# Galois'n teoria

Pirita Paajanen
pirita.paajanen@helsinki.fi

18. lokakuuta 2011

## Sisältö

Évariste Galois (1811-1832) on yksi matematiikan tunnetuimpia traagisia sankareita. Hän kuoli kaksintaistelussa vain kaksikymmentä vuotiaana toukokuussa 1832. Kaksintaistelua edeltävänä yönä hän luonnosteli kirjeessä ystävälleen Chevalierille abstraktin algebran alkeet, sisältäen ryhmäteorian perusteet sekä lauseen, että polynomiyhtälön voi ratkaista radikaalien avulla vain jos yhtälöön liittyvä ryhmä on ratkeava. Nykyään tätä teoriaa kutsutaan ansaitusti Galois'n teoriaksi.

Galois'n teoria on yksi kauneimpia matematiikan osa-alueita. Vihdoin toisinaan kovin abstrakteilta näyttävät algebralliset määritelmät kantavat hedelmää ja todistetaan, miten ryhmäteoria liittyy kuntateoriaan ja miten eri rakenteitten avulla voidaan tutkia toisia rakenteita. Tällä kurssilla käydään läpi Galois'n teorian perusteet. Kurssi kulminoituu todistukseen viidennen asteen polynomiyhtälön ratkeamattomuudesta radikaalien avulla.

Luennot: I periodissa ma ja ti laskuharjoitukset pe 8-10.

Kurssi suoritetaan laskuharjoituksia tekemällä.

**Tiivistelmä**

Tämän kurssin tarkoituksena on tutkia kuntia, liittää kuntalaajennoksen automorfismiryhmä, sekä tarkastella kuntalaajennosten rakennetta sekä automorfismiryhmän aliryhmärakennetta. Tämä on tyypillinen lähestymistapa algebrassa: yhteen (algebralliseen) objektiin liitetään toinen algebrallinen objekti, jonka ominaisuuksista on helpompi tutkia ja joista voidaan voidaan päätellä jotain alkuperäisestä objektista. Erityissovellutuksena ovat polynomien ratkaisukaavat.

# 1 Historiallinen katsaus

Matematiikan historia alkaa ajoitetaan usein muinaiseen Egyptiin ja Niilin tulvien jälkeiseen maanmittaukseen. Tästä juontaa sana geometria. Ensimmäisen ja toisen asteen yhtälöt ovat luonnollisia mitattaessa maa-alaa ja esimerkiksi suorakaiteenmuotoisen pinta-alan sivujen pituuksia. Ensimmäisen asteen yhtälöitä ratkaistiin hyvin aikaisin matematiikan historiassa, ovathan ne nykyäänkin jo ala-asteen oppikirjoissa.

## 1.1 Toisen asteen polynomi

Jo antiikissa osattiin ratkaista toiseen asteen polynomi käyttäen juurilausekkeita. Tosin ratkaisu vaatii irrationaalilukujen käyttöönottoa, joten ihan selvää ei ollut, että ratkaisu oli olemassa. Samoin toisen asteen ratkaisukaavan antamat kompleksiluvut hyväksyttiin matematiikkaan vasta pari vuosituhatta myöhemmin.

Yhtälön $ax^2 + bx + c = 0$ ratkaisut ovat

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

Kutsutaan juuria nimillä $\alpha_1, \alpha_2$. Oletetaan, että ne ovat irrationaalisia. Galois'n teorian idea voidaan tiivistää havaintoon, että nämä juuret käyttäytyvät symmetrisesti. Nimittäin jos laaditaan kuntalaajennos $\mathbb{Q}(\alpha_1, \alpha_2)$, on laajennoksen aste 2, ja tällä uudella kunnalla on kunta-automorfismi $\phi(\alpha_1) = \alpha_2$, joka virittää ryhmän $G = \{Id_K, \phi\} \cong C_2$, jolla on toiminta kunnassa $K$. Kaiken lisäksi toiminta jättää vakaaksi alikunnan $\mathbb{Q}$. Tässä konstruoitiin Galois'n laajennos, Galois'n automorfismi ja sen virittämä ryhmä. Ryhmä on kahden alkion syklinen ryhmä, ja siis ratkeava.

## 1.2 Kolmannen asteen polynomi

Tartaglia, Ferrari, Cardano ja Vieta

## 1.3 Neljännen asteen polynomi:

samat

## 1.4 Viidennen asteen polynomi: Abel ja Galois

Galois'n koko matemaatikon ura oli pettymyksiä täynnä, ja hän kokikin itsensä väärinymmärretyksi neroksi. Epäonnistuttuaan École Polytechniquen pääsykokeissa kahdesti hän opiskeli École Normalessa. Hänet kuitenkin erotettiin sieltä poliittisen aktivismin vuoksi. Hänen yrityksensä matemaattisten tutkimustensa julkaisuun myös kohtasi takaiskuja. Cauchy hylkäsi kaksi paperia, jotka hän lähetti Pariisin tiedeakatemialle, ja kumpikin paperi katosi lopullisesti. Tämän jälkeen hän lähetti tutkimuksensa Tiedeakatemian matematiikan Grand Prix-kilpailuun. Akatemian sihteeri Fourier kuoli ennen kuin hän ehti lukea tutkimuksen, eikä paperia löydetty Fourierin arkistosta. Tammikuussa 1831 Galois lähetti uuden paperin Tiedeakatemialle. Vasta heinäkuussa hän sai palautteen, jossa Poisson toteaa paperin käsittämättömäksi ja pyytää Galois'ta kirjoittamaan teoriansa kokonaisuudessa. Valitettavasti Galois'lta loppui aika kesken, sillä vasta kaksintaistelua edeltävänä yönä hän kävi käsiksi työhön.

# 2 Renkaat, kunnat ja polynomirenkaat

**Määritelmä 2.1.** *Rengas* $R$ on Abelin ryhmä operaation $+$ suhteen, ja lisäksi $R$:ssä on assosiatiivinen binäärioperaatio $\cdot$, jolle pätee $a(b+c) = ab + ac$ ja $(a+b)c = ac + bc$.

**Määritelmä 2.2.** Renkaan $R$ osajoukko on *alirengas*, jos se on suljettu operaatioiden $+$ ja $\cdot$ suhteen, siihen kuuluu additiivinen nolla-alkio.

**Määritelmä 2.3.** Renkaan $R$ osajoukko $I$ on *ideaali*, jos se on renkaan $R$ additiivinen aliryhmä, ja kaikille $a \in I$ ja $r \in R$ pätee, että $ar \in I$ ja $ra \in I$. Jos vain toinen näistä pätee, kutsutaan ideaalia oikeaksi tai vasemmaksi ideaaliksi. Ideaali on aito, jos $I \neq R$. Ideaali $I$ on *maksimaalinen*, jos ja vain jos $I \subseteq J \subseteq R$ tai $J$ on ideaali, tästä seuraa, että $J = I$ ja $J = R$.

**Määritelmä 2.4.** Rengas $R$

1. on *vaihdannainen*, jos $xy = yx$ kaikille $x, y \in R$.
2. *sisältää ykkösalkion*, jos on olemassa yksikäsitteinen $0 \neq 1 \in R$, jolle pätee $1x = x1 = x\ \forall x$.
3. on *kokonaisalue*, jos se on vaihdannainen, ja siinä on ykkösalkio, sekä $ab = 0$ väistämättä tarkoittaa sitä, että $a = 0$ tai $b = 0$.

4. on *jakorengas*, jos siinä on ykkösalkio ja $R \setminus \{0\}$ on multiplikatiivinen ryhmä.
5. on *kunta*, jos se on kommutatiivinen jakorengas.

**Esimerkki 2.5.** (a) Kokonaisluvut $\mathbb{Z}$ on rengas, se on vaihdannainen, sillä kertolasku on vaihdannainen. Sillä on ykkösalkio 1, se on myös kokonaisalue, koska vain kertomalla nollalla saadaan nolla. Kuitenkaan $\mathbb{Z} \setminus \{0\}$ ei ole multiplikatiivinen ryhmä, sillä käänteisalkioita ei ole. Näin ollen, $\mathbb{Z}$ ei ole myöskään kunta.

(b) Tuttuja esimerkkejä kunnista ovat $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$.

(c) Rengas $\mathbb{Z}/m\mathbb{Z}$, eli kokonaisluvut $\mod m$ on selvästikin rengas. Se on vaihdannainen, ja siinä on ykkösalkio, mutta kokonaisalue se on vain siinä tapauksessa, että $m$ on alkuluku. Esimerkiksi $m = 6$, silloin $2 \cdot 3 \equiv 0 \mod 6$, joten renkaassa on nollajakajia. Jos $m$ on alkuluku, on rakenne myös kunta.

(d) $n \times n$ matriisit muodostavat renkaan, joka ei ole vaihdannainen, mutta sisältää ykkösalkion.

**Määritelmä 2.6.** Olkoot $R$ ja $S$ renkaita. Kuvaus $\varphi : R \longrightarrow S$ on *rengashomomorfismi*, jos $\varphi(a + b) = \varphi(a) + \varphi(b)$ ja $\varphi(ab) = \varphi(a)\varphi(b)$ kaikille $a, b \in R$.

**Lause 2.7.** *Olkoon $R$ rengas, ja $I$ ideaali, silloin on olemassa rengas $R/I$, jonka operaatio on $(a + I)(b + I) = ab + I$ ja lisäksi, $R/I$ on vaihdannainen, jos $R$ on vaihdannainen. $R/I$ sisältää ykkösalkion jos $I \neq R$ ja $R$ sisältää ykkösalkion.*

*Todistus.* Algebra I. □

**Esimerkki 2.8.** $\mathbb{Z}$ on rengas, $m\mathbb{Z}$ on ideaali, ja $\mathbb{Z}/m\mathbb{Z}$ on tekijärengas.

Tällä kurssilla kaikki renkaat ovat kommutatiivisia ja sisältävät ykkösalkion, vaikka tätä ei erikseen mainittaisikaan. Tyypillinen esimerkki on kokonaislukujen rengas $\mathbb{Z}$.

**Määritelmä 2.9.** *Kokonaisalue* on kommutatiivinen rengas, jossa on ykkösalkio, ja jossa pätee $ab = 0$ vain jos $a = 0$ tai $b = 0$. (no zero divisors)

**Esimerkki 2.10.** $\mathbb{Z}$, $k[x]$, missä $k$ on mikä tahansa kunta.

**Lemma 2.11.** *Äärellinen kokonaisalue on aina kunta.*

*Todistus.* Tehtävä. □

**Määritelmä 2.12.** Olkoon $R$ kommutatiivinen rengas, jossa on ykkösalkio. Olkoon $I \lhd R$ ideaali. Silloin $I$ on *alkuideaali* jo $ab \in I \Rightarrow a \in I$ tai $b \in I$.

**Esimerkki 2.13.** $\mathbb{Z}$, jossa $I = p\mathbb{Z}$.

**Lause 2.14.** *Okoon $R$ kommutatiivinen rengas, jossa on ykkösalkio, ja olkoon $I \lhd R$. Silloin $I$ on alkuideaali, jos ja vain jos $R/I$ on kokonaisalue.*

*Todistus.* Olkoon $I$ alkuideaali. Tehdään vastaoletus, että renkaassa $R/I$ on olemassa nollajakajia $a, b \neq 0$. Eli $(a+I)(b+I) = 0+I = 0_{R/I}$. Silloin $ab+I = 0+I$, mistä seuraa, että $ab \in I$. Koska $I$ on alkuideaali, tämä tarkoittaa sitä, että $a \in I$ tai $b \in I$, joten oikeasti $a + I = 0 + I$ tai $b + I = 0 + I$, ja nollasta eroavia nollajakajia ei ole.

Oletetaan, että $R/I$ on kokonaisalue, ja todistetaan, että $I$ on alkuideaali. Oletetaan, että $ab \in I$, jolloin $ab + I = 0 + I$, mistä seuraa $(a + I)(b + I) = 0 + I = 0_{R/I}$. Koska $R/I$ on kokonaisalue, tästä seuraa, että $a + I = 0 + I$ tai $b + I = 0 + I$ ja näin ollen $a \in I$ tai $b \in I$, ja $I$ on alkuideaali. □

**Lause 2.15.** *Okoon $R$ kommutatiivinen rengas, jossa on ykkösalkio, ja olkoon $I \lhd R$. Silloin $I$ on maksimaalinen ideaali, jos ja vain jos $R/I$ on kunta.*

*Todistus.* Harjoitustehtävä I/3. □

**Määritelmä 2.16.** Olkoon $R$ kokonaisalue, ja olkoot $I, J$ ideaaleja. Silloin

$$IJ = \{\sum_{i=1}^{k} a_i b_i : a_i \in I, b_i \in J, k \geq 1\}.$$

Huomaa, että $IJ$ koostuu äärellisistä summista, mutta että summan pituus $k$ vaihtelee.

Rengas $K$ on kunta, silloin kun kaikilla nollasta eroavilla alkioilla on multiplikatiivinen vasta-alkio. Kunta on automaattisesti kokonaisalue.

**Esimerkki 2.17.** Kunnan karakteristika, tehtävänä!

**Propositio 2.18.** *Olkoon $R$ kokonaisalue. $R$:stä voidaan konstruoida jakokunta $K$ seuraavalla tavalla. On olemassa homomorfismi $\phi : R \longrightarrow K$, joka on injektiivinen, ja kaikille $x \in K$ on olemassa $a, b \in R$, joille $x = \frac{\phi(a)}{\phi(b)}$.*

**Lemma 2.19.** *i) Olkoon $K$ kunta, ja $I \leq K$. Silloin $I = \{0\}$ tai $I = K$. ii) Olkoot $K$ ja $L$ kuntia. Rengashomomorfismi $f : K \longrightarrow L$ on väistämättä injektio.*

Olkoon $R$ rengas. Tästä voidaan muodostaa polynomirengas

$$R[x] = \left\{ \sum_{i=0}^{d} a_i x^i : a_i \in R \right\},$$

joka koostuu kaikista polynomeista, joiden kertoimet kuuluvat kuntaan $R$. Rengasoperaatiot saadaan laajentamalla $R$:n operaatiot polynomeihin normaalilla tavalla. Nollasta eroavan polynomin $f \in R[x]$ aste on korkein $n$, jolle $a_n \neq 0$. Astetta merkitään $degf$. Polynomia kutsutaan pääpolynomiksi jos sen korkeimman asteen termin kerroin on 1. Kun $f \in K[x]$, ja $\alpha \in K$ on polynomin juuri, silloin $f(\alpha) = 0$.

**Lemma 2.20.** *Jos $R$ on kokonaisalue, silloin myös $R[x]$ on kokonaisalue.*

Olkoon $K$ nyt kunta, silloin saadaan polynomirengas $K[x]$ sekä jakokunta

$$K(x) = \left\{ \frac{f(x)}{g(x)} : f, g \in K[x], g \neq 0 \right\}.$$

**Määritelmä 2.21.** Olkoon $R$ kokonaisalue.

1. $u \in R$ on *yksikkö/kääntyvä alkio*, jos $\exists v \in R$, jolle pätee $uv = vu = 1$.
2. $a \in R$ on *jaoton/redusoimaton*, jos $a \neq 0$, $a$ ei ole yksikkö ja $a = bc$ tarkoittaa, että joko $b$ tai $c$ on yksikkö.
3. $a \in R$ on *alkualkio*, jos $a \neq 0$, $a$ ei ole yksikkö, ja $a \mid bc$ johtaa siihen, että $a \mid b$ tai $a \mid c$.

**Lemma 2.22.** *Kun $R$ on kokonaisalue, alkualkiot ovat jaottomia.*

*Todistus.* Olkoon $p$ alkualkio, ja oletetaan, että $p = ab$. Alkualkion määritelmän nojalla $p \mid a$ tai $p \mid b$. Valitaan, $p \mid a$, joten $a = pc$, jollekin $c$. Siispä $p = ab = pcb$. Tästä seuraa, että $p(1 - cb) = 0$, koska $p \neq 0$, ja kyseessä on kokonaisalue, tästä seuraa, että $cb = 1$, ja $b$ on yksikkö. Näin ollen $p$ on redusoimaton. □

Huomaa, että jaottomat alkiot eivät välttämättä ole alkualkioita. Tämä on totta kun $R$ on pääideaalialue. Palaamme tähän myöhemmin.

**Esimerkki 2.23.** Renkaassa $\mathbb{Z}$ yksiköt ovat alkiot $\pm 1$. Sen jaottomat alkiot ovat täsmälleen $\pm p$, jossa $p$ on alkuluku, nämä ovat myös alkualkiot. Renkaassa $K[x]$, mikä tahansa astetta 1 oleva polynomi on jaoton. Yksiköitä ovat nollasta eroavat vakiopolynomit.

**Määritelmä 2.24.** Kokonaisalueella $R$ on *yksikäsitteinen tekijöihinjako*, jos jokaiselle $a \in R$, joka ei ole nolla tai yksikkö, pätee

1. $a = p_1 p_2 \dots p_k$ jossa jokainen $p_i$ on alkualkio.
2. Jos $p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$, missä $p_i$ ja $q_j$ ovat alkualkioita, silloin $k = l$ ja on olemassa indeksien $\{1, 2, \dots, k\}$ permutaatio $\sigma$, ja yksiköt $u_1, u_2, \dots, u_k$ siten, että

$$p_i = u_i q_{\sigma(i)}$$

kaikille $i = 1, 2, \dots, k$.

**Propositio 2.25.** *Jos $f \in K[x]$ on vähintään astetta 1 oleva polynomi, silloin on olemassa jaottomat polynomit $q_1, \dots, q_k$ joille pätee $f = q_1 \dots q_k$. Tekijöihinjako on yksikäsitteinen, järjestystä vaille.*

*Todistus.* Todistetaan väite induktiolla. Jos $f$:n aste on 1, on se redusoimaton. Oletetaan, että väite on tosi polynomeille, joiden aste on $< k$. Olkoon $f$ polynomi, jonka aste on täsmälleen $k$. Jos $f$ on redusoimaton, silloin ei ole mitään todistettavaa. Jos $f$ ei ole redusoimaton, se voidaan kirjoittaa $f = gh$, ja $deg\ g, deg\ h < k$. Nyt voidaan soveltaa induktio hypoteesia polynomeihin $g$ ja $h$, ja ne voidaan kirjoittaa redusoimattomien polynomien tulona

$$\begin{aligned} g &= q_1 \dots q_s \\ h &= q_{s+1} \dots q_r, \end{aligned}$$

mistä seuraa, että $f = q_1 \dots q_s$. □

Jaottomuus riippuu kunnasta! Esimerkiksi $x^2 - 2$ on jaoton kunnassa $\mathbb{Q}$, kun taas kunnassa $\mathbb{R}$ se hajoaa tuloksi $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. Polynomi $x^2 + 1$ on jaoton kunnassa $\mathbb{Q}$ tai $\mathbb{R}$, mutta hajoaa kunnassa $\mathbb{C}$ kahden tuloksi $x^2 + 1 = (x - i)(x + i)$. Algebran peruslauseen nojalla tiedämme, että epävakio polynomi $f \in \mathbb{C}[x]$ hajoaa aina äärelliseksi tuloksi lineaarisia tekijöitä. Aina ei kuitenkaan tarvitse mennä kompleksilukujen kuntaan $\mathbb{C}$ saakka, jotta saamme polynomin hajoamaan lineaarisiksi tekijöiksi. Esimerkiksi kunta $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ on kunta, se on reaalilukujen $\mathbb{R}$ pienen alikunta, jossa $f(x) = x^2 - 2$ voidaan kirjoittaa lineaaristen polynomien tulona.

Samalla lailla $\{a + bi : a, b \in \mathbb{Q}\}$ on pienin kompleksilukujen $\mathbb{C}$ alikunta, jossa $x^2 + 1$ hajoaa lineaarisiksi tekijöiksi.

Seuraava lause on hyödyllinen pieni tulos, kun halutaan etsiä juuria.

**Lause 2.26.** *Jos $f \in K[x]$, missä $K$ on kunta. Olkoon $a \in K$, silloin $(x - a) \mid f$ jos ja vain jos $f(a) = 0$.*

*Todistus.* $f(x) = (x - a)q(x) + r(x)$, missä $r(x) = 0$ tai se on vakiopolynomi. Sijoita $x = a$ ja silloin $f(a) = r$. □

Tarkastellaan seuraavaksi polynomeja renkaassa $\mathbb{Z}[x]$, ja niiden jaottomuutta, koska käytännössä kaikki kurssin esimerkit tulevat kunnasta $\mathbb{Q}$ ja sen kokonaislukujen renkaasta $\mathbb{Z}$.

