldots, n$ ja $j = 1, \ldots, m$. Siten joukon A alkiot ovat lineaarisesti riippumattomia. □

Lause 2.23. *Olkoot $K \subset L \subset M \subset \mathbb{C}$ kuntia. Jos kuntalaajennus $K \hookrightarrow L$ tai $L \hookrightarrow M$ on ääretönasteinen, niin*

$$[K \hookrightarrow M] = \infty.$$

Todistus. Oletetaan ensiksi, että $[K \hookrightarrow L] = \infty$. Tällöin K-vektoriavaruudella L on ääretön kanta $\{x_i\}_{i\in I}$. Koska $K \subset L \subset M$, niin $\{x_i\}_{i\in I}$ on K-lineaarisesti riippumaton myös K-vektoriavaruudessa M. Tällöin K-vektoriavaruuden M kannan täytyy olla ääretön. Oletetaan sitten, että $[K \hookrightarrow L] = \infty$, jolloin L-vektoriavaruudella M on olemassa ääretön kanta $\{y_j\}_{j\in J}$. Koska $K \subset L$, niin $\{y_j\}_{j\in J}$ on K-lineaarisesti riippumaton K-vektoriavaruudessa M, jolloin sen kanta on ääretön. Molemmissa tapauksissa siis $[K \hookrightarrow M] = \infty$. □

Lause 2.24. *Olkoon $K \subset \mathbb{C}$ kunta ja $\alpha \in \mathbb{C}$ algebrallinen kunnan K suhteen sekä olkoon $K \hookrightarrow K(\alpha)$ yksinkertainen kuntalaajennus. Tällöin*

$$[K \hookrightarrow K(\alpha)] = \partial m,$$

missä m on luvun α minimaalipolynomi.

Todistus. Olkoon

$$A = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\},$$

missä $n = \partial m$. Riittää osoittaa, että A on K-vektoriavaruuden $K(\alpha)$ kanta. Sitä varten osoitetaan ensiksi, että A on K-lineaarisesti riippumaton. Oletetaan siis, että $\lambda_0, \ldots, \lambda_{n-1} \in K$ ja

$$\sum_{i=0}^{n-1} \lambda_i \alpha^i = 0. \tag{2.49}$$

Määritellään seuraavaksi polynomi

$$p(y) = \sum_{i=0}^{n-1} \lambda_i y^i. \tag{2.50}$$

Sille pätee

$$p(\alpha) = \sum_{i=0}^{n-1} \lambda_i \alpha^i,$$

jolloin yhtälöstä (2.49) seuraa, että $p(\alpha) = 0$. Yhtälöstä (2.50) nähdään, että polynomin p aste on korkeintaan $n - 1 < n$. Jos olisi $p \neq 0$, niin p voitaisiin tarvittaessa kertoa sen johtavan kertoimen käänteisluvulla, jolloin se olisi perusmuotoinen. Näin ollen m ei voi olla luvun α minimaalipolynomi, ellei ole $p = 0$. Tästä kuitenkin seuraa, että $\lambda_i = 0$ kaikilla $i = 0, \ldots, n-1$, mikä todistaa lineaarisen riippumattomuuden.

Vielä jää osoitettavaksi, että A virittää K-vektoriavaruuden $K(\alpha)$. Toisin sanoen jos $y \in K(\alpha)$, niin täytyy löytää kertoimet $\lambda_0, \ldots, \lambda_{n-1} \in K$, joille

$$y = \sum_{i=0}^{n-1} \lambda_i \alpha^i. \tag{2.51}$$

Lemman 2.18 perusteella on olemassa polynomi $p \in K[x]$, jolle pätee

$$p(\alpha) = y \tag{2.52}$$

sekä

$$\partial p < n = \partial m.$$

Tällöin p voidaan kirjoittaa muodossa

$$p = \sum_{i=0}^{n-1} a_i x^i, \tag{2.53}$$

missä $a_i \in K$ kaikilla $i = 1, \ldots, n-1$. Yhtälöistä (2.52) ja (2.53) seuraa, että

$$y = \sum_{i=0}^{n-1} a_i \alpha^i. \tag{2.54}$$

Nyt yhtälöön (2.54) voidaan valita $\lambda_i = a_i \in K$, jolloin päädytään muotoon (2.51). Väite on siis todistettu. □

Lause 2.25. *Olkoot $K \subset L \subset \mathbb{C}$ kuntia. Kuntalaajennus $K \hookrightarrow L$ on äärellisasteinen, jos ja vain jos se on on olemassa kunnan K suhteen algebralliset luvut $\alpha_1, \ldots, \alpha_s$, joille pätee $L = K(\alpha_1, \ldots, \alpha_s)$. Lisäksi jos $L = K(\alpha_1, \ldots, \alpha_s)$ ja $\alpha_1, \ldots, \alpha_s$ ovat algebrallisia kunnan K suhteen, niin $K \hookrightarrow L$ on algebrallinen.*

Todistus. Osoitetaan ensiksi, että jos kuntalaajennus $K \hookrightarrow L$ on äärellisasteinen, niin se on algebrallinen ja on olemassa luvut $\alpha_1, \ldots, \alpha_s$, joille pätee $L = K(\alpha_1, \ldots, \alpha_s)$. Koska $K \hookrightarrow L$ on äärellisasteinen, niin K-vektoriavaruuden L kanta on muotoa $\{\alpha_1, \ldots, \alpha_s\}$, jolloin $L = K(\alpha_1, \ldots, \alpha_s)$.

Osoitetaan vielä, että jokainen $y \in L$ on algebrallinen kunnan K suhteen. Olkoon $n = [K \hookrightarrow L]$, jolloin K-vektoriavaruuden L kannassa on n alkiota. Olkoon lisäksi

$A = \{1, y, \ldots, y^n\}$. Nyt joukossa A on $n+1 > n$ alkiota, jolloin A on K-lineaarisesti riippuva. Tällöin on olemassa alkiot $k_0, \ldots, k_n \in K$, joille pätee

$$\sum_{i=0}^{n} k_i y^i = 0 \tag{2.55}$$

ja $k_i \neq 0$ jollain $i = 0, \ldots, n$. Nyt voidaan valita renkaan $K[x]$ polynomi

$$p(x) = \sum_{i=0}^{n} k_i x^i.$$

Yhtälön (2.55) perusteella polynomin p nollakohta on y, joten y on algebrallinen kunnan K suhteen.

Todistetaan seuraavaksi väitteen toinen suunta. Olkoon $K \hookrightarrow L$ kuntalaajennus ja olkoon $L = K(\alpha_1, \ldots, \alpha_s)$, missä $\alpha_1, \ldots, \alpha_s$ ovat algebrallisia kunnan K suhteen. Käytetään induktiota luvun s suhteen. Jos $s = 1$, niin $L = K(\alpha_1)$. Koska α_1 on algebrallinen kunnan K suhteen, niin lauseen 2.24 mukaan

$$[K \hookrightarrow L] = \partial m_1,$$

missä m_1 on luvun α_1 minimaalipolynomi. Kuntalaajennus $K \hookrightarrow L$ on tällöin äärellisasteinen.

Oletetaan seuraavaksi, että väite pätee, kun $s = r \in \mathbb{N}, r \geq 1$ eli $L = K(\alpha_1, \ldots, \alpha_r)$. Olkoon tällöin $[K \hookrightarrow L] = l$. Tarkastellaan seuraavaksi tilannetta $s = r + 1$. Tällöin $L = K(\alpha_1, \ldots, \alpha_r, \alpha_{r+1})$, missä $\alpha_1, \ldots, \alpha_r, \alpha_{r+1}$ ovat algebrallisia kunnan K suhteen. Tällöin myös α_{r+1} on algebrallinen kunnan $K(\alpha_1, \ldots, \alpha_r)$ suhteen. Siten lauseen 2.24 nojalla

$$[K(\alpha_1, \ldots, \alpha_r) \hookrightarrow K(\alpha_1, \ldots, \alpha_{r+1})] = \partial m_{r+1}, \tag{2.56}$$

missä $m_{r+1} \in K(\alpha_1, \ldots, \alpha_r)[x]$ on luvun α_{r+1} minimaalipolynomi. Koska nyt pätee $K(\alpha_1, \ldots, \alpha_r) \subset K(\alpha_1, \ldots, \alpha_{r+1})$, niin voidaan käyttää ketjusääntöä eli lausetta 2.22. Sen ja yhtälön (2.56) mukaan

(2.57)
$$\begin{aligned}[K \hookrightarrow K(\alpha_1, \ldots, \alpha_{r+1})] &= [K \hookrightarrow K(\alpha_1, \ldots, \alpha_r)][K(\alpha_1, \ldots, \alpha_r) \hookrightarrow K(\alpha_1, \ldots, \alpha_{r+1})] \\ &= [K \hookrightarrow K(\alpha_1, \ldots, \alpha_r)] \cdot \partial m_{r+1}.\end{aligned}$$

Induktio-oletuksen mukaan $[K \hookrightarrow K(\alpha_1, \ldots, \alpha_r)] = l$, jolloin yhtälö (2.57) saadaan muotoon

$$[K \hookrightarrow K(\alpha_1, \ldots, \alpha_{r+1})] = l \cdot \partial m_{r+1}$$

Koska $l \cdot \partial m_{r+1} \in \mathbb{N} \setminus \{0\}$, niin kuntalaajennus $K \hookrightarrow K(\alpha_1, \ldots, \alpha_{r+1})$ on äärellisasteinen. Siten edellä todistetun nojalla $K \hookrightarrow L$ on myös algebrallinen. □

LUKU 3

Polynomien hajoaminen

3.1. Hajotuskunnat

MÄÄRITELMÄ 3.1. Olkoon $K \subset \mathbb{C}$ kunta ja $p(x) \in K[x]$ polynomi. Polynomi $p(x)$ *hajoaa* kunnassa K, jos se voidaan esittää muodossa

$$p(x) = k(x - a_1) \cdots (x - a_n),$$

missä $k, a_1, \ldots, a_n \in K$.

MÄÄRITELMÄ 3.2. Olkoon $K \subset \mathbb{C}$ kunta ja $p(x) \in K[x]$ polynomi kunnassa K. Kuntaa $\Sigma \subset \mathbb{C}$ sanotaan *polynomin* $p(x)$ *hajotuskunnaksi kunnan* K *suhteen*, jos

(1) $K \subset \Sigma$,

(2) $p(x)$ hajoaa kunnassa Σ ja

(3) jos $K \subset \Sigma' \subset \Sigma$ ja $p(x)$ hajoaa kunnassa Σ', niin $\Sigma = \Sigma'$.

LAUSE 3.3. *Olkoon $K \subset \mathbb{C}$ kunta ja $p(x)$ renkaan $K[x]$ vakiosta eroava polynomi. Tällöin polynomille p on olemassa yksikäsitteinen hajotuskunta Σ kunnan K suhteen: Lisäksi $K \hookrightarrow \Sigma$ on äärellisasteinen.*

TODISTUS. Polynomi p hajoaa algebran peruslauseen mukaan kunnassa $\mathbb{C}$. Olkoon sen nollakohdat $\sigma_1, \ldots, \sigma_n \in \mathbb{C}$. Nyt voidaan valita $\Sigma = K(\sigma_1, \ldots, \sigma_n)$, jolloin p hajoaa kunnassa Σ. Koska $\sigma_1, \ldots, \sigma_n$ ovat täsmälleen polynomin p nollakohdat, ei $p(x) \in K[x]$ voi hajota missään kunnassa $L \subset \Sigma$, ellei ole $L = \Sigma$. Siten Σ on polynomin p hajotuskunta. Kuntalaajennus $K \hookrightarrow \Sigma$ on lisäksi äärellisasteinen lauseen 2.25 mukaan, sillä alkioita $\sigma_1, \ldots, \sigma_n$ on äärellinen määrä ja ne ovat kaikki algebrallisia. □

LEMMA 3.4. *Olkoot $K \subset L \subset \mathbb{C}$ kuntia ja $p(x) \in K[x]$ polynomi, jolle $p = qr$ joillekin polynomeille $q, r \in K[x]$. Tällöin p hajoaa kunnassa L, jos ja vain jos polynomit q ja r hajoavat kunnassa L.*

TODISTUS. Oletetaan ensiksi, että polynomit q ja r hajoavat kunnassa L. Olkoon $q = (x - \alpha_1) \cdots (x - \alpha_n)$ ja $r = (x - \beta_1) \cdots (x - \beta_m)$, missä $\alpha_1, \ldots, \alpha_n, n \in \mathbb{N} \setminus \{0\}$, ovat polynomin q nollakohdat ja $\beta_1, \ldots, \beta_m, m \in \mathbb{N} \setminus \{0\}$ polynomin r nollakohdat. Tällöin $\alpha_i, \beta_j \in L$ kaikilla $i, = 1, \ldots, n$ ja $j = 1, \ldots, m$. Lauseen 1.19 nojalla $p = (x - a_1) \cdots (x - \alpha_n)(x - \beta_1) \cdots (x - \beta_m)$. Lauseen 1.19 mukaan $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$ ovat täsmälleen polynomin p nollakohdat ja koska ne ovat kunnassa L, niin p hajoaa kunnassa L.

Oletetaan sitten, että p hajoaa kunnassa L. Tällöin kaikki polynomin p nollakohdat ovat kunnassa L. Riittää osoittaa, että kaikki polynomin q nollakohdat ovat myös polynomin p nollakohtia, jolloin q hajoaa kunnassa L. Tehdään vastaväite ja oletetaan, että $\alpha \in \mathbb{C}$ on polynomin q nollakohta, muttei polynomin p nollakohta. Tällöin lauseen 1.19 nojalla $q = (x-\alpha)r_1$ jollekin polynomille $r_1 \in K[x]$. Koska q jakaa polynomin p, niin $p = qr_2 = (x-\alpha)r_1r_2$ jollekin polynomille $r_2 \in K[x]$. Tällöin lauseen 1.19 nojalla α on polynomin p nollakohta, mikä on mahdotonta. □

LEMMA 3.5. *Olkoot $K \subset \mathbb{C}$, $K' \subset \mathbb{C}$ ja $L \subset \mathbb{C}$ kuntia. Olkoon näiden välillä isomorfismi $f : K \to K'$. Olkoon lisäksi $p(x) \in K[x]$ vakiosta eroava polynomi ja olkoon sen hajotuskunta Σ. Jos $K' \hookrightarrow L$ on sellainen kuntalaajennus, että polynomi $f(p)$ hajoaa kunnassa L, niin tällöin on olemassa monomorfismi $g : \Sigma \to L$ siten, että $g|_K = f$.*

TODISTUS. Väitettä voidaan havainnollistaa kaaviona:

$$\begin{array}{ccc} K & \longrightarrow & \Sigma \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ K' & \longrightarrow & L \end{array}$$

Täytyy siis löytää isomorfismi g sekä saada kaavio kommutoimaan. Konstruoidaan g käyttämällä induktiota asteen ∂p suhteen. Jos $\partial p = 1$, niin p on muotoa

$$p = a_1x + a_0,$$

missä $a_1 \in K \setminus \{0\}$ ja $a_0 \in K$. Polynomi p saadaan muokattua muotoon

$$p = a_1(x - (-a_1^{-1}a_0)).$$

Koska $a_1^{-1} \in K$ ja siten myös $-a^{-1}\alpha_0 \in K$, niin polynomi p hajoaa kunnassa K. Siten K on polynomin p hajotuskunta kunnan K suhteen. Tällöin hajotuskunnan yksikäsitteisyydestä seuraa, että $K = \Sigma$. Koska on olemassa isomorfismi $f : K \to K'$ ja kuntalaajennus $K' \hookrightarrow L$ on monomorfismi, niin yhdistämällä nämä kaksi kuvausta saadaan monomorfismi $g : \Sigma \to L$, jolle pätee $g|_K = f$.

Oletetaan seuraavaksi, että väite pätee kaikille $\partial p = k$, kun $1 \leq k < n$ ja $n \in \mathbb{N}$. Tarkastellaan sitten tapausta $\partial p = n$. Koska p hajoaa kunnassa Σ, niin p on muotoa

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

missä $\alpha_i \in \Sigma$ kaikilla $i = 1, \dots, n$. Olkoon $m(x)$ alkion α_1 minimaalipolynomi renkaassa $K[x]$. Nyt polynomi m jakaa polynomin p lemman 2.14 nojalla. Koska lisäksi f on isomorfismi, niin $f(m)$ jakaa polynomin $f(p)$. Koska $f(p)$ hajoaa kunnassa L, niin lemman 3.4 perusteella myös $f(m)$ hajoaa kunnassa L. Tällöin $f(m)$ voidaan kirjoittaa muodossa

$$f(m) = (x - \beta_1)\dots(x - \beta_l),$$

missä $\beta_i \in L$ kaikilla $i = 1, \dots, l$, kun $l \in \mathbb{N}$. Minimaalipolynomi on määritelmänsä perusteella jaoton, joten $f(m)$ on jaoton polynomi renkaassa $K'[x]$. Sen täytyy lauseen 2.15 perusteella olla alkion β_1 minimaalipolynomi renkaassa $K'[x]$. Tällöin lauseen 2.19 mukaan on olemassa isomorfismi

$$g_1 : K(\alpha_1) \to K'(\beta_1),$$

jolle pätee $g_1|_K = f$ ja $g_1(\alpha_1) = \beta_1$.

Tarkastellaan seuraavaksi renkaan $K(\alpha_1)[x]$ polynomia

$$q = \frac{p}{(x - \alpha_1)}.$$

Koska $\alpha_1 \in K(\alpha_1)$ on polynomin p nollakohta, niin lauseen 1.19 nojalla $(x-\alpha_1)$ jakaa polynomin p renkaassa $K(\alpha_1)[x]$. Tällöin q on todella $K(\alpha_1)$-kertoiminen polynomi. Polynomin q hajotuskunta kunnan $K(\alpha_1)$ suhteen on

$$K(\alpha_1)(\alpha_2, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n) = \Sigma.$$

Tämän lisäksi $\partial q < \partial p$, joten voidaan käyttää induktio-oletusta. Sen nojalla on olemassa monomorfismi $g : \Sigma \to L$ siten, että $g|_{K(\alpha_1)} = g_1$. Koska kuitenkin pätee $g_1|_K = f$ ja $K \subset K(\alpha_1)$, niin $g|_K = f$, jolloin etsitty monomorfismi g on löydetty. □

LAUSE 3.6. *Olkoot $K \subset \Sigma \subset \mathbb{C}$ ja $K' \subset \Sigma' \subset \mathbb{C}$ kuntia ja olkoon $f : K \to K'$ isomorfismi. Jos Σ on polynomin $p \in K[x]$ hajotuskunta kunnan K suhteen ja Σ' on polynomin $f(p) \in K'[x]$ hajotuskunta kunnan K' suhteen, niin kuntalaajennukset $K \to \Sigma$ ja $K' \to \Sigma'$ ovat isomorfisia. Toisin sanoen on olemassa isomorfismi $g : \Sigma \to \Sigma'$ siten, että $g|_K = f$.*

TODISTUS. Väitettä vastaava kaavio on seuraava:

$$\begin{array}{ccc} K & \longrightarrow & \Sigma \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ K' & \longrightarrow & \Sigma' \end{array}$$

Lemman 3.5 mukaan on olemassa monomorfismi $g : \Sigma \to \Sigma'$ siten, että $g|_K = f$. Kuvauksen g osoittaminen isomorfismiksi vaatii kuitenkin vielä, että g on surjektio eli $g(\Sigma) = \Sigma'$. Koska g on monomorfismi, f isomorfismi ja S on polynomin p hajotuskunta kunnan K suhteen, niin kunta $g(\Sigma)$ on polynomin $f(p)$ hajotuskunta kunnan K' suhteen. Koska $g(\Sigma) \subset \Sigma'$, niin hajotuskunnan määritelmästä seuraa suoraan, että $g(\Sigma) = \Sigma'$, jolloin g on surjektio. □

3.2. Normaalit kuntalaajennukset

MÄÄRITELMÄ 3.7. Olkoot $K \subset L \subset \mathbb{C}$ kuntia. Kuntalaajennus $K \hookrightarrow L$ on *normaali*, jos jokainen renkaan $K[x]$ jaoton polynomi p, jolla on vähintään yksi nollakohta kunnassa L, hajoaa kunnassa L.

LAUSE 3.8. *Olkoot $K \subset L \subset \mathbb{C}$ kuntia. Kuntalaajennus $K \hookrightarrow L$ on normaali ja äärellisasteinen, jos ja vain jos L on jonkin polynomin $p \in K[x]$ hajotuskunta.*

TODISTUS. Todistetaan ensiksi, että jos $K \hookrightarrow L$ on normaali ja äärellisasteinen, niin L on jonkin polynomin hajotuskunta. Koska $K \hookrightarrow L$ on äärellisasteinen, niin lauseen 2.25 mukaan $L = K(\alpha_1, \ldots, \alpha_n)$, missä alkiot α_i ovat algebrallisia kunnan K suhteen. Olkoon m_j alkion α_j minimaalipolynomi. Määritellään seuraavaksi polynomi p siten, että

$$p = m_1 \cdots m_n,$$

jolloin $p \in K[x]$. Jokainen polynomi $m_j, j = 1, \ldots, n$ on lauseen 2.13 nojalla jaoton renkaassa $K[x]$ ja lisäksi jokaisella polynomilla m_i on nollakohta $\alpha_i \in L$. Koska kuntalaajennus $K \hookrightarrow L$ on normaali, niin polynomi m_i hajoaa kunnassa L. Koska p on määritelty polynomien m_j tulona, niin soveltamalla lemmaa 3.4 $j-1$ kertaa nähdään, että myös p hajoaa kunnassa L. Olkoot $\beta_1, \ldots, \beta_k \in L$ polynomin p nollakohdat. Polynomien m_i nollakohdat ovat myös polynomin p nollakohtia, joten

$$L = K(\alpha_1, \ldots, \alpha_n) \subset K(\beta_1, \ldots, \beta_k). \tag{3.1}$$

Koska p hajoaa kunnassa L, niin $K(\beta_1, \ldots, \beta_k) \subset L$, jolloin ehdosta (3.1) seuraa, että $K(\alpha_1, \ldots, \alpha_n) = K(\beta_1, \ldots, \beta_k)$. Kunta $K(\beta_1, \ldots, \beta_k)$ on kuitenkin polynomin p hajotuskunta, joten L on polynomin p hajotuskunta.

Toinen suunta on vaikeampi osoittaa todeksi, mutta se on jatkon kannalta hyvin tärkeä tieto. Oletetaan, että L on hajotuskunta jollekin polynomille p. Jos polynomin p nollakohdat ovat $\alpha_1, \ldots, \alpha_n$, niin $L = K(\alpha_1, \ldots, \alpha_n)$, jolloin lauseen 2.25 mukaan kuntalaajennus $K \hookrightarrow L$ on äärellisasteinen.

Oletaan seuraavaksi, että $q \in K[x]$ on mielivaltainen jaoton polynomi, jolla on vähintään yksi nollakohta kunnassa L. Täytyy siis osoittaa, että q hajoaa kunnassa L. Olkoon Σ polynomin pq hajotuskunta. Tällöin on oltava $L \subset \Sigma$. Koska pq hajoaa kunnassa Σ, niin lemman 3.4 nojalla q hajoaa kunnassa Σ. Olkoot polynomin q nollakohdat $\beta_1, \ldots, \beta_r \in \Sigma$, missä $r \in \mathbb{N} \setminus \{0\}$. Tällöin jollain $i = 1, \ldots, r$ pätee $\beta_i \in L$. Jos polynomilla q ei ole enempää nollakohtia kunnassa Σ eli $r = 1$, niin q hajoaa kunnassa L ja väite on todistettu. Voidaan siis olettaa, että polynomilla q on myös jokin toinen nollakohta kunnassa Σ. Olkoon tämä mielivaltainen nollakohta $\beta_j \in \Sigma$, $j = 1, \ldots, r, j \neq i$. Koska q on jaoton polynomi, niin se on lauseen 2.15 nojalla alkioiden β_i ja β_j minimaalipolynomi renkaassa $K[x]$.

