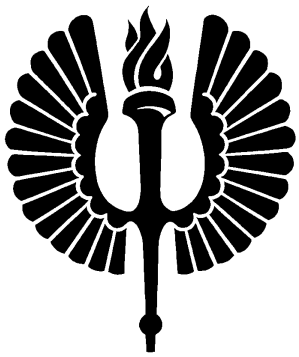

Minimaalidiskriminanttisia jakoalgebroja

Taneli Lehtilä

Pro gradu -tutkielma
Marraskuu 2017

MATEMATIIKAN JA TILASTOTIETEEN LAITOS
TURUN YLIOPISTO

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

LEHTILÄ, TANELI: Minimaalidiskriminanttisia jakoalgebroja
Pro gradu -tutkielma, 47 s.
Matematiikka
Marraskuu 2017

Tässä tutkielmassa konstruoidaan minimaalidiskriminanttisia jakoalgebroja. Jakoalgebroja on mahdollista hyödyntää langattomassa tiedonsiirrossa käytettävien ns. aika-avaruuskoodien tuottamisessa. Syy etsiä mahdollisimman pienen diskriminantin omaavia jakoalgebroja juontuu siitä, että ne johtavat parempiin koodeihin. Tässä työssä jakoalgebrojen konstruointia kuitenkin käsitellään täysin lukuteoreettisena ongelmana.

Työn alussa esitetään myöhemmissä luvuissa tarvittavat algebrallisen lukuteorian perusteet. Tutustutaan muun muassa Frobenius-automorfismin, Tšebotarevin tiheyslauseen ja lukukuntien täydellistymien käsitteisiin. Tämän jälkeen tarkastellaan jakoalgebroihin liittyviä tuloksia ja todistetaan niiden pienimmälle mahdolliselle diskriminantille alaraja käyttäen luokkakuntateoreettisia menetelmiä. Lopuksi esitetään konstruktio $\mathbb{Q}(\sqrt{-7})$-keskeisille minimaalidiskriminanttisille jakoalgebroille.

Asiasanat: algebrallinen lukuteoria, jakoalgebra, diskriminantti, Hasse-invariantti.

Sisältö

1 Johdanto

Useammilla lähetysantenneilla tapahtuvassa langattomassa tiedonsiirrossa käytetään viestien koodaamiseen niin sanottuja aika-avaruuskoodeja. Näitä koodeja on mahdollista tuottaa jakoalgebrojen tietynlaisista alirenkaista, *järjestöistä*. Järjestön *diskriminantilla* voidaan näyttää olevan yhteys koodauksesta saatavan hyödyn kanssa [18]. Yleisesti ottaen aika-avaruuskoodit ovat sitä parempia, mitä pienempi käytetyn järjestön diskriminantti on. Artikkelissa [6] osoitetaan, että erityisen hyviä valintoja järjestöiksi ovat jakoalgebran *maksimaaliset järjestöt*. Maksimaalisen järjestön diskriminanttia kutsutaan tässä tutkielmassa jakoalgebran diskriminantiksi. Optimaalisten aika-avaruuskoodien tuottamiseksi tulee siis konstruoida minimaalidiskriminanttisia jakoalgebroja.

Tässä tutkielmassa käsitellään minimaalidiskriminanttisten jakoalgebrojen konstruointia algebrallisen lukuteorian ongelmana. Asiaan ei siis ollenkaan perehdytä koodausteorian näkökulmasta. Artikkelissa [18] näytetään, että jakoalgebran diskriminantti riippuu algebran keskeisistä lokaaleista ominaisuuksista, *Hasse-invarianteista*. Näiden invarienttien käyttäytyminen puolestaan tunnetaan hyvin luokkakuntateorian antamien tulosten pohjalta, ja niiden avulla jakoalgebran diskriminantille pystytään johtamaan alaraja. Vaikka tämän diskriminanttirajan todistus ei olekaan konstruktiivinen, se kertoo, että rajan saavuttavia jakoalgebroja on olemassa. Se myös kuvaa niitä riittävän hyvin, jotta minimaalisen diskriminantin omaavia jakoalgebroja pystytään konstruoimaan.

Tutkielman alussa esitellään myöhemmin jakoalgebrojen konstruoinnissa tarvittavan algebrallisen lukuteorian perusteet. Luvussa 2 perehdytään esimerkiksi Frobenius-automorfismeihin ja Tšebotarevin tiheyslauseeseen. Jakoalgebrojen *lokalisaatioiden* tarkastelemiseksi esitellään myös lukukuntien täydellistymät.

Luvussa 3 esitetään artikkelia [18] seuraten jakoalgebrojen teoriaa ja todistetaan niiden diskriminanttiraja. Viimeisessä pykälässä 3.3 konstruoidaan minimaalidiskriminanttisia jakoalgebroja, joiden *keskuksena* on kunta $\mathbb{Q}(\sqrt{-7})$. Kuten tullaan näkemään, niin tämä valinta soveltuu konstruktioihimme erityisen hyvin johtuen siitä, että kunnassa $\mathbb{Q}(\sqrt{-7})$ alkuluvun 2 päällä on kaksi pieninormista alkuihannetta.

2 Algebrallisen lukuteorian perusteita

Tässä luvussa esitellään algebralliseen lukuteoriaan liittyviä perusteita niiltä osin, kun niitä tutkielman seuraavassa luvussa tullaan tarvitsemaan. Kaikkia tuloksia ei todisteta, sillä se ei tämän tutkielman laajuudessa olisi mahdollista. Kaikki esitetyt tulokset ovat kuitenkin hyvin tunnettuja, ja niiden todistukset voi löytää monista algebrallisen lukuteorian perusteita käsittelevistä kirjoista, esimerkiksi kirjasta [5].

Lukijan oletetaan tuntevan luentomonisteesta [11] löytyvät Turun yliopiston syventävällä algebran kurssilla käsiteltävät asiat. Erityisesti kuntalaajennuksien ja Galois'n teorian perusteiden tuntemus on välttämätöntä.

Vaikka kaikki tarvittavat algebralliseen lukuteoriaan liittyvät käsitteet esitelläänkin, niin todennäköisesti tämän työn seuraaminen on haastavaa ilman aiempaa tuntemusta aiheesta. Esimerkiksi kirjat [10] ja [12] soveltuvat hyvin alkeiden opiskeluun.

Koko luvussa K ja L ovat aina lukukuntia. Jos ei toisin mainita, niin L on kunnan K äärellinen kuntalaajennus. Kaikki renkaat ovat kommutatiivisia ja sisältävät ykkösalkion.

2.1 Lukukunnat

Tähän pykälään on koottu lukukunnista ja kokonaislukujen renkaista keskeisimpiä asioita

Lukukunnalla K tarkoitetaan kompleksilukujen kunnan $\mathbb{C}$ alikuntaa, jonka aste yli rationaalilukujen kunnan $\mathbb{Q}$ on äärellinen. Tätä astetta merkitään $[K : \mathbb{Q}]$. Alkio $\alpha \in K$ on kunnan K *algebrallinen kokonaisluku*, jos se on jonkin $\mathbb{Z}$-kertoimisen pääpolynomin nollakohta. Kaikkien kunnan K algebrallisten kokonaislukujen joukosta käytetään merkintää $\mathcal{O}_K$. Seuraava lause antaa tietoa joukon $\mathcal{O}_K$ rakenteesta.

Lause 2.1. *Olkoon K lukukunta.*

(i) *$\mathcal{O}_K$ on kunnan $\mathbb{C}$ alirengas ja sen osamääräkunta on K.*

(ii) *$\mathcal{O}_K$ on astetta $[K : \mathbb{Q}]$ oleva vapaa $\mathbb{Z}$-moduli.*

Rengasta $\mathcal{O}_K$ kutsutaan kunnan K *kokonaislukujen renkaaksi.*

Esimerkki 2.2. Olkoon m neliövapaa kokonaisluku, $m \neq 0, 1$. Tällöin voidaan osoittaa, että neliökunnan $\mathbb{Q}(\sqrt{m})$ kokonaislukujen rengas on

$$\mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \begin{cases} \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}, & \text{kun } m \equiv 2, 3 \pmod 4, \\ \mathbb{Z}\left[\dfrac{1+\sqrt{m}}{2}\right] = \left\{a + b\dfrac{1+\sqrt{m}}{2} \mid a, b \in \mathbb{Z}\right\}, & \text{kun } m \equiv 1 \pmod 4. \end{cases}$$

Alkion $\alpha \in \mathcal{O}_K$ generoimaa ihannetta merkitään $[\alpha]$. Kokonaislukujen renkaan $\mathcal{O}_K$ ihannetta $\mathfrak{p}$ kutsutaan *alkuihanteeksi*, jos $\mathfrak{p} \neq \mathcal{O}_K$ ja jokaisella alkiolla $a, b \in \mathcal{O}_K$ pätee

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ tai } b \in \mathfrak{p}.$$

Sanomme myös hieman epätarkasti alkuihannetta $\mathfrak{p}$ kunnan K alkuihanteeksi ja käytämme useasti termiä "alkuihanne" ilmaisun "nollaihanteesta eroava alkuihanne" sijaan. Tunnetusti renkaan $\mathcal{O}_K$ alkuihanteet ovat tarkalleen sen maksimaaliset ihanteet ja jäännösluokkarengas $\mathcal{O}_K/\mathfrak{p}$ on siis kunta. Tämä kunta on myös äärellinen ja sen kertaluku $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ on *ihanteen* $\mathfrak{p}$ *normi*. Ihanteen normi määritellään vastaavasti myös muille ihanteille $\mathfrak{a} \neq [0]$ sivuluokkien lukumääränä $\#(\mathcal{O}_K/\mathfrak{a})$.

Seuraavan lauseen mukaan lukukunnan kokonaislukujen renkaassa $\mathcal{O}$ ihanteilla on yksikäsitteinen tekijöihinjako alkuihanteiden tuloksi eli toisin sanoen $\mathcal{O}$ on *Dedekindin alue*.

Lause 2.3 (**Ihanneteorian päälause**). *Olkoon K lukukunta ja $\mathfrak{a} \neq 0$ renkaan $\mathcal{O}_K$ ihanne. Tällöin $\mathfrak{a}$ voidaan kirjoittaa alkuihanteiden tulona*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n.$$

Hajotelma on järjestystä vaille yksikäsitteinen, ja lisäksi alkuihanteet $\mathfrak{p}_i$, $i = 1, ..., n$, ovat tarkalleen kaikki ihanteen $\mathfrak{a}$ sisältävät alkuihanteet.

Seuraavassa renkaan $\mathcal{O}_K$ nollaihanteesta eroavien ihanteiden muodostama puoliryhmä laajennetaan ryhmäksi.

Määritelmä 2.4. Olkoot $\alpha_1, ..., \alpha_s$ kunnan K alkioita. Niiden generoimaa $\mathcal{O}_K$-modulin K alimodulia

$$\mathfrak{a} = \mathcal{O}_K\alpha_1 + \cdots + \mathcal{O}_K\alpha_s$$

kutsutaan kunnan K *murtoihanteeksi*.

Renkaan $\mathcal{O}_K$ ihanteen käsitteeseen verrattuna tässä on siis se ero, että $\mathcal{O}_K$-moduli $\mathcal{O}_K$ on laajennettu $\mathcal{O}_K$-moduliksi K.

Lause 2.5. *Jokaisella murtoihanteella $\mathfrak{a}$ on kanoninen esitys*

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_t^{k_t},$$

missä ihanteet $\mathfrak{p}_i$ ovat eri alkuihanteita ja $k_i \in \mathbb{Z}\backslash\{0\}$ jokaisella $i \in \{1, ..., t\}$.

Esitellään seuraavaksi ihanteiden haaroittumisen käsite laajennuskunnissa. Oletetaan, että K on lukukunta ja L sen äärellinen laajennus. Jos $\mathfrak{p} \subset \mathcal{O}_K$ on alkuihanne, niin sen *nosto* $\mathfrak{p}\mathcal{O}_L$ renkaalle $\mathcal{O}_L$ on myös ihanne. Näin ollen sillä on alkuihannehajotelma

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, \tag{1}$$

missä ihanteet $\mathfrak{P}_i$, $i = 1, ..., g$, ovat kunnan L eri alkuihanteita, ja ne kaikki sisältävät ihanteen $\mathfrak{p}$. Ihanteiden $\mathfrak{P}_i$ sanotaan olevan ihanteen $\mathfrak{p}$ *päällä* kunnassa L ja vastaavasti $\mathfrak{p}$ on ihanteiden $\mathfrak{P}_i$ *alla*. Eksponentteja e_i kaavassa (1), joita merkitään myös $e_{\mathfrak{P}_i|\mathfrak{p}}$ tai $e(\mathfrak{P}_i|\mathfrak{p})$, kutsutaan alkuihanteen $\mathfrak{p}$ *haaroittumisindekseiksi ihanteissa* $\mathfrak{P}_i$. Jokainen ihanteen $\mathfrak{p}$ sisältävä alkuihanne $\mathfrak{P}_i$ määrittää myös jäännösluokkakuntien laajennuksen $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}_i$. Tämän laajennuksen astetta, josta käytetään merkintää f_i, $f_{\mathfrak{P}_i|\mathfrak{p}}$ tai $f(\mathfrak{P}_i|\mathfrak{p})$, kutsutaan alkuihanteen $\mathfrak{p}$ *jäännösluokka-asteeksi ihanteessa* $\mathfrak{P}_i$. Hajoamislaki kertoo indeksien e_i ja f_i yhteyden.

Lause 2.6 (**Hajoamislaki**). *Olkoon L/K äärellinen kuntalaajennus ja $\mathfrak{p}$ kunnan K alkuihanne. Olkoot kokonaisluvut e_i, f_i ja g määritelty kuten edellä. Tällöin pätee*

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

Jos jokin luvuista e_i on suurempi kuin yksi, niin sanotaan, että $\mathfrak{p}$ *haaroittuu* kunnassa L. Jos $g > 1$, niin sanotaan, että $\mathfrak{p}$ *lohkeaa* kunnassa L. Jos $\mathfrak{p}$ ei haaroitu eikä lohkea, eli $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$ on alkuihanne renkaassa $\mathcal{O}_L$, niin sanotaan, että $\mathfrak{p}$ on *hidas* kunnassa L.

Esimerkki 2.7. Tarkastellaan alkuluvun 2 alkuihannehajotelmaa kunnassa $\mathbb{Q}(\sqrt{-7})$. Merkitään $\mathfrak{p}_1 = \left[2, \frac{1+\sqrt{-7}}{2}\right]$ ja $\mathfrak{p}_2 = \left[2, \frac{1-\sqrt{-7}}{2}\right]$. Tällöin

$$\mathfrak{p}_1\mathfrak{p}_2 = [4, 1+\sqrt{-7}, 1-\sqrt{-7}, 2] = [2].$$

Selvästi $\mathfrak{p}_1 \neq [1]$ ja $\mathfrak{p}_2 \neq [1]$. Jos olisi $\mathfrak{p}_1 = \mathfrak{p}_2$, niin seuraisi ristiriita $1 \in \mathfrak{p}_1$. Alkuluku 2 siis lohkeaa kunnassa $\mathbb{Q}(\sqrt{-7})$ ihanteiden $\mathfrak{p}_1$ ja $\mathfrak{p}_2$ tuloksi. Nämä alkuihanteet osoittautuvat myöhemmin minimaalidiskriminanttisia jakoalgebroja konstruoidessamme tärkeiksi johtuen siitä, että ne ovat kokonaislukujen renkaan $\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}$ ihanteista pieninormisimmat.

On myös helppoa todistaa seuraava lause, jonka mukaan alkuihanteen haaroittumisindeksi ja jäännösluokka-aste ovat multiplikatiivisia päällekkäin olevien laajennusten suhteen.

Lause 2.8. *Olkoon L/K kuntalaajennus ja E sen välikunta, ts. $K \subseteq E \subseteq L$. Olkoon lisäksi $\mathfrak{p}$, $\mathfrak{q}$ ja $\mathfrak{P}$ päällekkäin olevia alkuihanteita vastaavasti kunnissa K, E ja L. Tällöin*

$$e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{q})e(\mathfrak{q}|\mathfrak{p})$$

ja

$$f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{q})f(\mathfrak{q}|\mathfrak{p}).$$

Tarkastellaan seuraavaksi kuntalaajennuksessa L/K kuntaa L vektoriavaruutena yli kunnan K. Alkiolla $\alpha \in L$ kertominen

$$m_\alpha : L \longrightarrow L, \quad x \longmapsto \alpha x \tag{2}$$

on K-lineaarinen kuvaus vektoriavaruudesta L itselleen. Alkion $\alpha \in L$ *jälki* $\mathrm{Tr}_{L/K}(\alpha)$ määritellään tämän lineaarikuvauksen jälkenä. Jos $\sigma_1(\alpha), ..., \sigma_n(\alpha)$ ovat alkion α K-konjugaatit, niin

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{j=1}^{n} \sigma_j(\alpha).$$

Lineaarikuvauksen (2) determinanttia kutsutaan alkion $\alpha \in L$ *normiksi*, ja sitä merkitään $\mathcal{N}_{L/K}(\alpha)$. Normi $\mathcal{N}_{L/K}(\alpha)$ on kunnan K alkio ja jos $\alpha \in \mathcal{O}_L$, niin $\mathcal{N}_{L/K}(\alpha) \in \mathcal{O}_K$. Jos L/K on Galois'n laajennus, niin alkion α normi on sen K-konjugaattien tulo, ts.

$$\mathcal{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

Normikuvaus $\mathcal{N}_{L/K}$ on ryhmähomomorfismi kunnan L multiplikatiivisesta ryhmästä kunnan K multiplikatiiviseen ryhmään, eli

$$\mathcal{N}_{L/K}(\alpha\beta) = \mathcal{N}_{L/K}(\alpha)\mathcal{N}_{L/K}(\beta)$$

jokaisella $\alpha, \beta \in L^*$. Lisäksi, jos $a \in K$, niin

$$\mathcal{N}_{L/K}(a\alpha) = a^{[L:K]}\mathcal{N}_{L/K}(\alpha)$$

jokaisella $\alpha \in L$. Normi myös käyttäytyy hyvin päällekkäisissä kuntalaajennuksissa. Jos $K \subseteq E \subseteq L$ ovat lukukuntia, niin

$$\mathcal{N}_{L/K} = \mathcal{N}_{E/K} \circ \mathcal{N}_{L/E}.$$

Ihanteen $\mathfrak{a}$ normi jakaa luvun $\mathcal{N}_{L/K}(\alpha)$ aina, kun $\alpha \in \mathfrak{a}$. Lisäksi $N(\mathfrak{a}) = |\mathcal{N}_{L/K}(\alpha)|$, jos ja vain jos $\mathfrak{a} = [\alpha]$.

Kunnan L K-*kannan* $\{b_1, ..., b_n\}$ *diskriminantti* määritellään

$$d(b_1, ..., b_n) = \det[\mathrm{Tr}_{L/K}(b_i b_j)] = \det[\sigma_i(b_j)]^2,$$

missä $\sigma_1, ..., \sigma_n : L \hookrightarrow \mathbb{C}$ ovat injektiiviset K-homomorfismit.

Määritelmä 2.9. Lukukunnan K kokonaislukujen renkaan $\mathcal{O}_K$ $\mathbb{Z}$-modulikantaa kutsutaan kunnan K *kokonaiskannaksi*. Tämän kannan diskriminanttia kutsutaan *kunnan K diskriminantiksi* ja siitä käytetään merkintää d_K.

Esimerkki 2.10. Neliökunnan $\mathbb{Q}(\sqrt{m})$ kokonaiskanta saadaan suoraan esimerkistä 2.2. Kun $m \equiv 2, 3 \pmod 4$, niin $\{1, \sqrt{m}\}$ on kokonaiskanta. Kun $m \equiv 1 \pmod 4$, niin kokonaiskannaksi kelpaa $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$. Tämän jälkeen kunnan diskriminantti lasketaan esimerkiksi seuraavasti:

$$d(1, \sqrt{m}) = \begin{vmatrix} 1 & 1 \\ \sqrt{m} & -\sqrt{m} \end{vmatrix}^2 = 4m, \quad d(1, \frac{1+\sqrt{m}}{2}) = \begin{vmatrix} 1 & 1 \\ \frac{1+\sqrt{m}}{2} & \frac{1-\sqrt{m}}{2} \end{vmatrix}^2 = m.$$

Määritelmä 2.11. *Laajennuksen L/K diskriminantti* on kokonaislukujen renkaan $\mathcal{O}_K$ ihanne, joka on joukon

$$\{\det(\mathrm{Tr}_{L/K}(x_i x_j))_{i,j=1}^n \mid (x_1, ..., x_n) \in \mathcal{O}_L^n \text{ on laajennuksen } L/K \text{ kanta}\}$$

generoima. Sitä merkitään $d(L/K)$ tai $d(\mathcal{O}_L/\mathcal{O}_K)$.

Kunnan K diskriminantti on rationaalinen kokonaisluku, joka generoi pääihanteen $d(K/\mathbb{Q})$. Päällekkäisten laajennusten $L/E/K$ tilanteessa laajennusten diskriminanteille on voimassa

$$d(L/K) = \mathcal{N}_{E/K}(d(L/E))d(E/K)^{[L:E]}.$$

Yksi syy sille, miksi diskriminantit tulevat olemaan meille hyödyllisiä, on se, että ne antavat tietoa laajennuksessa haaroittuvista alkuihanteista.