**Lemma 2.27** (Gaussin lemma)**.** *Olkoon $f \in Z[x]$ mooninen (pääpolynomi?) polynomi. Silloin $f$ on redusoimaton renkaassa $\mathbb{Z}[x]$ jos ja vain jos se on redusoimaton renkaassa $\mathbb{Q}[x]$.*

**Korollaari 2.28.** *Jos $f$ on pääpolynomi, jonka kertoimet ovat kaikki $\mathbb{Z}$:ssa, ja $f$:n aste on pienempi tai yhtäsuuri kuin 3. Jos $f$:llä ei ole yhtään kokonaislukujuurta, on $f$ redusoimaton renkaassa $\mathbb{Q}[x]$.*

*Todistus.* Gaussin lemma ja tekiköjihinjako. □

**Lemma 2.29** (Eisensteinin kriteerio)**.** *Olkoon $f = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ pääpolynomi renkaassa $\mathbb{Z}[x]$. Oletetaan, että on olemassa alkuluku $p$, jolle $p \mid a_i$ kaikille $0 \leq i < n$ mutta $p^2 \not| a_0$. Silloin $f$ on redusoimaton renkaassa $\mathbb{Z}[x]$.*

# 3 Ryhmän toiminnat kunnissa ja polynomirenkaissa

**Määritelmä 3.1.** Olkoon $G$ ryhmä ja $\Omega$ joukko. Ryhmä $G$ toimii joukossa $\Omega$, jos on olemassa kuvaus $G \times \Omega \to \Omega$, jossa $(g, \omega) \mapsto g * \omega$ joka toteuttaa seuraavat ehdot: (i)

$$1 * \omega = \omega$$

(ii)

$$(gh) * \omega = g * (h * (\omega)).$$

Tämä on ryhmän vasen toiminta.

Oikea toiminta on $\omega * (gh) = (\omega * g) * h$. Yritän välttää käyttämästä oikeaa toimintaa tällä kurssilla. Tapana on pudottaa $*$ merkinnästä pois, ja kirjoittaa vain $g * \omega$.

**Lemma 3.2.** *Toimikoon $G$ joukossa $\Omega$. Tällöin jokainen $g \in G$ indusoi kuvauksen*

$$\begin{aligned} \phi_g : \quad & \Omega \to \Omega, \\ & \alpha \mapsto g * \alpha \end{aligned}$$

*joka määrittää joukon $\Omega$ permutaation. Toisin sanoen, toiminta määrittelee homomorfismin $\phi : G \longrightarrow S_n$.*

*Todistus.* On selvää, että kuvauksen $\phi_g$ käänteiskuvaus on $\phi_{g^{-1}}$, koska jokaiselle $\alpha \in \Omega$ pätee

$$\phi_g \phi_{g^{-1}}(\alpha) := g * (g^{-1} * \alpha)) = g * g^{-1} * \alpha = 1 * \alpha = \alpha.$$

Olemme todistaneet, että kuvaus $\phi_g : \Omega \to \Omega$ on bijektio, ja näin ollen se on permutaation määritelmän mukaan $\Omega$:n permutaatio. □

Toiminta jakaa $\Omega$:n radoiksi. Rata on ekvivalenssiluokka ekvivalenssirelaatiossa $\equiv$, missä $a \equiv b$ jos ja vain jos $\exists g \in G$ jolle $ga = b$

Merkitään $\Omega_a = \{ga : \forall g \in G\}$.

Ekvivalenssiluokkien määritelmän nojalla joukko $\Omega$ hajoaa ratojen pistevieraaksi unioniksi.

Kutsumme ryhmän $G$ toimintaa joukossa $\Omega$ *transitiiviseksi*, jos jokaiselle $\omega_1, \omega_2 \in \Omega$, on olemassa $g \in G$ ja $g * \omega_1 = \omega_2$. Toisin sanoen, kaikki $\Omega$:n alkiot kuuluvat samalle radalle.

Alkion $\omega$ *vakauttaja* on joukko

$$G_\omega = \{g \in G : g * \omega = \omega\}.$$

Näistä seuraa:

**Lause 3.3.** *Olkoon $G$ äärellinen ryhmä ja $\Omega$ äärellinen joukko. Kun $G$ toimii $\Omega$:ssa, jokaiselle $\alpha \in \Omega$, on voimassa*

$$|\Omega_\alpha| = |G : G_\alpha|.$$

Toiminta on *uskollinen*, jos kuvauksen $\phi : G \longrightarrow S_n$ ydin koostuu neutraalialkiosta, toisin sanoen, kuvaus on injektio, joten jokainen $G$:n alkio antaa eri permutaation joukossa $n$.

Monet ryhmäteorian lauseet, jotka riippuvat ryhmän mahtavuudeta tai alkion kertaluvusta, on usein helppo todistaa toimintojen avulla. Tässä yksi esimerkki klassisesta lauseesta.

**Lause 3.4** (Cayley)**.** *Jokainen äärellinen ryhmä $G$, jonka kertaluku on pienempi tai yhtäsuuri kuin $n$, on ryhmän $S_n$ aliryhmä.*

*Todistus.* Jos $k \leq n$, on $S_k \leq S_n$. Voidaan siis olettaa, että $G$:n kertaluku on tasan $n$. Osoitetaan, että ryhmä, jonka kertaluku on $n$ on symmetrisen ryhmän $S_n$ aliryhmä. Määritellään $G$-toiminta triviaalin aliryhmän $\{1\}$ sivuluokissa. Näitä sivuluokkia on luonnollisesti $n$ kappaletta ja ne vastaavat $G$:n alkioita. Yllä olevan lemman perusteella toiminta määrittelee homomorfismin $\phi : G \to S_n$. Homomorfismin ytimeen kuuluvat sellaiset $G$:n alkiot, jotka kiinnittävät jokaisen sivuluokan. Vain ykkösalkio kuuluu ytimeen ja kuvaus $\phi$ on injektio. Tästä seuraa ensimmäisen isomorfialauseen perusteella

$$G \cong G/\{1\} \cong G/Ker\phi \cong Im\phi \leq S_n.$$

□

Yksi tämän kurssin kannalta tärkeä sovellutus rata-vakauttajalauseelle on Cauchyn lause. Tämä on osittainen käänteistulos Lagrangen lauseelle.

**Lause 3.5** (Cauchyn lause)**.** *Jos alkukulu $p$ jakaa ryhmän kertaluvun $|G|$, silloin $G$ sisältää alkion, jonka kertaluku on $p$.*

*Todistus.* Määritellään $\Omega = \{(x_1, \ldots, x_p) : x_i \in G \text{ ja } x_1 x_2 \ldots x_p = 1\}$. Olkoon $H = \langle\sigma\rangle \cong C_p$, missä $\sigma$ toimii $\Omega$:ssa

$$\sigma : (x_1, \ldots, x_p) \to (x_2, \ldots, x_p, x_1).$$

Rata-vakauttajalause sanoo, että $H$-radan mahtavuus jakaa $H$:n kertaluvun. Näin ollen $H$-radan mahtavuus on joko 1 tai $p$. Lisäksi $|\Omega| = |G|^{p-1}$, koska ensimmäiset $p-1$ alkiota voidaan valita vapaasti. Koska $p$ jakaa $|G|$:n, jakaa $p$ myös $|\Omega|$:n. Siispä $\Omega$ on $H$-ratojen pistevieras unioni, ja kukin radoista on joko kokoa $p$ tai 1. Huomaa, että $(1, 1, \ldots, 1)$ muodostaa oman ratansa, joten ainakin yksi rata on mahtavuutta yksi. Olkoon kokoa yksi olevien ratojen määrä $a$ ja kokoa $p$ olevien ratojen lukumäärä $b$. Silloin $|\Omega| = a \cdot 1 + b \cdot p$. Koska $p$ jakaa $|\Omega|$:n, jakaa $p$ myös $a$:n. Niinpä on olemassa ainakin $p$ rataa, joiden koko on 1. Jotta $\alpha$:n rata olisi kokoa 1, täytyy olla niin, että $x_1 = x_2 = \cdots = x_p \neq 1$. Mutta $x_1 x_2 \cdots x_p = 1$, joten $x_1^p = 1$ ja $x_1$:n kertaluku on $p$. □

Nyt siirrytään käsittelemään mielivaltaisen joukon $\Omega$ tilalla rengasta $R$. Toisin sanoen vaaditaan kohdejoukolta enemmän algebrallista rakennetta.

**Määritelmä 3.6.** Ryhmä $G$ toimii renkaassa $R$, jos jokainen $g$ antaa rengasautomorfismin $g : R \longrightarrow R$, joka lähettää $a \mapsto g(a)$, ja kaikille $a \in R$ ja $g, h \in G$ pätee $h(g(a)) = (hg)(a)$.

Rengasautomorfismi on bijektiivinen rengashomomorfismi. Ryhmän toiminta renkaassa määrittää alirenkaita ja alikuntia.

**Lemma 3.7.** *Olkoon $G$ ryhmä, joka toimii renkaassa $R$. Silloin*

1. *Merkitään $R^G = \{a \in R : g(a) = a \forall g \in G\}$. Silloin $R^G$ on $R$:n alirengas. Tätä renkasta kutsutaan kiintorenkaaksi.*
2. *Jos $R = K$ on kunta, silloin $g(1) = 1$ kaikille $g \in G$ ja jos $a \neq 0$, silloin $g(a^{-1}) = (g(a))^{-1}$.*
3. *Jos $R = K$ on kunta, silloin $K^G$ on alikunta, joka sisältää jonkun $K$:n alkukunnan.*

**Lemma 3.8** (Lause 10.2. Häsä)**.** *Alkukunta on kunnan yksikäsitteinen minimaalinen alikunta. Jos kunnan karakteristika on p, al- kukunta on isomorfinen äärellisen kunnan $\mathbb{F}_p$ kanssa. Jos karakteristika on nolla, alkukunta on isomorfinen rationaalilukujen kunnan $\mathbb{Q}$ kanssa.*

*Todistus.* Jos $K$ on kunta, mikä tahansa alikunta sisältää kaikki ykkösalkion monikerrat. Jos karakteristika on $p > 0$ ykkösalkion monikerrat muodostavat kunnan $\mathbb{F}_p$. Jos $K$:n karakte- ristika on 0, niin ykkösalkion monikerrat muodostavat rakenteen, joka on isomorfinen renkaan $\mathbb{Z}$ kanssa. Jokainen $K$:n alikunta sisältää paitsi nämä monikerrat, myös niiden käänteisalkiot. Täten alikunnan täytyy sisältää $\mathbb{Z}$:n osamääräkunta $\mathbb{Q}$. □

*Todistus.* 1) Alirengastestin perusteella. 2) koska $g(1) = g(1^2) = g(1)g(1)$, tästä seuraa $g(1) = 1$. Näin ollen $1 = g(1) = g(aa^{-1}) = g(a)g(a^{-1})$ 3) Olkoon $a \in K^G$, silloin $g(a^{-1}) = g(a)^{-1} = a^{-1}$, joten $a^{-1} \in K^G$. Lisäksi $1 \in K^G$, ja koska alkukunta koostuu kaikista alkioista, joiden summat ovat ovat 1:n osamääriä, tästä seuraa, että alkukunta kuuluu kiintokuntaan. □

## 3.1 Symmetriset polynomit

Olkoon $K$ kunta. Tarkastellaan polynomirengasta

$$R = K[x_1, \ldots, x_n],$$

eli $n$:n muuttujan polynomeja. Tämäkin polynomirengas on kokonaisalue. Edellinen todistus pätee suoraan, sillä muuttujia voidaan lisätä kuntaan yksi kerrallaan iteroiden. Symmetrinen ryhmä $S_n$ toimii renkaassa $R$ permutoiden renkaan muuttujia. Jos siis $f(x_1, \ldots x_n)$ on polynomi ja $\sigma \in S_n$ on permutaatio, toiminta määritellään $f^\sigma(x_1, \ldots, x_n) = f(x_{\sigma 1}, \ldots, x_{\sigma n})$. Tämä on vasen toiminta. Perinteisesti symmetrinen ryhmän alkio $\sigma \in S_n$ toimii joukossa $\{1, \ldots, n\}$ oikealta. Tähän on syynä mm. symmetrisen ryhmän alkioitten sykliesitys ja syklien kertolasku, mutta tällä kurssilla yritän pitäytyä vasemmassa toiminnassa.

**Määritelmä 3.9.** Symmetristen polynomien rengas on kiintorengas $K[x_1, \ldots, x_n]^{S_n}$.

Symmetristen polynomien renkaaseen kuuluvat siis täsmälleen ne polynomit, joissa voidaan vaihtaa minkä tahansa muuttujien paikkaa ja saada edelleen sama polynomi.

Tarkastellaan muutamia selvästikin symmetrisiä polynomeja:

$$\begin{aligned} s_1 &= \sum_i x_i \\ s_2 &= \sum_{i<j} x_i x_j \\ s_3 &= \sum_{i<j<k} x_i x_j x_k \\ &\vdots \\ s_n &= x_1 \dots x_n \end{aligned}$$

Näitä kutsutaan alkeellisiksi symmetrisiksi polynomeiksi.

**Lause 3.10.** *Symmetristen polynomien renkaalla $K[x_1, \dots, x_n]^{S_n}$ on seuraava rakenne*

$$K[x_1, \dots, x_n]^{S_n} = K[s_1, \dots, s_n].$$

*Toisin sanoen, jokainen symmetrinen polynomi $f \in K[x_1, \dots, x_n]^{S_n}$ voidaan yksikäsitteisesti esittää alkeellisten symmetristen polynomien polynomina.*

*Todistus.* Annetaan monomeille sanakirjajärjestys, eli sanotaan monomia $x_1^{a_1} \dots x_n^{a_n}$ suuremmaksi kuin monomia $x_1^{b_1} \dots x_n^{b_n}$, jos $a_1 > b_1$ tai $a_1 = b_1$ ja $a_2 > b_2$ jne.

Olkoon $f \in K[x_1, \dots, x_n]^{S_n}$, ja olkoon monomi $\prod_i x_i^{a_i}$ suurin sanakirjajärjestyksessä. Koska $f$ on symmetrinen ja $\prod_i x_i^{a_i}$ on suurin monomi, väistämättä $a_1 \geq a_2 \geq \cdots \geq a_n$. Huomataan, että $\prod_i x_i^{a_i}$ on suurin monomitermi alkeellisten symmetristen polynomien tulossa $\prod_i s_i^{a_i - a_{i+1}}$, joten on olemassa joku $c \in K$, jolle

$$g = f - c \prod_i s_i^{a_i - a_{i+1}} \in K[x_1, \dots, x_n]^{S_n}.$$

Huomataan, että $g$:n suurin termi on pienempi kuin $f$:n suurin termi. Joten toistetaan prosessi $g$:lle. Näin ollen $f$ voidaan kirjoittaa $s_i$:n polynomina ja kyseinen esitys on yksikäsitteinen. □

**Esimerkki 3.11.** Polynomi $\sum_i x_i^2$ on selvästikin symmetrinen, mutta se ei ole alkeellinen symmetrinen polynomi. Alkeellisten symmetristen polynomien avulla se voidaan esittää muodossa $\sum_i x_i^2 = s_1^2 - 2s_2$.

**Propositio 3.12.** *Oletetaan, että $K$:n karakteristika ei ole 2, ja olkoon $f \in K[x]$. Merkitään $f$:n juuria $\alpha_1, \dots, \alpha_n$.*

1. *Muuttujien/juurien $\alpha_1, \dots, \alpha_n$ diskriminantti*

$$\Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2,$$

*on symmetrinen polynomi.*

2. *Diskriminantin neliöjuuri*

$$\delta = \prod_{i<i}(\alpha_i - \alpha_j)$$

*puolestaan ei ole symmetrinen, mutta se on kuitenkin invariantti alternoivan ryhmän $A_n \leq S_n$ toiminnossa.*

3. $\Delta(f) = 0$ *jos ja vain jos $f$:llä on moninkertainen nollakohta.*

*Todistus.* 1) selvä. 2) havaitaan, että transpositio $(ii+1) \in S_n$ kertoo $\delta$:n -1:llä. Joten $\delta$ ei säily muuttumattomana $S_n$:n toiminnossa. Jos näitä transpositioita on kuitenkin parillinen määrä, se on invariantti. Transpositioiden parilliset tulos virittävät ryhmän $A_n$. 3) selvä, sillä $\alpha_i$:t ovat polynomin juuria. □

**Esimerkki 3.13.** Olkoon $f = (x-\alpha_1)(x-\alpha_2) = x^2 - s_1x + s_2$. silloin kahden muuttujan/juuren tapauksessa, diskriminantti on

$$\Delta = (\alpha_1 - \alpha_2)^2 = s_1^2 - 4s_2,$$

joka siis esiintyy muodossa $b^2 - 4ac$ toisen asteen yhtälön ratkaisukaavassa.

Olkoon $K$ kunta, jonka karakteristika ei ole 2,3 ja $f$ jaoton kolmannen asteen yhtälö.

Kukin kolmannen asteen yhtälö voidaan redusoida muotoon $g(x) = x^3 + px + q$ ja tästä seuraa, että diskriminantti on $\Delta = -4p^3 - 27q^2$. Merkitään yhtälön ratkaisuja ovat $\alpha_1, \alpha_2, \alpha_3$ ja olkoon $\omega$ on primitiivinen kolmas ykkösenjuuri.

Asetetaan

$$\beta = \alpha_1 + \omega\alpha_2 + \omega\alpha_3,$$
$$\gamma = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3.$$

Silloin

$$\begin{aligned}\beta\gamma &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + (\omega + \omega^2)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\ &= (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = -3p,\end{aligned}$$

joten $\beta^3\gamma^3 = -27p^3$.

Nyt

$$\begin{aligned}\beta^3 + \gamma^3 &= (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)^3 + (\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3)^3 + (\alpha_1 + \alpha_2 + \alpha_3)^3 \\ &= 3(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) + 18\alpha_1\alpha_2\alpha_3.\end{aligned}$$

Mutta $\alpha_i^3 = -p\alpha_i - q$ (yhtälön nojalla) ja näin ollen $\alpha_1^3 + \alpha_2^3 + \alpha_3^3 = -3q$ (koska $x^2$ kerroin on 0), ja siis $\beta^3 + \gamma^3 = -27q$. Joten $\beta^3$ ja $\gamma^3$ ovat

yhtälön $x^2+27qx-27p^3 = 0$ juuria, joka toisen asteen yhtälönä voidaan ratkaista muodossa

$$-\frac{27}{2}q \pm \frac{3\sqrt{-3}}{2}(-27q^2 - 4p^3)^{\frac{1}{2}} = -\frac{27}{2}q \pm \frac{3\sqrt{-3}}{2}\sqrt{D}.$$

Joten saadaan ratkaisu $\beta^3$ ja $\gamma^3$:lle kunnassa $K(\sqrt{-3D})$, ja $\beta$ saadaan ratkaisemalla $\beta^3$:n kuutiojuuri. Tämän lisäksi $\gamma = -3p/\beta$, saadaan ylläolevasta yhtälöstä $\beta\gamma$. Lopulta voidaan kirjoittaa $\alpha_1 = \frac{1}{3}(\beta + \gamma), \alpha_2 = \frac{1}{3}(\omega^2\beta + \omega\gamma), \alpha_3 = \frac{1}{3}(\omega\beta + \omega^2\gamma)$.

# 4 Kuntalaajennokset

Kerrataan kuntalaajennosten teoriaa.

**Määritelmä 4.1.** Kuntalaajennos $M/K$ on yksinkertaisesti injektio

$$f : K \longrightarrow M,$$

tai sitten voidaan ajatella $K$:ta $M$:n alikuntana.

Myöhemmin myös käytetään diagrammia

Kuntalaajennoksia voidaan ajatella myös vektoriavaruuksina, ja näin ollen niille voidaan antaa kanta. Tarkemmin sanoen, olkoon $K \leq L$ kuntalaajennos. Kunnan $L$ alkioita voidaan tarkastella vektoreina, ja kunnan $K$ alkioita skalaareina. Määritellään skalaaritulo $a \in K, \beta \in L$ olemaan $a\beta := a\beta$, jossa jälkimmäinen kertolasku tapahtuu kunnassa $L$. Näin $L$ on vektoriavaruus kunnan $K$ yli.

