Proäärelliset ryhmät ja kuntalaajennukset

Matti Åstrand

Helsinki 25.5.2009

Pro gradu -tutkielma

HELSINGIN YLIOPISTO
Matematiikan ja tilastotieteen laitos

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen tiedekunta	Matematiikan ja tilastotieteen laitos

Tekijä — Författare — Author

Matti Åstrand

Työn nimi — Arbetets titel — Title

Proäärelliset ryhmät ja kuntalaajennukset

Oppiaine — Läroämne — Subject

Matematiikka

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Pro gradu -tutkielma	25.5.2009	34 sivua

Tiivistelmä — Referat — Abstract

Topologinen ryhmä on *proäärellinen*, jos se voidaan esittää äärellisten diskreettien ryhmien käänteisenä rajana. Tämä voidaan muotoilla topologisesti siten, että ryhmä on topologisena avaruutena kompakti täysin epäyhtenäinen Hausdorff-avaruus. Tässä pro gradu-tutkielmassa tutustutaan proäärellisiin ryhmiin ja esitellään, miten ne liittyvät kuntalaajennuksiin.

Yksi päätuloksista on se, että algebrallisten Galois-laajennusten Galois-ryhmät ovat proäärellisiä ja toisaalta kaikki proäärelliset ryhmät ovat isomorfisia jonkin Galois-ryhmän kanssa. Tässä Galois-ryhmälle annetaan Krullin topologia, jolloin siitä tulee topologinen ryhmä.

Ilman Krullin topologiaa äärettömillä Galois-laajennuksilla ei olisi samanlaisia ominaisuuksia kuin äärellisillä laajennuksilla. Esimerkiksi Galois-ryhmän aliryhmien ja laajennuksen alilaajennusten välillä ei ole samanlaista vastaavuutta. Tämä korjaantuu, kun rajoitutaan suljettuihin aliryhmiin.

Tutkielmassa myös luokitellaan äärelliset kunnat eli osoitetaan, että äärellisen kunnan koko on aina alkuluvun potenssi ja että kaikilla alkuluvun potensseilla p^n on olemassa yksikäsitteinen kunta, jonka koko on p^n. Tämä tehdään laskemalla kombinatorisesti jaottomien polynomien lukumääriä, jolloin nähdään, että kaikenasteisia jaottomia polynomeja on olemassa. Laskennassa käytetään formaaleja potenssisarjoja.

Loppupuolella tutustutaan Nottinghamin ryhmään. Sen alkiot ovat $\mathbb{F}_p$-kertoimisia potenssisarjoja, mutta ne voi ajatella myös renkaan $\mathbb{F}_p[[t]]$ automorfismeiksi. Nottinghamin ryhmä on esimerkki pro-p-ryhmästä, eli se on äärellisten p-ryhmien projektiivinen raja. Tämä ehto on yhtäpitävä sen kanssa, että ryhmän jokaisen avoimen aliryhmän indeksi on p:n potenssi.

Kaikille proäärellisille ryhmille voidaan määritellä todennäköisyysmitta, joka on translaatioinvariantti, eli $\mu(aS) = \mu(S)$ kaikilla alkioilla a ja mitallisilla joukoilla S. Tätä mittaa kutsutaan Haarin mitaksi. Sille pätee myös, että koko ryhmän mitta on 1 (eli kyseessä on todennäköisyysmitta), ja kaikki Borel-joukot ovat mitallisia.

Avainsanat — Nyckelord — Keywords

kunnat, kuntalaajennukset, Galois-teoria, topologiset ryhmät, proäärelliset ryhmät

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — övriga uppgifter — Additional information

Sisältö

1 Johdanto

Tässä tutkielmassa tutkitaan proäärellisiä ryhmiä erityisesti Galois-teorian näkökulmasta. Galois-teoria tutkii kuntalaajennuksia ja niiden symmetrioita. Nämä symmetriat muodostavat ryhmän, jota kutsutaan *Galois-ryhmäksi*.

Galois-teoria on saanut nimensä ranskalaisen Évariste Galois'n mukaan. Galois tunnetaan siitä, että hän selvitti polynomiyhtälöiden ratkeavuuden kriteerin. Nykyaikaisella terminologialla ilmaistuna hän todisti, että polynomiyhtälö ratkeaa juurilausekkeilla, jos ja vain jos polynomin juurikunnan Galois-ryhmä on ratkeava. Myös ratkeavan ryhmän käsite on saanut nimensä tästä yhteydestä ryhmäteorian ja polynomiyhtälöiden ratkeavuuden välillä. Tässä tutkielmassa ei puhuta ratkeavista ryhmistä, mutta käsitteet *juurikunta* ja *Galois-ryhmä* määritellään luvussa 5.

Kun Galois-ryhmälle annetaan sopiva topologia – niin kutsuttu *Krullin topologia* – saadaan topologinen ryhmä, joka on *proäärellinen*. Tämä tarkoittaa, että Galois-ryhmät ovat aina äärellisten ryhmien käänteisiä rajoja eli projektiivisesti äärellisiä. Toisaalta kaikki tällaiset ryhmät ovat Galois-ryhmiä. Tämä muotoillaan tarkemmin ja todistetaan luvussa 8. Tätä ennen esitellään tarpeellisia esitietoja topologiasta, ryhmäteoriasta sekä kunnista ja niiden laajennuksista.

Krullin topologia on nimetty saksalaisen Wolfgang Krullin mukaan, joka tunnetaan paremmin hänen renkaisiin liittyvistä tuloksistaan. Krull määritteli topologian Galois-ryhmiin 1920-luvulla ja sen avulla onnistui laajentamaan kuntalaajennusten teorian äärellisistä laajennuksista äärettömiin. Ilman topologiaa äärettömien laajennusten tutkiminen on vaikeaa, sillä äärellisten laajennusten tulokset eivät päde sellaisinaan.

Tutkielmassa tarkastellaan myöhemmin Nottinghamin ryhmää, joka on esimerkki *pro-p-ryhmästä*. Tämä tarkoittaa, että se on raja äärellisistä ryhmistä, joiden koko on jonkin kiinnitetyn alkuluvun potenssi. Lopuksi näytetään, miten jokaiselle proäärelliselle ryhmälle voidaan antaa mitta, jolla on hyödyllisiä ominaisuuksia.

Lukijan on syytä tuntea kuntalaajennusten perusteet esimerkiksi kurssin Algebra II laajuudessa. Topologian alkeista olisi hyvä tuntea ainakin kompaktisuus ja yhtenäisyys. Joitain topologian tietoja esitellään tutkielman alussa. Aivan lopussa tarvitaan myös mittateoriaa, mutta muissa osissa sitä ei tarvita.

Merkinnöistä

- Luonnollisten lukujen joukko $\mathbb{N}$ sisältää nollan.
- Aina, kun $\mathcal{A}$ on joukkoperhe, niin $\bigcup \mathcal{A} = \bigcup_{A \in \mathcal{A}} A$ on $\mathcal{A}$:n joukkojen yhdiste ja $\bigcap \mathcal{A} = \bigcap_{A \in \mathcal{A}} A$ niiden leikkaus.

2 Topologian perustietoja

Tässä luvussa käydään läpi sellaisia topologian tietoja, jotka ovat myöhemmin tarpeen. Myös muissa luvuissa tullaan kertaamaan joitain yksittäisiä tuloksia, jos niitä tarvitaan todistuksissa.

2.1 Kannat ja esikannat

Määritelmä. Olkoon (X, τ) topologinen avaruus.

- Joukko $\mathcal{B} \subset \tau$ on topologian τ *kanta*, jos jokainen avoin joukko $U \in \tau$ voidaan esittää $\mathcal{B}$:n joukkojen yhdisteenä.
- Joukko $\mathcal{B}_x \subset \tau$ on pisteen $x \in X$ *ympäristökanta*, jos jokaiselle pisteen x ympäristölle $U \in \tau$ on olemassa joukko $V \in \mathcal{B}_x$, jolle $V \subset U$.
- Joukko $\mathcal{S} \subset \tau$ on topologian τ *esikanta*, jos sen joukkojen äärelliset leikkaukset muodostavat τ:n kannan.
- Joukko $\mathcal{S}_x \subset \tau$ on pisteen $x \in X$ *ympäristöesikanta*, jos $\mathcal{S}_x$:n joukkojen äärelliset leikkaukset muodostavat x:n ympäristökannan.

Kantojen avulla voidaan määritellä uusia topologioita. Esimerkiksi, jos X_i on topologinen avaruus kaikilla $i \in I$, niin näiden tulojoukolle $X = \prod_{i \in I} X_i$ saadaan topologia ottamalla esikannaksi joukot muotoa $p_i^{-1}(U)$, jossa $U \subset X_i$ on avoin ja p_i on projektiokuvaus $p_i : X \to X_i$. Saatua topologiaa kutsutaan avaruuksien X_i topologioiden *tulotopologiaksi*.

Lause 2.1. *Olkoot X ja Y topologisia avaruuksia ja $f : X \to Y$ kuvaus.*

1. *Jos $\mathcal{S}$ on avaruuden Y esikanta ja $f^{-1}(U)$ on avoin kaikilla $U \in \mathcal{S}$, niin f on jatkuva.*
2. *Jos $\mathcal{B}$ on avaruuden X kanta ja $f(U)$ on avoin kaikilla $U \in \mathcal{B}$, niin f on avoin.*

Todistus. Olkoon $\mathcal{S}$ avaruuden Y esikanta. Jos $A \subset Y$ on avoin ja $x \in f^{-1}(A)$, niin on olemassa äärellinen määrä esikannan $\mathcal{S}$ joukkoja $U_1, \ldots, U_r$, joille $f(x) \in U_1 \cap \cdots \cap U_r \subset A$. Tällöin

$$x \in f^{-1}(U_1) \cap \cdots \cap f^{-1}(U_r) \subset f^{-1}(A).$$

Ylläoleva leikkaus on avoin, joten $f^{-1}(A)$ on alkion x ympäristö. Tämä pätee kaikilla $x \in f^{-1}(A)$, joten $f^{-1}(A)$ on avoin ja f on jatkuva.

Olkoon nyt $\mathcal{B}$ avaruuden X kanta. Tällöin jokainen avoin joukko $A \subset X$ on yhdiste jostain kokoelmasta $C_A \subset \mathcal{B}$, ja tällöin

$$f(A) = f(\bigcup C_A) = \bigcup f(C_A),$$

joka on avoin, sillä jokainen $f(C_A)$:n joukko on oletuksen nojalla avoin. □

2.2 Kompaktisuus ja Tihonovin lause

Kompaktisuudelle on monta vaihtoehtoista määritelmää, joita käytetään tarpeen mukaan eri paikoissa. Otetaan seuraava tulos käyttöön ilman todistusta:

Lause 2.2. *Olkoon X topologinen avaruus. Seuraavat ehdot ovat yhtäpitäviä:*

1. *Jos $\mathcal{U}$ on perhe X:n avoimia joukkoja, joiden yhdiste on koko avaruus X, niin on olemassa äärellinen osaperhe $\mathcal{U}_0 \subset \mathcal{U}$, jonka yhdiste on myös X.*
2. *Jos $\mathcal{F}$ on perhe X:n suljettuja joukkoja, jolle jokaiselle äärelliselle $\mathcal{F}_0 \subset \mathcal{F}$ pätee $\bigcap \mathcal{F}_0 \neq \emptyset$, niin $\bigcap \mathcal{F} \neq \emptyset$. Toisin sanoen, jos $\mathcal{F}$:n kaikki äärelliset leikkaukset ovat epätyhjiä, niin koko $\mathcal{F}$:n leikkaus on epätyhjä.*
3. *Jos U on avoin joukko ja $\mathcal{F}$ perhe X:n suljettuja joukkoja, joiden leikkaus on U:n osajoukko, niin myös jonkin $\mathcal{F}$:n äärellisen osaperheen leikkaus on U:n osajoukko.*

Avaruutta, jolle jokin näistä ehdoista on voimassa, kutsutaan *kompaktiksi.*

Seuraavaa käsitettä käytetään Tihonovin lauseen todistuksessa.

Määritelmä. Olkoon X joukko ja $\mathcal{P}(X)$ joukon X osajoukkojen joukko. Oletetaan, että perhe $\mathcal{L} \subset \mathcal{P}(X)$ on suljettu leikkauksen suhteen. Perhe $\mathcal{F} \subset \mathcal{L}$ on $\mathcal{L}$*-filtteri*, jos seuraavat ehdot ovat voimassa:

1. Jos $A, B \in \mathcal{F}$, niin $A \cap B \in \mathcal{F}$
2. Jos $A \in \mathcal{F}$ ja $A \subset B \in \mathcal{L}$, niin $B \in \mathcal{F}$.
3. $\emptyset \notin \mathcal{F}$

Kaikkien $\mathcal{L}$-filttereiden joukko voidaan järjestää sisältymisen suhteen. Maksimaalista $\mathcal{L}$-filtteriä kutsutaan $\mathcal{L}$*-ultrafiltteriksi.* Zornin lemmasta seuraa, että jokaisen $\mathcal{L}$-filtterin voi laajentaa $\mathcal{L}$-ultrafiltteriksi.

Lemma 2.3. *Topologinen avaruus X on kompakti, jos ja vain jos jokaisen suljettujen joukkojen perheen ultrafiltterin $\mathcal{U}$ leikkaus $\bigcap \mathcal{U}$ on epätyhjä.*

Todistus. Olkoon A perhe X:n suljettuja osajoukkoja, joiden äärelliset leikkaukset ovat epätyhjiä. Tällöin A voidaan laajentaa filtteriksi $\mathcal{F}$ ottamalla mukaan kaikki X:n suljetut osajoukot, jotka sisältävät jonkin A:n äärellisen leikkauksen. Filtteri $\mathcal{F}$ voidaan puolestaan laajentaa ultrafiltteriksi $\mathcal{U}$, joka edelleen sisältää perheen A. Koska $\mathcal{U}$:n leikkaus on epätyhjä, on myös A:n leikkauksen oltava epätyhjä, joten X on kompakti.

Oletetaan nyt, että X on kompakti ja $\mathcal{U}$ on suljettujen joukkojen ultrafiltteri. Tällöin $\mathcal{U}$:n äärelliset leikkaukset ovat epätyhjiä, joten $\mathcal{U}$:n koko leikkauskin on epätyhjä. □

Tihonovin lause. *Jos avaruudet X_i ovat kompakteja kaikilla $i \in I$, niin myös niiden tuloavaruus $X = \prod_{i\in I} X_i$ on kompakti.*

Todistus. Lemman 2.3 nojalla riittää näyttää, että mielivaltaisella X:n suljettujen joukkojen perheen ultrafiltterillä $\mathcal{F}$ on epätyhjä leikkaus.

Jos $\mathcal{F}$ on annettu ultrafiltteri, määritellään kaikille $i \in I$ perhe

$$\mathcal{F}_i = \{F \subset X_i \mid F \text{ suljettu ja } F \supset p_i(A) \text{ jollain } A \in \mathcal{F}\}.$$

Tällöin $\mathcal{F}_i$ on X_i:n suljettujen joukkojen perheen filtteri:

- $p_i(A) \neq \emptyset$ aina, kun $A \in \mathcal{F}$, joten $\emptyset \notin \mathcal{F}_i$.
- Jos F on mielivaltainen $\mathcal{F}_i$:n joukko, jossa $F \supset p_i(A)$ ja $A \in \mathcal{F}$, niin kaikilla suljetuilla $H \supset F$ pätee $H \supset p_i(A)$. Siis $H \in \mathcal{F}_i$.
- Jos $F \supset p_i(A)$ ja $H \supset p_i(B)$ ovat mielivaltaisia $\mathcal{F}_i$:n joukkoja, jossa $A, B \in \mathcal{F}$, niin niiden leikkaus toteuttaa

  $$F \cap H \supset p_i(A) \cap p_i(B) \supset p_i(A \cap B).$$

  Tässä myös $A \cap B \in \mathcal{F}$, joten $F \cap H \in \mathcal{F}_i$.

Näin ollen joukolla $\mathcal{F}_i$ on epätyhjä leikkaus: olkoon $a_i \in \bigcap \mathcal{F}_i$. Merkitään $a = (a_i)_{i\in I} \in X$.