Lause 2.12. *Lukukunnan K alkuihanne $\mathfrak{p}$ haaroittuu laajennuskunnassa L, jos ja vain jos $\mathfrak{p}$ jakaa laajennuksen L/K diskriminantin.*

Erityisesti siis lukukuntien laajennuksessa haaroittuu vain äärellinen määrä alkuihanteita.

Siirrytään seuraavaksi tarkastelemaan Galois'n laajennuksia. Olkoon nyt L/K Galois'n laajennus ja merkitään sen Galois'n ryhmää $G(L/K)$.

Jokaisen ryhmän $G(L/K)$ alkion σ restriktio renkaaseen $\mathcal{O}_L$ on renkaan $\mathcal{O}_L$ automorfismi. Nimittäin $\sigma(\mathcal{O}_L) = \mathcal{O}_L$, sillä tietenkin $\sigma(\mathcal{O}_L) \subseteq \mathcal{O}_L$ ja toisaalta $\mathcal{O}_L = \sigma(\sigma^{-1}(\mathcal{O}_L)) \subseteq \sigma(\mathcal{O}_L)$. Olkoon seuraavassa $\mathfrak{a}$ kunnan L ihanne, ja määritellään $\sigma(\mathfrak{a}) = \{\sigma(\alpha) \mid \alpha \in \mathfrak{a}\}$. Jos $\alpha \in \mathfrak{a}$ ja $\gamma \in \mathcal{O}_L$, niin voidaan kirjoittaa $\gamma\sigma(\alpha) = \sigma(\sigma^{-1}(\gamma)\alpha)$. Tämän avulla nähdään, että $\sigma(\mathfrak{a})$ on renkaan $\mathcal{O}_L$ ihanne. Sitä kutsutaan ihanteen $\mathfrak{a}$ *liittoihanteeksi*.

Renkaan $\mathcal{O}_L$ alkuihanteen $\mathfrak{P}$ liittoihanteetkin ovat renkaan $\mathcal{O}_L$ alkuihanteita. Nimittäin, jos $\alpha\beta \in \sigma(\mathfrak{P})$, niin

$$\sigma^{-1}(\alpha)\sigma^{-1}(\beta) = \sigma^{-1}(\alpha\beta) \in \mathfrak{P}.$$

Saadaan, että esimerkiksi $\sigma^{-1}(\alpha) \in \mathfrak{P}$, joten $\alpha \in \sigma(\mathfrak{P})$. Koska myös $1 \notin \sigma(\mathfrak{P})$, niin $\sigma(\mathfrak{P}) \neq \mathcal{O}_L$.

Kun $\mathfrak{a}$ on renkaan $\mathcal{O}_L$ ihanne, niin jokainen $\sigma \in G(L/K)$ indusoi kuvauksen

$$\overline{\sigma} : \mathcal{O}_L/\mathfrak{a} \longrightarrow \mathcal{O}_L/\sigma(\mathfrak{a}), \quad \overline{\sigma}(\alpha + \mathfrak{a}) = \sigma(\alpha) + \sigma(\mathfrak{a}) \tag{3}$$

kaikilla $\alpha \in \mathcal{O}_L$. Tämä kuvaus on hyvinmääritelty, sillä jos $\alpha_1 + \mathfrak{a} = \alpha_2 + \mathfrak{a}$, niin $\sigma(\alpha_1) - \sigma(\alpha_2) = \sigma(\alpha_1 - \alpha_2) \in \sigma(\mathfrak{a})$. Yhtä suoraviivaisesti kuvauksen $\overline{\sigma}$ voidaan myös todeta olevan rengasisomorfismi. Erityisesti siis saadaan $\mathcal{O}_L/\mathfrak{a} \cong \mathcal{O}_L/\sigma(\mathfrak{a})$.

Lemma 2.13. *Olkoot $\mathfrak{p}_1, ..., \mathfrak{p}_r$ lukukunnan K pareittain erisuuria alkuihanteita. On olemassa sellainen alkio $x \in \mathcal{O}_K$, että $x \in \mathfrak{p}_1$ ja $x \notin \mathfrak{p}_i$, kun $i = 2, ..., r$.*

Todistus. Merkitään $\mathfrak{p} = \mathfrak{p}_1$ ja $\mathfrak{q}_i = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_r$ $(i = 1, ..., r)$. Koska $\mathfrak{q}_i\mathfrak{p}_i \subset \mathfrak{q}_i$, niin voidaan valita $x_i \in \mathfrak{q}_i \backslash \mathfrak{q}_i\mathfrak{p}_i$ $(i = 1, ..., r)$. Merkitään $x = x_1 + ... + x_r$. Koska $x_i \in \mathfrak{q}_i \subseteq \mathfrak{p}$ jokaisella indeksillä i, niin $x \in \mathfrak{p}$.

Oletetaan $x \in \mathfrak{p}_2$. Koska $x_i \in \mathfrak{q}_i \subseteq \mathfrak{p}^2$, kun $i \geq 2$, niin $x_1 \in \mathfrak{p}^2 \subseteq \mathfrak{q}_1\mathfrak{p}$, mikä on ristiriita. Siis $x \notin \mathfrak{p}_2$ ja vastaavasti saadaan $x \notin \mathfrak{p}_j$ $(j = 3, ..., r)$. □

Seuraavan lauseen mukaan $G(L/K)$ operoi transitiivisesti sellaisten renkaan $\mathcal{O}_L$ alkuihanteiden joukossa, joiden alla on sama alkuihanne renkaassa $\mathcal{O}_K$. Lauseiden 2.14 ja 2.15 todistukset ovat kirjasta [16].

Lause 2.14. *Olkoot $\mathfrak{P}$ ja $\mathfrak{P}'$ sellaisia renkaan $\mathcal{O}_L$ alkuihanteita, joille on voimassa $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{P}' \cap \mathcal{O}_K \neq [0]$. Tällöin on olemassa alkio $\sigma \in G(L/K)$, jolle pätee $\sigma(\mathfrak{P}) = \mathfrak{P}'$.*

Todistus. Olkoon $G(L/K) = \{\sigma_1, ..., \sigma_n\}$ laajennuksen L/K Galois'n ryhmä. Oletetaan, että $\mathfrak{P}' \neq \sigma_i(\mathfrak{P})$ jokaisella $i = 1, ..., n$. Lemman 2.13 mukaan on olemassa alkio $x \in \mathcal{O}_L$, jolle on voimassa $x \in \mathfrak{P}'$ ja $x \notin \sigma_i(\mathfrak{P})$ jokaisella $i = 1, ..., n$. Olkoon

$$\alpha = \prod_{i=1}^{n} \sigma_i(x).$$

Tällöin $\alpha \in \mathcal{O}_K$ ja koska $id(x) \in \mathfrak{P}'$, niin myös $\alpha \in \mathfrak{P}'$. Jos olisi $\sigma_i(x) \in \mathfrak{P}$ jollakin $i = 1, ..., n$, niin seuraisi $x = \sigma_i^{-1}\sigma_i(x) \in \sigma_i^{-1}(\mathfrak{P})$, mikä ei ole

mahdollista. Siitä seuraisi, että $\sigma_i(x) \notin \mathfrak{P}$ jokaisella $i = 1, ..., n$. Näin ollen $\alpha \notin \mathfrak{P}$. Tämä on ristiriita, joten on olemassa alkio $\sigma_i \in G(L/K)$, jolle pätee $\sigma_i(\mathfrak{P}) = \mathfrak{P}'$. □

Galois'n laajennusten tapauksessa hajoamislain 2.6 voi ilmaista yksinkertaisemmassa muodossa.

Lause 2.15. *Olkoon L/K Galois'n laajennus ja $\mathfrak{p}$ kunnan K alkuihanne. Olkoot $\mathfrak{P}_1, ..., \mathfrak{P}_g$ ne kunnan L alkuihanteet, jotka ovat ihanteen $\mathfrak{p}$ päällä. Tällöin jokaisella alkuihanteella $\mathfrak{P}_i$ on sama haaroittumisindeksi $e = e_{\mathfrak{P}_i|\mathfrak{p}}$ ja sama jäännösluokka-aste $f = f_{\mathfrak{P}_i|\mathfrak{p}}$, ja lisäksi on voimassa*

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

Todistus. Olkoon $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$. Lauseen 2.14 mukaan jokaisella indeksillä $j = 1, ..., g$ on olemassa sellainen kuvaus $\sigma \in G(L/K)$, jolle pätee $\sigma(\mathfrak{P}_1) = \mathfrak{P}_j$. Yhtälöstä $\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L) = \prod_{i=1}^{g} \sigma(\mathfrak{P}_i)^{e_i}$ ja alkuihannehajotelman yksikäsitteisyydestä seuraa, että $e_j = e_1$ jokaisella $j = 1, ..., g$. Yhtälöstä $\mathcal{O}_L/\sigma(\mathfrak{P}_j) = \mathcal{O}_L/\sigma(\mathfrak{P}_1) \cong \mathcal{O}_L/\mathfrak{P}_1$ puolestaan seuraa, että $f_{\mathfrak{P}_j|\mathfrak{p}} = f_{\mathfrak{P}_1|\mathfrak{p}}$ jokaisella $j = 1, ..., g$. Kaava $efg = [L : K]$ seuraa nyt suoraan hajoamislaista 2.6. □

Galois'n laajennuksen L/K tapauksessa kunnan K alkuihanne $\mathfrak{p}$ haaroittuu, jos $e > 1$, ja on haaroittumaton, jos $e = 1$. Alkuihanne $\mathfrak{p}$ on *täysin haaroittunut* kunnassa L tai laajennuksessa L/K, jos haaroittumisindeksi e on yhtä suuri kuin laajennuksen aste $[L : K]$. Jos $e = f = 1$, eli $\mathfrak{p}\mathcal{O}_L$ on $[L : K]$ eri alkuihanteen tulo, niin ihanteen $\mathfrak{p}$ sanotaan *lohkeavan täysin.*

2.2 Lohkeamisryhmä

Tässä pykälässä esitellään myöhemmin käyttöön tuleva lohkeamisryhmän käsite ja todistetaan siihen liittyviä tuloksia.

Kuten edellisen luvun lopussakin L/K on nyt Galois'n laajennus ja sen Galois'n ryhmää merkitään joko $\mathrm{Gal}(L/K)$ tai $G(L/K)$. Merkinnällä $\mathfrak{p}$ tarkoitetaan renkaan $\mathcal{O}_K$ alkuihannetta, ja sen päällä renkaassa $\mathcal{O}_L$ on alkuihanne $\mathfrak{P}$.

Pykälän todistukset ovat kirjoista [10] ja [16].

Määritelmä 2.16. Renkaan $\mathcal{O}_L$ alkuihanteen $\mathfrak{P}$ *lohkeamisryhmä* on joukko

$$\mathcal{Z}_{\mathfrak{P}}(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Hyvin suoraviivaisesti voidaan osoittaa, että lohkeamisryhmä $\mathcal{Z}_{\mathfrak{P}}(L/K)$ todella on ryhmän $\mathrm{Gal}(L/K)$ aliryhmä. Galois'n vastaavuuden määräämää ryhmän $\mathcal{Z}_{\mathfrak{P}}(L/K)$ kiintokuntaa laajennuksessa L/K merkitään $Z_{\mathfrak{P}}(L/K)$ ja sitä kutsutaan *lohkeamiskunnaksi*.

Lohkeamisryhmälle käytetään myös lyhyempää merkintää $\mathcal{Z}_{\mathfrak{P}}$, jos on ilmeistä, mihin laajennukseen viitataan. Vastaavasti käytetään lyhennystä $Z_{\mathfrak{P}} = Z_{\mathfrak{P}}(L/K)$.

Lemma 2.17. *Oletetaan, että alkuihanteen $\mathfrak{p}$ päällä kunnassa L on g eri alkuihannetta, ja olkoon $\mathfrak{P}$ yksi niistä. Tällöin*

$$[Z_{\mathfrak{P}} : K] = (Gal(L/K) : \mathcal{Z}_{\mathfrak{P}}) = g.$$

Todistus. Olkoot $\sigma, \tau \in G(L/K)$. Näytetään, että $\sigma\mathcal{Z}_{\mathfrak{P}} = \tau\mathcal{Z}_{\mathfrak{P}}$, jos ja vain jos $\sigma(\mathfrak{P}) = \tau(\mathfrak{P})$. Jos $\sigma\mathcal{Z}_{\mathfrak{P}} = \tau\mathcal{Z}_{\mathfrak{P}}$, niin $\sigma^{-1}\tau \in \mathcal{Z}_{\mathfrak{P}}$. Lohkeamisryhmän määritelmän mukaan nyt $\sigma^{-1}\tau(\mathfrak{P}) = \mathfrak{P}$, ja siis $\tau(\mathfrak{P}) = \sigma(\mathfrak{P})$. Kääntäen, jos $\sigma(\mathfrak{P}) = \tau(\mathfrak{P})$, niin $\sigma^{-1}\tau \in \mathcal{Z}_{\mathfrak{P}}$ ja edelleen $\tau\mathcal{Z}_{\mathfrak{P}} = \sigma\mathcal{Z}_{\mathfrak{P}}$.

Koska $G(L/K)$ operoi transitiivisesti alkuihanteen $\mathfrak{p}$ päällä kunnassa L olevien alkuihanteiden joukossa, niin nähdään, että g on yhtä suuri kuin sivuluokkien modulo $\mathcal{Z}_{\mathfrak{P}}$ lukumäärä, ts. $g = (\mathrm{Gal}(L/K) : \mathcal{Z}_{\mathfrak{P}})$. Galois'n vastaavuuden perusteella $(\mathrm{Gal}(L/K) : \mathcal{Z}_{\mathfrak{P}}) = [Z_{\mathfrak{P}} : K]$. □

Lemma 2.18. *Jos $\mathfrak{q} = \mathfrak{P} \cap Z_{\mathfrak{P}}$, niin $\mathfrak{P}$ on ainut alkuihanteen $\mathfrak{q}$ päällä kunnassa L oleva alkuihanne.*

Todistus. Koska $\mathcal{Z}_{\mathfrak{P}} = \mathrm{Gal}(L/Z_{\mathfrak{P}})$, niin $\mathcal{Z}_{\mathfrak{P}}$ operoi transitiivisesti alkuihanteen $\mathfrak{q}$ päällä kunnassa L olevien alkuihanteiden joukossa. Määritelmän mukaan jokaisella $\sigma \in \mathcal{Z}_{\mathfrak{P}}$ pätee $\sigma(\mathfrak{P}) = \mathfrak{P}$, joten $\mathfrak{P}$ on ainut alkuihanne ihanteen $\mathfrak{q}$ päällä. □

Käytetään edellisen lemman tapaan merkintää $\mathfrak{q} = \mathfrak{P} \cap Z_{\mathfrak{P}}$ alkuihanteen $\mathfrak{P}$ alla sen lohkeamiskunnassa olevasta alkuihanteesta. Merkitään lisäksi $F_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$, $F_{\mathfrak{q}} = \mathcal{O}_Z/\mathfrak{q}$ ja $F_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$. Olkoon e alkuihanteen $\mathfrak{P}$ haaroittumisindeksi yli ihanteen $\mathfrak{p}$, f alkuihanteen $\mathfrak{P}$ jäännösluokka-aste yli ihanteen $\mathfrak{p}$ ja g alkuihanteen $\mathfrak{P}$ liittoihanteiden lukumäärä laajennuksessa L/K.

Lemma 2.19. *Yllä olevin merkinnöin $F_{\mathfrak{p}} = F_{\mathfrak{q}}$.*

Todistus. Hajoamislain 2.6 ja lemman 2.18 perusteella

$$[L : Z_{\mathfrak{P}}] = e_{\mathfrak{P}|\mathfrak{q}} \cdot f_{\mathfrak{P}|\mathfrak{q}}.$$

Koska $[L:K] = efg$ ja lemman 2.17 mukaan $[Z_\mathfrak{P}:K] = g$, niin nähdään, että $\mathfrak{p}$ lohkeaa täysin laajennuksessa $Z_\mathfrak{P}/K$. Siis $f_{\mathfrak{q}|\mathfrak{p}} = 1$. Tästä seuraa

$$[F_\mathfrak{P}:F_\mathfrak{q}] = f_{\mathfrak{P}|\mathfrak{q}} = f = [F_\mathfrak{P}:F_\mathfrak{p}],$$

joten $F_\mathfrak{q} = F_\mathfrak{p}$. □

Kun x on renkaan $\mathcal{O}_L$ alkio, niin merkitään symbolilla $\overline{x}$ sen kuvaa luonnollisessa homomorfismissa $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}$. Kuten jo kaavan (3) yhteydessä todettiin, alkio $\sigma \in \mathcal{Z}_\mathfrak{P}$ indusoi isomorfismin

$$\overline{\sigma} : F_\mathfrak{P} \longrightarrow F_\mathfrak{P},$$

missä $\overline{\sigma}(\overline{x}) = \overline{\sigma(x)}$ jokaisella $x \in \mathcal{O}_L$. Tämä on lisäksi myös kunnan $F_\mathfrak{P}$ $F_\mathfrak{p}$-automorfismi. Nimittäin, jos $x \in \mathcal{O}_K$, niin $\overline{\sigma}(\overline{x}) = \overline{\sigma(x)} = \overline{x}$, eli kuvauksen $\overline{\sigma}$ restriktio kunnalle $F_\mathfrak{p}$ on identiteettikuvaus. Nyt lemman 2.19 perusteella $\overline{\sigma} \in \mathrm{Gal}(F_\mathfrak{P}/F_\mathfrak{q})$. Tarvitsemme tätä tietoa, jotta seuraavan lauseen kuvaus olisi hyvinmääritelty.

Lause 2.20. *Kuvaus $f : \mathcal{Z}_\mathfrak{P} \to Gal(F_\mathfrak{P}/F_\mathfrak{p})$, joka kuvaa alkion σ alkioksi $\overline{\sigma}$, on surjektiivinen ryhmähomomorfismi, jonka ydin on*

$$\mathcal{I}_\mathfrak{P} = \{\sigma \in \mathcal{Z}_\mathfrak{P} \mid \sigma(x) \equiv x \ (mod\ \mathfrak{P})\ jokaisella\ x \in \mathcal{O}_L\}.$$

Todistus. Ensinnäkin f on ryhmähomomorfismi, sillä kun $\sigma_1, \sigma_2 \in \mathcal{Z}_\mathfrak{P}$ ja $x \in \mathcal{O}_L$, niin

$$\begin{aligned} f(\sigma_1 \circ \sigma_2)(\overline{x}) &= \overline{(\sigma_1 \circ \sigma_2)}(\overline{x}) = \overline{\sigma_1(\sigma_2(x))} = \overline{\sigma_1}(\overline{\sigma_2(x)}) \\ &= (\overline{\sigma_1} \circ \overline{\sigma_2})(\overline{x}) = (f(\sigma_1) \circ f(\sigma_2))(\overline{x}). \end{aligned}$$

Osoitetaan, että kuvauksen f arvojoukko on koko $\mathrm{Gal}(F_\mathfrak{P}/F_\mathfrak{p})$. Koska $F_\mathfrak{p}$ on äärellinen kunta, niin on olemassa sellainen alkio $\alpha \in \mathcal{O}_L$, että $F_\mathfrak{P} = F_\mathfrak{p}(\overline{\alpha})$. Jos $\xi \in \mathrm{Gal}(F_\mathfrak{P}/F_\mathfrak{p})$, niin $\xi(\overline{\alpha})$ on alkion $\overline{\alpha}$ konjugaatti yli kunnan $F_\mathfrak{p}$.

Olkoon $h(X)$ alkion α minimaalipolynomi yli ihanteen $\mathfrak{P}$ lohkeamiskunnan $Z_\mathfrak{P}$. Koska $L/Z_\mathfrak{P}$ on Galois'n laajennus ja $\alpha \in \mathcal{O}_L$, niin jokainen alkion α $Z_\mathfrak{P}$-konjugaatti kuuluu myös renkaaseen $\mathcal{O}_L$. Tällöin siis $h = \prod_{\sigma \in \mathcal{Z}} (X - \sigma(\alpha))$. Kun tarkastellaan polynomin h kertoimia luonnollisessa homomorfismissa $\mathcal{O}_Z \to F_\mathfrak{q}$, niin nähdään, että polynomi $\prod_{\sigma \in \mathcal{Z}} (X - \overline{\sigma(\alpha)}) \in F_\mathfrak{p}[X]$. Merkitään tätä polynomia symbolilla $\overline{h}$. Koska $\overline{\alpha}$ on yksi polynomin $\overline{h}$ juurista, niin alkion $\overline{\alpha}$ minimaalipolynomi yli kunnan $F_\mathfrak{p}$ jakaa polynomin $\overline{h}$. Tämän vuoksi alkion $\overline{\alpha}$ $F_\mathfrak{p}$-konjugaatit ovat alkioiden $\overline{\sigma(\alpha)} \in F_\mathfrak{P}$ joukossa. Tällöin

siis $\xi(\overline{\alpha}) = \overline{\sigma(\alpha)} = \overline{\sigma}(\overline{\alpha})$ jollakin $\sigma \in \mathcal{Z}_\mathfrak{P}$, ja siksi kuvauksien ξ ja $\overline{\sigma}$ täytyy olla samat.

