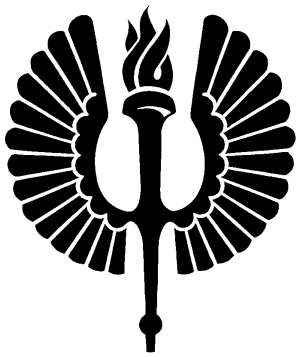


Catalanin yhtälön ratkaisut pienillä, parittomilla alkulukupotensseilla

Neea Palojärvi

Pro gradu -tutkielma
Toukokuu 2016

MATEMATIIKAN JA TILASTOTIETEEN LAITOS
TURUN YLIOPISTO

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

PALOJÄRVI, NEEA: Catalanin yhtälön ratkaisut pienillä, parittomilla alkulukupotensseilla
Pro gradu -tutkielma, 55 s.
Matematiikka
Toukokuu 2016

Catalanin konjektuurin mukaan Diofantoksen yhtälön $x^p - y^q = 1$, missä $p, q \geq 2$, ainoat nollasta eroavat ratkaisut ovat $(x, y, p, q) = (\pm 3, 2, 2, 3)$. Yhtälöä $x^p - y^q = 1$ kutsutaan Catalanin yhtälöksi. Konjektuuri on yritetty todistaa oikeaksi 1800-luvulta lähtien, mutta saatiin lopulta todistettua oikeaksi 2000-luvun alussa Preda Mihăilescun todistuksen myötä. Mihăilescun todistus perustuu ympyräkuntien käyttöön ja Galois'n moduleihin.

Tässä tutkielmassa esitetään yksi Catalanin konjektuurin ratkaisua helpottava tulos. Tutkielmassa esitetään Mihăilescun todistus väitteelle, ettei yhtälöllä $x^p - y^q = 1$ ole nollasta eroavia ratkaisuja, kun p ja q ovat parittomia alkulukuja ja vähintään toinen niistä on pienempi kuin 43. Todistus perustuu, Mihăilescun todistusten mukaisesti, ympyräkuntien käyttöön. Tutkielman lopussa kerrotaan, miten todistettua aputulosta voi käyttää apuna Catalanin konjektuurin ratkaisemisessa.

Asiasanat: Catalanin konjektuuri, p-adiset luvut, ympyräkunta

Sisältö

1 Johdanto

Vuonna 1844 matemaatikko E. Catalan esitti myöhemmin Catalanin konjektuurina tunnetun väittämän. Väittämä koskee Catalanin yhtälöä $x^p - y^q = 1$:

> Olkoot x, y, p ja q kokonaislukuja, $xy \neq 0$ sekä $\min\{p, q\} \geq 2$. Tällöin yhtälön $x^p - y^q = 1$ kaikki ratkaisut ovat $(x, y, p, q) = (\pm 3, 2, 2, 3)$.

Catalanin konjektuurin todistaminen osoittautui vaikeaksi ja kuluikin yli 150 vuotta ennen kuin se osoitettiin oikeaksi. 1800-luvulla V.A. Lebesgue [6] todisti, ettei Catalanin yhtälöllä ole ratkaisuja, kun $q = 2$ ja $p > 3$. 1900-luvulla muun muassa E.Z. Chein [3] ratkaisi tapauksen $p = 2$. Useat matemaatikot yrittivät myös todistaa Catalanin konjektuurin pitävän paikkansa, kun $\min\{p, q\} \geq 3$. Joitain edistysaskeliakin syntyi. Esimerkiksi Rob Tijdeman [15] todisti, että Catalanin konjektuurin toteuttavia lukunelikoita (x, y, p, q) on vain äärellisen monta. Konjektuurin todistamisen apuna yritettiin käyttää myös tietokonelaskentaa. Esimerkiksi M. Mignotte [8] todisti, että Catalanin konjektuuri pitää paikkansa, kun vähintään toinen luvuista p tai q on pienempi kuin 10^7.

Lopulta 2000-luvun alussa Preda Mihăilescun todisti, ettei yhtälöllä $x^p - y^q = 1$ ole ratkaisuja, kun $\min\{p, q\} \geq 3$. Todistus perustuu ympyräkuntiin ja Galois'n moduleihin, eikä siinä käytetä lainkaan apuna tietokonelaskentaa. Mihăilescun todistus koostuu pääpiirteittään kolmesta ominaisuudesta lukuihin p ja q liittyen. Näiden avulla saadaan todistettua, ettei Catalanin yhtälöllä ole ratkaisuja, kun $\min\{p, q\} \geq 3$. Nämä löytyvät lähteistä [9], [10] ja [11].

Tässä tutkielmassa esitetään Mihăilescun todistus väitteelle, ettei Catalanin yhtälöllä ole ratkaisuja, kun p ja q ovat parittomia alkulukuja ja vähintään toinen niistä on pienempi kuin 43. Todistus perustuu ympyräkuntiin, äärellisten kuntalaajennusten normeihin ja p-adisuuteen. Tätä varten luvussa 2 esitetään tarvittavat perusteet ympyräkunnista ja p-adisuudesta. Luvussa 3 todistetaan tutkielman pääväite. Tutkielman lopussa luvussa 4 tehdään yhteenveto todistuksesta ja kerrotaan, miten todistettua väittämää voidaan käyttää apuna Catalanin konjektuurin todistuksessa.

2 Perusteet

Ennen Catalanin yhtälön tarkastelua tutustutaan todistuksessa apuna käytettäviin määritelmiin ja lauseisiin. Luvussa 2.1 tarkastellaan algebrallisia lukuja ja luodaan algebrallista pohjaa varsinaisten tulosten ymmärtämiseksi. Luvussa 2.2 konstruoidaan p-adisten lukujen kunta sekä tutustaan tämän kunnan ja sen tietyn laajennuksen ominaisuuksiin.

Tässä luvussa symbolilla ζ_p tarkoitetaan p:nnettä primitiivistä ykkösenjuurta, missä p on pariton alkuluku. Luonnollisilla luvuilla tarkoitetaan einegatiivisia kokonaislukuja.

2.1 Kokonaislukujen renkaasta ja normista

Tässä luvussa tarkastellaan algebrallisia kokonaislukuja ja määritellään äärellisille Galois'n laajennuksille normin käsite. Luvun alussa määritellään näihin liittyviä käsitteitä ja yleisiä ominaisuuksia. Tämän jälkeen tarkastellaan algebrallisia kokonaislukuja kunnassa $\mathbb{Q}(\zeta_p)$. Luvun lopussa tutustutaan vielä pääihanteiden normiin. Luku seuraa kirjan [14] lähestymistapaa, joskin osa kirjan [14] todistuksista on muutettu sopivaksi vähemmän kokeneelle lukijalle. Näin ollen kaikkia väitteitä esitetä tässä luvussa niin yleisessä muodossa kuin kirjassa [14]. Lukijan oletetaan tuntevan ne kuntia ja renkaita koskevat perustulokset, jotka käsitellään Turun yliopiston syventävällä algebran kurssilla. Nämä asiat löytyvät luentomonisteesta [7]. Lisäksi lukijan oletetaan hallitsevan matriisilaskennan perusteita. Näihin voi perehtyä esimerkiksi Bernsteinin kirjan [1] avulla.

Olkoon L/K äärellinen kuntalaajennus ja $\alpha \in L/K$. Luvun α konjugaateilla yli kunnan K tarkoitetaan luvun α minimaalipolynomin nollakohtia yli kunnan K. Merkinnällä $\mathrm{char}(K)$ tarkoitetaan kunnan K karakteristikaa. Lisäksi renkaan R alkion α generoimasta ihanteessa käytetään merkintää $[\alpha]$.

Tutustutaan seuraavaksi renkaiden jaollisuuden määritelmään, algebrallisen kokonaisluvun käsitteeseen ja niiden ominaisuuksiin. Algebralliset kokonaisluvut ovat tietynlaisia algebrallisia lukuja.

Määritelmä 2.1. Olkoot R kommutatiivinen rengas ja $\alpha, \beta, \gamma \in R$. Tällöin merkinnällä $\alpha \equiv \beta \bmod \gamma$ tarkoitetaan, että $\alpha - \beta = r\gamma$ jollain $r \in R$. Jos $\alpha \equiv 0 \bmod \gamma$ renkaassa R, niin voidaan merkitä $\gamma|\alpha$. Sanotaan, että α *on jaollinen alkiolla* γ *renkaassa* R.

Määritelmä 2.2. Lukua α kutsutaan *algebralliseksi kokonaisluvuksi*, jos $f(\alpha) = 0$ jollain kokonaislukukertoimisella pääpolynomilla $f(x)$.

Lause 2.3. Olkoon K lukukunta ja $\alpha \in K$. Luku α on algebrallinen kokonaisluku, jos ja vain jos potenssien $1, \alpha, \alpha^2 \ldots$ generoima additiivinen ryhmä on äärellisesti generoitu.

Todistus. Oletetaan ensin, että α on algebrallinen kokonaisluku. Tällöin jollain kokonaisluvulla n

$$\alpha^n = -a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - \ldots - a_0, \text{ missä } a_k \in \mathbb{Z} \text{ kaikilla } k.$$

Näin ollen luvut $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ generoivat potenssien $1, \alpha, \alpha^2 \ldots$ generoiman additiivinen ryhmän. Täten potenssin $1, \alpha, \alpha^2 \ldots$ generoima additiivinen ryhmä on äärellisesti generoitu.