Osoitetaan seuraavaksi, että

$$[L \hookrightarrow L(\beta_i)] = [L \hookrightarrow L(\beta_j)]. \tag{3.2}$$

Nyt $K, K(\beta_i), K(\beta_j), L(\beta_i), L(\beta_j)$ ja Σ ovat kaikki kuntia, joille pätee

$$K \subset K(\beta_i) \subset L(\beta_i) \subset \Sigma. \tag{3.3}$$

Koska lisäksi $L \subset L(\beta_i)$, niin voidaan soveltaa lausetta 2.22, jolloin pätee

$$[K \hookrightarrow L(\beta_i)] = [K \hookrightarrow L][L \hookrightarrow L(\beta_i)]. \tag{3.4}$$

Edelleen voidaan ehdon (3.3) perusteella soveltaa lausetta 2.22, jolloin pätee myös

$$[K \hookrightarrow L(\beta_i)] = [K \hookrightarrow K(\beta_i)][K(\beta_i) \hookrightarrow L(\beta_i)]. \tag{3.5}$$

Yhdistämällä yhtälöt (3.4) ja (3.5) saadaan

$$[K \hookrightarrow L][L \hookrightarrow L(\beta_i)] = [K \hookrightarrow K(\beta_i)][K(\beta_i) \hookrightarrow L(\beta_i)],$$

mikä on yhtäpitävää sen kanssa, että

$$[L \hookrightarrow L(\beta_i)] = \frac{[K \hookrightarrow K(\beta_i)][K(\beta_i) \hookrightarrow L(\beta_i)]}{[K \hookrightarrow L]}. \tag{3.6}$$

Koska pätee myös

$$K \subset K(\beta_j) \subset L(\beta_j) \subset \Sigma$$

sekä $L \subset L(\beta_j)$, saadaan vastaavasti kuin edellä yhtälö

$$[L \hookrightarrow L(\beta_j)] = \frac{[K \hookrightarrow K(\beta_j)][K(\beta_j) \hookrightarrow L(\beta_j)]}{[K \hookrightarrow L]}. \tag{3.7}$$

Koska alkioilla β_i ja β_j on sama minimaalipolynomi q, ovat kuntalaajennukset $K \hookrightarrow K(\beta_i)$ ja $K \hookrightarrow K(\beta_j)$ lauseen 2.19 nojalla isomorfiset. Tällöin pätee

$$[K \hookrightarrow K(\beta_i)] = [K \hookrightarrow K(\beta_j)] \tag{3.8}$$

ja $K(\beta_i)$ ja $K(\beta_j)$ ovat isomorfiset. Lisäksi kunta L on polynomin p hajotuskunta kunnan K suhteen, joten kunta $L(\beta_i)$ on polynomin p hajotuskunta kunnan $K(\beta_i)$ suhteen. Vastaavasti kunta $L(\beta_j)$ on polynomin p hajotuskunta kunnan $K(\beta_j)$ suhteen. Näin ollen lauseen 3.6 oletukset pätevät, mistä seuraa, että kuntalaajennukset $K(\beta_i) \hookrightarrow L(\beta_i)$ ja $K(\beta_j) \hookrightarrow L(\beta_j)$ ovat isomorfiset. Tällöin myös niiden aste on sama eli

$$[K(\beta_i) \hookrightarrow L(\beta_i)] = [K(\beta_j) \hookrightarrow L(\beta_j)]. \tag{3.9}$$

Sijoittamalla yhtälöt (3.8) ja (3.9) yhtälöön (3.6) saadaan

$$[L \hookrightarrow L(\beta_i)] = \frac{[K \hookrightarrow K(\beta_j)][K(\beta_j) \hookrightarrow L(\beta_j)]}{[K \hookrightarrow L]}. \tag{3.10}$$

Sijoittamalla yhtälö (3.11) yhtälöön (3.7) saadaan väite (3.2):

$$[L \hookrightarrow L(\beta_i)] = [L \hookrightarrow L(\beta_j)]. \tag{3.11}$$

Koska $\beta_i \in L$, niin $[L \hookrightarrow L(\beta_i)] = 1$. Yhtälöstä (3.11) kuitenkin seuraa, että myös $[L \hookrightarrow L(\beta_j)] = 1$ eli $\beta_j \in L$. Koska β_j on polynomin q mielivaltainen nollakohta, niin polynomin q kaikille nollakohdille pätee $\beta_1, \ldots, \beta_r \in L$. Siten q hajoaa kunnassa L eli $K \hookrightarrow L$ on normaali. □

3.3. Separoituvat polynomit

Seuraavaksi palataan polynomin moninkertaisten nollakohtien määritelmään 1.20. Tarkoituksena on selvittää, milloin polynomilla voi olla moninkertaisia nollakohtia. Tämän kappaleen lopussa selviää, että tarkasteltaessa kompleksilukujen alikuntia yhdelläkään jaottomalla polynomilla ei ole moninkertaisia nollakohtia.

MÄÄRITELMÄ 3.9. Olkoon $K \subset \mathbb{C}$ kunta ja Σ polynomin p hajotuskunta. Tällöin kunnan K jaoton polynomi p on *separoituva*, jos sen nollakohdat ovat erilliset eli se voidaan ilmoittaa muodossa

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

missä $k \in K$ ja $\sigma_i \in \Sigma$ kaikilla $i = 1, 2, \ldots, n$ sekä kaikille $i,\ j = 1, 2, \ldots, n$ pätee $\sigma_i \neq \sigma_j$ aina, kun $i \neq j$.

MÄÄRITELMÄ 3.10. Olkoon $K \subset \mathbb{C}$ kunta ja olkoon

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$$

polynomi. Polynomin p *formaali derivaatta* on polynomi

$$Dp = a_1 + 2a_2 x + \ldots n a_n x^{n-1} \in K[x].$$

HUOMAUTUS 3.11. Jos $K = \mathbb{R}$, niin polynomin p formaali derivaatta vastaa analyysissä käytettävää polynomin derivointisääntöä. Formaali derivaatta eroaa kuitenkin analyysissä käytettävästä derivaatasta siinä, että se on määritelty missä tahansa kunnassa − ei siis pelkästään reaalilukujen tai kompleksilukujen joukossa. Lisäksi formaalin derivaatan määritelmä on puhtaan algebrallinen eli siinä ei käytetä rajaarvon käsitettä lainkaan. Näin ollen ei ole mielekästä ajatella polynomin p formaalia derivaattaa esimerkiksi polynomin p muutosnopeutena.

Monet analyysistä tutut derivaatan ominaisuudet pätevät kuitenkin myös formaalille derivaatalle. Suoraan formaalin derivaatan määritelmästä seuraa, että jos p ja q ovat polynomeja, niin

$$D(p+q) = D(p) + D(q). \tag{3.12}$$

Lisäksi yhtä helposti nähdään, että jos $\lambda \in K$, niin

$$D(\lambda p) = \lambda(Dq). \tag{3.13}$$

Tulon derivointisääntö formaalille derivaatalle vaatii kuitenkin tarkemman perustelun.

LEMMA 3.12. *Olkoon $K \subset \mathbb{C}$ kunta ja olkoot $p \in K[x]$ ja $q \in K[x]$ polynomeja. Tällöin*

$$D(pq) = (Dp)q + p(Dq).$$

TODISTUS. Olkoon $p = \sum_{i=0}^{n} a_i x^i$ ja $q = \sum_{i=0}^{m} b_i x^i$ kunnan $K[x]$ polynomeja. Tällöin $Dp = \sum_{k=0}^{n-1}(k+1)a_{k+1}x^k$ ja $Dq = \sum_{i=0}^{m-1}(i+1)b_{i+1}x^i$. Käyttämällä polynomien kertolaskun määritelmää saadaan

$$p(Dq)+(Dp)q = \sum_{i=0}^{n+m-1}\left(\sum_{k=0}^{i} a_k b_{i+1-k}(i+1-k)\right)x^i + \sum_{i=0}^{n+m-1}\left(\sum_{k=0}^{i} b_{i-k}(k+1)a_{k+1}\right)x^i.$$

Tämä on yhtäpitävää sen kanssa, että

$$p(Dq) + (Dp)q = \sum_{i=0}^{n+m-1}\left(\sum_{k=0}^{i} a_k b_{i+1-k}(i+1-k) + \sum_{k=0}^{i} b_{i-k}(k+1)a_{k+1}\right)x^i. \tag{3.14}$$

Muuttamalla jälkimmäisen summan indeksiä saadaan yhtälö (3.14) muotoon

$$p(Dq) + (Dp)q = \sum_{i=0}^{n+m-1}\left(\sum_{k=0}^{i} a_k b_{i+1-k}(i+1-k) + \sum_{k=0}^{i+1} b_{i-k+1}k a_k\right)x^i.$$

Tämä puolestaan on yhtäpitävää sen kanssa, että

$$p(Dq) + (Dp)q = \sum_{i=0}^{n+m}\left((i+1)\sum_{k=0}^{i+1} a_k b_{i+1-k}x^i\right). \tag{3.15}$$

Käyttämällä formaalin derivaatan määritelmää ja polynomien tulon määritelmää seuraa yhtälöstä (3.15), että

$$p(Dq) + (Dp)q = D(pq).$$

□

Näiden derivointisääntöjen avulla todistetaan seuraava kätevä lemma.

LEMMA 3.13. *Olkoon $K \subset \mathbb{C}$ kunta ja olkoon $p(x) \in K[x]$ vakiosta eroava polynomi. Olkoon lisäksi Σ polynomin p hajotuskunta. Polynomilla p on moninkertainen nollakohta kunnassa Σ, jos ja vain jos polynomeilla p ja Dp on yhteinen vakiosta eroava tekijä renkaassa $K[x]$.*

TODISTUS. Osoitetaan ensiksi, että jos polynomilla p on vähintään yksi moninkertainen nollakohta joukossa Σ, niin sillä on yhteinen tekijä formaalin derivaattansa kanssa. Olkoon tämä moninkertainen nollakohta $\alpha \in \Sigma$. Tällöin $p = (x-\alpha)^2 q$, missä $q \in K[x]$ on polynomi. Formaalin derivaatan määritelmästä ja lemmasta 3.12 saadaan

$$\begin{aligned} Dp &= 2(x-\alpha)q + (x-\alpha)^2 Dq \\ &= (x-\alpha)\big(2q + (x-\alpha)Dq\big). \end{aligned}$$

Polynomeilla p ja Dp on siis yhteinen vakiosta poikkeava tekijä $(x-\alpha) \in K[x]$.

Oletetaan seuraavaksi, että on olemassa vakiosta poikkeava polynomi $q \in K[x]$, jolle $q \mid p$ ja $q \mid Dp$. Koska p hajoaa kunnassa Σ, niin lemman 3.4 perusteella q hajoaa kunnassa Σ. Tällöin on olemassa $\alpha \in \Sigma$, jolle $q(\alpha) = 0$. Koska $q \mid p$, niin myös $p(\alpha) = 0$. Siten lauseen 1.19 mukaan

$$p = (x-\alpha)p' \tag{3.16}$$

jollekin nollasta eroavalle polynomille $p' \in \Sigma[x]$. Tällöin lemman 3.12 nojalla

$$Dp = D((x-\alpha))p' + (x-\alpha)Dp' = p' + (x-\alpha)Dp'. \tag{3.17}$$

Koska oletuksen mukaan $q \mid Dp$ ja $q(\alpha) = 0$, niin myös

$$Dp(\alpha) = 0. \tag{3.18}$$

Lisäksi yhtälön (3.17) perusteella

$$Dp(\alpha) = p'(\alpha) + (\alpha - \alpha)Dp' = p'(\alpha), \tag{3.19}$$

jolloin yhtälöiden (3.18) ja (3.19) nojalla $p'(\alpha) = 0$. Siten lauseen 1.19 nojalla $(x-\alpha)$ jakaa polynomin p' renkaassa $\Sigma[x]$ eli $p' = (x-\alpha)p''$ jollekin polynomille $p'' \in \Sigma[x]$. Sijoittamalla tämä tieto yhtälöön (3.16) saadaan

$$p = (x-\alpha)^2 p'',$$

mikä todistaa väitteen. □

LAUSE 3.14. *Olkoon $K \subset \mathbb{C}$ kunta. Tällöin jokainen nollasta eroava renkaassa $K[x]$ jaoton polynomi $p \in K[x]$ on separoituva.*

TODISTUS. Tehdään vastaväite ja oletetaan, että p ei ole separoituva. Lemma 3.13 antaa tiedon, että polynomilla $p(x)$ on yhteinen vakiosta poikkeava tekijä formaalin derivaattansa Dp kanssa renkaassa $K[x]$. Koska polynomi p on kuitenkin jaoton, täytyy tämän tekijän olla $k \cdot p$, missä $k \in K$. Koska $\partial p > \partial Dp$, niin tämä on mahdotonta. □

LUKU 4

Galois'n ryhmät

4.1. Galois'n ryhmät ja kiintopistekunnat

MÄÄRITELMÄ 4.1. Olkoot K ja L kuntia siten, että $K \subset L \subset \mathbb{C}$. Kunnan L *K-automorfismi* on isomorfismi $f : L \to L$, jolle pätee

$$f(k) = k \text{ kaikilla } k \in K.$$

HUOMAUTUS 4.2. Olkoot K ja L kuntia, joille pätee $K \subset L \subset \mathbb{C}$. Kunnan L K-automorfismit muodostavat selvästi ryhmän laskutoimituksenaan kuvausten yhdistäminen.

MÄÄRITELMÄ 4.3. Olkoot K ja L kuntia ja $K \subset L \subset \mathbb{C}$. Kuntalaajennuksen $K \hookrightarrow L$ *Galois'n ryhmä* $\Gamma(K, L)$ on kunnan L K-automorfismien muodostama ryhmä laskutoimituksenaan kuvausten yhdistäminen.

MÄÄRITELMÄ 4.4. Olkoon $K \hookrightarrow L$ kuntalaajennus ja $\Gamma(K, L)$ sen Galois'n ryhmä. Olkoon lisäksi $H \subset \Gamma(K, L)$ Galois'n ryhmän aliryhmä. Aliryhmän H *kiintopistekunta* on joukko

$$\mathrm{fix}(H) = \{x \in L : h(x) = x \text{ kaikille } h \in H\} \subset L.$$

LAUSE 4.5. *Galois'n ryhmän $\Gamma(K, L)$ aliryhmän H kiintopistekunta* $\mathrm{fix}(H)$ *on kunnan L alikunta, joka sisältää kunnan K.*

TODISTUS. Olkoon $h \in H$. Ainakin $K \subset \mathrm{fix}(H)$, sillä $h(k) = k$ kaikille $h \in H$ ja $k \in K$. Olkoot seuraavaksi $x, y \in \mathrm{fix}(H)$. Tällöin kaikille $h \in H$ pätee

$$h(x + y) = h(x) + h(y) = x + y$$

ja

$$h(xy) = h(x)h(y) = xy,$$

joten $x + y \in \mathrm{fix}(H)$ ja $xy \in \mathrm{fix}(H)$. Tällöin $\mathrm{fix}(H)$ on suljettu yhteen- ja kertolaskun suhteen. Lisäksi kakille $h \in H$

$$h(-x) = -h(x) = -x,$$

joten $-x \in \mathrm{fix}(H)$. Kun $x \neq 0$, niin kaikille $h \in H$

$$h(x^{-1}) = h(x)^{-1} = x^{-1},$$

jolloin myös $x^{-1} \in \mathrm{fix}(H)$.

Koska assosiatiivisuus, kommutatiivisuus ja distributiivisuus ovat selviä, niin $\mathrm{fix}(H)$ on kunta. Tällöin väite pätee. □

LAUSE 4.6. *Olkoon $K \subset L \subset \mathbb{C}$ kuntia. Tällöin pätee*

$$K \subset \mathrm{fix}(\Gamma(K, L)).$$

TODISTUS. Olkoon $k \in K$ ja $f \in \Gamma(K, L)$. Tällöin $f(k) = k$, joten kiintopistekunnan määritelmän perusteella $k \in \mathrm{fix}(\Gamma(K, L))$, mikä todistaa väitteen. □

LAUSE 4.7. *Olkoot $K \subset L \subset \mathbb{C}$ kuntia ja olkoon H Galois'n ryhmän $\Gamma(K, L)$ aliryhmä. Tällöin*

$$H \subset \Gamma(\mathrm{fix}(H), L).$$

TODISTUS. Olkoon $h \in H$. Täytyy osoittaa, että $h \in \Gamma(\mathrm{fix}(H), L)$. Koska $h \in H$ ja H on ryhmän $\Gamma(K, L)$ aliryhmä, niin h on isomorfismi $L \to L$. Edelleen koska $h \in H$, niin kiintopistekunnan $\mathrm{fix}(H)$ määritelmän perusteella $h(x) = x$ kaikilla $x \in \mathrm{fix}(H)$. Tällöin siis h on isomorfismi $L \to L$, jolle pätee $h(x) = x$ kaikilla $x \in \mathrm{fix}(H)$. Tämä on yhtäpitävää sen kanssa, että $h \in \Gamma(\mathrm{fix}(H), L)$. □

4.2. Lineaarialgebraa

Jotta saataisiin enemmän tietoa kiintopistekunnista, on käytävä ensiksi läpi hieman lineaarialgebraa. Tätä varten oletetaan, että $K \subset L \subset \mathbb{C}$ ovat kuntia ja määritellään joukko

$$\mathcal{F}(K, L) = \{f : K \to L \mid f \text{ on kuvaus }\}.$$

Joukosta $\mathcal{F}(K, L)$ saadaan L-vektoriavaruus asettamalla kaikille $f, g \in \mathcal{F}(K, L)$

$$(f + g)(x) = f(x) + g(x)$$

kaikilla $x \in K$ sekä

$$(\lambda f)(x) = \lambda f(x)$$

kaikilla $x \in K$ ja $\lambda \in L$.

LEMMA 4.8 (Dedekindin lemma). *Olkoon $K \subset L \subset \mathbb{C}$ kuntia. Tällöin mikä tahansa homomorfismien $f : K \to L$ joukko on lineaarisesti riippumaton L-vektoriavaruudessa $\mathcal{F}(K, L)$.*

TODISTUS. Olkoon $S \subset \mathcal{F}(K, L)$ erillisten homomorfismien $f : K \to L$ joukko. Tehdään vastaväite ja oletetaan, että S on lineaarisesti riippuva. Tällöin jollekin luvulle $n \geq 1$ on olemassa erilliset homomorfismit $f_1, \ldots, f_n$ sekä alkiot $\lambda_1, \ldots, \lambda_n \in L$, joille pätee

$$\lambda_1 f_1(x) + \cdots + \lambda_n f_n(x) \equiv 0 \tag{4.1}$$

kaikille $x \in K$. Lisäksi yhtälössä (4.1) $\lambda_j \neq 0$ jollain $j = 1, \ldots, n$. Tarvittaessa numerointia vaihtamalla voidaan olettaa, että $\lambda_n \neq 0$. Täytyy olla $n \geq 2$, sillä muuten pätisi $\lambda_1 f_1(x) \equiv 0$. Tällöin f_1 olisi nollakuvaus. Se on kuitenkin mahdotonta, sillä nollakuvaus ei ole kuntahomomorfismi. Nyt esityksessä (4.1) n voidaan valita siten, että se on mahdollisimman pieni.

Koska homomorfismit f_1 ja f_n ovat erilliset, on olemassa sellainen $y \in K$, jolle pätee

$$f_1(y) \neq f_n(y). \tag{4.2}$$

Koska K on kunta, niin $yx \in K$ kaikille $x \in K$. Tällöin yhtälön (4.1) nojalla pätee

$$\lambda_1 f_1(xy) + \cdots + \lambda_n f_n(xy) = 0$$

kaikille $x \in K$. Koska f on homomorfismi, tämä merkitsee sitä, että

$$\lambda_1 f_1(x) f_1(y) + \cdots + \lambda_n f_n(x) f_n(y) = 0 \tag{4.3}$$

kaikille $x \in K$. Kertomalla yhtälö (4.1) termillä $f_1(y)$ saadaan

$$\lambda_1 f_1(x) f_1(y) + \cdots + \lambda_n f_n(x) f_1(y) = 0 \tag{4.4}$$

kaikille $x \in K$. Vähentämällä yhtälö (4.3) yhtälöstä (4.4) saadaan

$$\lambda_2\big(f_1(y) - f_2(y)\big) f_2(x) + \cdots + \lambda_n(f_1(y) - f_n(y)\big) f_n(x) = 0 \tag{4.5}$$

kaikille $x \in K$. Yhtälön (4.2) perusteella pätee $f_1(y) - f_n(y) \neq 0$. Koska myös $\lambda_n \neq 0$, niin $\lambda_n\big(f_1(y) - f_n(y)\big) \neq 0$. Siten yhtälö (4.5) on muotoa (4.1). Yhtälössä (4.5) on yhteenlaskettavia termejä $n-1$ kappaletta. Yhtälössä (4.1) n valittiin kuitenkin mahdollisimman pieneksi. Syntynyt ristiriita osoittaa, ettei yhtälö (4.1) voi päteä, kun $\lambda_i \neq 0$ vähintään yhdellä $i = 1, \ldots, n$. □

LEMMA 4.9. *Olkoon $K \subset \mathbb{C}$ kunta ja $a_{ij} \in K$ kaikilla $i = 1, \ldots, m$ ja $j = 1, \ldots, n$. Jos $m < n$, niin yhtälöryhmällä*

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases}$$

on olemassa nollasta eroava ratkaisu $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$.

TODISTUS. Lauseen todistus kuuluu lineaarialgebran alkeisiin. Katso esimerkiksi [**7**, Theorem 4.2]. □

LEMMA 4.10. *Olkoon G ryhmä ja $g \in G$ kiinteä. Tällöin kuvaus $f : G \to G, f(x) = gx$ on bijektio kaikilla $x \in G$.*

TODISTUS. Todistetaan, että kuvaus $h : G \to G, h(x) = g^{-1}x$ on kuvauksen f käänteiskuvaus. Ensinnäkin pätee $f(h(x)) = f(g^{-1}x) = gg^{-1}x = x$. Vastaavasti $h(f(x)) = h(gx) = x$, joten f ja h ovat todella toistensa käänteiskuvaukset. Siten f on bijektio. □

Seuraavaksi saadaan tärkeä lause, jonka vuoksi koko lineaarialgebran tarkastelu tehtiin.

LAUSE 4.11. *Olkoon $K \subset L \subset \mathbb{C}$ kuntia ja H Galois'n ryhmän $\Gamma(K, L)$ äärellinen aliryhmä. Tällöin pätee*

$$[\mathrm{fix}(H) \hookrightarrow L] = \#H.$$

TODISTUS. Olkoon $H = \{h_1, \ldots, h_n\}$ ja $\#H = n \in \mathbb{N} \setminus \{0\}$. Tehdään vastaväite ja oletetaan, että $[\mathrm{fix}(H) \hookrightarrow L] \neq n$. Tällöin joko $[\mathrm{fix}(H) \hookrightarrow L] < n$ tai $[\mathrm{fix}(H) \hookrightarrow L] > n$.

Oletetaan ensiksi, että $[\mathrm{fix}(H) \hookrightarrow L] < n$. Suoraan kuntalaajennuksen asteen määritelmästä saadaan, että $\mathrm{fix}(H)$-vektoriavaruudessa L on kanta $\{x_1, \ldots, x_m\}$. Oletuksen perusteella $m < n$. Lemman 4.9 nojalla yhtälöryhmälle

$$\begin{cases} y_1 h_1(x_1) + \cdots + y_n h_n(x_1) = 0 \\ y_1 h_1(x_2) + \cdots + y_n h_n(x_2) = 0 \\ \vdots \\ y_1 h_1(x_m) + \cdots + y_n h_n(x_m) = 0 \end{cases} \tag{4.6}$$

on olemassa ratkaisu $\{y_1, \ldots, y_n\} \neq \{0, \ldots, 0\}$.

Oletetaan seuraavaksi, että $x \in L$ on mielivaltainen. Tällöin on olemassa sellaiset $\lambda_1, \ldots, \lambda_m \in \mathrm{fix}(H)$, joille pätee

$$x = \sum_{i=1}^{m} \lambda_i x_i. \tag{4.7}$$

Tällöin käyttämällä ensin yhtälöä (4.7), sitten tietoa siitä, että h_k on $\mathrm{fix}(H)$-automorfismi kaikilla k, sekä lopuksi käyttämällä yhtälöä (4.6) saadaan yhtälö

$$\begin{aligned} y_1 h_1(x) + \cdots + y_n h_n(x) &= y_1 h_1\Big(\sum_{i=1}^{m} \lambda_i x_i\Big) + \cdots + y_n h_n\Big(\sum_{i=1}^{m} \lambda_i x_i\Big) \\ &= \sum_{i=1}^{m} \lambda_i \big(y_1 h_1(x_i) + \cdots + y_n h_n(x_i)\big) \\ &= \sum_{i=1}^{m} \lambda_i \cdot 0 = 0. \end{aligned} \tag{4.8}$$

Koska vektori $(y_1, \ldots, y_n) \in L^n$ ei ole nollavektori ja $x \in L$ on mielivaltainen, niin yhtälön (4.8) perusteella joukko $\{h_1, \ldots, h_n\}$ on L-lineaarisesti riippuva. Tämä on kuitenkin vastoin lemmaa 4.8, joten tässä tapauksessa ajaudutaan ristiriitaan.