Kuvauksen f ydin on selvästi niiden alkioiden $\sigma \in \mathcal{Z}_\mathfrak{P}$ joukko, joille pätee $\overline{\sigma}(\overline{x}) = \overline{x}$ jokaisella $\overline{x} \in F_\mathfrak{P}$, eli toisin sanoen $\sigma(x) \equiv x \pmod{\mathfrak{P}}$ jokaisella $x \in \mathcal{O}_L$. □

Käytetään ryhmän $\mathcal{I}_\mathfrak{P}$ kiintokunnasta merkintää $I_\mathfrak{P}$. Lauseen 2.20 perusteella $\mathcal{Z}_\mathfrak{P}/\mathcal{I}_\mathfrak{P} \cong \mathrm{Gal}(F_\mathfrak{P}/F_\mathfrak{p})$ jokaisella alkuihanteella $\mathfrak{P}$. Tätä isomorfiaa hyödyntämällä nähdään, että

$$[I_\mathfrak{P} : Z_\mathfrak{P}] = \#(\mathcal{Z}_\mathfrak{P}/\mathcal{I}_\mathfrak{P}) = \#(\mathrm{Gal}(F_\mathfrak{P}/F_\mathfrak{p})) = [F_\mathfrak{P} : F_\mathfrak{p}] = f.$$

Koska $[L : K] = efg$, $[I_\mathfrak{P} : Z_\mathfrak{P}] = f$ ja lemman 2.17 mukaan $[Z_\mathfrak{P} : K] = g$, niin $[L : I_\mathfrak{P}] = e$. Näin ollen

$$\#\mathcal{I}_\mathfrak{P} = e_{\mathfrak{P}|\mathfrak{p}}. \tag{4}$$

Tarkastellaan kuntatornia $K \subseteq E \subseteq L$. Merkitään yhä alkuihanteen $\mathfrak{P}$ alla lohkeamiskunnassa $Z_\mathfrak{P}(L/K)$ olevaa alkuihannetta $\mathfrak{q} = \mathfrak{P} \cap Z_\mathfrak{P}(L/K)$ ja merkitään lisäksi $\mathfrak{q}' = \mathfrak{P} \cap E$.

Lemma 2.21. *Sisältyminen $E \subseteq Z_\mathfrak{P}(L/K)$ on voimassa, jos ja vain jos $e(\mathfrak{q}'|\mathfrak{p}) = f(\mathfrak{q}'|\mathfrak{p}) = 1$.*

Todistus. Oletetaan ensin $E \subseteq Z_\mathfrak{P}(L/K)$. Lauseen 2.19 todistuksessa jo nähtiin, että $\mathfrak{p}$ lohkeaa täysin laajennuksessa $Z_\mathfrak{P}(L/K)/K$, joten $e(\mathfrak{q}|\mathfrak{p}) = f(\mathfrak{q}|\mathfrak{p}) = 1$. Koska haaroittumisindeksi ja jäännösluokka-aste ovat multiplikatiivisia kuntatornissa $K \subseteq E \subseteq Z_\mathfrak{P}(L/K)$, niin $e(\mathfrak{q}'|\mathfrak{p}) = f(\mathfrak{q}'|\mathfrak{p}) = 1$.

Oletetaan nyt $e(\mathfrak{q}'|\mathfrak{p}) = f(\mathfrak{q}'|\mathfrak{p}) = 1$. Olkoon H se ryhmän $\mathrm{G}(L/K)$ aliryhmä, jonka kiintokunta on E. Lohkeamisryhmän määritelmästä nähdään, että $\mathcal{Z}_\mathfrak{P}(L/E) = \mathcal{Z}_\mathfrak{P}(L/K) \cap H$. Galois'n teoriasta tiedetään, että lohkeamiskunta $Z_\mathfrak{P}(L/E) = Z_\mathfrak{P}(L/K)E$. Käyttäen oletusta, yhtälöitä $e(\mathfrak{q}|\mathfrak{p}) = f(\mathfrak{q}|\mathfrak{p}) = 1$ sekä multiplikatiivisuutta kuntatorneissa saadaan

$$[L : Z_\mathfrak{P}(L/K)] = e(\mathfrak{P}|\mathfrak{q})f(\mathfrak{P}|\mathfrak{q}) = e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{q}')f(\mathfrak{P}|\mathfrak{q}').$$

Koska lisäksi $\mathfrak{q}'$ lohkeaa täysin lohkeamiskunnassa $Z_\mathfrak{P}(L/E) = Z_\mathfrak{P}(L/K)E$, niin $[L : Z_\mathfrak{P}(L/K)] = [L : Z_\mathfrak{P}(L/K)E]$. Tällöin siis $Z_\mathfrak{P}(L/K) = Z_\mathfrak{P}(L/K)E$ ja edelleen $E \subseteq Z_\mathfrak{P}(L/K)$.

□

Seuraavaa lausetta tulemme tarvitsemaan myöhemmin luvussa 3.3.

Lause 2.22. *Olkoot F_1/K ja F_2/K Galois'n laajennuksia, $F_1 \cap F_2 = K$. Jos kunnan K alkuihanne $\mathfrak{p}$ lohkeaa täysin molemmissa kunnissa F_1 ja F_2, niin se lohkeaa täysin myös kunnassa $L = F_1F_2$.*

Todistus. Olkoon $\mathfrak{q}_1 = \mathfrak{P} \cap F_1$ ja $\mathfrak{q}_2 = \mathfrak{P} \cap F_2$. Koska F_1/K ja F_2/K ovat Galois'n laajennuksia, niin myös L/K on Galois. Oletuksen mukaan $e(\mathfrak{q}_i|\mathfrak{p}) = f(\mathfrak{q}_i|\mathfrak{p}) = 1$, $i \in \{1, 2\}$, joten nyt lemman 2.21 perusteella $F_1, F_2 \subseteq Z_{\mathfrak{P}}(L/K)$. Tällöin $L = F_1F_2 \subseteq Z_{\mathfrak{P}}(L/K)$. Lemman 2.21 mukaan alkuihanteen $\mathfrak{P}$ jäännösluokka-asteen ja haaroittumisindeksin yli kunnan K täytyy olla yksi, eli $\mathfrak{p}$ lohkeaa täysin kunnassa L. □

2.3 Frobenius-automorfismi

Esitellään seuraavaksi Frobenius-automorfismin käsite. Frobenius-automorfismiin liittyvien tuloksien todistukset ovat peräisin kirjoista [3] ja [13].

Edelleen L/K on kuntalaajennus, $\mathfrak{p}$ on renkaan $\mathcal{O}_K$ alkuihanne ja sen päällä renkaassa $\mathcal{O}_L$ on alkuihanne $\mathfrak{P}$.

Lause 2.23. *Olkoon L/K Galois'n laajennus ja $\mathfrak{p}$ renkaan $\mathcal{O}_K$ alkuihanne, joka on haaroittumaton kunnassa L. Jos renkaan $\mathcal{O}_L$ alkuihanne $\mathfrak{P}$ sisältää ihanteen $\mathfrak{p}$, niin on olemassa yksikäsitteinen sellainen alkio $\sigma \in Gal(L/K)$, jolle on voimassa*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \ (mod\ \mathfrak{P})$$

jokaisella alkiolla $\alpha \in \mathcal{O}_L$.

Todistus. Koska $\mathfrak{p}$ on haaroittumaton kunnassa L, niin kaavasta (4) nähdään, että $\#\mathcal{I}_{\mathfrak{P}} = e_{\mathfrak{P}|\mathfrak{p}} = 1$. Nyt lauseen 2.20 perusteella lohkeamisryhmän alkion $\sigma \in \mathcal{Z}_{\mathfrak{P}}$ indusoima kuvaus $f : \sigma \to \overline{\sigma}$ määrittelee isomorfismin

$$\mathcal{Z}_{\mathfrak{P}} \xrightarrow{\sim} \mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}}).$$

Galois'n ryhmän $\mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}})$ rakenne tunnetaan hyvin. Jos kunnassa $\mathcal{O}_K/\mathfrak{p}$ on $q = N(\mathfrak{p})$ alkiota, niin $\mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}})$ on syklinen ryhmä, jonka generoi automorfismi $x \mapsto x^q$ (ks. esim. [11]). On siis olemassa yksikäsitteinen alkio $\sigma \in \mathcal{Z}_{\mathfrak{P}}$, jonka f kuvaa kuvaukseksi $x \mapsto x^q$. Kuvaus σ toteuttaa vaaditun ehdon

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \ (\mathrm{mod}\ \mathfrak{P})$$

jokaisella $\alpha \in \mathcal{O}_L$. Yksikäsitteisyys on selvää, koska jokaisen automorfismin σ, joka toteuttaa kyseisen ehdon, täytyy kuulua lohkeamisryhmään $\mathcal{Z}_{\mathfrak{P}}$. □

Lauseen 2.23 yksikäsitteistä alkiota σ kutsutaan *Frobenius-automorfismiksi* ja sitä merkitään $((L/K)/\mathfrak{P})$, sillä se riippuu kunnan L alkuihanteesta $\mathfrak{P}$. Sen keskeinen ominaisuus on, että jokaisella $\alpha \in \mathcal{O}_L$

$$\left(\frac{L/K}{\mathfrak{P}}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}}, \tag{5}$$

missä $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Tarkastellaan myös muita myöhemmin käyttöön tulevia Frobenius-automorfismin ominaisuuksia.

Lause 2.24. *Olkoon L/K Galois'n laajennus ja $\mathfrak{p}$ kunnan K alkuihanne, joka on haaroittumaton kunnassa L. Olkoon $\mathfrak{P}$ ihanteen $\mathfrak{p}$ päällä kunnassa L oleva alkuihanne. Tällöin*

(i) $\left(\frac{L/K}{\tau(\mathfrak{P})}\right) = \tau \circ \left(\frac{L/K}{\mathfrak{P}}\right) \circ \tau^{-1}$ *jokaisella* $\tau \in Gal(L/K)$.

(ii) *Alkion $((L/K)/\mathfrak{P})$ kertaluku on jäännösluokka-aste $f = f_{\mathfrak{P}|\mathfrak{p}}$.*

Todistus. (i) Jokainen renkaan $\mathcal{O}_L$ alkio voidaan kirjoittaa muodossa $\tau^{-1}(\alpha)$, missä $\alpha \in \mathcal{O}_L$ ja τ on Galois'n ryhmän $\mathrm{Gal}(L/K)$ alkio. Ominaisuuden (5) perusteella

$$\left(\frac{L/K}{\mathfrak{P}}\right) \circ \tau^{-1}(\alpha) \equiv \tau^{-1}(\alpha)^{N(\mathfrak{p})} \pmod{\mathfrak{P}}.$$

Kuvaamalla alkiolla τ saadaan

$$\tau \circ \left(\frac{L/K}{\mathfrak{P}}\right) \circ \tau^{-1}(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\tau(\mathfrak{P})}.$$

Nyt väite seuraa Frobenius-automorfismin yksikäsitteisyydestä.

(ii) Lauseen 2.23 todistuksessa nähtiin, että lohkeamisryhmä $\mathcal{Z}_{\mathfrak{P}}(L/K)$ on isomorfinen laajennuksen $F_{\mathfrak{P}}/F_{\mathfrak{p}}$ Galois'n ryhmän kanssa. Frobenius-automorfismi kuvautuu tässä isomorfismissa ryhmän $\mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}})$ generoijaksi. Koska laajennuksen $F_{\mathfrak{P}}/F_{\mathfrak{p}}$ aste on jäännösluokka-aste f, niin nähdään, että Frobenius-automorfismin $((L/K)/\mathfrak{P})$ kertaluku on f. □

Määritelmä 2.25. Olkoon L/K Galois'n laajennus. Jos sen Galois'n ryhmä on Abelin ryhmä, niin laajennusta L/K kutsutaan *Abelin laajennukseksi.* Lisäksi, jos Galois'n ryhmä $\mathrm{Gal}(L/K)$ on syklinen, niin laajennusta L/K kutsutaan *sykliseksi laajennukseksi.*

Abelin laajennuksen L/K tapauksessa Frobenius-automorfismi $((L/K)/\mathfrak{P})$ riippuu vain alla olevasta alkuihanteesta $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Nimittäin, jos $\mathfrak{P}'$ on toinen ihanteen $\mathfrak{p}$ sisältävä alkuihanne, niin $\mathfrak{P}' = \tau(\mathfrak{P})$

jollakin $\tau \in \mathrm{Gal}(L/K)$. Nyt lauseen 2.24 mukaan

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \left(\frac{L/K}{\tau(\mathfrak{P})}\right) = \tau \circ \left(\frac{L/K}{\mathfrak{P}}\right) \circ \tau^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right).$$

Abelin laajennuksen L/K tapauksessa Frobenius-automorfismi voidaan siis kirjoittaa $((L/K)/\mathfrak{p})$.

Seuraus 2.26. *Galois'n laajennuksessa L/K kunnan K haaroittumaton alkuihanne $\mathfrak{p}$ pysyy alkuihanteena kunnassa L, jos ja vain jos Galois'n ryhmä $Gal(L/K)$ on syklinen ja $\left(\frac{L/K}{\mathfrak{p}}\right)$ on sen generoija.*

Todistus. Olkoon $\mathfrak{P}$ kunnan L alkuihanne, joka on ihanteen $\mathfrak{p}$ päällä. Alkuihanne $\mathfrak{p}$ pysyy alkuihanteena kunnassa L, jos ja vain jos $f_{\mathfrak{P}|\mathfrak{p}} = [L : K]$. Lauseen 2.24 kohdan (ii) perusteella tämä on ekvivalenttia väitteen kanssa. □

Lemma 2.27. *Olkoon $K \subseteq E \subseteq L$, missä L/K ja E/K ovat Galois'n laajennuksia. Olkoon $\mathfrak{P}$ sellainen kunnan L alkuihanne, jonka alla oleva alkuihanne $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ on haaroittumaton laajennuksessa L/K. Tällöin*

$$\left(\frac{L/K}{\mathfrak{P}}\right)\Big|_E = \left(\frac{E/K}{\mathfrak{q}}\right),$$

missä $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_E$.

Todistus. Olkoon α kunnan E algebrallinen kokonaisluku ja σ ihanteen $\mathfrak{P}$ lohkeamisryhmän $\mathcal{Z}_{\mathfrak{P}}(L/K)$ alkio. Kongruenssi

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$$

on ekvivalentti kongruenssin

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{q}}$$

kanssa, sillä jokainen ryhmän $\mathcal{Z}_{\mathfrak{P}}(L/K)$ alkio kuvaa ihanteen $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_E$ itselleen, kun E on Galois yli kunnan K. Tämän vuoksi valitsemalla

$$\sigma = \left(\frac{L/K}{\mathfrak{P}}\right)$$

nähdään, että

$$\sigma|_E = \left(\frac{E/K}{\mathfrak{q}}\right).$$

□

2.4 Tšebotarevin tiheyslause

Tšebotarevin tiheyslause antaa tietoa eräiden alkuihannejoukkojen tiheydestä lukukunnassa. Tässä luvussa esitellään kyseinen tulos, koska tulemme sitä tarvitsemaan myöhemmin lauseen 3.57 todistuksessa osoittaessamme tietynlaisia alkuihanteita olevan ääretön määrä. Tätä varten määritellään ensin Dirichlet'n tiheyden käsite ja sen ominaisuuksien tutkimiseksi tarkastellaan Dedekindin zeetafunktiota. Itse Tšebotarevin tiheyslauseen todistus vaatisi avukseen syvällisempiä menetelmiä, ja siksi se sivuutetaan. Luokkakuntateoriaan pohjautuva todistus löytyy esimerkiksi kirjoista [5] ja [14].

Määritelmä 2.28. Lukukunnan K *Dedekindin zeetafunktio* on

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1},$$

missä tulo on otettu yli kaikkien kunnan K alkuihanteiden $\mathfrak{p} \neq [0]$ ja $s \in \mathbb{R}, s > 1$.

Tässä esityksessä rajoitumme tarkastelemaan Dedekindin zeetafunkiota vain luvun s reaaliarvoilla. Tavallisesti tämä funktio määritellään sarjana $\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$, missä $\mathfrak{a}$ käy kaikki kunnan K nollaihanteesta eroavat ihanteet, ja edellinen määritelmäksemme ottama muoto on oikeastaan niin sanottu Dedekindin zeetafunktion *Eulerin tuloesitys*.

Seuraavassa merkinnällä log tarkoitetaan luonnollista logaritmia. Näytetään, että Dedekindin zeetafunktio suppenee, kun $s \in \mathbb{R}, s > 1$. Ensinnäkin yleisesti on voimassa, että jos $a_n > 0$ jokaisella $n \in \mathbb{N}$, niin

$$\log\left(\lim_{N\to\infty} \prod_{n=1}^{N} a_n\right) = \lim_{N\to\infty} \log \prod_{n=1}^{N} a_n = \lim_{N\to\infty} \sum_{n=1}^{N} \log\, a_n.$$

Tässä käytettiin ensimmäisessä välivaiheessa logaritmin jatkuvuutta välillä $(0, \infty)$ ja toisessa välivaiheessa logaritmin ominaisuutta $\log(xy) = \log\, x + \log\, y$. Tästä seuraa, että tulon $\prod_{n=1}^{\infty} a_n$ suppeneminen on ekvivalenttia summan $\sum_{n=1}^{\infty} \log(a_n)$ suppenemisen kanssa. Tätä tulosta hyödyntämällä puolestaan helposti nähdään, että tulo $\prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$ suppenee, jos ja vain jos tulo $\prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})$ suppenee. Tunnetusti ääretön tulo $\prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})$ suppenee itseisesti (mistä seuraa, että tulon tekijät voidaan kirjoittaa mihin järjestykseen tahansa), jos sarja $\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}$ suppenee. Koska ihanteella $p\mathcal{O}_K$, missä p on alkuluku, on tekijöinään korkeintaan $[K : \mathbb{Q}]$ eri alkuihannetta $\mathfrak{p}$

ja näillä alkuihanteilla pätee $N(\mathfrak{p}) \geq p$, niin saadaan

$$\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s} \leq \sum_{p} \frac{[K:\mathbb{Q}]}{p^s} < \infty,$$

eli $\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}$ suppenee.

Määritelmä 2.29. Olkoon K lukukunta ja $\mathcal{P}_K$ kaikkien kunnan K alkuihanteiden joukko. Osajoukon $\mathcal{S} \subseteq \mathcal{P}_K$ *Dirichlet'n tiheys* on

$$\delta(\mathcal{S}) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}}{-\log(s-1)},$$

jos tämä raja-arvo on olemassa.

Olkoot funktiot $f(s)$ ja $g(s)$ määriteltyjä kaikilla $s \in \mathbb{R}, s > 1$. Merkinnällä $f(s) \sim g(s)$ tarkoitetaan, että $f(s) - g(s)$ on rajoitettu, kun $s \to 1^+$.

Käsitellään joitain Dirichlet'n tiheyden ominaisuuksia. Lauseen 2.30 todistuksessa käytetään apuna tunnettua tulosta, jonka mukaan raja-arvo $\lim_{s\to 1^+}(s-1)\zeta_K(s)$ on olemassa äärellisenä. Tämän todistus sivuutetaan, koska se on pitkähkö ja vaatisi avukseen sellaista teoriaa, jota ei tässä tutkielmassa käsitellä. Se on kuitenkin todistettu esimerkiksi luentomonisteessa [12].

Lauseen 2.30 todistus on lähteestä [2].