**Määritelmä 4.2.** Laajennoksen *aste*, jota merkitään $[L : K]$, on $L$:n dimensio vektoriavaruutena kunnan $K$ yli, jos tämä on äärellinen. Muuten määritellään asteeksi ääretön.

**Propositio 4.3** (Torni-lemma)**.** *Jos $L/M/K$ ovat kuntalaajennoksia (äärellisiä tai äärettömiä), silloin*

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

**Määritelmä 4.4.** Olkoon $L/K$ kuntalaajennos, ja olkoon $\alpha \in L$. Kutsumme alkiota $\alpha$ algebralliseksi kunnan $K$ yli, jos on olemassa sellainen nollasta poikkeava $f \in K[x]$, jolle $f(\alpha) = 0$ kunnassa $L$. Jos tämä kirjoitetaan auki, on olemassa $a_0, \ldots, a_n \in K$, jolle pätee $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$.

Jos $\alpha \in L$ on algebrallinen kunnan $K$ yli, sen minimipolynomi $m_\alpha \in K[x]$ on yksikäsitteinen, pienintä mahdollista astetta oleva pääpolynomi, jolle pätee $m_\alpha(\alpha) = 0$. Tämä polynomi on aina jaoton, ja jos

jollekin muulle $f \in K[x]$ pätee $f(\alpha) = 0$ silloin $m_\alpha$ jakaa polynomin $f$ renkaassa $K[x]$.

Kuntalaajennosta $M/K$ kutsutaan algebralliseksi, jos jokainen alkio $a \in M$ on algebrallinen kunnan $K$ yli. Muussa tapauksessa laajennosta kutsutaan transkendenttiseksi.

Alkion algebrallisuus tai transkendenttisuus riippuu kunnasta, esimerkiksi $2\pi i$ on algebrallinen kunnan $\mathbb{R}$ yli, mutta transkendentti kunnan $\mathbb{Q}$ yli.

**Määritelmä 4.5** (Määritelmä 14.7. Häsä)**.** Kunta $K$ on algebrallisesti suljettu, jos jokaisen polynomi $f \in K[x]$ kaikki juuret kuuluvat kuntaan $K$, toisin sanoen, polynomi $f$ jakautuu ensimmäisen asteen tek?öihin renkaassa $K[X]$.

**Määritelmä 4.6** (Määritelmä 14.9. Häsä)**.** Kunnan $K$ laajennosta $L$ nimitetään $K$:n algebralliseksi sulkeumaksi, jos se on algebrallisesti suljettu ja algebrallinen $K$:n suhteen.

Kunnan algebrallinen sulkeuma on pienin algebrallisesti suljettu kunta, joka sisältää alkuperäisen kunnan. Jos nimittäin algebrallisesta sulkeumasta poistaa yhdenkin alkion, poistuu samalla jonkin polynomin juuri, koska jokainen sulkeu- man alkio on algebrallinen. Toisaalta algebrallinen sulkeuma on algebrallisista laajennoksista suurin, koska se on algebrallisesti suljettu.

**Lemma 4.7.** *Jos $M/K$ ovat kuntia, ja $[M : K] = n$, silloin jokainen alkio $a \in M$ on algebrallinen kunnan $K$ yli.*

*Todistus.* Tarkastellaan alkioita $1, a, \ldots, a^n$ kunnassa $M$. Nämä ovat $n+1$ alkiota $n$ ulotteisessa vaktoriavaruudessa $M$ kunnan $K$ yli, niinpä ne ovat lineaarisesti riippuvaisia $K$:n yli, joten on olemassa $u_0, \ldots, u_n$, jotka eivät kaikki ole 0, joille $u_0 1 + u_1 a + \cdots + u_n a^n = 0$, ja tässä $a$:n toteuttama polynomiyhtälö. □

Jokainen äärellinen laajennos on siis algebrallinen, mutta jokainen algebrallinen laajennos ei ole äärellinen. Esimerkkinä algebrallinen sulkeuma.

**Määritelmä 4.8** (Yksinkertainen laajennos)**.** Olkoon $M/K$ laajennos, ja $a \in M$, silloin $K$:n laajennosta, jonka virittäjä on $a$, merkitään $K(a)$, on pienin $M$:n alikunta, joka sisältää $K$:n ja $a$:n, kutsutaan yksinkertaiseksi laajennokseksi. Yleisemmin, jos $S$ on $M$:n osajoukko, kunta $K(S)$ on pienin alikunta, joka sisältää $K$:n ja $S$:n.

**Esimerkki 4.9.** 1. Olkoon $K$ kunta ja $K(t)$ polynomirenkaan $K[t]$ jakokunta. Silloin $K(t)$ on $K$:n yksinkertainen transkendentti laajennos.

2. $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$ on $\mathbb{Q}$:n yksinkertainen algebrallinen laajennos, jonka virittää alkio $\sqrt{2} + i$.

**Lause 4.10** (Yksinkertaisten laajennosten olemassaolo)**.** *1. Olkoon $K$ kunta ja $m \in K[x]$ jaoton pääpolynomi, silloin on olemassa kuntalaajennos $M/K$, jolla on seuraavat ominaisuudet*

*(a) $M = K(\alpha)$, jollekin $\alpha \in M$.*

*(b) $\alpha \in M$ minimipolynomi on täsmälleen $m$.*

*(c) $[M : K] = \deg m$*

*2. Olkoon $L/K$ ja $\alpha \in L$ algebrallinen $K$:n yli, silloin yksinkertainen laajennos $K(\alpha)/K$, kunnan $L$ alikuntana on isomorfinen kohdassa (1) minimipolynomin avulla konstruoidun laajennoksen kanssa.*

*Todistus.* (1) Koska $m$ on jaoton pääpolynomi, muodostaa $(m)$ maksimaalisen ideaalin renkaassa $K[x]$, silloin tekijärengas

$$M = K[x]/(m)$$

on kunta. Olkoon $\alpha \in M$ muuttujan $x$ kuva kunnassa $M$. Selvästikin jokainen $M$ alkio voidaan esittää $\alpha$:n polynomina, jonka kertoimet ovat $K$:ssa ja näin ollen $M = K(\alpha)$. Huomataan myös, että $m \in K[x]$ kuvautuu $0 \in M$, joten $m(\alpha) = 0$ kunnassa $M$. Määritelmän mukaan minimipolynomi $m_\alpha$ jakaa $m$:n renkaassa $K[x]$, mutta koska $m$ oli jaoton, väistämättä $m = m_\alpha$. Lopuksi, olkoon $m = x^d +$pienet termit $\in K[x]$. Silloin $\{1, x, x^2, \ldots, x^{d-1}\}$ on $M$:n kanta $K$:n yli.

(2) Jos $\alpha \in L$ on algebrallinen, silloin sillä on minimipolynomi $m_\alpha$. Nyt voidaan määritellä kuntahomomorfismi

$$K[x]/(m_\alpha) \longrightarrow L$$

kuvaamalla $f(x) \mapsto f(\alpha)$. Tämä on hyvinmääritelty, sillä $m_\alpha(\alpha) = 0$. Joten $M \longrightarrow L$ ja sen kuva on täsmälleen $K(\alpha)$, joten $M \cong K(\alpha)$. □

**Esimerkki 4.11.** 1. $\mathbb{R}(i) = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{C}$. Edellisessä merkintätavassa $(K = \mathbb{R}, L = \mathbb{C}, \alpha = i)$. Tälle pätee $i^2 + 1 = 0$, joten $x^2 + 1$ on minimipolynomi.

2. $K = \mathbb{Q}$, $L = \mathbb{R}$, $\alpha = \sqrt{2}$, minimipolynomi on $x^2 - 2$, sen aste on 2, joten $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

3. $K = \mathbb{Q}, L = \mathbb{R}, \alpha = 2^{1/4}$. Minimipolynomi on $x^4 - 2$, tämä on jaoton, joten $\mathbb{Q}(2^{1/4}) = \{b_0 + b_1 2^{1/4} + b_2 2^{1/2} + b_3 2^{3/4} : b_i \in \mathbb{Q}\}$.

4. $K = \mathbb{Q}, L = \mathbb{C}, \alpha = \omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$, eli $\omega$ toteuttaa yhtälön $x^3 - 1 = 0$. Mutta tämä yhtälö ei ole minimipolynomi, sillä sen

voi hajottaa $(x-1)(x^2+x+1)$, jonka kumpikin osa on jaottomia. Koska $\omega$ on polynomin $x^2+x+1$ juuri, on tämä $\omega$:n minimipolynomi. Siispä $\mathbb{Q}(\omega) = \{a+b\omega : a,b \in \mathbb{Q}\} = \{a+b\frac{-1\pm i\sqrt{3}}{2} : a,b \in \mathbb{Q}\} = \{c+di\sqrt{3} : c,d \in \mathbb{Q}\} = \mathbb{Q}(i\sqrt{3})$, jolla on minimipolynomi $x^2+3$.

5. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ kunnan $\mathbb{Q}$ yli on astetta 4.
6. $\mathbb{Q}(\sqrt{2},i) = \mathbb{Q}(\sqrt{2}+i)$.

Osoitetaan, että $\mathbb{Q}(\sqrt{2},\sqrt{3}) = (\mathbb{Q}(\sqrt{2})(\sqrt{3})$.

$[\mathbb{Q}(\sqrt{2},\sqrt{3} : \mathbb{Q}(\sqrt{2})]$ on $\sqrt{3}$:n minimipolynomin aste yli kunnan $\mathbb{Q}(\sqrt{2})$.

Kunnan $\mathbb{Q}$ yli $\sqrt{3}$:n minimipolynomi on $x^2-3$, ja sama toimii kunnassa $\mathbb{Q}(\sqrt{2})$, pitää vain tarkastaa, että tämä on minimipolynomi. Aste on 2, joten ainoa parannus voisi olla, jos löytäisimme lineaarisen polynominen $\mathbb{Q}(\sqrt{2})$:n yli. Silloin $\sqrt{3} = a+b\sqrt{2}$ ja $a,b \in \mathbb{Q}$.

Nyt

$$3 = a^2 + 2b^2 + 2ab\sqrt{2}$$

, mutta koska $1, \sqrt{2}$ ovat lineaarisesti riippumattomia yli kunnan $\mathbb{Q}$, muodostavat ne kannan kunnalle $\mathbb{Q}(\sqrt{2})$. Näin ollen $ab = 0$ josta seuraa, että $a = 0$ tai $b = 0$.

Jos $b = 0$, silloin $a^2 = 3$, mutta $a \in \mathbb{Q}$ ristiriita. Samoin, jos $a = 0$, silloin $2b^2 = 3$, mutta $b \in \mathbb{Q}$, taas ristiriita. Joten $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ ja näin ollen sen minimipolynomin aste yli kunnan $\mathbb{Q}(\sqrt{2})$ on 2.

Torni-lemman perusteella

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3} : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Todistetaan myös yksinkertaisten laajennosten yksikäsitteisyys. Sitä varten tarvitaan aputulos.

**Lause 4.12.** *Olkoon $M/K$ kuntalaajennos, $\alpha \in M$ algebrallinen kunnan $K$ yli, ja $m_\alpha$ sen minimipolynomi. Olkoon $i : K \longrightarrow L$ kuntahomomorfismi ja $\beta \in L$, silloin on olmeassa homomorfismi $j : K(\alpha) \longrightarrow L$, jolle pätee*

$$j|_K = i$$
$$j(\alpha) = \beta$$

*jos ja vain jos $i(m_\alpha(\beta)) = 0$, missä $i(m_\alpha) \in L[x]$ on $m_\alpha \in K[x]$:n kuva kuvauksessa $i$.*

*Todistus.* Oletetaan, että tällainen $j$ on olemassa, silloin

$$i(m_\alpha(\beta)) = j(m_\alpha)(j(\alpha)) = j(m_\alpha(\alpha)) = 0.$$

Siis $\beta = j(\alpha)$ on minimipolynomin juuri, kuten vaadittua.

Toiseen suuntaan, olkoon $i(m_\alpha(\beta)) = 0$. Ja merkitään $\tilde{K} = i(K) \subseteq L$. Silloin $i(m_\alpha) \in \tilde{K}[x]$ on jaoton pääpolynomi, eli $\beta$:n minimipolynomi kunnan $\tilde{K}$ yli. Edellisen lauseen perusteella

$$K(\alpha) \cong K[x]/(m_\alpha),$$

ja

$$\tilde{K}(\beta) \cong \tilde{K}[x]/i(m_\alpha).$$

Nyt voidaan kosntruoida kuvaus $j$ seuraavana kompositiona:

$$K(\alpha) \cong K[x]/(m_\alpha) \longrightarrow \tilde{K}[x]/i(m_\alpha) \cong \tilde{K}(\beta) \subset L.$$

Tämä on kuntahomomorfismi $j : K(\alpha) \longrightarrow L$, joka toteuttaa $j|_K = i$ ja $j(\alpha) = \beta$. □

**Korollaari 4.13** (Yksinkertaisesten laajennosten yksikäsitteisyys)**.** *Oletetaan, että $M/K$ on kuntalaajennos, ja $\alpha, \beta \in M$ ovat algebrallisia kunnan $K$ yli, ja niillä on sama minimipolynomi $m \in K[x]$. Silloin on olemassa isomorfismi $j : K(\alpha) \longrightarrow K(\beta)$, jolle $j_K = Id$.*

*Todistus.* Edellisessä lauseessa otetaan $i = Id_K$ ja $L = K(\beta)$, silloin saadaan kommutatiivinen kaavio

ja $j$ on olemassa, sillä $m(\beta) = 0$. Nyt $j : K(\alpha) \longrightarrow K(\beta)$ on injektio ja tornilemman perusteella

$$[K(\beta) : j(K(\alpha))][K(\alpha) : K] = [K(\beta) : K]$$

ja näin ollen $K(\alpha) = K(\beta)$. □

Tästä seuraa myös

**Korollaari 4.14** (Yksinkertaisten laajennosten homomorfismit)**.** *Olkoon $K(\alpha)/K$ yksinkertainen laajennos, jonka minimipolynomi on $m_\alpha$ kunnan $K$ yli. Olkoon $i : K \longrightarrow L$ homomorfismi. Oletetaan, että polynomilla $i(m_\alpha) \in L[x]$ on täsmälleen $k$ erillistä juurta $\{\beta_i\}$ kunnassa $L$. Silloin on olemassa täsmälleen $k$ erillistä homomorfismia $j_m : K(\alpha) \longrightarrow L$, joille $j_m|_K = i$ ja jotka erottaa kuva $j_m(\alpha) = \beta_m$ kaikille $m \leq k$.*

**Esimerkki 4.15.** 1. Olkoon $K = \mathbb{Q}$ ja $M = \mathbb{C}$, ja $\alpha = i$, silloin $m_\alpha = x^2 + 1$. Jos $L = \mathbb{Q}(i)$ ja $\beta = -i$, silloin $i(m_\alpha) = x^2 + 1$ ja näin ollen $i(m_\alpha)(\beta) = 0$. Joten on olemassa kuntahomomorfismi $j : \mathbb{Q}(i) \longrightarrow \mathbb{Q}(i)$ jolle $i \mapsto -i$. Tämä on itseasiassa Galois'n automorfismi.

2. Olkoon $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$,$\alpha = \sqrt{2}$,$m_\alpha = x^2 - 2$ ja $\beta = \pm i$. Voidaanko homomorfismia $i$ laajentaa $K(\sqrt{2})$? Ei, sillä $i(m_\alpha(\pm i)) = (\pm i)^2 - 2 \neq 0$.

**Lause 4.16.** *Olkoon $M/K$ kuntalaajennos, silloin $M$:n algebralliset alkiot muodostavat $M$:n alikunnan.*

*Todistus.* Olkoot $a, b \in M$ algebrallisia kunnan $K$ yli. Osoitetaan, että $a \pm b$, $ab$ ja $a^{-1}$ $(a \neq 0)$ ovat algebrallisia.

Koska $a$ on algebrallinen, $[K(a) : K]$=n, ja koska $b$ on algebrallinen $K$:n yli, on se algebrallinen myös kunnan $K(a)$ yli. Näin ollen

$$[K(a, b) : K] \leq [K(a) : K][K(b) : K].$$

Toisaalta, jokainen $K(a, b)$:n alkio on algebrallinen $K$:n yli, ja $a \pm b$, $ab$ ja $a^{-1} \in K(a, b)$, joten ne ovat algebrallisia $K$:n yli. Näin ollen algebralliset alkiot muodostavat alikunnan. Lemman ??? perusteella. □

**Lause 4.17.** *Olkoon $M/L/K$ torni kuntalaajennoksia. Jos $M$ on algebrallinen $L$:n yli ja $L$ on algebrallinen $K$:n yli, myös $M$ on algebrallinen $K$:n yli.*

*Todistus.* Todistetaan, että $\alpha \in M$ toteuttaa polynomiyhtälön, jonka kertoimet ovat kunnassa $K$. Koska $\alpha \in M$ on algebrallinen $L$:n yli, on olemassa polynomi $f(x) \in L[x]$, jolle $f(\alpha) = 0$, olkoon

$$f(x) = a_0 + a_1 x + \cdots + a_r x^r, a_i \in L,$$

ja jokainen $a_i \in L$ on algebrallinen kunnan $K$ yli. Jokaisella $a_i$:lla on minimipolynomi $q_i(x)$, astetta $m_i$, eli $[K(a_i) : K] = m_i$.

Tarkastellaan $E = K(a_0, \ldots, a_r)$, silloin $[E : K] \leq m_0 \ldots m_r$, eli laajennos on äärellinen. Nyt on konstruoitu kunta $E$, jonka yli $\alpha$ toteuttaa polynomiyhtälön $f(x)$, joten $\alpha$ on algebrallinen $E$:n yli, ja $[E(\alpha) : E]$ on äärellinen, tässä on torni laajennoksia $E(\alpha) \geq E \geq K$, joten tornilemman perusteella

$$[E(\alpha) : K] = [E(\alpha) : E][E : K] < \infty,$$

siispä $E(\alpha)$:n alkiot ovat algebrallisia $K$:n yli, $\alpha$ on algebrallinen $K$:n yli ja näin ollen $M$ on algebrallinen $K$:n yli, koska $\alpha$ oli $M$:n mielivaltainen alkio.

□

# 5 Juurikunnat

Olkoon $K$ kunta, ja $f \in K[x]$ pääpolynomi. Sanotaan, että $f$ hajoaa (täysin) kunnan $K$ yli, jos

$$f(x) = \prod_{i=1}^{n}(x - a_i) \in K[x].$$

Algebran peruslauseen nojalla, mikä tahansa reaalipolynomi hajoaa lineaariksiksi tekijöiksi kompleksilukujen kunnan yli. Joten kompleksilukujen kunnan yli myös mikä tahansa rationaalipolynomi hajoaa.

Jaottomuus riippuu kunnasta! Esimerkiksi $x^2-2$ on jaoton kunnassa $\mathbb{Q}$, kun taas kunnassa $\mathbb{R}$ se hajoaa tuloksi $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$. Polynomi $x^2 + 1$ on jaoton kunnassa $\mathbb{Q}$ tai $\mathbb{R}$, mutta hajoaa kunnassa $\mathbb{C}$ kahden tuloksi $x^2 + 1 = (x - i)(x + i)$. Palaamme tähän asiaan parin luennon päästä, kun puhumme kuntalaajennosten teoriasta. Algebran peruslauseen nojalla tiedämme, että epävakio polynomi $f \in \mathbb{C}[x]$ hajoaa aina äärelliseksi tuloksi lineaarisia tekijöitä. Aina ei kuitenkaan tarvitse mennä kompleksilukujen kuntaan $\mathbb{C}$ saakka, jotta saamme polynomin hajoamaan lineaarisiksi tekijöiksi. Esimerkiksi kunta $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ on kunta, se on reaalilukujen $\mathbb{R}$ pienen alikunta, jossa $f(x) = x^2 - 2$ voidaan kirjoittaa lineaaristen polynomien tulona.

Samalla lailla $\{a + bi : a, b \in \mathbb{Q}\}$ on pienin kompleksilukujen $\mathbb{C}$ alikunta, jossa $x^2 + 1$ hajoaa lineaarisiksi tekijöiksi.

Triviaalisti, jaoton polynomi kunnan $K$ yli, jonka aste on vähintään kaksi, ei hajoa kunnassa $K$.