Otetaan seuraavaksi tapaus $[\mathrm{fix}(H) \hookrightarrow L] > n$ käsittelyyn. Koska $[\mathrm{fix}(H) \hookrightarrow L] > 0$, niin voidaan valita alkiot $x_1, \ldots, x_{n+1} \in L$ siten, että joukko $\{x_1, \ldots, x_{n+1}\}$ on lineaarisesti riippumaton $\mathrm{fix}(H)$-vektoriavaruudessa L. Tarkastellaan sitten yhtälöryhmää

$$\begin{cases} y_1 h_1(x_1) + \cdots + y_{n+1} h_1(x_{n+1}) = 0 \\ y_1 h_2(x_1) + \cdots + y_{n+1} h_2(x_{n+1}) = 0 \\ \vdots \\ y_1 h_n(x_1) + \cdots + y_{n+1} h_n(x_{n+1}) = 0. \end{cases} \tag{4.9}$$

Lemman 4.9 nojalla yhtälöryhmällä (4.9) on ratkaisu $(y_1, \ldots, y_{n+1}) \neq (0, \ldots, 0)$. Kaikista yhtälöryhmän (4.9) ratkaisuista valitaan tarkasteltavaksi se, jossa on eniten

nollia. Tarvittaessa numerointia vaihtamalla voidaan olettaa, että $y_1, \ldots, y_r \neq 0$ ja $y_{r+1}, \ldots, y_{n+1} = 0$ jollekin $r \in \mathbb{N}$. Nyt yhtälöryhmä (4.9) tulee muotoon

$$\begin{cases} y_1 h_1(x_1) + \cdots + y_r h_1(x_r) = 0 \\ y_1 h_2(x_1) + \cdots + y_r h_2(x_r) = 0 \\ \vdots \\ y_1 h_n(x_1) + \cdots + y_r h_n(x_r) = 0. \end{cases} \tag{4.10}$$

Olkoon $h \in H$ mielivaltainen. Tällöin yhtälöryhmän (4.10) ratkaisu $(y_1, \ldots, y_r)$ on myös yhtälöryhmän

$$\begin{cases} h(y_1)h \circ h_1(x_1) + \cdots + h(y_r)h \circ h_1(x_r) = 0 \\ h(y_1)h \circ h_2(x_1) + \cdots + h(y_r)h \circ h_2(x_r) = 0 \\ \vdots \\ h(y_1)h \circ h_n(x_1) + \cdots + h(y_r)h \circ h_n(x_r) = 0 \end{cases} \tag{4.11}$$

ratkaisu. Lemman 4.10 perusteella alkiot $h \circ h_i$ käyvät läpi kaikki alkiot $h_i \in H$ täsmälleen kerran. Siten $H = \{h_1, \ldots, h_n\} = \{h \circ h_1, \ldots, h \circ h_n\}$. Tämän vuoksi yhtälöryhmä (4.11) voidaan muokata muotoon

$$\begin{cases} h(y_1)h_1(x_1) + \cdots + h(y_r)h_1(x_r) = 0 \\ h(y_1)h_2(x_1) + \cdots + h(y_r)h_2(x_r) = 0 \\ \vdots \\ h(y_1)h_n(x_1) + \cdots + h(y_r)h_n(x_r) = 0. \end{cases} \tag{4.12}$$

Kerrotaan seuraavaksi yhtälöryhmä (4.12) termillä y_1, jolloin saadaan yhtälöryhmä

$$\begin{cases} h(y_1)y_1h_1(x_1) + \cdots + h(y_r)y_1h_1(x_r) = 0 \\ h(y_1)y_1h_2(x_1) + \cdots + h(y_r)y_1h_2(x_r) = 0 \\ \vdots \\ h(y_1)y_1h_n(x_1) + \cdots + h(y_r)y_1h_n(x_r) = 0. \end{cases} \tag{4.13}$$

Yhtälöryhmällä (4.13) on sama ratkaisu $(y_1, \ldots, y_r)$ kuin yhtälöryhmällä (4.10). Kertomalla sitten yhtälö (4.10) termillä $h(y_1)$ saadaan yhtälö

$$\begin{cases} y_1h_1(x_1)h(y_1) + \cdots + y_rh_1(x_r)h(y_1) = 0 \\ y_1h_2(x_1)h(y_1) + \cdots + y_rh_2(x_r)h(y_1) = 0 \\ \vdots \\ y_1h_n(x_1)h(y_1) + \cdots + y_rh_n(x_r)h(y_1) = 0, \end{cases} \tag{4.14}$$

jonka ratkaisu $(y_1, \ldots, y_r)$ edelleen toteuttaa. Koska tämä ratkaisu toteuttaa sekä yhtälöryhmän (4.13) että (4.14), toteuttaa se myös yhtälöryhmän, joka on saatu vähentämällä yhtälöryhmät (4.13) ja (4.14) toisistaan. Vähentämällä yhtälöryhmä (4.14)

yhtälöryhmästä (4.13) ja ottamalla sopivat yhteiset tekijät saadaan yhtälöryhmä

$$\begin{cases} h_1(x_2)\big(y_2h(y_1) - y_1h(y_2)\big) + \cdots + h_1(x_r)\big(y_rh(y_1) - y_1h(y_r)\big) = 0 \\ h_2(x_2)\big(y_2h(y_1) - y_1h(y_2)\big) + \cdots + h_2(x_r)\big(y_rh(y_1) - y_1h(y_r)\big) = 0 \\ \vdots \\ h_n(x_2)\big(y_2h(y_1) - y_1h(y_2)\big) + \cdots + h_n(x_r)\big(y_rh(y_1) - y_1h(y_r)\big) = 0, \end{cases} \tag{4.15}$$

Vertaamalla yhtälöryhmiä (4.10) ja (4.15) huomataan, että yhtälöryhmän (4.15) kussakin yhtälössä on vähemmän termejä kuin yhtälöryhmän (4.10) yhtälöissä. Näin ollen yhtälöryhmällä (4.15) on ratkaisu, jossa on enemmän nollia kuin yhtälöryhmän (4.10) ratkaisussa. Ratkaisu $(y_1, \ldots, y_r)$ on kuitenkin valittu siten, että siinä on mahdollisimman paljon nollia. Näin ollen yhtälöryhmällä (4.15) ei voi olla nollasta poikkeavia ratkaisuja. Täytyy siis olla $y_jh(y_1) - y_1h(y_j) = 0$ kaikilla $j = 2, \ldots, r$. Tämä tarkoittaa sitä, että

$$y_jh(y_1) = y_1h(y_j)$$

kaikilla $j = 2, \ldots, r$. Koska $y_1 \neq 0$ ja $h(y_1) \neq 0$, niin tästä seuraa, että $y_jy_1^{-1} = h(y_j)h(y_1)^{-1}$ kaikilla $j = 2, \ldots, r$. Lisäksi h on homomorfismi, joten edelleen pätee

$$y_jy_1^{-1} = h(y_jy_1^{-1}) \tag{4.16}$$

kaikilla $j = 2, \ldots, r$. Koska $h \in H$ on mielivaltainen, niin kiintopistekunnan määritelmän ja yhtälön (4.16) nojalla

$$y_jy_1^{-1} \in \operatorname{fix}(H) \tag{4.17}$$

kaikilla j. Tarkastellaan nyt yhtälöryhmän (4.10) ensimmäistä yhtälöä. Kertomalla se termillä y_1^{-1} saadaan yhtälö

$$h_1(x_1) + \sum_{j=2}^{r} h_1(x_j)y_jy_1^{-1} = 0. \tag{4.18}$$

Käyttäen yhtälöä (4.16) voidaan yhtälöä (4.18) voidaan muokata muotoon

$$h_1(x_1) + \sum_{j=2}^{r} h_1(x_j)h_1(y_jy_1^{-1}) = h_1\left(x_1 + \sum_{j=2}^{r} x_jy_jy_1^{-1}\right) = 0. \tag{4.19}$$

Koska $h_1 \in H$ on monomorfismi, niin yhtälön (4.19) mukaan

$$1 \cdot x_1 + \sum_{j=2}^{r} x_jy_jy_1^{-1} = 0. \tag{4.20}$$

Yhtälön (4.20) termin x_1 kertoimelle pätee $1 \in \operatorname{fix}(H)$, sillä $\operatorname{fix}(H)$ on kunnan $\mathbb{C}$ alikunta. Myös jokaisen termin x_j, $j = 2, \ldots, n$, kertoimelle pätee $y_jy_1^{-1} \in \operatorname{fix}(H)$ yhtälön (4.17) mukaan. Tällöin yhtälöstä (4.20) seuraa, että joukko $\{x_1, \ldots, x_r\}$ on lineaarisesti riippuva $\operatorname{fix}(H)$-vektoriavaruudessa L. Edellä kuitenkin oletettiin, että $\{x_1, \ldots, x_r\}$ on lineaarisesti riippumaton $\operatorname{fix}(H)$-vektoriavaruudessa L. Näin ollen myös tapaus $[\operatorname{fix}(H) \hookrightarrow L] > n$ on mahdoton. Siten on oltava $[\operatorname{fix}(H) \hookrightarrow L] = n$. □

4.3. K-monomorfismit

MÄÄRITELMÄ 4.12. Olkoot K, M ja L kuntia siten, että $K \subset M \subset L \subset \mathbb{C}$. Sanotaan, että kuvaus f on *K-monomorfismi kunnalta M kuntaan L*, jos f on monomorfismi $f : M \to L$, jolle pätee

$$f(k) = k \text{ kaikilla } k \in K.$$

LAUSE 4.13. *Olkoon $K \hookrightarrow L$ normaali äärellisasteinen kuntalaajennus ja olkoon M kunta siten, että $K \subset M \subset L$. Olkoon $\tau : M \to L$ mielivaltainen K-monomorfismi. Tällöin on olemassa K-automorfismi $\sigma : L \to L$ siten, että rajoittumakuvaus $\sigma|_M = \tau$.*

TODISTUS. Koska $K \hookrightarrow L$ on äärellisasteinen ja normaali, niin lauseen 3.8 mukaan L on nyt hajotuskunta jollekin polynomille $p \in K[x] \subset M[x]$ kunnan K suhteen. Koska $K \subset M$, niin L on hajotuskunta polynomille p myös kunnan M suhteen. Tavoitteena on siis löytää kuvaus σ sekä saada seuraava kaavio kommutoimaan:

$$\begin{array}{ccc} M & \longrightarrow & L \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\sigma} \\ \tau(M) & \longrightarrow & L \end{array}$$

Koska K-monomorfismille $\tau : M \to \tau(M)$ pätee $\tau|_K = I_K$ ja $p \in K[x]$, niin $\tau(p) = p$. Koska lisäksi $\tau(K) \subset \tau(M)$ sekä L on polynomin p hajotuskunta kunnan $K = \tau(K)$ suhteen, niin L on myös polynomin $\tau(p) = p$ hajotuskunta kunnan $\tau(M)$ suhteen.

Koska L on polynomin p hajotuskunta sekä kunnan M että kunnan $\tau(M)$ suhteen sekä on olemassa isomorfismi τ kuntien M ja $\tau(M)$ välillä, voidaan käyttää lausetta 3.6. Tällöin on olemassa isomorfismi $\sigma : L \to L$ siten, että $\sigma|_M = \tau$. Koska $K \subset M$, niin $\sigma|_K = \tau|_K = I_K$. Siten $\sigma : L \to L$ on K-automorfismi. □

LAUSE 4.14. *Olkoot $K \subset L \subset \mathbb{C}$ kuntia ja olkoon $K \hookrightarrow L$ normaali ja äärellisasteinen kuntalaajennus. Olkoon lisäksi p jaoton renkaan $K[x]$ polynomi, jolla on nollakohdat α ja β kunnassa L. Tällöin on olemassa kunnan K-automorfismi $\sigma : L \to L$ siten, että $\sigma(\alpha) = \beta$.*

TODISTUS. Koska p on jaoton polynomi, on p lukujen α ja β minimaalipolynomi. Tällöin lauseesta 2.19 seuraa, että on olemassa isomorfismi $\tau : K(\alpha) \to K(\beta)$ siten, että $\tau|_K = I_K$ ja $\tau(\alpha) = \beta$. Koska $K \hookrightarrow L$ on normaali ja äärellisasteinen kuntalaajennus, lauseen 4.13 nojalla on olemassa K-automorfismi $\sigma : L \to L$ siten, että $\sigma|_{K(\alpha)} = \tau$. Tällöin K-automorfismille σ pätee $\sigma(\alpha) = \beta$. □

4.4. Normaalisulkeumat

Jos topologiassa joukko ei ole suljettu, voidaan siitä ottaa sulkeuma. Tällöin joukkoon lisätään täsmälleen niin monta pistettä, että siitä tulee suljettu. Kuntalaajennuksille puhutaan normaalisulkeumasta, joka muistuttaa topologista sulkeumaa: jos luonnollinen kuntalaajennus $K \hookrightarrow L$ ei ole normaali, voidaan kuntaa L kasvattaa täsmälleen sen verran, että laajennus on normaali. Normaalisulkeuma määritellään vain äärellisasteisille kuntalaajennuksille.

MÄÄRITELMÄ 4.15. Olkoot $K \subset L \subset \mathbb{C}$ kuntia ja $K \hookrightarrow L$ äärellisasteinen kuntalaajennus. Tällöin laajennuksen $K \hookrightarrow L$ *normaalisulkeuma* on kunta N jolle pätee

(1) $L \subset N$

(2) $K \hookrightarrow N$ on normaali kuntalaajennus,

(3) Jos $L \subset M \subset N$ jollekin kunnalle M siten, että $K \to M$ on normaali kuntalaajennus, niin $M = N$.

HUOMAUTUS 4.16. Jos $K \hookrightarrow L$ on äärellisasteinen ja normaali kuntalaajennus, niin sen normaalisulkeuma on määritelmän 4.15 mukaan L.

LAUSE 4.17. *Olkoon $K \hookrightarrow L$ äärellisasteinen kuntalaajennus. Tällöin on olemassa yksikäsitteinen kuntalaajennuksen $K \hookrightarrow L$ normaalisulkeuma N. Lisäksi kuntalaajennus $K \hookrightarrow N$ on äärellisasteinen.*

TODISTUS. Osoitetaan ensiksi, että normaalisulkeuma on aina olemassa. Koska laajennus $K \hookrightarrow L$ on äärellisasteinen, niin K-vektoriavaruudella L on kanta $\{x_1, \ldots, x_n\}$. Alkiot x_i ovat lauseen 2.25 nojalla algebrallisia kunnan K suhteen kaikilla $i = 1, \ldots, n$. Olkoon m_i alkion x_i minimaalipolynomi. Määritellään seuraavaksi kunnan L polynomi

$$p = m_1 m_2 \cdots m_n. \tag{4.21}$$

Olkoon N polynomin p hajotuskunta kuntalaajennuksen $L \hookrightarrow N$ suhteen. Tällöin määritelmän 4.15 ehto (1) pätee kunnalle N. Todistetaan seuraavaksi, että N on polynomin p hajotuskunta kuntalaajennuksen $K \hookrightarrow N$ suhteen. Ainakin p hajoaa kunnassa N. Täytyy kuitenkin osoittaa, ettei p voi hajota missään kunnassa M, jolle $K \subset M \subset N$ ja $M \neq N$. Tehdään vastaväite ja oletetaan, että p hajoaa kunnassa M. Tällöin $p = k(x - \alpha_1) \cdots (x - \alpha_s)$, missä $k \in M$ ja $\alpha_i \in M$ kaikilla $i = 1, \ldots, s$. Koska jokainen x_i on polynomin m_i nollakohta, niin polynomin p määritelmästä (4.21) seuraa, että jokainen x_i on polynomin p nollakohta. Tällöin

$$\{x_1, \ldots, x_n\} \subset \{\alpha_1, \ldots, \alpha_s\} \subset M. \tag{4.22}$$

Koska $\{x_1, \ldots, x_n\}$ on K-vektoriavaruuden L kanta, niin yhtälöstä (4.22) seuraa, että $L \subset M$. Toisaalta tiedetään, että N on polynomin p hajotuskunta kuntalaajennuksen $L \hookrightarrow N$ suhteen. Tämä tarkoittaa, että jos p hajoaa kunnassa M', jolle $L \subset M' \subset N$, niin $M' = N$. Voidaan valita $M = M'$, jolloin $M = N$. Tämä on kuitenkin ristiriita.

On siis osoitettu, että N on polynomin p hajotuskunta kuntalaajennuksen $K \hookrightarrow N$ suhteen. Lauseen 3.8 mukaan $K \hookrightarrow N$ on tällöin äärellisasteinen ja normaali. Tämä riittää todistamaan ehdon (2). Todistetaan vielä, että ehto (3) on voimassa. Olkoon $\tilde{M}$ kunta, jolle pätee $L \subset \tilde{M} \subset N$ ja $K \hookrightarrow \tilde{M}$ on normaali. Koska kaikilla polynomeilla m_i on vähintään yksi nollakohta $x_i \in L \subset \tilde{M}$, niin m_i hajoaa kunnassa $\tilde{M}$. Tällöin soveltamalla lemmaa 3.4 $n - 1$ kertaa peräkkäin nähdään, että p hajoaa kunnassa $\tilde{M}$. Koska N on kuitenkin polynomin p hajotuskunta kuntalaajennuksen $K \hookrightarrow N$ suhteen, niin $\tilde{M} = N$.

Osoitetaan seuraavaksi normaalisulkeuman yksikäsitteisyys. Olkoon sitä varten laajennuksella $K \hookrightarrow L$ kaksi normaalisulkeumaa N ja N'. Olkoon lisäksi Σ kohdassa

(4.21) määritellyn polynomin p hajotuskunta kunnan K suhteen. Jokaisella polynomilla $m_i, i = 1, \ldots, n$ on vähintään yksi nollakohta kunnassa L ja siten myös kunnissa N ja N'. Tällöin jokainen m_i hajoaa kunnissa N ja N', jolloin lemman 3.4 nojalla p hajoaa kunnissa N ja N'. Tällöin $\Sigma \subset N$ ja $\Sigma \subset N'$. Koska $K \hookrightarrow \Sigma$ on lauseen 3.8 nojalla normaali kuntalaajennus, niin normaalisulkeuman määritelmän perusteella $\Sigma = N = N'$. □

LEMMA 4.18. *Olkoot $K \subset L \subset N \subset M \subset \mathbb{C}$ kuntia. Olkoon lisäksi $K \hookrightarrow L$ äärellisasteinen kuntalaajennus ja N sen normaalisulkeuma. Tällöin mielivaltaiselle K-monomorfismille $\tau : L \to M$ pätee $\tau(L) \subset N$.*

TODISTUS. Olkoon $\alpha \in L$ mielivaltainen. Täytyy osoittaa, että $\tau(\alpha) \in N$. Lauseen 2.25 nojalla α on algebrallinen kunnan K suhteen. Olkoon m alkion α minimaalipolynomi kuntalaajennuksen $K \hookrightarrow L$ suhteen. Minimaalipolynomin määritelmän perusteella $m(\alpha) = 0$. Koska τ on homomorfismi, niin myös $\tau(m(\alpha)) = 0$. Lisäksi koska τ on K-monomorfismi ja $m \in K[x]$, niin $\tau(m) = m$. Tällöin $\tau(m(\alpha)) = m(\tau(\alpha))$ eli myös $\tau(\alpha)$ on polynomin m nollakohta. Nyt polynomilla m on ainakin yksi nollakohta $\alpha \in L \subset N$. Koska laajennus $K \hookrightarrow N$ on normaali, täytyy polynomin m jokaisen nollakohdan kuulua kuntaan N. Näin ollen $\tau(\alpha) \in N$. □

LEMMA 4.19. *Olkoot $K \subset L \subset \mathbb{C}$ kuntia ja $K \hookrightarrow L$ äärellisasteinen kuntalaajennus. Tällöin seuraavat väitteet ovat yhtäpitäviä.*

(1) *$K \hookrightarrow L$ on normaali kuntalaajennus*

(2) *On olemassa sellainen kunta N, jolle $L \subset N$, $K \hookrightarrow N$ on äärellisasteinen ja normaali sekä jokainen K-monomorfismi $\tau : L \to N$ on K-automorfismi $L \to L$.*

(3) *Jokaiselle kunnalle M, jolle pätee $L \subset M$, jokainen K-monomorfismi $\tau : L \to M$ on myös K-automorfismi $L \to L$.*

TODISTUS. Aloitetaan todistamalla, että väitteestä (1) seuraa väite (3). Koska $K \hookrightarrow L$ on normaali kuntalaajennus, sen normaalisulkeuma huomautuksen 4.16 perusteella on L. Nyt lemmasta 4.18 saadaan, että $\tau(L) \subset L$. Koska τ on K-lineaarinen injektio ja se on määritelty äärellisulotteisessa K-vektoriavaruudessa L, täytyy K-vektoriavaruudella $\tau(L)$ olla sama dimensio kuin K-vektoriavaruudella L. Tästä seuraa, että $\tau(L) = L$, ja koska $K \subset L$, niin τ on K-automorfismi kunnassa L.

Todistetaan seuraavaksi, että väitteestä (3) seuraa väite (2). Lauseen 4.17 nojalla kuntalaajennuksella $K \hookrightarrow L$ on olemassa normaalisulkeuma N siten, että $K \hookrightarrow N$ on äärellisasteinen. Tällöin oletusten nojalla jokainen K-monomorfismi $\tau : L \hookrightarrow N$ on kunnan L K-automorfismi.

Todistetaan vielä, että väitteestä (2) seuraa väite (1). Olkoon $p \in K[x]$ jaoton polynomi, jolla on vähintään yksi nollakohta $\alpha \in L$. Täytyy osoittaa, että p hajoaa kunnassa L. Olkoon myös $\beta \in N$ polynomin p nollakohta. Koska $K \hookrightarrow N$ on normaali kuntalaajennus ja $\alpha \in L \subset N$, niin p hajoaa kunnassa N. Nyt voidaan käyttää lausetta 4.14, jonka mukaan on olemassa K-automorfismi $\tau : N \to N$, jolle pätee

$\tau(\alpha) = \beta$. Nyt rajoittumakuvaus $\tau|_L : L \to N$ on K-monomorfismi, jolloin se on oletuksen nojalla myös K-automorfismi $L \to L$. Tällöin koska $\alpha \in L$, niin pätee

$$\beta = \tau|_L(\alpha) \in \tau|_L(L) = L.$$

Siten polynomin p mielivaltainen nollakohta $\beta \in N$ kuuluu kuntaan L. Siten, koska p hajoaa kunnassa N, niin p hajoaa myös kunnassa L. Tämä todistaa lopulta, että väitteet (1)-(3) ovat yhtäpitävät. □

LEMMA 4.20. *Olkoot $K \subset L \subset N \subset \mathbb{C}$ kuntia ja olkoon $K \hookrightarrow L$ äärellisasteinen kuntalaajennus, jonka aste on n. Olkoon lisäksi $K \hookrightarrow N$ normaali kuntalaajennus. Tällöin on täsmälleen n erillistä K-monomorfismia kunnalta L kuntaan N.*

TODISTUS. Todistetaan väite induktiolla kuntalaajennuksen $K \hookrightarrow L$ asteen suhteen. Jos $[K \hookrightarrow L] = 1$, niin $K = L$, jolloin ainoa K-monomorfismi kunnalta L kunnalle N on identtinen kuvaus I. Näin ollen K-monomorfismeja on täsmälleen yksi, jolloin väite pätee.

Oletetaan seuraavaksi, että väite pätee kaikille $[K \hookrightarrow L] = k$, kun $1 \leq k < n$. Osoitetaan, että väite pätee tällöin myös luvulle n. Olkoon $\alpha \in L \setminus K$. Koska $K \hookrightarrow L$ on äärellisasteinen, niin lauseen 2.25 nojalla $K \hookrightarrow L$ on algebrallinen. Tällöin alkiolla α on minimaalipolynomi m, jolle pätee lauseen 2.24 mukaan

$$\partial m = [K \hookrightarrow K(\alpha)] = r > 1. \tag{4.23}$$

Nyt polynomi m on lauseen 2.13 perusteella jaoton renkaassa $K[x]$ ja sillä on lisäksi vähintään yksi nollakohta α joukossa $K(\alpha) \subset L \subset N$. Tällöin sillä on vähintään yksi nollakohta myös kunnassa N. Koska laajennus $K \hookrightarrow N$ on normaali, niin m hajoaa kunnassa N. Algebran peruslauseen mukaan polynomilla m on $\partial m = r$ kappaletta nollakohtia. Olkoot nämä nollakohdat $\alpha_1, \ldots, \alpha_r$. Tarvittaessa numerointia vaihtamalla voidaan olettaa, että $\alpha = \alpha_1$. Koska $N \subset \mathbb{C}$, niin lauseen 3.14 nojalla nollakohdat ovat erillisiä eli $\alpha_j \neq \alpha_i$, kun $i, j = 1, \ldots, r$ ja $i \neq j$.

Koska kuntalaajennus $K \hookrightarrow N$ on normaali, niin N on lauseen 3.8 nojalla jonkin polynomin $q \in K[x]$ hajotuskunta. Nyt $q \in K(\alpha)[x]$, joten N on myös $K(\alpha)$-kertoimisen polynomin hajotuskunta. Siten lauseen 3.8 mukaan $K(\alpha) \hookrightarrow N$ on normaali.

Merkitään seuraavaksi $s = [K(\alpha) \hookrightarrow L]$. Koska $[K \hookrightarrow L] = n$, niin lauseen 2.22 ja yhtälön (4.23) perusteella saadaan

$$s = [K(\alpha) \hookrightarrow L] = \frac{n}{r} < n. \tag{4.24}$$

Koska $s < n$ ja $K(\alpha) \hookrightarrow N$ on normaali, niin voidaan soveltaa induktio-oletusta. Tällöin on olemassa täsmälleen s kappaletta erillisiä $K(\alpha)$-monomorfismeja. Olkoot nämä $\pi_1, \ldots, \pi_s$. Lauseen 4.14 mukaan on olemassa r kappaletta erillisiä kunnan N K-automorfismeja $\tau_1, \ldots, \tau_r$, joille pätee

$$\tau_i(\alpha_i) = \alpha_i \tag{4.25}$$

kaikille $i = 1, \ldots, r$. Tarkastellaan seuraavaksi yhdistettyä kuvausta

$$\phi_{ij} = \tau_i \circ \pi_j. \tag{4.26}$$

Kuvauksia ϕ_{ij} on $r \cdot s$ kappaletta, sillä ne ovat toisistaan erilliset. Todistetaan tämä seuraavaksi osoittamalla, että jos $\phi_{ij} = \phi_{kl}$, niin $i = k$ ja $j = l$. Ensinnäkin jos $\phi_{ij} = \phi_{kl}$, niin $\phi_{ij}(\alpha) = \phi_{kl}(\alpha)$. Käyttämällä kuvauksen ϕ määritelmää saadaan yhtälö.

$$\tau_i \circ \pi_j(\alpha) = \tau_k \circ \pi_l(\alpha).$$

Muistaen, että π_j ja π_l ovat $K(\alpha)$-automorfismeja saadaan yhtälö muotoon

$$\tau_i(\alpha) = \tau_k(\alpha). \tag{4.27}$$

Yhdistämällä tieto yhtälö (4.25) yhtälöön (4.27) sekä valintaan $\alpha = \alpha_1$ saadaan $\alpha_i = \alpha_k$, jolloin

$$i = k. \tag{4.28}$$

Toisaalta kuvauksen ϕ määritelmästä seuraa, että

$$\pi_j = \tau_i^{-1} \circ \phi_{ij}. \tag{4.29}$$

Sijoittamalla yhtälöön (4.29) yhtälö (4.28) sekä oletus $\phi_{ij} = \phi_{kl}$ saadaan yhtälö

$$\pi_j = \tau_k^{-1} \circ \phi_{kl}. \tag{4.30}$$

Toisaalta $\phi_{kl} = \tau_k \circ \pi_l$, jolloin yhtälö (4.30) tulee muotoon $\pi_j = \pi_l$. Siten myös

$$j = l. \tag{4.31}$$

Yhtälöt (4.28) ja (4.30) osoittavat, että kuvauksia ϕ_{ij} on täsmälleen $r \cdot s$ kappaletta. Koska yhtälön (4.24) perusteella $rs = n$, niin riittää osoittaa, että jokainen K-monomorfismi kunnalta L kunnalle N on muotoa (4.26).