Lause 2.30. *Olkoon $K/\mathbb{Q}$ Galois'n laajennus ja $\mathcal{T}$ niiden kunnan K alkuihanteiden joukko, joiden jäännösluokka-aste yli kunnan $\mathbb{Q}$ on yksi ja jotka eivät ole haaroittuneita laajennuksessa $K/\mathbb{Q}$. Tällöin joukon $\mathcal{T}$ Dirichlet'n tiheys $\delta(\mathcal{T}) = 1$.*

Todistus. Tarkastellaan Dedekindin zeetafunktiota $\zeta_K(s) = \prod_{\mathfrak{p}}(1 - N(\mathfrak{p})^{-s})^{-1}$, kun $s \in \mathbb{R}, s > 1$. Luonnollisen logaritmin Taylorin sarjaa käyttäen nähdään, että

$$\begin{aligned} \log \zeta_K(s) &= -\sum_{\mathfrak{p}} \log(1 - N(\mathfrak{p})^{-s}) \\ &= \sum_{\mathfrak{p}} \sum_{n=1}^{\infty} \frac{1}{n} N(\mathfrak{p})^{-ns}. \end{aligned}$$

Koska $\log \zeta_K(s) = \log((s-1)\zeta_K(s)) + \log(1/(s-1))$, niin

$$\begin{aligned}\log \zeta_K(s) &\sim \log(1/(s-1)) \\ &\sim \sum_{\mathfrak{p}} \sum_{n=1}^{\infty} \frac{1}{n} N(\mathfrak{p})^{-ns} \\ &\sim \sum_{\mathfrak{p}} N(\mathfrak{p})^{-s} + \sum_{\mathfrak{p}} \sum_{n=2}^{\infty} \frac{1}{n} N(\mathfrak{p})^{-ns} \\ &\sim \sum_{\mathfrak{p}} N(\mathfrak{p})^{-s},\end{aligned}$$

sillä $\sum_{\mathfrak{p}} \sum_{n=2}^{\infty} \frac{1}{n} N(\mathfrak{p})^{-ns}$ on rajoitettu, kun $s \to 1^+$. Saadaan

$$\begin{aligned}\log \zeta_K(s) \sim \log\left(\frac{1}{s-1}\right) &\sim \sum_{\mathfrak{p}} N(\mathfrak{p})^{-s} \\ &\sim \sum_{\substack{\mathfrak{p} \\ f(\mathfrak{p}|p)=1=e(\mathfrak{p}|p)}} p^{-s} + \sum_{\substack{\mathfrak{p} \\ f(\mathfrak{p}|p)>1}} p^{-f(\mathfrak{p}|p)s} + \sum_{\substack{\mathfrak{p} \\ f(\mathfrak{p}|p)=1 \\ e(\mathfrak{p}|p)>1}} p^{-s}.\end{aligned}$$

Toinen sarja on rajoitettu, kun $s \to 1^+$, kuten on myös kolmaskin, koska haaroittuvia alkuihanteita on äärellinen määrä. Näin ollen

$$\log \zeta_K(s) \sim \log\left(\frac{1}{s-1}\right) \sim \sum_{\mathfrak{p} \in \mathcal{T}} N(\mathfrak{p})^{-s},$$

joten

$$\log\left(\frac{1}{s-1}\right) = \sum_{\mathfrak{p} \in \mathcal{T}} N(\mathfrak{p})^{-s} + b(s),$$

missä $b(s)$ on rajoitettu, kun $s \to 1^+$. Nyt voidaan laskea joukon $\mathcal{T}$ Dirichlet'n tiheys:

$$\begin{aligned}\delta(\mathcal{T}) &= \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{T}} N(\mathfrak{p})^{-s}}{-\log(s-1)} \\ &= \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{T}} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \mathcal{T}} N(\mathfrak{p})^{-s} + b(s)} \\ &= 1.\end{aligned}$$

□

Seuraus 2.31. *Jos $\mathcal{S} \subseteq \mathcal{P}_K$ on joukko, jolla on Dirichlet'n tiheys, niin $\delta(\mathcal{S}) = \delta(\mathcal{S} \cap \mathcal{T})$.*

Todistus. Kuten jo lauseen 2.30 todistuksesta käy ilmi, niin

$$\sum_{\substack{\mathfrak{p}\in\mathcal{S}\\ \mathfrak{p}\notin\mathcal{T}}} N(\mathfrak{p})^{-s} \sim 0.$$

Näin ollen

$$\sum_{\mathfrak{p}\in\mathcal{S}} N(\mathfrak{p})^{-s} \sim \sum_{\mathfrak{p}\in\mathcal{S}\cap\mathcal{T}} N(\mathfrak{p})^{-s},$$

mistä väite seuraa. □

Jos $\mathcal{S} \subseteq \mathcal{P}_K$ on äärellinen joukko, niin

$$\sum_{\mathfrak{p}\in\mathcal{S}} N(\mathfrak{p})^{-s} \sim 0,$$

joten äärellisen joukon Dirichlet'n tiheys on nolla. Dirichlet'n tiheyden määritelmästä myös nähdään, ettei minkään joukon tiheys voi olla negatiivinen. Tämän vuoksi jos $\mathcal{S} \subseteq \mathcal{S}'$, niin silloin $\delta(\mathcal{S}) \leq \delta(\mathcal{S}')$ aina, kun molemmat tiheydet ovat määritellyt.

Näistä huomioista nähdään, että $0 \leq \delta(\mathcal{S}) \leq 1$ aina, kun joukolla $\mathcal{S}$ on tiheys. Tiheydellä δ voidaan siis mitata joukon $\mathcal{S}$ alkuihanteiden määrän suhdetta kaikkien kunnan K alkuihanteiden määrään.

Olkoon nyt L kunnan K Galois'n laajennus ja $\mathfrak{p}$ kunnan K alkuihanne, joka ei haaroitu kunnassa L. Tällöin kunnan L ihanteen $\mathfrak{p}$ sisältävät eri alkuihanteet $\mathfrak{P}$ saattavat määritellä eri Frobenius-automorfismin $((L/K)/\mathfrak{P})$. Lauseen 2.24 mukaan kaikki kuvaukset $((L/K)/\mathfrak{P})$ saadaan kuitenkin toisistaan konjugoimalla ja edelleen lauseesta 2.14 seuraa, että ne muodostavat kokonaisen konjugaattiluokan ryhmässä $\mathrm{Gal}(L/K)$. Alkuihanteen $\mathfrak{p}$ Frobenius-automorfismi $((L/K)/\mathfrak{p})$ voidaan siis samaistaa kyseisen konjugaattiluokan kanssa.

Lause 2.32 (**Tšebotarevin tiheyslause**). *Olkoon L lukukunnan K laajennuskunta ja $\langle\sigma\rangle$ alkion $\sigma \in Gal(L/K)$ konjugaattiluokka. Tällöin joukon*

$$\mathcal{S} = \{\mathfrak{p} \in \mathcal{P}_K \mid \mathfrak{p} \text{ on haaroittumaton kunnassa } L \text{ ja } ((L/K)/\mathfrak{p}) = \langle\sigma\rangle\}$$

Dirichlet'n tiheys on

$$\delta(\mathcal{S}) = \frac{|\langle\sigma\rangle|}{|Gal(L/K)|} = \frac{|\langle\sigma\rangle|}{[L:K]}.$$

Lauseen joukon $\mathcal{S}$ täytyy siis olla ääretön, koska sen Dirichlet'n tiheys on positiivinen.

Seuraus 2.33. *On olemassa ääretön määrä sellaisia kunnan K alkuihanteita, jotka pysyvät hitaina syklisessä laajennuksessa L/K.*

Todistus. Olkoon σ ryhmän $\mathrm{Gal}(L/K)$ generoija-alkio. Jos $\mathfrak{p} \in \mathcal{P}_K$ on alkuihanne, jolle pätee $((L/K)/\mathfrak{p}) = \sigma$, niin lauseen 2.24 kohdan (ii) perusteella alkuihanteen $\mathfrak{p}$ jäännösluokka-aste $f = [L : K]$. Alkuihanne $\mathfrak{p}$ siis pysyy hitaana kunnassa L. Väite seuraa nyt Tšebotarevin tiheyslauseesta. □

Tarkemmin ottaen astetta n olevassa syklisessä laajennuksessa hitaana pysyvien alkuihanteiden muodostaman joukon Dirichlet'n tiheys on $\varphi(n)/n$, mutta näin tarkkaa tulosta emme tarvitse.

2.5 Lukukuntien täydellistymistä

Tähän pykälään on kerätty myöhemmin käyttöön tulevia perustietoja lukukuntien arvotuksista ja täydellistymistä. Tulemme tarvitsemaan niitä luvussa 3.2 johtaessamme kaavan jakoalgebran pienimmälle mahdolliselle diskriminantille.

Todistukset esitetyille tuloksille voi löytää monista algebrallisen lukuteorian perusteita käsittelevistä kirjoista, esimerkiksi kirjoista [5] tai [9].

Määritelmä 2.34. Lukukunnan K *arvotus* on kuvaus

$$|\cdot| : K \to \mathbb{R},$$

jolle on voimassa jokaisella $x, y \in K$

(i) $|x| \geq 0$, ja $|x| = 0 \iff x = 0$,

(ii) $|xy| = |x||y|$,

(iii) $|x + y| \leq |x| + |y|$ (*kolmioepäyhtälö*).

Paria $(K, |\cdot|)$ (tai lyhyesti kuntaa K) kutsutaan tällöin *arvotetuksi kunnaksi*. Lukua $|x|$ kutsutaan alkion x *arvoksi*.

Määritelmä 2.35. Arvotusta $|\cdot|$ kutsutaan *epäarkhimediseksi*, jos se täyttää jokaisella $x, y \in K$ ehtoa (iii) vahvemman ehdon

(iii') $|x + y| \leq \max\{|x|, |y|\}$.

Muussa tapauksessa arvotusta $|\cdot|$ kutsutaan *arkhimediseksi*.

Esimerkki 2.36. Olkoon K reaalilukujen kunnan alikunta. Tällöin tavallinen itseisarvo $|x|$ on kunnan K epäarkhimedinen arvotus.

Kunnan K arvotus $|\cdot|$ indusoi luonnollisella tavalla kunnalle K metriikan

$$d(x,y) = |x-y| \quad \forall\, x,y \in K.$$

Tämä tekee kunnasta K metrisen avaruuden.

Määritelmä 2.37. Kunnan K arvotuksia $|\cdot|_1$ ja $|\cdot|_2$ kutsutaan *ekvivalenteiksi*, jos niiden indusoimat kunnan K metriikat ovat ekvivalentit, eli toisin sanoen jos metrisen avaruuden $(K, |\cdot|_1)$ avoimet joukot ovat samat kuin avaruuden $(K, |\cdot|_2)$ avoimet joukot.

Olkoon $\mathfrak{p} \neq [0]$ lukukunnan K alkuihanne. Alkion $x \in K^*$ generoimalla murtoihanteella on kanoninen esitys

$$x\mathcal{O}_K = \mathfrak{p}^{\alpha}\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_t^{\alpha_t}, \tag{6}$$

missä ihanteet $\mathfrak{p}_i$ ovat eri alkuihanteita kuin $\mathfrak{p}$ ja $\alpha, \alpha_i \in \mathbb{Z}$. Alkuihannehajotelman (6) yksikäsitteisyyden vuoksi voidaan määritellä kuvaus

$$v_{\mathfrak{p}} : K^* \to \mathbb{Z},$$

missä $v_{\mathfrak{p}}(x) = \alpha$. Kuvausta $v_{\mathfrak{p}}$ kutsutaan kunnan K *eksponenttiarvotukseksi*. Sille pätee $v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$ ja $v_{\mathfrak{p}}(x+y) \geq \min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\}$.

Eksponenttiarvotusta $v_{\mathfrak{p}}$ käyttäen voidaan määritellä kunnalle K $\mathfrak{p}$-*adinen arvotus*

$$|x|_{\mathfrak{p}} = \begin{cases} 0, & \text{jos } x = 0 \\ c^{v_{\mathfrak{p}}(x)}, & \text{jos } x \neq 0, \end{cases}$$

missä c on reaaliluku, $0 < c < 1$. Helposti voitaisiin varmistaa, että $|x|_{\mathfrak{p}}$ on kunnan K epäarkhimedinen arvotus. Eri reaaliluvun c valinnat määräävät ekvivalentit arvotukset. Lisäksi, jos $\mathfrak{p} \neq \mathfrak{q}$, niin kunnan K arvotukset $|\cdot|_{\mathfrak{p}}$ ja $|\cdot|_{\mathfrak{q}}$ eivät ole ekvivalentteja. Tyypillisiä valintoja reaaliluvulle c ovat $1/p$, missä $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$, ja luku $1/N(\mathfrak{p})$.

Määritelmä 2.38. Metrisen avaruuden (M,d) pistejonoa (x_n) kutsutaan *Cauchyn jonoksi*, jos jokaista positiivilukua ϵ kohti on sellainen positiivinen kokonaisluku n_1, että

$$d(x_m, x_n) < \epsilon$$

kaikilla $m > n \geq n_1$.

Olkoon K lukukunta, $|\cdot|$ sen arvotus ja d tämän arvotuksen indusoima metriikka. Määritellään

$$\mathcal{C} = \{(x_n) \mid (x_n) \text{ on Cauchyn jono metriikan } d \text{ suhteen avaruudessa } K\}$$

ja

$$\mathcal{N} = \{(x_n) \mid a_n \in K \text{ jokaisella } n \text{ ja } a_n \to 0\}.$$

Voidaan osoittaa, että $\mathcal{C}$ on kommutatiivinen rengas, kun siinä määritellään operaatiot $(x_n) + (y_n) = (x_n + y_n)$ ja $(x_n)(y_n) = (x_n y_n)$. Lisäksi voidaan näyttää, että joukko $\mathcal{N}$ on renkaan $\mathcal{C}$ maksimaalinen ihanne. Tällöin siis $\mathcal{C}/\mathcal{N}$ on kunta.

Määritelmä 2.39. Kunta $\mathcal{C}/\mathcal{N}$ on lukukunnan K *täydellistymä* arvotuksen $|\cdot|$ suhteen.

Lukukuntaa K voidaan ajatella minkä tahansa sen täydellistymän alikuntana samaistamalla kunnan alkiot vakiojonojen kanssa. Jos kunnan K arvotus $|\cdot| = |\cdot|_{\mathfrak{p}}$, missä $\mathfrak{p} \neq [0]$ on jokin renkaan $\mathcal{O}_K$ alkuihanne, niin tällöin kunnan K täydellistymää merkitään $K_{\mathfrak{p}}$. Tätä kutsutaan kunnan K $\mathfrak{p}$-*adiseksi täydellistymäksi*. Kunnan K arvotus $|\cdot|_{\mathfrak{p}}$ voidaan laajentaa täydellistymään $K_{\mathfrak{p}}$ määrittelemällä

$$|(x_n) + \mathcal{N}|_{\mathfrak{p}} = \lim_{n\to\infty} |x_n|_{\mathfrak{p}}.$$

On helppo tarkistaa, että tämä kuvaus todella on kunnan $K_{\mathfrak{p}}$ arvotus, jonka rajoittuma kuntaan K on alkuperäinen $\mathfrak{p}$-adinen arvotus.

Tarkastellaan $\mathfrak{p}$-adista täydellistymää $K_{\mathfrak{p}}$ yksityiskohtaisemmin. Olkoon

$$\mathcal{O}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} \mid |x|_{\mathfrak{p}} \leq 1\}.$$

Joukon $\mathcal{O}_{\mathfrak{p}}$ voidaan näyttää olevan kommutatiivinen rengas. Sitä kutsutaan $\mathfrak{p}$-*adisten kokonaislukujen renkaaksi* ja sen alkiot ovat $\mathfrak{p}$-*adisia kokonaislukuja*. Renkaalla $\mathcal{O}_{\mathfrak{p}}$ on yksikäsitteinen maksimaalinen ihanne

$$\mathcal{P}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} \mid |x|_{\mathfrak{p}} < 1\},$$

ja renkaan $\mathcal{O}_{\mathfrak{p}}$ yksiköt ovat tarkalleen ne alkiot, joiden arvo on yksi. Huomaa, että $\mathcal{O}_K$ on renkaan $\mathcal{O}_{\mathfrak{p}}$ alirengas. Lisäksi on voimassa $\mathcal{P}_{\mathfrak{p}} = \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ ja

$$\mathcal{O}_{\mathfrak{p}}/\mathcal{P}_{\mathfrak{p}} \cong \mathcal{O}_K/\mathfrak{p}.$$

Esimerkki 2.40. Rationaalilukujen kunnan $\mathbb{Q}$ p-adisen täydellistymän $\mathbb{Q}_p$ kokonaislukujen rengasta merkitään $\mathbb{Z}_p$. Renkaan $\mathbb{Z}_p$ kaikki nollaihanteesta eroavat ihanteet ovat $p^m\mathbb{Z}_p$, missä $m \geq 0$. Erityisesti siis $\mathbb{Z}_p$ on pääihannealue ja $p\mathbb{Z}$ on sen maksimaalinen ihanne. Rationaalisten p-adisten kokonaislukujen joukko on $\mathbb{Q} \cap \mathbb{Z}_p = \left\{ \frac{x}{y} \in \mathbb{Q} \,\middle|\, p \nmid y \right\}$.

Olkoon $\pi \in \mathfrak{p} \backslash \mathfrak{p}^2$ ja tulkitaan se täydellistymän $K_\mathfrak{p}$ alkioksi. Alkio π generoi ihanteen $\mathcal{P}_\mathfrak{p}$. Tällaista alkiota kutsutaan täydellistymän $K_\mathfrak{p}$ *alkualkioksi*. Jokainen alkio $x \in K_\mathfrak{p}$ voidaan kirjoittaa muodossa $x = \epsilon\pi^t$, missä $t \in \mathbb{Z}$ ja ϵ on renkaan $\mathcal{O}_\mathfrak{p}$ yksikkö. Huomaa myös, että jos $x \in K$ ja $v_\mathfrak{p}(x) = \alpha$, niin kunnassa $K_\mathfrak{p}$ pätee $x = \epsilon\pi^\alpha$, missä $\epsilon \in \mathcal{O}_\mathfrak{p}$ on jokin yksikkö.

Olkoon L/K kuntalaajennus ja $\mathfrak{p} \neq [0]$ renkaan $\mathcal{O}_K$ alkuihanne. Olkoon alkuihanteen $\mathfrak{p}$ alkuihannehajotelma renkaassa $\mathcal{O}_L$

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Tällöin mitkään kaksi arvotuksista $|\cdot|_{\mathfrak{P}_1}, ..., |\cdot|_{\mathfrak{P}_g}$ eivät ole ekvivalentteja kunnassa L, mutta niiden kaikkien rajoittumat alikuntaan K indusoivat saman topologian kunnalle K kuin arvotus $|\cdot|_\mathfrak{p}$. Jokainen täydellistymä $L_{\mathfrak{P}_j}$ on kunnan $K_\mathfrak{p}$ äärellinen laajennus. Käänteinen tulos on myös voimassa. Jos l on kunnan $K_\mathfrak{p}$ äärellinen laajennus, niin on olemassa sellainen kunnan K äärellinen laajennus L ja renkaan $\mathcal{O}_L$ alkuihanne $\mathfrak{P}$, että $l = L_\mathfrak{P}$.

Kuten lukukuntien kokonaislukujen renkaissa myös $\mathfrak{p}$-adisten kokonaislukujen renkaassa $\mathcal{O}_\mathfrak{p}$ ihanteilla on yksikäsitteinen alkuihannehajotelma. Tietenkin hajotelmat ovat hyvin yksinkertaisia, sillä renkaassa $\mathcal{O}_\mathfrak{p}$ on vain yksi alkuihanne. Kunnan $K_\mathfrak{p}$ alkuihanne $\mathcal{P}_\mathfrak{p} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$ hajoaa laajennuskunnassa $L_\mathfrak{P}$ tekijöiksi $\mathcal{P}_\mathfrak{p}\mathcal{O}_\mathfrak{P} = \mathcal{P}_\mathfrak{P}^e$, missä $e = (\mathcal{P}_\mathfrak{P}|\mathcal{P}_\mathfrak{p})$ on positiivinen kokonaisluku. Kun merkitään $f = f(\mathcal{P}_\mathfrak{P}|\mathcal{P}_\mathfrak{p}) = [\mathcal{O}_\mathfrak{P}/\mathcal{P}_\mathfrak{P} : \mathcal{O}_\mathfrak{p}/\mathcal{P}_\mathfrak{p}]$, niin tällöin $ef = [L_\mathfrak{P} : K_\mathfrak{p}]$. Lohkeamista laajennuksessa $L_\mathfrak{P}/K_\mathfrak{p}$ ei luonnollisestikaan tapahdu. Jos $e = 1$, niin sanotaan, että laajennus $L_\mathfrak{P}/K_\mathfrak{p}$ on *haaroittumaton*.

Olkoon taas L/K kuntalaajennus ja $\mathfrak{p} \neq [0]$ renkaan $\mathcal{O}_K$ alkuihanne, joka hajoaa alkuihanteiden tuloksi $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$. Voidaan osoittaa, että $e(\mathcal{P}_{\mathfrak{P}_i}|\mathcal{P}_\mathfrak{p}) = e(\mathfrak{P}_i|\mathfrak{p})$ ja $f(\mathcal{P}_{\mathfrak{P}_i}|\mathcal{P}_\mathfrak{p}) = f(\mathfrak{P}_i|\mathfrak{p})$. Lisäksi, jos L/K on Galois'n laajennus, niin tällöin myös $L_{\mathfrak{P}_i}/K_\mathfrak{p}$ on Galois'n laajennus. Laajennuksen $L_{\mathfrak{P}_i}/K_\mathfrak{p}$ Galois'n ryhmä on

$$\mathrm{Gal}(L_{\mathfrak{P}_i}/K_\mathfrak{p}) \cong \mathcal{Z}_{\mathfrak{P}_i}(L/K).$$

Seuraavaa lausetta tarvitsemme luvussa 3.2.1 jakoalgebran niin sanottua Hasse-invarianttia määriteltäessä.

Lause 2.41. *Olkoon K lukukunta, $\mathfrak{p}$ sen nollaihanteesta eroava alkuihanne ja $K_\mathfrak{p}$ kunnan K täydellistymä. Olkoon lisäksi f positiivinen kokonaisluku. Tällöin on olemassa yksikäsitteinen astetta f oleva kunnan $K_\mathfrak{p}$ haaroittumaton laajennus. Se on Galois'n laajennus ja sen Galois'n ryhmä on syklinen.*

3 Jakoalgebrat

Tutkielman pääkiinnostuksen kohteena ovat jakoalgebrat. Tavoitteena on konstruoida minimaalidiskriminanttisia jakoalgebroja, joiden keskuksena on kunta $\mathbb{Q}(\sqrt{-7})$. Sitä ennen todistetaan alaraja jakoalgebrojen diskriminanteille pykälässä 3.2. Luvussa 2 esiteltiin tarvitsemamme algebrallinen lukuteoria ja seuraavaksi pykälässä 3.1 esitellään vielä algebroihin liittyvät perusteet.