Oletetaan, että potenssien $1, \alpha, \alpha^2 \ldots$ generoima additiivinen ryhmä on äärellisesti generoitu. Oletetaan, että alkiot $v_1, v_2, \ldots, v_n$ muodostavat tämän ryhmän kannan. Pyritään löytämään näiden avulla kokonaislukukertoiminen pääpolynomi, joka saa luvulla α arvon nolla. Voidaan kirjoittaa

$$\alpha v_k = \sum_{j=1}^{n} b_{jk} v_j, \text{ missä } b_{jk} \in \mathbb{Z} \text{ kaikilla } j, k.$$

Saadaan

$$\begin{aligned} (b_{11} - \alpha)v_1 + b_{12}v_2 \ldots + b_{1n}v_n &= 0 \\ b_{21}v_1 + (b_{22} - \alpha)v_2 \ldots + b_{2n}v_n &= 0 \\ \cdots & \\ b_{n1}v_1 + b_{n2}v_n + \ldots + (b_{nn} - \alpha)v_n &= 0 \end{aligned} . \tag{1}$$

Merkitään nyt

$$f(x) = (-1)^n \begin{vmatrix} b_{11} - x & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} - x & \ldots & b_{2n} \\ \vdots & \cdots & \cdots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} - x \end{vmatrix}.$$

Yhtälöiden (1) mukaan $f(\alpha) = 0$. Lisäksi selvästi $f(x)$ on pääpolynomi ja $f(x) \in \mathbb{Z}[x]$. Siis α on algebrallinen kokonaisluku. □

Lause 2.4. Olkoon K lukukunta. Sen algebrallisten kokonaislukujen joukko on rengas.

Todistus. Koska K on lukukunta, se on myös rengas. Olkoon $\mathcal{O}_K$ kunnan K algebrallisten kokonaislukujen joukko. Todistetaan, että $\mathcal{O}_K$ on rengas tarkistamalla alirengaskriteerin voimassaolo. Koska $p(x) = x - 1$ on kokonaislukukertoiminen pääpolynomi ja $p(1) = 0$, niin $1 \in \mathcal{O}_K$. Siis joukko $\mathcal{O}_K$ on

epätyhjä. Olkoot α ja β joukon $\mathcal{O}_K$ alkioita. Todistetaan vielä, että $\alpha+\beta$ ja $\alpha\beta$ ovat algebrallisia kokonaislukuja.

Lauseen 2.3 luvut $1, \alpha, \alpha^2, \ldots$ ja $1, \beta, \beta^2, \ldots$ generoivat äärelliset additiiviset ryhmät T_α ja T_β. Oletetaan, että alkiot $v_1, v_2, \ldots, v_n$ ja $w_1, w_2, \ldots, w_m$ muodostavat vastaavasti ryhmien T_α ja T_β kannat. Merkitään lukujen $1, (\alpha+\beta), (\alpha+\beta)^2, \ldots$ ja $1, \alpha\beta, (\alpha\beta)^2, \ldots$ generoimia additiivisia ryhmiä merkinnöillä $T_{\alpha+\beta}$ ja $T_{\alpha\beta}$. Ryhmien $T_{\alpha+\beta}$ ja $T_{\alpha\beta}$ alkiot kuuluvat ryhmään $T_\alpha T_\beta$. Lisäksi alkiot $v_i w_j$, missä kokonaisluvuille i ja j pätee $i \in [1, n]$ sekä $j \in [1, m]$, generoivat ryhmän $T_\alpha T_\beta$. Näin ollen ryhmä $T_\alpha T_\beta$ on äärellisesti generoitu. Täten myös ryhmät $T_{\alpha+\beta}$ sekä $T_{\alpha\beta}$ ovat äärellisesti generoituja. Lauseen 2.3 mukaan alkiot $\alpha+\beta$ ja $\alpha\beta$ ovat algebrallisia kokonaislukuja. Alirengaskriteerin nojalla $\mathcal{O}_K$ on rengas. □

Määritelmä 2.5. Olkoon K lukukunta. Sen algebrallisten kokonaislukujen joukkoa kutsutaan kunnan K *kokonaislukujen renkaaksi*. Merkitään kunnan K kokonaislukujen rengasta symbolilla $\mathcal{O}_K$.

Nyt tiedetään, että jos kompleksiluku α on algebrallinen kokonaisluku, niin myös α^n on algebrallinen kokonaisluku kaikilla positiivisilla kokonaisluvuilla n. Seuraava lause kertoo, että myös luvut $\alpha^{\frac{1}{n}}$ ovat algebrallisia kokonaislukuja. Tämän todistamiseksi hyödynnetään algebrallisen kokonaisluvun määritelmässä esiintyvää polynomia $f(x)$.

Lause 2.6. Jos kompleksiluku α on algebrallinen kokonaisluku ja n positiivinen kokonaisluku, niin $\alpha^{\frac{1}{n}}$ on algebrallinen kokonaisluku.

Todistus. Koska α on algebrallinen kokonaisluku, niin on olemassa kokonaislukukertoiminen pääpolynomi $f(x)$, jolle $f(x) = 0$. Olkoon $m = \deg f(x)$. Merkitään $f(x) = \sum_{k=0}^{m} a_k x^k$, missä luvut a_k ovat kokonaislukuja ja $a_m = 1$. Tällöin polynomi $g(x) = \sum_{k=0}^{m} a_k x^{kn}$ on kokonaislukukertoiminen pääpolynomi ja $g(\alpha^{\frac{1}{n}}) = 0$. Siis myös $\alpha^{\frac{1}{n}}$ on algebrallinen kokonaisluku. □

Siirrytään tarkastelemaan äärellisiä Galois'n laajennuksia. Päämääränä on määritellä äärellisille Galois'n laajennuksille normin käsite ja tutkia, mitä arvoja algebrallisen kokonaisluvun normi voi saada.

Määritelmä 2.7. Olkoon L/K äärellinen Galois'n laajennus ja $\alpha \in L$. Tällöin lukua $\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)$ kutsutaan luvun α *normiksi* yli laajennuksen L/K. Merkitään $N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)$.

Lause 2.8. Olkoot $K \subseteq F \subseteq L$ sekä L/K, L/F ja F/K äärellisiä Galois'n laajennuksia. Tällöin kaikille $\alpha \in L$ pätee $N_{L/K}(\alpha) = N_{F/K}(N_{L/F}(\alpha))$.

Todistus. Olkoon $\mathrm{Gal}(F/K) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ ja $\mathrm{Gal}(L/F) = \{\tau_1, \tau_2, \ldots, \tau_m\}$. Normin määritelmän mukaan

$$N_{F/K}(N_{L/F}(\alpha)) = \prod_{j=1}^{n} \sigma_j(\prod_{i=1}^{m} \tau_i(\alpha)).$$

Automorfismien ominaisuuksien takia

$$\prod_{j=1}^{n} \sigma_j(\prod_{i=1}^{m} \tau_i(\alpha)) = \prod_{j=1}^{n} \prod_{i=1}^{m} \sigma_j(\tau_i(\alpha)). \tag{2}$$

Koska $\sigma_j\tau_i \in \mathrm{Gal}(L/K)$ kaikilla i, j, niin riittää todistaa, että kukin ryhmän $\mathrm{Gal}(L/K)$ alkio esiintyy tulossa $\prod_{j=1}^{n} \prod_{i=1}^{m} \sigma_j(\tau_i(\alpha)$ täsmälleen kerran.

Astelukulauseen mukaan $[L : K] = [L : F][F : K] = mn$, joten riittää todistaa, että alkiot $\sigma_j\tau_i$ ovat keskenään erisuuria. Oletetaan, että pätee $\sigma_{j_1}\tau_{i_1} = \sigma_{j_2}\tau_{i_2}$. Koska τ_{i_1} ja τ_{i_2} kuvaavat kunnan F alkiot itselleen, niin $\sigma_{j_1} = \sigma_{j_2}$. Näin ollen $j_1 = j_2$. Tästä seuraa, että $\tau_{i_1} = \tau_{i_2}$ ja edelleen $i_1 = i_2$. Yhtälössä (2) esiintyvät kaikki ryhmän $\mathrm{Gal}(L/K)$ alkiot täsmälleen kerran. Siis $N_{L/K}(\alpha) = N_{F/K}(N_{L/F}(\alpha))$. □

Lause 2.9. Olkoon L/K äärellinen Galois'n laajennus, $n = [L : K]$ ja $\alpha \in L$. Lisäksi olkoot $\alpha = \alpha_1, \alpha_2, ..., \alpha_s$ alkion α konjugaatit yli kunnan K. Kun $\sigma \in \mathrm{Gal}(L/K)$, niin $\sigma(\alpha) = \alpha_k$ jollain kokonaisluvulla $k \in [1, s]$ ja kukin α_k esiintyy kuvana $\frac{n}{s}$ kertaa.

Todistus. Tunnetusti $\sigma(\alpha) = \alpha_k$ jollain kokonaisluvulla $k \in [1, s]$, kun $\sigma \in \mathrm{Gal}(L/K)$. Riittää siis todistaa, että kukin α_k esiintyy kuvana $\frac{n}{s}$ kertaa.

Merkitään $H = \mathrm{Gal}(L/K(\alpha))$ ja $G = \mathrm{Gal}(L/K)$. Tällöin $H \leq G$ ja $[G : H] = [K(\alpha) : K] = s$. Siis ryhmä G voidaan kirjoittaa sivuluokkiensa partitiona $G = \sigma_1 H \cup \sigma_2 H \cup \ldots \cup \sigma_s H$, missä $\sigma_k \in G$ kaikilla kokonaisluvuilla $k \in [1, s]$. Oletetaan nyt, että $\sigma \in G$. Tavoitteena on todistaa, että $\sigma(\alpha) = \sigma_k(\alpha)$ jos ja vain jos $\sigma \in \sigma_k H$. Tällöin nimittäin väite on todistettu, sillä jokaisessa sivuluokassa $\sigma_k H$ on $\frac{n}{s}$ alkiota ja luvun k eri arvoilla $\sigma_k(\alpha) = \alpha_i$ saa eri arvot.