**Määritelmä 5.1.** Olkoon $K$ kunta, ja $f \in K[x]$. Kuntalaajennos $M/K$ on polynomin $f$ hajoamiskunta, jos

1. $f \in M[x]$ hajoaa kunnan $M$ yli
2. jos $K \subset L \subseteq M$ silloin $f \in L[x]$ ei hajoa kunnassa $L$.

Esimerkiksi $x^2 + 1$ hajoamiskunta on $\mathbb{Q}(i)$, koska $x^2 + 1$ hajoaa tässä kunnassa, ja koska kunnan aste on vain 2, pienempää kuntaa ei ole olemassa.

**Lause 5.2.** *1. Polynomilla $f \in K[x]$ on olemassa hajoamiskunta $M/K$ kunnan $K$ yli*

*2. Olkoon $f \in K[x]$ ja kuntaisomorfismi $i : K \longrightarrow K'$, joka lähettää*

$$f \mapsto i(f) = f' \in K'[x].$$

*Olkoot $M/K$ polynomin $f$ hajoamiskunta, ja $M'/K'$ hajoamiskunta $f'$:lle. Silloin on olemassa isomorfismi $j : M \longrightarrow M'$ joka laajentaa $i : K \longrightarrow K'$*

*Todistus.* Todistetaan väite induktiolla polynomin $f$ asteen suhteen. Kaikki väittämät ovat triviaaleja, jos aste on 1.

1) Induktiohypoteesi: olkoon $K$ mikä tahansa kunta ja $f \in K[x]$, $degf < n$, silloin on olemassa juurikunta $M/K$ polynomille $f$ kunnan $K$ yli.

Olkoon $f \in K[x]$ astetta $n$, ja olkoon $f_1$ joku $f$:n jaoton tekijä. Asetetaan $K_1 = K[x]/(f_1)$. Tämä on $K$:n äärellinen laajennos, joten $K_1[x]$:ssä $f(x) = (x-\alpha)^{m_1} g(x)$. Polynomin $g$ aste on pienempi kuin $f$:n aste, joten induktiohypoteesin perusteella $g$:llä on juurikunta $N/K_1$, ja kunnassa $N$ myös $f$ hajoaa täysin. Otetaan pienin $N$:n alikunta $M$, jossa $f$ hajoaa täysin. Tämä on $f$:n juurikunta.

2) Induktiohypoteesi: olkoot $i : K \cong K'$ kaksi kuntaa, $f \in K[x]$ polynomi, jonka aste on pienempi kuin $n$, tällöin $f$:n ja $i(f)$:n juurikunnat yli $K$ ja $K'$:n ovat isomorfiset.

Valitaan satunnainen $f \in K[x]$, jonka aste on $n$. Olkoon $M/K$ polynomin $f$ juurikunta $K$:n yli, ja olkoon $\alpha_1 \in M$ polynomin $f$ juuri. Merkitään $\alpha_1$:n minimipolynomia $m$. Nyt $f(\alpha_1) = 0$, joten $m \mid f$ renkaassa $K[x]$. Kun taas $m' = i(m) \in K'[x]$ ja $m'$ on jaoton renkaassa $K'[x]$, joten samalla tavalla $m' \mid f'$ renkaassa $K'[x]$, joten $m'$ hajoaa $f'$:n juurikunnassa $M'$ yli $K'$:n. Olkoon $\beta_1 \in M'$ polynomin $m'$ juuri. Yksinkertaisten laajennosten isomorfian perusteella $K(\alpha_1$ ja $K(\beta_1)$ ovat isomorfisia keskenään, koska ne vastaavat minimipolynomeja $m$ ja $m' = i(m)$.

Nyt $M$ on polynomin $f/(x - \alpha_1)$ juurikunta kunnan $K(\alpha_1)$ yli, ja $M'$ on juurikunta polynomille $f'/(x - \beta_1)$ yli isomorfisen kunnan $K(\beta_1)$. Induktion nojalla, on olemassa isomorfismi $M \cong M'$, joka laajentaa isomorfismia $K(\alpha_1) \cong K'(\beta_1)$ joka puolestaan laajensi isomorfismia $K \cong K'$.

□

## 5.1 Normaalit laajennokset

**Määritelmä 5.3.** Kuntalaajennosta $L/K$ kutsutaan normaaliksi, jos jokainen jaoton polynomi $f \in K[x]$, jolla on yksi juuri $a \in L$, hajoaa kunnassa $L$.

**Esimerkki 5.4.** Olkoon $K = \mathbb{Q}$. Tarkastellaan polynomia $x^3 - 2$, ja kuntalaajennosta $L = \mathbb{Q}(2^{\frac{1}{3}})$. Laajennos $L$ ei ole normaali.

**Esimerkki 5.5.** Toisen asteen laajennokset $\mathbb{Q}(i)/\mathbb{Q}$ ja $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ovat normaaleja laajennoksia.

**Lause 5.6.** *Äärellinen laajennos $L/K$ on normaali jos ja vain jos se on jonkun polynomin $f \in K[x]$ hajoamiskunta.*

*Todistus.* Oletetaan, että $L/K$ on normaali äärellinen laajennos. Jos $L = K$ mitään ei tarvitse todistaa. Oletetaan siis, että laajennos on aito. Koska se on äärellinen, on olemassa kanta $\alpha_1, \ldots, \alpha_s$ kunnalle $L$ yli kunnan $K$, joten $L = K(\alpha_1, \ldots, \alpha_s)$ ja jokainen $\alpha_i$ on algebrallinen $K$:n yli.

Olkoon $m_i$ kunkin $\alpha_i$:n minimipolynomi, ja konstruoidaan $f = m_1 \ldots m_s$. Koska $L$ on normaali laajennos, jokainen $m_i$ hajoaa $L$:n yli, ja näin ollen $f$ hajoaa $L$:ssä. Koska $L$ on kunnan $K$ ja $f$:n nollakohtien virittämä laajennos, on se $f$:n hajoamiskunta.

Toiseen suuntaan, olkoon $L$ jonkun polynomin $f$ hajoamiskunta $K$:n yli. Laajennos on äärellinen, osoitetaan, että se on normaali.

Otetaan joku jaoton $g$ kunnan $K$ yli, ja oletetaan, että sillä on yksi juuri kunnassa $\theta_1 \in L$.

Olkoon $L \subseteq F$ hajoamiskunta polynomille $fg$ yli $K$:n. Oletetaan, että $\theta_2 \in F$ on toinen $g$:n juuri. Halutaan osoittaa, että $\theta_2 \in L$.

Koska $\theta_1, \theta_2$ toteuttavat jaottoman polynomin $g$ kunnan $K$ yli, silloin $K(\theta_1) \cong K(\theta_2)$ ja $[K(\theta_1) : K] = [K(\theta_2) : K] = d = \deg g$, koska laajennos on yksinkertainen ja niillä on sama minimipolynomi $g$.

Selvästikin $L(\theta_i)$ on $f$:n hajoamiskunta yli $K(\theta_i)$:n, koska $L$ on $f$:n hajoamiskunta yli $K$:n ja $K(\theta_1)$ on isomorfinen $K(\theta_2)$ kanssa, kun isomorfismi lähettää $\theta_1 \mapsto \theta_2$ ja kiinnittää $K$:n.

Hajoamiskunnan yksikäsitteisyyden perusteella, laajennos $L(\theta_1)/K(\theta_1)$:n on isomorfinen laajennoksen $L(\theta_2)/K(\theta_2)$ kanssa. Näin ollen niillä on sama aste, sanotaan $e$.

Koska $\theta_1 \in L$, saadaan $[L(\theta_1) : L] = 1$ ja tornilemman perusteella

$$[L : K] = \frac{[L(\theta_1) : K(\theta_1)][K(\theta_1) : K]}{[L(\theta_1) : L]} = de.$$

Tästä seuraa, että

$$[L(\theta_2) : L] = \frac{[L(\theta_2) : K(\theta_2)][K(\theta_2) : K]}{[L : K]} = \frac{de}{de} = 1,$$

ja siis $\theta_2 \in L$, joten kun yksi $f$:n juuri on kunnassa $L$, silloin mikä tahansa muu juuri on kunnassa $L$ ja näin ollen $L$ on normaali laajennos. □

## 5.2 Separoituvat laajennokset

**Määritelmä 5.7.** Jaotonta polynomia $f \in K[x]$ kutsutaan separoituvaksi, jos sillä on asteensa verran eri juuria hajoamiskunnassaan. Mielivaltainen polynomi $f \in K[x]$ on separoituva, jos kaikki sen jaottomat tekijät ovat separoituvia.

Määritellään polynomin muodollinen derivaatta, $D : K[x] \longrightarrow K[x]$, joka on lineaarikuvaus $K$-vektoriavaruuksien välillä, ja määritellään

$$D(x^n) = nx^{n-1}, \forall n > 0,$$

ja $D(c) = 0$, kaikille $c \in K$

Jaottoman polynomin monikertaiset nollakohdat saadaan selville muodollisen determinantin avulla.

**Lemma 5.8** (Formal derivative)**.** $D(fg) = fD(g) + gD(f)$.

*Todistus.* Koska $D$ on lineaarikuvaus, voidaan redusoida tapaukseen, että $f$ on monomi, tämä on helppo. □

Tästä lähtien kirjoitetaan $D(f)$ sijaan $f'$.

**Lemma 5.9.** *Nollasta eroavalla polynomilla $f \in K[x]$ on moninkertainen juuri juurikunnassaan jos ja vain jos $f$ ja $f'$:lla on yhteinen tekijä, jonka aste on suurempi tai yhtäsuuri kuin 1.*

*Todistus.* Oletetaan, että $\alpha \in L$ on moninkertainen $f$:n juuri sen juurikunnassa $L$, silloin $f = (x-\alpha)^2 g \in L[x]$. Nyt $f' = (x-\alpha)^2 g' + 2(x-\alpha)g$, joten $f$:llä ja $f'$:lla on yhteinen tekijä $(x - \alpha)$ renkaassa $L[x]$ ja näin ollen $f$ ja $f'$:lla on yhteinen tekijä, eli $\alpha$:n minimipolynomi kunnan $K$ yli.

Toiseen suuntaan, oletetaan, että $f$:llä ei ole yhtään moninkertaista juurta juurikunnassaan $L$. Osoitetaan, että $f$:llä ja $f'$:lla ei ole yhteistä tekijää. Oletetaan, että $f = (x - \alpha)g$, missä $(x - \alpha) \not| g$, ja havaitaan, että $f' = (x - \alpha)g' + g$, joten $(x - \alpha) \not| f'$. □

**Määritelmä 5.10.** Olkoon $L/K$ kuntalaajennos, alkio $\alpha \in L$ on separoituva $K$:n yli, jos sen minimipolynomi $m_\alpha \in K[x]$ kunnan $K$ yli on separoituvat polynomi. Kuntalaajennosta $L/K$ kutsutaan separoituvaksi, jos jokainen $\alpha \in L$ on separoituva $K$:n yli.

**Lause 5.11.** *Oletetaan, että $K$:n karakteristika on 0, silloin mikä tahansa $K$:n äärellinen laajennos $L/K$ on separoituva.*

*Todistus.* Olkoon $m \in K[x]$ jonkun $\alpha \in L$ minimipolynomi, oletetaan, että $m$:llä on tuplajuuri jossain juurikunnassa $M \supset K$, silloin $m(\beta) = m'(\beta) = 0$, missä $D$ on formaali derivaatta.

Toisaalta, $m'$ on polynomi, jossa termin $x^{d-1}$ kerroin on erisuuri kuin 0, koska kunnan karakteristika on 0, silloin $m'$ on nollasta eroava polynomi. Koska $m \in K[x]$ on jaoton ja $m'$:lla on pienempi aste, väistämättä $(m, m') = 1$ ja näin on olemassa kaksi polynomia $a, b \in K[x]$, joille $am + bm' = 1$, mutta nyt kun sijoitetaan $\beta$, saadaan ristiriita. □

**Esimerkki 5.12.** Valitaan $K = \mathbb{F}_p(t)$, eli kaikkien rationaalifunktioiden kunta yli äärellisen kunnan $\mathbb{F}_p$. Tarkastellaan polynomia $f(x) = x^p - t \in K[x]$. Olkoon $L/K$ sen juurikunta ja merkitään yhtä juurta $\alpha \in L$, silloin renkaassa $L[x]$, saadaan $(x^p - t) = (x - \alpha)^p$, koska $\alpha \mapsto \alpha^p$ on kuntahomomorfismi kunnassa, jonka karakteristika on $p$ (tehtäväpaperi 1). Ja näin ollen $f$ ei ole separoituva polynomi. Huomaa, että edellinen todistus ei toimi, sillä $f' = px^{p-1} = 0$, koska karakteristika on $p$.

**Propositio 5.13.** *Jos $M/K$ on separoituva, ja $L$ on mikä tahansa välikunta, niin myös laajennokset $M/L$ ja $L/K$ ovat separoituvia.*

*Todistus.* Laajennos $L/K$ on selvästikin separoituva, sillä $\alpha \in L$:n minimipolynomiksi, käy $\alpha \in M$:n minimipolynomista, sillä sen kertoimet ovat $K$:ssa, ja laajennos $M/K$ on separoituva. Toisaalta, $\beta$:n minimipolynomi $m \in L[x]$ jakaa saman alkion minimipolynomin $m' \in K[x]$. Jos $m'$:lla ei ole moninkertaisia juuria juurikunnassaan, ei myöskään $m$:llä ole moninkertaisia juuria juurikunnassaan. □

**Lause 5.14** (Primitiivisen alkion lause)**.** *Olkoon $L/K$ äärellinen separoituva laajennos. Silloin on olemassa alkio $\theta \in L$, jolle $L = K(\theta)$.*

*Todistus.* Koska $L$ on äärellinen laajennos, on se äärellisesti viritetty

$$L = K(\alpha_1, \ldots, \alpha_n).$$

Todistetaan lause induktiolla.

Jos $n = 1$ todistettavaa ei ole. Jos $n > 1$, induktio-oletus kertoo väitteen olevan totta kunnalle $K(\alpha_1, \ldots, \alpha_{n-1})$. Merkitään tätä kuntaa $K(\beta)$, ja $\alpha_n = \alpha$. Riittää siis todistaa väite $L = K(\alpha, \beta)$ ja näin voidaan olettaa, että $n = 2$.

Tässä todistuksessa oletetaan, että $K$ on ääretön. Olkoon $f, g \in K[x]$ alkioitten $\alpha$ ja $\beta$ minimipolynomit. Ja merkitään näitten polynomien juuria $\alpha = \alpha_1, \ldots, \alpha_r$ ja $\beta = \beta_1, \ldots, \beta_s$. Nämä juuret kuuluvat polynomin $fg$ juurikuntaan $M/L$. Koska oletettiin, että laajennos on separoituva, kaikki juuret ovat erisuuria, ja niistä tulee yhteensä $r + s = degf + degg$ eri alkiota kuntaan $M$.

Valitaan $c \in K$ siten, että $\alpha_i + c\beta_j$ ovat eri alkioita kunnassa $M$, tämä on mahdollista, sillä $K$ on ääretön. Asetetaan $\theta = \alpha + c\beta$.

Väite $K(\theta) = L$

Selvästikin $K(\theta) \subset L = K(\alpha, \beta)$, joten riittää osoitettaa, että $\beta \in K(\theta)$. (Koska sitten $\alpha = \theta - c\beta$.)

Määritellään polynomi

$$F(x) := f(\theta - cx) \in K(\theta)[x].$$

Polynomilla on seuraavat ominaisuudet:

1. $F(\beta) = f(\theta - c\beta) = f(\alpha) = 0$.
2. $g(\beta) = 0$ koska $g$ oli $\beta$:n minimipolynomi.
3. $F(\beta_i) = f(\theta - c\beta_i) \neq 0$ kun $i > 1$ koska $\theta - c\beta_i$ ei ole $\alpha_j$.

Siis, $g$:n ja $F$:n ainoa yhteinen juuri on $\beta$. Olkoon $H \in K(\theta)[x]$ polynomien $F$ ja $g$ suurin yhteinen tekijä renkaassa $K(\theta)[x]$. Polynomirengas on pääideaalialue, joten on olemassa polynomit $A, B$, joille $AF + Bg = H$. Tarkastellaan tilannetta $fg$:n juurikunnassa $M$.

1. $g$ hajoaa erillisiksi lineaarisiksi tekijöiksi
2. $H \in M[x]$ hajoaa erillisiksi lineaarisiksi tekijöiksi.
3. $H \mid F$ joten mikä tahansa $H$:n juuri on myös $F$:n ja $g$:n juuri.

Joten $H = X - \beta \in K(\theta)[x]$ ja näin ollen $\beta \in K(\theta)$.

□

**Lause 5.15** (Separoituvien laajennosten homomorfismit)**.** *Olkoon $M/K$ äärellinen laajennos, jonka aste on $d$, ja olkoon $i : K \longrightarrow L$ kuntahomomorfismi. Silloin on olemassa ekvivalenssi joukkojen*

$$\{\exists d \text{ homomorfismia } j_k : M \longrightarrow L, \text{jotka laajentavat } i : K \longrightarrow L\}$$

*ja*

$$\{M/K\text{separoituva}, \forall \alpha \in M\text{minimipolynomi hajoaa renkaassa } L[x]\}.$$

*Muussa tapauksessa on olemassa vähemmän kuin $d$ homomorfismia, jotka laajentavat $i$:n.*

*Todistus.* Todistettiin luennolla. □

**Korollaari 5.16.** *Separoituvan polynomin $f \in K[x]$ juurikunta $L$ on kunnan $K$ separoituva laajennos.*

# 6 Galois'n laajennokset ja Galois'n ryhmät

Olkoon $K$ kunta, merkitään $Aut(K)$ kaikkien $K$:n automorfismien ryhmää, eli kaikkia kuvauksia $g : K \longrightarrow K$, joille ryhmäoperaatioksi määritellään kuvausten yhdistäminen.

Yleisemmin, jos $L/K$ on kuntalaajennos, määritellään

$$\mathrm{Aut}_K(L) = \{g \in Aut(L) : \forall a \in K, g(a) = a\},$$

olemaan kaikkien niiden $L$-automorfismien ryhmä, jotka kiinnittävät kaikki $K$:n alkiot. Kutsumme tätä ryhmää $L$:n Galois'n ryhmäksi yli $K$:n, ja merkitään sitä $G(L/K)$.

Galois'n teoria antaa yhteyden

1. Galois'n ryhmän $G(L/K)$ aliryhmien ja
2. välikuntien $K \subseteq M \subseteq L$

välille.

Galois'n ryhmä $G(L/K)$ on kaikkien $K$-automorfismien ryhmä, eli niiden automorfismien, jotka kiinnittävät $K$:n.

Olkoon $M$ välikunta, kuten yllä. Silloin muodostamme $M$ vastaavan Galois'n ryhmän $M^*$. Yksinkertaisesti $M^* = G(L/M)$, eli $L$:n sellaisten automorfismien ryhmä, jotka kiinnittävät $M$:n. Vastaavasti merkitään $K^* = G(L/K)$ ja $L^* = G(L/L) = 1$. Tämä antaa kuvauksen välille $M \longrightarrow M^*$.

Jos puolestaan katsotaan Galois'n ryhmän $G(L/K)$ aliryhmiä $H$, voidaan määritellä alikunta $H^\dagger$, joka on ryhmän $H$ kiintokunta. Kiintokunta määriteltiin

**Määritelmä 6.1.** Jos $H \leq G(L/K)$, silloin

$$H^\dagger = \{x \in L : \alpha(x) = x \forall \alpha \in H\}.$$

Joten jos $H_1 \leq H_2 \leq G(L/K)$, silloin

$$H_2^\dagger \subseteq H_1^\dagger,$$

koska, jos $x \in L$ ja $\alpha(x) = x$ kaikille $\alpha \in H_2$, silloin $\alpha(x) = x$ kaikille $\alpha \in H_1$.

Myös $K \subseteq H^\dagger$, koska jokainen $H$:n alkio on $K$-automorfismi.

**Lemma 6.2.** *Jos $H \leq G(L/K)$, silloin $H^\dagger$ on $L$:n alikunta, joka sisältää $K$:n.*

*Todistus.* Jos $x, y \in H^\dagger$ ja $\alpha \in H$, silloin $\alpha(x+y) = \alpha(x) + \alpha(y) = x + y$, joten $H^\dagger$ on suljettu yhteenlaskun suhteen, samalla lailla $H^\dagger$ on suljettu kertolaskun suhteen. □

Jos nyt on olemassa välikunnat $L/M/K$ ja $H \leq G(L/K)$, silloin

$$M \subseteq M^{*\dagger}$$

ja

$$H \leq H^{\dagger *},$$

koska jokainen $M$:n alkio jää kiinnitetyksi kaikilla automorfismeilla, jotka kiinnittävät $M$:n. ja samoin jokainen $H$:n alkio kiinnittää kaikki ne alkiot, jotka ovat jäänneet kiinnitetyiksi niillä alkioilla, jotka ovat kiinnittäneet $H$:n.