Olkoon tätä varten $\rho : L \hookrightarrow N$ mielivaltainen K-monomorfismi. Koska α on polynomin $m \in K[x]$ nollakohta kunnassa L ja ρ on K-monomorfismi, niin $\rho(\alpha)$ on polynomin $m = \rho(m)$ nollakohta kunnassa N eli $\rho(\alpha) = \alpha_i$ jollekin $i = 1, \ldots, r$. Kuvaus τ_i on K-automorfismi kunnassa N ja kuvaus $\rho : L \to N$ on K-monomorfismi. Tällöin yhdistetty kuvaus

$$\pi = \tau_i^{-1} \circ \rho \tag{4.32}$$

on $K(\alpha)$-monomorfismi joukolta L joukolle N, jos $\pi|_{K(\alpha)} = I$. Nyt

$$\pi(\alpha) = \tau_i^{-1} \circ \rho(\alpha) = \tau_i^{-1}(\alpha_i). \tag{4.33}$$

Yhtälön (4.25) ja valinnan $\alpha = \alpha_1$ perusteella yhtälöstä (4.33) seuraa, että $\pi(\alpha) = \alpha$. Koska lisäksi $\pi|_K = I$, niin π on $K(\alpha)$-monomorfismi kunnalta K kunnalle N. $K(\alpha)$-monomorfismeja $L \to N$ on tasan s kappaletta ja ne ovat nimeltään $\pi_1, \ldots, \pi_s$, joten $\pi = \pi_j$ jollekin $j = 1, \ldots, s$. Yhdistämällä tämä yhtälöön (4.32) saadaan

$$\pi_j = \tau_i^{-1} \circ \rho$$

eli

$$\rho = \tau_i \circ \pi_j = \phi_{ij},$$

mikä on muotoa (4.26). Tämä todistaa väitteen. □

LAUSE 4.21 (Ensimmäinen Galois'n lause). *Olkoon $K \hookrightarrow L$ normaali ja äärellisasteinen kuntalaajennus. Tällöin laajennuksen $K \hookrightarrow L$ Galois'n ryhmän $\Gamma(K, L)$ kertaluku on laajennuksen $K \hookrightarrow L$ aste eli*

$$\#\Gamma(K, L) = [K \hookrightarrow L].$$

TODISTUS. Lauseen 4.20 perusteella on olemassa täsmälleen $[K \hookrightarrow L]$ kappaletta erillisiä K-monomorfismeja kunnalta L kunnalle L. Edelleen lemman 4.19 nojalla jokainen tällainen K-monomorfismi kunnalta L kunnalle L on myös K-automorfismi kunnassa L. Täten on olemassa täsmälleen $[K \hookrightarrow L]$ erillistä K-automorfismia kunnassa L. Nämä K-automorfismit ovat ryhmän $\Gamma(K, L)$ alkiot, joten väite pätee. □

LAUSE 4.22. *Olkoot $K \subset L \subset \mathbb{C}$ kuntia sekä $K \hookrightarrow L$ normaali ja äärellisasteinen kuntalaajennus. Tällöin pätee*

$$\mathrm{fix}(\Gamma(K, L)) = K$$

TODISTUS. Koska $K \hookrightarrow L$ on normaali ja äärellisasteinen kuntalaajennus, niin ensimmäisen Galois'n lauseen 4.21 mukaan

$$\#\Gamma(K, L) = [K \hookrightarrow L]. \tag{4.34}$$

Toisaalta lauseen 4.11 mukaan

$$[\mathrm{fix}(\Gamma(K, L)) \hookrightarrow L] = \#\Gamma(K, L). \tag{4.35}$$

Yhdistämällä yhtälöt (4.34) ja (4.35) saadaan selville, että

$$[\mathrm{fix}(\Gamma(K, L)) \hookrightarrow L] = [K \hookrightarrow L].$$

Lauseen 4.6 perusteella tiedetään, että $K \subset \mathrm{fix}(\Gamma(K, L))$. Tällöin käyttämällä lausetta 2.22 saadaan yhtälö

$$[\mathrm{fix}(\Gamma(K, L)) \hookrightarrow L] = [K \hookrightarrow L] = [K \hookrightarrow \mathrm{fix}(\Gamma(K, L))] \cdot [\mathrm{fix}(\Gamma(K, L)) \hookrightarrow L]. \tag{4.36}$$

Yhtälö (4.36) ei voi kuitenkaan päteä, ellei ole $[K \hookrightarrow \mathrm{fix}(\Gamma(K, L))] = 1$. Silloin on oltava $K = \mathrm{fix}(\Gamma(K, L))$. □

Lause 4.22 pätee myös kääntäen. Todistetaan tämä seuraavaksi.

LAUSE 4.23. *Olkoot $K \subset L \subset \mathbb{C}$ kuntia ja olkoon $K \hookrightarrow L$ äärellisasteinen kuntalaajennus. Jos*

$$\mathrm{fix}(\Gamma(K, L)) = K,$$

niin kuntalaajennus $K \hookrightarrow L$ on normaali.

TODISTUS. Osoitetaan, että on olemassa kunta N, jolle $L \subset N$ sekä $K \hookrightarrow N$ on äärellisasteinen ja normaali ja jokainen K-monorfismi $\tau : L \to N$ on kunnan L K-automorfismi. Koska $K \hookrightarrow L$ on äärellisasteinen, niin ensimmäisen Galois'n lauseen 4.21 mukaan Galois'n ryhmä $\Gamma(K, L)$ on äärellinen. Nyt voidaan käyttää lausetta 4.11. Sen ja oletuksen $\mathrm{fix}(\Gamma(K, L)) = K$ mukaan

$$[K \hookrightarrow L] = [\mathrm{fix}(\Gamma(K, L)) \hookrightarrow L] = \#\Gamma(K, L) = n \tag{4.37}$$

jollain $n \in \mathbb{N}$.

Olkoon N kuntalaajennuksen $K \hookrightarrow L$ normaalisulkeuma. Lauseen 4.17 perusteella $K \hookrightarrow N$ on äärellisasteinen. Olkoon τ K-monomorfismi $L \to N$. Jokainen ryhmän $\Gamma(K, L)$ alkio määrittelee kunnan L K-automorfismin, joita on yhtälön (4.37) nojalla yhteensä n kappaletta. Koska $L \subset N$, niin jokainen ryhmän $\Gamma(K, L)$ alkio määrittelee myös K-monomorfismin $\pi_i : L \to N, i = 1, \ldots, n$. Jos olisi $\tau \neq \pi_i$ kaikilla $i = 1, \ldots, n$, niin K-monomorfismeja $L \to N$ olisi vähintään $n + 1$ kappaletta. Tämä on ristiriidassa lemman 4.20 kanssa, jonka mukaan niitä on tasan $[K \hookrightarrow L] = n$ kappaletta. Siten on oltava $\tau = \pi_i$ jollain i eli mielivaltainen K-monomorfismi $\tau : L \to N$ on K-automorfismi $L \to L$. Näin ollen lemman 4.19 mukaan $K \hookrightarrow L$ on normaali. □

4.5. Galois'n lauseet

Edellisessä kappaleessa todistettiin ensimmäinen Galois'n lause eli lause 4.21. Galois'n mukaan on nimetty myös neljä muuta Galois'n ryhmiä ja kiintopistekuntia koskevaa lausetta, jotka todistetaan tässä kappaleessa. Näitä lauseita varten tarvitaan ensin muutama merkintä.

Olkoot $K \subset L \subset \mathbb{C}$ kuntia. Määritellään joukot

$$\mathcal{F} = \{M \mid M \text{ on kunnan } L \text{ alikunta ja } K \subset M\}$$

sekä

$$\mathcal{G} = \{H \mid \ H \text{ on ryhmän } \Gamma(K, L) \text{ aliryhmä}\}.$$

Määritellään lisäksi kuvaus $\Phi : \mathcal{F} \to \mathcal{G}$,

$$\Phi(M) = \Gamma(M, L)$$

kaikille $M \in \mathcal{F}$ sekä kuvaus $\Psi : \mathcal{G} \to \mathcal{F}$,

$$\Psi(H) = \text{fix}(H)$$

kaikille $H \in \mathcal{G}$. Lauseet 4.6 ja 4.7 varmistavat, että kuvaukset on määritelty järkevästi.

Lause 4.24 (Toinen Galois'n lause). *Olkoon $K \subset L \subset \mathbb{C}$ kuntia ja $K \hookrightarrow L$ äärellisasteinen ja normaali. Tällöin kuvaukset $\Phi : \mathcal{F} \to \mathcal{G}$ ja $\Psi : \mathcal{G} \to \mathcal{F}$ ovat toistensa käänteiskuvauksia.*

Todistus. Todistetaan ensiksi, että

$$\Psi \circ \Phi = I_{\mathcal{F}}.$$

Olkoon $M \in \mathcal{F}$ mielivaltainen kunta. Koska kuntalaajennus $K \hookrightarrow L$ on äärellisasteinen ja $K \subset M \subset L$, niin lauseen 2.23 perusteella $M \hookrightarrow L$ on äärellisasteinen. Lisäksi lauseen 3.8 mukaan L on jonkin polynomin $p \in K[x]$ hajotuskunta. Olkoot $\alpha_1, \ldots, \alpha_n$ polynomin p nollakohdat kunnassa L. Tällöin

$$L = K(\alpha_1, \ldots, \alpha_n). \tag{4.38}$$

Polynomin p hajotuskunta kunnan M suhteen on puolestaan $M(\alpha_1, \ldots, \alpha_n)$. Seuraavaksi osoitetaan, että $L = M(\alpha_1, \ldots, \alpha_n)$. Koska $K \subset M$, niin yhtälön (4.38) nojalla $L \subset M(\alpha_1, \ldots, \alpha_n)$. Lisäksi $M(\alpha_1, \ldots, \alpha_n) \subset L$, sillä $M \subset L$ ja $\alpha_1, \ldots, \alpha_n \in L$. Siten $L = M(\alpha_1, \ldots, \alpha_n)$, jolloin lauseen 3.8 perusteella $M \hookrightarrow L$ on normaali.

Lauseen 4.22 mukaiset oletukset ovat nyt voimassa. Sen perusteella

$$M = \mathrm{fix}(\Gamma(M, L)).$$

Tämä on yhtäpitävää sen kanssa, että

$$\Psi(\Phi(M)) = M,$$

mikä todistaa väitteen ensimmäisen osan.

Todistetaan seuraavaksi, että

$$\Phi \circ \Psi = I_{\mathcal{G}}. \tag{4.39}$$

Olkoon siis $H \in \mathcal{G}$ ryhmä. Todistuksen ensimmäisen osan perusteella pätee

$$\Psi(\Phi(\Psi(H))) = \Psi(H). \tag{4.40}$$

Koska $K \hookrightarrow L$ on äärellisasteinen kuntalaajennus, niin ensimmäisen Galois'n lauseen 4.21 nojalla ryhmä $\Gamma(K, L)$ on äärellinen. Koska $H \in \mathcal{G}$, niin $H \subset \Gamma(K, L)$, jolloin H on äärellinen. Tällöin voidaan käyttää lausetta 4.11, jonka mukaan

$$[\Psi(H) \hookrightarrow L] = \#H. \tag{4.41}$$

Yhdistämällä yhtälöt (4.40) ja (4.42) saadaan

$$[\Psi(\Phi(\Psi(H))) \hookrightarrow L] = \#H. \tag{4.42}$$

Tarkastellaan seuraavaksi ryhmää $\Phi(\Psi(H))$. Se on myös äärellinen ryhmä, sillä $\Phi(\Psi(H)) \subset \Gamma(K, L)$. Näin ollen voidaan käyttää toisen kerran lausetta 4.11. Tällöin saadaan

$$[\Psi(\Phi(\Psi(H))) \hookrightarrow L] = \#\Phi(\Psi(H)). \tag{4.43}$$

Yhtälöiden (4.42) ja (4.43) perusteella on oltava $\#\Phi(\Psi(H)) = \#H$. Toisaalta, koska lauseen 4.7 mukaan

$$H \subset \Phi(\Psi(H)),$$

niin on oltava

$$\Phi(\Psi(H)) = H.$$

Tämä on yhtäpitävää väitteen (4.39) kanssa. □

Lause 4.25 (Kolmas Galois'n lause). *Olkoot $K \subset M \subset L \subset \mathbb{C}$ kuntia ja olkoon $K \hookrightarrow L$ normaali ja äärellisasteinen kuntalaajennus. Tällöin $[M \hookrightarrow L] = \#\Gamma(M, L)$ ja*

$$[K \hookrightarrow M] = \frac{\#\Gamma(K, L)}{\#\Gamma(M, L)}$$

Todistus. Täsmälleen samoin kuin lauseessa 4.24 nähdään, että kuntalaajennus $M \hookrightarrow L$ on äärellisasteinen ja normaali. Tällöin ensimmäisestä Galois'n lauseesta 4.21 seuraa, että

$$[M \hookrightarrow L] = \#\Gamma(M, L). \tag{4.44}$$

Käyttämällä yhtälöä (4.44) saadaan toinen todistettava väite muotoon

$$[K \hookrightarrow M] \cdot [M \hookrightarrow L] = [K \hookrightarrow L]. \tag{4.45}$$

Yhtälö (4.45) seuraa suoraan lauseesta 2.22. □

LEMMA 4.26. *Olkoot $K \subset M \subset L \subset \mathbb{C}$ kuntia, $K \hookrightarrow L$ normaali ja äärellisasteinen kuntalaajennus sekä $f : L \to L$ K-automorfismi. Tällöin pätee*

$$\Phi(f(M)) = \{f \circ \tau \circ f^{-1} \,|\, \tau \in \Phi(M)\}$$

TODISTUS. Todistetaan ensiksi, että

$$\{f \circ \tau \circ f^{-1} \,|\, \tau \in \Phi(M)\} \subset \Phi(f(M)). \tag{4.46}$$

Valitaan mielivaltaiset $\tau \in \Phi(M)$ ja $x \in f(M)$. Nyt on olemassa $m \in M$, jolle pätee $f(m) = x$. Muistaen, että τ on M-automorfismi, saadaan

$$f \circ \tau \circ f^{-1}(x) = f \circ \tau(m) = f(m) = x. \tag{4.47}$$

Koska τ, f ja f^{-1} ovat kunnan L automorfismeja, niin myös $f \circ \tau \circ f^{-1}$ on kunnan L automorfismi. Tällöin yhtälön (4.47) mukaan $f \circ \tau \circ f^{-1}$ on kunnan L $f(M)$-automorfismi. Siten $f \circ \tau \circ f^{-1} \in \Gamma(f(M), L)$, jolloin väite (4.46) seuraa.

Todistetaan seuraavaksi, että

$$\Phi(f(M)) \subset \{f \circ \tau \circ f^{-1} \,|\, \tau \in \Phi(M)\}. \tag{4.48}$$

Tätä varten muokataan joukko $\Phi(f(M))$ muotoon

$$\Phi(f(M)) = \{\tau \,|\, \tau \in \Phi(f(M))\} = \{f \circ f^{-1} \circ \tau \circ f \circ f^{-1} \,|\, \tau \in \Phi(f(M))\}. \tag{4.49}$$

Käyttämällä jo todistettua inkluusiota (4.46) K-automorfismille f^{-1} ja kunnalle $f(M)$, $K \subset f(M)$,saadaan

$$\{f^{-1} \circ \tau \circ f \,|\, \tau \in \Phi(f(M))\} \subset \Phi(f^{-1}(f(M))) = \Phi(M). \tag{4.50}$$

Lopulta yhdistämällä yhtälöt (4.49) ja (4.50) saadaan yhtälö

$$\Phi(f(M)) \subset \{f \circ \sigma \circ f^{-1} \,|\, \sigma \in \Phi(M)\},$$

mikä todistaa väitteen (4.48). Koska sekä (4.46) että (4.48) pätevät, on väite todistettu. □

Seuraava lause antaa yhteyden normaalin kuntalaajennuksen ja normaalin aliryhmän välille.

LAUSE 4.27 (Neljäs Galois'n lause). *Olkoot $K \subset M \subset L \subset \mathbb{C}$ kuntia ja $K \hookrightarrow L$ normaali ja äärellisasteinen kuntalaajennus. Kuntalaajennus $K \hookrightarrow M$ on normaali ja äärellisasteinen, jos ja vain jos ryhmä $\Gamma(M, L)$ on ryhmän $\Gamma(K, L)$ normaali aliryhmä.*

TODISTUS. Oletetaan ensiksi, että kuntalaajennus $K \hookrightarrow L$ on normaali. Koska $K \subset M$, niin $\Gamma(M, L)$ on suoraan Galois'n ryhmän määritelmän mukaan ryhmän $\Gamma(K, L)$ aliryhmä. Täytyy siis osoittaa, että se on normaali. Olkoon $f \in \Gamma(K, L)$. Tällöin f on kunnan L K-automorfismi ja $f|_M : M \to L$ K-monomorfismi. Oletuksen ja lemman 4.19 kohdan (1) $\Rightarrow$ (3) mukaan $f|_M$ on kunnan M K-automorfismi. Siten pätee $f(M) = M$. Mielivaltaiselle $g \in \Gamma(M, L)$ on voimassa lemman 4.26 ja kuvauksen Φ määritelmän perusteella

$$f \circ g \circ f^{-1} \in \Phi(f(M)) = \Gamma(f(M), L). \tag{4.51}$$

Koska $f(M) = M$, niin yhtälö (4.51) tarkoittaa sitä, että

$$f \circ g \circ f^{-1} \in \Gamma(M, L).$$

Tämä osoittaa, että $\Gamma(M, L)$ on ryhmän $\Gamma(K, L)$ normaali aliryhmä.

Oletetaan sitten, että $\Gamma(M, L)$ on ryhmän $\Gamma(K, L)$ normaali aliryhmä. Olkoon $\sigma : M \to L$ mielivaltainen K-monomorfismi. Osoitetaan, että σ on kunnan M K-automorfismi. Koska $K \hookrightarrow L$ on äärellisasteinen ja normaali, voidaan käyttää lausetta 4.13. Sen mukaan on olemassa kunnan L K-automorfismi τ, jolle pätee $\tau|_M = \sigma$. Koska $\tau \in \Gamma(K, L)$ ja $\Gamma(M, L)$ on ryhmän $\Gamma(K, L)$ normaali aliryhmä, niin

$$\{\tau \circ \phi \circ \tau^{-1} \mid \phi \in \Gamma(M, L)\} = \Gamma(M, L) = \Phi(M). \tag{4.52}$$

Käyttämällä lemmaa 4.26 ja yhtälöä (4.52) saadaan

$$\Phi(\tau(M)) = \Phi(M).$$

Toisen Galois'n lauseen 4.24 mukaan Φ on bijektio ja siten injektio. Tällöin pätee $\tau(M) = M$. Tällöin kuitenkin $\sigma(M) = M$, jolloin σ on kunnan M K-automorfismi. Lemman 4.19 nojalla $K \hookrightarrow M$ on normaali kuntalaajennus. □

Lause 4.28 (Viides Galois'n lause). *Olkoot $K \subset M \subset L \subset \mathbb{C}$ kuntia ja $K \hookrightarrow L$ sekä $K \hookrightarrow M$ äärellisasteisia ja normaaleja kuntalaajennuksia. Tällöin*

$$\Gamma(K, M) \cong \Gamma(K, L)/\Gamma(M, L).$$

Todistus. Jotta väite olisi järkevä, täytyy tekijäryhmän $\Gamma(K, L)/\Gamma(M, L)$ olla olemassa. Tämän sanoo neljäs Galois'n lause.

Määritellään seuraavaksi kuvaus $\Xi : \Gamma(K, L) \to \Gamma(K, M)$ asettamalla $\Xi(\tau) = \tau|_M$ kaikille $\tau \in \Gamma(K, L)$. Koska τ on K-automorfismi $L \to L$ ja $M \subset L$, niin $\tau|_M$ on K-monomorfismi $M \to L$. Tällöin lemman 4.19 mukaan $\tau|_M$ on myös K-automorfismi $M \to M$. Siten $\tau|_M = \Xi(\tau) \in \Gamma(K, M)$, jolloin Ξ on ainakin kuvaus. Lisäksi se on selvästi homomorfismi.

Lauseen 4.13 nojalla jokaiselle $\sigma \in \Gamma(K, M)$ on olemassa sellainen $\tau \in \Gamma(K, L)$, jolle pätee $\tau|_M = \sigma$. Kuvaus Ξ on siis surjektio eli

$$\operatorname{im}(\Xi) = \Gamma(K, M). \tag{4.53}$$

Ryhmän $\Gamma(K, M)$ neutraalialkio on I_M. Jos $\Xi(\tau) = I_M$, niin kuvauksen Ξ määritelmän perusteella $\tau \in \Gamma(M, L)$. Jos taas $\tau \in \Gamma(M, L)$, niin $\Xi(\tau) = I_M$. Siten kuvauksen Ξ ytimelle pätee

$$\ker(\Xi) = \Gamma(M, L). \tag{4.54}$$

Nyt ryhmäteorian peruslausetta sekä yhtälöitä (4.53) ja (4.54) käyttämällä saadaan

$$\Gamma(K, M) = \operatorname{im}(\Xi) \cong \Gamma(K, L)/\ker(\Xi) = \Gamma(K, L)/\Gamma(M, L),$$

mikä todistaa väitteen. □

LUKU 5

Ryhmäteoriaa

Jotta Galois'n ryhmistä saataisiin merkittävää apua polynomiyhtälöiden ratkeavuuksien selvittämiseen, täytyy ensiksi tutkia hieman ryhmäteoriaa. Olennaisimmat käsitteet Galois'n ryhmien kannalta ovat tässä luvussa esiteltävät ratkeavat ja yksinkertaiset ryhmät.

5.1. Symmetriset ja alternoivat ryhmät

MÄÄRITELMÄ 5.1. Bijektiosta $f : \{1, 2 \ldots, n\} \to \{1, 2, \ldots, n\}$ käytetään nimeä *n-permutaatio* tai yleisemmin vain *permutaatio*.

MÄÄRITELMÄ 5.2. Kun kuvausten yhdistäminen toimii laskutoimituksena, sanotaan n-permutaatioiden muodostamaa ryhmää *symmetriseksi ryhmäksi* ja siitä käytetään merkintää $\mathbb{S}_n$. Symmetrisen ryhmän neutraalialkiosta eli identtisestä kuvauksesta käytetään merkintää (1).

MÄÄRITELMÄ 5.3. Olkoon $2 \leq k \leq n$ ja olkoot $a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n\}$ sekä $a_i \neq a_j$, kun $i \neq j$. Permutaatio $f \in \mathbb{S}$ on *k-sykli*, jos se täyttää seuraavat ehdot:

(1) $f(a_i) = a_{i+1}$ kaikilla $i = 1, 2, \ldots, k-1$

(2) $f(a_k) = a_1$

(3) $f(b) = b$, kun $b \in \{1, 2, \ldots, n\} \setminus \{a_1, a_2, \ldots, a_k\}$.

Jos permutaatio toteuttaa ehdot (1)-(3), siitä käytetään merkintää $(a_1 a_2 \ldots a_k)$. Sanotaan, että syklit $(a_1 a_2 \ldots a_k)$ ja $(b_1 b_2 \ldots b_m)$ ovat *erilliset*, jos

$$\{a_1 a_2 \ldots a_k\} \cap \{b_1 b_2 \ldots b_m\} = \emptyset.$$

HUOMAUTUS 5.4. Erilliset syklit ovat siinä mielessä mielenkiintoisia, että − toisin kuin syklit yleensä − ne kommutoivat. Toinen niiden tärkeä piirre on, että jokainen permutaatio voidaan esittää erillisten syklien tulona. Jokainen permutaatio voidaan esittää myös 2-syklien tulona, mutta tällöin kaikki syklit eivät ole välttämättä toisistaan erillisiä. Myöskään esitys ei ole tällöin yksikäsitteinen. Kuitenkin jos permutaatio voidaan esittää parillisen monen 2-syklin tulona, sitä ei voida esittää parittoman monen 2-syklin tulona. Tämä johtaa seuraavaan määritelmään.

MÄÄRITELMÄ 5.5. Permutaatiota, joka voidaan esittää parillisen monen 2-syklin tulona, kutsutaan *parilliseksi permutaatioksi*. Vastaavasti muita permutaatioita kutsutaan *parittomiksi permutaatioiksi*. Parillisten permutaatioiden joukkoa kutsutaan *alternoivaksi ryhmäksi* ja merkitään $\mathbb{A}_n$.

HUOMAUTUS 5.6. Symmetrisen ryhmän $\mathbb{S}_n$ alkioiden lukumäärä on $n!$. Alternoiva ryhmä $\mathbb{A}_n$ on symmetrisen ryhmän $\mathbb{S}_n$ aliryhmä. Alternoiva ryhmä $\mathbb{A}_n$ sisältää täsmälleen puolet symmetrisen ryhmän $\mathbb{S}_n$ alkioista, ja siten $\#\mathbb{A}_n = \frac{1}{2}n!$. Lisäksi jokainen k-sykli on parillinen permutaatio, jos ja vain jos k on pariton.

LEMMA 5.7. *Olkoon $n \geq 2$ ja $a \in \{1, 2, \ldots, n\}$ kiinteä. Tällöin kaikki 2-syklit muotoa $(ar), r \in \{1, 2, \ldots, n\}$ virittävät symmetrisen ryhmän $\mathbb{S}_n$.*

TODISTUS. Symmetrisen ryhmän $\mathbb{S}_n$ jokainen alkio voidaan esittää 2-syklien tulona. Tällöin riittää osoittaa, että jos $(bc) \in \mathbb{S}_n$ on mielivaltainen 2-sykli, niin se voidaan esittää tulona muotoa (ar) olevista alkioista.

Jos $a \neq b$ ja $a \neq c$, nähdään alkioiden kuvautumisia tarkastelemalla, että

$$(ab)(ac)(ab) = (bc).$$

Koska (ab) ja (bc) ovat muotoa (ar), niin tällöin väite pätee. Osoitettavaksi jää vielä tapaukset, joissa $b = a$ tai $c = a$. Jos $b = a$, niin $(bc) = (ac)$, jolloin väite seuraa. Jos taas $c = a$, niin $(bc) = (ba) = (ab)$, sillä 2-syklien tapauksessa alkioiden keskinäisellä järjestyksellä ei ole väliä. Jälleen päädytään haluttuun muoton (ar), joten väite pätee myös näissä poikkeustapauksissa. □

LEMMA 5.8. *Olkoon $n \geq 3$ ja $a \in \{1, 2, \ldots, n\}$ kiinteä. Tällöin kaikki 3-syklit muotoa $(ars), r, s \in \{1, 2, \ldots, n\}$, virittävät alternoivan ryhmän $\mathbb{A}_n$.*

TODISTUS. Olkoon $f \in \mathbb{A}_n$ mielivaltainen. Täytyy osoittaa, että f voidaan esittää tulona alkioista, jotka ovat muotoa (ars). Jos $f = (1)$, niin kaikille r ja s pätee $(ars)^3 = (1) = f$, joten ainakin permutaatio (1) voidaan esittää 3-syklien tulona.

Tarkastellaan sitten tapausta, jossa $f \neq (1)$. Lemman 5.7 nojalla f voidaan esittää muodossa

$$f = (ar_1)(ar_2)\ldots(ar_m),$$

missä $r_i \in \{1, 2, \ldots, n\} \setminus \{a\}$. Koska $f \in \mathbb{A}_n$, niin 2-syklejä (ar_j) on parillinen määrä, joten f voidaan jakaa perättäisiin 2-syklien pareihin. Koska lisäksi kuvausten yhdistäminen on assosiatiivinen laskutoimitus, voidaan jokaista paria tarkastella erikseen. Jos siis voidaan osoittaa, että mielivaltainen peräkkäisten 2-syklien pari $(ar_j)(ar_{j+1}), j \in \{1, 2, \ldots, m-1\}$, voidaan esittää tulona 3-sykleistä, niin silloin myös f voidaan esittää tulona 3-sykleistä.