Oletetaan ensin, että $\sigma(\alpha) = \sigma_k(\alpha)$ ja todistetaan, että $\sigma \in \sigma_k H$. Oletuksen nojalla $(\sigma_k^{-1}\sigma)(\alpha) = \alpha$. Siis $\sigma_k^{-1}\sigma \in H$ ja edelleen $\sigma \in \sigma_k H$. Oletetaan seuraavaksi, että $\sigma \in \sigma_k H$ ja todistetaan, että $\sigma(\alpha) = \sigma_k(\alpha)$. Oletuksen mukaan voidaan kirjoittaa kuvaus σ muodossa $\sigma_k\tau$, missä $\tau \in H$. Näin ollen $\sigma(\alpha) = (\sigma_k\tau)(\alpha)$. Koska $\tau \in H$, niin $\tau(\alpha) = \alpha$. Siis $\sigma(\alpha) = \sigma_k(\alpha)$. Täten väite on todistettu. □

Seuraavan lauseen tarkoituksena on valaista eri tapoja laskea normi. Lausetta pystytään käyttämään apuna, kun tarkastellaan algebrallisen kokonaisluvun normia.

Lause 2.10. Olkoon L/K äärellinen Galois'n laajennus, $n = [L : K]$ ja $\alpha \in L$. Lisäksi olkoon $f(x)$ luvun α minimaalipolynomi yli kunnan K ja $s = \deg f(x)$. Tällöin $N_{L/K}(\alpha) = (-1)^n f(0)^{\frac{n}{s}}$.

Todistus. Olkoot $\alpha = \alpha_1, \alpha_2, ..., \alpha_s$ alkion α konjugaatit yli kunnan K. Kun $\sigma \in \mathrm{Gal}(L/K)$, niin $\sigma(\alpha) = \alpha_k$ jollain kokonaisluvulla $k \in [1, s]$. Lisäksi lauseen 2.9 mukaan kukin α_k esiintyy kuvana $\frac{n}{s}$ kertaa, joten

$$\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha) = \prod_{k=1}^{s} \alpha_k^{\frac{n}{s}}.$$

Koska $f(0) = (-1)^s \alpha_1 \alpha_2 \cdots \alpha_s$, niin $N_{L/K}(\alpha) = (-1)^n f(0)^{\frac{n}{s}}$. □

Seuraavassa kahdessa lauseessa todistetaan algebrallisten kokonaislukujen ja normin välisiä yhteyksiä. Koska algebrallinen kokonaisluku on määritelty vain lukukunnille ja normi äärellisille Galois'n laajennuksille, niin tarkastellaan vain äärellisiä Galois'n laajennuksia $\mathbb{Q}(\alpha)/\mathbb{Q}$.

Lause 2.11. Olkoon $\mathbb{Q}(\alpha)/\mathbb{Q}$ äärellinen Galois'n laajennus ja $\beta \in \mathcal{O}_{\mathbb{Q}(\alpha)}$. Tällöin $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)$ on kokonaisluku.

Todistus. Todistetaan ensin, että luvun β minimaalipolynomi yli kunnan $\mathbb{Q}$ on kokonaislukukertoiminen. Olkoon $f(x) \in \mathbb{Z}[x]$ alinta astetta oleva pääpolynomi, jolle $f(\beta) = 0$. Tällainen polynomi löytyy, koska β on algebrallinen kokonaisluku. Polynomi $f(x)$ on jaoton yli renkaan $\mathbb{Z}$. Näin ollen se on myös jaoton yli kunnan $\mathbb{Q}$ ja täten alkion β minimaalipolynomi. Siis luvun β minimaalipolynomi yli kunnan $\mathbb{Q}$ on kokonaislukukertoiminen.

Lauseen 2.10 mukaan $N_{L/K}(\beta) = (-1)^n f(0)^{\frac{n}{s}}$, missä $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ ja $s = \deg f(x)$. Edellisen kappaleen mukaan $f(0) \in \mathbb{Z}$ ja tunnetusti $\frac{n}{s} \in \mathbb{Z}$. Näin ollen $N_{L/K}(\beta) \in \mathbb{Z}$. □

Lause 2.12. Olkoon $\mathbb{Q}(\alpha)/\mathbb{Q}$ äärellinen Galois'n laajennus ja $\beta \in \mathcal{O}_{\mathbb{Q}(\alpha)}$. Tällöin β on renkaan $\mathcal{O}_{\mathbb{Q}(\alpha)}$ yksikkö täsmälleen silloin, kun $|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)| = 1$.

Todistus. Oletetaan ensin, että β on renkaan $\mathcal{O}_{\mathbb{Q}(\alpha)}$ yksikkö ja todistetaan, että sen normin itseisarvo on 1. Tällöin $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta\beta^{-1})$. Automorfismien ominaisuuksien mukaan pätee:

$$\begin{cases} N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1) = 1 \\ N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta\beta^{-1}) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta) N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta^{-1}) \end{cases}$$

Yhdistämällä edelliset tiedot saadaan yhtälö $1 = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta^{-1})$. Koska lauseen 2.11 mukaan normit $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)$ ja $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta^{-1})$ ovat kokonaislukuja, niin kokonaisluvun $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)$ on jaettava luku 1. Siis $|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)| = 1$.

Oletetaan nyt, että $|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)| = 1$ ja todistetaan, että β on renkaan $\mathcal{O}_{\mathbb{Q}(\alpha)}$ yksikkö. Algebrallisen kokonaisluvun määritelmän mukaan luvulla β on kokonaislukukertoiminen minimaalipolynomi $f(x)$. Lauseen 2.10 mukaan tämän polynomin vakiotermi on ± 1. Saadaan

$$\beta^n + a_{n-1}\beta^{n-1} + ... + a_1\beta \pm 1 = 0 \tag{3}$$

joillain kokonaisluvuilla $a_1, a_2, ..., a_{n-1}$. Kerrotaan yhtälö (3) luvulla β^{-n}. Saadaan

$$1 + a_{n-1}\beta^{-1} + ... + a_1\beta^{-n+1} \pm \beta^{-n} = 0.$$

Kerrotaan tarvittaessa edellinen yhtälö luvulla -1, jotta saadaan polynomi $1 + a_{n-1}\beta^{-1} + ... + a_1\beta^{-n+1} \pm \beta^{-n}$ pääpolynomiksi. Siis on olemassa kokonaislukukertoiminen pääpolynomi $g(x)$, jolle $g(\beta^{-1}) = 0$. Näin ollen myös $\beta^{-1} \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ eli β on renkaan $\mathcal{O}_{\mathbb{Q}(\alpha)}$ yksikkö. □

Tarkastellaan seuraavaksi laajennusta $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Joukko $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ muodostaa tämän laajennuksen kannan ja tätä kantaa käytetään yleensä hyödyksi todistuksissa. Joskus todistukset on kuitenkin helpompi esittää kannan $\{\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}\}$ avulla, joten tätä kantaa käytetään osassa todistuksia. Halutaan tarkastella laajennuksen $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ algebrallisia kokonaislukuja ja näiden kokonaislukujen normeja. Jotta tämä on mahdollista, on ensin todistettava, että $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ on Galois'n laajennus.

Lause 2.13. Laajennus $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ on Galois'n laajennus.

Todistus. Koska $\mathrm{char}(\mathbb{Q}) = 0$, niin laajennus $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ on separoituva. Tarkastellaan polynomin $\phi(x) = \sum_{k=0}^{p-1} x^k = \prod_{k=1}^{p-1}(x - \zeta_p^k)$ hajoamiskuntaa yli rationaalilukujen kunnan. Merkitään tätä kuntaa symbolilla K_ϕ. Koska $\zeta_p^k \in \mathbb{Q}(\zeta_p)$ kaikilla kokonaisluvuilla k, niin $K_\phi \subseteq \mathbb{Q}(\zeta_p)$. Toisaalta on oltava $\zeta_p \in K_\phi$ eli $\mathbb{Q}(\zeta_p) \subseteq K_\phi$. Täten $\mathbb{Q}(\zeta_p)$ on polynomin $\phi(x)$ hajoamiskunta yli rationaalilukujen kunnan ja laajennus $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ normaali. Siis laajennus $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ on Galois'n laajennus □

Tästä lähtien merkitään $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Tarkastellaan seuraavaksi, millainen ryhmä G on.

Lause 2.14. $G = \{\sigma_1, \sigma_2, \cdots, \sigma_{p-1}\}$, missä $\sigma_k(\zeta_p) = \zeta_p^k$

Todistus. Lauseen 2.13 mukaan $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ on Galois'n laajennus ja tunnetusti laajennuksen kertaluku on $p-1$. Alkion ζ_p konjugaatit ovat luvut ζ_p^k, missä kokonaisluku $k \in [1, p-1]$. Täten $G = \{\sigma_1, \sigma_2, \cdots, \sigma_{p-1}\}$, missä $\sigma_k(\zeta_p) = \zeta_p^k$. □

Koska $\mathbb{Q}(\zeta_p)$ on lukukunta, on sille olemassa kokonaislukujen rengas. Tämä rengas löydetään seuraavan todistuksen avulla.

Lause 2.15. Kunnan $\mathbb{Q}(\zeta_p)$ kokonaislukujen rengas on $\mathbb{Z}[\zeta_p]$.