Merkitään $\mathcal{F}$ kaikkia välikuntia ja $\mathcal{G}$ kaikkia Galois'n ryhmän aliryhmiä, silloin ylläolevat kuvaukset antavat

$$* : \mathcal{F} \longrightarrow \mathcal{G}$$
$$\dagger : \mathcal{G} \longrightarrow \mathcal{F}.$$

Nämä kuvaukset kääntävät sisältymisrelaatiota ja toteuttavat yllä olevan ehdon.

**Lause 6.3** (Galois'n teorian päälause)**.** *Olkoon $L/K$ äärellinen, separoituva, normaali laajennos, jonka aste on $n$, ja jolla on Galois'n ryhmä $G$, jos $\mathcal{F}, \mathcal{G}, *, \dagger$ on määritelty, kuten yllä, silloin*

1. *Galois'n ryhmän kertaluku on $n$.*
2. *Kuvaukset $*$ ja $\dagger$ ovat toistensa käänteiskuvauksia ja luovat järjestyksen kääntävän bijektion $\mathcal{F}$:n ja $\mathcal{G}$:n välille.*
3. *Jos $M$ on välikunta, silloin $[L : M] = |M^*|$ ja $[M : K] = \frac{|G|}{|M^*|}$.*
4. *Välikunta $M$ on $K$:n normaali laajennos jos ja vain jos $M^* \lhd G$.*
5. *Jos $L/M/K$ on kuntatorni ja välikunta $M$ on $K$:n normaali laajennos, silloin $G(M/K) \cong G/M^*$.*

**Esimerkki 6.4.** Tarkastellaan laajennosta $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$. Laajennoksen kanta on $1, i, \sqrt{2}, i\sqrt{2}$ yli $\mathbb{Q}$:n ja näin ollen tyypillinen alkio on muotoa $a_0 + a_1 i + a_2\sqrt{2} + a_3 i\sqrt{2}$.

Laajennoksen aste on 4, ja saadaan tornilemmasta. ja havaitsemalla, että $i \notin \mathbb{Q}(\sqrt{2})$.

Automorfismit ovat $\sigma, \tau, \sigma\tau, 1$, jotka kiinnittävät $\mathbb{Q}$:n.

Jos tiedetään automorfismien vaikutus kannassa, tai juurissa, se määrää koko automorfismin. Nämä neljä automorfismia muodostavat Kleinin neliryhmän, joka on isomorfinen $C_2 \times C_2$ kanssa.

Tällä ryhmällä on kolme aitoa aliryhmää, joten on olemassa kolme välikuntaa, jotka ovat Galois'n laajennoksia (sillä ryhmät ovat normaaleja aliryhmiä). ja ne ovat $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(i\sqrt{2})$.

**Esimerkki 6.5** (Epänormaali laajennos)**.** Tarkastellaan laajennosta $\mathbb{Q}(2^{1/3})/\mathbb{Q}$. Tämä laajennos ei ole normaali. Mitkä ovat ne kunta-automorfismit, jotka kiinnittävät $\mathbb{Q}$:n? Kunta-automorfismin pitää lähettää jaottoman polynomin $f \in \mathbb{Q}[x]$ juuri jollekin toiselle juurelle, sillä polynomin kertoimet kuuluvat kuntaan $\mathbb{Q}$ ja ne automorfismin pitää kiinnittää. Alkion $2^{1/3}$ minimipolynomi on $f(x) = x^3 - 2$, ja näin ollen mille tahansa $\sigma \in G(\mathbb{Q}(2^{1/3})/\mathbb{Q})$ alkio $\sigma(2^{1/3})$ pitää olla polynomin $x^3 - 2$ juuri. On kuitenkin niin, että tällä polynomilla on vain yksi juuri kunnassa $\mathbb{Q}(2^{1/3})$, joten $\sigma(2^{1/3}) = 2^{1/3}$ ja näin ollen $\sigma = Id$. Näin ollen Galois'n ryhmä olisi vain triviaaliryhmä, eikä sen kertaluku olekaan 3, niin kuin yllä oleva lause antaa ymmärtää.

**Esimerkki 6.6** (Separoitumaton laajennos)**.** Polynomi $x?p - t$ kunnan $\mathbb{F}_p(t)$ yli ei ole separoituva, sillä juurikunnassaan $\mathbb{F}_p(t^{1/p})$ sillä on $p$-kertainen juuri. Onko olemassa juurikunnan automorfismeja, jotka kiinnittävät $\mathbb{F}_p(t)$:n? Koska polynomilla on vain yksi juuri juurikunnassaan, ainoa automorfismi on identiteettiautomorfismi, eikä Galois'n ryhmän koko olekaan $p$ niin kuin pitäisi.

**Määritelmä 6.7.** Laajennosta $L/K$ kutsutaan Galois'n laajennokseksi, jos $G(L/K)$:n kiintokunta $G^\dagger$ on täsmälleen $K$.

Eli, ylläolevissa esimerkeissä $\mathbb{Q}(i, \sqrt{2})$ on Galois'n, laajennos, sillä $G(L/K) \cong C_2 \times C_2$ kiinnittää kunnan $\mathbb{Q}$, kun taas $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ ei ole Galois'n laajennos, koska $G(\mathbb{Q}(2^{1/3})/\mathbb{Q}) \cong 1$ ja kiintokunta näin ollen on $\mathbb{Q}(2^{1/3})$. Samalla argumentilla $\mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)$ ei ole Galois'n laajennos.

**Lause 6.8.** *Äärellinen laajennos $L/K$ on Galois'n laajennos, jos ja vain jos $L/K$ on normaali ja separoituva.*

## 6.1 Kunnan asteet ja ryhmän mahtavuudet

**Lemma 6.9.** *Olkoot $L, K$ kuntia ja $\sigma_k : K \longrightarrow L$ erillisiä kuntahomomorfismeja $k = 1, \ldots, n$. Silloin $\{\sigma_1, \ldots, \sigma_k\}$ ovat lineaarisesti riippumattomia kunnan $L$ yli.*

*Todistus.* Tehdään vastaoletus. Silloin kuntahomomorfismit ovat lineaarisesti riippuvaisia, ja valitaan $\sum_{i=1}^m \lambda_i \sigma_i = 0$ lyhyin riippuvuus ($m \leq n$), missä $\lambda_i \in L \setminus \{0\}$, joten mille tahansa $x \in K$ myös $\sum_{i=1}^m \lambda_i \sigma_i(x) = 0$. Valitaan sellainen $\alpha \in K$, jolle $\sigma_1(\alpha) \neq \sigma_2(\alpha)$. Tässä tapauksessa $x \in K$

$$\begin{aligned}
\sum_{i=1}^m \lambda_i \sigma_i(\alpha x) &= 0 \\
\sum_{i=1}^m \lambda_i \sigma_i(\alpha)\sigma_i(x) &= 0 \\
\sum_{i=1}^m \lambda_i \sigma_1(\alpha)\sigma_i(x) &= 0 \\
\sum_{i=2}^m \lambda_i (\sigma_i(\alpha) - \sigma_1(\alpha))\sigma_i(\alpha) &= 0
\end{aligned}$$

Kun valitaan $\mu_i = \lambda_i(\sigma_i(\alpha) - \sigma_1(\alpha)$, silloin

$$\sum_{i=2}^m \mu_i \sigma_i = 0,$$

joka on lyhyempi riippuvuus kuin valittu lyhyin riippuvuus. Ristiriita. □

Ryhmä $G$ toimii kunnassa $L$ uskollisesti, jos $G \longrightarrow \mathrm{Aut}(L)$ on injektio.

**Lause 6.10.** *Oletetaan, että äärellinen ryhmä $G$ toimii uskollisesti kunnassa $L$, silloin $[L : L^G] = |G|$.*

*Todistus.* Olkoon $G = \{1 = g_1, g_2, \ldots, g_n\}$ missä jokainen $g_i : L \longrightarrow L$ on kunta-automorfismi. Asetetaan $m = [L : G^\dagger]$, mahdollisesti $m = \infty$. Oletetaan kuitenkin ensin, että $m < n$, ja olkoon $\{\alpha_1, \ldots, \alpha_m\}$ kanta kunnalle $L$ kiintokunnan $G^\dagger$ yli. Tarkastellaan $n$:n muuttujan $\beta_1, \ldots, \beta_n \in L$ ja $m$ yhtälön ryhmää

$$\sum_{k=1}^{n} g_k(\alpha_i)\beta_k = 0,$$

kaikille $i = 1, \ldots, m$.

Koska $n > m$ ryhmässä on enemmän muuttujia kuin yhtälöitä, näin ollen on olemassa joku vastausjoukko $\{\beta_k\}$. Nyt kun $\alpha \in L$,

$$\sum_{i=1}^{n} \beta_i g_i(\alpha) = 0,$$

ja

$$\sum_{i=1}^{n} \beta_i g_i \equiv 0,$$

kun sitä ajatellaan kuvauksena $L \longrightarrow L$. Tämä on ristiriidassa sen kanssa, että kuntahomomorfismit ovat lineaarisesti riippumattomia.

Nyt oletetaan, että $n < m$, joten on olemassa lineaarisesti riippumaton $n + 1$ alkion osajoukko $\{\alpha_1, \alpha_2, \ldots, \alpha_{n+1}\}$ kunnan $L$ alkioita kiintokunnan $G^\dagger$ yli. Tällä kertaa tarkastellaan $n$ yhtälön ryhmää

$$\sum_{i=1}^{n+1} g_j(\alpha_i)\beta_i = 0$$

kun $j = 1, \ldots, n$, ja $\beta_i \in L$ muodostavat $n+1$ muuttujan joukon. Koska jälleen kerran on enemmän muuttujia kuin yhtälöitä, on olemassa nollasta poikkeava ratkaisu. Järjestetään ratkaisu niin, että vektorissa $\{\beta_1, \ldots, \beta_{n+1}\}$ ensimmäiset $r$ alkiota ovat erisuuria kuin 0, ja valitaan se ratkaisu, jossa $r \geq 1$ on pienin mahdollinen. Joten

$$\sum_{i=1}^{r} g_j(\alpha)\beta_i = 0. \tag{1}$$

Kerrotaan tämä Galois'n ryhmän alkiolla $g$ ja saadaan

$$\sum_{i=1}^{r} gg_j(\alpha)g(\beta_i) = 0,$$

ja kun ryhmän alkiot nimetään uudelleen, saadaan

$$\sum_{i=1}^{r} g_j(\alpha_i)g(\beta_i) = 0. \tag{2}$$

Nyt lasketaan $g(\beta_1)(1) - \beta_1(2)$ ja näin ollen saadaan

$$\sum_{i=2}^{r} g_j(\alpha_i)(\beta_i g(\beta_1) - \beta_1 g(\beta_i)) = 0.$$

Koska $r$ oli valittu minimaaliseksi, kaikki kertoimet ovat nollia, joten jokaiselle $g \in G$

$$\beta_i g(\beta_1) - \beta_1 g(\beta_i) = 0,$$

mikä tarkoittaa

$$\beta_i/\beta_1 = g(\beta_i/\beta_1)$$

ja näin ollen $\beta_i/\beta_1$ kuuluu $G$:n kiintokuntaan. Yhtälöstä (2) kuitenkin saadaan

$$\sum_{i=1}^{r} \alpha_i \frac{\beta_i}{\beta_1} = 0$$

mikä on ristiriita, sillä $\{\alpha_1, \ldots, \alpha_{n+1}\}$ oli valittu lineaarisesti riippumattomaksi joukoksi kunnan $G^\dagger$ yli. □

**Korollaari 6.11.** *Olkoon $L/K$ äärellinen Galois'n laajennos. Silloin Galois'n ryhmän koko $|G(L/K)|$ on sama kuin laajennoksen $[L : K]$ aste.*

**Korollaari 6.12.** *Jos $G$ on Galois'n ryhmä $G(L/K)$ ja $H \leq G$, silloin*

$$[H^\dagger : K] = \frac{[L : K]}{|H|}.$$

*Todistus.* $[L : H^\dagger][H^\dagger : K] = [L : K]$, mistä seuraa

$$[H^\dagger : K] = \frac{[L : K]}{[L : H^\dagger]} = \frac{[L : K]}{|H|}.$$

□

**Lause 6.13.** *Äärellinen laajennos $L/K$ on Galois'n laajennos, jos ja vain jos, $L/K$ on separoituva ja normaali.*

*Todistus.* Oletetaan, että $L/K$ on separoituva ja normaali ja sen aste on $n$. Separoituvan laajennoksen homomorfismien laajantamislauseen perusteella, silloin on olemassa täsmälleen $n = [L : K]$ homomorfismia $L \longrightarrow L$ jotka laajentavat (inkluusio)homomorfismin $K \longrightarrow L$. Näin ollen $|G(L/K)| = n$, ja myös $[L : G^\dagger] = n$. Toisaalta $G^\dagger \supset K$ ja $[L : K] = n$, joten $G^\dagger = K$ ja laajennos $L/K$ on Galois.

Toisin päin, oletetaan, että $L/K$ on Galois'n laajennos, jonka aste on $m$. Silloin on olemassa täsmälleen $m$ homomorfismia $L \longrightarrow L$ jotka laajentavat (inkluusio)homomorfismin $K \longrightarrow L$, ja nämä ovat täsmälleen Galois'n ryhmän $G(L/K)$ alkiot. Joten kun käytetään samaa lausetta separoituvista laajennoksista, saadaan, että $L/K$ on separoituva, ja jokaisen $\alpha \in L$ minimipolynomi $K$:n yli hajoaa lineaarisiksi tekijöiksi $L[x]$:ssä. Joten $L/K$ on normaali. □

Todistetaan sitten kohdat (2) ja (3) Galois'n teorian päälauseesta.

*Todistus.* Olkoon $M$ välikunta, silloin $L/M$ on normaali (koska se on juurikunta $K$:n yli, on se väistämättä juurikunta kunnan $M$ yli). Myös, koska $L/K$ on separoituva, on välilaajennos $L/M$ separoituva, joten laajennos $L/M$ on Galois'n laajennos ja sen Galois'n ryhmä on $G(L/M) = M*$, joka toimii kunnassa $L$ Galois'n ryhmän $G(L/K)$ aliryhmänä, ja sen kiintokunta on $M^{*\dagger} = M$.

Toiseen suuntaan, olkoon $H \leq G$, selvästikin $H \subset G^{\dagger *}$, koska $H$ sisältyy siihen ryhmään, joka kiinnittää kaikki alkiot, jotka $H$ on kiinnittänyt. Edellisen askelen perusteella

$$L^{*\dagger *} = L^*.$$

Toisaalta, kiintokuntien ja ryhmien kertalukujen vertailu tuottaa

$$|H| = [L : H^\dagger] = [L : H^{\dagger *\dagger}] = |H^{\dagger *}|.$$

Joten sekä $H$ että $H^{\dagger *}$ ovat $G$:n aliryhmiä, lisäksi $H \subset G^{\dagger *}$, mutta niillä on sama koko, joten $H = G^{\dagger *}$.

Näin ollen kuvaukset $M \mapsto M^*$ ja $H \mapsto H^\dagger$ ovat toistensa käänteiskuvaukseia, ja itseasiassa kuvaukset antavat 1-1 vastaavuuden. Selvästikin, kun $M$ kasvaa, $M^*$ pienenee, ja päin vastoin. Näin ollen kuvaukset ovat järjestyksen kääntäviä. □

Kohtia (4) ja (5) varten tarvitaan lemma.

**Lemma 6.14.** *Olkoon $L/K$ kuntalaajennos ja $M$ aito välikunta. Olkoon $\tau \in G(L/K) = G$. Silloin $\tau(M)^* = \tau M^* \tau^{-1}$.*

*Todistus.* Jos $\alpha \in M$ ja $g \in M^*$, niin $g\alpha = \alpha$, silloin

$$(\tau g \tau^{-1})(\tau\alpha) = \tau g \alpha = \tau\alpha,$$

ja näin ollen $\tau g \tau^{-1} \in \tau(M)^*$. Argumentti kääntyy. □

*Todistus.* Tarkasteltiin kuntalaajennostornia $L/M/K$. Oletetaan, että $M/K$ on Galois'n laajennos, mikä tarkoittaa erityisesti sitä, että se on normaali laajennos. Olkoon $g \in G$ ja $\alpha \in M$ ja olkoon $m$ alkion $\alpha$ minimipolynomi $K$:n yli. Nyt

$$m(g(\alpha)) = g(m(\alpha)) = 0,$$

joten $g(\alpha)$ on jaottoman polynomin $m \in K[x]$ toinen juuri, koska $m$:llä oli juuri $\alpha \in M$ ja $M$ oli normaalilaajennos, ovat kaikki sen juuret kunnassa $M$. Tästä seuraa $g(\alpha) \in M$, ja samalla $gM = M$ kaikille $g \in G$. Edellisen lemman perusteella kaikille $g \in G$,

$$gM^*g = M^*$$

ja näin ollen $M^* \lhd G$.

Toiseen suuntaan, oletetaan, että $M^* \lhd G$. Halutaan osoittaa, että vastaava laajennos $M/K$ on Galois'n laajennos. Olkoot $\alpha \in M$ ja $\beta \in L$ kaksi erillistä $\alpha$:n minimipolynomin $m \in K[x]$ juurta. Silloin $K(\alpha) \subset L$ ja $K(\beta) \subset L$. Lisäksi on olemassa kuntaisomorfismi

$$K(\alpha) \cong K(\beta),$$

joka lähettää $\alpha \mapsto \beta$. Juurikuntien yksikäsitteisyyden perusteella, tämä laajenee isomorfismiksi

$$L \cong L,$$

joten on olemassa alkio $g \in G(L/K)$, jolle $g(\alpha) = \beta$. Kuitenkin lemman perusteella $gM^*g^{-1} = (gM)^*$, mutta koska oletettiin, että $M^* \lhd G$, tästä seuraa, että $M^* = g(M)^*$, ja koska kuvaus $*$ oli 1-1, tästä seuraa, että $M = g(M)$. Joten $\beta \in M$ ja näin ollen laajennos $M/K$ on normaali. Laajennoksen separoituvuus seuraa siitä, että $L/K$ on separoituva. Näin ollen $M/K$ on Galois'n laajennos.

Viimeiseksi, jos $M/K$ on Galois'n laajennos, määritellään kuvaus

$$\sigma : G \longrightarrow G(M/K)$$

rajoittamalla $\sigma(g) = g|_M$. Tämä kuvaus on surjektio, ja sen ydin on $ker\sigma = M^*$, näin ollen ensimmäisen isomorfialauseen perusteella

$$G(M/K) \cong G/M^*.$$

□

# 7 Polynomin Galois'n ryhmä

**Määritelmä 7.1.** Olkoon $f$ polynomi yli kunnan $K$, jonka juurikunta on $L/K$, silloin $f$:n Galois'n ryhmä on $G(L/K)$.

**Esimerkki 7.2.** 1. $f(x) = x^3 - 1 = (x-1)(x^2+x+1)$, joista jälkimmäinen on jaoton polynomi, jonka juuri on $\omega = e^{2\pi i/3}$. Näin ollen $Gal(x^3-1)$ kertaluku on $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ ja Galois'n ryhmä on isomorfinen ryhmän $C_2$ kanssa.

2. $g(x) = x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$, joista jälkimmäinen on jaoton. Olkoon $\zeta = e^{2\pi i/5}$, silloin polynomin juurikunta on $\mathbb{Q}(\zeta)$ ja Galois'n ryhmän kertaluku on 4. Kuvaus $\phi : \zeta \mapsto \zeta^2$ määrittää $\mathbb{Q}$-automorfismin, jonka kertaluku on 4, näin ollen Galois'n ryhmä on $C_4$.

Polynomin Galois'n ryhmä heijastelee polynomin rakennetta. Itse asiassa Galois määritteli Galois'n ryhmän täsmälleen polynomin juurten symmetriaryhmäksi, ja pitkään matemaatikot käsittelivät ainoastaan permutaatioryhmiä. Cayley oli ensimmäinen joka määritteli abstraktin ryhmän, mutta vasta Kronecker vuonna 1870 antoi ryhmille tyydyttävät aksioomat. Eli noin 40 vuotta ryhmä tarkoitti permutaatioryhmiä.