Jos $r_j = r_{j+1}$, niin $(ar_j)(ar_{j+1}) = (1)$. Koska oletettin, että $f \neq (1)$, niin ei voi olla $r_j = r_{j+1}$ kaikille pareille r_j ja r_{j+1}. Koska neutraalialkiolla kertominen ei muuta permutaatiota f, rajaudutaan tarkastelemaan tilanteita $r_j \neq r_{j+1}$. Tällöin eri alkioiden kuvautumisia tarkastelemalla havaitaan, että

$$(ar_j)(ar_{j+1}) = (ar_{j+1}r_j),$$

joten jokainen pari voidaan esittää 3-syklien tulona. □

LEMMA 5.9. *Olkoon $n \geq 3$ ja olkoot $a, b \in \{1, 2, \ldots, n\}$ kiinteitä siten, että $a \neq b$. Tällöin kaikki 3-syklit muotoa $(abt), t \in \{1, 2, \ldots, n\}$ virittävät alternoivan ryhmän $\mathbb{A}_n$.*

TODISTUS. Lemman 5.8 mukaan permutaatio $f \in \mathbb{A}_n$ voidaan esittää tulona 3-sykleistä (ars), missä $a \in \{1, 2, \ldots, n\}$ on kiinteä. Nyt osoitetaan, että jokainen tällainen 3-sykli (ars) voidaan esittää tulona 3-sykleistä (abt), missä $t \in \{1, 2, \ldots n\}$.

Jos $r = b$, niin sykli $(ars) = (abs)$ on haluttua muotoa. Jos taas $s = b$, niin

$$(ars) = (arb) = (abr)^2,$$

jolloin (ars) on myös haluttua muotoa.

Oletetaan siis, että $r \neq b$ ja $s \neq b$. Tällöin eri alkioiden kuvautumisia tarkastelemalla saadaan

$$(ars) = (abs)^2(abr)(abs).$$

Koska (abs) ja (abr) ovat molemmat etsittyä muotoa, niin (ars) ja siten f voidaan esittää tulona 3-sykleistä (abt). □

LAUSE 5.10. *Olkoon $\sigma \in \mathbb{S}_p \setminus \{(1)\}$ permutaatio. Jos p on alkuluku ja $\sigma^p = (1)$, niin σ on p-sykli.*

TODISTUS. Täytyy siis osoittaa, että $\sigma = (a_1 \ldots a_p)$, missä $\{a_1, \ldots, a_p\} = \{1, \ldots, p\}$. Permutaatio $\sigma \neq (1)$ voidaan esittää erillisten syklien tulona, jolloin

$$\sigma = (a_1 \ldots a_n)\tau$$

jollekin $n = 2, \ldots, p$ ja jollekin syklistä $(a_1 \ldots a_n)$ erilliselle permutaatiolle $\tau \in \mathbb{S}_p$. Koska erilliset permutaatiot kommutoivat ja $\sigma^p = (1)$, niin

$$\sigma^p = (a_1 \ldots a_n)^p \tau^p = (1). \tag{5.1}$$

Permutaatiot $(a_1 \ldots a_n)$ ja τ ovat erilliset, jolloin $\tau(a_i) = a_i$ kaikilla $i = 1, \ldots, n$ ja $(a_1 \ldots a_n)(j) = j$ kaikilla $j \in \{1, \ldots, p\} \setminus \{a_1, \ldots, a_n\}$. Silloin yhtälö (5.1) ei voi päteä, ellei ole

$$(a_1 \ldots a_n)^p = (1) \tag{5.2}$$

ja

$$\tau^p = (1).$$

Syklin $(a_1 \ldots a_n)$ kertaluku on n. Toisaalta yhtälön (5.2) perusteella syklin $(a_1 \ldots a_n)$ kertaluku n jakaa luvun p. Koska p on kuitenkin alkuluku ja $n \geq 2$, niin $n = p$, jolloin $\sigma = (a_1 \ldots a_p)$. □

LEMMA 5.11. *Olkoon p alkuluku. Tällöin mielivaltainen p-sykli ja 2-sykli virittävät symmetrisen ryhmän $\mathbb{S}_p$.*

TODISTUS. Olkoon (ab) mielivaltainen 2-sykli ja $\kappa = (a_1 a_2 \ldots a_p)$ mielivaltainen p-sykli sekä $H \subset \mathbb{S}_p$ näiden virittämä ryhmä. Täytyy osoittaa, että $H = \mathbb{S}_p$. Koska lemman 5.7 mukaan 2-syklit (ar) virittävät koko symmetrisen ryhmän, riittää osoittaa, että

$$(as) \in H \tag{5.3}$$

kaikilla $s \in \{1, 2, \ldots, p\} \setminus \{a, b\}$. Nyt kaikille $m = 1, 2, \ldots, p-1$ pätee

$$(\kappa^m)^p = (\kappa^p)^m = (1)^m = (1).$$

Tällöin lauseesta 5.10 seuraa, että κ^m on p-sykli. Koska lisäksi pätee $a, b \in \{1, 2, \ldots, p\} = \{a_1, a_2, \ldots, a_p\}$ ja $a \neq b$ eli a ja b ovat myös p-syklin alkioita, niin voidaan valita $m \in \{1, 2, \ldots, p-1\}$ siten, että

$$\kappa^m = (abs_1 s_2 \cdots s_{p-2}), \tag{5.4}$$

missä $\{s_1, s_2, \ldots s_{p-2}\} \in \{1, 2, \ldots, p\} \setminus \{a, b\}$ eli alkiot s_i ovat niitä permutaation κ alkioita, jotka eivät ole alkioita a ja b.

Koska $\kappa \in H$, niin $\kappa^m \in H$. Koska myös $(ab) \in H$, niin tällöin myös

$$\kappa^m (ab) \kappa^{-m} \in H. \tag{5.5}$$

Käyttäen permutaation κ^m määritelmää (5.4) ja tarkastelemalla eri alkioiden kuvautumisia saadaan

$$\kappa^m (ab) \kappa^{-m} = (bs_1), \tag{5.6}$$

joten yhtälöistä (5.5) ja (5.6) seuraa, että

$$(bs_1) \in H. \tag{5.7}$$

Siten myös $\kappa^m (bs_1) \kappa^{-m} \in H$ ja syklien tuloksi saadaan

$$\kappa^m (bs_1) \kappa^{-m} = (s_1 s_2) \in H. \tag{5.8}$$

Vastaavasti voidaan jatkaa, jolloin voidaan induktiivisesti päätellä, että

$$(s_i s_{i+1}) \in H \text{ kaikilla } i \in \{1, 2, \ldots, p-3\}. \tag{5.9}$$

Koska yhtälön (5.7) nojalla $(bs_1) \in H$, niin saadaan

$$(ab)(bs_1)(ab) = (as_1) \in H.$$

Seuraavaksi tarkastelemalla eri alkioiden kuvautumisia ja käyttämällä ehtoa (5.9) saadaan

$$(ab)(s_1 s_2)(ab) = (as_2) \in H.$$

Yhtälön (5.9) nojalla tätäkin voidaan jatkaa induktiivisesti ja todeta, että

$$(as_i) \in H \text{ kaikilla } i \in \{1, 2, \ldots, p-2\}. \tag{5.10}$$

Yhtälö (5.10) on yhtäpitävä yhtälön (5.3) kanssa, joten $H = \mathbb{S}_p$. □

5.2. Ratkeavat ryhmät

Seuraavaksi määritelään ryhmille ominaisuus, jota kutsutaan ratkeavuudeksi. Ratkeavuus muistuttaa kommutatiivisuutta, mutta on paljon löysempi ominaisuus: kaikki kommutatiiviset ryhmät ovat ratkeavia. Käsitteen nimityksen perusteella voi olettaa, että ratkeavuudella on paljonkin tekemistä ratkaisukaavan kanssa. Syy siihen, miksi tämä ominaisuus nimetään juuri ratkeavuudeksi paljastuu vasta luvussa 6.

Tässä luvussa otetaan käyttöön muutamia standardimerkintöjä. Jos H ja G ovat ryhmiä ja H on ryhmän G aliryhmä, niin merkitään $H \leq G$. Jos lisäksi H on ryhmän G normaali aliryhmä, merkitään $H \lhd G$. Jos $H_1 \leq G$ ja $H_2 \leq G$, niin käytetään merkintää $H_1 H_2 = \{h_1 h_2 \mid h_1 \in H_1 \text{ ja } h_2 \in H_2\}$.

MÄÄRITELMÄ 5.12. Ryhmä G on ratkeava, jos on olemassa sellainen äärellinen ryhmien jono

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G,$$

jolle pätee

(1) $G_i \lhd G_{i+1}$ kaikilla $i = 0, \ldots, n-1$,

(2) G_{i+1}/G_i on kommutatiivinen ryhmä kaikilla $i = 0, \ldots, n-1$.

HUOMAUTUS 5.13. Edellisen määritelmän ehdosta (1) ei seuraa, että $G_i \lhd G$, kun $i < n-1$.

ESIMERKKI 5.14. Kommutatiivinen ryhmä on aina ratkeava. Voidaan nimittäin valita ketjuksi $G_0 = \{e\} \subset G$, jolloin $G_0 \lhd G$ ja tekijäryhmä G/G_0 on myös kommutatiivinen. Symmetrinen ryhmä $\mathbb{S}_2$ on kaksialkioisena ryhmänä kommutatiivinen, joten se on ratkeava ryhmä.

ESIMERKKI 5.15. Symmetriset ryhmät $\mathbb{S}_2, \mathbb{S}_3$ ja $\mathbb{S}_4$ ovat ratkeavia. Symmetrinen ryhmä $\mathbb{S}_2$ on kaksialkioisena ryhmänä kommutatiivinen ja siten esimerkin 5.14 nojalla ratkeava. Symmetrinen ryhmä $\mathbb{S}_3$ on ratkeava, sillä voidaan valita jono ryhmiä $G_0 \lhd G_1 \lhd G$ missä $G_0 = \{e\}, G = \mathbb{S}_3$ ja G_1 permutaation $(123) \in \mathbb{S}_3$ virittämä syklinen ryhmä. Lisäksi G_1/G_0 ja G/G_1 ovat kommutatiivisia ryhmiä.

Ryhmälle $\mathbb{S}_4$ voidaan puolestaan muodostaa jono $H_0 \lhd H_1 \lhd H_2 \lhd H_3$, missä $H_0 = \{e\}, H_1 = \{(12)(34), (13)(24), (14)(23)\}, H_2 = \mathbb{A}_4$ ja $H_3 = \mathbb{S}_4$. Sen sijaan symmetrinen ryhmä $\mathbb{S}_5$ ei ole ratkeava. Tämä voidaan todistaa vasta myöhemmin.

Otetaan seuraavaksi tekijäryhmän merkinnän rinnalle toinen vaihtoehtoinen merkintä $\frac{G}{H} := G/H$, jotta peräkkäisten tekijäryhmien esittäminen olisi selkeämpää.

LEMMA 5.16. *Olkoot G, H ja A ryhmiä. Tällöin jos $H \lhd G$ ja $A \leq G$, niin pätee*

$$\frac{A}{H \cap A} \cong \frac{HA}{H}.$$

TODISTUS. Koska $H \lhd G$ niin selvästi $H \cap A \lhd A$ ja $H \lhd HA$. Siten $\frac{A}{H \cap A}$ ja $\frac{HA}{H}$ ovat hyvin määriteltyjä tekijäryhmiä. Merkitään tekijäryhmän alkioita

$$[a]_1 \in \frac{A}{H \cap A},$$

kun $a \in A$, ja

$$[x]_2 \in \frac{HA}{H},$$

kun $x \in HA$. Määritellään seuraavaksi kuvaus

$$f : \frac{A}{H \cap A} \to \frac{HA}{H}$$

asettamalla

$$f([a]_1) = [a]_2 \text{ kaikille } a \in A.$$

Osoitetaan seuraavaksi, että kuvaus f on hyvin määritelty. Tätä varten oletetaan, että

$$[a]_1 = [a']_1 \in \frac{A}{H \cap A}.$$

Tällöin $a - a' \in H \cap A$ eli $a - a' \in H$. Tämä on puolestaan yhtäpitävää sen kanssa, että

$$[a]_2 = [a']_2 \in \frac{HA}{H}.$$

Lisäksi $a \in A \subset HA$, jolloin f on hyvin määritelty. Riittää osoittaa, että f on isomorfismi. Kuvaus f on ensinnäkin homorfismi, sillä

$$f([a]_1[b]_1) = f([ab]_1) = [ab]_2 = [a]_2[b]_2 = f([a]_1)f([b]_1).$$

Kuvauksen f injektiivisyyden todistamiseksi oletetaan, että $f([a]_1) = f([b]_1)$, jolloin $[a]_2 = [b]_2$. Tällöin $ab^{-1} \in H$. Koska lisäksi $a, b \in A$, niin $ab^{-1} \in H \cap A$. Tästä seuraa, että $[a]_1 = [b]_1$, jolloin injektiivisyys pätee.

Oletetaan, että $b \in (HA)/A$. Tällöin b on muotoa $b = [ha]_2$, missä $h \in H$ ja $a \in A$. Koska $h = (ha)a^{-1}$ ja $h \in H$, niin $(ha)a^{-1} \in H$. Tällöin $b = [ha]_2 = [a]_2 = f([a]_1)$. Siten jokaisella joukon $(HA)/A$ alkiolla on alkukuva, joten f on surjektio. Koska f on bijektiivinen homomorfismi, se on isomorfismi. □

LEMMA 5.17. *Olkoot G, H ja A ryhmiä. Tällöin jos $H \lhd G$, $A \lhd G$ sekä $H \subset A$, niin $H \lhd A$, $A/H \lhd G/H$ sekä*

$$\frac{G/H}{A/H} \cong \frac{G}{A}$$

TODISTUS. Väitteet $H \lhd A$ ja $A/H \lhd G/H$ ovat ilmeisiä. Siten $\frac{G/H}{A/H}$ on hyvin määritelty tekijäryhmä. Olkoot

$$f_1 : G \to G/H$$

ja

$$f_2 : G/H \to \frac{G/H}{A/H}$$

tekijäkuvauksia. Tällöin kuvauksen f_2 ytimelle pätee

$$\ker(f_2) = \{[a] \in G/H \mid a \in A\} \cong A/H.$$

Tästä seuraa, että

$$\ker(f_2 \circ f_1) = f_1^{-1}(\{[a] \in G/H \mid a \in A\}) = A. \tag{5.11}$$

Koska f_1 ja f_2 ovat surjektiivisia homomorfismeja, niin myös $f_2 \circ f_1$ on surjektiivinen homomorfismi. Tällöin ryhmäisomorfismien peruslauseesta (ks. esimerkiksi [**6**, §4]) seuraa, että

$$G/\ker(f_1 \circ f_2) \cong \frac{G/H}{A/H}. \tag{5.12}$$

Yhdistämällä yhtälöt (5.11) ja (5.12) saadaan

$$\frac{G}{A} \cong \frac{G/H}{A/H}.$$

□

LAUSE 5.18. *Olkoot G ja H ryhmiä siten, että $H \lhd G$. Tällöin jos G on ratkeava, niin myös H on ratkeava.*

TODISTUS. Koska ryhmä G on ratkeava, niin on olemassa jono ryhmiä G_i, $i = 0, \ldots, n$, siten, että

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

ja G_{i+1}/G_i on kommutatiivinen kaikilla $i \in \{0, 1, 2, \ldots, n-1\}$. Nyt aliryhmällä $H \subset G$ voidaan valita vastaava jono aliryhmistä H_i määrittelemällä $H_i = G_i \cap H$. Tällöin ilmeisesti pätee

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = H,$$

joten täytyy enää osoittaa, että H_{i+1}/H_i on kommutatiivinen ryhmä. Alkion H_i määritelmän perusteella

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H}. \tag{5.13}$$

Koska $G_i \subset G_{i+1}$, niin $G_i = G_i \cap G_{i+1}$, jolloin

$$\frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap G_{i+1} \cap H}. \tag{5.14}$$

Käyttämällä lemmaa 5.16 saadaan

$$\frac{G_{i+1} \cap H}{G_i \cap G_{i+1} \cap H} \cong \frac{G_i(G_{i+1} \cap H)}{G_i}. \tag{5.15}$$

Koska kuitenkin G_i on ryhmän G_{i+1} aliryhmä, niin $G_i(G_{i+1} \cap H)$ on ryhmän G_{i+1} aliryhmä. Tällöin saadaan

$$\frac{G_i(G_{i+1} \cap H)}{G_i} \leq \frac{G_{i+1}}{G_i}. \tag{5.16}$$

Koska tekijäryhmä G_{i+1}/G_i on oletuksen perusteella kommutatiivinen, niin myös sen aliryhmät ovat kommutatiivisia. Tällöin yhtälön (5.16) perusteella $\frac{G_i(G_{i+1} \cap H)}{G_i}$ on kommutatiivinen. Yhtälön (5.15) nojalla myös sen kanssa isomorfinen ryhmä $\frac{G_{i+1} \cap H}{G_i \cap G_{i+1} \cap H}$ on kommutatiivinen. Nyt yhtälöistä (5.14) ja (5.13) seuraa, että H_{i+1}/H_i on kommutatiivinen, ja siten lause on todistettu. □

LAUSE 5.19. *Olkoot G ja H ryhmiä siten, että $H \lhd G$. Jos G on ratkeava, niin myös tekijäryhmä G/H on ratkeava.*

TODISTUS. Oletuksen nojalla on olemassa jono aliryhmiä $G_i, i \in \{1, 2, \ldots, n\}$, siten, että

$$e = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G \tag{5.17}$$

sekä G_{i+1}/G_i on kommutatiivinen kaikille $i \in \{0, 1, 2, \ldots, n-1\}$. Koska $H \lhd G$, niin $H \lhd G_iH$. Tällöin on olemassa jono ryhmiä $G_iH/H, i \in \{1, 2, \ldots k\}$, joille pätee

$$H/H = G_0H/H \subset G_1H/H \subset \ldots \subset G_kH/H = G/H. \tag{5.18}$$

Koska $H \lhd G$ ja yhtälön (5.17) perusteella $G_i \lhd G_{i+1}$, niin $G_iH \lhd G_{i+1}H$. Siten yhtälön (5.18) nojalla myös $G_iH/H \lhd G_{i+1}H/H$, joten

$$H/H = G_0H/H \lhd G_1H/H \lhd \ldots \lhd G_kH/H = G/H.$$

Täytyy siis vielä osoittaa, että tekijäryhmä

$$\frac{G_{i+1}H/H}{G_iH/H} \tag{5.19}$$

on kommutatiivinen. Lemmasta 5.17 saadaan

$$\frac{G_{i+1}H/H}{G_iH/H} \cong \frac{G_{i+1}H}{G_iH}. \tag{5.20}$$

Koska $G_i \subset G_{i+1}$, niin $G_{i+1}H = G_{i+1}(G_iH)$ ja siten

$$\frac{G_{i+1}H}{G_iH} = \frac{G_{i+1}(G_iH)}{G_iH}. \tag{5.21}$$

Lemmasta 5.16 saadaan, että

$$\frac{G_{i+1}(G_iH)}{G_iH} \cong \frac{G_{i+1}}{G_iH \cap G_{i+1}}. \tag{5.22}$$

Käytetetään toisen kerran lemmaa 5.17, josta seuraa

$$\frac{G_{i+1}}{G_iH \cap G_{i+1}} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iH))/G_i}. \tag{5.23}$$

Huomataan vielä, että ryhmä

$$\frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iH))/G_i}$$

on kommutatiivisen ryhmän G_{i+1}/G_i tekijäryhmä. Koska kommutatiivisen ryhmän tekijäryhmä on kommutatiivinen, niin myös tekiryhmä

$$\frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iH))/G_i}$$

on kommutatiivinen. Yhtälöiden (5.23), (5.22), (5.21) ja (5.20) mukaan se on isomorfinen ryhmän (5.19) kanssa. Siten ryhmä (5.19) on kommutatiivinen. □

Lause 5.20. *Olkoot G ja H ryhmiä siten, että $H \lhd G$. Jos H ja G/H ovat ratkeavia, niin G on ratkeava.*

Todistus. Oletuksen nojalla on olemassa jono aliryhmiä $H_i, i = 0, 1, \ldots, n$, joille pätee

$$\{e\} = H_0 \lhd H_1 \lhd \ldots \lhd H_n = H \tag{5.24}$$

sekä H_{i+1}/H_i on kommutatiivinen kaikilla i. Toisaalta oletus antaa myös jonon aliryhmiä $G_i/H, i = 0, 1, \ldots m$, joille pätee

$$H/H = G_0/H \lhd G_1/H \lhd \ldots \lhd G_m/H = G/H \tag{5.25}$$

sekä $\frac{G_{i+1}/H}{G_i/H}$ on kommutatiivinen ryhmä kaikilla i. Määritellään nyt tekijäkuvaus $f : G \to G/H$. Koska $f^{-1}(\{e\}) = H$, $f^{-1}(G/H) = G$ ja $f^{-1}(G_i/H) \leq G$ kaikille $i = 0, 1, \ldots, m$, niin jonon (5.25) olemassaolon perusteella aliryhmät $G_i \leq G$ toteuttavat ehdon

$$H = G_0 \lhd G_1 \ldots \lhd G_m = G. \tag{5.26}$$

Yhdistämällä jonot (5.24) ja (5.26) saadaan

$$\{e\} = H_0 \lhd H_1 \lhd \ldots \lhd H_n = H = G_0 \lhd G_1 \lhd \ldots \lhd G_m = G.$$

On siis löydetty jono ryhmiä M_i, joille pätee $\{e\} \lhd M_1 \lhd \ldots \lhd M = G$. Täytyy osoittaa vielä, että M_{i+1}/M_i on kommutatiivinen ryhmä. Jos M_{i+1}/M_i on muotoa H_{i+1}/H_i, niin se on kommutatiivinen. Toinen vaihtoehto on, että M_{i+1}/M on muotoa G_{i+1}/G_i. Lemman 5.17 perusteella

$$\frac{G_{i+1}}{G_i} \cong \frac{G_{i+1}/H}{G_i/H}. \tag{5.27}$$

Jonoon (5.25) liittyvän oletuksen mukaan

$$\frac{G_{i+1}/H}{G_i/H}$$

on kommutatiivinen. Siten yhtälöstä (5.27) seuraa, että myös G_{i+1}/G_i on kommutatiivinen. □

5.3. Yksinkertaiset ryhmät

Ratkeavalle ryhmälle määritellään eräänlaiseksi vastakohdaksi yksinkertainen ryhmä. Tarkalleen ottaen yksinkertaista ryhmää ei kuitenkaan määritellä ratkeavan ryhmän loogisena vastakohtana, vaan ryhmä voi olla sekä ratkeava että yksinkertainen. Kuitenkin jo lauseessa 5.22 pystytään todistamaan, että yksinkertainen ja ratkeava ryhmä on aina tiettyä muotoa.

MÄÄRITELMÄ 5.21. Olkoon G ryhmä ja e sen neutraalialkio. Sanotaan, että ryhmä G on *yksinkertainen*, jos sen ainoat normaalit aliryhmät ovat $\{e\}$ ja G.

LAUSE 5.22. *Ryhmä G on ratkeava ja yksinkertainen, jos ja vain jos se on syklinen ryhmä, jonka kertaluku on alkuluku tai $G = \{e\}$.*

TODISTUS. Osoitetaan ensiksi, että jos ryhmä G on ratkeava ja yksinkertainen, niin se on syklinen ja sen kertaluku on alkuku tai $G = \{e\}$. Koska G on ratkeava, niin on olemassa jono

$$\{e\} = G_0 \subset \ldots \subset G_n = G$$

siten, että $G_i \lhd G_{i+1}$ ja G_{i+1}/G_i on kommutatiivinen kaikilla $i = 1, \ldots, n-1$. Poistamalla useammin kuin kerran esiintyvät alkiot jonosta voidaan olettaa, että $G_i \neq G_{i+1}$. Koska G on yksinkertainen, niin sen ainoat normaalit aliryhmät ovat $\{e\}$ ja G. Koska $G_{n-1} \lhd G_n$, niin on oltava $G_{n-1} = G_0 = \{e\}$. Tällöin $G_n/G_{n-1} \cong G$. Koska G_n/G_{n-1} on kommutatiivinen, niin myös G on kommutatiivinen.

Jos $G = \{e\}$, niin väite pätee, joten oletetaan, että $G \neq \{e\}$. Tällöin on olemassa $g \in G \setminus \{e\}$, joka virittää syklisen aliryhmän $\langle g \rangle$. Koska $\langle g \rangle \leq G$ ja kommutatiivisen ryhmän G jokainen aliryhmä on normaali, niin $\langle g \rangle \lhd G$. Ryhmän G yksinkertaisuuden perusteella kuitenkin sen ainoat normaalit aliryhmät ovat $\{e\}$ ja G, joten $\langle g \rangle = \{e\}$ tai $\langle g \rangle = G$. Koska $g \neq e$, niin tapaus $\langle g \rangle = \{e\}$ on mahdoton. Siten $\langle g \rangle = G$ eli $G = \langle g \rangle$ on syklinen ryhmä. Täytyy vielä todistaa, että ryhmän G kertaluku

$\#G = k$ on alkuluku. Oletetaan, että tämä ei ole totta, toisin sanoen $k = ml$, jollain $m, l \in \mathbb{N} \setminus \{0, 1\}$. Tällöin

$$(g^m)^l = g^k = e,$$

eli

$$\#\langle g^m \rangle \leq l. \tag{5.28}$$

Koska G on kommutatiivinen, niin $\langle g^m \rangle \lhd G$. Ryhmän G yksinkertaisuuden perusteella siis $\langle g^m \rangle = G$ tai $\langle g^m \rangle = \{e\}$. Ei voi olla $\langle g^m \rangle = G$, sillä yhtälön (5.28) nojalla $\#\langle g^m \rangle \leq l < k$. Täytyy siis olla $\langle g^m \rangle = \{e\}$, jolloin $g^m = e$. Koska kuitenkin k on ryhmän G kertaluku ja g sen virittäjä, ei voi olla olemassa lukua $m < k$, jolle $g^m = e$. Ajaudutaan siis ristiriitaan, ja väite pätee.