Diskriminanttirajan todistamiseksi tarvitsemme tietoa myös esimerkiksi jakoalgebrojen niin sanotuista Hasse-invarianteista sekä Brauerin ryhmistä. Suurin osa näiden asioiden todistuksista sivuutetaan. Monet todistuksista vaatisivat avukseen syvällisiä tuloksia luokkakuntateoriasta. Tavoitteena on vain esitellä välttämätön teoria, jota tarvitsemme diskriminanttirajan todistamiseksi. Todistamatta jätetyt tulokset löytyvät kirjasta [15], ellei toisin ole mainittu.

Pykälässä 3.3 konstruoidessamme halutunlaisia jakoalgebroja palaamme enimmäkseen algebrallisen lukuteorian pariin, jolloin hyödynnämme luvussa 2 esiteltyä teoriaa.

Tämä luku seuraa lähes kokonaisuudessaan artikkelia [18] ja enemmistö todistuksista on siitä peräisin.

3.1 Perusteet

Vaikka sykliset jakoalgebrat ovatkin keskeisin tarkastelun kohteemme, niin niiden käsittelemiseksi meidän tarvitsee tarkastella myös laajempaa algebrojen joukkoa, *yksinkertaisia keskeisiä algebroja*.

Tässä pykälässä kunnat ovat useimmiten algebrallisia lukukuntia, mutta tulokset ovat myös voimassa, vaikka lukukunnat korvattaisiin $\mathfrak{p}$-adisilla kunnilla.

Määritelmä 3.1. Olkoon K kunta ja L/K syklinen Galois'n laajennus, jonka aste on n ja jonka Galois'n ryhmä on $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Voidaan määritellä K-algebra

$$\mathcal{A} = (L/K, \sigma, \gamma) = L \oplus uL \oplus u^2L \oplus \cdots \oplus u^{n-1}L,$$

missä $u \in \mathcal{A}$ on generoija-alkio, jolle on voimassa $xu = u\sigma(x)$ kaikilla $x \in L$ ja $u^n = \gamma \in K^*$. Tällaista algebraa kutsutaan *sykliseksi algebraksi*.

Huomaa, että syklisen algebran $\mathcal{A} = (L/K, \sigma, \gamma)$ aste vektoriavaruutena yli kunnan K on laajennuksen L/K asteen neliö.

Määritelmä 3.2. Algebraa $\mathcal{A}$ kutsutaan *yksinkertaiseksi*, jos sillä ei ole epätriviaaleja ihanteita. Algebran $\mathcal{A}$ *keskus* $Z(\mathcal{A}) = \{a \in \mathcal{A} \mid aa' = a'a \; \forall a' \in \mathcal{A}\}$ on niiden algebran $\mathcal{A}$ alkioiden joukko, jotka kommutoivat kaikkien algebran $\mathcal{A}$ alkioiden kanssa. Algebra $\mathcal{A}$ yli kunnan K on *keskeinen algebra*, jos sen keskus $Z(\mathcal{A}) = 1_{\mathcal{A}}K$.

Määritelmä 3.3. *Yksinkertainen K-keskeinen algebra* on yksinkertainen algebra, joka on äärellisulotteinen yli keskuksen K.

Lause 3.4. *Jokainen syklinen algebra on yksinkertainen keskeinen algebra.*

Lause on voimassa myös toiseen suuntaan, jos tarkastellaan yksinkertaista keskeistä algebraa, jonka keskus on lukukunta K.

Lause 3.5. *Olkoon K lukukunta. Jokainen yksinkertainen K-keskeinen algebra on syklinen algebra.*

Määritelmä 3.6. Yksinkertainen keskeinen algebra $\mathcal{A}$ on *jakoalgebra*, jos kaikki sen nollasta eroavat alkiot ovat kääntyviä.

Esimerkki 3.7. Helpoimpia esimerkkejä yksinkertaisista keskeisistä algebroista ovat matriisialgebrat yli kunnan K. Jokaisella positiivisella kokonaisluvulla n K-algebra $\mathcal{M}_n(K) = \{(a_{ij})_{n\times n} \mid a_{ij} \in K\}$ on yksinkertainen keskeinen algebra. Nimittäin tunnetusti algebran $\mathcal{M}_n(K)$ ihanteet ovat triviaaleja, kun K on kunta, ja ainoastaan alkiot $\mathbf{1}K = \{\mathrm{diag}(a, ..., a) \mid a \in K\}$ kommutoivat kaikkien muiden algebran $\mathcal{M}_n(K)$ alkioiden kanssa. Tämä algebra ei kuitenkaan ole jakoalgebra, kun $n \geq 2$, sillä nollamatriisista eroavat matriisit, joiden aste on korkeintaan $n-1$, eivät ole kääntyviä.

Tarvitsemme keinon tunnistaa jakoalgebrat syklisistä algebroista. Seuraava lause on todistettu kirjassa [1].

Lause 3.8. *Astetta n oleva syklinen algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ on jakoalgebra, jos ja vain jos mikään alkioista γ^t, $0 < t < n$, ei ole joukon L^* minkään alkion normi.*

Lauseen 3.8 vuoksi alkiota γ kutsutaan *epänormialkioksi.*

Esimerkki 3.9. *Hamiltonin kvaternioalgebrassa* $\mathbb{H}_{\mathbb{Q}} = (\mathbb{Q}(i)/\mathbb{Q}, \sigma, -1)$, missä σ on tavallinen kompleksikonjugointi, tyypillisesti generoija-alkiota merkitään symbolilla j eikä u, ja kirjoitetaan $k = ij$. Siis $i^2 = j^2 = k^2 = -1$ ja $ji = -ij$. Alkion $a + bi$, $a, b \in \mathbb{Q}$, normi on $(a + bi)(a - bi) = a^2 + b^2 \neq -1$, joten -1 ei ole minkään alkion normi. Lauseen 3.8 mukaan tämä osoittaa algebran $\mathbb{H}_{\mathbb{Q}}$ olevan jakoalgebra.

Määritelmä 3.10. Olkoon L/K syklinen kuntalaajennus ja $\mathcal{A} = (L/K, \sigma, \gamma)$ jakoalgebra. Osajoukko $\Lambda \subseteq \mathcal{A}$ on *$\mathcal{O}_K$-järjestö*, jos

(i) Λ on renkaan $\mathcal{A}$ alirengas, jolla on sama neutraalialkio.
(ii) Λ on äärellisesti generoitu $\mathcal{O}_K$-moduli.
(iii) Λ generoi algebran $\mathcal{A}$ vektoriavaruutena yli kunnan K.

Esimerkki 3.11. Olkoon $\mathcal{A} = (L/K, \sigma, \gamma)$ kuten edeltävässä määritelmässä ja oletetaan, että sen epänormialkio $\gamma \in K^*$ on algebrallinen kokonaisluku. Tällöin $\mathcal{O}_K$-moduli

$$\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L \oplus u^2\mathcal{O}_L \oplus \cdots \oplus u^{n-1}\mathcal{O}_L$$

on alirengas syklisessä algebrassa $(L/K, \sigma, \gamma)$. Tätä kutsutaan algebran $\mathcal{A}$ *luonnolliseksi järjestöksi*. Epänormialkioksi γ täytyi valita algebrallinen kokonaisluku, sillä muutoin Λ ei olisi suljettu kertolaskun suhteen.

Jakoalgebran $\mathcal{A}$ järjestö Λ on *maksimaalinen järjestö*, jos ei ole olemassa toista järjestöä Λ', $\Lambda \subset \Lambda' \subset \mathcal{A}$. Maksimaalisia järjestöjä voi pitää lukukuntien kokonaislukujen renkaan analogiana jakoalgebroissa.

Lause 3.12. *Jokaisella K-keskeisellä jakoalgebralla $\mathcal{A}$ on maksimaalinen $\mathcal{O}_K$-järjestö ja jokainen algebran $\mathcal{A}$ järjestö sisältyy vähintään yhteen maksimaaliseen järjestöön.*

Tutkiaksemme renkaan $\mathcal{O}_K$ ja $\mathcal{O}_K$-järjestön Λ välistä suhdetta on hyödyllistä tarkastella jakoalgebraa $\mathcal{A}$ matriisialgebran alialgebrana.

Lause 3.13. *Olkoon $\mathcal{A}$ jakoalgebra, jonka keskus on K ja aste $[\mathcal{A} : K] = n^2$. Tällöin jokainen algebran $\mathcal{A}$ maksimaalinen alikunta L sisältää kunnan K ja aste*

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

Huomautus 3.14. On ilmeistä, että jokainen jakoalgebra sisältää vähintään yhden maksimaalisen alikunnan.

Olkoon $\mathcal{A}$ K-keskeinen jakoalgebra, $[\mathcal{A} : K] = n^2$, ja oletetaan, että L on algebran $\mathcal{A}$ maksimaalinen alikunta. Tällöin $\mathcal{A}$ on n-dimensioinen oikeanpuoleinen vektoriavaruus yli kunnan L. Algebra $\mathcal{A}$ operoi vektoriavaruuteen $\mathcal{A}$ kertolaskulla vasemmalta. Jos $c \in \mathcal{A}$, niin olkoon $\lambda_c : \mathcal{A} \to \mathcal{A}$ kuvaus, joka kuvaa alkion $x \in \mathcal{A}$ alkioksi cx. Koska tämä kuvaus ja oikeanpuoleinen skalaarikertolasku kommutoivat, ts. $c(xl) = (cx)l$, missä $l \in L$, niin λ_c on L-lineaarinen. Saadaan upotus $\mathcal{A} \to \mathrm{End}_L(\mathcal{A})$, joka kuvaa alkion

$c \in \mathcal{A}$ kuvaukseksi λ_c. Kiinnittämällä vektoriavaruudelle $\mathcal{A}$ L-kanta jokainen $\lambda_c \in \mathrm{End}_L(\mathcal{A})$ voidaan esittää matriisilla $M(\lambda_c)$, ja tunnetusti kuvaus $\lambda_c \mapsto M(\lambda_c)$ on algebraisomorfismi $\mathrm{End}_L(\mathcal{A}) \to \mathcal{M}_n(K)$. Saadaan siis injektiivinen K-algebrahomomorfismi ψ algebrasta $\mathcal{A}$ matriisialgebraan $\mathcal{M}_n(L)$. Näin ollen alkio $c \in \mathcal{A}$ ja matriisi $\psi(c) \in \mathcal{M}_n(L)$ voidaan samaistaa. Kuvausta ψ kutsutaan *maksimaaliseksi esitykseksi*.

Määritelmä 3.15. Matriisin $\psi(c)$ jälkeä kutsutaan alkion $c \in \mathcal{A}$ *redusoiduksi jäljeksi* ja sitä merkitään $\mathrm{tr}_{\mathcal{A}/K}(c)$.

Huomautus 3.16. Voidaan osoittaa, että alkion $a \in \mathcal{A}$ jälkikuvauksen $T_{\mathcal{A}/K}(a)$ ja redusoidun jäljen $\mathrm{tr}(a)$ yhteys on $T_{\mathcal{A}/K}(a) = n\mathrm{tr}(a)$, missä n on laajennuksen L/K aste.

Lause 3.17. *Olkoon $\mathcal{A}$ K-keskeinen jakoalgebra ja $a \in \mathcal{A}$. Tällöin redusoitu jälki $tr(a) \in K$. Jos lisäksi Λ on algebran $\mathcal{A}$ $\mathcal{O}_K$-järjestö ja alkio $a \in \Lambda$, niin redusoitu jälki $tr(a)$ on kokonaislukujen renkaan $\mathcal{O}_K$ alkio.*

Esimerkki 3.18. Olkoon L/K syklinen kuntalaajennus ja $\mathcal{A} = (L/K, \sigma, \gamma)$ jakoalgebra. Tarkastellaan algebraa $\mathcal{A}$ oikeanpuoleisena vektoriavaruutena yli kunnan L. Valitaan avaruudelle $\mathcal{A}$ L-kanta $\{1, u, ..., u^{n-1}\}$ ja olkoon $a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{A}$. Tämän alkion matriisiesityksen $\psi(a)$ is pystyrivi, $i \in \{0, 1, ..., n-1\}$, on vektorin

$$au^i = (x_0 + ux_1 + \cdots + u^{n-1}x_{n-1})u^i = u^i\sigma(x_0) + u^{i+1}\sigma(x_1) + \cdots + u^{n-1+i}\sigma(x_{n-1})$$

koordinaattivektori. Tällöin siis

$$\psi(a) = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \dots & \gamma\sigma^{n-2}(x_2) & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \dots & \gamma\sigma^{n-2}(x_3) & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & \dots & \gamma\sigma^{n-2}(x_4) & \gamma\sigma^{n-1}(x_3) \\ x_3 & \sigma(x_2) & \sigma^2(x_1) & \dots & \gamma\sigma^{n-2}(x_5) & \gamma\sigma^{n-1}(x_4) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \dots & \sigma^{n-2}(x_1) & \sigma^{n-1}(x_0) \end{pmatrix}. \quad (7)$$

Lause 3.19. *Jälkikuvaus ei riipu maksimaalisesta esityksestä.*

Määritelmä 3.20. Olkoon $\mathcal{A}$ K-keskeinen jakoalgebra ja $m = dim_K\mathcal{A}$. $\mathcal{O}_K$-järjestön Λ $\mathcal{O}_K$-*diskriminantti* on renkaan $\mathcal{O}_K$ ihanne $d(\Lambda/\mathcal{O}_K)$, joka on alkioiden

$$\{\det(\mathrm{tr}_{\mathcal{A}/K}(x_ix_j))_{i,j=1}^m \mid (x_1, ..., x_m) \in \Lambda^m\}$$

generoima. Kun sekaannuksen vaaraa ei ole, käytetään myös lyhyempää merkintää $d(\Lambda/\mathcal{O}_K) = d(\Lambda)$.

Esimerkiksi kunnan $K = \mathbb{Q}(\sqrt{-7})$ tapauksessa sen kokonaislukujen rengas $\mathcal{O}_K = \mathcal{O}_{\mathbb{Q}(\sqrt{-7})}$ on Eukleideen alue, jolloin on järkevää puhua diskriminantista alkiona eikä ihanteena. Järjestö Λ on vapaa $\mathcal{O}_K$-moduli, joten voimme samaistaa diskriminantti-ihanteen generoivan alkion jonkin kannan diskriminantin kanssa. Järjestön Λ diskriminantti voidaan tällöin laskea kaavalla

$$d(\Lambda/\mathcal{O}_K) = \det(\mathrm{tr}(x_i x_j))_{i,j=1}^m,$$

missä $\{x_1, ..., x_m\}$ on mikä tahansa järjestön Λ $\mathcal{O}_K$-kanta. Tästä näemme, että kun $\Lambda \subseteq \Gamma$ ovat $\mathcal{O}_K$-järjestöjä, niin $d(\Gamma)$ on diskriminantin $d(\Lambda)$ tekijä.

Lause 3.21. *Kaikilla K-keskeisen jakoalgebran maksimaalisilla järjestöillä on sama diskriminantti.*

Määritelmä 3.22. Olkoon $\mathcal{A}$ K-keskeinen jakoalgebra ja olkoon Λ jokin sen maksimaalinen järjestö. Tämän järjestön diskriminanttia $d(\Lambda/\mathcal{O}_K) = d_{\mathcal{A}}$ kutsutaan *jakoalgebran $\mathcal{A}$ diskriminantiksi.*

Lauseen 3.21 mukaan jakoalgebran diskriminantti on hyvinmääritelty, eikä siis riipu maksimaalisen järjestön valinnasta.

Huomautus 3.23. Olkoon L/K syklinen kuntalaajennus ja $\mathcal{A} = (L/K, \sigma, \gamma)$ jakoalgebra. Esimerkin 3.18 matriisin (7) jälkeen ei selvästikään vaikuta se, mikä alkio σ on valittu ryhmän $\mathrm{Gal}(L/K)$ generoijaksi. Koska jälkikuvaus $\mathrm{tr}_{\mathcal{A}/K}$ ei riipu maksimaalisesta esityksestä, niin nyt jakoalgebran $\mathcal{A}$ diskriminantin määritelmästä nähdään, ettei alkion σ valinta vaikuta algebran $\mathcal{A}$ diskriminanttiin.

3.2 Diskriminanttiraja

Tavoitteena tässä pykälässä on todistaa jakoalgebran diskriminantille alaraja. Tätä varten tarvitsemme ensin paremman ymmärryksen algebran diskriminantista ja siksi tutustumme algebran Hasse-invariantin sekä Brauerin ryhmän käsitteisiin. Diskriminanttirajan todistus seuraa artikkelin [18] esitystä.

3.2.1 Hasse-invariantti

Olkoot $\mathcal{A}$ ja $\mathcal{B}$ K-algebroja ja olkoon $\mathcal{A} \otimes_K \mathcal{B}$ niiden tensoritulo K-vektoriavaruuksina. On olemassa yksikäsitteinen avaruuden $\mathcal{A} \otimes_K \mathcal{B}$ K-bilineaarinen kertolasku, jolle pätee

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'$$

jokaisella $a, a' \in \mathcal{A}$ ja $b, b' \in \mathcal{B}$. Kun kunta K samaistetaan osajoukon $K \cdot (1 \otimes 1) \subset \mathcal{A} \otimes_K \mathcal{B}$ kanssa, niin avaruudesta $\mathcal{A} \otimes_K \mathcal{B}$ tulee K-algebra. Tensoritulot ovat kommutatiivisia siinä mielessä, että kaikilla K-algebroilla $\mathcal{A}$ ja $\mathcal{B}$ kuvaus $a \otimes b \mapsto b \otimes a$ laajenee K-algebrojen isomorfismiksi

$$\mathcal{A} \otimes_K \mathcal{B} \longrightarrow \mathcal{B} \otimes_K \mathcal{A}.$$

Ne ovat myös assosiatiivisia siinä mielessä, että kaikilla K-algebroilla $\mathcal{A}$, $\mathcal{B}$ ja $\mathcal{C}$ kuvaus $a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c$ laajenee K-algebrojen isomorfismiksi

$$\mathcal{A} \otimes_K (\mathcal{B} \otimes_K \mathcal{C}) \longrightarrow (\mathcal{A} \otimes_K \mathcal{B}) \otimes_K \mathcal{C}.$$

Olkoon K' lukukunnan K laajennuskunta. Jos $\mathcal{A}$ on yksinkertainen K-keskeinen algebra, niin tensoritulo $\mathcal{A}' = K' \otimes \mathcal{A}$ on yksinkertainen K'-keskeinen algebra. Sanotaan, että algebra $\mathcal{A}'$ on algebran $\mathcal{A}$ *skalaarilaajennus*.

Määritelmä 3.24. Olkoon $K_\mathfrak{p}$ lukukunnan K täydellistymä alkuihanteen $\mathfrak{p}$ suhteen. Jos $\mathcal{A}$ on yksinkertainen K-keskeinen algebra, niin algebraa $\mathcal{A}_\mathfrak{p} = K_\mathfrak{p} \otimes_K \mathcal{A}$ kutsutaan algebran $\mathcal{A}$ *lokalisaatioksi alkuihanteen* $\mathfrak{p}$ *suhteen*.

Lause 3.25. *Edellisen määritelmän merkinnöin*

$$[\mathcal{A} : K] = [\mathcal{A}_\mathfrak{p} : K_\mathfrak{p}].$$

Seuraavan Wedderburnin lauseen mukaan yksinkertaisten keskeisten algebrojen luokittelu palautuu jakoalgebrojen tapaukseen.

Lause 3.26. *Olkoon $\mathcal{A}$ yksinkertainen K-keskeinen algebra. Tällöin*

$$\mathcal{A} \cong \mathcal{M}_n(\mathcal{D}),$$

missä $\mathcal{D}$ on jokin K-keskeinen jakoalgebra. Kokonaisluku n ja algebra $\mathcal{D}$ ovat (isomorfiaa vaille) yksikäsitteisesti määrättyjä.

Määritelmä 3.27. Olkoon $\mathcal{A}$ kuten edellisessä lauseessa. Kokonaislukua $\sqrt{[\mathcal{D} : K]}$ kutsutaan algebran $\mathcal{A}$ *indeksiksi*.

Olkoon edelleen K lukukunta ja $K_\mathfrak{p}$ sen täydellistymä alkuihanteen $\mathfrak{p}$ suhteen. Lauseen 3.26 mukaan $K_\mathfrak{p} \otimes_K \mathcal{A} \cong \mathcal{M}_s(\mathcal{D}_\mathfrak{p})$, missä $\mathcal{D}_\mathfrak{p}$ on jokin $K_\mathfrak{p}$-keskeinen jakoalgebra. Tarkastellaan seuraavaksi tällaisia jakoalgebroja.

Lause 3.28. *Syklinen algebra*

$$\mathcal{A}(n,r) = (L/K_\mathfrak{p}, \sigma, \pi^r), \;\; (r,n) = 1, \;\; 0 \leqslant r < n,$$

missä L on yksikäsitteinen täydellistymän $K_\mathfrak{p}$ astetta n oleva haaroittumaton laajennus, σ on Frobenius-automorfismi ja π on täydellistymän $K_\mathfrak{p}$ alkualkio, on jakoalgebra. Algebrat $\mathcal{A}(n,r_1)$ ja $\mathcal{A}(n,r_2)$ ovat isomorfisia, jos ja vain jos $r_1 = r_2$.