Oletetaan, että kunnan $K$ karakteristika on 0.

**Propositio 7.3.** *Olkoon $L/K$ polynomin $f(x) \in K[x]$ juurikunta, jossa polynomilla on $n$ erillistä juurta. Silloin Galois'n ryhmä $G(L/K)$ on symmetrisen ryhmän $S_n$ aliryhmä.*

*Todistus.* Jos $\alpha \in L$ on polynomin $f \in K[x]$ juuri, silloin kaikille $g \in G(f)$ pätee $g(f(\alpha)) = f(g(\alpha)) = 0$ ja näin ollen $g(\alpha) \in L$ on polynomin $f$ toinen juuri. Jos $\alpha_1, \ldots, \alpha_n$ ovat polynomin $f$ kaikki juuret, silloin

$$L = K(\alpha_1, \ldots, \alpha_n).$$

Joten saadaan homomofrismi $G \longrightarrow S_n$, missä alkio $g$ indusoi permutaation $\alpha_i \mapsto \alpha_j$. Tämä homomorfismi on injektio, sillä se kiinnittää kunnan $K$, ja $g : \alpha_i \mapsto \alpha_j$ määrittelee alkoin $g$ toiminnan kunnassa $L$. □

**Propositio 7.4.** *Polynomi $f$ on jaoton jos ja vain jos kaikki juuret kuuluvat samalle radalle, ja $G(f)$ on ryhmän $S_n$ transitiivinen aliryhmä.*

*Todistus.* Jos $f$ on jaoton, ja $\alpha_i$ ja $\alpha_j$ kaksi sen erillistä juurta, on olemassa isomorfismi $K(\alpha_i) \cong K(\alpha_j)$, joka kiinnittää $K$:n ja lähettää $\alpha_i \mapsto \alpha_j$. Tämä isomorfismi laajenee automorfismiksi $g : L \longrightarrow L$, jolle $g(\alpha_i) = \alpha_j$ ja näin ollen $G(f)$ on transitiivinen, joka on sama asia, että kaikki alkiot ovat samalla radalla.

Toiseen suuntaan, jos $f \in K[x]$ on jaollinen, vaikkapa $f = gh$, missä $g, h \in K[x]$ ja ne eivät ole vakiopolynomeja. Jos $\alpha_1$ on $g$:n juuri,

silloin $g(\alpha_1)$ on toinen $g$:n juuri, kun $g \in G(f)$, ja näin ollen $G(f)$ permutoi ainoastaan juuria jaottomien tekijöiden sisällä, ja siis toiminta ei ole transitiivinen. □

**Esimerkki 7.5.** Olkoon $f \in K[x]$ muotoa $f(x) = x^2 + bx + c$, jos polynomi on jaoton, sen Galois'n ryhmä on $C_2$ jos se on jaollinen, sen Galois'n ryhmä on 1.

**Esimerkki 7.6.** Kolmannen asteen polynomin Galois'n ryhmä on joko $S_3$ tai $A_3 \cong C_3$. Näin ollen saadaan helposti, että polynomin $g(x) = x^3 - 2$ Galois'n ryhmä on $S_3$, sillä sen juurikunnan aste on 6, ja ainoastaan $S_3$ on kertalukua 6. Tarkastellaan tätä esimerkkiä nyt kuitenkin juurten kannalta vielä kerran.

Onko aina mahdollista konstruoida polynomi, jolla on annettu Galois'n ryhmä?

Olkoon $k$ kunta, jonka karakteristika on 0. Tarkastellaan polynomia

$$\prod_i^n (x - \alpha_i) = \sum_{i=0}^n (-1)^n s_{n-1} x^i.$$

Polynomin kertoimet kuuluvat kuntaan $K = k(s_1, \ldots, s_n)$, joka muodostuu $n$ kappaleesta $\alpha_i$:n alkeellisia symmetrisiä polynomeja, joita merkitään $s_j$. Polynomin juurikunta on $L = k(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n)$

**Lause 7.7.** *Laajennos $L/K$ on äärellinen Galois'n laajennos ja $G(L/K) \cong S_n$.*

*Todistus.* Ryhmä $S_n$ toimii kunnassa $L = k(\alpha_1, \ldots, \alpha_n)$ permutoimalla alkioita $\alpha_i$. Symmetristen polynomien lauseen pohjalta

$$L^{S_n} = k(\alpha_1, \ldots, \alpha_n)^{S_n} \cong k(s_1, \ldots, s_n) = K.$$

Näin ollen $L/K$ on Galois'n laajennos ja sen Galois'n ryhmä on $S_n$. □

Tämä oli hieman teennäinen esimerkki. Palataan nyt tarkastelemeaan polynomin

$$f(x) = \prod_i^n (x - \alpha_i) = \sum_{i=0}^n (-1)^n s_{n-1} x^i = x^n + \sum_{i=0}^{n-1} b_i x^i \in K[x]$$

diskrinanttia

$$\Delta_f = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Diskriminantti on kerrointen $b_i$ polynomi, jotka puolestaan ovat symmetrisiä polynomia juurissa $\alpha_i$. Diskriminantin neliöjuuri on

$$\delta_f = \prod_{i<j}(\alpha_i - \alpha_j)$$

joka ei ole symmetrinen polynomi, mutta se on kuitenkin invariantti ryhmän $A_n \leq S_n$ suhteen. Tästä seuraa:

**Propositio 7.8.** *Olkoon $f \in K[x]$ polynomi, jonka aste on $n$ ja jolla on $n$ erillistä juurta. Silloin $G(f)$ on alternoivan ryhmän $A_n$ aliryhmä, jos ja vain jos*

$$\Delta_f \in K^2 = \{a^2 : a \in K\}.$$

*Todistus.* Nyt $\Delta_f \in K^2$ jos ja vain jos $\delta_f \in K$, mikä on totta, jos ja vain jos $\delta_f \in G(f)^\dagger = K$. Viimeisen huomautuksen perusteella tämä toteutuu jos ja vain jos $G(f) \leq A_n$. □

**Määritelmä 7.9.** Olkoon $f(x) = x^3 - s_1x^2 + s_2x - s_3 \in \mathbb{Q}[x]$, silloin

$$\Delta_f = s_1^2s_2^2 + 18s_1s_2s_3 - 27s_2^3 - 4s_1^3s_3 - 4a_2^3.$$

**Esimerkki 7.10.**

1. $x^3 - 2$ diskriminantti on $-27 \cdot 4$, joka ei ole neliö kunnassa $\mathbb{Q}$, joten kuten todettua, Galois'n ryhmä on $S_3$.
2. $f(x) = x^3 + 3x + 1$, polynomi on jaoton, ja $\Delta_f = -27 - 4 \cdot 27 = -135$ joka ei ole neliö.
3. $g(x) = x^3 - 3x - 1$ on myöskin jaoton ja $\Delta_g = 81$, joka on neliö ja näin ollen Galois'n ryhmä on $A_3$.

Nyt siis tiedetään, että jaottoman $n$:n asteen polynomin Galois'n ryhmä on ryhmän $S_n$ transitiivinen aliryhmä.

Tarkastellaan seuraavaksi $S_n$:n transitiivisia aliryhmiä.

Ryhmän $S_4$ transitiiviset aliryhmät ovat $S_4$, $A_4$, $D_8$, $C_4$ ja $V_4 \cong C_2 \times C_2$.

Ryhmän $S_5$ transitiiviset aliryhmät ovat $S_5$, $A_5$, $G_{20}$ $D_{10}$, $C_5$, missä $G_{20}$ on virittänyt mikä tahansa 5-sykli ja mikä tahansa 4-sykli.

# 8 Symmetriset ryhmät, niiden rakenne, ratkeavuus

Tutkitaan neljän alkion joukon permutaatioryhmää $S_4$. Tämän ryhmän koko on 4!=24. Symmetrisen ryhmän alkiot esitetään yleensä erillisten syklien tulona.

**Esimerkki 8.1.** Permutaatiot

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

voidaan syklinotaatiossa kirjoittaa muotoon (13)(24) ja (134).

Kutsumme sykliä, jonka pituus on kaksi, transpositioksi. Voimme hajottaa jokaisen $n$:n pituisen syklin aina transpositioiden (ei välttämättä erillisten) tuloksi. Jos transpositiohajotelmassa on parillinen määrä termejä, kutsumme permutaatiota parilliseksi, muussa tapauksessa parittomaksi. Molemmat ylläolevat permutaatiot ovat parillisia, sillä $(134) = (13)(34)$.

**Määritelmä 8.2.** Symmetrisen ryhmän alkion syklityyppi määräytyy sen alkiovieraan syklihajotelman perusteella. Syklityyppi listaa yksinkertaisesti eripituisten syklien määrät.

**Esimerkki 8.3.** Alkion (14) syklityyppi on 2, kun taas alkion (125)(346)(78)(9) syklityyppi on $3^2, 2, 1$, huomaa, että 3+3+2+1=9. Monesti ykkössyklejä ei kirjoiteta ollenkaan.

**Lause 8.4.** *Kaksi symmetrisen ryhmän $S_n$ alkiota ovat toistensa konjugaatteja, jos ja vain jos niillä on sama syklityyppi.*

*Todistus.* Olkoon $(a_1 \dots a_m)$ $m$-sykli ja $\rho \in S_n$, silloin $\rho^{-1}(a_1 \dots a_m)\rho = (a_1\rho \dots a_m\rho)$ (vakuutu tästä esimerkkien avulla).

Olkoon nyt $\tau = \tau_1\tau_2 \dots \tau_r$ syklihajotelma. Silloin

$$\rho^{-1}\tau\rho = \rho^{-1}\tau_1 \dots \tau_r\rho = \rho^{-1}\tau_1\rho\rho^{-1}\tau_2\rho \dots \rho^{-1}\tau_r\rho,$$

missä jokainen $\rho^{-1}\tau_i\rho$ on sykli, jonka pituus on sama kuin $\tau_i$:n pituus. Niinpä $\rho^{-1}\tau\rho^{-1}$:lla ja $\tau$:lla on sama syklityyppi.

Jos taas $\tau$:lla ja $\sigma$:lla on sama syklityyppi, meidän täytyy konstruoida $\rho$, joka konjugoi nämä alkiot keskenään. Kirjoitetaan $\tau$ ja $\sigma$ sellaiseen järjestykseen, että samanpituiset syklit ovat samassa järjestyksessä.

$$\begin{aligned} \sigma &= (a_1 \dots a_m)(a_{m+1} \dots a_r)(a_{r+1} \dots )() \\ \tau &= (b_1 \dots b_m)(b_{m+1} \dots b_r)(b_{r+1} \dots )() \end{aligned}$$

Nyt luomme alkion $\rho$ kuvaamaan $a_i \mapsto b_i$ mukaan lukien ykkössyklit. Tällainen $\rho$ permutoi $\{1, \dots, n\}$ ja on siis ryhmän $S_n$ alkio, kuten vaadittua. □

**Tehtävä 1.** Osoitetaan, että syklit (12) ja (123...$n$) virittävät symmetrisen ryhmän $S_n$.

Taulukko 1: Ryhmän $S_4$ alkiot

| Konjugaatioluokka | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| edustaja | 1 | (12) | (12)(34) | (123) | (1234) |
| alkion kertaluku | 1 | 2 | 2 | 3 | 4 |
| konjugaattien määrä | 1 | 6 | 3 | 8 | 6 |
| keskittäjän koko | 24 | 4 | 8 | 3 | 4 |

Kootaan taulukkoon $S_4$:n alkiot konjugaatioluokkien mukaan

Koska syklityyppi määrittää konjugaatioluokan, on luonnollista, että normaalit aliryhmät ovat konjugaatioluokkien yhdisteitä. $S_4$:ssä on kaksi normaalia aliryhmää. $V_4$ on konjuvaatioluokkien 1 ja 3 yhdiste ja alternoiva ryhmä $A_4$ on konjugaatioluokkien 1,3 ja 4 yhdiste.

Kokoamme myös ryhmän $A_4$ vastaavat tiedot taulukkoon.

Taulukko 2: Ryhmän $A_4$ alkiot

| Konjugaatioluokka | 1 | 2 | 3a | 3b |
|---|---|---|---|---|
| edustaja | 1 | (12)(34) | (123) | (134) |
| alkion kertaluku | 1 | 2 | 3 | 3 |
| konjugaattien määrä | 1 | 3 | 4 | 4 |
| keskittäjän koko | 12 | 4 | 3 | 3 |

Näin ollen $A_4 \lhd S_4$, jonka indeksi on 2, ja $V_4 \lhd A_4$ ja indeksi on 3.

Etsitään vielä $D_8$ ja $C_4$ ryhmän $S_4$ aliryhmänä. Syklinen ryhmä $C_4$ on minkä tahansa 4-syklin virittämä. Ryhmä $D_8$ on neliön rymmetria-ryhmä ja saadaan sen virittäjät helposti geometrisesti tarkastelemalla. $D_8 = \{1, (12)(34), (14)(23), (13), (24), (12334), (1432), (13)(24)\}$

**Propositio 8.5.** *Symmetrisen ryhmän $S_n$ virittää yksi $n$-sykli ja yksi transpositio.*

*Todistus.* Harjoitustehtävä. □

# 9 $A_5$, alternoiva ryhmä ja muita yksinkertaisia ryhmiä

Tutustutaan ensin ryhmään $S_5$. Jos käytetään syklinotaatiota, se sisältää syklejä, jotka ovat muotoa (12), (123), (1234), (12345), (12)(34),

(123)(45). Kukin syklityyppi määrittää konjugaattiluokan. Jos rajoitutaan vain parillisiin sykleihin, niin saadaan alternoivan ryhmän $A_5$. Alternoivassa ryhmässä syklit (123) jakautuvat kahteen eri konjugaattiluokkaan.

**Määritelmä 9.1.** Äärellistä ryhmää $G$ kutsutaan yksinkertaiseksi, jos sen ainoat normaalit aliryhmät ovat ryhmä itse ja ykkösalkio.

**Esimerkki 9.2.**
1. Jokainen syklinen ryhmä $C_p$, jonka kertaluku on joku alkuluku $p$, on yksinkertainen.
2. Ryhmä $A_4$ ei ole yksinkertainen, sillä $V_4 \lhd A_4$.

Pienin epätriviaali esimerkki yksinkertaisesta ryhmästä on $A_5$. Tämä on erityisen tärkeä myös todistuksessa, että viidennen asteen polynomille ei ole olemassa ratkaisukaavaa. Todistamme hieman laajemmin.

**Propositio 9.3.** *Alternoiva ryhmä $A_n$ on yksinkertainen, kun $n \geq 5$.*

*Todistus.* Todistus jaetaan kolmeen osaan.

1. Jos $H \neq 1$ ja $H \lhd A_n$, silloin $H$ sisältää kolmossyklin.
2. $H$ sisältää kaikki kolmossyklit.
3. kolmossyklit virittävät $A_n$:n.

Tällöin $H = A_n$, joten $A_n$ on yksinkertainen.

1. Olkoon $H \lhd A_n$ ja olkoon $h$ sellainen alkio, jonka kertaluku on joku alkuluku $p$. Kirjoitamme $h$:n nyt alkiovieraina sykleinä, joista luonnollisesti jokaisen pituuden pitää olla $p$. Vaihtoehdot ovat
(a) $o(h) = p \geq 5$ ja jos $h = (a_1, \ldots, a_p) \ldots (r_1, \ldots, r_p)$ voidaan kirjoittaa

$$(a_1a_2a_3)h(a_3a_2a_1)h^{-1} = (a_2a_3a_p),$$

joten $H$ sisältää 3-syklin.
(b) Jos $o(h) = 3$ ja $h = (abc)(def)\ldots$ saadaan

$$(abcde)h(edcba)h^{-1} = (bcdef) \in H.$$

Jos nyt käytetään kohtaa (a), saadaan todistettua, että $h$ sisältää kolmossyklin.
(c) Jos $o(h) = 2$, silloin $h = (ab)(cd)$ tai $h = (ab)(cd) \cdot (ef)(gh)\ldots$ jälkimmäisessä tietysti parillinen määrä transpositioita. Ensimmäisessä tapauksessa

$$(bde)h(edb)h = (aebdc) \in H$$

ja nyt voidaan taas löytää (a)-kohdan perusteella kolmossykli. Toisessa tapauksessa

$$(bde)(h(edb)h = (afc)(bde)$$

ja voidaan käyttää (b)-kohtaa kolmossyklin löytämiseen.

Joten jokaisessa tapauksessa $H$ sisältää kolmossyklin.

2. Seuraavaksi todistetaan, että jos $H$:ssa on yksi kolmossykli, ovat kaikki kolmossyklit $H$:ssa.

Tiedätään, että kaikki kolmossyklit ovat toistensa konjugaatteja ryhmässä $S_n$ ja niitä on ja yhteensä näitä on $\binom{n}{3} \cdot 2$ kappaletta.

Jos $\alpha = (xyz) \in H$ on kolmossykli ryhmässä $S_n$, saadaan $\alpha$:n keskittäjän koko laskettua rata-vakauttajalauseella. Sillä $|Orb_{S_n}| = |S_n : C_{S_n}(\alpha)| = \frac{n(n-1)(n-2)}{3}$, mistä seuraa, että $|C_{S_n}(\alpha)| = 3(n-3)!$. Tässä yhteydessä ollaan kuitenkin kiinnostuneita konjugoinnista ryhmässä $A_n$, ja laskemalla $C_{A_n}(\alpha)$:n koon, saadaan selville $\alpha$:n konjugaattien määrän.

Nyt $C_{S_n}(\alpha)$ on symmetrisen ryhmän aliryhmä, joko kaikki sen alkiot ovat parillisia, tai täsmälleen puolet ovat parillisia ja puolet parittomia. Selvästikin jälkimmäinen tapaus pätee, sillä $(xyz)(lm)$ on pariton permutaatio, joka keskittää $\alpha$:n. Muista, että $n \geq 5$. Jos tarkastellaan siis parillisia permutaatioita tässä ryhmässä, on niitä $\frac{1}{2}3(n-3)! = |C_{A_n}(\alpha)|$. Rata-vakauttajalauseen perusteella

$$|A_n : C_{A_n}(\alpha)| = \frac{n(n-1)(n-2)}{3},$$

joten kaikki $S_n$:n kolmossyklit ovat konjugaatteja keskenään. Koska $H \lhd A_n$, tästä seuraa, että kaikki kolmossyklit kuuluvat $H$:n.

3. Halutaan osoittaa, että kolmossyklit generoivat $A_n$:n. Jokainen $A_n$:n alkio voidaan kirjoittaa parillisena määränä transpositioita. Koska $(ab)(bc) = (abc)$ ja $(ab)(cd) = (ab)(bc)(bc)(ad) = (abc)(bcd)$, jokainen $A_n$:n alkio voidaan kirjoittaa kolmossyklien tulona.

□

Yksinkertaiset ryhmät ovat kaikkien äärellisten ryhmien rakennuspalikoita samaan tapaan kuin alkuluvut ovat kaikkien luonnollisten lukujen rakennuspalikoita. Sykliset ryhmät, joiden kertaluku on alkuluku $p$ ovat puolestaan kaikkien ratkeavien ryhmien rakennuspalikoita. Nimitys ratkeava tulee täsmälleen yhtälöitten ratkaisemisen teoriasta, Nimittäin, polynomiyhtälö ratkeaa radikaalien avulla täsmälleen silloin kun sen yhtälöön liitetty Galois'n ryhmä on ratkeava. Seurauksena on muun muassa se, että viidennen asteen yhtälölle ei ole yleistä ratkaisukaavaa, koska ryhmä $A_5$ on yksinkertainen, eikä siis ratkeava – kuten ei myöskään tällä perusteella $S_5$.

**Määritelmä 9.4.** Äärellinen ryhmä $G$ on ratkeava, jos sillä on olemassa ketju

$$1 = G_n \lhd G_{n-1} \lhd \ldots \lhd G_1 \lhd G_0 = G,$$

jossa jokainen $G_{i+1} \lhd G_i$ ja $G_i/G_{i+1}$ on Abelin ryhmä.