Osoitetaan nyt, että $a \in C$ kaikilla $C \in \mathcal{F}$, jolloin $\mathcal{F}$:n leikkaus on epätyhjä. Olkoon $C \in \mathcal{F}$, jolloin C on suljettu joukko. Jos $a \notin C$, niin a:lla on jokin avoin ympäristö $U = \bigcap_{i\in I_0} p_i^{-1}(U_i)$, jossa $I_0 \subset I$ on äärellinen, $U_i \subset X_i$ on avoin ja $C \cap U = \emptyset$. Tällöin

$$C \subset X \setminus U = \bigcup_{i\in I_0} X \setminus p_i^{-1}(U_i),$$

joten jokin suljetuista joukoista $X \setminus p_i^{-1}(U_i) \in \mathcal{F}$, koska $\mathcal{F}$ on ultrafiltteri. Nyt $p_i(X \setminus p_i^{-1}(U_i)) = X_i \setminus U_i \in \mathcal{F}_i$, mutta $a_i \notin X_i \setminus U_i$, joka on ristiriita, sillä a_i valittiin joukosta $\bigcap \mathcal{F}_i$. Siis $a \in C$ kaikilla $C \in \mathcal{F}$. □

3 Polynomit ja potenssisarjat

3.1 Renkaat ja kunnat

Määritelmä. Olkoon $(R, +, \cdot, 0, 1)$ struktuuri, jossa R on joukko, $+$ ja $\cdot$ joukon R laskutoimituksia sekä 0 ja 1 joukon R alkioita. Tällöin $(R, +, \cdot, 0, 1)$ on *rengas*, jos seuraavat aksioomat pätevät:

1. $(R, +)$ on vaihdannainen ryhmä, jonka neutraalialkio on 0.

2. $(R, \cdot)$ on monoidi, jonka neutraalialkio on 1.

3. Kaikilla $a, b, c \in R$ pätee $a(b + c) = ab + ac$ sekä $(a + b)c = ac + bc$.

Jos lisäksi $(R \setminus \{0\}, \cdot)$ on vaihdannainen ryhmä, niin R on *kunta*.

Tässä siis määritelmän mukaan rengas on aina ykkösellinen ja liitännäinen. Renkaan ei tarvitse olla vaihdannainen, mutta kunta on aina vaihdannainen.

Määritelmä. Olkoon R rengas. Joukko $I \subset R$ on *ideaali*, jos seuraavat ehdot ovat voimassa:

1. Kaikilla $a, b \in I$ myös $a + b \in I$.

2. Kaikilla $a \in I$ ja $x \in R$ pätee $ax \in I$ ja $xa \in I$.

Ideaali I on *maksimaalinen*, jos $I \subsetneq R$ ja ei ole olemassa ideaalia J, jolle $I \subsetneq J \subsetneq R$.

Huomataan, että ideaali $I \subsetneq R$, jos ja vain jos $1 \notin I$. Tämän ja Zornin lemman avulla voidaan näyttää, että jokainen R:n ideaali $I \subsetneq R$ voidaan laajentaa maksimaaliseksi ideaaliksi.

Renkaan ideaali on tietyssä mielessä sama asia kuin ryhmän normaali aliryhmä. Sellaisen avulla voidaan määritellä ekvivalenssirelaatio, jonka suhteen laskutoimitukset ovat hyvin määriteltyjä.

Lause 3.1. *Olkoon R rengas ja I sen ideaali. Tällöin relaatio*

$$a \sim b \Leftrightarrow a - b \in I$$

on ekvivalenssirelaatio ja renkaan R laskutoimitukset ovat ekvivalenssiluokissa hyvin määriteltyjä: Jos $a_1 \sim a_2$ ja $b_1 \sim b_2$, niin $(a_1 + b_1) \sim (a_2 + b_2)$ ja $a_1 b_1 \sim a_2 b_2$.

Lisäksi, jos $\sim$ on tällainen ekvivalenssirelaatio, niin se on yllämainittua muotoa ideaalille I, joka on 0:n ekvivalenssiluokka $\sim$:ssä.

Todistus. Olkoon I renkaan R ideaali. Jos $a_1 - a_2 \in I$ ja $b_1 - b_2 \in I$, niin

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I,$$

koska I on suljettu yhteenlaskun suhteen. Myös

$$a_1 b_1 - a_2 b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2 \in I.$$

Olkoon nyt $\sim$ renkaan R ekvivalenssirelaatio, joka toteuttaa yllämainitut ehdot. Merkitään I:llä alkion 0 ekvivalenssiluottaa $\sim$:ssä. Nyt jos $a \in I$ ja $b \in I$, niin $a + b \sim 0 + 0 = 0$, joten $a + b \in I$. Jos $x \in R$, niin edelleen $ax \sim 0x = 0$, joten $ax \in I$ ja vastaavasti $xa \in I$. Joukko I on siis ideaali.

Jos $a, b \in R$, niin

$$a \sim b \iff a - b \sim 0 \iff a - b \in I,$$

joten $\sim$ on väitettyä muotoa. □

Jos I on renkaan R ideaali, voidaan muodostaa *tekijärengas* R/I, jonka alkiot ovat I:n määräämiä ekvivalenssiluokkia. Tällöin Lauseen 3.1 nojalla R/I:ssä laskutoimitukset voidaan määritellä R:n laskutoimitusten avulla. Osoitetaan nyt hyödyllinen kriteeri sille, milloin tekijärengas on kunta.

Lause 3.2. *Olkoon R vaihdannainen rengas ja I sen ideaali, jolle $I \neq R$. Tällöin tekijärengas R/I on kunta, jos ja vain jos I on maksimaalinen.*

Todistus. Seuraavat ehdot ovat yhtäpitäviä:

1. R/I on kunta.
2. Kaikilla $x \in R/I$, jossa $x \neq 0$, on olemassa $y \in R/I$, jolle $yx = 1$.
3. Kaikilla $x \in R \setminus I$ on olemassa $y \in R$, jolle $yx - 1 \in I$.
4. Kaikilla $x \in R \setminus I$ pätee $1 \in \{yx + a \mid y \in R, a \in I\}$.
5. Kaikilla $x \in R \setminus I$ joukon $I \cup \{x\}$ virittämä ideaali on R.
6. I on maksimaalinen.

□

3.2 Potenssisarjat

Jos F on kunta, niin F-kertoimisten polynomien joukko $F[t]$ on *kokonaisalue*. Tämä tarkoittaa, että kahden nollasta eroavan alkion $f(t), g(t) \in F[t]$ tulo ei ole nolla: $f(t)g(t) \neq 0$. Sen jakokunta on $F(t)$ eli rationaalilausekkeiden kunta.

Jos polynomeissa sallitaan äärettömän monta nollasta eroavaa termiä, niin saadaan F:n *potenssisarjojen* rengas $F[[t]]$. Niiden kertolasku on hyvin määritelty, sillä jokaiseen termiin vaikuttaa vain äärellinen määrä tekijöiden termejä. Tarkemmin: potenssisarjojen rengas $F[[t]]$ on funktioiden $f : \mathbb{N} \to F$ joukko. Niiden yhteenlasku suoritetaan pisteittäin, eli $(f + g)(n) = f(n) + g(n)$ ja kertolasku *konvoluutiolla*:

$$(fg)(n) = \sum_{i=0}^{n} f(i)g(n-i).$$

Alkiota $f \in F[[t]]$ merkitään $f(t) = \sum_{n\geq 0} a_n t^n$, jossa $a_n = f(n)$ ja t on vapaa muuttujasymboli. Ensimmäistä termiä kutsutaan *vakiotermiksi* ja merkitään $a_0 = f(0)$.

Jos $f(t) = \sum_{i\geq 0} a_i t^i \in F[[t]]$, jossa $a_0 \neq 0$, niin sillä on käänteisalkio $g(t) = f(t)^{-1} \in F[[t]]$. Merkitään $g(t) = \sum_{j\geq 0} b_j t^j$, ja kirjoitetaan auki yhtälö $g(t)f(t) = 1$:

$$\begin{aligned} a_0 b_0 &= 1 \\ a_0 b_1 + a_1 b_0 &= 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 &= 0 \end{aligned}$$

Tästä voidaan ratkaista kertoimet $b_0 = a_0^{-1}$ ja $b_j = -a_0^{-1} \sum_{i<j} a_{j-i} b_i$, kun $j \geq 0$. Näin saatu sarja $g(t)$ on sarjan $f(t)$ käänteisalkio renkaassa $F[[t]]$.

Potenssisarjojen renkaan jakokuntaa merkitään $F((t))$. Ylläolevasta seuraa, että jokainen nollasta eroava alkio $f(t) \in F((t)) \setminus \{0\}$ on muotoa $t^n f_1(t)$, jossa n on kokonaisluku, $f_1(t) \in F[[t]]$ ja $f_1(0) \neq 0$. Tällaisen sarjan käänteisalkio on nimittäin $t^{-n} f_1(t)^{-1}$, jossa $f_1(t)^{-1} \in F[[t]]$.

Toisin sanoen sarja on ääretön vain "yhteen suuntaan". Tällaisia sarjoja kutsutaan *Laurent-sarjoiksi*. Huomaa, että tämä on eri asia kuin kompleksianalyysin Laurent-sarja, joka voi olla "molempiin suuntiin" ääretön.

3.3 Potenssisarjojen itseisarvo

Oletetaan, että R on kokonaisalue. Määritellään renkaaseen $R[[t]]$ itseisarvo seuraavasti:

$$\left| \sum_{i \geq 0} a_i t^i \right| = 2^{-n}, \text{jossa } n \text{ on pienin indeksi, jolle pätee } a_n \neq 0 \tag{1}$$

sekä $|0| = 0$.

Lause 3.3. *Yhtälöllä* (1) *määritelty itseisarvo toteuttaa seuraavat ominaisuudet:*

1. $|f(t) - g(t)| \leq 2^{-n}$*, jos ja vain jos* $f(t) \equiv g(t) \pmod{t^n}$.
2. *Jos* $a \in R$ *ja* $a \neq 0$*, niin* $|a| = 1$.
3. *Jos* $|f(t) + g(t)| \leq \max\{|f(t)|, |g(t)|\}$.
4. $|f(t)g(t)| = |f(t)||g(t)|$.
5. *Metriikka* $d(f(t), g(t)) = |f(t) - g(t)|$ *on täydellinen, eli jokainen Cauchy-jono suppenee.*
6. *Summa* $\sum_{n \geq 0} f_n(t)$ *suppenee, jos ja vain jos* $|f_n(t)| \to 0$*, kun* $n \to \infty$.

Todistus. Itseisarvolle pätee, että $|f(t)| \leq 2^{-n}$, jos ja vain jos $f(t) = t^n f_1(t)$, jossa $f_1(t) \in R[[t]]$. Tästä kohta 1 seuraa suoraan.

Jos $a \in R$ ja $a \neq 0$, niin $a \neq t^n h(t)$ millään $h(t) \in R[[t]]$, joten $|a| = 1$. Jos $f(t) = t^n f_1(t)$ ja $g(t) = t^n g_1(t)$, niin $f(t) + g(t) = t^n(f_1(t) + g_1(t))$. Kohdat 2 ja 3 siis pätevät.

Olkoot $f(t) = t^n f_1(t)$ ja $g(t) = t^m g_1(t)$, jossa $f_1(t), g_1(t) \neq 0$ eli $|f(t)| = 2^{-n}$ ja $|g(t)| = 2^{-m}$. Tällöin $f(t)g(t) = t^{n+m} f_1(t) g_1(t)$ ja koska R on kokonaisalue, niin $f_1(0)g_1(0) \neq 0$. Siis $|f(t)g(t)| = 2^{-(n+m)} = |f(t)||g(t)|$.

Osoitetaan, että metriikka on täydellinen. Jos $(f_i(t))_i$ on Cauchy-jono, niin kaikilla $n \in \mathbb{N}$ on jokin m, jolle $|f_i(t) - f_j(t)| \leq 2^{-(n+1)}$ kaikilla $i, j \geq m$. Toisin sanoen

$f_i(t) \equiv f_j(t) \pmod{t^{n+1}}$ kaikilla $i, j \geq m$. Valitaan tällainen m ja merkitään a_n:llä termin t^n kerrointa sarjassa $f_m(t)$.

Merkitään

$$f(t) = \sum_{n \geq 0} a_n t^n.$$

Jos nyt $n \in \mathbb{N}$ ja $i \geq m$, jossa m on valittu kuten yllä, niin

$$f_i(t) \equiv f_m(t) \equiv f(t) \pmod{t^n},$$

joten $|f_i(t) - f(t)| \leq 2^{-n}$. Siis $f_i(t) \to f(t)$, kun $i \to \infty$.

Näin ollen jono suppenee, jos ja vain jos se on Cauchy-jono. Kohdan 6 ehto on selvästi välttämätön; osoitetaan että se on riittävä. Olkoon $(f_i(t))_{i \in \mathbb{N}}$ jono potenssisarjoja, joille $|f_i(t)| \to 0$, kun $i \to 0$. Merkitään $s_k(t) = \sum_{i=0}^{k} f_i(t)$. Jos nyt $n \in \mathbb{N}$, niin jollain m pätee $|f_i(t)| \leq 2^{-n}$, kun $i \geq m$. Tällöin kaikilla $i \geq j \geq m$ voidaan arvioida kohdan 3 nojalla

$$|s_i(t) - s_j(t)| = |f_{j+1}(t) + \cdots + f_i(t)| \leq \max\{|f_{j+1}(t)|, \ldots, |f_i(t)|\} \leq 2^{-n}.$$

Siis jono $(s_i(t))_i$ on Cauchy-jono, joten täydellisyyden nojalla se suppenee. □

Itseisarvoa, joka toteuttaa kohdan 3, kutsutaan *epäarkimeediseksi itseisarvoksi.*

3.4 Sijoitushomomorfismit

Polynomirenkaasta $R[t]$ voi määritellä sijoitushomomorfismeja mihin tahansa R-algebraan. Tässä tutkielmassa ei kuitenkaan tarvita yleistä tapausta, vaan erikoistapaus, jossa polynomeihin sijoitetaan polynomeja. Myöhemmin käytetään erityisesti homomorfismia, jossa potenssisarjaan sijoitetaan tietynlaisia potenssisarjoja.

Lause 3.4. *Olkoon $f(t) \in R[[t]]$ potenssisarja, jolle $f(0) = 0$ eli $f(t) = tf_1(t)$ jollain $f_1(t) \in R[[t]]$. Tällöin on olemassa yksikäsitteinen jatkuva homomorfismi $h_f : R[[t]] \to R[[t]]$, jolle $h_f(t) = f(t)$.*

Todistus. Jos $h_f(t) = f(t)$ ja h_f on homeomorfismi, täytyy olla $h_f(\sum_{i \leq n} a_i t^i) = \sum_{i \leq n} a_i f(t)^i$ kaikilla äärellisillä summilla. Jotta h_f olisi myös jatkuva, on määriteltävä

$$h_f\left(\sum_{i \geq 0} a_i t^i\right) = \sum_{i \geq 0} a_i f(t)^i.$$

Summa suppenee, sillä $|f(t)| < 1$, joten $|f(t)^i| \to 0$, kun $i \to \infty$. □

Tätä homomorfismiä kutsutaan *sijoitushomomorfismiksi*, jossa t:n paikalle sijoitetaan $f(t)$. Sen arvoa sarjalla $g(t) \in R[[t]]$ merkitään $g(f(t))$.

Lause 3.5. *Olkoot $f(t), g(t), k(t) \in R[[t]]$ ja $g(0) = k(0) = 0$. Tällöin $h_{g(k)}(f(t)) = h_k(h_g(f(t)))$, eli sarja $f(g(k(t)))$ on sama riippumatta siitä, missä järjestyksessä sijoitukset tehdään.*

Todistus. Tarkastellaan homomorfismia $\alpha = h_k \circ h_g : R[[t]] \to R[[t]]$. Tälle pätee

$$\alpha(t) = h_k(h_g(t)) = h_k(g(t)) = g(k(t)). \tag{2}$$

Toisaalta $h_{g(k)}$ on ainoa homomorfismi, jolle (2) pätee, joten $\alpha = h_{g(k)}$. Näin ollen $h_{g(k)}(f(t)) = \alpha(f(t)) = h_k(h_g(f(t)))$. □

Tämä tarkoittaa, että sijoitusoperaatio on liitännäinen.

3.5 Laskutoimitukset modulo t^n

Osoitetaan, että potenssisarjojen laskutoimitukset ovat hyvinmääriteltyjä modulo t^n kaikilla $n \in \mathbb{N}$. Intuitiivisesti on selvää, että suurempi t:n potenssi ei vaikuta pienempiin: esimerkiksi

$$(1 + 2t + at^2)(-1 + t + bt^2) = -1 - t + (-a + b + 2)t^2 + (a + 2b)t^3 + abt^4,$$

jossa ensimmäinen ja toinen termi eivät riipu a:sta ja b:stä.