Todistus. Koska $1, \zeta_p \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$ ja lauseen 2.4 mukaan $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ on rengas, niin $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_p)}$. Näin ollen riittää todistaa, että $\mathcal{O}_{\mathbb{Q}(\zeta_p)} \subseteq \mathbb{Z}[\zeta_p]$. Määritellään tätä varten apukuvaus S. Olkoon $\alpha \in \mathbb{Q}(\zeta_p)$ mielivaltainen ja $\alpha = \alpha_1, \alpha_2, \cdots, \alpha_s$ sen konjugaatit yli kunnan $\mathbb{Q}$. Tällöin määritellään $S(\alpha) = \sum_{k=1}^{s} \alpha_k$. Havaitaan, että luku $S(\alpha)$ voidaan laskea luvun α minimaalipolynomin yli kunnan $\mathbb{Q}$ avulla. Olkoon $f(x)$ luvun α minimaalipolynomi yli kunnan $\mathbb{Q}$ ja sen toiseksi korkeimman termin kerroin a. Tällöin $S(\alpha) = (-1)^{\deg f(x)} a$. Näin ollen jos $\alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$, niin lauseen 2.11 todistuksen mukaan $S(\alpha) \in \mathbb{Z}$.

Olkoon $\alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$ mielivaltainen. Tällöin voidaan kirjoittaa $\alpha = \sum_{k=0}^{p-2} a_k \zeta_p^k$, missä $a_k \in \mathbb{Q}$ kaikilla kokonaisluvuilla $k \in [0, p-2]$. Pyritään tämän esityksen avulla löytämään luvulle α esitys, jossa jokaiselle luvulle a_k pätee $a_k \in \mathbb{Z}$. Tällöin nimittäin pätee $\alpha \in \mathbb{Z}[\zeta_p]$. Lasketaan tätä varten ensin luvut $S(\zeta_p^k), S(\zeta_p \alpha)$ ja $S(\alpha \zeta_p^{-j})$ kaikilla kokonaisluvuilla $j \in [0, p-2]$. Luvun ζ_p minimaalipolynomista yli kunnan $\mathbb{Q}$ nähdään, että $S(\zeta_p^k) = \sum_{j=1}^{p-1} \zeta_p^j = -1$, kun $k \in [1, p-1]$ ja $S(1) = p-1$. Tämän avulla saadaan laskettua $S(\alpha \zeta_p^{-j})$. Koska $\alpha \zeta_p^{-j} = \sum_{k=0}^{p-2} a_k \zeta_p^{k-j}$ ja $S(\sum_{k=0}^{p-2} a_k \zeta_p^{k-j}) = \sum_{k=0}^{p-2} a_k S(\zeta_p^{k-j})$, niin

$$S(\alpha \zeta_p^{-j}) = (p-1) a_j + \sum_{k=0, k \neq j}^{p-2} a_k S(\zeta_p^{k-j}). \tag{4}$$

Edellä todistetun nojalla $S(\zeta_p^{k-j}) = -1$, joten

$$\sum_{k=0, k \neq j}^{p-2} a_k S(\zeta_p^{k-j}) = -\sum_{k=0, k \neq j}^{p-2} a_k. \tag{5}$$

Siis yhtälöiden (4) ja (5) nojalla $S(\alpha \zeta_p^{-j}) = p a_j - \sum_{k=0}^{p-2} a_k$. Lisäksi $S(\zeta_p \alpha) = -\sum_{k=0}^{p-2} a_k$. Koska $\alpha \zeta_p^{-j}, \alpha \zeta_p \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$, niin $S(\alpha \zeta_p^{-j}), S(\alpha \zeta_p) \in \mathbb{Z}$. Näin ollen $S(\alpha \zeta_p^{-j}) - S(\alpha \zeta_p) = p a_j \in \mathbb{Z}$. Voidaan kirjoittaa $a_j = \frac{b_j}{p}$ jollain kokonaisluvulla b_j.

Edellisessä kappaleessa tehtyjen huomioiden mukaan $p\alpha = \sum_{k=0}^{p-2} b_k \zeta_p^k$. Osoitetaan, että $p | b_k$ kokonaislukujen renkaassa kaikilla kokonaisluvuilla k.

Tällöin nimittäin olisi löydetty luvulle α esitys, jossa rationaaliluvut a_k olisivat kokonaislukuja. Olkoon $\pi = 1 - \zeta_p$. Tällöin $\zeta_p^k = (-\pi + 1)^k$. Saadaan

$$p\alpha = \sum_{k=0}^{p-2} c_k \pi^k, \tag{6}$$

missä $c_k \in \mathbb{Z}$ kaikilla k. Todistetaan seuraavaksi, että π jakaa yhtälön (6) vasemman puolen renkaassa $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$. Tehdään tämä todistamalla, että π jakaa luvun p renkaassa $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$. Merkitään

$$\phi(x) = \sum_{k=0}^{p-1} x^k = \prod_{k=1}^{p-1} (x - \zeta_p^k). \tag{7}$$

Nyt $\prod_{k=1}^{p-1}(1 - \zeta_p^k) = \phi(1) = p$. Koska $1 - \zeta_p^k \in \mathbb{Z}[\zeta_p]$ kaikilla kokonaisluvuilla k ja todistuksen alussa on todettu, että $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_p)}$, niin π jakaa luvun p renkaassa $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$. Lisäksi $\alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$, joten π jakaa yhtälön (6) vasemman puolen renkaassa $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$

Koska π jakaa yhtälön (6) vasemman puolen, niin se jakaa myös yhtälön (6) oikean puolen. Täten π jakaa luvun c_0 renkaassa $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$. Voidaan kirjoittaa $c_0 = \pi\gamma_0$, missä $\gamma_0 \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$. Koska c_0 on kokonaisluku ja $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, niin $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(c_0) = c_0^{p-1}$. Toisaalta $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(c_0) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\pi\gamma_0)$. Automorfismien ominaisuuksien vuoksi

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\pi\gamma_0) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\pi) N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\gamma_0).$$

Lasketaan luvun π normi. Normin määritelmän mukaan

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\pi) = \prod_{\sigma \in G} \sigma(1 - \zeta_p).$$

Lauseen 2.14 nojalla $\prod_{\sigma\in G} \sigma(1-\zeta_p) = \prod_{k=1}^{p-1}(1-\zeta_p^k)$. Olkoon merkintä ϕ kuten kaavassa 7. Nyt $\prod_{k=1}^{p-1}(1 - \zeta_p^k) = \phi(1) = p$. Siis $c_0^{p-1} = pN_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\gamma_0)$. Lauseen 2.11 mukaan $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\gamma_0) \in \mathbb{Z}$. Näin ollen $p|c_0$ kokonaislukujen renkaassa. Vastaavalla tavalla voidaan päätellä, että $p|c_k$ kaikilla kokonaisluvuilla $c_k k$. Siis kaikilla kokonaisluvuilla $k \in [0, p-2]$ voidaan kirjoittaa $c_k = d_k p$, missä $d_k \in \mathbb{Z}$.

Yhtälön (6) ja edellisen kappaleen nojalla $\alpha = \sum_{k=0}^{p-2} d_k \pi^k$. Suoraan laskemalla nähdään, että $\pi^k = \sum_{j=0}^{k} \binom{k}{j} (-\zeta_p)^j (-1)^{k-j}$. Täten $\alpha = \sum_{k=0}^{p-2} l_k \zeta_p^k$, missä $l_k \in \mathbb{Z}$ kaikilla kokonaisluvuilla $k \in [0, p-2]$. Siis $\alpha \in \mathbb{Z}[\zeta_p]$. Näin ollen $\mathcal{O}_{\mathbb{Q}(\zeta_p)} \subseteq \mathbb{Z}[\zeta_p]$. Saadaan $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$. □

Tästä lähtien, jos käsitellään rengasta $\mathbb{Z}[\zeta_p]$ ihanteena, tarkoitetaan sitä nimenomaan kunnan $\mathbb{Q}(\zeta_p)$ kokonaislukujen renkaana. Seuraavassa esimerkissä tutustutaan osaan renkaan $\mathbb{Z}[\zeta_p]$ yksiköistä.

Esimerkki 2.16. Olkoon p pariton alkuluku ja s mikä tahansa kokonaisluku väliltä $[1, p-1]$. Osoitetaan, että $1+\zeta_p^s$ on renkaan $\mathbb{Z}[\zeta_p]$ yksikkö.

Olkoon $\sigma \in G$ mielivaltainen. Lauseen 2.14 mukaan $\sigma(1+\zeta_p^s) = 1+\zeta_p^{ks}$ jollain kokonaisluvulla $k \in [1, p-1]$. Saadaan $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1+\zeta_p^s) = \prod_{k=1}^{p-1}(1+\zeta_p^{ks})$. Kun k käy läpi supistetun jäännössysteemin modulo p, myös ks käy läpi supistetun jäännössysteemin modulo p. Siis voidaan kirjoittaa

$$\prod_{k=1}^{p-1}(1+\zeta_p^{ks}) = \prod_{k=1}^{p-1}(1+\zeta_p^k).$$

Tämä voidaan edelleen kirjoittaa muotoon $\prod_{k=1}^{p-1}(1+\zeta_p^k) = \prod_{k=1}^{p-1}(1-(-\zeta_p^k))$. Koska luvut $-\zeta_p, -\zeta_p^2, ..., \zeta_p^{p-1}$ ovat yhtälön $\frac{x^p+1}{x+1} = 0$ kaikki ratkaisut, niin $\frac{x^p+1}{x+1} = \prod_{k=1}^{p-1}(x-(-\zeta_p^k))$. Siis

$$\prod_{k=1}^{p-1}(1-(-\zeta_p^k)) = \frac{1^p+1}{1+1} = 1.$$

Lauseen 2.12 mukaan luku $1+\zeta_p^s$ on renkaan $\mathbb{Z}[\zeta_p]$ yksikkö. □

Huomataan, että edellisen esimerkin nojalla $1+\zeta_p^s$ on renkaan $\mathbb{Z}[\zeta_p]$ yksikkö, kun kokonaisluvulle s pätee $s \not\equiv 0 \bmod p$. Nimittäin jokaista tällaista kokonaislukua s kohti löytyy kokonaisluku m, jolle $s \equiv m \bmod p$ ja $m \in [1, p-1]$. Tällöin $1+\zeta_p^s = 1+\zeta_p^m$. Edellisen esimerkin mukaan $1+\zeta_p^m$ on renkaan $\mathbb{Z}[\zeta_p]$ yksikkö. Huomionarvoista on myös, ettei $1+\zeta_p^s$ ole renkaan $\mathbb{Z}[\zeta_p]$ yksikkö, kun $s \equiv 0 \bmod p$. Tällöin nimittäin $1+\zeta_p^s = 2$, eikä luku 2 ole renkaan $\mathbb{Z}[\zeta_p]$ yksikkö. Tämä seuraa esimerkiksi lauseista 2.12 ja 2.15.