Lause 3.29. *Olkoon $\mathcal{A}$ indeksiä n oleva $K_\mathfrak{p}$-keskeinen jakoalgebra. Tällöin*

$$\mathcal{A} \cong \mathcal{A}(n,r)$$

jollakin luvulla r.

Määritelmä 3.30. Olkoon $\mathcal{A}$ kuten edeltävässä lauseessa. Rationaalilukua r/n kutsutaan algebran $\mathcal{A}$ *Hasse-invariantiksi.*

Koska jokaisella tekijäryhmän $\mathbb{Q}/\mathbb{Z}$ alkiolla on yksikäsitteinen edustaja välillä $[0,1)$, niin voimme samaistaa sivuluokat näiden edustajien kanssa. Hasse-invariantit voidaan siis tulkita tekijäryhmän $\mathbb{Q}/\mathbb{Z}$ alkioiksi. Lause 3.28 voitaisiin myös kirjoittaa ilman rajoitusta $0 \leqslant r < n$ todeten, että algebrat $\mathcal{A}(n,r_1)$ ja $\mathcal{A}(n,r_2)$ ovat isomorfisia, jos ja vain jos $r_1 \equiv r_2 \pmod{n}$. Jos osoittajat r_1 ja r_2 toteuttavat tämän kongruenssin, niin osamäärät r_1/n ja r_2/n ovat saman sivuluokan edustajia.

Määritelmä 3.31. Olkoon K lukukunta ja $\mathfrak{p}$ sen alkuihanne. Olkoon $\mathcal{A}$ yksinkertainen K-keskeinen algebra ja

$$K_\mathfrak{p} \otimes_K \mathcal{A} = \mathcal{M}_{\kappa_\mathfrak{p}}(\mathcal{D}_\mathfrak{p}),$$

missä $\mathcal{D}_\mathfrak{p}$ on $K_\mathfrak{p}$-keskeinen jakoalgebra. Lukua $h_\mathfrak{p} = r_\mathfrak{p}/m_\mathfrak{p}$ kutsutaan algebran $\mathcal{A}$ *Hasse-invariantiksi alkuihanteen $\mathfrak{p}$ suhteen* ja lukua $m_\mathfrak{p}$ *lokaaliksi indeksiksi*. Kokonaisluku $\kappa_\mathfrak{p}$ on *lokaali kapasiteetti alkuihanteen $\mathfrak{p}$ suhteen.*

Huomautus 3.32. Se, että lokaali kapasiteetti ja Hasse-invariantti ovat hyvinmäriteltyjä, seuraa lauseen 3.26 jälkimmäisestä osasta.

Lokaali indeksi $m_\mathfrak{p} = 1$, jos ja vain jos

$$\mathcal{A}_\mathfrak{p} \cong \mathcal{M}_{\kappa_\mathfrak{p}}(K_\mathfrak{p}).$$

Sanomme, että alkuihanne $\mathfrak{p}$ *haaroittuu* algebrassa $\mathcal{A}$, jos vastaava lokaali indeksi ei ole 1.

Lause 3.33. *Olkoon $\mathcal{A}$ yksinkertainen K-keskeinen algebra. On olemassa vain äärellinen määrä kunnan K alkuihanteita $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$, joiden Hasse-invariantit ovat nollasta eroavia. Algebran $\mathcal{A}$ indeksi on yhtä suuri kuin lukujen $m_{\mathfrak{p}_i}$, $i = 1, ..., n$, pienin yhteinen jaettava.*

Hasse-invarianttia kutsutaan *triviaaliksi*, jos se on nolla.

Seuraus 3.34. *Olkoon $\mathcal{A}$ astetta n oleva yksinkertainen K-keskeinen algebra. Jos algebralla $\mathcal{A}$ on sellainen lokaali indeksi $m_{\mathfrak{p}}$, että*

$$m_{\mathfrak{p}} = n,$$

niin $\mathcal{A}$ on jakoalgebra.

3.2.2 Brauerin ryhmä

Seuraavassa yksinkertaisia keskeisiä algebroja käsitellään ryhmän alkioina. Tarvitsemme näitä alun perin Richard Brauerin määrittelemiä ryhmiä joidenkin luokkakuntateoreettisten tulosten esittelemiseen.

Lause 3.35. *Olkoot $\mathcal{A}$ ja $\mathcal{B}$ yksinkertaisia K-keskeisiä algebroja. Tällöin $\mathcal{A} \otimes_K \mathcal{B}$ on yksinkertainen K-keskeinen algebra.*

Tarkastellaan kaikkien yksinkertaisten K-keskeisten algebrojen muodostamaa perhettä. Sanomme, että kaksi yksinkertaista K-keskeistä algebraa $\mathcal{A} = \mathcal{M}_n(\mathcal{D}_\mathcal{A})$ ja $\mathcal{B} = \mathcal{M}_m(\mathcal{D}_\mathcal{B})$ ovat *similaarisia*, $\mathcal{A} \sim \mathcal{B}$, jos $\mathcal{D}_\mathcal{A} \cong \mathcal{D}_\mathcal{B}$. Similaarisuus on selvästi ekvivalenssirelaatio ja sen ekvivalenssiluokkia kutsutaan *similaarisuusluokiksi*. Yksinkertaisen keskeisen algebran $\mathcal{A}$ similaarisuusluokkaa merkitään $[\mathcal{A}]$.

Similaarisuusluokille $[\mathcal{A}]$ ja $[\mathcal{B}]$ määritellään

$$[\mathcal{A}][\mathcal{B}] = [\mathcal{A} \otimes_K \mathcal{B}].$$

Tämä on hyvinmääritelty (siis, jos $\mathcal{A} \sim \mathcal{A}'$ ja $\mathcal{B} \sim \mathcal{B}'$, niin $\mathcal{A} \otimes_K \mathcal{B} \sim \mathcal{A}' \otimes_K \mathcal{B}'$) ja se on assosiatiivinen ja kommutatiivinen tensoritulojen assosiatiivisuuden ja kommutatiivisuuden perusteella. Yksinkertaisten K-keskeisten algebrojen similaarisuusluokat muodostavat ryhmän tämän operaation suhteen. Tätä ryhmää kutsutaan kunnan K *Brauerin ryhmäksi* ja sitä merkitään $\mathrm{Br}(K)$.

K-algebran $\mathcal{A}$ *vasta-algebralla* $\mathcal{A}^{\mathrm{opp}}$ tarkoitetaan algebraa, jolla on sama alkioiden joukko ja additiivinen operaatio, mutta kertolasku $\cdot$ määritellään $\alpha \cdot \beta = \beta\alpha$. Brauerin ryhmän $\mathrm{Br}(K)$ identiteettialkio on luokka $[K]$ ja luokan $[\mathcal{A}]$ käänteisalkio on vasta-algebran $\mathcal{A}^{\mathrm{opp}}$ määräämä similaarisuusluokka.

Similaarisuusluokkien tensoritulon havainnollistamiseksi esitetään seuraava lemma, jonka todistus löytyy kirjasta [4].

Lemma 3.36. *Olkoon L/K syklinen kuntalaajennus. Olkoot $\mathcal{A}_1 = (L/K, \sigma, \gamma_1)$, $\mathcal{A}_2 = (L/K, \sigma, \gamma_2)$ ja $\mathcal{A}_3 = (L/K, \sigma, \gamma_1\gamma_2)$ syklisiä algebroja. Tällöin ryhmässä $Br(K)$ on voimassa*

$$[\mathcal{A}_1][\mathcal{A}_2] = [\mathcal{A}_3].$$

Siis Brauerin ryhmän ryhmäoperaatio vastaa alkioiden γ_i, $i = 1, 2$, tuloa.

Brauerin ryhmän similaarisuusluokkien tulo vastaa Hasse-invarienttien yhteenlaskua modulo 1.

Lause 3.37. *Olkoon K lukukunta, $\mathfrak{p}$ sen alkuihanne ja $K_\mathfrak{p}$ kunnan K täydellistymä. Kuvaus ryhmästä $Br(K_\mathfrak{p})$ additiiviseen ryhmään $\mathbb{Q}/\mathbb{Z}$, joka kuvaa jakoalgebran similaarisuusluokan sen Hasse-invariantiksi, on ryhmäisomorfismi.*

Yksinkertainen keskeinen algebra määräytyy isomorfiaa vaille sen lokalisaatioista kaikkien alkuihanteiden suhteen.

Lause 3.38. *Olkoon K lukukunta, $\mathcal{P}_K$ kaikkien kunnan K alkuihanteiden muodostama perhe ja olkoot $\mathcal{A}$ ja $\mathcal{B}$ yksinkertaisia K-keskeisiä algebroja. Tällöin*

$$\mathcal{A} \sim \mathcal{B} \Longleftrightarrow \mathcal{A}_\mathfrak{p} \sim \mathcal{B}_\mathfrak{p}, \quad \forall\ \mathfrak{p} \in \mathcal{P}_K.$$

Nyt voimme esitellä seuraavan kuvauksen.

Lemma 3.39. *Olkoon $\mathcal{A}$ yksinkertainen K-keskeinen algebra ja $\mathfrak{p}$ kunnan K alkuihanne. Kuvaus*

$$\mathcal{A} \longmapsto K_\mathfrak{p} \otimes_K \mathcal{A}$$

on ryhmähomomorfismi ryhmästä $Br(K)$ ryhmään $Br(K_\mathfrak{p})$.

Lause 3.40 antaa konkreettisemman kuvan edeltävästä homomorfismista.

Lause 3.40. *Olkoon L/K syklinen laajennus, $Gal(L/K) = \langle\sigma\rangle$ ja $a \in K$. Olkoon E mikä tahansa kunta, joka sisältää kunnan K, ja olkoon EL kuntien E ja L kompositio jonkin laajemman kunnan sisällä. Tällöin pätee*

$$H = \langle\sigma^k\rangle = Gal(L/L \cap E) \cong Gal(EL/E),$$

missä k on pienin sellainen positiivinen kokonaisluku, että σ^k kuvaa joukon $L \cap E$ itselleen. Tällöin

$$E \otimes_K (L/K, \sigma, a) \sim (EL/E, \sigma^k, a).$$

3.2.3 Diskriminanttirajan todistaminen

Tässä pykälässä puhutaan lukukunnan K kokonaislukujen renkaan ihanteen koosta. Tällä tarkoitetaan, että renkaan $\mathcal{O}_K$ ihanteet ovat järjestetty niiden normin mukaan. Sanotaan, että ihanne $\mathfrak{a}_1$ on *pienempi* kuin ihanne $\mathfrak{a}_2$, jos $N(\mathfrak{a}_1) < N(\mathfrak{a}_2)$.

Tulemme johtamaan eksplisiittisen kaavan jakoalgebran, jonka keskus on annettu lukukunta K ja indeksi annettu luku n, pienimmälle mahdolliselle diskriminantille. Diskriminanttirajan todistamisessa tärkeässä roolissa on seuraava syvällinen tulos luokkakuntateoriasta. Olkoon lukukunta K *täysin imaginäärinen*, eli toisin sanoen sitä ei voida upottaa reaalilukujen kuntaan. Tällöin ryhmistä ja ryhmähomomorfismeista koostuva jono

$$0 \longrightarrow \mathrm{Br}(K) \xrightarrow{f} \oplus \mathrm{Br}(K_\mathfrak{p}) \xrightarrow{g} \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \tag{8}$$

on eksakti.

Tässä f kuvaa yksinkertaisen K-keskeisen algebran $\mathcal{A}$ similaarisuusluokan vektoriksi, joka koostuu lokalisaatioiden $\mathcal{A}_\mathfrak{p}$ similaarisuusluokista, missä $\mathfrak{p}$ käy läpi kaikki kokonaislukujen renkaan $\mathcal{O}_K$ alkuihanteet. Tämän kuvauksen injektiivisyys todettiin lauseessa 3.38, ja sen hyvinmääriteltävyys seuraa lemmasta 3.39 ja lauseesta 3.33.

Kyseisen jonon toinen epätriviaali kuvaus g on yksinkertaisesti lauseen 3.37 mukainen Brauerin ryhmien $\mathrm{Br}(K_\mathfrak{p})$ alkioita edustavien jakoalgebrojen $\mathcal{A}_\mathfrak{p}$ Hasse-invarienttien summa.

Jonon (8) eksaktisuudesta seuraa, että yskinkertaisen keskeisen algebran epätriviaalien Hasse-invarienttien summa on kokonaisluku. Lisäksi tämä on ainut rajoitus Hasse-invarianteille. Mikä tahansa yhdistelmä Hasse-invariantteja $(a/m_\mathfrak{p})$, joista vain äärellinen määrä on nollasta eroavia ja joiden summa on kokonaisluku, on siis jonkin yksinkertaisen K-keskeisen algebran Hasse-invarienttien joukko.

Lemma 3.41. *Olkoon K lukukunta, $\mathcal{A}$ K-keskeinen jakoalgebra ja Λ algebran $\mathcal{A}$ maksimaalinen $\mathcal{O}_K$-järjestö. Tällöin*

$$d(\Lambda/\mathcal{O}_K) = \left(\prod_\mathfrak{p} \mathfrak{p}^{(m_\mathfrak{p}-1)\kappa_\mathfrak{p}} \right)^{\sqrt{[\mathcal{A}:K]}},$$

missä $\mathfrak{p}$ käy läpi kaikki renkaan $\mathcal{O}_K$ alkuihanteet, $m_\mathfrak{p}$ on algebran $\mathcal{A}$ lokaali indeksi alkuihanteen $\mathfrak{p}$ suhteen ja $\kappa_\mathfrak{p}$ on algebran $\mathcal{A}$ lokaali kapasiteetti alkuihanteen $\mathfrak{p}$ suhteen.

Lause 3.42. *Olkoon K täysin imaginäärinen lukukunta ja olkoot $\mathfrak{p}_1, .., \mathfrak{p}_n$ sen alkuihanteita. Oletetaan, että rationaaliluvut $a_1/m_{\mathfrak{p}_1}, ..., a_n/m_{\mathfrak{p}_n}$ toteuttavat ehdot*

$$\sum_{i=1}^{n} \frac{a_i}{m_{\mathfrak{p}_i}} \equiv 0 \pmod 1,$$

$1 \leq a_i \leq m_{\mathfrak{p}_i}$ *ja* $(a_i, m_{\mathfrak{p}_i}) = 1$.

Tällöin on olemassa K-keskeinen jakoalgebra $\mathcal{A}$, jonka indeksi on lukujen $m_{\mathfrak{p}_i}$ pienin yhteinen jaettava ja jolla on lokaalit indeksit $m_{\mathfrak{p}_i}$. Jos Λ on jakoalgebran $\mathcal{A}$ maksimaalinen $\mathcal{O}_K$-järjestö, niin järjestön Λ diskriminantti on

$$d(\Lambda/\mathcal{O}_K) = \prod_{i=1}^{n} \mathfrak{p}_i^{(m_{\mathfrak{p}_i}-1)\frac{[\mathcal{A}:K]}{m_{\mathfrak{p}_i}}}. \tag{9}$$

Todistus. Jonon (8) eksaktisuudesta seuraa, että on olemassa K-keskeinen jakoalgebra $\mathcal{A}$, jolla on lokaalit indeksit $m_{\mathfrak{p}_i}$. Tiedämme myös, että indeksi $\sqrt{[\mathcal{A}:K]}$ on yhtä suuri kuin lokaalien indeksien $m_{\mathfrak{p}_i}$ pienin yhteinen jaettava. Lemman 3.41 mukaan

$$d(\Lambda/\mathcal{O}_K) = \left(\prod_{i=1}^{n} \mathfrak{p}_i^{(m_{\mathfrak{p}_i}-1)\kappa_{\mathfrak{p}_i}} \right)^{\sqrt{[\mathcal{A}:K]}}, \tag{10}$$

missä $\kappa_{\mathfrak{p}_i}$ on lokaali kapasiteetti.

Dimensioita laskemalla nähdään, että

$$\kappa_{\mathfrak{p}} = \frac{\sqrt{[\mathcal{A}:K]}}{m_{\mathfrak{p}}}.$$

Sijoittamalla tämä kaavaan (10) saadaan väite. □

Nyt on selvää, että jakoalgebran diskriminantti $d(\Lambda)$ riippuu vain sen lokaaleista indekseistä $m_{\mathfrak{p}_i}$.

Oletetaan, että keskus K ja indeksi n ovat annetut. Seuraavaksi pitää ratkaista, miten lokaalit indeksit ja Hasse-invariantit voidaan valita niin, että lokaalien indeksien pienin yhteinen jaettava on n, Hasse-invarianttien summa on kokonaisluku ja saatava diskriminantti on niin pieni kuin mahdollista. Näemme heti, että ainakin kahden Hasse-invariantin tulee olla kokonaisluvusta eroava.

Alkuihanteen $\mathfrak{p}$ eksponentti $d(\mathfrak{p})$ diskriminanttikaavassa (9) on

$$d(\mathfrak{p}) = (m_{\mathfrak{p}} - 1)\frac{[\mathcal{A}:K]}{m_{\mathfrak{p}}} = n^2 \left(1 - \frac{1}{m_{\mathfrak{p}}}\right).$$

Koska epätriviaaleilla Hasse-invarianteilla $n \geq m_{\mathfrak{p}} \geq 2$, niin $n^2/2 \leq d(\mathfrak{p}) \leq n(n-1)$. Esimerkiksi, kun $n = 6$, niin $d(\mathfrak{p})$ on $18, 24$ tai 30 riippuen siitä, onko $m_{\mathfrak{p}}$ $2, 3$ vai 6.

Osoittautuu, että optimaalisinta on valita vain kaksi epätriviaalia Hasse-invarianttia ja yhdistää ne renkaan $\mathcal{O}_K$ kahteen pienimpään alkuihanteeseen.

Lause 3.43 (**Diskriminanttiraja**). *Olkoon K täysin imaginäärinen lukukunta, jonka pienimmät alkuihanteet ovat $\mathfrak{p}_1$ ja $\mathfrak{p}_2$. Indeksiä n olevan K-keskeisen jakoalgebran pienin mahdollinen diskriminantti on*

$$(\mathfrak{p}_1\mathfrak{p}_2)^{n(n-1)}.$$

Todistus. Lauseen 3.42 mukaan jakoalgebran, jonka Hasse-invariantit alkuihanteiden $\mathfrak{p}_1$ ja $\mathfrak{p}_2$ suhteen ovat $1/n$ ja $(n-1)/n$, diskriminantti on $(\mathfrak{p}_1\mathfrak{p}_2)^{n(n-1)}$. Täytyy siis vain näyttää, että tämä on pienin mahdollinen. Kun jakoalgebralla on vain kaksi epätriviaalia Hasse-invarianttia, niin niiden lokaalien indeksien täytyy olla yhtä suuria kuin n. Emme siis voi saada kahdella Hasse-invariantilla rajaa $(\mathfrak{p}_1\mathfrak{p}_2)^{n(n-1)}$ pienempää diskriminanttia.

Näytetään seuraavaksi, että minimoidaksemme diskriminantin epätriviaaleja Hasse-invarientteja ei voi olla enempää kuin kolme. Alkuihanteille $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$, jotka ovat listattu pienimmästä suurimpaan, pätee aina

$$\mathfrak{p}_1^{d(\mathfrak{p}_1)}\mathfrak{p}_2^{d(\mathfrak{p}_2)}\mathfrak{p}_3^{d(\mathfrak{p}_3)}\mathfrak{p}_4^{d(\mathfrak{p}_4)} > (\mathfrak{p}_1\mathfrak{p}_2)^{n(n-1)},$$

sillä eksponentit $d(\mathfrak{p}_i) \geq n^2/2$ riippumatta Hasse-invarienttien arvoista. Tarkastellaan seuraavaksi kolmen epätriviaalin Hasse-invariantin $(a_i/m_{\mathfrak{p}_i})$, $i = 1, 2, 3$, tapausta. Oletetaan, että jakoalgebralla $\mathcal{D}$ on nämä kolme epätriviaalia Hasse-invarianttia alkuihanteiden $\mathfrak{p}_1, \mathfrak{p}_2$ ja $\mathfrak{p}_3$ suhteen.

Oletetaan ensin, että lokaalilla indeksillä $m_{\mathfrak{p}_1}$ on vain yksi alkutekijä p, eli $m_{\mathfrak{p}_1} = p^t, t > 0$. Kirjoitetaan $m_{\mathfrak{p}_2} = c_2p^a$ ja $m_{\mathfrak{p}_3} = c_3p^b$, missä $(c_2, p) = 1$ ja $(c_3, p) = 1$. Voidaan olettaa, että $a \leq b$. Koska Hasse-invarienttien summa

$$\frac{a_1}{p^t} + \frac{a_2}{c_2p^a} + \frac{a_3}{c_3p^b} = \frac{a_1c_2c_3p^{a+b} + a_2c_3p^{b+t} + a_3c_2p^{a+t}}{p^{t+a+b}c_2c_3}$$

on rationaalinen kokonaisluku, niin c_2 jakaa tämän summan osoittajan. Seuraa, että c_2 jakaa myös termin $a_2c_3p^{b+t}$ ja edelleen c_2 jakaa luvun c_3. Vastaavasti nähdään, että c_3 jakaa luvun c_2, joten $c_2 = c_3$.