Lause 3.6. *Olkoon R rengas ja $f(t), g(t), h(t) \in R[[t]]$. Tällöin seuraavat väitteet pätevät:*

1. *Jos $f(t) \equiv g(t) \pmod{t^n}$, niin $f(t)h(t) \equiv g(t)h(t) \pmod{t^n}$.*
2. *Jos $g(0) = h(0) = 0$ ja $g(t) \equiv h(t) \pmod{t^n}$, niin $f(g(t)) \equiv f(h(t)) \pmod{t^n}$.*
3. *Jos $h(0) = 0$ ja $f(t) \equiv g(t) \pmod{t^n}$, niin $f(h(t)) \equiv g(h(t)) \pmod{t^n}$.*

Todistus. Kohta 1 seuraa siitä, että $(t^n) = \{t^n f(t) \mid f(t) \in R[[t]]\}$ on ideaali.

Olkoon nyt $g(t) - h(t) = t^n r(t)$ ja $g(0) = h(0) = 0$. Nyt kaikilla $k \in \mathbb{N}$ pätee

$$\begin{aligned} g(t)^k - h(t)^k &= \sum_{j=0}^{k-1} g(t)^j (g(t) - h(t)) h(t)^{k-1-j} \\ &= t^n \sum_{j=0}^{k-1} g(t)^j r(t) h(t)^{k-1-j} \end{aligned}$$

joten $g(t)^k \equiv h(t)^k \pmod{t^n}$ kaikilla $k \in \mathbb{N}$. Näin ollen $f(g(t)) \equiv f(h(t)) \pmod{t^n}$.

Lopuksi: jos $h(t) = th_1(t)$ ja $f(t) - g(t) = t^n r(t)$, niin

$$f(h(t)) - g(h(t)) = t^n h_1(t)^n r(h(t)),$$

joten $f(h(t)) \equiv g(h(t)) \pmod{t^n}$. □

Lauseen 3.6 nojalla yhteenlasku, kertolasku ja sijoitus ovat hyvin määriteltyjä modulo t^n. Voidaan siis määritellä tekijärengas $R[[t]]/(t^n)$, jonka alkiot ovat polynomien jäännösluokkia modulo t^n. Tässä renkaassa on edelleen määritelty renkaan laskutoimitusten lisäksi sijoitusoperaatio, kunhan sijoitettavan vakiotermi on 0.

4 Äärelliset kunnat

4.1 Alkukunnat

Olkoon p alkuluku. Tällöin $p\mathbb{Z}$ on kokonaislukujen renkaan $\mathbb{Z}$ maksimaalinen ideaali, joten tekijärengas $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ on kunta.

Määritelmä. Olkoon F kunta. Pienintä F:n alikuntaa kutsutaan kunnan F *alkukunnaksi*. Jos F:n alkukunta on äärellinen, niin sen koko on F:n *karakteristika*, jota merkitään $\operatorname{char} F$. Muuten $\operatorname{char} F = 0$.

Osoitetaan, että kunnan karakteristika on aina 0 tai alkuluku ja että karakteristika määrää alkukunnan isomorfiaa vaille.

Lause 4.1. *Olkoon F kunta. Jos $\operatorname{char} F$ on positiivinen, niin se on alkuluku p ja F:n alkukunta on isomorfinen kunnan $\mathbb{F}_p$ kanssa. Tällöin pätee myös*

$$\operatorname{char} F = \min\{j > 0 \mid j1 = 0\}.$$

Jos $\operatorname{char} F = 0$, niin F:n alkukunta on isomorfinen rationaalilukujen kunnan $\mathbb{Q}$ kanssa.

Todistus. Olkoon $\operatorname{char} F$ positiivinen. Koska jokainen F:n alikunta sisältää alkiot $j1$ kaikilla $j \in \mathbb{Z}$, niin näitä alkioita voi olla vain äärellinen määrä. Olkoon p pienin positiivinen kokonaisluku, jolle $p1 = 0$. Jos $p = ab$, jossa a ja b ovat positiivisia kokonaislukuja, niin $(a1)(b1) = p1 = 0$, joten joko $a1 = 0$ tai $b1 = 0$, koska F on kunta. Luvun p valinnan nojalla joko $a \geq p$ tai $b \geq p$, eli toinen luvuista on p. Näin ollen p on alkuluku.

Merkitään $L = \{j1 \mid j \in \mathbb{Z}\} \subset F$. Jos $j \in \mathbb{Z}$, niin $j = qp + r$ joillain kokonaisluvuilla q ja r, jolle $0 \leq r \leq p - 1$. Tällöin $j1 = r1$, joten L on äärellinen ja sisältää p alkiota. Koska L on äärellinen kokonaisalue, niin se on kunta. Kunta L on pienin F:n sisältämä alikunta, joten $\operatorname{char} F = p$. Kun määritellään $g(x) = x1$, jossa $g : \mathbb{Z} \to L$, niin g:n ydin on $p\mathbb{Z}$, joten g indusoi isomorfismin $\mathbb{F}_p \to L$.

Olkoon nyt $\operatorname{char} F = 0$, eli F ei sisällä yhtään äärellistä kuntaa. Ylläolevan nojalla $j1 \neq 0$ kaikilla kokonaisluvulla $j \neq 0$. Määritellään kuvaus $g : \mathbb{Q} \to F$, $g(a/b) = a1/b1$ aina, kun $a, b \in \mathbb{Z}$ ja $b \neq 0$. Tällöin g on hyvin määritelty, sillä jos $a_1/b_1 = a_2/b_2$ kunnassa $\mathbb{Q}$, niin $a_1b_2 = a_2b_1$ eli $(a_11)(b_21) = (a_21)(b_11)$ ja $g(a_1/b_1) = g(a_2/b_2)$.

Koska g on homomorfismi kunnasta $\mathbb{Q}$ kuntaan F, niin g on injektio. Kuvaus g on siis isomorfismi johonkin F:n alikuntaan. Koska jokainen F:n alikunta sisältää g:n kuvan, niin F:n alkukunta on $g(\mathbb{Q})$, joka on isomorfinen $\mathbb{Q}$:n kanssa. □

4.2 Olemassaolo ja yksikäsitteisyys

Tutkitaan nyt, minkäkokoisia äärellisiä kuntia on olemassa. Olkoon F äärellinen kunta. Sen karakteristika on alkuluku p ja se sisältää alikunnan $\mathbb{F}_p$. Tällöin F on

äärellisulotteinen vektoriavaruus yli $\mathbb{F}_p$:n, olkoon sen dimensio n. Vektoriavaruudella F on kanta $\{x_1, \ldots, x_n\}$ ja jokainen F:n alkio on yksikäsitteisellä tavalla esitettävissä muodossa $c_1x_1 + \cdots + c_nx_n$, jossa kertoimet $c_i \in \mathbb{F}_p$. Tällaisia esityksiä on tasan p^n kappaletta, joten F:ssä on tasan p^n alkiota. Näin ollen jokaisen äärellisen kunnan koko on p^n jollain alkuluvulla p ja positiivisella kokonaisluvulla n.

Jos p on alkuluku ja n positiivinen kokonaisluku, niin luonnollinen kysymys kuuluu: onko olemassa kunta, jossa on p^n alkiota? Vastaus on myönteinen, ja jokaista kokoa vastaa isomorfiaa vaille yksikäsitteinen kunta.

Todistetaan ensin olemassaolo. Tämä tehdään konstruoimalla jaottomia polynomeja yli p:n alkion kunnan $\mathbb{F}_p$. Jos onnistutaan konstruoimaan jaoton polynomi $f(t) \in \mathbb{F}_p[t]$, jonka aste on n, niin saadaan kunta $\mathbb{F}_p[t]/(f(t))$, jossa on p^n alkiota.

Todistetaan hieman yleisempi väite, että aina, kun F on äärellinen kunta ja n on positiivinen kokonaisluku, on olemassa jaoton F-kertoiminen polynomi, jonka aste on n. Tämä tapahtuu yksinkertaisesti laskemalla tällaisten polynomien lukumäärä. Lasku on peräisin kirjasta [2].

Laskennassa käytetään potenssisarjoja, joita yleensä kombinatoriikan yhteydessä kutsutaan *generoiviksi funktioiksi*. Tällöin yleensä määritellään potenssisarja, jonka kertoimet ovat laskettavien asioiden lukumääriä. Tässä tapauksessa ei toimita näin, vaan johdetaan tuntemattomalle lukujonolle rekursioyhtälö ja kirjoitetaan se potenssisarjojen muotoon.

Olkoon F äärellinen kunta, jonka koko on q. Merkitään astetta i olevien jaottomien pääpolynomien lukumäärää a_i:llä. Selvästi $a_i \leq q^i$, koska kaikkia F-kertoimisia pääpolynomeja, joiden aste on i, on q^i kappaletta. Jokainen astetta n oleva pääpolynomi on yksikäsitteisellä tavalla esitettävissä jaottomien pääpolynomien tulona. Jos tällaisessa esityksessä m_i on niiden tekijöiden lukumäärä, joiden aste on i, niin $m_1 + 2m_2 \cdots + nm_n = n$. Ne m_i tekijää, jotka esiintyvät tulossa, voidaan valita $\binom{a_i+m_i-1}{m_i}$ tavalla. Tällaisia esityksiä on siis yhteensä

$$\sum_{m_1+\cdots+nm_n=n} \prod_{i=1}^{n} \binom{a_i + m_i - 1}{m_i}.$$

Astetta n olevia pääpolynomeja on q^n kappaletta, joten ylläolevan lausekkeen arvo on q^n. Tästä saadaan rekursioyhtälö, josta periaatteessa voi ratkaista jonon (a_i).

$$\sum_{m_1+\cdots+nm_n=n} \prod_{i=1}^{n} \binom{a_i + m_i - 1}{m_i} = q^n. \tag{3}$$

Tavoitteena on todistaa, että $a_i > 0$ kaikilla i, eli että kaikenasteisia jaottomia polynomeja on olemassa.

Jos yhtälö (3) kerrotaan t^n:llä, jossa t on muuttujasymboli, ja summataan yli n:n,

saadaan vastaaville potenssisarjoille seuraava yhtälö:

$$(1-qt)^{-1} = \sum_{n=0}^{\infty} t^n q^n = \sum_{n=0}^{\infty} t^n \sum_{m_1+\cdots+nm_n=n} \prod_{i=1}^{n} \binom{a_i+m_i-1}{m_i}$$
$$= \sum_{m_i \geq 0} \prod_{i=1}^{\infty} \binom{a_i+m_i-1}{m_i} t^{im_i} = \prod_{i=1}^{\infty} \left(\sum_{m=0}^{\infty} \binom{a_i+m-1}{m} t^{im} \right)$$

Koska $\binom{a_i+m-1}{m} = (-1)^m \binom{-a_i}{m}$, niin

$$\sum_{m=0}^{\infty} \binom{a_i+m-1}{m} t^{im} = \sum_{m=0}^{\infty} \binom{-a_i}{m} (-t^i)^m = (1-t^i)^{-a_i},$$

joten yhtälö (3) saadaan muotoon

$$(1-qt)^{-1} = \prod_{i=1}^{\infty} (1-t^i)^{-a_i}.$$

Molempien puolten vakiotermi on 1, joten molemmille puolille voi soveltaa logaritmia:

$$-\log(1-qt) = -\sum_{i=1}^{\infty} a_i \log(1-t^i).$$

Sijoitetaan lauseke $\sum_{n\geq 1} x^n/n = -\log(1-x)$ yhtälöön:

$$\sum_{n=1}^{\infty} \frac{q^n t^n}{n} = \sum_{i=1}^{\infty} a_i \sum_{k=1}^{\infty} \frac{t^{ik}}{k}.$$

Vertaamalla n:n asteen kertoimia tästä saadaan

$$q^n/n = \sum_{i|n} \frac{a_i}{n/i}, \quad \text{eli} \quad q^n = \sum_{i|n} i a_i.$$

Jos i on luvun n aito tekijä, niin $i \leq n/2$, joten $a_i \leq q^i \leq q^{n/2}$. Koska

$$q^n > (n-1)q^{n/2} \geq \sum_{\substack{i|n \\ i<n}} i a_i,$$

niin $a_n > 0$. Toisin sanoen kaikilla $n \geq 1$ on olemassa n:n asteen jaoton pääpolynomi $f(t) \in F[t]$.

Lemma 4.2. *Jos F on kunta, jossa on q alkiota, polynomi $t^q - t$ hajoaa ensimmäisen asteen tekijöihin kunnassa F. Kaikki F:n alkiot ovat $(t^q - t)$:n juuria.*

Todistus. Multiplikatiivisessa ryhmässä $F^* = F \setminus \{0\}$ on $q-1$ alkiota, joten jokaisen alkion kertaluku on $q-1$:n tekijä. Näin ollen jokaiselle $\alpha \in F^*$ pätee $\alpha^{q-1} = 1$, joten $\alpha^q - \alpha = 0$. Tämä pätee myös, jos $\alpha = 0$, joten polynomilla $t^q - t$ on q juurta kunnassa F. Toisin sanoen polynomin $t^q - t$ voi esittää tulona $\prod_{a \in F} (t - \alpha)$. □

Lemma 4.3. *Jos F on kunta, jossa on q alkiota, niin jokainen asteen n jaoton F-kertoiminen polynomi jakaa polynomin $t^{q^n} - t$.*

Todistus. Jos $f(t)$ on jaoton n:n asteen polynomi, niin kunnassa $F[t]/(f(t))$ on q^n alkiota, joten Lemman 4.2 nojalla jokainen alkio on polynomin $t^{q^n} - t$ juuri. Erityisesti alkio t toteuttaa $t^{q^n} - t = 0$ kunnassa $F[t]/(f(t))$, joten $f(t)$ jakaa $(t^{q^n} - t)$:n. □

Lause 4.4. *Olkoon p alkuluku ja n positiivinen kokonaisluku. Tällöin on olemassa kunta F, jossa on $q = p^n$ alkiota, ja kaikki tämänkokoiset kunnat ovat isomorfisia keskenään.*

Todistus. Valitaan asteen n jaoton polynomi $f(t) \in \mathbb{F}_p[t]$. Tällöin tekijärengas $\mathbb{F}_p[t]/(f(t))$ on kunta ja siinä on q alkiota.

Olkoon F kunta, jonka koko on q. Koska $f(t)$ Lemman 4.3 nojalla jakaa polynomin $t^q - t$, joka hajoaa ensimmäisen asteen tekijöihin kunnassa F, niin myös $f(t)$ hajoaa ensimmäisen asteen tekijöihin kunnassa F. Siis polynomilla $f(t)$ on juuria kunnassa F; olkoon α yksi niistä. Koska $f(t)$ on alkion α minimaalipolynomi yli kunnan $\mathbb{F}_p$, niin laajennuksen $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ aste on $\deg(f(t)) = n$. Kunnan $\mathbb{F}_p(\alpha)$ koko on siis p^n. Näin ollen $F = \mathbb{F}_p(\alpha)$, joka on isomorfinen kunnan $\mathbb{F}_p[t]/(f(t))$ kanssa. □

5 Galois-teorian perusteet

Tässä luvussa esitellään tarvittavat tiedot kuntalaajennusten teoriasta. Jos K on kunta ja F sen alikunta, niin K on F:n *laajennus*. Tällöin puhutaan yleensä laajennuksesta K/F.

5.1 Kuntalaajennusten Galois-ryhmät

Määritelmä. Olkoon K/F kuntalaajennus.

- Jos $x \in K$, niin x on *algebrallinen yli kunnan F*, jos on olemassa F-kertoiminen polynomi $f(t) \neq 0$, jolle $f(x) = 0$. Jos jokainen $x \in K$ on algebrallinen yli F:n, niin K/F on *algebrallinen laajennus*.

- Jos yllämainittu $f(t) \in F[t]$ on pääpolynomi ja pienintä mahdollista astetta, niin se on alkion x *minimaalipolynomi yli kunnan F*. On helppo osoittaa, että minimaalipolynomi on jaoton ja että se on yksikäsitteinen.

- Jos K/F on laajennus ja $S \subset F[t]$ joukko polynomeja, niin K on S:n *juurikunta*, jos jokaisella polynomilla $f(t) \in S$ on $\deg(f(t))$ juurta K:ssa ja K on kaikkien S:n polynomien juurten virittämä laajennus.