Seuraavan lauseen todistus on peräisin Spenceriltä vuodelta 1997 ja se on esitetty lähteessä [13]. Todistuksessa käytetään apuna matriisilaskentaa ja todistus valottaa renkaan $\mathbb{Z}[\zeta_p]$ alkioiden ominaisuuksia.

Lause 2.17. Olkoon α renkaan $\mathbb{Z}[\zeta_p]$ yksikkö ja $|\sigma(\alpha)| = 1$ kaikilla $\sigma \in G$. Tällöin α on ykkösenjuuri.

Todistus. Olkoon R rengas. Symbolilla $\mathcal{M}_n(R)$ tarkoitetaan $n \times n$ matriisien joukkoa, jossa jokaisen joukon matriisin kaikki alkiot kuuluvat renkaaseen R.

Olkoon $f(x) = x^s + \sum_{k=0}^{s-1} a_k x^k$ alkion α minimaalipolynomi yli kunnan $\mathbb{Q}$. Lauseen 2.11 todistuksen alkuosan mukaan $f(x) \in \mathbb{Z}[x]$. Tarkastellaan nyt polynomin $f(x)$ seuralaismatriisia

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{s-2} & -a_{s-1} \end{pmatrix} \in \mathcal{M}_s(\mathbb{Z}).$$

Matriisin A ominaisarvot ovat luvun α konjugaatit $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_s$ Merkitään

$$D = \begin{pmatrix} \alpha_1 & 0 & 0 & \cdots & 0 \\ 0 & \alpha_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_s \end{pmatrix} \in \mathcal{M}_s(\mathbb{C}).$$

Merkinnällä $|M|$ tarkoitetaan, että jokaisesta matriisin M alkioista otetaan itseisarvo. Tarkastellaan matriisia $|D|$. Koska lauseen 2.13 mukaan $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ on äärellinen Galois'n laajennus, niin kaikilla $\sigma \in G$ pätee $\sigma(\alpha) = \alpha_k$ jollain kokonaisluvulla $k \in [1, s]$. Lisäksi lauseen 2.9 mukaan jokainen α_k esiintyy kuvana $\frac{p-1}{s}$ kertaa. Oletusten mukaan $|\alpha_k| = 1$ kaikilla kokonaisluvuilla $k \in [1, s]$. Siis $|D| = I$. Havaitaan myös, että $|MD| = |M||D|$ kaikilla matriiseilla $M \in \mathcal{M}_s(\mathbb{C})$, koska D on diagonaalimatriisi.

Matriisin D valinnan takia on olemassa kääntyvä $P \in \mathcal{M}_s(\mathbb{C})$, jolle $A = PDP^{-1}$. Edellisten havaintojen mukaan kaikilla luonnollisilla luvuilla m pätee $|PD^m| = |P|$. Koska lisäksi $|PD^mP^{-1}| \leq |PD^m||P^{-1}|$, niin $|A^m| \leq |P||P^{-1}|$. Siis $|A|$ on rajoitettu. Koska $A \in \mathcal{M}_s(\mathbb{Z})$, niin A^m voi saada vain äärellisen monta eri arvoa. Siis joillain luvuilla $m, r \in \mathbb{Z}_+$ pätee $A^{m+r} = A^m$. Tällöin $D^{m+r} = D^m$ eli $\alpha^{m+r} = \alpha^m$. Koska α on renkaan $\mathbb{Z}[\zeta_p]$ yksikkö, niin $\alpha^r = 1$. Siis α on ykkösenjuuri. □

Siirrytään tarkastelemaan ihanteita. Useimmissa lauseissa rajoitutaan tarkastelemaan äärellisiä Galois'n laajennuksia ja pääihanteita, koska yleisempää teoriaa ei tarvita tässä tutkielmassa.

Määritelmä 2.18. Olkoon R kommutatiivinen rengas. Sen ihanne $P \neq R$ on alkuihanne jos ja vain jos aina, kun $\alpha, \beta \in R$ ja $\alpha\beta \in P$, niin $\alpha \in P$ tai $\beta \in P$.

Määritelmä 2.19. Olkoon K kunnan $\mathbb{Q}$ äärellinen Galois'n laajennus ja $\alpha \in \mathcal{O}_K$. Tällöin määritellään alkion α generoiman ihanteen normiksi $N([\alpha]) = |N_{K/\mathbb{Q}}(\alpha)|$.

On selvää, että edellä määritelty normi on ihanteen generaattorin valinnasta riippumaton. Jos nimittäin renkaan $\mathcal{O}_K$ pääihanne A on $A = [\alpha] = [\beta]$, niin $\alpha|\beta$ ja $\beta|\alpha$ renkaassa $\mathcal{O}_K$. Täten $\alpha = u\beta$, missä u on renkaan $\mathcal{O}_K$ yksikkö. Koska K on kunnan $\mathbb{Q}$ äärellinen laajennus ja $\text{char}(\mathbb{Q}) = 0$, niin laajennus $K/\mathbb{Q}$ on yksinkertainen. Täten lauseen 2.12 mukaan $|N_{K/\mathbb{Q}}(u)| = 1$. Siis $|N_{K/\mathbb{Q}}(\alpha)| = |N_{K/\mathbb{Q}}(\beta)|$.

Lause 2.20. Olkoon K kunnan $\mathbb{Q}$ äärellinen Galois'n laajennus ja A renkaan $\mathcal{O}_K$ pääihanne. Tällöin $N(A) \in A$.

Todistus. Koska A on pääihanne, voidaan kirjoittaa $A = [\alpha]$ jollain $\alpha \in \mathcal{O}_K$. Olkoot $\alpha = \alpha_1, \alpha_2, \cdots, \alpha_s$ luvun α konjugaatit. Lisäksi olkoon $f(x)$ kokonaislukukertoiminen pääpolynomi, jolle $f(\alpha) = 0$. Olkoon $g(x)$ luvun α minimaalipolynomi yli kunnan $\mathbb{Q}$. Koska $g(x)$ jakaa polynomin $f(x)$, niin myös luvun α konjugaatit ovat algebrallisia kokonaislukuja.

Koska $K/\mathbb{Q}$ on äärellinen Galois'n laajennus, niin $\text{Gal}(K/\mathbb{Q})$ koostuu kuvauksista σ, joille $\sigma(\alpha) = \alpha_k$ jollain kokonaisluvulla $k \in [1, s]$. Lisäksi lauseen 2.9 jokainen α_k esiintyy kuvana yhtä monta kertaa. Näin ollen $N(A) = |N_{K/\mathbb{Q}}(\alpha)|$ voidaan kirjoittaa muodossa $N(A) = |\alpha^{\frac{[K:\mathbb{Q}]}{s}} \prod_{k=2}^{n} \alpha_k^{\frac{[K:\mathbb{Q}]}{s}}|$. Koska $\mathcal{O}_K$ on lauseen 2.4 nojalla rengas, niin $\prod_{k=2}^{s} \alpha_k^{\frac{[K:\mathbb{Q}]}{s}} \in \mathcal{O}_K$. Siis $\alpha^{\frac{[K:\mathbb{Q}]}{s}} \prod_{k=2}^{n} \alpha_k^{\frac{[K:\mathbb{Q}]}{s}} \in A$. Lauseesta 2.11 seuraa, että $N(A) \in \mathbb{Z}$, joten $|\alpha^{\frac{[K:\mathbb{Q}]}{s}} \prod_{k=2}^{n} \alpha_k^{\frac{[K:\mathbb{Q}]}{s}}|$ on etumerkkiä vaille luku $\alpha^{\frac{[K:\mathbb{Q}]}{s}} \prod_{k=2}^{n} \alpha_k^{\frac{[K:\mathbb{Q}]}{s}}$. Täten $N(A) \in A$. □

Seuraavassa esimerkissä näytetään, miten pääihanteen normi voidaan laskea. Lisäksi esitetään yksi tapa todistaa, että ihanne on alkuihanne.

Esimerkki 2.21. Olkoon $\mathfrak{p}$ alkion $1 - \zeta_p$ generoima renkaan $\mathbb{Z}[\zeta_p]$ ihanne. Osoitetaan, että ihanteen $\mathfrak{p}$ normi on p ja se on alkuihanne.

Todistetaan ensin, että alkion $[1 - \zeta_p]$ generoiman ihanteen normi on p. Tätä käytetään myöhemmin hyödyksi todistettaessa, että $[1 - \zeta_p]$ on alkuihanne. Lauseen 2.15 mukaan $\mathbb{Z}[\zeta_p]$ on kunnan $\mathbb{Q}(\zeta_p)$ kokonaislukujen rengas ja lauseen 2.13 mukaan $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ on Galois'n laajennus. Normi voidaan siis laskea. Ihanteen normin määritelmän mukaan $N([1-\zeta_p]) = |N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p)|$. Normi $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1 - \zeta_p)$ on laskettu lauseen 2.15 todistuksen toiseksi viimeisessä kappaleessa ja se on p. Siis $N([1 - \zeta_p]) = p$.