Merkitään $c_2 = c_3 = c$. Laventamalla taas Hasse-invariantit samannimisiksi nähdään, että p^{t+a+b} jakaa luvun $a_1cp^{a+b} + a_2p^{b+t} + a_3p^{a+t}$. Tällöin siis p^{b+t} jakaa luvun $a_1cp^b + a_2p^{b-a+t} + a_3p^t$, sillä oletimme $a \leq b$. Tämä

on mahdollista vain, jos $t = b$ tai $a = b > t$. Molemmissa tapauksissa $m_{\mathfrak{p}_3} = \text{pyj}(m_{\mathfrak{p}_1}, m_{\mathfrak{p}_2})$, joten $m_{\mathfrak{p}_3} = \text{pyj}(m_{\mathfrak{p}_1}, m_{\mathfrak{p}_2}, m_{\mathfrak{p}_3}) = n$.

Merkitään alkuihanteista $\mathfrak{p}_1$ ja $\mathfrak{p}_2$ pienempää symbolilla $\mathfrak{p}'$. Näytetään, että diskriminantista tulee pienempi, jos alkuihanteen $\mathfrak{p}'$ Hasse-invariantiksi valitaan

$$a_1/m_{\mathfrak{p}_1} + a_2/m_{\mathfrak{p}_2} = a'/m'_{\mathfrak{p}'} \pmod 1.$$

Olkoon $\mathcal{D}'$ jakoalgebra, jonka ainoat epätriviaalit Hasse-invariantit ovat $a'/m'_{\mathfrak{p}'}$ alkuihanteen $\mathfrak{p}'$ suhteen ja $a_3/m_{\mathfrak{p}_3}$ alkuihanteen $\mathfrak{p}_3$ suhteen. Koska $a'/m'_{\mathfrak{p}'} + a_3/m_{\mathfrak{p}_3}$ on kokonaisluku, niin nähdään, että $m'_{\mathfrak{p}'} = m_{\mathfrak{p}_3}$. Näin ollen jakoalgebran $\mathcal{D}'$ indeksi n' on $n' = m_{\mathfrak{p}_3} = n$. Koska $d(\mathfrak{p}_1) + d(\mathfrak{p}_2) > n(n-1) \geq d'(\mathfrak{p}')$, missä $d'(\mathfrak{p}')$ on lokaalia indeksiä $m'_{\mathfrak{p}'}$ vastaava eksponentti, niin jakoalgebralla $\mathcal{D}'$ on pienempi diskriminantti kuin algebralla $\mathcal{D}$.

Käsittelemättä on enää tapaus, jossa kaikilla kolmella lokaalilla indeksillä on vähintään kaksi eri alkutekijää. Tässä tapauksessa jokaisen lokaalin indeksin suuruus on vähintään 6. Tällöin $d(\mathfrak{p}_1) + d(\mathfrak{p}_2) + d(\mathfrak{p}_3) > 2n(n-1)$, joten myös nyt diskriminantti ylittää alarajan $(\mathfrak{p}_1\mathfrak{p}_2)^{n(n-1)}$. □

Huomautus 3.44. Diskriminanttirajan saavuttava jakoalgebra ei missään nimessä ole yksikäsitteinen. Esimerkiksi mikä tahansa pari Hasse-invariantteja $a/n, (n-a)/n$, missä $0 < a < n$ ja $(a, n) = 1$, johtaa jakoalgebraan, jolla on sama diskriminantti.

3.3 Minimaalidiskriminanttisten jakoalgebrojen konstruointi

Konstruoimme tässä luvussa kaikilla indekseillä, jotka eivät ole jaollisia luvulla 2 tai 7, lauseen 3.43 diskriminanttirajan saavuttavan $\mathbb{Q}(\sqrt{-7})$-keskeisen jakoalgebran. Konstruktio seuraa artikkelia [18], jossa on käsitelty erityisesti $\mathbb{Q}(i)$- ja $\mathbb{Q}(\sqrt{-3})$-keskeisten minimaalidiskriminanttisten jakoalgebrojen konstruointia.

Seuraavien kahden lauseen perusteella meidän tarvitsee tarkastella vain tilannetta, jossa indeksi n on jonkin alkuluvun potenssi.

Lause 3.45 on todistettu kirjassa [1].

Lause 3.45. *Olkoot $\mathcal{D}_1 = (L_1/K, \sigma_1, \gamma_1)$ ja $\mathcal{D}_2 = (L_2/K, \sigma_2, \gamma_2)$ jakoalgebroja, joiden indeksit ovat vastaavasti n_1 ja n_2. Oletetaan, että $(n_1, n_2) = 1$. Tällöin $\mathcal{D}_1 \otimes \mathcal{D}_2$ on jakoalgebra, jonka indeksi on $n_1 n_2$. Lisäksi*

$$\mathcal{D}_1 \otimes \mathcal{D}_2 \cong (L_1L_2/K, \sigma_1\sigma_2, \gamma_1^{n_2}\gamma_2^{n_1}),$$

missä $\sigma_1\sigma_2$ on Galois'n ryhmän $Gal(L_1L_2/K) \cong Gal(L_1/K) \times Gal(L_2/K)$ alkio.

Lause 3.46. *Olkoot $\mathcal{D}_1$ ja $\mathcal{D}_2$ kuten edeltävässä lauseessa ja olkoot $\mathfrak{p}_1$ ja $\mathfrak{p}_2$ kunnan K kaksi pieninormisinta alkuihannetta. Jos jakoalgebrojen $\mathcal{D}_1$ ja $\mathcal{D}_2$ diskriminantit ovat minimaalisia ja ne ovat jaollisia vain alkuihanteilla $\mathfrak{p}_1$ ja $\mathfrak{p}_2$, niin jakoalgebralla $\mathcal{D}_1 \otimes \mathcal{D}_2$ on minimaalinen diskriminantti, joka on jaollinen vain alkuihanteilla $\mathfrak{p}_1$ ja $\mathfrak{p}_2$.*

Todistus. Alkuihanteiden $\mathfrak{p}_1$ ja $\mathfrak{p}_2$ Hasse-invariantit ovat jakoalgebrojen $\mathcal{D}_1$ ja $\mathcal{D}_2$ ainoat epätriviaalit Hasse-invariantit. Eksaktin jonon (8) kuvaukset ovat ryhmähomomorfismeja. Tästä sekä siitä, että skalaarien laajentaminen täydellistymiin $K_\mathfrak{p}$ kommutoi tensoritulon muodostamisen kanssa, seuraa, että jakoalgebran $\mathcal{D}_1 \otimes \mathcal{D}_2$ Hasse-invariantit ovat algebrojen $\mathcal{D}_1$ ja $\mathcal{D}_2$ Hasse-invarianttien summia. Tämän vuoksi jakoalgebran $\mathcal{D}_1 \otimes \mathcal{D}_2$ diskriminantti on jaollinen vain alkuihanteilla $\mathfrak{p}_1$ ja $\mathfrak{p}_2$. Lauseen 3.43 todistuksen perusteella kyseinen diskriminantti on minimaalinen. □

Seuraava lemma mukailee artikkelissa [8] esitettyä vastaavankaltaista tulosta.

Lemma 3.47. *Olkoot L/K Galois'n laajennus ja alkuihanne $\mathfrak{p} \subset \mathcal{O}_K$ alkuihanteen $\mathfrak{P} \subset \mathcal{O}_L$ alla. Jos alkuihanteen $\mathfrak{p}$ jäännösluokka-aste laajennuksessa L/K on f ja γ on sellainen kunnan K alkio, että $(v_\mathfrak{p}(\gamma), f) = 1$, niin $\gamma^i \notin \mathcal{N}_{L/K}(L)$ jokaisella $i = 1, 2, ..., f-1$.*

Todistus. Oletetaan, että $\gamma^j \in \mathcal{N}_{L/K}(L)$ jollakin $j \in \{1, ..., f-1\}$. Olkoon $\alpha \in \mathfrak{P}$ sellainen, että $\mathcal{N}_{L/K}(\alpha) = \gamma^j$. Koska normi on multiplikatiivinen kuntatorneissa, niin

$$\mathcal{N}_{L/\mathbb{Q}}(\alpha) = \mathcal{N}_{K/\mathbb{Q}}(\mathcal{N}_{L/K}(\alpha)) = \mathcal{N}_{K/\mathbb{Q}}(\gamma^j) = N([\gamma^j]).$$

Toisaalta $|\mathcal{N}_{K/\mathbb{Q}}(\gamma^j)| = N([\gamma^j])$ ja $N(\mathfrak{p})^f = N(\mathfrak{P}) \mid \mathcal{N}_{L/\mathbb{Q}}(\alpha)$, mikä on ristiriita, sillä jäännösluokka-aste f ei jaa lukua $j \cdot v_\mathfrak{p}(\gamma)$. □

Erityisesti edeltävästä lemmasta ja lauseesta 3.8 seuraa, että jos alkuihanne $\mathfrak{p} \subset K$ on hidas syklisessä laajennuksessa L/K, $[L : K] = n$ ja $(v_\mathfrak{p}(\gamma), n) = 1$, niin syklinen algebra $(L/K, \sigma, \gamma)$ on jakoalgebra.

Lemma 3.48. *Olkoon L/K syklinen kuntalaajennus ja $\mathfrak{p}$ kunnan K alkuihanne, joka on hidas laajennuksessa L/K. Olkoon*

$$\mathcal{A} = (L/K, \sigma, \gamma)$$

jakoalgebra, missä $\gamma \in K^*$, $[L : K] = n$ ja σ on alkuihanteen $\mathfrak{p}$ Frobenius-automorfismi. Tällöin Hasse-invariantti

$$h_\mathfrak{p} = \frac{v_\mathfrak{p}(\gamma)}{n}.$$

Todistus. Olkoon $\mathfrak{P} = \mathfrak{p}\mathcal{O}_L$. Lauseen 3.40 mukaan

$$\mathcal{A}_\mathfrak{p} \sim (L_\mathfrak{P}/K_\mathfrak{p}, \sigma, \gamma).$$

Koska $\mathfrak{p}$ on haaroittumaton laajennuksessa L/K, niin $L_\mathfrak{P}/K_\mathfrak{p}$ on haaroittumaton laajennus. Jos kunnassa $K_\mathfrak{p}$ pätee $\gamma = \epsilon\pi^t$, missä ϵ on renkaan $\mathcal{O}_\mathfrak{p}$ yksikkö ja π on kunnan $K_\mathfrak{p}$ alkualkio, niin $v_\mathfrak{p}(\gamma) = t$. Hasse-invariantin määritelmästä ja lauseesta 3.28 nähdään nyt, että

$$h_\mathfrak{p} = \frac{v_\mathfrak{p}(\gamma)}{n}.$$

□

Käytetään merkintää $\mathbb{Z}_m$ jäännösluokkarenkaasta modulo m, eli $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. Tämän renkaan yksiköiden muodostama ryhmä on siis $\mathbb{Z}_m^*$.

Lemma 3.49. *Jos p on alkuluku ja n kokonaisluku, $n \mid (p-1)$, niin kunnalla $\mathbb{Q}(\zeta_p)$ on yksikäsitteinen alikunta Z, jonka aste $[Z : \mathbb{Q}] = n$.*

Laajennus $Z/\mathbb{Q}$ on Galois'n laajennus ja on myös olemassa ryhmäisomorfismi ϕ ryhmästä $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^n$ ryhmään $Gal(Z/\mathbb{Q})$, joka kuvaa alkuluvun $q \neq p$ vastaavaksi Frobenius-automorfismiksi $((Z/\mathbb{Q}), q)$.

Lisäksi alkuluku $q \neq p$ on hidas laajennuksessa $Z/\mathbb{Q}$, jos ja vain jos q^t ei ole ns potenssi $(mod\ p)$ millään $t = 1, ..., n-1$.

Todistus. Ympyräkuntien teoriasta tiedetään, että (ks. esim. [12])

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}_p^*.$$

Tämän isomorfismin välittää kuvaus, joka kuvaa ehdolla $\tau_a(\zeta_p) = \zeta_p^a$, $1 \leq a \leq p-1$, määritellyn Galois'n ryhmän automorfismin τ_a renkaan $\mathbb{Z}_p^*$ alkioksi a. Frobenius-automorfismi $((\mathbb{Q}(\zeta_p)/\mathbb{Q}), q)$ voidaan määritellä kaavalla

$$((\mathbb{Q}(\zeta_p)/\mathbb{Q}), q)(\zeta_p) = \zeta_p^q.$$

On siis olemassa isomorfismi $\psi : \mathbb{Z}_p^* \to \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, joka kuvaa alkuluvun $q \neq p$ Frobenius-automorfismiksi $((\mathbb{Q}(\zeta_p)/\mathbb{Q}), q)$. Käytetään ryhmän $\psi(\mathbb{Z}_p^*)^n$ kiintokunnasta merkintää Z. Nyt on selvää, että Z on yksikäsitteinen ja $[Z : \mathbb{Q}] = n$. Jos ensin kuvataan ryhmän $\mathbb{Z}_p^*$ alkiot kuvauksella ψ ryhmään $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ ja sitten otetaan näiden automorfismien rajoittuma kuntaan Z, niin saadaan isomorfismi ϕ ryhmästä $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^n$ ryhmään $\mathrm{Gal}(Z/\mathbb{Q})$. Lauseen 2.27 mukaan kuvauksella ϕ on väitetyt ominaisuudet.

Viimeinen väittämä saadaan seurauksesta 2.26, sillä $((Z/\mathbb{Q}), q)$ generoi ryhmän $\mathrm{Gal}(Z/\mathbb{Q})$, jos ja vain jos q^t ei ole ns potenssi (mod p) millään $t = 1, ..., n-1$. □

Käytetään jatkossa merkintöjä $F = \mathbb{Q}(\sqrt{-7})$, $\mathfrak{p}_1 = \left[2, \frac{1+\sqrt{-7}}{2}\right]$ ja $\mathfrak{p}_2 = \left[2, \frac{1-\sqrt{-7}}{2}\right]$. Ihanteet $\mathfrak{p}_1$ ja $\mathfrak{p}_2$ ovat alkuluvun 2 päällä kunnassa F olevat alkuihanteet ja ne ovat myös kunnan F pieninormisimmat alkuihanteet.

Lause 3.50. *Olkoon $q \neq 2$ alkuluku, n jokin kokonaisluku ja $p \neq 7$ alkuluku, jolle pätee $q^n \mid (p-1)$. Oletetaan, että luku 2 on hidas laajennuksessa $Z/\mathbb{Q}$, missä Z on kunnan $\mathbb{Q}(\zeta_p)$ yksikäsitteinen astetta q^n oleva alikunta, ja oletetaan myös, että p on hidas laajennuksessa $F/\mathbb{Q}$. Tällöin FZ/F on astetta q^n oleva syklinen Galois'n laajennus, missä alkuihanteet $\mathfrak{p}_1$ ja $\mathfrak{p}_2$ ovat hitaita ja $\mathfrak{p} = p\mathcal{O}_F$ on ainut haaroittuva alkuihanne laajennuksessa FZ/F.*

Todistus. Koska $7 \nmid q$, niin F ei ole kunnan Z alikunta, ja siis $[FZ : F] = q^n$. Koska $F/\mathbb{Q}$ ja $Z/\mathbb{Q}$ ovat Galois'n laajennuksia, niin myös $FZ/\mathbb{Q}$ on Galois ja edelleen FZ/F on Galois. Lemman 3.49 mukaan $Z/\mathbb{Q}$ on syklinen laajennus, sillä $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^n$ on syklinen laajennus. Laajennuksen $Z/\mathbb{Q}$ syklisyydestä seuraa, että myös FZ/F on myös syklinen.

Olkoon $\mathfrak{P}$ kunnan FZ alkuihanne, $\mathfrak{p}_Z = \mathcal{O}_Z \cap \mathfrak{P}$, $\mathfrak{p}_F = \mathcal{O}_F \cap \mathfrak{P}$ ja $b = \mathbb{Q} \cap \mathfrak{P}$. Lauseen 2.8 mukaan

$$e(\mathfrak{P}|\mathfrak{b}) = e(\mathfrak{P}|\mathfrak{p}_Z)e(\mathfrak{p}_Z|b) = e(\mathfrak{P}|\mathfrak{p}_F)e(\mathfrak{p}_F|b).$$

Koska lisäksi $e(\mathfrak{P}|\mathfrak{p}_Z)$, $e(\mathfrak{p}_F|b) \mid 2$ ja $e(\mathfrak{p}_Z|b)$, $e(\mathfrak{P}|\mathfrak{p}_F) \mid q^n$, niin nähdään, että alkuihanne $\mathfrak{p}_F$ haaroittuu laajennuksessa FZ/F, jos ja vain jos alkuluku b haaroittuu laajennuksessa $Z/\mathbb{Q}$.

Koska p haaroittuu laajennuksessa $Z/\mathbb{Q}$ ja p on hidas kunnassa F, niin nähdään, että $\mathfrak{p}$ on ainut haaroittuva alkuihanne laajennuksessa ZF/F.

Jos $\mathfrak{P}$ valitaan niin, että $\mathfrak{p}_F = \mathfrak{p}_1$ tai $\mathfrak{p}_F = \mathfrak{p}_2$, saadaan

$$f(\mathfrak{P}|2) = f(\mathfrak{P}|\mathfrak{p}_Z)f(\mathfrak{p}_Z|2) = f(\mathfrak{P}|\mathfrak{p}_F)f(\mathfrak{p}_F|2) = q^n,$$

sillä oletuksen mukaan luku 2 on hidas laajennuksessa $Z/\mathbb{Q}$ ja $f(\mathfrak{p}_F|2) = 1$. Tällöin siis $f(\mathfrak{P}|\mathfrak{p}_F) = q^n$, josta seuraa, että $\mathfrak{p}_1$ ja $\mathfrak{p}_2$ ovat hitaita laajennuksessa FZ/F.

□

Seuraavassa käytetään lauseen 3.50 merkintöjä.

Lemma 3.51. *On olemassa sellainen ryhmäisomorfismi ρ joukolta $Gal(FZ/F)$ joukolle $Gal(Z/\mathbb{Q})$, että*

$$\rho\left(\left(\frac{FZ/F}{\mathfrak{p}_i}\right)\right) = \left(\frac{Z/\mathbb{Q}}{2}\right).$$

Todistus. Galois'n teoriasta tiedetään, että on olemassa surjektiivinen ryhmähomomorfismi

$$\sigma : \mathrm{Gal}(FZ/\mathbb{Q}) \longrightarrow \mathrm{Gal}(Z/\mathbb{Q}),$$

missä $\sigma(\tau) = \tau_{|Z}$. Tämän kuvauksen ytimeen kuuluvat ne ryhmän $\mathrm{Gal}(FZ/\mathbb{Q})$ alkiot, jotka operoivat triviaalisti kunnassa Z. Toisaalta, jos kuvauksen σ määrittelyjoukko rajoitetaan niihin alkiohin, jotka operoivat triviaalisti kunnassa F, niin saadaan injektio, sillä ainut ryhmän $\mathrm{Gal}(FZ/\mathbb{Q})$ alkio, joka operoi triviaalisti molemmissa kunnissa F ja Z, on identiteettikuvaus. Koska $|\mathrm{Gal}(FZ/F)| = |\mathrm{Gal}(Z/\mathbb{Q})|$, niin kyseisen kuvauksen täytyy olla isomorfismi.

Osoitetaan vielä Frobenius-automorfismia koskeva väite. Ensinnäkin merkinnät $(FZ/F, \mathfrak{p}_i)$, $i \in \{1, 2\}$, ja $(Z/\mathbb{Q}, 2)$ ovat mielekkäitä, koska kyseiset laajennukset ovat syklisiä ja alkuihanteet $\mathfrak{p}_i$ ja 2 eivät haaroitu näissä. Olkoon x kunnan Z algebrallinen kokonaisluku ja $\mathfrak{P}_i$ kunnan L alkuihanne, $\mathfrak{P}_i \cap \mathcal{O}_F = \mathfrak{p}_i$. Määritelmän mukaan

$$x^{N(\mathfrak{p}_i)} \equiv \left(\frac{FZ/F}{\mathfrak{p}_i}\right)(x) \pmod{\mathfrak{P}_i}.$$

Merkitään $\mathfrak{p}_Z = \mathfrak{P}_1 \cap \mathcal{O}_Z = \mathfrak{P}_2 \cap \mathcal{O}_Z$. Koska $N(\mathfrak{p}_i) = 2$ ja

$$x^2 \equiv \left(\frac{Z/\mathbb{Q}}{2}\right)(x) \pmod{\mathfrak{p}_Z},$$

niin

$$\left(\frac{FZ/F}{\mathfrak{p}_i}\right)(x) \equiv \left(\frac{Z/\mathbb{Q}}{2}\right)(x) \pmod{\mathfrak{p}_Z}.$$

Tämä voi olla voimassa kaikilla $x \in \mathcal{O}_Z$ vain, jos $(FZ/F, \mathfrak{p}_i)$ ja $(Z/\mathbb{Q}, 2)$ yhtyvät. □

Lause 3.52. *Olkoon q pariton alkuluku ja n positiivinen kokonaisluku. Olkoon $p \neq 7$ alkuluku, jolle on voimassa $q^n \mid (p-1)$, ja oletetaan, että p on hidas laajennuksessa $F/\mathbb{Q}$. Oletetaan lisäksi, että alkuluku 2 on hidas laajennuksessa $Z/\mathbb{Q}$, missä Z on yksikäsitteinen astetta q^n oleva kunnan $\mathbb{Q}(\zeta_p)$ alikunta.*

Tällöin

$$\mathcal{A} = \left(FZ/F, \sigma, a_1 a_2^{q^n-1}\right),$$

missä a_i on jokin ihanteen $\mathfrak{p}_i$ generoija ja $\langle\sigma\rangle = Gal(FZ/F)$, on minimaalidiskriminanttinen jakoalgebra.