- Jos $x \in K$, niin x on *separoituva yli F:n*, jos x on algebrallinen yli F:n ja alkion x minimaalipolynomilla $f(t)$ ei ole derivaattansa $f'(t)$ kanssa yhteisiä

tekijöitä. Jos jokainen $x \in K$ on separoituva yli F:n, niin K/F on *separoituva laajennus*. Voidaan osoittaa, että separoituvassa laajennuksessa alkioiden minimaalipolynomeilla ei ole moninkertaisia juuria.

- Laajennus K/F on *normaali laajennus*, jos se on algebrallinen ja jokaisen alkion $x \in K$ minimaalipolynomi $f(t) \in F[t]$ hajoaa ensimmäisen asteen tekijöihin $K[t]$:ssä.
- Laajennus K/F on *Galois-laajennus*, jos se on algebrallinen, normaali ja separoituva.
- Kunnan K automorfismia φ sanotaan *F-automorfismiksi*, jos $\varphi|_F = id$. On helppo nähdä, että K:n F-automorfismit muodostavat ryhmän, kun laskutoimituksena on kuvausten yhdistäminen. Jos K/F on Galois-laajennus, niin tätä ryhmää kutsutaan *Galois-ryhmäksi* ja merkitään $\mathrm{Gal}(K/F)$.

Osoitetaan, että juurikunnat ovat tietyssä mielessä isomorfiaa vaille yksikäsitteisiä. Tätä lemmaa käytetään myös seuraavan lauseen todistuksessa.

Kun $\tau : K \to L$ on kuntien välinen homomorfismi ja $f(t) \in K[t]$, niin merkintä $\tau(f(t))$ tarkoittaa L-kertoimista polynomia, jossa jokainen $f(t)$:n kerroin on korvattu kuvallaan τ:ssa. Toisin sanoen

$$\tau\left(\sum_{i=0}^{n} a_i t^i\right) = \sum_{i=0}^{n} \tau(a_i) t^i.$$

Näin laajennettuna τ on renkaiden $K[t]$ ja $L[t]$ välinen homomorfismi.

Lemma 5.1. *Olkoon $\tau : F \to L$ kuntien F ja L välinen isomorfismi ja $f(t) \in F[t]$ polynomi. Jos $K \supset F$ on polynomin $f(t)$ juurikunta ja $M \supset L$ polynomin $\tau(f(t))$ juurikunta, niin on olemassa isomorfismi $\sigma : K \to M$, jolle $\sigma|_F = \tau$.*

Todistus. Käytetään induktiota yli $\deg(f(t))$:n. Jos $\deg(f(t)) = 1$, niin $K = F$, $M = L$ ja voidaan asettaa $\sigma = \tau$.

Olkoon nyt $\deg(f(t)) > 1$. Jos kaikki $f(t)$:n jaottomat tekijät $F[t]$:ssä ovat astetta 1, niin jälleen $K = F$ ja $M = L$. Oletetaan, että jokin $f(t)$:n jaoton tekijä $g(t) \in F[t]$ toteuttaa $\deg(g(t)) > 1$. Nyt $g(t)$:llä on juuri $\alpha \in K$, koska K on $f(t)$:n juurikunta. Vastaavasti polynomilla $\tau(g(t))$ on juuri $\beta \in M$.

Isomorfismi τ voidaan laajentaa isomorfismiksi τ' kuntien $F(\alpha)$ ja $L(\beta)$ välille siten, että $\tau'(h(\alpha)) = (\tau(h))(\beta)$ kaikilla $h \in F[t]$. On helppo nähdä, että näin määritelty kuvaus on todellakin isomorfismi ja laajentaa kuvausta τ. Pätee myös $f(t) = (t - \alpha)f_1(t)$ jollain $f_1(t) \in F(\alpha)[t]$ ja $\tau(f(t)) = \tau'(f(t)) = (t - \beta)\tau'(f_1(t))$.

Nyt kunta K on polynomin $f_1(t)$ juurikunta yli $F(\alpha)$:n ja M on polynomin $\tau'(f_1(t))$ juurikunta yli $L(\beta)$:n. Koska $\deg(f_1(t)) < \deg(f(t))$, niin induktio-oletuksen nojalla isomorfismi $\tau' : F(\alpha) \to L(\beta)$ voidaan siis laajentaa isomorfismiksi $\sigma : K \to M$. Tällöin σ laajentaa myös isomorfismia τ. □

Huomaa, että Lemma 5.1 antaa uuden todistuksen sille, että q:n alkion äärellinen kunta on isomorfiaa vaille yksikäsitteinen. Nimittäin tällainen kunta on aina polynomin $t^q - t$ juurikunta yli alkukuntansa.

Annetaan nyt yksinkertainen kriteeri sille, milloin kuntalaajennus on Galois-laajennus.

Lause 5.2. *Olkoot K ja $F \subset K$ kuntia, joille K/F on algebrallinen laajennus. Nyt K/F on Galois-laajennus, jos ja vain jos F on jonkin K:n automorfismiryhmän kiintokunta.*

Todistus. Merkitään kunnan K kaikkien automorfismien ryhmää $\mathrm{Aut}(K)$:llä. Olkoon G jokin $\mathrm{Aut}(K)$:n aliryhmä ja F ryhmän G kiintokunta eli

$$F = \{x \in K \mid \varphi(x) = x \ \forall \varphi \in G\}.$$

Osoitetaan, että tällöin laajennus K/F on separoituva ja normaali.

Olkoon $x \in K$ ja $f(t)$ alkion x minimaalipolynomi yli kunnan F. Osoitetaan, että $f(t)$:llä on $\deg(f(t))$ eri juurta K:ssa, jolloin K/F on normaali ja separoituva. Merkitään $\{x_1, \ldots, x_r\}$:llä alkion x rataa G:n toiminnassa ja

$$g(t) = (t - x_1) \ldots (t - x_r).$$

Koska kaikki $\varphi \in G$ ovat F-automorfismeja ja $f(t)$ on F-kertoiminen polynomi, niin kaikilla $\varphi \in G$ pätee

$$f(\varphi(x)) = \varphi(f(x)) = \varphi(0) = 0.$$

Toisin sanoen kaikki alkiot x_i ovat $f(t)$:n juuria. Tästä seuraa, että $g(t)$ jakaa $f(t)$:n.

Toisaalta kaikilla $\varphi \in G$ pätee

$$\varphi(g(t)) = (t - \varphi(x_1)) \ldots (t - \varphi(x_r)) = (t - x_1) \ldots (t - x_r) = g(t),$$

koska φ permutoi alkion x rataa. Näin ollen jokainen $\varphi \in G$ kiinnittää polynomin $g(t)$ kertoimet, joten kertoimet kuuluvat F:n eli $g(t) \in F[t]$. Koska x on $g(t)$:n juuri ja $f(t)$ alkion x minimaalipolynomi, niin myös $f(t)$ jakaa $g(t)$:n. Koska $f(t)$ ja $g(t)$ ovat pääpolynomeja, niin $f(t) = g(t)$, eli $f(t)$:n aste on r ja $f(t)$:llä on r eri juurta K:ssa. Laajennus K/F on siis normaali ja separoituva.

Olkoon K/F nyt Galois-laajennus. Merkitään $G = \mathrm{Gal}(K/F)$, eli niiden K:n automorfismien φ ryhmä, joille $\varphi|_F = id$. Nyt selvästi F sisältyy G:n kiintokuntaan, mutta ei ole itsestään selvää, ettei kiintokunta ole suurempi.

Olkoon $x \in K \setminus F$. Tavoitteena on todistaa, että $\varphi(x) \neq x$ jollain $\varphi \in G$, eli että x ei kuulu G:n kiintokuntaan. Konstruoidaan φ transfiniittisella induktiolla. Merkitään $\kappa = |K|$ ja hyvinjärjestetään kunnan K alkiot ordinaaleilla: $K = \{\alpha_i \mid i < \kappa\}$.

Olkoon $f(t)$ alkion x minimaalipolynomi yli F:n. Tällöin $f(t)$:llä on $\deg(f(t)) > 1$ eri juurta K:ssa, koska K/F on separoituva ja normaali laajennus. Olkoon y toinen $f(t)$:n juuri. Tällöin on olemassa F-isomorfismi $\varphi_0 : F(x) \to F(y)$, jolle $\varphi_0(x) = y$. Kun $i \leq \kappa$, määritellään φ_0:aa laajentava isomorfismi $\varphi_i : F_i \to L_i$, jossa F_i sisältää kaikki alkiot α_j, jossa $j < i$. Tehdään tämä induktiolla seuraavasti:

- Jos $\delta \leq \kappa$ on rajaordinaali, valitaan

$$F_\delta = \bigcup_{i<\delta} F_i,\ L_\delta = \bigcup_{i<\delta} L_i,\ \varphi_\delta = \bigcup_{i<\delta} \varphi_i.$$

- Jos $i = j + 1$ on seuraajaordinaali, otetaan alkion α_j minimaalipolynomi $f(t) \in F[t]$. Valitaan kunnaksi F_i polynomin $f(t)$ juurikunta, kun ajatellaan $f(t)$:n olevan F_j-kertoiminen polynomi. Nyt siis F_i laajentaa F_j:tä. Samoin laajennetaan L_j kunnaksi L_i, joka on $f(t)$:n juurikunta yli kunnan L_j. Lemman 5.1 nojalla isomorfismi $\varphi_j : F_j \to L_j$ voidaan laajentaa isomorfismiksi $\varphi_i : F_i \to L_i$. Huomataan, että $\alpha_j \in F_i$ sekä $\alpha_j \in L_i$.

Määritellään $\varphi = \varphi_\kappa$ ja huomataan, että $F_\kappa = L_\kappa = K$. Näin ollen φ on kunnan K automorfismi ja $\varphi(x) = y \neq x$. □

Otetaan vielä käyttöön tulos äärellisistä Galois-laajennuksista, jota käytetään myöhemmin useaan kertaan. Lause on hieman eri lailla muotoiltuna todistettu esimerkiksi kirjassa [6].

Lause 5.3. *Laajennus K/F on äärellinen Galois-laajennus, jos ja vain jos F on jonkin äärellisen ryhmän $G \leq \mathrm{Aut}(K)$ kiintokunta. Tällöin* $\mathrm{Gal}(K/F) = G$ *ja laajennuksen aste* $[K : F] = |G|$.

5.2 Krullin topologia

Annetaan seuraavaksi Galois-laajennukseen liittyvälle Galois-ryhmälle topologia. Olkoon K/F Galois-laajennus ja $G = \mathrm{Gal}(K/F)$ sen Galois-ryhmä. Tarkastellaan G:n aliryhmiä, jotka ovat muotoa $\mathrm{Gal}(K/L)$, jossa L on kuntien K ja F välissä oleva kunta ja L/F on äärellinen Galois-laajennus.

Tällaiset laajennukset ovat muotoa $L = F(\alpha_1, \ldots, \alpha_r)$, jossa virittäjäalkiot $\alpha_1, \ldots, \alpha_r$ ovat jonkin polynomin $f(t) \in F[t]$ juuret. Toisin sanoen L on aina jonkin F-kertoimisen polynomin juurikunta. Jos L_1 ja L_2 ovat kaksi tällaista kuntaa, jossa L_i on polynomin $f_i(t)$ juurikunta, niin polynomin $f_1(t)f_2(t)$ juurikunta L sisältää molemmat kunnat L_i. Ryhmien kannalta tämä tarkoittaa, että

$$\mathrm{Gal}(K/L) \subset \mathrm{Gal}(K/L_1) \cap \mathrm{Gal}(K/L_2).$$

Merkitään $\mathcal{S}$:llä kaikkien ryhmien $\mathrm{Gal}(K/L) \leq G$ joukkoa, jossa L/F on jonkin $F[t]$:n polynomin juurikunta. Ylläolevan perusteella kaikilla $H_1, H_2 \in \mathcal{S}$ on olemassa $H \in \mathcal{S}$, jolle $H \leq H_1 \cap H_2$. Tämän perusteella on olemassa G:n topologia, jonka kannan muodostavat $\mathcal{S}$:n ryhmien kaikki sivuluokat. Tätä topologiaa kutsutaan *Krullin topologiaksi*.

Luvussa 8 todistetaan, että G varustettuna Krullin topologialla on topologinen ryhmä ja tutkitaan sen muita ominaisuuksia.

5.3 Esimerkki: Symmetriset rationaalilausekkeet

Tässä esitellään yksi esimerkki *käänteisestä Galois-ongelmasta*, eli etsitään annetulle ryhmälle (tässä tapauksessa S_n:lle) kuntalaajennus, jonka Galois-ryhmä on isomorfinen annetun ryhmän kanssa. Ryhmälle S_n yksi ratkaisu on laajennus, jossa kaikkien rationaalilausekkeiden kunta laajentaa symmetristen rationaalilausekkeiden kuntaa.

Muuttujien $t_1, \ldots, t_n$ rationaalilauseke $h(t_1, \ldots, t_n)$ on *symmetrinen*, jos kaikki muuttujat ovat samassa asemassa, eli mitkä tahansa kaksi muuttujaa voidaan vaihtaa keskenään ilman, että lauseke muuttuu. Täsmällisemmin tämän voi ilmaista niin, että ryhmän S_n toiminta

$$\sigma\left(h(t_1, \ldots, t_n)\right) = h(t_{\sigma(1)}, \ldots, t_{\sigma(n)})$$

rationaalilausekkeiden joukossa kiinnittää h:n kaikilla $\sigma \in S_n$.

Jos F on kunta ja ryhmä S_n toimii kunnassa $F(t_1, \ldots, t_n)$ yllämainitulla tavalla, niin sen kiintokuntaa K kutsutaan siis symmetristen rationaalilausekkeiden kunnaksi. Tällöin K on äärellisen automorfismiryhmän S_n kiintokunta, joten Lauseen 5.3 nojalla $F(t_1, \ldots, t_n)$ on kunnan K Galois-laajennus, sen aste on $[F(t_1, \ldots, t_n) : K] = |S_n| = n!$ ja Galois-ryhmä S_n.

Polynomin $f(X) = (X - t_1) \cdots (X - t_n)$ kertoimet kuuluvat selvästi ryhmän S_n kiintokuntaan, koska kaikilla $\sigma \in S_n$ pätee $\sigma(f(X)) = f(X)$. Siis $f \in K[X]$. Merkitään kertoimia seuraavasti:

$$f(X) = \sum_{i=0}^{n} (-1)^i s_i X^{n-i}.$$

Nyt siis pätee muun muassa $s_1 = t_1 + \cdots + t_n$, $s_2 = t_1 t_2 + \cdots + t_{n-1} t_n$ ja $s_n = t_1 \cdots t_n$. Polynomeja s_i kutsutaan *symmetrisiksi alkeispolynomeiksi*.

Käy ilmi, että polynomit s_i virittävät kaikki symmetriset rationaalilausekkeet, eli $K = F(s_1, \ldots, s_n)$. Olkoon $L = F(s_1, \ldots, s_n)$. Nyt polynomin $f(X)$ kertoimet kuuluvat myös kuntaan L, joten $F(t_1, \ldots, t_n)$ on $f(X)$:n juurikunta myös yli kunnan L. Siis

$$[F(t_1, \ldots, t_n) : L] \leq \deg(f(X))! = n! = [F(t_1, \ldots, t_n) : K].$$

Koska $L \leq K$, niin $L = K$.

Lause 5.4. *Jos F on mielivaltainen kunta, ja $t_1, \ldots, t_n$ ovat muuttujasymboleita ja $s_1, \ldots, s_n$ symmetriset alkeispolynomit, niin laajennuksen $F(t_1, \ldots, t_n)/F(s_1, \ldots, s_n)$ Galois-ryhmä on isomorfinen ryhmän S_n kanssa.*

5.4 Esimerkki: Äärellisen kunnan äärellinen laajennus

Olkoon F äärellinen kunta, jossa on q alkiota ja K on sen laajennus, jossa on q^n alkiota. Nyt kuvaus $f(x) = x^q$ on K:n F-automorfismi. Sitä kutsutaan *Frobenius-automorfismiksi* saksalaisen Ferdinand Georg Frobeniuksen mukaan. Osoitetaan, että kaikki K:n F-automorfismit ovat muotoa f^k, jossa $0 \leq k \leq n - 1$.

Selvästi pätee $f^n = id$, koska f^n kuvaa alkion $x \in K$ alkioksi $x^{q^n} = x$, koska kunnassa K on q^n alkiota. Jos $0 < k < n$, niin $f^k(x) = x^{q^k}$, joten f^k ei ole id, koska polynomilla $x^{q^k} - x$ on korkeintaan q^k juurta.