Todistetaan vielä, että $[1 - \zeta_p]$ on alkuihanne. Selvästi $[1 - \zeta_p] \neq \mathbb{Z}[\zeta_p]$, sillä

$$N([1 - \zeta_p]) = p \neq 1 = N([1]).$$

Oletetaan, että $\alpha\beta \in [1-\zeta_p]$ ja $\alpha, \beta \in \mathbb{Z}[\zeta_p]$. Voidaan kirjoittaa $\alpha\beta = \gamma(1-\zeta_p)$, missä $\gamma \in \mathbb{Z}[\zeta_p]$. Lasketaan ihanteen $[\alpha\beta]$ normi kahdella eri tavalla. Ensimmäiseksi lasketaan normi muodosta $[\alpha\beta]$. Normin määritelmän mukaan $N([\alpha\beta]) = |N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha\beta)|$. Tämä voidaan edelleen kirjoittaa muodossa $|N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha)||N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\beta)|$. Koska $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$, niin lauseen 2.11 mukaan $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha), N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\beta) \in \mathbb{Z}$. Seuraavaksi lasketaan normi ihanteen $[\gamma(1-\zeta_p)]$ avulla. Nimittäin, koska $\alpha\beta = \gamma(1-\zeta_p)$, niin $[\alpha\beta] = [\gamma(1-\zeta_p)]$. Samoin kuin aiemmin ihanteen $[\alpha\beta]$ normia laskettaessa voidaan päätellä, että

$$N([\gamma(1-\zeta_p)]) = |N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\gamma)||N_{\mathbb{Q}(1-\zeta_p)/\mathbb{Q}}(\zeta_p)|$$

ja $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\gamma) \in \mathbb{Z}$. Siis $p = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p)$ jakaa luvun $|N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha)||N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\beta)|$. Koska p on alkuluku, niin p jakaa vähintään toisen luvuista $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha)$ tai $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\beta)$. Voidaan valita $p|N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha)$.

Kirjoitetaan α muodossa $\alpha = \sum_{k=0}^{p-2} a_k \zeta_p^k$, missä $a_k \in \mathbb{Z}$ kaikilla k. Tavoitteena on todistaa, että $\alpha \equiv 0 \bmod 1-\zeta_p$. Koska $\zeta_p \equiv 1 \bmod 1-\zeta_p$, niin $\alpha \equiv \sum_{k=0}^{p-2} a_k \bmod 1-\zeta_p$. Näin ollen riittää todistaa, että

$$\sum_{k=0}^{p-2} a_k \equiv 0 \bmod 1-\zeta_p.$$

Nyt koska $\alpha \equiv \sum_{k=0}^{p-2} a_k \bmod 1-\zeta_p$, niin

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha) \equiv N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\sum_{k=0}^{p-2} a_k) \bmod 1-\zeta_p.$$

Koska luvut a_k ovat kokonaislukuja, niin

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\sum_{k=0}^{p-2} a_k) = (\sum_{k=0}^{p-2} a_k)^{p-1}.$$

Lisäksi on oletettu, että p jakaa normin $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha)$, joten

$$(\sum_{k=0}^{p-2} a_k)^{p-1} \equiv 0 \bmod 1-\zeta_p.$$

Koska $\sum_{k=0}^{p-2} a_k \in \mathbb{Z}$, niin $(\sum_{k=0}^{p-2} a_k)^{p-1} \equiv 0 \bmod p$. Täten p jakaa luvun $\sum_{k=0}^{p-2} a_k$ ja saadaan $\sum_{k=0}^{p-2} a_k \equiv 0 \bmod 1-\zeta_p$. Siis $\alpha \equiv 0 \bmod 1-\zeta_p$. Näin ollen $\mathfrak{p}$ on alkuihanne. $\square$

2.2 p-adiset luvut

Tässä luvussa tutustutaan p-adisten lukujen kuntaan ja sen laajennukseen. Ensimmäiseksi konstruoidaan p-adisten lukujen kunta. Tämän konstruoinnin päämääränä on saada aikaiseksi täydellinen metrinen avaruus, jonka laajennus voidaan käyttää apuna kongruensseja laskettaessa. Kun p-adisten lukujen kunta on konstruoitu, tutustutaan muutamaan sen ominaisuuteen. Tämän jälkeen tarkastellaan p-adisten lukujen kunnan laajennusta, joka sisältää alkion ζ_p.

Luvun todistukset perustuvat Gouvêan kirjan [4] todistuksiin. Käsittely perustuu normiavaruuksiin, joten lukijan olisi hyvä tuntea perusteet normiavaruuksista ja topologiasta. Näihin voi tutustua esimerkiksi luentomonisteen [16] avulla.

Merkinnällä (x_n) tarkoitetaan jonoa $x_0, x_1, x_2, \ldots$. Jos jonon määrittelyssä ei esiinny indeksiä n, se on vakiojono. Esimerkiksi (1) tarkoittaa jonoa $1, 1, 1, \ldots$ ja (x) jonoa $x, x, x, \ldots$. Jokaisen jonon indeksointi alkaa luvusta nolla.

2.2.1 Kunta $\mathbb{Q}_p$

On monia eri tapoja konstruoida p-adisten lukujen kunta. Tässä tutkielmassa käytetään normiavaruuksiin perustuvaa tapaa. Tätä varten määrittelemme aluksi normin $|\cdot|_p$ rationaaliluvuille. Myöhemmin tätä normia käytetään apuna p-adisen lukukunnan konstruoinnissa. Otetaan ensin käyttöön apukuvaus v_p.

Määritelmä 2.22. Olkoon p kiinnitetty alkuluku ja $\frac{a}{b}$ rationaaliluku, jolle $a, b \neq 0$. Lisäksi olkoon $\frac{a}{b} = p^n \frac{a'}{b'}$, missä $n, a', b' \in \mathbb{Z}$ ja $p \nmid a'b'$. Määritellään tällöin $v_p(\frac{a}{b}) = n$. Lisäksi määritellään $v_p(0) = \infty$.

Kokonaislukujen yksikäsitteisen tekijöihinjaon takia kuvaus v_p on hyvinmääritelty rationaalilukujen joukossa. Todistetaan kuvaukselle v_p muutama ominaisuus.

Lause 2.23. Olkoot $x, y \in \mathbb{Q}$. Tällöin

- $v_p(xy) = v_p(x) + v_p(y)$ ja
- $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Todistus. Jos vähintään toinen luvuista x ja y on nolla, niin $xy = 0$ ja $v_p(xy) = \infty$. Toisaalta funktion v_p määritelmän mukaan $v_p(z)$ saa äärellisen arvon kaikilla rationaaliluvuilla $z \neq 0$. Täten, jos toinen luvuista x, y

on nolla, niin $v_p(x) + v_p(y) = \infty$. Siis väite $v_p(xy) = v_p(x) + v_p(y)$ on voimassa, kun vähintään toinen luvuista x, y on nolla. Voidaan olettaa, että molemmat luvut x, y eroavat nollasta. Olkoot $x = p^{n_1}\frac{a_1}{b_1}$ ja $y = p^{n_2}\frac{a_2}{b_2}$, missä $n_1, a_1, b_1, n_2, a_2, b_2 \in \mathbb{Z}$, $p \nmid a_1b_1$ ja $p \nmid a_2b_2$. Tällöin $xy = p^{n_1+n_2}\frac{a_1a_2}{b_1b_2}$ ja $p \nmid a_1a_2b_1b_2$. Siis $v_p(xy) = n_1 + n_2 = v_p(x) + v_p(y)$.

Todistetaan nyt, että $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$. Jos vähintään toinen luvuista x, y on nolla, niin väite on selvä. Oletetaan siis, että molemmat luvuista x, y ovat erisuuria kuin nolla. Kirjoitetaan x, y samassa muodossa kuin edellisessä kappaleessa. Tällöin $v_p(x) = n_1$ ja $v_p(y) = n_2$. Voidaan symmetrian nojalla olettaa, että $\min\{v_p(x), v_p(y)\} = v_p(x)$. Ottamalla p^{n_1} yhteiseksi tekijäksi nähdään, että $x + y = p^{n_1}(\frac{a_1}{b_1} + p^{n_2-n_1}\frac{a_2}{b_2})$. Koska $n_2 - n_1 = v_p(y) - v_p(x) \geq 0$, niin $p^{n_2-n_1}$ on kokonaisluku. Täten voidaan kirjoittaa $p^{n_1}(\frac{a_1}{b_1} + p^{n_2-n_1}\frac{a_2}{b_2}) = p^{n_1}(\frac{a_1b_2+p^{n_2-n_1}a_2b_1}{b_1b_2})$, missä osoittajassa ja nimittäjässä esiintyy kokonaislukuja. Koska $p \nmid b_1b_2$, niin $v_p(p^{n_1}(\frac{a_1b_2+p^{n_2-n_1}a_2b_1}{b_1b_2})) \geq n_1$. Siis $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$. □

Rationaalilukujen joukko voidaan tulkita avaruutena, jonka kerroinkuntana on joukko itse. Voidaan määritellä avaruudelle $\mathbb{Q}$ normi $|\cdot|_p$.

Määritelmä 2.24. Olkoon $x \neq 0$ rationaaliluku. Tällöin määritellään $|x|_p = p^{-v_p(x)}$. Lisäksi määritellään $|0|_p = 0$.