Todistus toiseen suuntaan on yksinkertaisempi. Jos nimittäin $G \neq \{e\}$ on syklinen ryhmä, jonka kertaluku on alkuluku, niin Lagrangen lauseen nojalla sen jokaisen aliryhmän täytyisi jakaa ryhmän G kertaluku. Koska $\#G$ on kuitenkin alkuluku, ovat sen ainoat aliryhmät $\{e\}$ ja G, joten G on yksinkertainen. Lisäksi koska G on syklinen, on se myös kommutatiivinen ja esimerkin 5.14 nojalla jokainen kommutatiivinen ryhmä on ratkeava.

Jos puolestaan $G = \{e\}$, niin se on selvästi ratkeava ja yksinkertainen. □

Seuraavaksi on tarkoituksena todistaa tämän luvun päätulos eli lause 5.25: symmetrinen ryhmä $\mathbb{S}_n$ ei ole ratkeva, kun $n \geq 5$. Tämän todistamiseksi tarvitaan kaksi lemmaa.

LEMMA 5.23. *Olkoon $\mathbb{A}_n$ alternoiva ryhmä ja $n \in \mathbb{N}, n \geq 5$. Jos ryhmälle $G \neq \{(1)\}$ pätee $G \lhd \mathbb{A}_n$, niin ryhmässä G on 3-sykli.*

TODISTUS. Olkoon $g \in G \setminus \{(1)\}$. Alkio g voidaan nyt esittää erillisten syklien tulona. Jaetaan tämä todistus neljään osaan alkion g esityksen muodon mukaan.

(1) Alkiossa g on vähintään yksi k-sykli, $k \geq 4$.

(2) Alkiossa g on vähintään kaksi 3-sykliä.

(3) Alkiossa g on 3-syklejä täsmälleen yksi.

(4) Alkio g koostuu pelkistä 2-sykleistä.

Nämä neljä kohtaa kattavat kaikki mahdolliset tapaukset $g \in G$.

Tapauksessa (1) oletetaan, että $g = ax$, missä

$$a = (a_1 \dots a_k), \qquad (k \geq 4),$$

sekä x on permutaatio, joka on erillinen syklistä a. Koska 3-sykli $(a_1 a_2 a_3) \in \mathbb{A}_n$ ja $G \lhd \mathbb{A}_n$, niin saadaan

$$(a_1 a_2 a_3)^{-1} g (a_1 a_2 a_3) = (a_1 a_2 a_3)^{-1} a x (a_1 a_2 a_3) \in G.$$

Erillisten syklien kommutatiivisuuden nojalla saadaan

$$(a_1 a_2 a_3)^{-1} a (a_1 a_2 a_3) x = (a_1 a_2 a_3)^{-1} a x (a_1 a_2 a_3) \in G.$$

Nyt $g^{-1} = x^{-1}a^{-1}$. Toisaalta koska $g^{-1} \in G$, niin

$$(a_1a_2a_3)^{-1}a(a_1a_2a_3)xx^{-1}a^{-1} = (a_1a_2a_3)^{-1}a(a_1a_2a_3)xg^{-1} \in G.$$

tämä on yhtäpitävää sen kanssa, että

$$(a_1a_2a_3)^{-1}(a_1 \dots a_k)(a_1a_2a_3)(a_1 \dots a_k)^{-1} = (a_1a_2a_3)^{-1}a(a_1a_2a_3)a^{-1} \in G. \tag{5.29}$$

Lopuksi vielä eri alkioiden kuvautumisia tarkastelemalla saadaan

$$(a_1a_2a_3)^{-1}(a_1 \dots a_k)(a_1a_2a_3)(a_1 \dots a_k)^{-1} = (a_1a_3a_4). \tag{5.30}$$

Yhtälöstä (5.30) ja (5.29) seuraa, että

$$(a_1a_3a_4) \in G,$$

ja siten joukosta G on löydetty 3-sykli.

Tarkastellaan seuraavaksi tapausta (2) eli alkio g sisältää vähintään kaksi 3-sykliä. Olkoot ne nimeltään $(a_1a_2a_3)$ ja $(a_4a_5a_6)$. Nyt siis g on muotoa $g = (a_1a_2a_3)(a_4a_5a_6)y$, missä $y = (1)$ tai y on tulo erillisistä sykleistä, jotka ovat erillisiä myös sykleistä $(a_1a_2a_3)$ ja $(a_4a_5a_6)$. Koska $G \lhd \mathbb{A}_n$ ja $(a_1a_2a_4) \in \mathbb{A}_n$, niin

$$(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6)y(a_1a_2a_4)^{-1} \in G.$$

Nyt pätee $g^{-1} = y^{-1}(a_1a_2a_3)^{-1}(a_4a_5a_6)^{-1}$, joten saadaan

$$(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6)y(a_1a_2a_4)^{-1}y^{-1}(a_1a_2a_3)^{-1}(a_4a_5a_6)^{-1} \in G.$$

Sykli y on nyt erillinen syklistä $(a_1a_2a_4)$, joten se on myös erillinen syklistä $(a_1a_2a_4)^{-1}$. Siten g ja $(a_1a_2a_4)^{-1}$ kommutoivat eli pätee

$$(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6)(a_1a_2a_4)^{-1}yy^{-1}(a_1a_2a_3)^{-1}(a_4a_5a_6)^{-1} \in G.$$

mikä on sama asia kuin

$$(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6)(a_1a_2a_4)^{-1}(a_1a_2a_3)^{-1}(a_4a_5a_6)^{-1} \in G \tag{5.31}$$

Yhtälölle (5.31) saadaan laskettua

$$(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6)(a_1a_2a_4)^{-1}(a_1a_2a_3)^{-1}(a_4a_5a_6)^{-1} = (a_1a_2a_5a_3a_4), \tag{5.32}$$

joten yhtälöiden (5.31) ja (5.32) perusteella

$$(a_1a_2a_5a_3a_4) \in G.$$

Siten aliryhmässä G on 5-sykli. Kohdan (1) nojalla tämä johtaa siihen, että ryhmässä G on myös 3-sykli.

Kohdassa (3) oletetaan, että alkiossa g 3-syklejä on täsmälleen yksi. Muita syklejä ei välttämättä tarvitse olla, mutta siinä tapauksessa $g \in G$ käy etsityksi 3-sykliksi. Oletetaan siis, että on muitakin syklejä. Nämä syklit ovat 2-syklejä, sillä muuten alkiossa g olisi vähintään yksi k-sykli, $k \geq 4$. Tämä tilanne on käsitelty jo tapauksessa (1).

Olkoon $g = az$, missä $a = (a_1a_2a_3)$ ja z on tulo erillisistä 2-sykleistä, jotka ovat erillisiä syklistä a. Erillisyysehtojen vuoksi pätee kommutatiivisuus ja siten

$$g^2 = (az)^2 = (a_1a_2a_3)^2z^2. \tag{5.33}$$

Koska 2-sykleille pätee $(ab)^2 = (1)$ ja z on tulo erillisistä ja siten kommutoivista 2-sykleistä, pätee $z^2 = (1)$. Näin ollen yhtälön (5.33) nojalla

$$g^2 = (a_1a_2a_3)^2 = (a_1a_3a_2) \in G,$$

joten myös tässä tapauksessa ryhmässä G on 3-sykli.

Jäljelle jää vielä tapaus (4) eli alkion g esitys koostuu pelkistä 2-sykleistä. Koska $g \in G \setminus \{(1)\} \subset \mathbb{A}_n$, niin alkio g on tulo vähintään kahdesta 2-syklistä ja siten voidaan ilmoittaa muodossa

$$g = (a_1a_2)(a_3a_4)y, \tag{5.34}$$

missä joko $y = (1)$ tai y on tulo toisistaan erillisistä 2-sykleistä. Lisäksi nämä kaikki syklit ovat erillisiä sykleistä (a_1a_2) ja (a_3a_4), jotka ovat myös erillisiä toisistaan.

Nyt alkio $(a_2a_3a_4) \in \mathbb{A}_n$, ja koska $G \lhd \mathbb{A}_n$, niin

$$(a_2a_3a_4)^{-1}g(a_2a_3a_4) \in G.$$

Koska myös $g^{-1} \in G$, niin

$$(a_2a_3a_4)^{-1}g(a_2a_3a_4)g^{-1} \in G. \tag{5.35}$$

Alkiolle g^{-1} saadaan

$$g^{-1} = y^{-1}(a_3a_4)^{-1}(a_1a_2)^{-1} = y^{-1}(a_3a_4)(a_1a_2), \tag{5.36}$$

sillä 2-syklit ovat itsensä käänteisalkioita. Käyttämällä yhtälöä (5.36) sekä yhtälöitä (5.36) ja (5.34) saadaan

$$(a_2a_3a_4)^{-1}(a_1a_2)(a_3a_4)y(a_2a_3a_4)y^{-1}(a_3a_4)(a_1a_2) \in G. \tag{5.37}$$

Koska kaikki syklit, joista y koostuu, ovat erillisiä sykleistä (a_1a_2) ja (a_3a_4), niin alkion y syklit ovat erillisiä myös syklistä $(a_2a_3a_4)$. Siten nämä kommutoivat eli pätee $y(a_2a_3a_4) = (a_2a_3a_4)y$. Tästä saadaan yhtälöä (5.37) käyttämällä, että

$$(a_2a_3a_4)^{-1}(a_1a_2)(a_3a_4)(a_2a_3a_4)(a_3a_4)(a_1a_2) \in G.$$

Tutkimalla eri alkoiden kuvautumista saadaan

$$(a_2a_3a_4)^{-1}(a_1a_2)(a_3a_4)(a_2a_3a_4)(a_3a_4)(a_1a_2) = (a_1a_3)(a_2a_4) \in G. \tag{5.38}$$

Koska $n \geq 5$, niin joukossa $\mathbb{A}_n$ on sellainen sykli $(a_1a_3a_5)$, jolle pätee $a_5 \neq a_1, a_2, a_3, a_4$. Koska $G \lhd \mathbb{A}_n$, niin yhtälön (5.38) mukaan

$$(a_1a_3a_5)^{-1}(a_1a_3)(a_2a_4)(a_1a_3a_5) \in G.$$

Tutkimalla eri alkioiden kuvautumista saadaan

$$(a_1a_3a_5)^{-1}(a_1a_3)(a_2a_4)(a_1a_3a_5) = (a_2a_4)(a_3a_5) \in G. \tag{5.39}$$

Tällöin yhtälöistä (5.39) ja (5.38) seuraa, että

$$(a_1a_3)(a_2a_4)(a_2a_4)(a_3a_5) \in G.$$

Kun eri alkoiden kuvautumisia tutkitaan, saadaan tulos

$$(a_1a_3)(a_2a_4)(a_2a_4)(a_3a_5) = (a_1a_3a_5) \in G.$$

Myös tässä tapauksessa löytyy siis aliryhmästä G 3-sykli. □

LEMMA 5.24. *Alternoiva ryhmä $\mathbb{A}_n$ on yksinkertainen, kun $n \geq 5$.*

TODISTUS. Olkoon $G \neq \{e\}$ ryhmän $\mathbb{A}_n, n \geq 5$, normaali aliryhmä. Lemman 5.23 mukaan siinä on vähintään yksi 3-sykli. Olkoon tämä $(a_1a_2a_3)$. Nyt $(a_3a_2a_s)$ on parillinen permutaatio mille tahansa $a_s \neq a_1, a_2, a_3$, joten $(a_3a_2a_s) \in \mathbb{A}_n$. Toisaalta $G \lhd \mathbb{A}_n$, joten tarkastelemalla eri alkioden kuvautumisia nähdään, että

$$(a_1a_sa_2) = (a_3a_2a_s)(a_1a_2a_3)(a_3a_2a_s)^{-1} \in G.$$

Tällöin myös

$$(a_1a_2a_s) = (a_1a_sa_2)^2 \in G \tag{5.40}$$

mille tahansa $a_s \neq a_1, a_2$. Koska lemman 5.8 mukaan kaikki tätä muotoa olevat permutaatiot virittävät ryhmän $\mathbb{A}_n$, niin kohta (5.40) riittää osoittamaan, että $\mathbb{A}_n \subset G$. Koska oletuksen mukaan $G \lhd \mathbb{A}_n$, niin täytyy olla $G = \mathbb{A}_n$. Tällöin ryhmän $\mathbb{A}_n$ ainoat normaalit aliryhmät ovat $\{e\}$ ja $\mathbb{A}_n$, joten se on yksinkertainen, kun $n \geq 5$. □

LAUSE 5.25. *Symmetrinen ryhmä $\mathbb{S}_n$ ei ole ratkeava, kun $n \geq 5$.*

TODISTUS. Tehdään vastaväite ja oletetaan, että $\mathbb{S}_n$ on ratkeava. Koska $\mathbb{A}_n \lhd \mathbb{S}_n$, niin lauseesta 5.18 seuraa, että myös $\mathbb{A}_n$ on ratkeava. Silloin lemman 5.24 nojalla se olisi yhtä aikaa ratkeava ja yksinkertainen, jolloin sen kertaluku olisi lauseen 5.22 perusteella alkuluku. Kuitenkin $\#\mathbb{A}_n = \frac{1}{2}n!$, joka ei voi olla alkuluku, kun $n \geq 5$. Ajaudutaan siis ristiriitaan, ja väite pätee. □

Lauseessa 5.25 on olennaista ehto $n \geq 5$. Esimerkin 5.15 mukaan ryhmä $\mathbb{S}_n$ on ratkeava, kun $n \leq 4$, joten luku 5 on siis symmetrisissä ryhmissä jollain tavalla erityisasemassa. Tulos antaa ensimmäisen vihjeen siitä, miksi toisen, kolmannen ja neljännen asteen yhtälöille on olemassa ratkaisukaava, mutta viidennen tai korkeamman asteen yhtälöille ei.

5.4. Cauchyn Lause

MÄÄRITELMÄ 5.26. Olkoon G ryhmä ja $a, b \in G$. Sanotaan, että alkiot a ja b ovat toistensa *konjugaatteja* eli ne *konjugoivat*, jos on olemassa $g \in G$, jolle $a = g^{-1}bg$. Konjugoinnista käytetään merkintää $a \sim b$. Joukkoa $C_a = \{g \in G : a \sim g\}$ sanotaan alkion a määräämäksi *konjugaattiluokaksi*.

LAUSE 5.27. *Konjugointirelaatio $\sim$ on ekvivalenssirelaatio.*

TODISTUS. Olkoot $a, b, c \in G$. Refleksiivisyys $a \sim a$ on selvää, sillä $a = e^{-1}ae$. Myös symmetrisyysehto pätee, sillä jos $a = g^{-1}bg$ jollain $g \in G$, niin

$$b = gag^{-1} = (g^{-1})^{-1}ag^{-1}.$$

Transitiivisuutta varten oletetaan, että $a \sim b$ ja $b \sim c$ eli $a = g^{-1}bg$ jollain $g \in G$ ja $b = h^{-1}ch$ jollain $h \in G$. Tällöin $ga = bg$ eli $hga = hbg$, josta edelleen saadaan

$$hga = hh^{-1}chg = chg. \tag{5.41}$$

Kertomalla yhtälö (5.41) vasemmalta termillä $(hg)^{-1}$ saadaan

$$a = (hg)^{-1}chg,$$

jolloin myös transitiivisuusehto on voimassa. Koska sekä refleksisyys, symmetrisyys että transitiivisuus ovat relaatiolle $\sim$ voimassa, se on ekvivalenssirelaatio. □

HUOMAUTUS 5.28. Koska konjugointi on ekvivalenssirelaatio, konjugaattiluokat ovat ekvivalenssiluokkia. Konjugaattiluokat muodostavat osituksen ryhmässä G. Ryhmä G voidaan siis ilmaista pistevieraiden konjugaattiluokkien yhdisteenä eli $G = \bigcup_{a \in G} C_a$, missä $C_a \cap C_b = \emptyset$, kun $C_a \neq C_b$.

MÄÄRITELMÄ 5.29. Olkoon G ryhmä ja olkoon $x \in G$. Alkion x keskittäjä joukossa G on $C_G(x) = \{g \in G : xg = gx\}$.

Alkion x keskittäjä $C_G(x)$ joukossa G on aina ryhmän G aliryhmä. Keskittäjä voidaan esittää myös muodossa $C_G(x) = \{g \in G : x = g^{-1}xg\}$, jolloin keskittäjällä on paljon yhteistä konjugaattiluokan määritelmän kanssa. Näille kahdelle saadaankin kätevä yhteys lauseesta 5.31 ja sen seurauksesta 5.32. Otetaan kuitenkin ensin käyttöön vielä yksi määritelmä.

MÄÄRITELMÄ 5.30. Olkoon G ryhmä ja H sen aliryhmä. Tällöin aliryhmän H *indeksi* on sen sivuluokkien lukumäärä.

LAUSE 5.31. *Olkoon G ryhmä ja $a \in G$. Tällöin konjugaattiluokan*

$$C_a = \{x \in G \,|\, x = gag^{-1}\}$$

kertaluku eli alkioiden lukumäärä on keskittäjän $C_G(a)$ indeksi.

TODISTUS. Konjugaattiluokan C_a kaikki alkiot voidaan esittää muodossa $g^{-1}ag$, missä $g \in G$. Olkoon $h \in G$ ja $g^{-1}ag = h^{-1}ah \in C_a$. Tällöin

$$hg^{-1}a = ahg^{-1},$$

joten ryhmän keskittäjän määritelmän 5.27 mukaan $hg^{-1} \in C_G(a)$. Tällöin h kuuluu alkion g määräämään oikeaan sivuluokkaan $C_G(a)g$, joten $C_a(a)h = C_a(a)g$.

Olkoon joukko A ryhmän $C_G(a)$ määräämä oikeiden sivuluokkien joukko. Nyt voidaan määritellä kuvaus $\phi : C_a \to A$ asettamalla $\phi(g^{-1}ag) = C_G(a)g$.

Osoitetaan ensiksi, että ϕ on injektio. Oletetaan, että $g^{-1}ag \neq h^{-1}ah$. Tällöin myös $hg^{-1}a \neq ahg^{-1}$, jolloin $hg^{-1} \notin C_G(a)$. Siten $C_G(a)g \neq C_G(a)h$. Kuvaus ϕ on myös surjektio, sillä jos $C_G(a)g \in A$ on mielivaltainen, niin $\phi(g^{-1}ag) = C_G(a)$. Siten ϕ on bijektio, jolloin joukoissa C_a ja A on yhtä monta alkiota. □

SEURAUS 5.32. *Äärellisen ryhmän G konjugaattiluokan C_a alkioiden lukumäärä jakaa ryhmän G kertaluvun.*

MÄÄRITELMÄ 5.33. Ryhmän G keskus $Z(G)$ on joukko

$$Z(G) = \{x \in G \,|\, xg = gx \text{ kaikille } g \in G\}.$$

Ryhmän G keskukselle pätee $Z(G) \neq \emptyset$, sillä aina neutraalialkio $e \in Z(G)$. Joukko $Z(G)$ on aina joukon G aliryhmä. Lisäksi ryhmä $Z(G)$ on määritelmänsä perusteella kommutatiivinen ja $Z(G)$ on ryhmän G normaali aliryhmä.

LEMMA 5.34. *Olkoon p alkuluku, joka jakaa äärellisen ja kommutatiivisen ryhmän G kertaluvun $\#G$. Tällöin ryhmässä G on kertalukua p oleva alkio.*

TODISTUS. Todistetaan lause induktiolla ryhmän kertaluvun $\#G$ suhteen. Olkoon m ja n luonnollisia lukuja, joille $m, n \geq 1$. Olkoot lisäksi p alkuku, jolle pätee $p \neq m$. Todistettava väite on siis seuraava: jos ryhmän G kertaluku $k = \#G$ on muotoa $k = p^n m$, niin ryhmässä G on kertalukua p oleva alkio.

Koska luku 1 ei ole muotoa $p^n m$, väite pätee, kun ryhmän G kertaluku on 1. Alkuaskel on siis otettu, joten muotoillaan seuraavaksi induktio-oletus. Olkoon ryhmän G kertaluku $k \geq 2$, m ja n luonnollisia lukuja, joille $m, n \geq 1$, sekä p alkuluku, jolle $p \neq m$. Kaikille $k' \in \mathbb{N}$, joille $k' < k$, pätee seuraava väite: jos ryhmän G kertaluku $k' = \#G$ on muotoa $k' = p^n m$, niin ryhmässä G on kertalukua p oleva alkio.

Todistetaan seuraavaksi induktio-oletuksen avulla, että väite pätee myös, kun ryhmän G kertaluku on k. Jos k ei ole muotoa $p^n m$, niin käy kuten tapauksessa $k = 1$ eli väite pätee. Oletetaan siis, että $k = p^n m$ joillekin luonnollisille luvuille $n, m \geq 1$.

Ryhmän G aidon aliryhmän kertaluku on aina pienempi kuin $\#G$. Koska lisäksi ryhmässä G on ainakin yksi aito aliryhmä $\{e\}$, voidaan valita ryhmän G aito aliryhmä $H \neq G$ siten, että sen kertaluku on maksimaalinen. Toisin sanoen

$$\text{jos } H \leq M \leq G, \text{ niin joko } M = H \text{ tai } M = G. \tag{5.42}$$

Nimetään $k' = \#H$. Koska H on ryhmän G aito aliryhmä, pätee $k' < k$. Siten induktio-oletus pätee ryhmälle H. Tällöin jos $k' = p^{n'} m'$ joillekin $n', m' \geq 1$, niin ryhmässä H on kertalukua p oleva alkio. Koska $H \subset G$, niin tämä alkio on myös ryhmässä G, joten todistettava väite pätee luvulle k. Oletetaan siis, että k' ei ole muotoa $p^{n'} m'$ eli p ei jaa lukua k'.

Koska H on ryhmän G aito aliryhmä voidaan valita alkio $x \in G \setminus H$. Tämä alkio virittää syklisen ryhmän $\langle x \rangle$. Koska G on kommutatiivinen, niin joukolle $H\langle x \rangle$ pätee $H\langle x \rangle \leq G$ ja $H \leq H\langle x \rangle$. Koska toisaalta $x \in H\langle x \rangle$, mutta $x \notin H$, niin ehdosta (5.42) saadaan

$$H\langle x \rangle = G.$$

Tästä puolestaan seuraa, että

$$\#H\langle x \rangle = \#G = p^n m. \tag{5.43}$$

Nyt lemmasta 5.16 saadaan

$$\frac{H\langle x \rangle}{\langle x \rangle} \cong \frac{H}{H \cap \langle x \rangle}.$$

Tästä seuraa, että

$$\#\frac{H\langle x \rangle}{\langle x \rangle} = \#\frac{H}{H \cap \langle x \rangle}$$

ja edelleen

$$\frac{\#H\langle x \rangle}{\#\langle x \rangle} = \frac{\#H}{\#(H \cap \langle x \rangle)}. \tag{5.44}$$

Yhtälö (5.44) saadaan muokattua muotoon

$$\#H\langle x \rangle \cdot \#(H \cap \langle x \rangle) = \#H \cdot \#\langle x \rangle. \tag{5.45}$$

Yhtälöistä (5.45) ja (5.43) sekä alkion k' määritelmästä seuraa, että

$$p^n m \cdot \#(H \cap \langle x \rangle) = k' \cdot \#\langle x \rangle \tag{5.46}$$

Koska oletettiin, että p ei jaa lukua k', niin yhtälön (5.46) perusteella alkuvun p täytyy jakaa luku $\#\langle x \rangle$. Tällöin $\#\langle x \rangle = p^q r$ joillekin $q, r \geq 1$. Tällöin pätee

$$x^{rp^q} = e \tag{5.47}$$

ja

$$x^l \neq e \text{ kaikille } l = 1, \ldots, x^{rp^q} - 1. \tag{5.48}$$

On siis löydettävä joukosta G alkio, jonka kertaluku on p. Tällainen alkio on $x^{rp^{q-1}}$. Ehdon (5.47) perusteella sille nimittäin pätee

$$\left(x^{rp^{q-1}}\right)^p = x^{rp^q} = e \tag{5.49}$$

ja lisäksi ehdon (5.48) perusteella pätee

$$\left(x^{rp^{q-1}}\right)^k = x^{krp^{q-1}} \neq e \text{ kaikilla } k = 1, \ldots p-1 \tag{5.50}$$

Koska $x^{rp^{q-1}} \in G$, niin yhtälöiden (5.49) ja (5.51) mukaan ryhmässä G on kertalukua p oleva alkio. Siten induktioperiaatteen nojalla väite pätee. □

Lause 5.35 (Cauchyn lause). *Olkoon p alkuluku, joka jakaa äärellisen ryhmän G kertaluvun. Tällöin ryhmässä G on kertalukua p oleva alkio.*

Todistus. Todistetaan väite induktiolla ryhmän kertaluvun suhteen. Muotoillaan väite uudelleen, kuten lemmassa 5.34. Olkoot $m, n \in \mathbb{N}$, joille pätee $m, n \geq 1$ sekä olkoon lisäksi p alkuluku, joka ei jaa lukua m. Jos ryhmän kertaluku $k = \#G$ on muotoa $k = mp^n$, niin ryhmässä G on kertalukua p oleva alkio.

Jos $k = 1$, niin väite pätee, koska k ei ole muotoa mp^n. Oletetaan siis, että väite pätee kaikilla $k' < k$, kun $k \geq 2$.

Koska ryhmän G konjugaattiluokat muodostavat osituksen, voidaan ryhmä ilmaista muodossa $G = C_{a_1} \cup C_{a_2} \cup \ldots \cup C_{a_r}$, missä $a_1, \ldots, a_r \in G$. Näistä täsmälleen yhden luokan muodostaa pelkkä neutraalialkio. Olkoon tämä luokka C_{a_1}. Tällöin saadaan

$$\#G = k = mp^n = 1 + \sum_{i=2}^{r} \#C_{a_i}. \tag{5.51}$$

Oletetaan seuraavaksi, että jollekin konjugaattiluokalle C_{a_j} pätevät ehdot

$$\#C_{a_j} \geq 2 \text{ ja} \tag{5.52}$$

$$p \text{ ei jaa lukua } \#C_{a_j}. \tag{5.53}$$

Tarkastellaan sitten tähän luokkaan kuuluvan alkion $a_j \in G$ keskittäjää $C_G(a_j)$. Lauseen 5.31 nojalla konjugaattiluokan C_{a_j} kertaluvulle pätee

$$\#C_{a_j} = \frac{\#G}{\#C_G(a_j)}. \tag{5.54}$$

Yhtälöstä (5.54) saadaan keskittäjän kertaluvuksi

$$\#C_G(a_j) = \frac{mp^n}{\#C_{a_j}}. \tag{5.55}$$

Nyt voidaan asettaa $k' = \#C_G(a_j)$, jolloin ehdon (5.52) nojalla $k' < k$ eli induktio-oletus pätee luvulle k'. Koska k' on yhtälön (5.55) ja ehdon (5.53) mukaan muotoa $k' = m'p^n$, missä $m', n \geq 1$ ja p on alkuluku, niin induktio-oletuksesta seuraa, että ryhmässä $C_G(a_j)$ on kertalukua p oleva alkio. Koska $C_G(a_j) \leq G$, niin myös ryhmässä G on kertalukua p oleva alkio.