Automorfismin f kiintokunta sisältää täsmälleen polynomin $t^q - t$ juuret. Niitä on korkeintaan q kappaletta ja toisaalta kaikki F:n alkiot ovat $(t^q - t)$:n juuria. Kiintokunta on siis F.

Näin ollen myös f:n virittämän syklisen ryhmän kiintokunta on F. Lauseen 5.3 nojalla laajennus K/F on Galois-laajennus, jonka Galois-ryhmä on $\{id, f, \ldots, f^{n-1}\}$. Ryhmä $\mathrm{Gal}(K/F)$ on siis n:n alkion syklinen ryhmä.

6 Ryhmien käänteiset rajat

Tässä luvussa esitellään käänteisen järjestelmän ja käänteisen rajan käsitteet. Niiden avulla voidaan muodostaa ryhmien perheestä uusi ryhmä, jota annettu perhe tietyssä mielessä "lähestyy". Näille annetaan myös sovellus, jossa kuntalaajennusten yhdisteen Galois-ryhmä on yksittäisten Galois-ryhmien käänteinen raja.

Määritelmä. Joukko I on *suunnattu joukko*, jos sillä on järjestysrelaatio $\leq$ ja kaikilla $i, j \in I$ on olemassa $k \in I$, jolle $i \leq k$ ja $j \leq k$.

Ryhmien *käänteinen järjestelmä* on kolmikko $((G_i)_{i\in I}, (\varphi_{ij})_{i\leq j}, I)$, jossa I on suunnattu joukko, G_i on ryhmä kaikilla $i \in I$ ja $\varphi_{ij} : G_j \to G_i$ on homomorfismi aina, kun $i \leq j$ sekä kaikilla $i \leq j \leq k$ pätee $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$.

Ongelmana on löytää tietynlainen ryhmä G ja homomorfismit $\psi_i : G \to G_i$, jotka muodostaisivat annetun käänteisen järjestelmän rajan. Ominaisuus, jonka haluamme rajan G toteuttavan, on se, että $\varphi_{ij} \circ \psi_j = \psi_i$ eli seuraava kaavio kommutoi:

$$\begin{array}{ccc} G & \xrightarrow{\psi_j} & G_j \\ & \searrow^{\psi_i} & \downarrow{\scriptstyle \varphi_{ij}} \\ & & G_i \end{array} \tag{4}$$

Tällöin sanotaan, että homomorfismit ψ_i ja φ_{ij} ovat *yhteensopivia*. Lisäksi haluamme, että G on "pienin" ryhmä, joka toteuttaa kaavion (4) eli jos H on ryhmä ja $\chi_i : H \to G_i$ ovat yhteensopivia homomorfismeja, niin on olemassa yksikäsitteinen homomorfismi $f : H \to G$, jolle $\chi_i = \psi_i \circ f$ kaikilla $i \in I$. Tämän voi ilmaista seuraavalla kaaviolla:

$$\begin{array}{ccc} H & \xrightarrow{f} & G \\ & \searrow^{\chi_i} & \downarrow{\scriptstyle \psi_i} \\ & & G_i \end{array}$$

Määritelmä. Olkoon $((G_i)_{i\in I}, (\varphi_{ij})_{i\leq j}, I)$ ryhmien käänteinen järjestelmä. Sen *käänteinen raja* on ryhmä G, joka on suoran tulon $\prod_{i\in I} G_i$ aliryhmä ja määritellään seu-

raavasti:

$$G = \{(g_i)_{i\in I} \mid \varphi_{ij}(g_j) = g_i \text{ kaikilla } i \leq j\}.$$

Jos $g = (g_i)_{i\in I}$ ja $h = (h_i)_{i\in I}$ kuuluvat rajaan G, niin niiden tulo ryhmässä $\prod_{i\in I} G_i$ on $(g_i h_i)_{i\in I}$, joka toteuttaa $\varphi_{ij}(g_j h_j) = \varphi_{ij}(g_j)\varphi_{ij}(h_j) = g_i h_i$, joten tulokin kuuluu G:hen. Vastaavasti $g^{-1} \in G$, joten G on ryhmä.

Osoitetaan nyt, että näin määritellyllä rajalla on halutut ominaisuudet.

Lause 6.1. *Olkoon $((G_i)_{i\in I}, (\varphi_{ij})_{i\leq j}, I)$ ryhmien G_i käänteinen järjestelmä ja G sen käänteinen raja. Merkitään $\psi_i((g_j)_{j\in I}) = g_i$, jossa $\psi_i : G \to G_i$ on siis projektio ryhmälle G_i. Tällöin $\varphi_{ij} \circ \psi_j = \psi_i$ kaikilla $i \leq j$.*

Lisäksi, jos H on ryhmä ja homomorfismit $\chi_i : H \to G_i$ toteuttavat $\varphi_{ij} \circ \chi_j = \chi_i$, niin on olemassa yksikäsitteinen homomorfismi $f : H \to G$, jolle pätee $\chi_i = \psi_i \circ f$ kaikilla $i \in I$.

Todistus. Jos $g = (g_i)_{i\in I} \in G$, niin $\varphi_{ij}(g_j) = g_i$ kaikilla $i \leq j$, eli $\varphi_{ij}(\psi_j(g)) = \psi_i(g)$ kaikilla $g \in G$ ja $i \leq j$. Siis $\varphi_{ij} \circ \psi_j = \psi_i$.

Olkoot nyt H ja χ_i kuten yllä. Jos $h \in H$, niin merkitään $f(h) = (\chi_i(h))_{i\in I}$. Tällöin oletuksen perusteella pätee $\varphi_{ij}(f(h)_j) = f(h)_i$ kaikilla $i \leq j$, joten $f(h) \in G$. Määritelmän perusteella pätee myös $\psi_i \circ f = \chi_i$. Tämä on ainoa mahdollinen tapa määritellä $f(h)$, sillä vaatimus on, että $\chi_i(h) = \psi_i(f(h)) = f(h)_i$, joten f on yksikäsitteinen. □

6.1 Galois-ryhmien rajat

Näytetään nyt, miten käänteiset rajat liittyvät Galois-ryhmiin. Osoittautuu, että ryhmien raja vastaa Galois-laajennusten yhdistettä.

Olkoon F kunta, K sen laajennus ja K_i jokin välissä oleva F:n Galois-laajennus aina, kun $i \in I$. Oletetaan, että kaikille kahdelle välissä olevalle kunnalle löytyy kolmas, joka sisältää molemmat. Yhtäpitävästi voidaan olettaa, että I on suunnattu joukko ja $K_i \leq K_j$ aina kun $i \leq j$. Tällöin kaikkien kuntien K_i yhdiste $L = \bigcup_{i\in I} K_i$ on myös kunta, ja se on F:n Galois-laajennus.

Merkitään G_i:llä laajennuksen K_i/F Galois-ryhmää, kun $i \in I$. Tutkitaan laajennuksen L/F Galois-ryhmää. Jos $\varphi \in \mathrm{Gal}(L/F)$, niin $\varphi|_{K_i} \in \mathrm{Gal}(K_i/F) = G_i$ kaikilla $i \in I$, sillä K_i on F:n normaali laajennus. Merkitään $s_i(\varphi) = \varphi|_{K_i}$, jolloin $s_i : \mathrm{Gal}(L/F) \to G_i$. Myös kaikilla $i \leq j$ voidaan määritellä homomorfismi $r_{ij} : G_j \to G_i$, jossa automorfismi $\varphi \in G_j$ kuvautuu automorfismiksi $\varphi|_{K_i} \in G_i$.

Nyt $r_{ij} \circ s_j = s_i$ kaikilla $i \leq j$, sillä $(\varphi|_{K_j})|_{K_i} = \varphi|_{K_i}$ aina, kun $K_i \subset K_j$. Samoin $r_{ij} \circ r_{jk} = r_{ik}$, kun $i \leq j \leq k$. Ryhmät G_i ja homomorfismit r_{ij} siis muodostavat käänteisen järjestelmän ja kuvaukset $s_i : \mathrm{Gal}(L/F) \to G_i$ ovat keskenään yhteensopivia.

Merkitään G:llä yllämainitun käänteisen järjestelmän käänteistä rajaa. Nyt on yksikäsitteinen homomorfismi $f : \mathrm{Gal}(L/F) \to G$, jolle $f(\varphi)_i = \varphi|_{K_i}$ kaikilla $i \in I$.

Osoitetaan, että f on isomorfismi. Jos $\varphi \in \mathrm{Ker}(f)$, niin $\varphi|_{K_i} = id$ kaikilla $i \in I$, joten $\varphi(x) = x$ aina, kun $x \in K_i$ jollain $i \in I$, eli aina, kun $x \in L$. Siis $\varphi = id$, eli f on injektio.

Osoitetaan, että f on myös surjektio. Olkoon $(\varphi_i)_{i\in I} \in G$. Nyt $\varphi_j|_{K_i} = \varphi_i$ kaikilla $i \leq j$, eli jos $x \in K_i \subset K_j$, niin $\varphi_i(x) = \varphi_j(x)$. Toisaalta, jos $x \in K_i$ ja $x \in K_j$ millä tahansa $i, j \in I$, niin on olemassa sellainen $k \in I$, että $i, j \leq k$ ja tällöin $\varphi_i(x) = \varphi_k(x) = \varphi_j(x)$. Siis $\varphi_i(x)$ on sama kaikilla $i \in I$, joilla se on määritelty. Kun $x \in L$, merkitään $\varphi(x)$:llä alkiota $\varphi_i(x) \in L$, jossa $i \in I$ on sellainen, jolle $x \in K_i$. Tällöin $\varphi \in \mathrm{Gal}(L/F)$ toteuttaa $\varphi|_{K_i} = \varphi_i$ eli $s_i(\varphi) = \varphi_i$ kaikilla $i \in I$. Toisin sanoen $f(\varphi) = (\varphi_i)_{i\in I}$, joka valittiin mielivaltaisesti ryhmästä G. Kuvaus f on siis surjektio, eli f on isomorfismi.

Lause 6.2. *Olkoon I suunnattu joukko ja K kunnan F laajennus. Oletetaan, että kaikilla $i \in I$ on annettu kuntien K ja F välissä oleva kunta K_i, joka on F:n Galois-laajennus. Jos $K_i \subset K_j$ kaikilla $i, j \in I$, joille $i \leq j$, niin yhdiste $L = \bigcup_{i\in I} K_i$ on F:n Galois-laajennus ja sen Galois-ryhmä on*

$$\mathrm{Gal}(L/F) = \varprojlim \mathrm{Gal}(K_i/F).$$

7 Topologiset ja proäärelliset ryhmät

Tässä luvussa yhdistetään topologia ja ryhmäteoria, erityisesti ryhmien käänteiset rajat. Äärellisten ryhmien käänteisillä rajoilla on mielenkiintoisia topologisia ominaisuuksia, joihin tutustutaan proäärellisten ryhmien yhteydessä.

Topologisessa ryhmässä on sekä ryhmän laskutoimitus että topologia, ja näiden on oltava keskenään yhteensopivia seuraavalla tavalla.

Määritelmä. Olkoon G ryhmä ja τ joukon G topologia. Tällöin (G, τ) on *topologinen ryhmä*, jos kertolasku $G \times G \to G$ ja käänteisalkion ottaminen $(\ )^{-1} : G \to G$ ovat jatkuvia kuvauksia.

Määritelmästä seuraa välittömästi, että kaikilla $a \in G$ kuvaus $x \mapsto ax$ on homeomorfismi $G \to G$. Se on nimittäin jatkuva ja myös sen käänteiskuvaus $x \mapsto a^{-1}x$ on jatkuva. Myös käänteisalkion ottaminen on homeomorfismi, sillä se on oma käänteiskuvauksensa.

Määritelmä. Jos G on topologinen ryhmä, niin G on *proäärellinen*, jos se on kompakti, täysin epäyhtenäinen ja toteuttaa Hausdorffin ehdon.

Lause 7.1. *Topologisessa ryhmässä G alkion 1 yhtenäinen komponentti on G:n aliryhmä ja sen sivuluokat ovat yhtenäisiä komponentteja.*

Todistus. Seuraavaa faktaa käytetään todistuksessa: jos $f : X \to Y$ on homeomorfismi, ja $a \in X$, niin f kuvaa a:n yhtenäisen komponentin $f(a)$:n yhtenäiseksi komponentiksi Y:ssä.

Olkoon A alkion 1 yhtenäinen komponentti ja $a \in A$. Kuvaus $x \mapsto ax$ on homeomorfismi, ja $1 \mapsto a \in A$, joten A:n kuva on A. Toisin sanoen $aA = A$ kaikilla $a \in A$, joten A on G:n aliryhmä.

Jos $b \in G$, niin kuvaus $x \mapsto bx$ on homeomorfismi, jolle $1 \mapsto b$, joten bA on alkion b yhtenäinen komponentti. □

Lause 7.2. *Jos G on kompakti topologinen ryhmä, niin jokaisen G:n avoimen aliryhmän indeksi on äärellinen.*

Todistus. Olkoon H kompaktin topologisen ryhmän G avoin aliryhmä. Tällöin sen sivuluokat muodostavat G:n erillisen avoimen peitteen. Koska peite on erillinen, niin sillä ei ole aitoa alipeitettä. Kompaktisuuden perusteella H:lla on siis vain äärellinen määrä sivuluokkia. □

Koska avoimen aliryhmän komplementti on sen muiden sivuluokkien yhdiste, niin komplementti on avoin. Jokainen avoin aliryhmä on siis suljettu. Vastaavasti jokainen suljettu aliryhmä, jonka indeksi on äärellinen, on avoin.

Lause 7.3. *Jos G on topologinen ryhmä ja $\mathcal{B}$ on alkion 1 ympäristökanta, niin kokoelma $\bigcup_{a \in G} a\mathcal{B}$ on topologisen avaruuden G kanta.*

Todistus. Olkoon $U \subset G$ avoin ja $x \in U$. Nyt joukko $x^{-1}U$ on 1:n avoin ympäristö, joten $\mathcal{B}$:ssä on joukko V_x, jolle $1 \in V_x \subset x^{-1}U$. Tällöin xV_x on alkion x avoin ympäristö ja xV_x sisältyy joukkoon U. Joukko U on siis yhdiste kaikista $xV_x \in x\mathcal{B}$, jossa $x \in U$. □

Seuraava tulos on topologisten ryhmien versio Lauseesta 2.1.

Lause 7.4. *Olkoot G ja H topologisia ryhmiä ja $g : G \to H$ homomorfismi.*

1. *Jos $\mathcal{S}_1$ on alkion 1 ympäristöesikanta H:ssa ja $g^{-1}(U)$ on avoin kaikilla $U \in \mathcal{S}_1$, niin g on jatkuva.*
2. *Jos $\mathcal{B}_1$ on alkion 1 ympäristökanta G:ssä ja $g(U)$ on avoin kaikilla $U \in \mathcal{B}_1$, niin g on avoin.*

Todistus. Olkoon $\mathcal{S}_1$ alkion 1 ympäristöesikanta H:ssa. Jos $x \in X$ ja U on H:n avoin osajoukko, jolle $g(x) \in U$, niin $g(x)^{-1}U$ on avoin ja $1 \in g(x)^{-1}U$. Tällöin on olemassa joukot $V_1, \ldots, V_r \in \mathcal{S}_1$, joille $1 \in \bigcap_i V_i \subset g(x)^{-1}U$. Merkitään $V = V_1 \cap \cdots \cap V_r$, jolloin $g(x)V \subset U$ eli $xg^{-1}(V) \subset g^{-1}(U)$. Toisaalta joukko $xg^{-1}(V)$ on avoin ja $x \in xg^{-1}(V)$, joten $g^{-1}(U)$ on alkion x ympäristö. Kuvaus g on siis jatkuva.

Olkoon nyt $\mathcal{B}_1$ alkion 1 ympäristökanta G:ssä. Nyt kokoelma $\bigcup_{x \in G} x\mathcal{B}_1$ on Lauseen 7.3 nojalla G:n ympäristökanta, ja $g(xU) = g(x)g(U)$, joka on avoin aina, kun $U \in \mathcal{B}_1$ ja $x \in G$. Lauseen 2.1 perusteella g on avoin. □

Lause 7.5. *Jos X on kompakti Hausdorff-avaruus, niin alkion $x \in X$ yhtenäinen komponentti on kaikkien niiden X:n osajoukkojen leikkaus, jotka sisältävät alkion x ja ovat sekä avoimia että suljettuja.*

Todistus. Olkoon $\mathcal{D}$ kaikkien x:n sisältävien avointen suljettujen joukkojen kokoelma ja olkoon $A = \bigcap \mathcal{D}$. Tällöin jokainen $C \in \mathcal{D}$ sisältää x:n yhtenäisen komponentin, joten myös A sisältää sen. Riittää siis näyttää, että A on itse yhtenäinen.