Lause 2.25. Kuvaus $|\cdot|_p$ toteuttaa ehdot

- $|x|_p \geq 0$ kaikilla rationaaliluvuilla x,
- $|x|_p = 0$ jos ja vain jos $x = 0$,
- $|xy|_p = |x|_p|y|_p$ kaikilla rationaaliluvuilla x, y ja
- $|x + y|_p \leq \max\{|x|_p, |y|_p\}$ kaikilla rationaaliluvuilla x, y.

Siis $|\cdot|_p$ on avaruuden $\mathbb{Q}$ normi.

Todistus. Koska kuvaus v_p on hyvinmääritelty kaikille rationaaliluvuille, niin kuvaus $|\cdot|_p$ on myös hyvinmääritelty kaikille rationaaliluvuille. Ensimmäinen ehto on voimassa, koska $p^{-n} > 0$ kaikilla kokonaisluvuilla n. Tästä myös nähdään, että $|x|_p = 0$ jos ja vain jos $x = 0$. Kaksi muuta ehtoa ovat selvästi voimassa, kun vähintään toinen luvuista x, y on nolla. Voidaan siis olettaa, että molemmat luvuista x, y eroavat nollasta. Määritelmän mukaan $|xy|_p = p^{-v_p(xy)}$ ja $|x|_p|y|_p = p^{-v_p(x)}p^{-v_p(y)}$. Lauseen 2.23 nojalla $p^{-v_p(xy)} = p^{-v_p(x)}p^{-v_p(y)}$, joten $|xy|_p = |x|_p|y|_p$. Koska $|x + y|_p = p^{-v_p(x+y)}$ ja lauseen 2.23 mukaan $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$, niin $|x + y|_p \leq$

$p^{-\min\{v_p(x),v_p(y)\}}$. Täten viimeinenkin ehto on voimassa. Koska ehdosta Koska $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ seuraa $|x+y|_p \leq |x|_p + |y|_p$, niin kuvaus $|\cdot|_p$ on avaruuden $\mathbb{Q}$ normi. □

Joissain myöhemmissä todistuksissa käytetään tavallista normiavaruuden kolmioepäyhtälön muotoilua $|x+y|_p \leq |x|_p+|y|_p$. Kuitenkin p-adisten lukujen teorian kannalta on oleellista, että normi $|\cdot|_p$ toteuttaa vahvemman ominaisuuden $|x+y|_p \leq \max\{|x|_p, |y|_p\}$. Tämä osoittautuu tarpeelliseksi esimerkiksi p-adisia kokonaislukuja tarkasteltaessa kuten lauseessa 2.42 nähdään.

Koska nyt on saatu määriteltyä rationaaliluvuille normi $|\cdot|_p$, niin voidaan siirtyä p-adisten lukujen kunnan konstruointiin. Tätä varten määritellään joukot $\mathcal{C}$ ja $\mathcal{N}$.

Määritelmä 2.26. Määritellään joukko $\mathcal{C}$ seuraavasti:

$$\mathcal{C} = \{(x_n) : (x_n) \text{ on Cauchy-jono normin } |\cdot|_p \text{ suhteen avaruudessa } \mathbb{Q}\}.$$

Todistetaan, että $\mathcal{C}$ on rengas, kun siinä on määritelty yhteen- ja kertolasku. Tätä varten todistetaan ensin aputulos, että joukon $\mathcal{C}$ jonot (x_n) ovat rajoitettuja normin $|\cdot|_p$ suhteen.

Lemma 2.27. Jokainen $(x_n) \in \mathcal{C}$ on rajoitettu rationaalilukujen normin $|\cdot|_p$ suhteen.

Todistus. Todistetaan ensin aputulos $||x|_p - |y|_p| \leq |x-y|_p$ kaikilla rationaaliluvuilla x ja y. Olkoot $x, y \in \mathbb{Q}$ mielivaltaiset. Voidaan kirjoittaa $|x|_p = |(x-y)+y|_p$. Lauseen 2.25 mukaan $|x-y+y|_p \leq |x-y|_p+|y|_p$. Täten $|x|_p-|y_p| \leq |x-y|_p$. Vastaavasti saadaan, että $|y|_p-|x|_p \leq |y-x|_p = |x-y|_p$. Näin ollen $||x|_p - |y|_p| \leq |x-y|_p$.

Todistetaan nyt lauseen pääväite edellisessä kappaleessa saadun ominaisuuden avulla. Olkoon $(x_n) \in \mathcal{C}$ mielivaltainen. Tällöin jostain indeksistä N lähtien $|x_n - x_{n'}|_p < 1$, kun $n, n' \geq N$. Erityisesti epäyhtälö pätee, kun $n' = N$. Edellisessä kappaleessa todistetun epäyhtälön nojalla

$$||x_n|_p - |x_N|_p| \leq |x_n - x_N|_p.$$

Täten $||x_n|_p - |x_N|_p| < 1$. Siis $|x_N|_p - 1 < |x_n|_p < 1 + |x_N|_p$. Näin ollen jono $(x_n)_{n\geq N}$ on rajoitettu metriikan $|\cdot|_p$ suhteen. Joukossa $\{|x_n|_p : n < N\}$ on vain äärellisen monta alkiota, joten sieltä löydetään minimi ja maksimi. Täten jono (x_n) on rajoitettu metriikan $|\cdot|_p$ suhteen. □

Lause 2.28. Olkoot $(x_n), (y_n) \in \mathcal{C}$. Määritellään tällöin

$$\begin{cases} (x_n) + (y_n) = (x_n + y_n) \\ (x_n)(y_n) = (x_n y_n). \end{cases}$$

Näin määriteltynä $\mathcal{C}$ on kommutatiivinen rengas.

Todistus. Määritellyt laskutoimitukset ovat selvästi hyvinmääriteltyjä. Todistetaan, että $\mathcal{C}$ on kommutatiivinen rengas tarkastamalla kommutatiivisen renkaan aksioomat.

Kaikki vakiojonot ovat Cauchy-jonoja metriikan $|\cdot|_p$ suhteen, joten $(1), (0) \in \mathcal{C}$. Todistetaan seuraavaksi, että $\mathcal{C}$ on suljettu yhteen- ja kertolaskun suhteen. Olkoot $(x_n), (y_n) \in \mathcal{C}$ mielivaltaisia. Todistetaan, että myös $(x_n + y_n)$ ja $(x_n y_n)$ ovat Cauchy-jonoja metriikan $|\cdot|_p$ suhteen. Olkoon $\epsilon > 0$ mielivaltainen. Tällöin on olemassa luonnolliset luvut $S, M \in \mathbb{N}$, joille $|x_{s'} - x_s|_p < \epsilon$ ja $|x_{m'} - x_m|_p < \epsilon$ kaikilla $s, s' \geq S, m, m' \geq M$. Olkoot $n, n' \geq \max\{S, M\}$ kokonaislukuja. Tällöin lauseen 2.25 nojalla

$$|x_n + y_n - x_{n'} - y_{n'}|_p = |x_n - x_{n'} + y_n - y_{n'}|_p < \epsilon.$$

Siis $(x_n) + (y_n) \in \mathcal{C}$.

Todistetaan, että $(x_n y_n) \in \mathcal{C}$. Lemman 2.27 mukaan jonot $(x_n), (y_n) \in \mathcal{C}$ ovat rajoitettuja. Näin ollen voidaan valita positiivinen kokonaisluku M, jolle $|x_n|_p < M$ ja $|y_n|_p < M$ kaikilla luonnollisilla luvuilla n. Olkoon $\epsilon > 0$ mielivaltainen. Samalla tavoin kuin edellisessä kappaleessa löydetään sellainen $N \in \mathbb{N}$, että $|x_n - x_{n'}|_p < \frac{\epsilon}{M}$ ja $|y_n - y_{n'}|_p < \frac{\epsilon}{M}$ kaikilla $n, n' \geq N$. Koska $|x_n y_n - x_{n'} y_{n'}|_p = |x_n y_n - x_n y_{n'} + x_n y_{n'} - x_{n'} y_{n'}|_p$, niin lauseen 2.25 nojalla

$$|x_n y_n - x_{n'} y_{n'}|_p \leq \max\{|x_n(y_n - y'_n)|_p, |y_{n'}(x_n - x'_n)|_p\}.$$

Lauseen 2.25 mukaan $\max\{|x_n(y_n - y'_n)|_p, |y_{n'}(x_n - x'_n)|_p\} < M\frac{\epsilon}{M} = \epsilon$, kun $n, n' \geq N$. Täten myös $(x_n)(y_n) \in \mathcal{C}$. Loput kommutatiivisen renkaan aksioomat ovat voimassa joukossa $\mathcal{C}$, koska ne ovat voimassa rationaaliluvuilla. Siis $\mathcal{C}$ on kommutatiivinen rengas. □

Seuraavaksi määritellään joukko $\mathcal{N}$. Joukko $\mathcal{N}$ määritellään sopivasti, jotta se on renkaan $\mathcal{C}$ maksimaalinen ihanne. Näin nimittäin saadaan määriteltyä p-adisten lukujen kunta $\mathcal{C}/\mathcal{N}$.

Määritelmä 2.29. $\mathcal{N} = \{(x_n) \in \mathcal{C} : \lim_{n\to\infty} |x_n|_p = 0\}$.

Lemma 2.30. Olkoon $(x_n) \in \mathcal{C}$ ja $\lim_{n\to\infty} |x_n|_p \neq 0$. Tällöin on olemassa positiiviset luvut c ja N, joille $|x_n|_p \geq c$ kaikilla $n \geq N$.