**Esimerkki 9.5.** 1. Abelin ryhmät ovat ratkeavia: $1 \lhd G$.

2. $1 \lhd C_2 \lhd C_4 \lhd D_8$, joten $D_8$ on ratkeava ryhmä, sillä kaikki tekijäryhmät ovat isomorfisia $C_2$:n kanssa.
3. $1 \lhd V_4 \lhd A_4 \lhd S_4$, joten $S_4$ on ratkeava.
4. $A_5$ ei ole ratkeava, koska sen ainoa normaali aliryhmä on 1, ja $A_5/1 \cong A_5$ ei ole Abelin ryhmä.

Ratkeavat ryhmät on ensimmäinen ryhmäluokka, joka on suljettu, niin laajennusten kuin aliryhmienkin suhteen.

**Lause 9.6.** *1. Jos $G$ on ratkeava ryhmä, silloin $H \leq G$ on ratkeava ryhmä.*

*2. Jos $G$ on ratkeava ryhmä, ja $N \lhd G$ silloin $G/N$ on ratkeava.*

*3. Olkoon $N \lhd G$ ja $N$ ja $G/N$ ratkeavia, silloin $G$ on ratkeava.*

Huomaa, että jos sekä $N$ että $G/N$ ovat Abelin ryhmiä, ryhmä $G$ on ratkeava (toisinaan sitä kutsutaan myös meta-abelin ryhmäksi), mutta ei välttämättä Abelin ryhmä. Abelin ryhmät eivät siis ole suljettu ryhmäluokka.

*Todistus.* 1) Olkoon $\{G_i\}_{i \leq n}$ ryhmän $G$ hajoamisjono, ja olkoon $H \leq G$. Määritellään $H_i = G_i \cap H$. Selvästikin $H_{i-1} \lhd H_i$ ja kuvaus $H_i = H \cap G_i \longrightarrow G_i$ määrittelee, kun jaetaan $H_{i-1}$ pois injektion

$$H_i/H_{i-1} = H \cap G_i / H \cap G_{i-1} \longrightarrow G_i/G_{i-1}.$$

Jälkimmäinen ryhmä on Abelin ryhmä oletuksen nojalla, joten $H_i/H_{i-1}$ on Abelin ryhmän aliryhmä ja näin itsekin Abelin ryhmä.

2) Olkoon $\{G_i\}_{i \leq n}$ jono ryhmälle $G$ ja $N_i = G_i N/N \leq G/N$. Selvästikin $N_{i-1} \lhd N_i$ ja kuvaukset tekijäryhmien välillä

$$G_i/G_{i-1} \longrightarrow N_i/N_{i-1} = \frac{(G_i N)/N}{(G_{i-1}N/N}$$

missä $g \mapsto g \cdot e + (G_{i-1}N)/N$ on surjektio. Koska $G_i/G_{i-1}$ on Abelin ryhmä, ryhmä $N_i/N_{i-1}$ on Abelin ryhmän tekijäryhmä ja näin olleen myös Abelin ryhmä itse.

3) Olkoon $\{N_i\}_{i \leq m}$ jono ryhmälle $N$. Mikä tahansa $G/N$:n aliryhmä voidaan kirjoittaa muotoon $G_i/N$, jollekin $G_i \leq G$. Otetaan jono $\{G_i/N\}_{i \leq n}$ ja liitetään nämä kaksi jonoa toisiinsa

$$N_1 \leq N_1 \leq \cdots \leq N_m = G_0 \leq G_1 \leq \cdots \leq G_n.$$

Oletuksen perusteella jokainen aliryhmä on normaali seuraavassa, ja kaikki tekijäryhmät ovat muotoa $N_i/N_{i-1}$, joka on Abelin ryhmä oletuksen nojalla, tai $G_i/G_{i-1} \cong \frac{G_i/N}{G_{i-1}/N}$ käyttäen kolmatta isomorfialausetta, mutta myös tämä ryhmä on oletuksen nojalla Abelin ryhmä. □

# 10 Syklotomiset ja Kummerin laajennokset

Abelin ryhmät olivat siis ratkeavien ryhmien rakennuspalikoita. Milloin Galois'n ryhmä on Abelin ryhmä? Tarkastellaan kahta esimerkkiä.

**Lause 10.1.** *Olkoon $K$ kunta, jonka karakteristika on 0, olkoon $p$ alkuluku ja olkoon $L$ polynomin $x^p - 1$ juurikunta. Laajennos $L/K$ on Galois'n laajennos ja sen Galois'n ryhmä on Abelin ryhmä.*

**Huomautus 10.2.** Tämä pätee kaikille syklotomisille polynomeille.

*Todistus.* Koska polynomin $x^p - 1$ muodollinen derivaatta on $px^{p-1}$, ei sillä ole moninkertaisia juuria kunnassa $L$. Polynomin nollakohdat ovat $p$:net ykkösenjuuret ja ne muodostavat ryhmän kertolaskun suhteen. Ryhmän kertaluku on $p$ ja ryhmä on syklinen. Olkoon $\zeta$ tämän ryhmän virittäjä.. Silloin $L = K(\zeta)$ joten mikä tahansa automorfismi $G(L/K)$ määräytyy sen mukaan, miten se toimii alkiolla $\zeta$. Lisäksi nämä automorfismit kuvaavat juuret juuriksi. Näin ollen, mikä tahansa $K$-automorfismi on muotoa

$$\alpha_j : \zeta \mapsto \zeta^j.$$

Mutta silloin $\alpha_i\alpha_j$ ja $\alpha_j\alpha_i$ kuvaavat $\zeta \mapsto \zeta^{ij}$, joten Galois'n ryhmä on Abelin ryhmä. □

**Lause 10.3.** *Olkoon $K$ polynomin $x^n - 1$ juurikunta ja oletetaan, että sen karakteristika on 0. Olkoon $a \in K$ ja $L$ polynomin $x^n - a$ juurikunta. Silloin $G(L/K)$ on Abelin ryhmä.*

*Todistus.* Olkoon $\alpha$ mikä tahansa polynomin $x^n - 1$ juuri. Koska $x^n - 1$ hajoaa kunnassa $K$, muut juuret ovat muotoa $\zeta\alpha$, missä $\zeta$ on ykkösenjuuri. Koska $L = K(\alpha)$, mikä tahansa $\sigma \in G(L/K)$ on määritelty sen, mukaan, mihin se lähettää $\alpha$:n. Olkoon

$$\phi : \alpha \mapsto \zeta\alpha$$
$$\psi : \alpha \mapsto \eta\alpha$$

missä $\zeta, \eta \in K$. Silloin

$$\phi\psi(\alpha) = \zeta\eta\alpha = \eta\zeta\alpha = \psi\phi(\alpha).$$

Ja näin ollen Galois'n ryhmä on Abelin ryhmä. □

# 11 Radikaalit laajennokset

Oletetaan tässäkin osassa, että kunnan karakteristika on 0.

Esimerkiksi toisen ja kolmannen asteen yhtälöitten ratkaisukaavoja kutsutaan radikaaleiksi esityksiksi. Radikaalit esitykset saadaan normaaleilla kuntaoperaatioilla sekä $n$:sillä juurilla. Tarkempi määritelmä on seuraava.

**Määritelmä 11.1.** Kuntalaajennosta $L/K$ kutsutaan radikaaliksi laajennokseksi, jos on olemassa jono alkioita $\alpha_1, \ldots, \alpha_n$ sekä positiiviset kokonaisluvut $m_1, \ldots, m_n$, joille

$$L = K(\alpha_1, \ldots, \alpha_n),$$

ja jokaiselle $i$

$$\alpha_i^{m_i} \in K(\alpha_1, \ldots, \alpha_{i-1}).$$

Alkioita $\alpha_1, \ldots, \alpha_n$ kutsutaan radikaaliksi jonoksi.

**Esimerkki 11.2.** Laajennos $\mathbb{Q}(2^{1/4}, i)/\mathbb{Q}$ on radikaalilaajennos. Alkiota $11^{1/3}\left(\frac{1+\sqrt{3}}{2}\right)^{1/5} + (1+4^{3/4})^{1/4}$ kutsutaan radikaaliksi. Jos halutaan löytää radikaali laajennos, joka sisältää tämän alkion, täytyy kuntaan $\mathbb{Q}$ liittää vuorollaan $\alpha = 11^{1/3}, \beta = \sqrt{3}, \gamma = ((7+\beta)/2)^{1/5}, \delta = 4^{1/3}, \varepsilon = (1+\delta)^{1/4}$. Nyt laajennos $\mathbb{Q}(\alpha, \beta, \gamma, \delta, \varepsilon)$ sisältää annetun alkion, ja on radikaali laajennos. Tässä radikaali jono on $\alpha^3 = 11, \beta^2 = 3, \gamma^5 = (7+\beta)/2, \delta^3 = 4, \varepsilon^4 = 1+\delta$.

**Määritelmä 11.3.** Olkoon $f \in K[x]$, ja olkoon $L/K$ polynomin $f$ juurikunta. Silloin $f$ ratkeaa radikaaleilla, jos on olemassa radikaalilaajennos $M/K$, ja $L \subseteq M$.

**Lause 11.4.** *Olkoon $L/K$ äärellinen Galois'n laajennos. Silloin on olemassa äärellinen laajennos $M/L$, jossa $M/K$ on radikaalilaajennos, jos ja vain jos $G(L/K)$ on ratkeava ryhmä.*

*Todistus.* Oletetaan, että on olemassa radikaali laajennos $M/K$, joka sisältää laajennoksen $L/K$. Olkoon $M = K(\alpha_i)$, missä

$$\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1}).$$

Olkoon $m_i$ alkion $\alpha_i$ minimipolynomi kunnan $K$ yli. Tarkastellaan polynomin $\prod_{i=1}^{n} m_i \in K[x]$ juurikuntaa $N$. Juurikunta $N$ on Galois'n laajennos, sillä jokainen $\alpha_i$ on separoituva $K$:n yli, se on lisäksi jokaisen $m_i$ juurikunta.

Seuraavaksi osoitetaan, että juurikunta $N/K$ on radikaali laajennos. Olkoon $\beta$ polynomin $m_i$ juuri. Koska minimipolynomi on jaoton,

on olemassa joku Galois'n ryhmän alkio $\sigma \in G(N/K)$, jolle $\sigma(\alpha_i) = \beta$. Näin ollen

$$\beta^{n_i} = \sigma(\alpha_i)^{n_i} \in K(\sigma(\alpha_j) : \sigma \in G(N/K), j < i).$$

Kun tätä toistetaan induktiivisesti, voidaan todeta, että laajennos $N/K$ on radikaali laajennos.

On siis konstruoitu laajennos $N/L/K$, jossa $N/K$ on Galoisn' laajennos, ja oletuksen mukaan myös $L/K$ on Galois'n laajennos. Galois'n teorian päälauseen perusteella, on olmeassa surjektio $G(N/K) \longrightarrow G(L/K)$ ja näin ollen riittää todistaa, että Galois'n ryhmä $G(N/K)$ on ratkeava.

Todistetaan tämän ryhmän ratkeavuus induktion avulla. Induktiossa käytetään laajennoksen $[N : K]$ astetta. Olkoon

$$N = K(\beta_1, \ldots, \beta_{i-1}).$$

Oletetaan myös, että $n_i = p_i$, eli alkuluku. Tämä ei vaikuta argumentointiin mitenkään. Silloin $\beta = \beta_1 \notin K$, mutta kun $p = p_1$, silloin $\gamma = \beta^p \in K$ alkukuvulle $p$. Näin ollen $\beta$:n minimipolynomi $K$:n yli jakaa polynomin $x^p - \gamma \in K[x]$. Olkoon $\beta'$ toinen minimipolynomin juuri. Silloin $(\beta'/\beta)^p = 1$ joten $N$ sisältää epätriviaalin $p$:n ykkösen juuren $\zeta$, tämä $\zeta$ on primitiivinen ykkösenjuuri.

Tarkastellaan inkluusiohomomorfismeja

$$K \longrightarrow K(\zeta) \longrightarrow K(\zeta, \beta_1) \longrightarrow N.$$

Laajennos $K(\zeta)/K$ on polynomin $x^p - 1$ juurikunta, se on syklotominen laajennos ja näin ollen san Galois'n ryhmä on Abelin ryhmä. Kun taas laajennos $K(\zeta, \beta)/K(\zeta)$ on polynomin $x^p - \gamma \in K(\zeta)$ juurikunta. Tämä laajennos on edellisen lemman perusteella Galois'n laajennos ja sen Galois'n ryhmä on Abelin ryhmä, itseasiassa Galois'n ryhmä on syklinen ryhmä. Laajennos $N/K(\zeta, \beta)$ on radikaali laajennos ja sen aste on aidosti pienempi kuin $[N : K]$.

Näitä laajennoksia vastaa seuraava ketju Galois'n ryhmän $G(N/K)$ aliryhmiä

$$G(N/(K(\zeta, \beta_1)) \lhd G(N/K(\zeta)) \lhd G(N/K).$$

Kaikki tekijäryhmät ovat Abelin ryhmiä, koska ne ovat syklotomisten tai Kummerin laajennosten Galois'n ryhmiä. Nyt $G(N/K(\zeta, \beta_1))$ on induktion nojalla ratkeava. Ja siis myös $G(N/K)$ on ratkeava.

Toiseen suuntaan käytetään induktiota Galois'n ryhmän $G(L/K)$ kertaluvun suhteen. Oletetaan siis, että $G$ on ratkeava.

Olkoon $H \lhd G(L/K) = G$, ja valitaan $H$ maksimaaliseksi normaaliksi aliryhmäksi. Silloin $G/H$ on ratkeava ja koska se on maksimaalinen, ei sillä ole yhtään epätrviaalia normaalia aliryhmää. Joten $G/H$

on Abelin ryhmä (koska sillä on ketju $1 \lhd G/H$), eikä sillä ole aliryhmiä, joten täytyy olla $G/H \cong C_p$, jollekin alkuluvulle $p$.

Merkitään polynomin $x^p - 1 \in L[x]$ juurikuntaa $L_1$, silloin $L_1 = L(\zeta)$, jossa $\zeta$ on primitiivinen $p$:s ykkösenjuuri. Näin ollen $L_1/K$ on Galois'n laajennos. Saadaan torni kuntalaajennoksia:

Jos $\sigma \in G(L(\zeta)/K(\zeta))$, silloin $\sigma$ kuvaa kunnan $L$ itselleen, koska $L/K$ on normaali laajennos. Tarkastellaan homomorfismia

$$\theta : G(L(\zeta)/K(\zeta) \longrightarrow G(L/K),$$

missä

$$\sigma \mapsto \sigma_{|_L}.$$

Jos $\theta(\sigma) = Id_L$ eli $\sigma_{|_L}$, silloin $\sigma$ kiinnittää $L$:n ja myös $\zeta$:n joten $\sigma = Id_{|_{L(\zeta)}}$. Näin ollen $\theta$ on injektio. On olemassa kaksi tapausta.

1) $\theta$ on injektio, mutta ei surjektio. Tällöin

$$|G(L(\zeta) : K(\zeta))| < |G(L/K)|,$$

mikä tarkoittaa sitä, että $G(L(\zeta) : K(\zeta))$ ratkeava, koska se on ratkeavan ryhmän aliryhmä. Lisäksi sen kertaluku on pienempi. Induktion nojalla $L(\zeta)$ sisältyy johonkin kunnan $K(\zeta)$ radikaaliin laajennokseen $M$, joten $L$ sisältyy $K$:n radikaaliin laajennokseen $M$.

2) $\theta$ on isomorfismi. Silloin $H \lhd G$ kuvautuu $\theta$:lla joksikin ryhmäksi $N \lhd G(L(\zeta)/K(\zeta))$.Tarkastellaan kuntia

$$K \subset K(\zeta) \subset L(\zeta)^N \subset L(\zeta).$$

Nyt $L(\zeta)^N/L(\zeta)$ on Galois'n laajennos ja sen Galois'n ryhmä on $N$, joka on ratkeava ryhmä ja sen kertaluku on pienempi kuin $G$:n kertaluku. Joten induktion nojalla $L(\zeta)$ sisältyy $L(\zeta)^N$:n radikaaliin laajennokseen.

Nyt $L(\zeta)^N/K(\zeta)$ on Galois'n laajennos ja sen Galois'n ryhmä on $G(L(\zeta)/K(\zeta)) \cong G/H \cong C_p$ ja koska $K(\zeta)$ sisältää kaikki $p$:nnet ykkösenjuuret, on tämä radikaali laajennos (Kummerin teorian nojalla). Tästä seuraa, että $K(\zeta)/K$ on radikaalilaajennos, joten $L \subseteq M$, joka on $H$:n radikaali laajennos.

□

**Lause 11.5.** *Olkoon $f \in K[x]$. Jos $f$ voidaan ratkaista radikaaleilla, silloin $G(f)$ on ratkeava ryhmä.*

**Korollaari 11.6.** *Olkoon $K$ kunta, jonka karakteristika on 0. Silloin polynomit $f \in K[x]$ voidaan ratkaista radikaalien avulla, kunhan $f$:n aste on korkeintaan neljä.*

*Todistus.* Galois'n ryhmä $G(f) \leq S_4$ ja $S_4$ on ratkeava. Ratkeavan ryhmän aliryhmä on aina myös ratkeava. □

# 12 Viidennen asteen polynomin ratkeamattomuus

Riittää siis osoittaa, että on olemassa viidennen asteen polynomi kunnan $\mathbb{Q}$ yli, jonka Galois'n ryhmä on $S_5$. Tätä polynomia ei voi ratkaista radikaaleilla ja näin ollen ei ole olemassa yleistä ratkaisukaavaa viidennen asteen polynomille.

**Propositio 12.1.** *Olkoon $p$ alkuluku, ja $f \in \mathbb{Q}[x]$ jaoton polynomi, jonka aste on $p$. Oletetaan lisäksi, että $f$:llä on täsmälleen kaksi imaginäärijuurta. Silloin $G(f) \cong S_p$.*

*Todistus.* Kompleksilukujen kunta $\mathbb{C}$ sisältää polynomin $f$ juurikunnan $M/\mathbb{Q}$, ja koska $\mathbb{Q}$:n karakteristika on 0, ovat kaikki sen nollat erillisiä. Tästä seuraa, että sen Galois'n ryhmä $G(f)$ on $S_p$:n aliryhmä.

Koska $f$ on jaoton polynomi ja sen aste on $p$, ensimmäinen juuren liittäminen kuntaan $\mathbb{Q}$ antaa laajennoksen jonka aste on $p$. Näin ollen tornilemman perusteella

$$p \mid [M : \mathbb{Q}] = |G(f)|.$$

Cauchyn lauseen perusteella $G$:ssä on alkio, jonka kertaluku on $p$, ja koska $G \leq S_p$ on tämä alkio väistämättä $p$-sykli.

Toinen oletus oli, että polynomilla $f$ on täsmälleen kaksi imaginäärijuurta. Kompleksi-konjugaatio on tuottaa kunnan $M$ automorfismin, joka kiinnittää $\mathbb{Q}$:n. Tämä automorfismi kiinnittää kaikki muut $p-2$ juurta, ja vaihtaa kompleksijuurten paikkaa, joten Galois'n ryhmä sisältää transposition. Oletetaan, että se on (12). Nyt harjoitustehtävän perusteella $p$ sykli $(123\ldots p)$ ja transposition (12) virittävät ryhmän $S_p$, joten $G(f) \cong S_p$ ja tämä ryhmä ei ole ratkeava. □

Tarkastellaan lopuksi tiettyä polynomia.

**Lause 12.2.** *Polynomia $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ ei voi ratkaista radikaaleilla.*

*Todistus.* $f$ on selvästikin jaoton Eisensteinin kriteerion perusteella. Seuraavaksi etsitään sen summittaiset juuret:

$$f(-2) = -17, f(-1) = 8, f(0) = 3, f(1) = -2, f(2) = 23.$$

Rollen lauseen perusteella $f$:n nollakohtien välissä on $Df$:n nollakohdat. Tässä $Df = 5x^4 - 6$, jolla on nollat $\pm(6/5)^{1/4}$.

Koska $f$ ja $Df$:llä ei ole yhteisiä tekijöitä, ei $f$:llä ole yhtään moninkertaista juurta. Joten $f$:llä on korkeintaan 3 reaalijuurta, mutta

sillä on myös vähintään 3 reaalijuurta, koska se on jatkuva funktio, eikä voi vaihtaa etumerkkiä ellei se mene nollan läpi.