Olkoon $A = U \cup V$, jossa U ja V ovat erillisiä ja suljettuja A:ssa. Oletetaan, että $x \in U$. Koska A on suljettu X:ssä, niin U ja V ovat suljettuja X:ssä ja ovat siis kompakteja. Nyt Hausdorffin ehdosta seuraa, että on olemassa sellaiset avoimet ja erilliset $U', V' \subset X$, että $U' \cap A = U$ ja $V' \cap A = V$.

Koska $A = \bigcap \mathcal{D} \subset U' \cup V'$ ja X on kompakti, niin on olemassa äärellinen $\mathcal{D}_0 \subset \mathcal{D}$, jolle $\bigcap \mathcal{D}_0 \subset U' \cup V'$. Merkitään $B = \bigcap \mathcal{D}_0$, jolloin B on avoin ja suljettu. Joukko $U' \cap B$ on selvästi avoin ja se on myös suljettu, sillä $V' \cap B$ on avoin ja

$$U' \cap B = (X \setminus (V' \cap B)) \cap B.$$

Mutta tällöinhän $U' \cap B \in \mathcal{D}$, sillä $x \in U' \cap B$. Siis

$$A \subset U' \cap B \subset U'$$

ja koska $U = A \cap U'$, niin $A = U$. Joukko A on siis yhtenäinen. □

Seuraavan lemman todistus on peräisin kirjasta [9].

Lemma 7.6. *Jos G on proäärellinen ryhmä, $C \subset G$ on avoin ja suljettu joukko ja $1 \in C$, niin C sisältää G:n avoimen normaalin aliryhmän.*

Todistus. Tavoitteena on muodostaa C:lle pienempiä ja pienempiä avoimia osajoukkoja, joista lopulta saadaan avoin normaali aliryhmä.

Merkitään $f : G \times G \to G$, $f(x, y) = xy$. Kuvaus f on siis ryhmän G kertolasku. Koska G on topologinen ryhmä, niin f on jatkuva.

Olkoon $x \in C$. Nyt $x^{-1}C$ on alkion 1 avoin ympäristö. Näin ollen on olemassa G:n avoimet joukot L_x ja R_x, jotka sisältävät 1:n ja joille $L_x \times R_x \subset f^{-1}(x^{-1}C)$. Toisin sanoen $L_x R_x \subset x^{-1}C$. Joukot L_x ja R_x voidaan valita niin, että ne sisältyvät joukkoon C.

Merkitään $S_x = L_x \cap R_x$, jolloin siis $S_x S_x \subset x^{-1}C$, ja S_x on avoin sekä $S \subset C$. Koska C on G:n suljettu osajoukko, se on kompakti. Joukko C voidaan peittää avoimilla joukoilla xS_x, jossa $x \in C$. Kompaktisuuden nojalla C:n voi peittää äärellisellä määrällä näitä joukkoja, olkoon siis

$$C = \bigcup_{i=1}^{n} x_i S_{x_i}.$$

Olkoon $S = \bigcap_{i=1}^{n} S_{x_i}$. Tällöin edelleen $1 \in S$ ja S on avoin. Nyt joukolle S pätee:

$$CS = \bigcup_{i=1}^{n} x_i S_{x_i} S \subset \bigcup_{i=1}^{n} x_i S_{x_i} S_{x_i} \subset C. \tag{5}$$

Viimeinen osajoukkous johtuu siitä, että $S_x S_x \subset x^{-1}C$ kaikilla $x \in C$.

Merkitään nyt $T = S \cap S^{-1}$ ja tarkastellaan joukon T virittämää ryhmää H. Koska T on avoin ja epätyhjä sekä $T \subset H$, on ryhmä H avoin. Osoitetaan, että $H \subset C$. Koska $T = T^{-1}$, niin $H = \bigcup_{n>0} T^n$, jossa joukko T^n sisältää kaikki T:n alkioiden tulot, jossa on n tekijää. Tällöin $T \subset C$ ja jos $T^{n-1} \subset C$, niin yhtälön (5) nojalla

$$T^n = T^{n-1}T \subset CS \subset C,$$

joten $T^n \subset C$ kaikilla $n > 0$, eli ryhmä H sisältyy joukkoon C.

Koska H on avoin, niin Lemman 7.2 nojalla H:n indeksi on äärellinen. Tällöin H:lla on vain äärellinen määrä konjugaatteja. Näiden konjugaattien leikkaus on avoin normaali aliryhmä, ja koska se sisältyy ryhmään H, niin se sisältyy joukkoon C. □

Lause 7.7. *Jos G on proäärellinen ryhmä, niin sen avoimet normaalit aliryhmät muodostavat alkion* 1 *avoimen ympäristökannan.*

Todistus. Olkoon A avoin joukko, jolle $1 \in A$. Osoitetaan, että on olemassa avoin ja suljettu joukko C, jolle $1 \in C \subset A$. Lemman 7.6 nojalla väite seuraa tästä.

Koska G on täysin epäyhtenäinen, niin alkion 1 yhtenäinen komponentti on $\{1\}$, joten Lauseen 7.5 nojalla pätee

$$\bigcap \mathcal{D} = \{1\} \subset A,$$

jossa $\mathcal{D}$ sisältää kaikki avoimet ja suljetut joukot, jotka sisältävät 1:n.

Koska A on avoin ja kaikki $\mathcal{D}$:n joukot suljettuja, niin kompaktisuuden nojalla on olemassa äärellinen kokoelma $\mathcal{D}_0 \subset \mathcal{D}$, jolle $\bigcap \mathcal{D}_0 \subset A$. Selvästi $\bigcap \mathcal{D}_0$ on avoin ja suljettu. □

Lause 7.8. *Topologinen ryhmä G on proäärellinen, jos ja vain jos se on isomorfinen käänteisen rajan $\varprojlim G_i$ kanssa, jossa G_i ovat äärellisiä ryhmiä, joilla on diskreetti topologia.*

Todistus. Jos G on äärellisten diskreettien ryhmien G_i käänteinen raja, niin G on tulon $\prod_i G_i$ aliavaruus. Tällöin G on Hausdorff-avaruus ja täysin epäyhtenäinen, sillä nämä ominaisuudet pätevät diskreeteille avaruuksille ja säilyvät tuloissa sekä aliavaruuksissa. Tihonovin lauseen perusteella tuloavaruus on kompakti, joten jos raja $G = \varprojlim G_i$ on suljettu, niin sekin on kompakti. Joukko G on leikkaus joukkojen

$$A_{ij} = \{a \in \prod_k G_k \mid \varphi_{ij}(a_j) = a_i\}$$

leikkaus. Nämä joukot ovat suljettuja, joten niiden leikkaus G on suljettu. Ryhmä G on siis kompakti, joten se on proäärellinen.

Oletetaan nyt, että ryhmä G on proäärellinen eli G on kompakti täysin epäyhtenäinen Hausdorff-avaruus. Tarkastellaan ryhmiä G/N, jossa N on ryhmän G avoin normaali aliryhmä. Jos $N_1 \leq N_2$ ovat kaksi tällaista aliryhmää, niin voidaan määritellä surjektiivinen homomorfismi $\varphi : G/N_1 \to G/N_2$, jolle $\varphi(xN_1) = xN_2$. Selvästi nämä homomorfismit ovat keskenään yhteensopivia.

Ryhmät N voidaan järjestää käänteisen sisältymisen suhteen. Tämä on suunnattu joukko: jos N_1 ja N_2 ovat kaksi avointa normaalia aliryhmää, niin niiden leikkaus $N_1 \cap N_2$ on avoin normaali aliryhmä, joka sisältyy molempiin. Tällöin ryhmät $N \lhd_\circ G$ ja homomorfismit φ muodostavat käänteisen järjestelmän.

Olkoon L tämän järjestelmän käänteinen raja. Osoitetaan, että L ja G ovat topologisina ryhminä isomorfisia.

Määritellään kuvaus $f : G \to L$ siten, että $f(x) = (xN)_{N \lhd_\circ G}$. Kuvausten φ määritelmän nojalla $f(x) \in L$.

Osoitetaan, että f on surjektio. Näytetään ensin, että jos $x = (a_N/N)_N \in L$, niin joukko $\bigcap_N a_N N$ on epätyhjä. Olkoot $N_1, \ldots, N_k$ ryhmän G avoimia normaaleja aliryhmiä. Niiden leikkaus $N' = N_1 \cap \cdots \cap N_k \lhd_\circ G$. Tällöin alkion x aliryhmää N' vastaavalle komponentille $a_{N'}N'$ pätee $a_{N'}N_i = a_{N_i}N_i$. Toisin sanoen $a_{N'} \in \bigcap a_{N_i}N_i$, joten äärellinen leikkaus on epätyhjä. Koska joukot $a_N N$ ovat suljettuja ja G on kompakti, niin myös koko leikkaus $\bigcap_N a_N N$ on epätyhjä. Olkoon $a \in \bigcap_N a_N N$. Nyt $f(a) = (aN)_N = (a_N N)_N = x$. Kuvaus f on siis surjektio.

Näytetään seuraavaksi, että f on injektio. Avoimet normaalit aliryhmät muodostavat alkion 1 ympäristökannan ja niiden leikkaukseen voi sisältyä vain yksi alkio, sillä G on Hausdorff-avaruus. Nyt jos $f(a) = f(b)$, niin $aN = bN$ kaikilla $N \lhd_\circ G$, joten

$$a^{-1}b \in \bigcap_{N \lhd_\circ G} N = \{1\},$$

eli $a = b$ ja f on injektio.

Vielä on näytettävä, että f on homeomorfismi. Tätä varten riittää näyttää, että f on jatkuva, sillä G on kompakti ja L on Hausdorff-avaruus.

Muotoa $p_N^{-1}(\{N\})$ olevat joukot muodostavat alkion 1 ympäristöesikannan ryhmässä L, jossa p_N on projektio $L \to G/N$. Koska f:n alkukuva joukosta $p_N^{-1}(\{N\})$ on N, joka on siis avoin, niin Lauseen 7.4 nojalla f on jatkuva. □

Sulkeuman voi määrittää proäärellisessä ryhmässä seuraavan muotoilun avulla.

Lause 7.9. *Olkoon G proäärellinen ryhmä ja $X \subset G$. Tällöin joukon X sulkeuma on $\overline{X} = \bigcap\{XN \mid N \lhd_\circ G\}$. Erityisesti, jos H on aliryhmä, niin $\overline{H} = \bigcap\{K | H \leq K \leq_\circ G\}$.*

Todistus. Olkoon $x \in G$. Seuraavat ehdot ovat yhtäpitäviä:

1. $x \in \overline{X}$

2. $xN \cap X \neq \emptyset$ kaikilla $N \lhd_\circ G$. (Joukot xN muodostavat alkion x ympäristökannan.)

3. Kaikilla $N \lhd_\circ X$ on olemassa $y \in X$, jolle $y \in xN$.

4. Kaikilla $N \lhd_\circ X$ on olemassa $y \in X$, jolle $x \in yN$.

5. Kaikilla $N \lhd_\circ X$ pätee $x \in XN$.

6. $x \in \bigcap\{XN \mid N \lhd_\circ G\}$.

Tämän perusteella väite on ilmeinen. □

8 Proäärelliset ryhmät Galois-ryhminä

Esitellään nyt yhteys Galois-ryhmien ja proäärellisten ryhmien välillä. Tässä luvussa osoitetaan, että Galois-ryhmät ovat aina proäärellisiä ja toisaalta kaikki proäärelliset ryhmät ovat Galois-laajennusten Galois-ryhmiä.

Olkoon K/F Galois-laajennus. Tällöin K on yhdiste äärellisistä normaaleista laajennuksista muotoa $K_i = F(x_1, \ldots, x_r)$, jossa $x_1, \ldots, x_r$ ovat jonkin F-kertoimisen polynomin juuret. Indeksit i voidaan järjestää sisältymisen mukaan, eli $i \leq j$, jos ja vain jos $K_i \subset K_j$. Joukko $(K_i)_i$ on tällöin suunnattu joukko, sillä kahden tällaisen laajennuksen yhdiste sisältyy aina johonkin kolmanteen:

$$F(x_1, \ldots, x_r) \cup F(x_{r+1}, \ldots, x_s) \subset F(x_1, \ldots, x_s).$$

Jos K_i ja K_j ovat K/F:n äärellisiä normaaleja alilaajennuksia ja $K_i \leq K_j$, niin kunnan K_j jokainen F-automorfismi voidaan rajoittaa K_i:n F-automorfismiksi. Näin saadaan kuvaus $\varphi_{ij} : \mathrm{Gal}(K_j/F) \to \mathrm{Gal}(K_i/F)$. Koska kaikki kuvaukset φ_{ij} ovat rajoittumia, niin selvästi pätee $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$ kaikilla $i \leq j \leq k$.

Lause 8.1. *Jos K/F on Galois-laajennus, niin sen Galois-ryhmä on*

$$\mathrm{Gal}(K/F) \cong \varprojlim \mathrm{Gal}(K_i/F),$$

jossa suunnattu joukko $(K_i)_{i\in I}$ sisältää kaikki ne laajennuksen K/F alilaajennukset K_i, joille K_i/F on äärellinen normaali laajennus. Erityisesti $\mathrm{Gal}(K/F)$ *on proäärellinen.*

Todistus. Olkoon $\alpha \in K$ mielivaltainen alkio ja $f(t) \in F[t]$ sen minimaalipolynomi. Tällöin $f(t)$:n juurikunta on F:n äärellinen normaali laajennus K_i, joka sisältää α:n. Toisin sanoen kaikki K:n alkiot kuuluvat johonkin alikuntaan K_i, joten $K = \bigcup_{i\in I} K_i$.

Määritellään homomorfismi

$$f : \mathrm{Gal}(K/F) \to \varprojlim \mathrm{Gal}(K_i/F),$$

jolle $f(\varphi)_i$ on automorfismin φ rajoittuma kunnalle K_i. Lauseen 6.2 nojalla f on ryhmien isomorfismi. Näytetään vielä, että f on myös topologisten ryhmien isomorfismi, eli että f on lisäksi homeomorfismi.

Muistetaan, että ryhmät $\mathrm{Gal}(K/K_i)$, jossa K_i on kunnan F äärellinen normaali laajennus, muodostavat alkion 1 ympäristökannan topologisessa avaruudessa $\mathrm{Gal}(K/F)$. Jokainen kantajoukko $\mathrm{Gal}(K/K_i)$ kuvautuu joukoksi alkioita $(g_j)_{j\in I}$, jossa komponentti $g_i \in \mathrm{Gal}(K_i/F)$ on 1, eli $f(\mathrm{Gal}(K/K_i)) = p_i^{-1}(\{1\})$. Joukot $p_i^{-1}(\{1\})$ muodostavat alkion 1 ympäristöesikannan avaruudessa $\varprojlim \mathrm{Gal}(K_i/F)$.

Siis 1:n ympäristökanta ryhmässä $\mathrm{Gal}(K/F)$ kuvautuu 1:n ympäristöesikannaksi ryhmässä $\varprojlim \mathrm{Gal}(K_i/F)$. Näin ollen f on Lauseen 2.1 nojalla jatkuva ja avoin bijektio, eli homeomorfismi.

Huomataan vielä, että laajennukset K_i/F ovat äärellisiä Galois-laajennuksia, joten Lauseen 5.3 nojalla kaikki $\mathrm{Gal}(K_i/F)$ ovat äärellisiä. Siis $\mathrm{Gal}(K/F)$ on proäärellinen. □

Lause 8.2. *Olkoon K/F Galois-laajennus ja G sen Galois-ryhmä. Tällöin aliryhmä $H \leq G$ on suljettu, jos ja vain jos se on muotoa $H = \mathrm{Gal}(K/L)$ jollain kuntien K ja F välissä olevalla kunnalla L.*

Todistus. Jos L on K:n ja F:n välissä oleva kunta, niin laajennus K/L on Galois-laajennus. Tällöin $\mathrm{Gal}(K/L)$ on Lauseen 8.1 nojalla kompakti. Tästä seuraa, että $\mathrm{Gal}(K/L)$ on G:n suljettu osajoukko.

Olkoon nyt H jokin G:n suljettu aliryhmä ja L sen kiintokunta. Nyt L on laajennuksen K/F alilaajennus ja K/L on Galois-laajennus. Nyt H selvästi sisältyy ryhmään $\mathrm{Gal}(K/L)$, sillä H kiinnittää L:n. Jos H on tiheä $\mathrm{Gal}(K/L)$:ssä, niin silloin on oltava $H = \mathrm{Gal}(K/L)$, koska H on suljettu.