Väite siis pätee oletuksien (5.52) ja (5.53) ollessa voimassa. Oletetaan siis seuraavaksi, etteivät ne ole voimassa. Toisin sanoen kaikilla $i = 2, \ldots, r$ pätee

$$\#C_{a_i} = 1 \text{ tai} \tag{5.56}$$

$$p \text{ jakaa luvun } \#C_{a_i}. \tag{5.57}$$

Olkoon $Z(G)$ ryhmän G keskus. Osoitetaan seuraavaksi, että sille pätee

$$Z(G) = \{e\} \cup \{a_i : C_{a_i} = \{a_i\}, i = 2, \ldots, r\}. \tag{5.58}$$

Todistetaan ensiksi, että pätee $Z(G) \subset \{e\} \cup \{a_i : C_{a_i} = \{a_i\}, i = 2, \ldots, r\}$. Olkoon $z \in Z(G)$. Koska $G = C_{a_1} \cup C_{a_2} \cup \ldots \cup C_{a_r}$, niin joko $z \in C_{a_1} = \{e\}$ tai

$$z \in C_{a_2} \cup \ldots \cup C_{a_r}.$$

Jos $z = e$, niin väite (5.58) pätee, joten oletetaan, että $z \in C_{a_2} \cup \ldots \cup C_{a_r}$. Tämä tarkoittaa, että $z \in C_{a_j}$ jollekin $j = 2, \ldots, r$. Täytyy siis osoittaa, että $C_{a_j} = \{a_j\}$.

Koska $z \in C_{a_j}$, niin konjugaattiluokan määritelmän perusteella $g^{-1}zg = a_j$ jollekin $g \in G$. Koska $z \in Z(G)$, niin $gz = zg$, jolloin $g^{-1}zg = z$. Tästä seuraa, että $z = a_j$. Täytyy vielä osoittaa, ettei joukossa C_{a_j} voi olla muita alkioita kuin $z = a_j$. Olkoon $z' \in C_{a_j}$. Tällöin $z' = h^{-1}a_jh$ jollekin $h \in G$. Koska $a_j = z \in Z(G)$, niin

$$z' = h^{-1}a_jh = h^{-1}ha_j = a_j.$$

Näin ollen joukon C_{a_j} ainoa alkio on a_j. Tällöin

$$Z(G) \subset \{e\} \cup \{a_i : C_{a_i} = \{a_i\}, i = 2, \ldots, r\}.$$

Täytyy kuitenkin vielä todistaa, että

$$\{e\} \cup \{a_i : C_{a_i} = \{a_i\}, i = 2, \ldots, r\} \subset Z(G). \tag{5.59}$$

Olkoon nyt puolestaan $z \in \{e\} \cup \{a_i : C_{a_i} = \{a_i\}, i = 2, \ldots, r\}$. Jos $z = e$, niin $z \in Z(G)$. Oletetaan siis, että $z = a_j$ jollekin sellaiselle $j = 2, \ldots r$, jolle $C_{a_j} = \{a_j\}$.

Koska konjugaattiluokan määritelmän perusteella $g^{-1}a_jg \in C_{a_j}$ kaikilla $g \in G$ ja $C_{a_j} = \{a_j\}$, niin $g^{-1}a_jg = a_j$ kaikille $g \in G$. Koska tästä seuraa, että $a_jg = ga_j$ kaikille $g \in G$, niin $a_j = z \in Z(G)$. Tällöin väite (5.59) ja siten myös väite (5.58) on todistettu.

Nyt yhtälöstä (5.58) seuraa, että

$$\#Z(G) = \#\{a_i : C_{a_i} = \{a_i\}, i = 2, \ldots, r\} + 1. \tag{5.60}$$

Otetaan käyttöön merkintä $M = \{a_i : C_{a_i} = \{a_i\}, i = 1, \ldots, r\}$. Joukolle M saadaan kertaluvuksi

$$\#M = \sum_{a_i \in M} 1 = \sum_{a_i \in M} \#C_{a_i}. \tag{5.61}$$

Joukon $Z(G)$ kertaluku taas voidaan ilmaista yhtälön (5.60) avulla seuraavasti:

$$\#Z(G) = 1 + \#M = 1 + \sum_{a_i \in M} \#C_{a_i}. \tag{5.62}$$

Muokkaamalla ensin yhtälöä (5.51) ja käyttämällä sitten kaksi kertaa yhtälöä (5.62) saadaan ryhmän G kertaluvuksi

$$\begin{aligned} \#G = 1 + \sum_{i=1}^{r} \#C_{a_i} &= 1 + \sum_{a_i \in M} \#C_{a_i} + \sum_{a_i \in \{a_1,\ldots,a_r\}\setminus M} \#C_{a_i} \\ &= 1 + \#M + \sum_{a_i \in \{a_1,\ldots,a_r\}\setminus M} \#C_{a_i} \\ &= \#Z(G) + \sum_{a_i \in \{a_1,\ldots,a_r\}\setminus M} \#C_{a_i} \end{aligned} \tag{5.63}$$

Yhdistämällä yhtälöt (5.51) ja (5.63) puolestaan saadaan

$$mp^n = \#Z(G) + \sum_{a_i \in \{a_1,\ldots,a_r\}\setminus M} \#C_{a_i}. \tag{5.64}$$

Koska indeksijoukosta

$$M' = \{a_1, \ldots, a_r\}\setminus M$$

puuttuvat ehdon (5.56) mukaiset alkiot, täytyy ehdon (5.57) ja yhtälön (5.64) mukaan alkuvun p jakaa luku $\#C_{a_i}$ kaikilla $a_i \in M'$. Tällöin yhtälön (5.64) nojalla täytyy alkuluvun p jakaa myös luku $\#Z(G)$. Siten $k' = \#Z(G) = m'p^{n'}$ joillekin $n' \geq 1$ ja $m' \geq 1$, jolle p ei jaa lukua m.

Keskus $Z(G)$ on ryhmän G aliryhmä. Jos $Z(G) = G$, niin ryhmä G on kommutatiivinen. Tällöin lemman 5.34 nojalla ryhmässä G on alkio, jonka kertaluku on p. Jos taas $Z(G) \neq G$, niin täytyy olla $k' < k$. Tällöin voidaan käyttää induktio-oletusta: koska p jakaa luvun $\#Z(G)$, niin ryhmässä $Z(G)$ on kertalukua p oleva alkio. Tämä alkio kuuluu myös ryhmään G, joten väite on todistettu. □

LUKU 6

Viidennen asteen yhtälön ratkaisukaava

6.1. Juurilaajennukset

Ennen kuin voidaan todistaa, ettei viidennen asteen yhtälölle ole olemassa ratkaisukaavaa, täytyy selvittää, mitä ratkaisukaavalla oikeastaan tarkoitetaan. Sovitaan, että ratkaisukaava on lauseke, jossa voidaan käyttää tavallisia rationaalilukujen laskutoimituksia sekä lisäksi ottaa kokonaislukujuuria. Näitä toimituksia voidaan tehdä vain äärellisen monta kertaa. Rationaalilukujen laskutoimitukset eivät tuota ongelmia, mutta jos rationaaliluvusta otetaan kokonaislukujuuri, ei saada aina rationaalilukua. Tällöin on siis tehtävä kuntalaajennus suurempaan kuntaan. Lisäksi suuremman kunnan uusien alkioiden ei tarvitse välttämättä olla rationaalilukujen juuria, vaan ne voivat olla juuria myös irrationaaliluvuista, joita ratkaisukaava on aiemmin antanut. Tämä johtaa määritelmään 6.1 juurilaajennuksesta, jonka avulla voidaan määritellä, milloin polynomilla on ratkaisukaava eli milloin se on ratkaistavissa juurin.

MÄÄRITELMÄ 6.1. Olkoot $K \subset \mathbb{C}$ ja $L \subset \mathbb{C}$ kuntia. Äärellisasteinen kuntalaajennus $K \hookrightarrow L$ on *juurilaajennus*, jos $L = K(\alpha_1, \ldots, \alpha_m)$ ja jokaiselle $j = 1, \ldots, m$ on olemassa sellainen positiivinen kokonaisluku n_j, että

$$\alpha_j^{n_j} \in K(\alpha_1, \ldots, \alpha_{j-1}).$$

Sanotaan, että alkiot α_j muodostavat juurilaajennuksen $K \hookrightarrow L$ *juurijonon* ja että alkion α_j *juuriaste* on n_j.

HUOMAUTUS 6.2. Koska juurilaajennus on $K \hookrightarrow L$ on määritelmänsä perusteella äärellisasteinen, se on lauseen 2.25 nojalla aina algebrallinen kunnan K suhteen.

HUOMAUTUS 6.3. Jos alkion juurijonon alkion $\alpha_j, j \geq 1$, juuriaste on $n_j = 1$, niin $\alpha_j \in K(\alpha_1, \ldots, \alpha_{j-1})$. Tällöin alkio α_j voidaan poistaa turhana alkiona. Voidaan siis olettaa, että alkion α_j juuriasteelle pätee $n_j > 1$, kun $j \geq 1$.

Lisäksi juurijonosta voidaan poistaa ne alkiot, joiden juuriaste ei ole alkuluku. Tällöin juurijonoa täytyy kuitenkin pidentää. Jos nimittäin alkion α_j juuriaste n_j ei ole alkuluku, niin $n_j = p_1 p_2 \ldots p_k$, missä luvut $p_1, \ldots, p_k$ ovat alkulukuja. Tällöin voidaan määritellä juurijonoon uudet alkiot $\beta_1, \ldots, \beta_{k-1}$ asettamalla $\beta_i = \alpha_j^{p_1 \cdots p_i}$ kaikilla $i = 1, \ldots, k-1$. Kun alkio α_j korvataan jonolla $\beta_{k-1} \ldots \beta_1$, saadaan juurijono: ensinnäkin

$$\beta_{k-1}^{p_k} = \alpha_j^{p_1 \cdots p_k} = \alpha_j^{n_j} \in K(\alpha_1, \ldots, \alpha_{k-1}),$$

toiseksi

$$\beta_i^{p_{i+1}} = \beta_{i+1} \in K(\alpha_1, \ldots, \alpha_{j-1}, \beta_{k-1}, \ldots, \beta_{i+1})$$

ja kolmanneksi

$$\alpha_j^{p_1} = \beta_1 \in K(\alpha_1, \ldots, \alpha_{j-1}, \beta_{k-1}, \ldots, \beta_1).$$

MÄÄRITELMÄ 6.4. Olkoon p polynomi renkaassa $K[x], K \subset \mathbb{C}$ ja olkoon Σ polynomin p hajotuskunta kunnan K suhteen. Polynomi p on *ratkaistavissa juurin*, jos on olemassa sellainen kunta M, jolle $\Sigma \subset M$ ja kuntalaajennus $K \hookrightarrow M$ on juurilaajennus.

Nyt kun juurin ratkeavuus on määritelty, voidaan perehtyä tarkemmin juurilaajennusten ominaisuuksiin. Tavoitteena on todistaa lause 6.9 eli jos kuntalaajennus $K \hookrightarrow M$ on juurilaajennus ja $L \subset M$, niin Galois'n ryhmä $\Gamma(K, L)$ on ratkeava. Juurilaajennuksen ja juurin ratkeavuuden välillä on selvä yhteys, joten lause 6.9 selvittää, miksi luvussa 5 eräs ryhmän ominaisuus nimettiin juuri ratkeavuudeksi.

LEMMA 6.5. *Olkoon $K \hookrightarrow L$ juurilaajennus kunnassa $\mathbb{C}$. Jos M on kuntalaajennuksen $K \hookrightarrow L$ normaalisulkeuma, niin kuntalaajennus $K \hookrightarrow M$ on myös juurilaajennus.*

TODISTUS. Koska $K \hookrightarrow L$ on juurilaajennus, niin $L = K(\alpha_1, \ldots, \alpha_r)$, missä $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ jollain $n_i \in \mathbb{N}$. Huomautuksen 6.2 mukaan $K \hookrightarrow L$ on algebrallinen. Alkiolla α_i on siis minimaalipolynomi m_i. Määritellään polynomi

$$m = m_1 m_2 \cdots m_r \in K[x].$$

Nyt $\alpha_i \in L \subset M$ ja α_i on polynomin m nollakohta. Koska kuntalaajennus $K \hookrightarrow M$ on normaali ja jokaisella polynomilla m_i on vähintään yksi nollakohta kunnassa M, niin jokainen m_i hajoaa kunnassa M. Siten soveltamalla lemmaa 3.4 nähdään, että kunta M sisältää kaikki polynomin m nollakohdat. Olkoot nämä $\beta_1, \ldots, \beta_s \in M$. Polynomin m hajotuskunta on tällöin $K(\beta_1, \ldots, \beta_s)$. Lauseesta 3.8 seuraa, että kuntalaajennus $K \hookrightarrow K(\beta_1, \ldots, \beta_s)$ on normaali. Koska kuitenkin

$$K(\alpha_1, \ldots, \alpha_r) \subset K(\beta_1, \ldots, \beta_s) \subset M$$

ja M on kuntalaajennuksen $K \hookrightarrow K(\alpha_1, \ldots, \alpha_r)$ normaalisulkeuma, niin täytyy olla

$$K(\beta_1, \ldots, \beta_s) = M. \tag{6.1}$$

Alkio β_j on polynomin m nollakohta kaikilla $j = 1, \ldots, s$, joten se on jonkin polynomin $m_i, i = 1, \ldots, r$, nollakohta. Toisaalta myös α_i on polynomin m_i nollakohta, ja koska m_i on jaoton, niin se on minimaalipolynomi sekä alkiolle β_j että α_i. Tällöin voidaan käyttää lausetta 2.19, jonka mukaan on olemassa isomorfismi $f : K(\alpha_i) \to K(\beta_j)$. Lisäksi isomorfismi f voidaan valita siten, että $f(\alpha_i) = \beta_j$. Koska kuntalaajennus $K \hookrightarrow M$ on äärellisasteinen ja normaali, niin lauseen 4.13 nojalla f laajenee K-automorfismiksi $\phi : M \to M$. Kuvaukselle ϕ pätee edelleen

$$\phi(\alpha_i) = \beta_j \tag{6.2}$$

jollekin $i = 1, \ldots, r$. Koska $K \hookrightarrow L$ on juurilaajennus, niin alkiolle α_i on olemassa kunnasta K alkava juurijono $\gamma_1, \ldots, \gamma_k = \alpha_i$. Koska ϕ on K-automorfismi $M \to M$, niin $\phi(\gamma_1), \ldots, \phi(\gamma_k) = \phi(\alpha_i)$ on kunnasta K alkava juurijono. Tällöin yhtälöstä (6.2) seuraa, että $K \hookrightarrow M$ on juurilaajennus. □

LEMMA 6.6. *Olkoon $K \subset \mathbb{C}$ kunta, p alkuluku ja $q = x^p - 1$ polynomi renkaassa $K[x]$. Olkoon lisäksi Σ polynomin q hajotuskunta. Tällöin Galois'n ryhmä $\Gamma(K, \Sigma)$ on kommutatiivinen.*

TODISTUS. Polynomin q nollakohdat kunnassa $\mathbb{C}$ ovat muotoa $e^{i\frac{2\pi}{p}k}$, missä $k = 0, 1, \ldots, p-1$. Merkitään $\alpha_1 = e^{i\frac{2\pi}{p}}$. Tällöin pätee

$$\Sigma = K(\alpha_1).$$

Tarkastellaan seuraavaksi Galois'n ryhmää $\Gamma(K, \Sigma)$. Jos kuvaukset $f, g \in \Gamma(K, \Sigma)$ ja $f(\alpha_1) = g(\alpha_1)$, niin $f = g$, sillä f ja g ovat kunnan Σ K-automorfismeja. Toisin sanoen arvo $f(\alpha_1)$ määrittelee koko kuvauksen f.

Jos nyt sijoitetaan arvo $f(\alpha_1)$ polynomiin q, saadaan

$$f(\alpha_1)^p - 1 = f(\alpha_1^p) - f(1) = f(\alpha_1^p - 1) = 0,$$

jolloin myös $f(\alpha_1) \in \{\alpha_1, \ldots, \alpha_p\}$. Koska α_1 on ryhmän $\{\alpha_1, \ldots, \alpha_p\}$ virittäjä, niin

$$f(\alpha_1) = \alpha_1^n, \tag{6.3}$$

jollekin $n = 0, \ldots, p-1$. Jos myös $g \in \Gamma(K, \Sigma)$, niin vastaavasti

$$g(\alpha_1) = \alpha_1^m \tag{6.4}$$

jollain $m \in 0, \ldots, p$. Kun tarkastellaan kuvausta $f \circ g(\alpha_1)$, saadaan

$$f \circ g(\alpha_1) = f(\alpha_1^m) \tag{6.5}$$

ehdon (6.4) perusteella. Käyttämällä ehtoa (6.3) saadaan

$$f(\alpha_1^m) = f(\alpha_1)^m = \alpha_1^{nm}. \tag{6.6}$$

Ehtojen (6.4) ja (6.3) perusteella pätee vielä, että

$$\alpha_1^{nm} = \alpha_1^{mn} = g(\alpha_1)^n = g(\alpha_1^n) = g \circ f(\alpha_1). \tag{6.7}$$

Yhdistämällä yhtälöt (6.5), (6.6) ja (6.7) saadaan

$$f \circ g(\alpha_1) = g \circ f(\alpha_1). \tag{6.8}$$

Kuvaukset $f \circ g$ ja $g \circ f$ määräytyvät kuitenkin täysin arvoista $f(\alpha_1)$ ja $g(\alpha_1)$, joten yhtälö (6.8) riittää kommutatiivisuuden osoittamiseksi. □

LEMMA 6.7. *Olkoon $K \subset \mathbb{C}$ sellainen kunta, että polynomi $p = x^n - 1$, $n \in \mathbb{N}$, hajoaa kunnassa K. Olkoon $a \in K$ ja L hajotuskunta polynomille $q = x^n - a \in K[x]$. Tällöin Galois'n ryhmä $\Gamma(K, L)$ on kommutatiivinen.*

TODISTUS. Olkoot $\alpha_1, \ldots, \alpha_n$ polynomin p nollakohdat. Koska p hajoaa kunnassa K, niin $\{\alpha_1, \ldots, \alpha_n\} \subset K$. Olkoot $\beta_1, \ldots, \beta_n$ polynomin q nollakohdat. Koska L on polynomin q hajotuskunta, niin

$$L = K(\beta_1, \ldots, \beta_n). \tag{6.9}$$

Jos $a = 0$, niin polynomin q kaikki nollakohdat ovat nollia, jolloin $L = K$. Triviaalin kuntalaajennuksen $K \hookrightarrow K$ Galois'n ryhmä on kommutatiivinen, joten väite pätee. Oletetaan siis, että $a \neq 0$, jolloin $\beta_i \neq 0$ kaikille $i = 1, \ldots, n$. Tällöin koska L on kunta, niin on olemassa $\beta_1^{-1} \in L$, jolloin saadaan

$$(\beta_j \beta_1^{-1})^n - 1 = \beta_j^n \beta_1^{-n} + \beta_1^{-n} a - \beta_1^{-n} a - \beta_1^{-n} \beta_1^n = \beta_1^{-n}(\beta_j^n + a) - \beta_1^{-n}(\beta_1^n - a) = 0.$$

Tällöin $\beta_j\beta_1^{-1}$ on polynomin p nollakohta eli $\beta_j\beta_1^{-1} \in \{\alpha_1, \ldots, \alpha_n\}$. Tästä seuraa, että kaikilla $j = 1, \ldots, n$ pätee

$$\beta_j \in \{\alpha_1\beta_1, \alpha_2\beta_1, \ldots, \alpha_n\beta_1\} \subset K(\beta_1), \tag{6.10}$$

jolloin yhtälön (6.9) ja ehdon $\{\alpha_1, \ldots, \alpha_n\} \subset K$ nojalla

$$L = K(\beta_1). \tag{6.11}$$

Tarkastellaan seuraavaksi Galois'n ryhmää $\Gamma(K, L)$. Jos $f \in \Gamma(K, L)$, niin

$$f(\beta_1)^n - a = f(\beta_1^n) - f(a) = f(\beta_1^n - a) = f(0) = 0,$$

jolloin $f(\beta_1)$ on polynomin q nollakohta. Siten $f(\beta_1) \in \{\beta_1, \ldots, \beta_n\}$. Käyttämällä ehtoa (6.10) saadaan

$$f(\beta_1) \in \{\alpha_1\beta_1, \ldots, \alpha_n\beta_1\}. \tag{6.12}$$

Olkoot $f, g \in \Gamma(K, L)$. Yhtälön (6.11) mukaan $L = K(\beta_1)$, joten kuvaukset f ja g määräytyvät täysin arvoista $f(\beta_1)$ ja $g(\beta_1)$, kuten lemman 6.6 todistuksessa. Siten riittää osoittaa, että

$$f \circ g(\beta_1) = g \circ f(\beta_1). \tag{6.13}$$

Yhtälön (6.12) perusteella joillain $k, m = 1, \ldots, n$ pätee

$$f \circ g(\beta_1) = f(\alpha_k\beta_1) = f(\alpha_k)f(\beta_1) = \alpha_k f(\beta_1) = \alpha_k\alpha_m\beta_1. \tag{6.14}$$

Vastaavasti

$$g \circ f(\beta_1) = g(\alpha_m\beta_1) = g(\alpha_m)g(\beta_1) = \alpha_m\alpha_k\beta_1 = \alpha_k\alpha_m\beta_1, \tag{6.15}$$

Siten väite (6.13) pätee. Ryhmä $\Gamma(K, L)$ on siis kommutatiivinen. □

LAUSE 6.8. *Olkoon $K \subset \mathbb{C}$ kunta ja $K \hookrightarrow L$ normaali juurilaajennus. Tällöin Galois'n ryhmä $\Gamma(K, L)$ on ratkeava.*

TODISTUS. Juurilaajennuksen määritelmän 6.1 ja huomautuksen 6.3 perusteella on olemassa alkiot $\alpha_1, \ldots, \alpha_m$, joille pätee

$$\alpha_1^{p_1} \in K, \tag{6.16}$$

$$\alpha_j^{p_j} \in K(\alpha_1, \ldots, \alpha_{j-1}) \tag{6.17}$$

ja

$$L = K(\alpha_1, \ldots, \alpha_m) \tag{6.18}$$

joillain alkuluvuilla p_1 ja p_j sekä kaikilla $j = 1, \ldots, m$. Lisäksi oletetaan, että kuntalaajennus $K \hookrightarrow L$ on normaali. Todistetaan väite induktiolla luvun m suhteen. Induktio-oletuksen mukaan kaikille normaaleille kuntalaajennuksille $K' \hookrightarrow L'$, joissa $L' = K'(\alpha_1, \ldots, \alpha_{m-1})$, ja joille pätee ehdot (6.16) ja (6.17), Galois'n ryhmä $\Gamma(K, L')$ on ratkeava. Induktioväite on puolestaan seuraava: Jos $K \hookrightarrow L$, missä $L = K(\alpha_1, \ldots, \alpha_m)$, on normaali ja toteuttaa ehdot (6.16) ja (6.17), niin Galois'n ryhmä $\Gamma(K, K(\alpha_1, \ldots, \alpha_m))$ on ratkeava. Koska alkuaskel eli tapaus $m = 1$ on tässä tapauksessa hyvin samankaltainen tapaus kuin induktioaskelkin, otetaan alkuaskel poikkeuksellisesti yhtäaikaisesti induktioaskeleen kanssa.

Tarkastellaan ensiksi tapausta $\alpha_1 \in K$. Tällöin $K(\alpha_1) = K$ ja

$$K(\alpha_1, \ldots, \alpha_m) = K(\alpha_2, \ldots, \alpha_m).$$

Lisäksi $K \hookrightarrow K(\alpha_2, \ldots, \alpha_m)$ on oletuksen perusteella normaali, joten induktio-oletuksen nojalla väite pätee.

Oletetaan seuraavaksi, että $\alpha_1 \notin K$. Juurilaajennukset ovat huomautuksen 6.2 nojalla aina algeberallisia kuntalaajennuksia, joten alkiolla α_1 on minimaalipolynomi $m \in K[x]$. Koska $K \subset \mathbb{C}$ ja $m \in K[x]$ on jaoton, niin lauseen 3.14 nojalla polynomin m nollakohdat ovat erilliset. Jos olisi $\partial m = 1$, niin m olisi muotoa $ax + b$, missä $a, b \in K$. Koska α_1 on polynomin nollakohta, niin $a\alpha_1 - b = 0$. Koska kuitenkin $\alpha_1 \notin K$, niin tällaisia a ja b ei ole olemassa. Siten $\partial m \geq 2$. Koska polynomin m nollakohdat ovat erilliset, niin sillä on myös toinen nollakohta

$$\beta \neq \alpha_1. \tag{6.19}$$

Lisäksi $\beta \in L$, sillä m on jaoton polynomi ja $K \hookrightarrow L$ on normaali kuntalaajennus. Koska $\partial m \geq 2$ ja m on minimaalipolynomina jaoton, täytyy sillä olla nollasta eroava vakiotermi. Tällöin 0 ei voi olla polynomin m nollakohta, joten $\beta \neq 0$. Täten on olemassa $\beta^{-1} \in L$. Merkitään

$$\gamma = \beta^{-1}\alpha_1 \in L. \tag{6.20}$$

Seuraavaksi halutaan osoittaa, että ryhmä $\Gamma(K, L)$ on kommutatiivinen. Tähän tarvitaan lemmaa 6.6. Tarkastellaan siis polynomia $q(x) = x^{p_1} - 1 \in K[x]$. Jotta lemmaa 6.6 voitaisiin soveltaa, täytyy ensin osoittaa, että q hajoaa kunnassa L. Polynomi q ei ole jaoton, joten tieto kuntalaajennuksen $K \hookrightarrow L$ normaalisuudesta ei suoraan johda polynomin q hajoamiseen kunnassa L.