Joten $f$:llä on 3 reaalijuurta ja 2 kompleksijuurta. Tämän lisäksi sen aste, 5, on alkuluku. Edellisen lauseen perusteella sen Galois'n ryhmä on $S_5$, ja tämä ryhmä ei ole ratkeava, joten edellisen luennon lauseen perusteella $f$:ää ei voi ratkaista radikaalien avulla. □

# 13 Äärellisten kuntien laajennokset ja Galois'n ryhmät

Olkoon $F$ äärellinen kunta, jossa on $q$ alkiota.

Määritelllään homomorfismi

$$\theta : \mathbb{Z} \longrightarrow F,$$

joka kuvaa $\theta(1) = 1$. Koska $\mathbb{Z}$ on ääretön ja $F$ on äärellinen, kuvauksen ytimen pitää olla nollasta poikkeava, sillä muuten $\theta$ upottaisi $\mathbb{Z}$:n kuntaan $F$.

$Ker\theta \lhd \mathbb{Z}$ ja koska $\mathbb{Z}$ on pääideaalialue, sillä on yksi virittäjä. Nyt

$$\mathbb{Z}/ker\theta \cong Im\theta \leq F,$$

ja koska $F$ on kunta, ei sillä ole nollajakajia, ja $Im\theta \cong \mathbb{Z}/Ker\theta$ on kokonaisalue. Tästä seuraa, että $ker\theta$ on alkuideaali, joten $ker\theta = (p)$, jollekin alkuluvulle $p$. Joten

$$\mathbb{Z}/\ker\theta = \mathbb{Z}/(p) \cong \mathbb{F}_p,$$

joten $F$:n karakteristika on äärellinen $p$, ja rengas $\mathbb{F}_p$ on upotettu $F$:ään.

Nyt $F$ voidaan ajatella vektoriavaruutena yli $\mathbb{F}_p$:n ja koska $F$ on äärellinen kunta, on se äärellisulotteinen vektoriavaruus yli kunnan $\mathbb{F}_p$. Olkoon $v_1, \ldots, v_n$ tämän kanta, joten jokainen $F$:n alkio voidaan kirjoittaa yksikäsitteisesti muodossa

$$\lambda_1 v_1 + \cdots + \lambda_n v_n, \lambda_i \in \mathbb{F}_p.$$

Tästä voidaan laskea $|F| = p^n$, koska $|\mathbb{F}_p| = p$.

Kunnan $F$ nollasta eroavia alkioita merkitään $F^*$ ja huomataan $|F^*| = p^n - 1$. Kirjoitetaan $p^n = q$. Kunnan nollasta eroavat alkiot muodostavat multiplikatiivisen ryhmän. Käytetään Lagrangen lausetta: jos $a \in F^*$, silloin $a$:n kertaluku jakaa luvun $q - 1$, eli $a^{q-1} = 1$. Näin ollen jokainen $a \in F^*$ toteuttaa yhtälön $x^{q-1} = 1$, josta seuraa,

että $x^q = x$ kaikille $a \in F$, koska myös 0 toteuttaa tämän yhtälön. Näin ollen polynomin

$$f(x) = x^q - x$$

juuret ovat täsmälleen $F$:n alkiot, sillä on $q$ erillistä juurta. Joten kunnan $F$ yli, polynomi

$$f(x) = x^q - x = \prod_{a \in F} (x - a),$$

joten $F$ on polynomin $f$ juurikunta. Tiedetään, että saman polynomin kaksi juurikuntaa ovat isomorfisia keskenään. Tätä käyttäen voidaan todeta, että jos on olemassa äärellinen kunta, jonka kertaluku on $p^n$, on tämä kunta polynomin $f(x) = x^{p^n} - x$ juurikunta yli $\mathbb{F}_p$:n ja se on isomorfiaa vaille yksikäsitteinen.

Nyt on todistettu seuraava lause:

**Lause 13.1.** *Olkoon $F$ äärellinen kunta, silloin jollekin alkuluvulle $p$*

1. *Kunnan $F$ karakteristika on $p > 0$, sen alkukunta on $\mathbb{F}_p$ ja $|F| = p^n$ ja $n = [F : \mathbb{F}_p]$*
2. *$F$ on polynomin $x^{p^n} - x \in \mathbb{F}_p[x]$ juurikunta. Erityisesti, kaksi äärellistä kuntaa, joiden koko on sama, ovat aina isomorfisia.*

**Lause 13.2.** *1. $F/\mathbb{F}_p$ on Galois'n laajennos ja $G(F/\mathbb{F}_p) \cong C_n$.*

2. *Olkoot $F_1, F_2$ kunnan $\mathbb{F}_p$ äärellisiä laajennoksia, joiden asteet ovat $m, n$. Silloin $F_1 \subseteq F_2$ jos ja vain jos $m \mid n$.*

*Todistus.* Laajennos $F/\mathbb{F}_p$ on polynomin $x^{p^n} - x$ juurikunta, ja se on myös separoituva, sillä $D(x^{p^n} - x) = -1 \neq 0$, minkä tahansa juuren kohdalla. Joten laajennos on Galois'n laajennos.

Tarkastellaan seuraavaksi Frobeniuksen homomorfismia

$$\phi : F \longrightarrow F, \alpha \mapsto \alpha^p.$$

Kuvaus on kuntien välillä, joten sen täytyy olla injektio, ja koska $F$ on äärellinen, on se myös isomorfismi (1. tehtäväpaperi). Jos $\alpha \in \mathbb{F}_p$, silloin $\phi(\alpha) = \alpha$, joten $\phi \in G(F/\mathbb{F}_p)$. Toisaalta, jos $\alpha \in F$ saadaan

$$\phi^n(\alpha) = \alpha^{p^n} = \alpha$$

ja näin ollen $\phi^n = 1 \in G(F/\mathbb{F}_p)$. Myös, jos $1 < i < n$, kuvaus $\phi^i$ ei voi olla triviaali, sillä $\alpha^{p^i} = \alpha$ ei voi päteä kaikille $\alpha \in F$ johtuen kuntalaajennoksen asteesta. Näin ollen $< \phi > \cong C_n \leq G(F/\mathbb{F}_p)$, mutta koska $[F : \mathbb{F}_p] = n$, tämä pakottaa $G(F/\mathbb{F}_p) \cong C_n$, ja Galois'n ryhmän on virittänyt Frobenius.

Toiseen kohtaan, jos $F_1 \subseteq F_2$, silloin saadaan torni kuntia ja Galois'n ryhmiä. Nyt $G(F_2/F_1) \leq G(F_2/\mathbb{F}_p) \cong C_n$, joten $G(F_2/F_1) \cong C_k$, jollekin $k \mid n$. Nyt $[F_2 : F_1] = k$ ja $n = [F_2 : \mathbb{F}_p] = [F_2 : F_1][F_1 : \mathbb{F}_p] = k \cdot m$, joten $m \mid n$. Jos toisaalta $m \mid n$, saadaan torni ryhmiä, missä $G = G(F_2/F_1) \cong C_{n/m}$, ja $F_1$ on tämän ryhmän kiintokunta ja näin ollen sisältyy $F_2$:een. □

**Esimerkki 13.3.** Kuinka monta jaotonta tekijää on polynomilla $x^{80} - 1$? Piirrä alikunnat laajennokselle $\mathbb{F}_{3^4}/\mathbb{F}_3$? Mikä on Galois'n ryhmä polynomille $x^2 + 2x + 2$ kunnan $\mathbb{F}_3$ yli? Vastaus $C_2$, koska polynomi on jaoton. Polynomilla ja sen derivaatalla ei myöskään ole yhteisiä juuria, joten polynomi on separoituva.

# 14 Proäärelliset Galois'n ryhmät

Tavallinen Galois'n yhteys välikuntien ja Galois'n ryhmien välillä toimii vain, jos Galois'n laajennos on äärellinen. Jos laajennos on ääretön törmätään välittömästi ongelmiin, varsinkin kiintokuntien kohdalla.

Olkoon $N/K$ äärellinen Galois'n laajennos, ja $H_1, H_2 \leq G(N/K)$, joilla on sama kiintokunta. Silloin $H_1 = H_2$. Tämä ei ole välttämättä totta, jos $N/K$ on ääretön laajennos.

Olkoon $\mathbb{F}_p$ kunta, jossa $p$ on alkuluku ja $N = \cup_{i=1}^{\infty} \mathbb{F}_{p^i}$. Olkoon $\phi$ Frobeniuksen automorfismi $N/\mathbb{F}_p$, eli $\phi(x) = x^p$ kaikille $x \in N$. Olkoon $G_0$ Frobeniuksen virittämä $G(N/\mathbb{F}_p)$:n diskreetti aliryhmä. Se on numeroituva, ja sen kiintokunta on $\mathbb{F}_p$. Toisaalta, jokainen Galois'n ryhmän $G(\mathbb{F}_{p^{2^i}}/\mathbb{F}_p)$ alkiolla $\sigma_i$ on kaksi laajennosta alkioksi Galois'n ryhmään $G(\mathbb{F}_{p^{2^{i+1}}}/\mathbb{F}_p)$. Näin ollen on olemassa $2^{\aleph_0}$ jonoa $(\sigma_1, \sigma_2, \ldots, ...)$, jossa $\sigma_i \in G(\mathbb{F}_{p^{2^i}}/\mathbb{F}_p)$ missä $\sigma_{i+1}|_{\mathbb{F}_{p^{2^i}}} = \sigma_i$ kaikille $i$. Nyt Jokainen tällainen jono määrittelee yksikäsitteisen alkion $\sigma \in G(N/\mathbb{F}_p)$, joka rajoittuu kuitenkin $\sigma_i$:si jokaisessa äärellisessä laajennoksessa. Näin ollen $G(N/\mathbb{F}_p)$:n mahtavuus on $2^{\aleph_0}$, joten $G(N/\mathbb{F}_p)$ on erisuuri kuin $G_0$, vaikka niiden kummankin kiintokunta on $\mathbb{F}_p$.

Ääretön Galois'n teoria vaatii topologiaa toimiakseen. Määritellään seuraavaksi käänteinen järjestelmä ja käänteinen raja-arvo.

Olkoon $I$ joukko, jossa on osittainen järjestys $\leq$. Tämä on $\leq$ on binäärirelaatio, joka on refleksiivinen ja transitiivinen ja lisäksi $a \leq b$ ja $b \leq a$ antaa $a = b$. Jos tämän lisäksi kaikille $i, j \in I$ on olemassa $k \in I$, jolla $i \leq k$ ja $j \leq k$, kutsutaan joukkoa $(I, \leq)$ suunnatuksi osittain järjestetyksi joukoksi.

Esimerkiksi $\mathbb{Z}$ ja normaali $\leq$ antavat suunnatun osittain järjestetyn joukon.

Käänteinen järjestys joukon $(I, \leq)$ yli koostuu joukoista $S_i$ ja kuvauksista $\pi_{ji} : S_j \longrightarrow S_i$ kaikille $i, j \in I$ ja toteuttaa seuraavat ehdot

1. $\pi_{ii}$ on identiteettikuvaus kaikille $i \in I$
2. $\pi_{ki} = \pi_{ji} \circ \pi_{kj}$ jos $i \leq j \leq k$.

Olkoon $S$ se karteesisen tulon $\prod_{i \in I} S_i$ osajoukko, joka koostuu jonoista $s = (s_i)$ ja $\pi_{ji}(s_j) = s_i$ kaikille $i \leq j$.

**Esimerkki 14.1.** Tarkastellaan syklisiä ryhmiä $C_{p^i}$, ne voidaan järjestää $\mathbb{N}$:n mukaan ja järjestyksellä on luonnollinen esitys. Nyt voidaan määritellä projektiiviset homomorfismit $\pi_{ji} : C_{p^j} \longrightarrow C_{p^i}$ kuvaamaan $\pi_{ji} : a \pmod{p^j} \mapsto a \pmod{p^i}$. Nämä projektiot toteuttavat käänteisen systeemin ehdot. Käänteinen raja-arvo on tässä tapauksessa kaikki ne jonot, joille kuvaukset pätevät. Esimerkiksi otettakoon $p = 2$, kuten yllä ja tarkastellaan muutamaa jonoa. Tätä käänteistä rajaa kutsutaan $p$-adisiksi luvuiksi ja sitä merkitään $\mathbb{Z}_p$. Tässä vihdoin selitys sille, miksi en halua merkitä syklistä ryhmää samalla tavalla!

Käänteiselle raja-arvolle voi antaa topologian karteesisen tulon $\prod_{i \in I} S_i$ topologian osajoukkona. Kaikki $S_i$:t ovat äärellisiä ja niille voi antaa diskreetin topologian. Ne ovat myös kompakteja, ja näin ollen Tychonovin lauseen perusteella $\prod_{i \in I} S_i$ on myös kompakti, ja $\varprojlim \prod_{i \in I} S_i$. Se toteuttaa myös Hausdorffin ehdon ja on täysin epäyhteinäinen.

**Määritelmä 14.2.** Proäärellinen ryhmä on topologinen ryhmä, joka on äärellisten ryhmien käänteinen raja-arvo.

**Määritelmä 14.3.** Topologinen ryhmä on ryhmä $G$, jolle on annettu topologia ja jossa kuvaukset

$$(g, h) \mapsto gh$$

ja

$$g \mapsto g^{-1}$$

ovat jatkuvia kuvauksia.

Jokaiselle $a \in G$ kuvaukset $x \mapsto ax$, $x \mapsto xa$ ja $x \mapsto x^{-1}$ ovat homeomorfismeja. Oletamme aina, että $\{1\}$ on suljettu joukko, ja yllä olevan perusteella kaikki $\{a\}$ ovat suljettuja joukkoja $G$:ssä.

Toinen ekvivalentti karakterisaatio proäärelliselle ryhmälle on seuraava.

**Lause 14.4.** *Kompakti, Hausdorffin ehdon toteuttava, täysin epäyhtenäinen topologinen ryhmä on proäärellinen ryhmä. Sen avoimet aliryhmät muodostavat kannan identiteettialkion ympäristöille.*

Mikä tahansa aliryhmä, joka sisältää avoimen joukon, on itsessään avoin, toinen ehto voidaan antaa muodossa: jokainen avoin joukko, joka sisältää identiteettialkion, sisältää avoimen aliryhmän.

**Propositio 14.5.** *Olkoon $G$ proäärellinen ryhmä.*

1. *Jokainen $G$:n avoin aliryhmä on suljettu, sen indeksi on äärellinen ja se sisältää $G$:n avoimen normaalin aliryhmän. Suljettu aliryhmä $G$:ssä on avoin, jos ja vain jos sen indeksi on äärellinen. Avointen aliryhmien perhe leikkaa pisteessä $\{1\}$.*
2. *$G$:n osajoukko on avoin jos ja vain jos se on avointen normaalien aliryhmien sivuluokkien yhdiste.*

**Määritelmä 14.6.** Algebrallinen laajennos $N/K$ on Galois'n laajennos, jos se on normaali ja separoituva. Äärettömässä tapauksessa tämä tarkoittaa sitä, että $N/K$ on Galois'n laajennos jos ja vain jos se on äärellisten Galois'n laajennosten yhdiste.

**Propositio 14.7.** *Jos $N/K$ on Galois'n laajennos, silloin myös $N/M$ on Galois'n laajennos, missä $M$ on mikä tahansa välikunta.*

**Propositio 14.8.** *Jos $N/K$ on Galois'n laajennos, ja $K \subset L \subset N$ on kuntatorni, silloin jokainen $K$:n kiinnittävä homomorfismi $L \longrightarrow N$ laajenee isomorfismiksi $N \longrightarrow N$, joka kiinnittää $K$:n.*

Äärettömän laajennoksen kohdalla käytetään Zornin lemmaa.

Merkitään nyt kaikkien välikuntien $K \subset L \subset N$ joukkoa, missä $L/K$ on äärellinen Galois'n laajennos, $\mathcal{L}$. Jokaista $L \in \mathcal{L}$ vastaa äärellinen Galois'n ryhmä $G(L/K)$. Jos nyt $L' \in \mathcal{L}$ ja $L \subseteq L'$, silloin $res_L : G(L'/K) \longrightarrow G(L/K)$ on surjektio, joten luodaan käänteinen raja $\varprojlim G(L/K)$, missä $L \in \mathcal{L}$. Jokainen $\sigma \in G(N/K)$ antaa yksikäsitteisesti $(res_L\sigma)_{L\in\mathcal{L}}$ käänteisessä rajassa $\varprojlim G(L/K)$.

Toiseen suuntaan, jokainen $(\sigma_L)_{L\in\mathcal{L}} \in \varprojlim G(L/K)$ määrettelee yksikäsitteisesti $\sigma \in G(N/K)$, jolle $res_L\sigma = \sigma_L$ kaikille $L \in \mathcal{L}$, joten $\sigma \mapsto (res_L\sigma)_{L\in\mathcal{L}}$ on isomorfismi

$$G(N/K) = \varprojlim G(L/K).$$

Tämä isomorfismi indusoi topologian ryhmälle $G(N/K)$ käänteisen raja-arvon topologian kautta. Tätä topologiaa kutsutaan Krullin topologiaksi. Nyt $G(N/K)$ on proäärellinen ryhmä, ja $\mathcal{N} = \{G(N/L) : L \in \mathcal{L}\}$ muodostaa identiteettialkion avoimen ympäristökannan.

**Määritelmä 14.9.** Oletetaan, että $L \subset N$ on $K$:n äärellinen laajennos. Kunnan $L$ Galois'n sulkeuma $\hat{L}$ on pienin $K$:n Galois'n laajennos, joka sisältää $L$:n.

Nyt $\hat{L}$ on äärellinen $K$:n laajennos ja se sisältyy kuntaan $N$. Ryhmä $G(N/L)$ voidaan nyt kirjoittaa ryhmän $G(N/\hat{L})$ oikeiden sivuluokkien yhdisteeksi. Näin ollen $G(N/L)$ on avoin ja suljettu $G(N/K)$:n aliryhmä.

Olkoon $L$ mielivaltainen välikunta. Silloin $L$ voidaan antaa jonkun perheen $\{L_i : i \in I\}$ yhdisteenä, jossa jokainen $L_i$ on $K$:n äärellinen laajennos.Näin ollen $G(N/L) = \cap_{i\in I} G(N/L_i)$. Ja $G(N/L)$ on $G(N/K)$:n suljettu aliryhmä. Huomaa, että tässä laajennos $L$ voi olla ääretön.

Olkoon $S$ nyt joukko $N$:n automorfismeja. Määritellään

$$N(S) = \{x \in N : \sigma x = x \forall \sigma \in S\}$$

$S$:n kiintokunta $N$:ssä. Havaitaan, että $N(S)$ on myös joukon $\langle S\rangle$ virittämän ryhmän kiintokunta. Ryhmä $\langle S\rangle$ on suljettu $G(N/K)$:n aliryhmä.

Jos $M$ on $K$:n Galois'n laajennos, joka sisältyy kuntaan $N$, merkitään homomorfismia $res_M : G(N/K) \longrightarrow G(M/K)$ jatkuvaa surjektiota, joka kuvaa $\sigma \mapsto res_M \sigma$.

**Lause 14.10** (Äärettömän Galois'n teorian päälause)**.** *Olkoon $N/K$ Galois'n laajennos ja $G(N/K)$ sen Galois'n ryhmä.*

1. *Kunta $N$ on Galois'n laajennos jokaisen välikunnan $L$ yli. Lisäksi $G(N/L)$ on $G(N/K)$:n suljettu aliryhmä, ja sen kiintokunta on $M$.*
2. *Jokaiselle aliryhmälle $H \leq G(N/K)$, Galois'n ryhmä $G(N/N^H)$ on ryhmän $H$ topologinen sulkeuma.*
3. *Kuvaukset $H \mapsto N^H$ ja $L \mapsto G(N/L)$ ovat toistensa käänteisbijektioita joukkojen*

   $$\{G(N/K) : n \text{ suljetut aliryhmat}\} \leftrightarrow \{\text{valikunnat } K \subset L \subset N\}.$$

4. *Kuvaus kääntää järjestyksen, eli $H_2 \leq H_1 \Leftrightarrow N^{H_1} \subseteq N^{H_2}$.*
5. *Suljettu aliryhmä $H \leq G$ on avoin, jos ja vain jos $N^H$:n aste yli $K$:n on äärellinen, missä tapauksessa $[G : H] = [N^H : K]$*
6. *Suljettu aliryhmä $H \leq G$ on normaali, jos ja vain jos $N^H$ on Galois'n laajennos yli $K$:n, missä tapauksessa $G(N^H/K) \cong G/H$.*