Näytetään, että H on tiheä ryhmässä $\mathrm{Gal}(K/L)$. Tätä varten riittää näyttää, että kaikilla $\varphi \in \mathrm{Gal}(K/L)$ pätee

$$\varphi\mathrm{Gal}(K/N) \cap H \neq \emptyset \tag{6}$$

aina, kun $N \subset K$ on L:n äärellinen normaali laajennus, koska sivuluokat $\varphi\mathrm{Gal}(K/N)$ muodostavat ryhmän $\mathrm{Gal}(K/L)$ topologian kannan. Yhtälö (6) on yhtäpitävä sen kanssa, että on olemassa $\tau \in H$, jolle $\tau|_N = \varphi|_N$.

Koska N/L on normaali laajennus, niin kaikilla $\tau \in H$ pätee $\tau|_N \in \mathrm{Gal}(N/L)$. Huomataan, että Lauseen 5.3 nojalla ryhmä $\mathrm{Gal}(N/L)$ on äärellinen. Ryhmän $H_0 = \{\tau|_N \mid \tau \in H\}$ kiintokunta on L, joten $H_0 = \mathrm{Gal}(N/L)$. Koska $\varphi|_N \in \mathrm{Gal}(N/L) = H_0$, niin on olemassa $\tau \in H$, jolle $\tau|_N = \varphi|_N$. Ryhmä H on siis tiheä $\mathrm{Gal}(K/L)$:ssä, joten $H = \overline{H} = \mathrm{Gal}(K/L)$. □

Lause 8.3. *Jokaiselle proäärelliselle ryhmälle G on olemassa sellaiset kunnat K ja L, että K on L:n Galois-laajennus ja Galois-ryhmä $\mathrm{Gal}(K/L)$ on isomorfinen ryhmän G kanssa. Lisäksi, jos F on mielivaltainen kunta, niin kunnat K ja L voidaan valita niin, että $F \leq L \leq K$.*

Todistus. Merkitään S:llä joukkojen G/N erillistä yhdistettä, jossa N käy läpi kaikki G:n avoimet normaalit aliryhmät. Olkoon F annettu kunta ja $K = F(t_s)$, jossa symbolit t_s ovat riippumattomia muuttujasymboleita, kun $s \in S$. Toisin sanoen K on muuttujien t_s rationaalilausekkeiden kunta.

Ryhmä G toimii joukossa S vasemmanpuoleisella kertolaskulla: jos $g \in G$ ja $hN \in T$, niin $g(hN) = ghN$. Toiminta voidaan laajentaa myös kuntaan K, jolloin $g(t_s) = t_{gs}$. Tällöin saadaan homomorfismi θ ryhmästä G kunnan K automorfismien ryhmään: $(\theta(g))(x) = g(x)$. Sen ydin on kaikkien avointen normaalien aliryhmien leikkaus, joka on Lauseen 7.7 ja Hausdorffin ehdon nojalla triviaali. Toisin sanoen θ on injektio.

Osoitetaan, että G:n toiminnassa radat ovat äärellisiä. Jos $x \in K$, niin x on rationaalilauseke, jossa esiintyy vain äärellinen määrä muuttujia. Oletetaan, että lausekkeessa x esiintyvien muuttujien joukko on $\{t_{s_1}, \ldots, t_{s_r}\}$, jossa $s_i = g_i N_i$. Tällöin alkion x vakauttaja G_x sisältää avoimen ryhmän $N_1 \cap \cdots \cap N_r$, joten se on itsekin avoin. Lauseen 7.2 nojalla G_x:n indeksi on äärellinen ja rata-vakauttajalauseesta seuraa, että x:n rata on äärellinen.

Olkoon L ryhmän $\theta(G)$ kiintokunta eli

$$L = \{x \in K \mid g(x) = x \ \forall g \in G\}.$$

Jos $x \in K$ on mielivaltainen alkio, niin ylläolevan perusteella sen rata on äärellinen, olkoon se $\{x_1, \ldots, x_r\}$. Nyt polynomin

$$f(t) = \prod_{i=1}^{r} (t - x_i)$$

kertoimet ovat kunnassa L, koska $g(f(t)) = f(t)$ kaikilla $g \in G$. Polynomin $f(t)$ arvo x:llä on $f(x) = 0$, koska x tietenkin kuuluu omaan rataansa. Näin ollen x on algebrallinen yli kunnan L ja K/L on algebrallinen laajennus. Koska L on automorfismiryhmän $\theta(G)$ kiintokunta, niin K/L on Lauseen 5.2 nojalla Galois-laajennus. Olkoon $H = \mathrm{Gal}(K/L)$ sen Galois-ryhmä.

Tavoitteena on nyt näyttää, että G on topologisena ryhmänä isomorfinen H:n kanssa. Osoitetaan, että kuvaus $\theta : G \to H$ on jatkuva. Jos U on H:n avoin normaali aliryhmä, niin sen kiintokunta on L:n äärellinen laajennus, merkitään sitä $L(x'_1, \ldots, x'_r)$. Nyt $\theta^{-1}(U) \supset \bigcap_{i=1}^{r} G_{x_i}$, joka on avoin, joten $\theta^{-1}(U)$ on avoin. Kuvaus θ on siis Lauseiden 7.7 ja 7.4 nojalla jatkuva, ja koska G on kompakti, niin sen kuva $\theta(G)$ on suljettu. Ryhmä G on kompakti ja $\theta(G)$ Hausdorff-avaruus, joten jokainen jatkuva bijektio $G \to \theta(G)$ on homeomorfismi. Erityisesti θ on homeomorfismi.

Koska $\theta(G)$ on H:n suljettu aliryhmä ja L on sen kiintokunta, niin Lauseen 8.2 nojalla $\theta(G) = \mathrm{Gal}(K/L) = H$. □

8.1 Esimerkki: Äärellisen kunnan algebrallinen sulkeuma

Nyt on kehitetty riittävästi koneistoa, jotta voidaan laskea äärellisen kunnan $\mathbb{F}_p$ *absoluuttinen Galois-ryhmä*. Tämä tarkoittaa ryhmää $\mathrm{Gal}(\mathbb{F}_p^{alg}/\mathbb{F}_p)$, jossa $\mathbb{F}_p^{alg}$ on

kunnan $\mathbb{F}_p$ *algebrallinen sulkeuma*. Määritellään tämä seuraavaksi.

Määritelmä. Olkoon F kunta. Sen laajennus $K \supset F$ on F:n *algebrallinen sulkeuma*, jos K/F on algebrallinen laajennus ja K:lla ei ole aitoa algebrallista laajennusta.

Ehto, että K:lla ei ole aitoa algebrallista laajennusta on yhtäpitävä sen kanssa, että jokaisella polynomilla $f(t) \in K[t]$, joka ei ole vakio, on juuri K:ssa. Nimittäin, jos näin ei olisi, niin voitaisiin muodostaa K:n algebrallinen laajennus, jossa $f(t)$:llä olisi juuri.

On tunnettua (katso [8]), että jokaisella kunnalla on algebrallinen sulkeuma ja että se on F-isomorfiaa vaille yksikäsitteinen.

Tarkastellaan, millaisia algebrallisia laajennuksia kunnalla $\mathbb{F}_p$ voi olla, kun p on alkuluku. Jos $K/\mathbb{F}_p$ on algebrallinen laajennus, niin jokainen $x \in K$ on jonkin polynomin $f(t) \in \mathbb{F}_p[t]$ juuri. Tällöin $\mathbb{F}_p(x)$ on kunnan $\mathbb{F}_p$ äärellinen laajennus, joten se on itsekin äärellinen kunta. Tarkemmin sanoen $\mathbb{F}_p(x) = \mathbb{F}_{p^n}$, jossa $n = \deg(f(t))$.

Koska sama pätee jokaiselle $x \in K$, niin itse asiassa K on yhdiste äärellisistä kunnista

$$K = \bigcup_{n \in S} \mathbb{F}_{p^n}$$

jollekin joukolle $S \subset \mathbb{Z}_+$. Näin ollen suurin mahdollinen $\mathbb{F}_p$:n algebrallinen laajennus on kaikkien tällaisten kuntien yhdiste, joka on siis $\mathbb{F}_p$:n algebrallinen sulkeuma

$$\mathbb{F}_p^{alg} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}.$$

Kunnille $\mathbb{F}_{p^n}$ ja $\mathbb{F}_{p^m}$ pätee, että $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, jos ja vain jos $n|m$. Jokainen automorfismiryhmä $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ on syklinen n:n alkion ryhmä C_n. Näin ollen Lauseen 6.2 nojalla

$$\mathrm{Gal}(\mathbb{F}_p^{alg}/\mathbb{F}_p) = \varprojlim C_n.$$

Tässä siis käänteisessä järjestelmässä ryhmältä C_m on luonnollinen surjektio ryhmälle C_n, kun $n|m$.

Ryhmää $\varprojlim C_n$ merkitään yleensä $\widehat{\mathbb{Z}}$ ja sitä kutsutaan kokonaislukujen *proäärelliseksi täydellistymäksi*. Sen alkioita voi kuvata eräänlaisilla Cauchy-jonoilla kokonaislukujen joukossa: jono (a_n) on Cauchy-jono, jos kaikilla $m \in \mathbb{Z}_+$ on olemassa N, jolle $a_i \equiv a_j \pmod{m}$ kaikilla $i, j \geq N$.

Samaistetaan jonot (a_n) ja (b_n), jos kaikilla $m \in \mathbb{Z}_+$ on olemassa N, jolle $a_n \equiv b_n \pmod{m}$ kaikilla $n \geq N$. Kun otetaan näin saadun ekvivalenssirelaation luokat, saadaan ryhmä, joka on isomorfinen $\widehat{\mathbb{Z}}$:n kanssa.

9 Nottinghamin ryhmä

Tutkitaan seuraavaksi yhtä esimerkkiä pro-p-ryhmästä. Topologinen ryhmä G on *pro-p-ryhmä*, jos se on proäärellinen ja sen jokaisen avoimen normaalin aliryhmän

indeksi on alkuluvun p potenssi. Yhtäpitävästi G on käänteinen raja äärellisistä p-ryhmistä.

Kiinnitetään ensin alkuluku p. Nottinghamin ryhmän $\mathcal{N}$ alkiot ovat potenssisarjoja, joiden kertoimet ovat kunnassa $\mathbb{F}_p$. Ryhmän laskutoimituksena ei ole yhteen- eikä kertolasku, vaan sijoittaminen. Ryhmä $\mathcal{N}$ sisältää kaikki ne kunnan $\mathbb{F}_p[[t]]$ alkiot, joiden vakiotermi on 0 ja ensimmäisen asteen termin kerroin on 1. Toisin sanoen

$$\mathcal{N} = \{t + t^2 f(t) \mid f(t) \in \mathbb{F}_p[[t]]\}.$$

Laskutoimitus on sijoitus, eli jos $f, g \in \mathcal{N}$, niin $fg = f(g)$. Tämä on hyvin määritelty, sillä kaikkien sijoitettavien vakiotermi on 0. Tulos fg myös kuuluu joukkoon $\mathcal{N}$, sillä jos $f(t) = t + t^2 f_1(t)$ ja $g(t) = t + t^2 g_1(t)$, niin

$$\begin{aligned} f(g(t)) &= (t + t^2 g_1(t)) + (t + t^2 g_1(t))^2 f_1(g(t)) \\ &= t + t^2 \left(g_1(t) + (1 + t g_1(t))^2 f_1(g(t))\right) \in \mathcal{N}. \end{aligned}$$

Lauseen 3.5 nojalla laskutoimitus on liitännäinen. Ryhmän $\mathcal{N}$ neutraalialkio on potenssisarja t. Jos $f(t) = t + t^2 f_1(t) \in \mathcal{N}$, niin alkion f käänteisalkion $g(t) = t + t^2 g_1(t)$ tulee toteuttaa $f(g(t)) = g(f(t)) = t$. Kirjoitetaan auki yhtälö $f(g(t)) = t$:

$$\begin{aligned} & t + t^2 \left(g_1(t) + (1 + t g_1(t))^2 f_1(g(t))\right) = t \\ \Leftrightarrow & g_1(t) = -(1 + t g_1(t))^2 f_1(t + t^2 g_1(t)) \end{aligned}$$

Merkitään

$$L(g_1(t)) = -(1 + t g_1(t))^2 f_1(t + t^2 g_1(t)).$$

Nyt alkion $f(t)$ käänteisalkion löytäminen vaatii funktion $L : \mathbb{F}_p[[t]] \to \mathbb{F}_p[[t]]$ kiintopisteen löytämistä. Lauseen 3.6 avulla nähdään, että jos $k(t) \equiv h(t) \pmod{t^n}$, niin $L(k(t)) \equiv L(h(t)) \pmod{t^{n+1}}$. Toisin sanoen

$$|L(k(t)) - L(h(t))| \leq \frac{1}{2} |k(t) - h(t)|$$

kaikilla $k(t), h(t) \in \mathbb{F}_p[[t]]$. Kuvaus L on siis kontraktio, joten Banachin kiintopistelauseen nojalla sillä on yksikäsitteinen kiintopiste joukossa $\mathbb{F}_p[[t]]$: merkitään sitä $g_1(t)$:llä ja valitaan $g(t) = t + t^2 g_1(t) \in \mathcal{N}$.

Aiemman nojalla nyt siis pätee $fg = t$. Vielä pitää osoittaa, että tästä seuraa $gf = t$. Koska laskutoimitus liitännäinen, niin pätee $(gf)g = g(fg) = g = tg$. Jos onnistutaan todistamaan, että kuvaus $x \mapsto xg$ on injektio, niin saadaan $gf = t$. Halutaan siis näyttää, että sijoitushomomorfismi $h_g : \mathbb{F}_p[t] \to \mathbb{F}_p[t]$, jolle $h_g(f(t)) = f(g(t))$, on injektio kaikilla $g \in \mathcal{N}$.

Lemma 9.1. *Jos $g \in \mathcal{N}$, niin sijoitushomomorfismi h_g on injektio.*

Todistus. Olkoon $g(t) = t(1 + t g_1(t))$. Näytetään, että $\mathrm{Ker}(h_g) = \{0\}$. Olkoon $k(t) = \sum_{i \geq 0} a_i t^i \in \mathbb{F}_p[[t]] \setminus \{0\}$. Valitaan pienin n, jolle $a_n \neq 0$. Nyt

$$h_g(k(t)) = k(g(t)) = a_n t^n (1 + t g_1(t))^n + \sum_{i > n} a_i t^i (1 + t g_1(t))^i \equiv a_n t^n \pmod{t^{n+1}},$$

ja toisaalta $a_n t^n \not\equiv 0 \pmod{t^{n+1}}$. Siis $h_g(k(t)) \neq 0$, eli $k(t) \notin \mathrm{Ker}(h_g)$. □

Nyt Lemman 9.1 ja ylläolevan nojalla $\mathcal{N}$ on ryhmä.

Koska $\mathcal{N} \subset \mathbb{F}_p[[t]]$, niin $\mathbb{F}_p[[t]]$ indusoi $\mathcal{N}$:lle topologian, jonka kanssa $\mathcal{N}$ on Hausdorff-avaruus. Osoitetaan, että $\mathcal{N}$ on myös topologinen ryhmä.

Lause 9.2. *Ryhmä $\mathcal{N}$ on topologinen ryhmä, kun sille annetaan joukosta $\mathbb{F}_p[[t]]$ peritty topologia.*

Todistus. Olkoon $n \geq 1$. Lauseen 3.6 nojalla projektiokuvaus p_n renkaalta $\mathbb{F}_p[[t]]$ sen tekijärenkaalle $\mathbb{F}_p[[t]]/(t^n)$ on kuvaus, joka säilyttää potenssisarjojen sijoituksen. Kun rajoitetaan p_n ryhmälle $\mathcal{N}$, niin sen kuva on tällöin ryhmä $\mathcal{N}/(t^n)$, jossa laskutoimituksena on edelleen sijoitus. Kuvaus p_n on homomorfismi ryhmältä $\mathcal{N}$ ryhmälle $\mathcal{N}/(t^n)$.