Todistus. Lauseen 3.50 mukaan $\mathfrak{p}_1$ on hidas laajennuksessa ZF/F. Siis $(v_{\mathfrak{p}_1}(a_1 a_2^{q^n-1}), f) = 1$, missä f on alkuihanteen $\mathfrak{p}_1$ jäännösluokka-aste laajennuksessa ZF/F. Nyt lemmasta 3.47 seuraa, että $\mathcal{A}$ on jakoalgebra.

Ryhmän $\mathrm{Gal}(FZ/F)$ generoivaksi alkioksi σ voidaan valita ihanteen $\mathfrak{p}_1$ Frobenius-automorfismi, sillä huomautuksen 3.23 perusteella alkion σ valinta ei vaikuta jakoalgebran $\mathcal{A}$ diskriminanttiin.

Jakoalgebran $\mathcal{A}$ Hasse-invarianteista ainoastaan $h_{\mathfrak{p}_1}$, $h_{\mathfrak{p}_2}$ ja $h_{\mathfrak{p}}$, missä $\mathfrak{p}$ on laajennuksen FZ/F ainut haaroittuva alkuihanne $p\mathcal{O}_F$, voivat olla epätriviaaleja. Nimittäin, jos $\mathfrak{q}$ on jokin muu kunnan F alkuihanne, niin tällöin $v_{\mathfrak{q}}(a_1 a_2^{q^n-1}) = 0$. Nyt lemmasta 3.48 seuraa, että sen Hasse-invariantti $h_{\mathfrak{q}}$ on triviaali. Näytetään seuraavaksi, että myös Hasse-invariantin $h_{\mathfrak{p}}$ täytyy olla triviaali.

Lemman 3.48 mukaan

$$h_{\mathfrak{p}_1} = \frac{v_{\mathfrak{p}_1}(a_1 a_2^{q^n-1})}{q^n} = \frac{1}{q^n}.$$

Lemman 3.51 perusteella

$$\left(\frac{FZ/F}{\mathfrak{p}_2}\right) = \left(\frac{Z/\mathbb{Q}}{2}\right) = \left(\frac{FZ/F}{\mathfrak{p}_1}\right),$$

joten

$$h_{\mathfrak{p}_2} = \frac{v_{\mathfrak{p}_2}(a_1 a_2^{q^n-1})}{q^n} = \frac{q^n - 1}{q^n}.$$

Koska algebran $\mathcal{A}$ epätriviaalien Hasse-invarienttien summa on kokonaisluku ja edeltävän perusteella $h_{\mathfrak{p}_1} + h_{\mathfrak{p}_2} \in \mathbb{Z}$, niin myös $h_{\mathfrak{p}} \in \mathbb{Z}$. Siis $h_{\mathfrak{p}}$ on triviaali ja jakoalgebran $\mathcal{A}$ diskriminantilla on vain kaksi jakajaa $\mathfrak{p}_1$ ja $\mathfrak{p}_2$. □

Esimerkki 3.53. Konstruoidaan $F = \mathbb{Q}(\sqrt{-7})$-keskeinen indeksiä 9 oleva minimaalidiskriminanttinen jakoalgebra. Renkaan $\mathcal{O}_F$ pieninormisimpien alkuihanteiden $\mathfrak{p}_1$ ja $\mathfrak{p}_2$ generoijiksi voidaan valita vastaavasti $\frac{1+\sqrt{-7}}{2}$ ja $\frac{1-\sqrt{-7}}{2}$. Voidaan helposti tarkistaa, että 2^t ei ole yhdeksäs potenssi (mod 19) millään $t = 1, ...8$ ja että alkuluku 19 on hidas laajennuksessa $\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$. Lemman 3.49 mukaan kunnalla $\mathbb{Q}(\zeta_{19})$ on yksikäsitteinen alikunta Z, $[Z : \mathbb{Q}] = 9$, ja alkuluku 2 on hidas laajennuksessa $Z/\mathbb{Q}$. Nyt lauseen 3.52 perusteella

$$\left(FZ/F, \sigma, \frac{1+\sqrt{-7}}{2}\left(\frac{1-\sqrt{-7}}{2}\right)^8\right)$$

on minimaalidiskriminanttinen jakoalgebra.

Vielä tarvitsee näyttää, että sopivan kaltaisia alkulukuja on olemassa riittävästi. Osoitamme tämän lauseessa 3.57, mutta tätä varten tarvitsemme joitain aputuloksia.

Seuraava lemma perustuu lähteen [7] ns. Kummerin laajennuksiin liittyviin tuloksiin, vaikkakin lemma ja sen todistus ovat täysin uudelleen muotoiltu tarkoitukseemme soveltuviksi.

Lemma 3.54. *Olkoot q alkuluku ja L/K astetta q oleva syklinen Galois'n laajennus, missä $L = K(\alpha)$, $\alpha^q = a \in \mathcal{O}_K$. Oletetaan, että K sisältää $q$nnet ykkösenjuuret ja $\mathfrak{p}$ on kunnan K alkuihanne, $a, q \notin \mathfrak{p}$. Oletetaan lisäksi, että kongruenssilla*

$$x^q \equiv a \pmod{\mathfrak{p}}$$

on ratkaisu b renkaassa $\mathcal{O}_K$. Tällöin alkuihanne $\mathfrak{p}$ ei ole hidas laajennuksessa L/K.

Todistus. Olkoon $f_\alpha(x)$ alkion α minimaalipolynomi yli kunnan K. Jos alkio $c \in \mathcal{O}_K$, niin käytetään merkintää $\overline{c} = c + \mathfrak{p} \in \mathcal{O}_K/\mathfrak{p}$. Koska $b^q \equiv a \pmod{\mathfrak{p}}$, niin $\overline{b^q} = \overline{a}$. Nyt renkaassa $(\mathcal{O}_K/\mathfrak{p})[x]$ saadaan

$$x^q - \overline{a} = \prod_{i=0}^{q-1} (x - \overline{\zeta^i b}),$$

missä ζ on primitiivinen qs ykkösenjuuri. Merkitään $f_i(x) = x - \zeta^i b \in \mathcal{O}_K[x]$, $i = 1, ..., q$, ja

$$\mathfrak{P}_i = (\mathfrak{p}, f_i(\alpha))\mathcal{O}_L,$$

missä siis $(\mathfrak{p}, f_i(\alpha))\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$ jokaisella $i = 1, ..., q$.

Koska

$$f_1(x) \cdots f_q(x) - f_\alpha(x) \in \mathfrak{p}\mathcal{O}_K[x],$$

niin

$$\mathfrak{P}_1 \cdots \mathfrak{P}_q \subseteq \mathfrak{p}\mathcal{O}_L.$$

Siis ainakin yksi ihanteista $\mathfrak{P}_1, ..., \mathfrak{P}_q$ on erisuuri kuin koko rengas $\mathcal{O}_L$; olkoon se $\mathfrak{P}_k$. Jos tämä ei ole alkuihanne, niin silloin myöskään $\mathfrak{p}\mathcal{O}_L$ ei ole alkuihanne, sillä $\mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{P}_k$. Jos $\mathfrak{P}_k$ on alkuihanne, niin sen jäännösluokka-aste $f_{\mathfrak{P}_k|\mathfrak{p}} = \deg(f_i(x)) = 1$, josta seuraa, ettei $\mathfrak{p}$ ole hidas laajennuksessa L/K. □

Lemma 3.55. *Oletetaan, että p ja q ovat alkulukuja ja $q^t \mid (p-1)$ jollakin kokonaisluvulla t. Jos c on kokonaisluku ja yhtälöllä*

$$c \equiv x^q \pmod{p} \tag{11}$$

ei ole ratkaisua, niin myöskään yhtälöillä

$$c^k \equiv x^{q^t} \pmod{p} \tag{12}$$

ei ole ratkaisua millään $k = 1, ..., q^t - 1$.

Todistus. Olkoon a syklisen ryhmän $\mathbb{Z}_p^*$ generoija-alkio. Nyt $c \equiv a^n \pmod{p}$ jollakin kokonaisluvulla n.

Oletetaan, että yhtälöllä (11) ei ole ratkaisuja, jolloin siis q ei ole luvun n tekijä. Tehdään vastaoletus, että jollain luvulla k yhtälöllä (12) on ratkaisu d. Jos kirjoitetaan $d \equiv a^s$, niin yhtälön (12) perusteella $kn - sq^t = v(p-1)$, missä v on jokin kokonaisluku. Koska $q^t \mid (p-1)$, niin saadaan $q^t \mid kn$, mikä on ristiriita. □

Todetaan vielä seuraava ympyräkuntien teoriasta hyvin tunnettu tulos.

Lemma 3.56. *Olkoon p alkuluku. Tällöin*

$$p \text{ lohkeaa täysin laajennuksessa } \mathbb{Q}(\zeta_m)/\mathbb{Q} \iff p \equiv 1 \pmod{m}.$$

Lause 3.57. *Olkoon $q \neq 7$ pariton alkuluku ja n positiivinen kokonaisluku. On olemassa äärettömän monta sellaista alkulukua p, että p on hidas kunnassa F ja ympyräkunnalla $\mathbb{Q}(\zeta_p)$ on yksikäsitteinen alikunta Z, $[Z : \mathbb{Q}] = q^n$, jossa alkuluku 2 on hidas.*

Todistus. Merkitään $K = \mathbb{Q}(\zeta_{q^n})$ ja $K_1 = \mathbb{Q}(\zeta_{q^n})(2^{\frac{1}{q}})$. Koska $[\mathbb{Q}(2^{\frac{1}{q}}) : \mathbb{Q}] = q$ ja q on alkuluku, niin joko $K \subseteq K_1$ tai $K \cap K_1 = \mathbb{Q}$. Siis $[K_1 : K] = 1$ tai q. Jos olisi $[K_1 : K] = 1$, niin siitä seuraisi, että $2^{\frac{1}{q}} \in \mathcal{O}_K$. Tällöin olisi $2 \in \left[2^{\frac{1}{q}}\right]^q$, eli alkuluku 2 haaroittuisi kunnassa K. Tämä on kuitenkin mahdotonta, sillä tunnetusti ympyräkunnassa $\mathbb{Q}(\zeta_{q^n})$ haaroittuu vain alkuluku q. Siis aste $[K_1 : K] = q$.

Koska $7 \nmid q$, niin kunnan F diskriminantti ei jaa kunnan K diskriminanttia, mistä seuraa $F \nsubseteq K$. Koska myös $(2, q) = 1$, niin laajennus K_1F/K on syklinen ja $[K_1F : K] = 2q$.

Merkitään symbolilla $\mathcal{P}_K$ kaikkien kunnan K alkuihanteiden joukkoa ja olkoon $\mathcal{S} \subseteq \mathcal{P}_K$ niiden ihanteiden joukko, jotka ovat hitaita laajennuksessa K_1F/K. Koska K_1F/K on syklinen, niin Tšebotarevin tiheyslauseen seurauksen 2.33 mukaan Dirichlet'n tiheys $\delta(\mathcal{S}) > 0$. Koska lisäksi seurauksen 2.31 perusteella

$$\delta(\mathcal{S}) = \delta(\mathcal{S} \cap \{\mathfrak{q} \in \mathcal{P}_K \mid N(\mathfrak{q}) \text{ on alkuluku}\}),$$

niin on olemassa ääretön määrä sellaisia renkaan $\mathcal{O}_K$ alkuihanteita, joiden jäännösluokka-aste laajennuksessa $K/\mathbb{Q}$ on yksi ja jotka ovat hitaita laajennuksessa K_1F/K. Valitaan niistä yksi, $\mathfrak{p}$, joka on myös haaroittumaton laajennuksessa $K/\mathbb{Q}$.

Olkoon ihanteen $\mathfrak{p}$ alla oleva alkuluku p, jolloin siis p lohkeaa täysin laajennuksessa $K/\mathbb{Q}$. Lemman 3.56 perusteella tällöin

$$p \equiv 1 \pmod{q^n}.$$

Tarkastellaan kongruenssiyhtälöä $2 \equiv x^q \pmod{p}$. Oletetaan, että $2 \equiv b^q \pmod{p}$ jollakin luonnollisella luvulla b, jolloin myös $2 \equiv b^q \pmod{\mathfrak{p}}$. Tämä yhtälö ei kuitenkaan voi olla tosi, koska lemman 3.54 mukaan $\mathfrak{p}$ ei tällöin olisi hidas laajennuksessa K_1/K. Nyt lemma 3.55 kertoo, ettei yhtälöllä $2^t \equiv x^{q^n} \pmod{p}$ ole ratkaisua millään $t = 1, ..., q^n - 1$.

Lemman 3.49 perusteella on olemassa sellainen kunnan $\mathbb{Q}(\zeta_p)$ yksikäsitteinen alikunta Z, jonka aste $[Z : \mathbb{Q}] = q^n$ ja jossa 2 on hidas.

Lopuksi osoitetaan, että p on hidas laajennuksessa $F/\mathbb{Q}$. Koska $\mathfrak{p}$ on hidas laajennuksessa K_1F/K, niin se on hidas myös laajennuksessa KF/K. Alkuluvun p jäännösluokka-aste laajennuksessa $KF/\mathbb{Q}$ on siis suurempi kuin yksi. Kongruenssista $p \equiv 1 \pmod{q^n}$ nähdään, että $p \neq 7$, joten se ei haaroitu kunnassa F. Koska p lohkeaa täysin laajennuksessa $K/\mathbb{Q}$, niin jos se lohkeaisi myös laajennuksessa $F/\mathbb{Q}$, lauseesta 2.22 seuraisi, että p lohkeaa täysin laajennuksessa $KF/\mathbb{Q}$. Tämä on ristiriita, joten alkuluvun p täytyy pysyä hitaana kunnassa F. □

Lauseesta 3.57 seuraa, että pystymme nyt konstruoimaan $\mathbb{Q}(\sqrt{-7})$-keskeisen minimaalidiskriminanttisen jakoalgebran kaikilla sellaisilla indekseillä, jotka eivät ole jaollisia luvulla 2 tai 7. Taulukossa 1 on esitetty eksplisiittisesti pieni-indeksisiä minimaalidiskriminanttisia jakoalgebroja. Jokaisessa niissä epänormialkioksi voidaan valita $\frac{1+\sqrt{-7}}{2}\left(\frac{1-\sqrt{-7}}{2}\right)^{n-1}$. Lauseen 3.57 alkuluku p on etsitty esimerkin 3.53 mukaisella tavalla. Tämän jälkeen laajennuksen $\mathbb{Q}(\sqrt{-7})Z/\mathbb{Q}(\sqrt{-7})$ minimaalipolynomi voidaan helposti löytää tarkastelemalla ympyräkunnan $\mathbb{Q}(\zeta_p)$ alikuntia. Taulukon alkuluvut ja minimaalipolynomit on laskettu tietokonealgebrajärjestelmällä PARI [17].

Esimerkki 3.58. Taulukosta 1 nähdään, että

$$\mathcal{A}_3 = \left(\mathbb{Q}(\sqrt{-7})(a_3)/\mathbb{Q}(\sqrt{-7}), \sigma_3, \frac{1+\sqrt{-7}}{2}\left(\frac{1-\sqrt{-7}}{2}\right)^2\right)$$

ja

$$\mathcal{A}_5 = \left(\mathbb{Q}(\sqrt{-7})(a_5)/\mathbb{Q}(\sqrt{-7}), \sigma_5, \frac{1+\sqrt{-7}}{2} \left(\frac{1-\sqrt{-7}}{2} \right)^4 \right),$$

missä a_3 ja a_5 ovat vastaavasti polynomien $x^3 + x^2 - 4x + 1$ ja $x^5 + x^4 - 16x^3 + 5x^2 + 21x - 9$ nollakohtia, ovat minimaalidiskriminanttisia jakoalgebroja. Lauseiden 3.45 ja 3.46 perusteella algebra

$$\mathcal{A}_3 \otimes \mathcal{A}_5 = \left(\mathbb{Q}(\sqrt{-7})(a_{15})/\mathbb{Q}(\sqrt{-7}), \sigma_3\sigma_5, \left(\frac{1+\sqrt{-7}}{2} \right)^8 \left(\frac{1-\sqrt{-7}}{2} \right)^{22} \right),$$

missä a_{15} on polynomin $x^{15} - 2x^{14} - 69x^{13} + 154x^{12} + 1536x^{11} - 3742x^{10} - 13104x^9 + 32905x^8 + 47584x^7 - 119624x^6 - 71155x^5 + 179526x^4 + 33394x^3 - 87985x^2 + 9x + 2293$ nollakohta, on indeksiä 15 oleva minimaalidiskriminanttinen jakoalgebra.

n	p	f_n
3	13	$x^3 + x^2 - 4x + 1$
5	41	$x^5 + x^4 - 16x^3 + 5x^2 + 21x - 9$
7	43	$x^7 + x^6 - 18x^5 - 35x^4 + 38x^3 + 104x^2 + 7x - 49$
9	19	$x^9 + x^8 - 8x^7 - 7x^6 + 21x^5 + 15x^4 - 20x^3 - 10x^2 + 5x + 1$
11	199	$x^{11} + x^{10} - 90x^9 - 115x^8 + 2349x^7 + 943x^6 - 26327x^5 + 21284x^4 + 102168x^3 - 217794x^2 + 148930x - 30647$
13	53	$x^{13} + x^{12} - 24x^{11} - 19x^{10} + 190x^9 + 116x^8 - 601x^7 - 246x^6 + 738x^5 + 215x^4 - 291x^3 - 68x^2 + 10x + 1$
17	137	$x^{17} + x^{16} - 64x^{15} - 43x^{14} + 1478x^{13} + 932x^{12} - 16008x^{11} - 12183x^{10} + 86347x^9 + 84507x^8 - 213223x^7 - 271237x^6 + 152800x^5 + 314540x^4 + 100605x^3 - 20132x^2 - 13981x - 1681$
19	419	$x^{19} + x^{18} - 198x^{17} - 37x^{16} + 12055x^{15} + 1727x^{14} - 335304x^{13} - 70692x^{12} + 4834266x^{11} + 1201976x^{10} - 37345852x^9 - 7325624x^8 + 153105664x^7 + 3418584x^6 - 328284116x^5 + 65770266x^4 + 325674937x^3 - 129492371x^2 - 92941225x + 41768519$

Taulukko 1: Indeksi n, ympyräkunnan $\mathbb{Q}(\zeta_p)$ johtaja p ja laajennuksen $\mathbb{Q}(\sqrt{-7})(a_n)/\mathbb{Q}(\sqrt{-7})$ minimaalipolynomi f_n.

Kirjallisuutta

[1] A. A. Albert: *Structure of Algebras*. American Mathematical Society. 1939.

[2] Nancy Childress: *Class Field Theory*. Springer. 2009.

[3] David A. Cox: *Primes of the Form $x^2 + ny^2$*. John Wiley & Sons, Inc. 1989.

[4] N. Jacobson: *Basic Algebra II*. San Francisco, CA: W. H. Freeman. 1980.

[5] Gerald J. Janusz: *Algebraic Number Fields*. Academic Press, Inc. 1973.

[6] C. Hollanti ja J. Lahtonen: *A New Tool: Constructing STBCs from Maximal Orders in Central Simple Algebras*. IEEE Information Theory Workshop, Punta del Este, 2006. s. 322-326.

[7] Helmut Koch: *Number Theory, Algebraic Numbers and Functions*. American Mathematical Society. 2000.

[8] Kiran T. ja B. Sundar Rajan: *STBC-Schemes With Nonvanishing Determinant for Certain Number of Transmit Antennas*. IEEE Transactions on Information Theory, vol. 51, 2005. s. 2984-2992.

[9] Serge Lang: *Algebraic Number Theory*. Springer-Verlag New York, Inc. 1986.

[10] Daniel A. Marcus: *Number Fields*. Springer-Verlag New York, Inc. 1977.

[11] Tauno Metsänkylä: *Algebra*. Turun yliopisto, Luentomoniste. 2004.

[12] Tauno Metsänkylä: *Algebralliset luvut*. Turun yliopisto, Luentomoniste. 2005.

[13] Wladyslaw Narkiewicz: *Elementary and Analytic Theory of Algebraic Numbers*. Springer-Verlag. 1990.

[14] Jürgen Neukirch: *Algebraic Number Theory*. Springer-Verlag. 1999.

[15] Irving Reiner: *Maximal Orders*. Academic Press Inc. 1975.

[16] Paulo Ribenboim: *Classical Theory of Algebraic Numbers*. Springer-Verlag New York, Inc. 2001.

[17] *PARI/GP* tietokonealgebrajärjestelmä. Versio 2.7.0, Bordeaux, 2014. http://pari.math.u-bordeaux.fr/

[18] R. Vehkalahti, C. Hollanti, J. Lahtonen, K. Ranto:
On the Densest MIMO Lattices From Cyclic Division Algebras. IEEE Transactions on Information Theory. Vol. 55, no. 8, 2009. s. 3751-3780.