Olkoon Σ polynomin q hajotuskunta. Tällöin

$$q = (x - \delta_1)(x - \delta_2) \cdots (x - \delta_{p_1}),$$

missä $\delta_i \in \Sigma, i = 1, \ldots, p_1$. Polynomilla q on formaali derivaatta $Dq = p_1 x^{p_1 - 1}$. Koska p_1 on alkuluku, niin $p_1 \geq 2$. Siten $x^{p_1 - 1}$ ei voi olla polynomin $x^{p_1} - 1$ tekijä, jolloin polynomeilla q ja Dq ei ole yhteisiä tekijöitä. Tällöin lemman 3.13 mukaan polynomin q nollakohdat ovat erilliset eli

$$\#\{\delta_1, \ldots, \delta_{p_1}\} = p_1.$$

Samoin kuin lemman 6.7 todistuksessa nähdään, että $\{\delta_1, \ldots, \delta_{p_1}\}$ on ryhmä. Koska sen kertaluku p_1 on alkuluku, niin Lagrangen lauseen nojalla (ks. esimerkiksi [**4**, Section 14]) se on syklinen ryhmä ja sen virittää mikä tahansa $\delta_i \neq 1$.

Tarkastellaan seuraavaksi polynomia $r(x) = x^{p_1} - \alpha_1^{p_1}$. Sen eräs nollakohta on selvästi α_1, joka on myös minimaalipolynominsa m nollakohta. Siten lemman 2.16 nojalla m jakaa polynomin r. Tästä seuraa, että koska β on polynomin m nollakohta, niin β on myös polynomin r nollakohta. Silloin

$$r(\beta) = \beta^{p_1} - \alpha_1^{p_1} = 0,$$

jolloin

$$\beta^{p_1} = \alpha^{p_1}. \tag{6.21}$$

Käyttämällä alkion γ määritelmää (6.20) sekä yhtälöä (6.21) saadaan

$$q(\gamma) = \gamma^{p_1} - 1 = \beta^{p_1}\alpha^{-p_1} - 1 = \alpha^{p_1 - p_1} - 1 = 0.$$

Näin ollen γ on polynomin q nollakohta. Tämä tarkoittaa, että $\gamma = \delta_i$ jollain $i = 1, \ldots, p_1$. Koska yhtälöiden (6.19) ja (6.20) perusteella $\delta_i = \gamma \neq 1$, niin γ on ryhmän $\{\delta_1, \ldots, \delta_{p_1}\}$ virittäjä eli $\langle\gamma\rangle = \{\delta_1 \ldots, \delta_{p_1}\}$. Koska $\gamma \in L$, niin $\langle\gamma\rangle \subset L$ eli $\{\delta_1, \ldots, \delta_{p_1}\} \subset L$. Tällöin polynomin q hajotuskunta

$$\Sigma = K(\delta_1, \ldots, \delta_{p_1}) \subset L.$$

Lauseen 3.8 mukaan $K \hookrightarrow \Sigma$ on äärellisasteinen ja normaali. Nyt voidaan siis käyttää lemmaa 6.6, jonka mukaan $\Gamma(K, \Sigma)$ on kommutatiivinen ryhmä. Viidennen Galois'n lauseen 4.28 mukaan

$$\Gamma(K, \Sigma) \cong \frac{\Gamma(K, L)}{\Gamma(\Sigma, L)}. \tag{6.22}$$

Koska kommutatiiviset ryhmät ovat ratkeavia, niin $\Gamma(K, \Sigma)$ on ratkeava. Tällöin lauseen 5.20 mukaan $\Gamma(K, L)$ on ratkeava, jos $\Gamma(\Sigma, L)$ on ratkeava.

Osoitetaan seuraavaksi, että $\Gamma(\Sigma, \Sigma(\alpha_1))$ on kommutatiivinen ja siten ratkeava ryhmä. Tämä voidaan tehdä käyttämällä lemmaa 6.7, mutta ensiksi täytyy osoittaa, että $\Sigma(\alpha_1)$ on polynomin $s(x) = x^{p_1} - \alpha_1^{p_1} \in \Sigma[x]$ hajotuskunta.

Polynomilla s on korkeintaan p_1 erillistä nollakohtaa, sillä $\partial s = p_1$. Koska δ_i on polynomin q nollakohta, niin $\delta_i^{p_1} = 1$ kaikilla $i = 1, \ldots, p_1$. Tällöin polynomille s pätee

$$s(\delta_i\alpha_1) = \delta_i^{p_1}\alpha_1^{p_1} - \alpha_1^{p_1} = \alpha_1^{p_1} - \alpha_1^{p_1} = 0,$$

jolloin $\delta_i\alpha_1$ on polynomin s nollakohta. Koska $\alpha_1 \notin K$, niin $\alpha_1 \neq 0 \in K$, ja koska lisäksi alkiot δ_i ovat toisistaan erilliset, niin $\#\{\delta_1\alpha_1, \ldots, \delta_{p_1}\alpha_1\} = p_1$. Nämä ovat kaikki polynomin s nollakohtia, ja koska niitä ei voi olla enempää, nollakohtia on tasan p_1 kappaletta. Tällöin polynomin s hajotuskunta on $\Sigma(\delta_1\alpha_1, \ldots, \delta_{p_1}\alpha_1)$. Koska $\delta_i \in \Sigma$, niin $\Sigma(\delta_1\alpha_1, \ldots, \delta_{p_1}\alpha_1) = \Sigma(\alpha_1)$.

Nyt voidaan siis käyttää lemmaa 6.7, jonka mukaan $\Gamma(\Sigma, \Sigma(\alpha_1))$ on kommutatiivinen. Koska $\Sigma \hookrightarrow \Sigma(\alpha_1)$ on äärellisasteinen ja normaali, voidaan käyttää jälleen viidettä Galois'n lausetta. Sen mukaan

$$\Gamma(\Sigma, \Sigma(\alpha_1)) \cong \frac{\Gamma(\Sigma, L)}{\Gamma(\Sigma(\alpha_1), L)}. \tag{6.23}$$

Koska $\Gamma(\Sigma, \Sigma(\alpha_1)$ on kommutatiivisena ryhmänä ratkeava, niin lauseen 5.20 nojalla riittää osoittaa, että $\Gamma(\Sigma(\alpha_1), L)$ on ratkeava.

Nyt $L = K(\alpha_1, \ldots, \alpha_m) \subset \Sigma(\alpha_1, \ldots, \alpha_m)$, sillä $K \subset \Sigma$. Toisaalta $\Sigma(\alpha_1, \ldots, \alpha_m) \subset L$, sillä $\Sigma \subset L$ ja $\{\alpha_1, \ldots, \alpha_m\} \subset L$. Tällöin

$$L = \Sigma(\alpha_1, \ldots, \alpha_m). \tag{6.24}$$

Tapauksessa $\alpha_1 \notin K$ alkuaskel on vielä ottamatta, joten otetaan se nyt. Jos $m = 1$, niin yhtälön (6.24) perusteella $L = \Sigma(\alpha_1)$, jolloin $\Gamma(\Sigma(\alpha_1), \Sigma(\alpha_1))$ on triviaalina Galois'n ryhmänä yksialkioinen ja siten ratkeava. Tarkastellaan seuraavaksi tapausta $m \geq 2$. Tällöin

$$\Sigma(\alpha_1) \hookrightarrow \Sigma(\alpha_1, \ldots, \alpha_m) = \Sigma(\alpha_1) \hookrightarrow \Sigma(\alpha_2, \ldots, \alpha_m). \tag{6.25}$$

Koska väite pätee tapauksessa $m = 1$, voidaan käyttää induktio-oletusta, jonka mukaan väite pätee kaikille normaaleille kuntalaajennuksille $K' \hookrightarrow L'$, jossa L' on saatu kunnasta K' liittämällä siihen $m - 1$ alkiota. Kuntalaajennus (6.25) on tätä muotoa, joten $\Gamma(\Sigma(\alpha_1), L)$ on ratkeava. Tällöin yhtälön (6.23) perusteella $\Gamma(\Sigma, L)$ on ratkeava, jolloin yhtälöstä (6.22) seuraa, että $\Gamma(K, L)$ on ratkeava. □

LAUSE 6.9. *Olkoot K, L, M kuntia, joille pätee $K \subset L \subset M \subset \mathbb{C}$. Jos kuntalaajennus $K \hookrightarrow M$ on juurilaajennus, niin Galois'n ryhmä $\Gamma(K, L)$ on ratkeava.*

TODISTUS. Olkoon N kuntalaajennuksen $\mathrm{fix}(\Gamma(K, L)) \hookrightarrow M$ normaalisulkeuma. Tällöin saadaan lauseen 4.6 perusteella ketju sisäkkäisiä kuntia:

$$K \subset \mathrm{fix}(\Gamma(K, L)) \subset L \subset M \subset N. \tag{6.26}$$

Koska $K \hookrightarrow M$ on juurilaajennus, niin suoraan juurilaajennuksen määritelmästä seuraa, että myös $\mathrm{fix}(\Gamma(K, L)) \hookrightarrow M$ on juurilaajennus. Nyt lemman 6.5 nojalla kuntalaajennus $\mathrm{fix}(\Gamma(K, L)) \hookrightarrow N$ on normaali juurilaajennus. Tällöin lauseen 6.8 perusteella

$$\Gamma(\mathrm{fix}(\Gamma(K, L)), N) \text{ on ratkeava ryhmä.} \tag{6.27}$$

Lisäksi ehdon (6.26) nojalla pätee

$$\Gamma(\mathrm{fix}(\Gamma(K, L)), L) \subset \Gamma(K, L). \tag{6.28}$$

Toisaalta, jos $f \in \Gamma(K, L)$, niin f on kunnan L K-automorfismi, joka kiinnittää kiintopistekunnan $\mathrm{fix}(\Gamma(K, L))$ alkiot. Siten $f \in \Gamma(\mathrm{fix}(\Gamma(K, L)), L)$ eli

$$\Gamma(K, L) \subset \Gamma(\mathrm{fix}(\Gamma(K, L)), L).$$

Yhdistämällä tämä tietoon (6.28) saadaan yhtälö

$$\Gamma(\mathrm{fix}(\Gamma(K, L)), L) = \Gamma(K, L). \tag{6.29}$$

Yhtälö (6.29) saadaan edelleen muotoon

$$\mathrm{fix}(\Gamma(\mathrm{fix}(\Gamma(K, L)), L)) = \mathrm{fix}(\Gamma(K, L)).$$

Koska $K \hookrightarrow M$ on juurilaajennuksena äärellisasteinen, niin ehdon (6.26) perusteella myös $\mathrm{fix}(\Gamma(K, L)) \hookrightarrow L$ on äärellisasteinen. Siten voidaan käyttää lausetta 4.23. Sen mukaan kuntalaajennus $\mathrm{fix}(\Gamma(K, L)) \hookrightarrow L$ on normaali. Koska myös kuntalaajennus $\mathrm{fix}(\Gamma(K, L)) \hookrightarrow N$ on normaali ja $L \subset N$, voidaan käyttää viidettä Galois'n lausetta eli lausetta 4.28. Sen mukaan

$$\Gamma(\mathrm{fix}(\Gamma(K, L), L) \cong \Gamma(\mathrm{fix}(\Gamma(K, L), N)/\Gamma(L, N). \tag{6.30}$$

Ehdon (6.27) ja lemman 5.19 nojalla $\Gamma(\mathrm{fix}(\Gamma(K, L), N)/\Gamma(L, N)$ on ratkeava ja siten myös $\Gamma(\mathrm{fix}(\Gamma(K, L), L)$ on ratkeava. Tällöin yhtälön (6.29) perusteella myös $\Gamma(K, L)$ on ratkeava ryhmä. □

MÄÄRITELMÄ 6.10. Olkoon q polynomi kunnassa $K \subset \mathbb{C}$, ja olkoon Σ polynomin q hajotuskunta. Sanotaan, että *polynomin q Galois'n ryhmä kunnan K suhteen* on Galois'n ryhmä $\Gamma(K, \Sigma)$. Seuraavaksi todistetaan lauseen 6.9 tämän tutkielman tärkein tulos. Se kertoo, että jos polynomilla on ratkaisukaava, sen Galois'n ryhmä on ratkeava.

LAUSE 6.11. *Olkoon $p \in \mathbb{Q}[x]$ polynomi. Jos p ratkeaa juurin, niin polynomin p Galois'n ryhmä kunnan $\mathbb{Q}$ suhteen on ratkeava.*

TODISTUS. Olkoon polynomin hajotuskunta $\Sigma \subset \mathbb{C}$. Koska p on ratkaistavissa juurin, määritelmän 6.4 perusteella on olemassa sellainen kunta $M \subset \mathbb{C}$, jolle $\Sigma \subset M$ ja $\mathbb{Q} \hookrightarrow M$ on juurilaajennus. Koska pätee $\mathbb{Q} \subset \Sigma \subset M$, niin lauseen 6.9 nojalla $\Gamma(\mathbb{Q}, \Sigma)$ on ratkeava. □

Lauseen 6.11 käänteinen tulos pätee myös: jos polynomin Galois'n ryhmä on ratkeava, niin p ratkeaa juurin. Tätä ei kuitenkaan todisteta tässä tutkielmassa. Tuloksesta kiinnostuneet voivat katsoa todistuksen Stewartin kirjasta [**12**, Theorem 18.19].

6.2. Viidennen asteen yhtälö

Lause 6.11 on todistettu, joten suurin osa työstä on tehty. Vielä ei olla kuitenkaan löydetty yhtään viidennen asteen polynomia, jolla ei ole ratkaisukaavaa. Jotta voitaisiin soveltaa lausetta 6.11, täytyy löytää sellainen viidennen asteen polynomi, jonka Galois'n ryhmä on ratkeava. Tähän tarvitaan seuraavat kaksi lemmaa.

LEMMA 6.12. *Olkoon p alkuluku ja q kunnassa $\mathbb{Q}$ jaoton polynomi, jonka aste on p. Jos polynomilla q on täsmälleen $p-2$ reaalista nollakohtaa kunnassa $\mathbb{C}$, niin sen Galois'n ryhmä kunnan $\mathbb{Q}$ suhteen on isomorfinen symmetrisen ryhmän $\mathbb{S}_p$ kanssa.*

TODISTUS. Olkoon $\Sigma \subset \mathbb{Q}$ polynomin q hajotuskunta. Lauseen 3.14 mukaan polynomin q nollakohdat ovat erilliset. Olkoot nämä nollakohdat $\alpha_1, \ldots, \alpha_p$. Tällöin

$$\Sigma = \mathbb{Q}(\alpha_1, \ldots, \alpha_p).$$

Olkoon $f \in \Gamma(\mathbb{Q}, \Sigma)$ $\mathbb{Q}$-automorfismi. Koska

$$q(f(\alpha_i)) = f(q(\alpha_i)) = f(0) = 0$$

kaikilla $i = 1, \ldots, p$, niin $f(\alpha_i)$ on polynomin q nollakohta. Siten $f(\alpha_i) = \alpha_j$ jollekin $j = 1, \ldots, p$. Tällöin rajoittumakuvaus $f : \{\alpha_1, \ldots, \alpha_p\} \to \{\alpha_1, \ldots, \alpha_p\}$ on bijektio eli se permutoi nollakohtia α_i. Määritellään kuvaus $\phi : \Gamma(\mathbb{Q}, \Sigma) \to \mathbb{S}_p$ asettamalla kaikille $f \in \Gamma(\mathbb{Q}, \Sigma)$

$$\phi(f) = \sigma,$$

missä $\sigma(i) = j$, jos ja vain jos $f(\alpha_i) = j$. Väite on todistettu, jos pystytään osoittamaan kuvaus ϕ isomorfismiksi. Ainakin ϕ on kuvaus, sillä

$$f : \{\alpha_1, \ldots, \alpha_p\} \to \{\alpha_1, \ldots, \alpha_p\}$$

on bijektio kaikilla $f \in \Gamma(\mathbb{Q}, \Sigma)$, jolloin $\phi(f) = \sigma \in \mathbb{S}_p$. Kuvaus ϕ on myös ryhmähomomorfismi, sillä sekä Galois'n ryhmissä että symmetrisissä ryhmissä on laskutoimituksena kuvausten yhdistäminen. Lisäksi kuvaus ϕ on injektio. Jos nimittäin $\phi(f_1) = \phi(f_2)$ joillain $f_1, f_2 \in \Gamma(\mathbb{Q}, \Sigma)$, niin $f_1(\alpha_i) = f_2(\alpha_i)$ kaikille $i = 1, \ldots, p$. Koska $\mathbb{Q}$-automorfismi f määräytyy täysin arvoistaan pisteissä α_i, niin $f_1 = g_1$.

Täytyy enää osoittaa, että ϕ on surjektio.

Olkoot polynomin q nollakohdat joukossa Σ nimeltään $\alpha_1, \alpha_2, \ldots, \alpha_p$. Koska ne ovat erilliset, pätee

$$\Sigma = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_p),$$

missä $\alpha_i \in \mathbb{C}$ ja $\alpha_i \neq \alpha_j$, kun $i \neq j$.

Jakamalla polynomi q tarvittaessa sen johtavalla kertoimella voidaan olettaa, että q on perusmuotoinen. Tällöin q on nollakohtiensa minimaalipolynomi, jolloin lauseesta 2.24 seuraa, että

$$[\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha_1)] = p.$$

Kuntajaalennus $\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_p)$ saadaan puolestaan yhdistämällä kuntalaajennuksia perättäin. Tällöin lause 2.22 kertoo, että alkuluku p jakaa kuntalaajennuksen $\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_p)$ asteen.

Toisaalta ensimmäisestä Galois'n lauseesta 4.21 seuraa, että alkuluku p jakaa myös joukon $\Gamma(\mathbb{Q}, \Sigma)$ alkioiden lukumäärän. Cauchyn lauseen 5.35 mukaan tällöin ryhmässä $\Gamma(\mathbb{Q}, \Sigma)$ on kertalukua p oleva alkio. Olkoon tämä $g \in \Gamma(\mathbb{Q}, \Sigma)$. Koska ϕ on monomorfismi, niin alkion $\phi(g)$ kertaluku on myös p. Lauseen 5.10 mukaan $\phi(g) \in \mathbb{S}_p$ on tällöin p-sykli. Siten ryhmä $\phi(\Gamma(\mathbb{Q}, \Sigma))$ sisältää p-syklin.

Tarkastellaan seuraavaksi kompleksikonjugaattikuvausta $f : \mathbb{C} \to \mathbb{C}, f(z) = \bar{z}$. Sen rajoittumakuvaus $f|_\Sigma : \Sigma \to \mathbb{C}$ on $\mathbb{Q}$-monomorfismi. Koska Σ on polynomin p hajotuskunta, niin lauseen 3.8 nojalla $\mathbb{Q} \hookrightarrow \Sigma$ on normaali. Lemman 4.19 kohdan (1) $\Rightarrow$ (3) nojalla $f|_\Sigma$ on myös $\mathbb{Q}$-automorfismi kunnassa Σ. Siten

$$f|_\Sigma \in \Gamma(\mathbb{Q}, \Sigma).$$

Tarvittaessa numerointia vaihtamalla voidaan olettaa, että polynomin q nollakohdista $\alpha_1, \ldots, \alpha_p$ imaginäärisiä ovat nollakohdat α_1 ja α_2 sekä reaalisia ovat $\alpha_3, \ldots, \alpha_p$. Tällöin $f|_\Sigma(\alpha_i) = \alpha_i$ kaikilla $i = 3, \ldots, p$ ja koska $f|_\Sigma \in \Gamma(\mathbb{Q}, \Sigma)$ on bijektio, niin täytyy olla $f|_\Sigma(\alpha_1) = \alpha_2$ ja $f|_\Sigma(\alpha_i) = \alpha_1$. Tällöin kuitenkin kuvauksen ϕ määritelmän perusteella $\phi(f|_\Sigma)$ on 2-sykli. Siten ryhmä $\phi(\Gamma(\mathbb{Q}, \Sigma))$ sisältää 2-syklin. Koska $\phi(\Gamma(\mathbb{Q}, \Sigma))$ sisältää myös p-syklin ja lemman 5.11 perusteella mikä tahansa 2-sykli ja mikä tahansa p-sykli virittävät symmetrisen ryhmän $\mathbb{S}_p$, niin

$$\phi(\Gamma(\mathbb{Q}, \Sigma)) = \mathbb{S}_p.$$

Tällöin ϕ on surjektio ja siten ryhmät $\Gamma(\mathbb{Q}, \Sigma)$ ja $\mathbb{S}_p$ ovat isomorfiset. □

Lemman 6.12 avulla on helppoa keksiä yksittäisiä viidennen asteen yhtälöitä, jotka eivät ole ratkaistavissa juurin: lauseen 6.11 ja lemman 6.12 mukaan jaoton, rationaalikertoiminen viidennen asteen polynomi, jolla on tasan kaksi imaginääristä nollakohtaa, ei ratkea juurin. Seuraavaksi lauseessa 6.13 esitetään tästä yksi esimerkki.

LAUSE 6.13. *Joukon $\mathbb{Q}$ viidennen asteen polynomia $x^5 - 4x^2 + 2$ ei voi ratkaista juurin.*

TODISTUS. Olkoon $p(x) = x^5 - 4x^2 + 2$. Osoitetaan ensiksi, että polynomilla p on täsmälleen $p - 2 = 3$ reaalista nollakohtaa. Tähän tarvitaan avuksi hieman tietoja analyysistä. Tutkitaan kuvausta $p : \mathbb{R} \to \mathbb{R}$, $p(x) = x^5 - 4x^2 + 2$. Koska $p(-2) = -46$, $p(-1) = -3$, $p(0) = 2$, $p(1) = -1$ ja $p(2) = 18$, on kuvauksella $p(x)$ jatkuvana kuvauksena Bolzanon lauseen mukaan ainakin kolme reaalista nollakohtaa. Polynomin

p derivaatta $Dp = 5x^4 - 8x$. Polynomilla $Dp(x)$ on nollakohdat $x = 0$ sekä $x = \frac{2}{\sqrt[3]{5}}$. Rollen lauseen perusteella (ks. esimerkiksi [**3**, s. 175-177]) kuvauksen $p(x)$ nollakohtien välissä on aina vähintään yksi derivaatan nollakohta. Siispä polynomilla $p(x)$ on täsmälleen kolme erisuurta reaalista nollakohtaa. Lisäksi koska p on perusmuotoinen ja alkuluvulle 2 pätee $2 \mid -4$ ja $2 \mid 2$, mutta $2^2 \nmid 2$, niin Eisensteinin ehdon 1.18 mukaan polynomi p on jaoton renkaassa $\mathbb{Q}[x]$. Jaottomalla polynomilla on lauseen 3.14 perusteella vain yksinkertaisia nollakohtia, joten polynomilla p täytyy olla tasan kolme reaalista nollakohtaa. Tällöin lemmasta 6.12 seuraa, että polynomin p Galois'n ryhmä on isomorfinen ryhmän $\mathbb{S}_5$ kanssa.

Lauseen 5.25 mukaan $\mathbb{S}_5$ ei ole ratkeava. Koska ratkeamattoman ryhmän kanssa isomorfinen ryhmä ole ratkeava, niin polynomin p Galois'n ryhmä ei ole ratkeava. Lauseen 6.11 mukaan se tarkoittaa, että $x^5 - 4x^2 + 2$ ei ole ratkaistavissa juurin.

□

Lause 6.13 osoittaa, ettei ole olemassa kaavaa, jolla löydettäisiin minkä tahansa viidennen asteen yhtälön nollakohdat. Entä onko olemassa ratkaisukaavaa, kun polynomin aste on $n > 5$? Lauseen 6.13 avulla voidaan helposti päätellä, että ratkaisukaavan olemassaolo on mahdotonta. Voidaan nimittäin valita viidennen asteen polynomi p, joka ei ratkea juurin. Tarkastellaan seuraavaksi polynomia $x^{n-5} \cdot p$. Koska polynomin x^{n+5} ainoa nollakohta on $0 \in \mathbb{Q}$, niin polynomilla $x^{5-n} \cdot p$ on sama hajotuskunta kuin polynomilla p. Siten myös niiden Galois'n ryhmät ovat samat, jolloin $x^{5-n} \cdot p$ ei ole ratkaistavissa juurin.

Toisaalta eräät viidennen asteen yhtälöt − esimerkiksi $x^5+1 = 0$ − ovat ratkaistavissa juurin. Tämä herättää kysymksen, milloin viidennen asteen yhtälö on ratkaistavissa juurin ja milloin ei. Tähän kysymykseen ei tässä tutkielmassa pystytä vastaamaan.

Kirjallisuutta

[1] Olivier Bordellès: *Arithmetic Tales*. Springer-Verlag, 2006.

[2] Carl Boyer: *Tieteiden kuningatar*. Toinen laitos, toim. Uta C. Merzbach, suom. Kimmo Pietiläinen, Art House 2000.

[3] Richard Courant ja Fritz John: *Introduction to Calculus and Analysis I*. Kolmas laitos, Springer-Verlag, 1999.

[4] John R. Durbin: *Modern algebra*. John Wiley & Sons, 1979.

[5] Benjamin Fine ja Gerhard Rosenberger: *The Fundamental Theorem of Algebra*. Springer-Verlag, 1997.

[6] Serge Lang: *Algebra*. Toinen laitos, Addison-Wesley, 1984.

[7] Serge Lang: *Introduction to Linear Algebra*. Toinen laitos, Springer-Verlag, 1970.

[8] Tauno Metsänkylä ja Marjatta Näätänen: *Algebra*. Limes, 2003.

[9] Lauri Myrberg: *Algebra korkeakouluja varten*. Kirjayhtymä, 1978.

[10] Veikko T. Purmonen: *Lineaarinen algebra ja geometria 1*. Jyväskylän yliopistopaino, 2007.

[11] Tony Rothman: *Genius and Biographers: The Fictionalization of Evariste Galois*. Elektroninen dokumentti osoitteessa http://www.physics.princeton.edu/∼trothman/galois.html (luettu 6.3.2014).

[12] Ian Stewart: *Galois Theory*. Kolmas laitos, Chapman & Hall, 2004.