Huomataan, että ryhmässä $\mathcal{N}$ pätee $|f - g| \leq 2^{-n}$, jos ja vain jos $p_n(f) = p_n(g)$. Jos $f, g \in \mathcal{N}$, joille $p_n(f) = p_n(g)$, niin myös

$$p_n(f^{-1}) = p_n(f)^{-1} = p_n(g)^{-1} = p_n(g^{-1}).$$

Näin ollen $|f^{-1} - g^{-1}| \leq |f - g|$ ja kuvaus $f \mapsto f^{-1}$ on jatkuva. Vastaavasti myös $\mathcal{N}$:n kertolasku on jatkuva. □

Lause 9.3. *Ryhmä $\mathcal{N}$ on proäärellinen.*

Todistus. Koska $\mathbb{F}_p[[t]]$ on topologisena avaruutena homeomorfinen tulon $\mathbb{F}_p^{\mathbb{N}}$ kanssa, niin se on Tihonovin lauseen nojalla kompakti. Joukko $\mathcal{N}$ on $\mathbb{F}_p[[t]]$:n kuva jatkuvassa kuvauksessa $f \mapsto t + t^2 f$, joten $\mathcal{N}$ on kompakti. Selvästi se on myös Hausdorff-avaruus.

Koska jokainen joukko muotoa $f + t^n \mathbb{F}_p[[t]]$ on avoin ja suljettu, niin Lauseen 7.5 nojalla $\mathcal{N}$:n kaikki yhtenäiset joukot ovat yksiöitä. Ryhmä $\mathcal{N}$ on siis täysin epäyhtenäinen. □

Huomataan, että joukot $t + t^n \mathbb{F}_p[[t]]$, jossa $n \geq 2$, ovat $\mathcal{N}$:n aliryhmiä ja muodostavat t:n ympäristökannan. Siis jokainen avoin aliryhmä sisältää jonkin tätä muotoa olevan ryhmän. Aliryhmän $t + t^n \mathbb{F}_p[[t]]$ indeksi on p^{n-2}, joten jokaisen avoimen aliryhmän indeksi on p:n potenssi. $\mathcal{N}$ on siis pro-p-ryhmä.

Nottinghamin ryhmää voi myös ajatella renkaan $\mathbb{F}_p[[t]]$ automorfismiryhmänä. Tällöin samaistetaan $f \in \mathcal{N}$ sijoitushomomorfismin h_f kanssa. Huomataan, että kuvauksen h_f käänteiskuvaus on $h_{f^{-1}}$, joten sijoitushomomorfismit ovat bijektioita ja siis automorfismeja.

Voidaan osoittaa (katso [7, luku 6]), että jokainen $\mathbb{F}_p[[t]]$:n automorfismi voidaan laajentaa yksikäsitteisellä tavalla kunnan $\mathbb{F}_p((t))$:n automorfismiksi, eli ryhmät $\mathrm{Aut}(\mathbb{F}_p[[t]])$ ja $\mathrm{Aut}(\mathbb{F}_p((t)))$ ovat isomorfisia. Näin Nottinghamin ryhmä on myös $\mathrm{Aut}(\mathbb{F}_p((t)))$:n aliryhmä. Sen radat ovat kuitenkin äärettömiä, joten se ei ole minkään algebrallisen laajennuksen Galois-ryhmä.

Galois-laajennuksen määritelmä voidaan yleistää siten, ettei laajennuksen tarvitse olla algebrallinen. Tällöin määritellään, että K/F on Galois-laajennus, jos F on jonkin ryhmän $G \leq \mathrm{Aut}(K)$ kiintokunta. Tämä on Lauseen 5.2 nojalla algebrallisille laajennuksille yhtäpitävä luvussa 5 annetun määritelmän kanssa. Tämän määritelmän mukaan myös $\mathcal{N}$ on Galois-ryhmä.

10 Haarin mitta

Esitellään nyt, miten jokaiselle proäärelliselle ryhmälle voidaan määritellä siirtoinvariantti todennäköisyysmitta. Sitä kutsutaan *Haarin mitaksi*.

Osoitetaan ensin aputulos siitä, miten avoimet suljetut joukot voidaan esittää.

Lemma 10.1. *Olkoon G proäärellinen ryhmä. Jos $C \subset G$ on avoin ja suljettu joukko, niin C on muotoa*

$$C = \bigcup_{i=1}^{n} x_i N,$$

jossa N on G:n avoin normaali aliryhmä.

Todistus. Lauseen 7.7 nojalla jokainen avoin joukko on yhdiste avointen normaalien aliryhmien sivuluokista. Koska C on myös suljettu, niin se on kompakti ja näin ollen C on äärellinen yhdiste $C = \bigcup_{j=1}^{k} x_j N_j$, jossa kaikki N_j ovat G:n avoimia normaaleja aliryhmiä. Merkitään $N = N_1 \cap \cdots \cap N_k$, jolloin N on myös avoin normaali aliryhmä. Koska jokainen $x_j N_j$ on äärellinen yhdiste N:n sivuluokista, niin myös C on tätä muotoa. □

Määritelmä. Topologisen avaruuden X *Borel-algebra* on pienin σ-algebra, joka sisältää kaikki avoimet joukot. Borel-algebran joukkoja kutsutaan *Borel-joukoiksi*.

Lause 10.2. *Olkoon G proäärellinen ryhmä. Merkitään G:n Borel-algebraa $\mathcal{B}$:llä. Tällöin on olemassa mitta $\mu : \mathcal{B} \to \mathbb{R}$, jolla on seuraavat ominaisuudet:*

- $\mu(G) = 1$
- *μ on siirtoinvariantti: jos $S \in \mathcal{B}$ ja $x \in G$, niin $\mu(S) = \mu(aS) = \mu(Sa)$.*
- *Jos $U \subset G$ on avoin epätyhjä joukko, niin $\mu(U) > 0$.*

Todistus. Määritellään Haarin mitta samaan tapaan kuin Lebesguen mitta (katso [5]): määritellään ensin kaikille joukoille ulkomitta, ja sen jälkeen rajoitutaan mitallisiin joukkoihin.

Merkitään $\mathcal{B}_0$:lla niiden joukkojen perhettä, jotka ovat avoimia ja suljettuja. Ensin määritellään mitta joukoille $C \in \mathcal{B}_0$: tällaiset joukot ovat Lemman 10.1 nojalla muotoa $C = \bigcup_{i=1}^{m} x_i N$, jossa N on avoin normaali aliryhmä. Jos sivuluokat $x_i N$

ovat erillisiä, niin määritellään $\mu_0(C) = m/[G : N]$. Koska mitasta halutaan siirtoinvariantti, niin tämä on ainoa mahdollinen tapa määritellä joukon C mitta.

Osoitetaan, että μ_0 on hyvin määritelty. Jos $C \in \mathcal{B}_0$ on esitettävissä kahden avoimen normaalin aliryhmän N ja N' avulla, niin $C = \bigcup_{i=1}^{m} x_i N$ joillain $x_i \in G$. Tässä voidaan olettaa, että $N' \leq N$. Merkitään N':n sivuluokkien edustajia N:ssä $y_1, \ldots, y_k$, jossa $k = [N : N']$. Tällöin

$$C = \bigcup_{i=1}^{m} \bigcup_{j=1}^{k} x_i y_j N',$$

joten laskettuna N':n mukaan

$$\mu_0(C) = mk/[G : N'] = mk/([G : N][N : N']) = m/[G : N],$$

joka on sama kuin N:n mukaan laskettuna. Kuvaus μ_0 on siis hyvin määritelty.

Huomataan, että $\mathcal{B}_0$ on joukkoalgebra ja $\mu_0 : \mathcal{B}_0 \to \mathbb{R}$ on additiivinen joukkofunktio: jos $A, B \in \mathcal{B}_0$ ovat erillisiä, niin $\mu_0(A \cup B) = \mu_0(A) + \mu_0(B)$.

Laajennetaan μ_0 avoimiin joukkoihin: jos $U \subset G$ on avoin, niin määritellään

$$\mu_1(U) = \sup\{\mu_0(C) \mid C \in \mathcal{B}_0, C \subset U\}.$$

Selvästi μ_1 on sisältymisen suhteen monotoninen ja sen rajoittuma $\mathcal{B}_0$:lle on μ_0.

μ_1 on subadditiivinen. Olkoot U ja V avoimia joukkoja ja $\epsilon > 0$. Valitaan $C \in \mathcal{B}_0$, jolle $\mu_0(C) > \mu_1(U \cup V) - \epsilon$. Lauseen 7.7 nojalla $\mathcal{B}_0$ on G:n topologian kanta, joten U ja V ovat yhdisteitä $\mathcal{B}_0$:n joukoista. Olkoon $U = \bigcup \mathcal{D}_1$ ja $V = \bigcup \mathcal{D}_2$, jossa $\mathcal{D}_i \subset \mathcal{B}_0$. Koska C on kompakti ja $C \subset \bigcup(\mathcal{D}_1 \cup \mathcal{D}_2)$, niin on olemassa äärelliset $\mathcal{D}_i' \subset \mathcal{D}_i$, joille $C \subset \bigcup(\mathcal{D}_1' \cup \mathcal{D}_2')$. Tällöin joukot $C_i' = \bigcup \mathcal{D}_i' \in \mathcal{B}_0$ ovat erillisiä ja toteuttavat $C \subset C_1' \cup C_2'$ sekä $C_1' \subset U$ ja $C_2' \subset V$. Nyt pätee

$$\mu_1(U \cup V) < \mu_0(C) + \epsilon \leq \mu_0(C_1') + \mu_0(C_2') + \epsilon \leq \mu_1(U) + \mu_1(V) + \epsilon.$$

Koska ϵ valittiin mielivaltaisesti, niin $\mu_1(U \cup V) \leq \mu_1(U) + \mu(V)$.

μ_1 on additiivinen. Näytetään, että jos U ja V ovat erillisiä avoimia joukkoja, niin niille pätee $\mu_1(U \cup V) = \mu_1(U) + \mu_1(V)$. Olkoon $\epsilon > 0$. Valitaan sellaiset $C, D \in \mathcal{B}_0$, joille $C \subset U$, $D \subset V$ sekä $\mu_0(C) > \mu_1(U) - \epsilon/2$ ja $\mu_0(D) > \mu_1(V) - \epsilon/2$. Nyt C ja D ovat erillisiä, joten μ_0:n additiivisuuden nojalla

$$\mu_1(U) + \mu_1(V) < \mu_0(C) + \mu_0(D) + \epsilon = \mu_0(C \cup D) + \epsilon \leq \mu_1(U \cup V) + \epsilon.$$

Koska ϵ valittiin mielivaltaisesti, niin $\mu_1(U) + \mu_1(V) = \mu_1(U \cup V)$.

Määritellään seuraavaksi mielivaltaisen joukon ulkomitta. Jos $A \subset G$, niin sen ulkomitta määritellään

$$\mu^*(A) = \inf\{\mu_1(U) \mid A \subset U,\ U \text{ avoin}\}.$$

Infimum otetaan siis kaikista avoimista joukoista, jotka sisältävät joukon A. Koska aina pätee $A \subset G$ ja $\mu_1(G) = 1$, niin kaikkien joukkojen ulkomitta on korkeintaan 1. Koska μ_1 on monotoninen, niin μ^* rajoitettuna avoimille joukoille on μ_1.

μ^* on ulkomitta. On helppo nähdä, että μ^* toteuttaa ulkomitan ehdot:

- $\mu^*(\emptyset) = 0$
- Jos $A \subset B$, niin $\mu^*(A) \leq \mu^*(B)$.
- Jos $A_i \subset G$ kaikilla $i \in \mathbb{N}$, niin
$$\mu^*(\bigcup_{i\in\mathbb{N}} A_i) \leq \sum_{i\in\mathbb{N}} \mu^*(A_i).$$

Vain viimeinen kohta ei ole itsestään selvä. Olkoot $A_i \subset G$ kaikilla $i \in \mathbb{N}$ ja $\epsilon > 0$. Valitaan sellainen avoin U_i, jolle $A_i \subset U_i$ ja $\mu_1(U_i) < \mu^*(A_i) + \epsilon/2^{i+1}$. Nyt
$$\mu^*(\bigcup_{i\in\mathbb{N}} A_i) \leq \mu_1(\bigcup_{i\in\mathbb{N}} U_i) \leq \sum_{i\in\mathbb{N}} \mu^*(A_i) + \epsilon.$$
Koska ϵ valittiin mielivaltaisesti, niin $\mu^*(\bigcup_{i\in\mathbb{N}} A_i) \leq \sum_{i\in\mathbb{N}} \mu^*(A_i)$.

Mitalliset joukot. Nyt voidaan määritellä, että joukko $A \subset G$ on *mitallinen*, jos kaikilla $X \subset G$ pätee
$$\mu^*(X) = \mu^*(X \cap A) + \mu^*(X \setminus A).$$
Merkitään $\mathcal{M}$:llä kaikkien G:n mitallisten osajoukkojen perhettä. On tunnettua, että $\mathcal{M}$ on tällöin σ-algebra ja μ^* rajoitettuna $\mathcal{M}$:lle on mitta (katso [1, Lause 9.22]).

Haluamme näyttää, että kaikki Borel-joukot kuuluvat $\mathcal{M}$:n. Näytetään ensin, että $\mathcal{B}_0 \subset \mathcal{M}$. Olkoon $C \in \mathcal{B}_0$. Jos $A \subset G$ ja U on avoin joukko, joka sisältää A:n, niin $U \cap C$ ja $U \setminus C$ ovat erillisiä avoimia joukkoja. Tällöin
$$\mu_1(U) = \mu_1(U \cap C) + \mu_1(U \setminus C) \geq \mu^*(A \cap C) + \mu^*(A \setminus C).$$
Tämä siis pätee kaikilla avoimilla U, jotka sisältävät joukon A. Kun otetaan infimum kaikista avoimista U, jotka sisältävät A:n, saadaan $\mu^*(A) \geq \mu^*(A \cap C) + \mu^*(A \setminus C)$. Päinvastainen epäyhtälö pitää aina paikkansa, sillä μ^* on ulkomitta. Siis $\mu^*(A) = \mu^*(A \cap C) + \mu^*(A \setminus C)$ ja C on mitallinen.

Näytetään nyt, että kaikki avoimet joukot ovat mitallisia. Olkoon U avoin, $A \subset G$ ja $\epsilon > 0$. Koska U on avoin, niin μ_1:n määritelmän nojalla on olemassa $C \in \mathcal{B}_0$, jolle $C \subset U$ ja $\mu_1(C) = \mu_0(C) > \mu_1(U) - \epsilon$. Tällöin joukot C ja $U \setminus C$ ovat erillisiä avoimia joukkoja, joten niille pätee $\mu_1(U) = \mu_1(C) + \mu_1(U \setminus C)$ eli $\mu_1(U \setminus C) < \epsilon$. Nyt joukolle A pätee:
$$\begin{aligned}\mu^*(A) \leq \mu^*(A \cap U) + \mu^*(A \setminus U) &\leq \mu^*(A \cap (U \setminus C)) + \mu^*(A \cap C) + \mu^*(A \setminus C) \\ &< \epsilon + \mu^*(A \cap C) + \mu^*(A \setminus C) = \epsilon + \mu^*(A).\end{aligned}$$
Viimeinen epäyhtälö seuraa siitä, että C on mitallinen. Koska ϵ valittiin mielivaltaisesti, niin $\mu^*(A) = \mu^*(A \cap U) + \mu^*(A \setminus U)$ ja U on mitallinen.

Perhe $\mathcal{M}$ siis sisältää avoimet joukot. Koska $\mathcal{M}$ on σ-algebra, niin se sisältää kaikki Borel-joukot. Nyt $\mu = \mu^*|_{\mathcal{M}}$ on mitta. Konstruktiosta on selvää, että μ on siirtoinvariantti ja että $\mu(G) = 1$. □

Lähteet

[1] Andrew Browder. *Mathematical Analysis: An Introduction.* Springer-Verlag, 1996.

[2] Peter J. Cameron. *Combinatorics: Topics, Techniques, Algorithms.* Cambridge University Press, 1995.

[3] Rachel Camina. Subgroups of the Nottingham group. *Journal of Algebra*, 196(1):101–113, October 1997.

[4] Michael D. Fried and Moshe Jarden. *Field Arithmetic.* Springer-Verlag, 1986.

[5] Ilkka Holopainen. Mitta ja integraali, 2002.

[6] Patrick Morandi. *Field and Galois Theory.* Springer-Verlag, 1996.

[7] Marcus Du Sautoy, Daniel Segal, and Aner Shalev. *New horizons in pro-p groups.* Birkhäuser, 2000.

[8] Kalevi Suominen. Algebra II.

[9] John S. Wilson. *Profinite groups.* Clarendon Press, 1998.