Todistus. Tehdään vastaoletus, että kaikkia positiivisten lukujen (c, N) pareja kohti löytyy ainakin yksi luonnollinen luku $n \geq N$, jolle $|x_n|_p < c$. Määritellään seuraavaksi luvut n_k. Olkoon $n_0 = 1$ ja

$$n_k = \min\{n : |x_n|_p < \frac{1}{k}, n_k > n_{k-1}\} \text{ kaikilla } k > 0.$$

Tällaiset luvut $n_0, n_1, n_2, \cdots$ ovat olemassa vastaoletuksen mukaan. Olkoon $(y_k) = (x_{n_k})$. Nyt $\lim_{k\to\infty} |y_k| = 0$. Koska (y_k) on jonon (x_n) osajono ja (x_n) on Cauchyn-jono, niin $\lim_{n\to\infty} |x_n| = 0$. Mutta tämä on ristiriita oletuksen kanssa. Siis vastaoletus oli väärin ja väite pätee. □

Lause 2.31. Joukko $\mathcal{N}$ on renkaan $\mathcal{C}$ maksimaalinen ihanne.

Todistus. Todistetaan ensin, että $\mathcal{N}$ on renkaan $\mathcal{C}$ ihanne. Tehdään tämä tarkastamalla ihannekriteerin ehdot. Joukon $\mathcal{N}$ määritelmästä seuraa, että $\mathcal{N} \subseteq \mathcal{C}$. Koska $(0) \in \mathcal{N}$, niin joukko $\mathcal{N}$ on epätyhjä. Olkoot $(x_n), (y_n) \in \mathcal{N}$ ja $(c_n) \in \mathcal{C}$ mielivaltaisia. Todistetaan, että $(x_n) - (y_n) \in \mathcal{N}$. Lauseen 2.28 mukaan $(x_n) + (y_n) \in \mathcal{C}$. On siis todistettava, että $\lim_{n\to\infty} |x_n - y_n|_p = 0$. Olkoon $\epsilon > 0$ mielivaltainen. Koska $(x_n), (y_n) \in \mathcal{N}$, niin on olemassa sellainen luonnollinen luku N, että $|x_n|_p < \epsilon$ ja $|y_n|_p < \epsilon$ kaikilla $n \geq N$. Lisäksi kuvauksen $|\cdot|_p$ määritelmän mukaan $|-y_n|_p = |y_n|_p$ kaikilla luonnollisilla luvuilla n. Täten lauseen 2.25 nojalla

$$|x_n - y_n|_p < \max\{|x_n|_p, |-y_n|_p\} < \epsilon, \text{ kun } n \geq N.$$

Siis $(x_n) - (y_n) \in \mathcal{N}$.

Ihannekriteerin voimassaolon varmistamiseksi todistetaan vielä, että $(c_n)(x_n) \in \mathcal{N}$. Lauseen 2.28 mukaan $(c_n)(x_n) \in \mathcal{C}$. On siis todistettava, että $\lim_{n\to\infty} |c_n x_n|_p = 0$. Lemman 2.27 mukaan on olemassa sellainen luonnollinen luku M, että $|c_n|_p < M$ kaikilla luonnollisilla luvuilla n. Olkoon $\epsilon > 0$ mielivaltainen. Tällöin on olemassa sellainen luonnollinen luku N, että $|x_n|_p < \frac{\epsilon}{M}$ kaikilla $n \geq M$. Täten lauseen 2.25 mukaan $|c_n x_n|_p < M\frac{\epsilon}{M} = \epsilon$ kaikilla $n \geq N$. Siis myös $(c_n)(x_n) \in \mathcal{N}$. Ihannekriteerin mukaan $\mathcal{N}$ on renkaan $\mathcal{C}$ ihanne.

Todistetaan vielä ihanteen $\mathcal{N}$ maksimaalisuus. Olkoon $(x_n) \in \mathcal{C}$, mutta $(x_n) \notin \mathcal{N}$. Merkitään tällöin symbolilla I alkion (x_n) ja ihanteen $\mathcal{N}$ generoimaa renkaan $\mathcal{C}$ ihannetta. Tavoitteena on todistaa, että $I = \mathcal{C}$, koska tästä seuraa ihanteen $\mathcal{N}$ maksimaalisuus. Tämä tehdään osoittamalla, että $(1) \in I$. Koska $(x_n) \notin \mathcal{N}$, niin lemman 2.30 mukaan on olemassa positiiviset luvut c ja N, joille $|x_n|_p \geq c$ kaikilla $n \geq N$. Näin ollen $x_n \neq 0$, kun $n \geq N$. Tämän tiedon avulla saadaan muodostettua jonolle $(x_n)_{n\geq N}$ käänteisalkio. Määritellään jono (y_n) seuraavasti

$$y_n = \begin{cases} \frac{1}{x_n}, & \text{kun } n \geq N \\ 0, & \text{kun } n < N \end{cases}.$$

Todistetaan, että $(y_n) \in \mathcal{C}$. Selvästi (y_n) on rationaalilukujen jono, koska $(x_n) \in \mathcal{C}$. Todistetaan vielä, että (y_n) on Cauchy-jono metriikan $|\cdot|_p$ suhteen.

Olkoon $\epsilon > 0$ mielivaltainen. Koska (x_n) on Cauchy-jono, niin on olemassa sellainen luonnollinen luku M, että $|x_m - x_{m'}|_p < \epsilon$, kun $m, m' \geq M$. Olkoot $S = \max\{N, M\}$ ja $s, s' \geq S$ luonnollisia lukuja. Tällöin jonon (y_n) määritelmän mukaan $|y_s - y_{s'}|_p = |\frac{1}{x_s} - \frac{1}{x_{s'}}|_p$. Tämä voidaan edelleen sieventää muotoon $|\frac{1}{x_s} - \frac{1}{x_{s'}}|_p = |\frac{x_{s'} - x_s}{x_s x_{s'}}|_p$. Lukujen s ja s' valinnan takia $|\frac{x_{s'} - x_s}{x_s x_{s'}}|_p < \frac{\epsilon}{c^2} < \epsilon$. Siis (y_n) on Cauchy-jono ja $(y_n) \in \mathcal{C}$.

Päätellään, että $I = \mathcal{C}$. Suoraan laskemalla saadaan

$$y_n x_n = \begin{cases} 1, & \text{kun } n \geq N \\ 0, & \text{kun } n < N \end{cases}.$$

Täten $(1) - (y_n x_n) \in \mathcal{N}$. Koska määritelmän mukaan $(x_n) \in I$ ja edellisen todistuksen nojalla $(y_n) \in \mathcal{C}$, niin $(y_n x_n) \in I$. Siis $(1) \in I$, koska $(1) = \mathcal{N} + (y_n x_n) \in I$. Täten $I = \mathcal{C}$ ja väite on todistettu.

□

Tähän mennessä saadun teorian avulla voidaan määritellä p-adisten lukujen kunta.

Määritelmä 2.32. $\mathbb{Q}_p = \mathcal{C}/\mathcal{N}$

Lause 2.33. Joukko $\mathbb{Q}_p$ on kunta. Sitä kutsutaan *p-adisten lukujen kunnaksi* ja sen alkiot ovat *p-adisia lukuja*.

Todistus. Lauseen 2.28 mukaan $\mathcal{C}$ on kommutatiivinen rengas ja lauseen 2.31 mukaan $\mathcal{N}$ on renkaan $\mathcal{C}$ maksimaalinen ihanne. Täten $\mathbb{Q}_p = \mathcal{C}/\mathcal{N}$ on kunta.
□

Tutustutaan seuraavaksi p-adisten lukujen kunnan hyödylliseen ominaisuuteen rationaalilukuihin liittyen.

Lause 2.34. On olemassa rengas K, jolle $\mathbb{Q} \simeq K$ ja $K \subseteq \mathbb{Q}_p$.

Todistus. Olkoon $K = \{(q) : q \in \mathbb{Q}\}$. Tällöin $K \subseteq \mathbb{Q}_p$. Tämä on rengas rationaalilukujen ominaisuuksien ja alirengaskriteerin takia. Tarkastellaan kuvausta $\psi : \mathbb{Q} \to K$, missä $\psi(q) = (q)$ kaikilla rationaaliluvuilla q. Kuvaus ψ on hyvinmääritelty ja bijektio. Todistetaan, että ψ on rengashomomorfismi. Olkoot $q_1, q_2 \in \mathbb{Q}$ mielivaltaisia. Tällöin $\psi(q_1 + q_2) = (q_1 + q_2)$. Renkaan $\mathcal{C}$ yhteenlaskun määritelmän mukaan $(q_1 + q_2) = (q_1) + (q_2) = \psi(q_1) + \psi(q_2)$. Siis $\psi(q_1 + q_2) = \psi(q_1) + \psi(q_2)$. Vastaavasti hyödyntäen renkaan $\mathcal{C}$ kertolaskun määritelmää saadaan $\psi(q_1 q_2) = \psi(q_1)\psi(q_2)$. Lisäksi $\psi(1) = (1)$. Täten K toteuttaa halutut ehdot. □

Isomorfisuuden takia voidaan tulkita $\mathbb{Q} \subseteq \mathbb{Q}_p$. Tällöin nimenomaan $q \to (q)$ jokaiselle rationaaliluvulle q. Tietoa käytetään useissa luvun 3 todistuksissa. Seuraavaksi laajennetaan normi $|\cdot|_p$ avaruuteen $\mathbb{Q}_p$. Tätä ennen on todistetaan aputulos, jotta kuvaus saadaan hyvinmääritellyksi.

Lause 2.35. Olkoon $(x_n) \in \mathcal{C}$ ja $(x_n) \notin \mathcal{N}$. Tällöin on olemassa sellainen kokonaisluku N, että $|x_n|_p = |x_{n'}|_p$ kaikilla $n, n' \geq N$.

Todistus. Olkoon (x_n) lukujono, joka toteuttaa lauseen ehdot. Lauseen 2.30 nojalla on olemassa kokonaisluku N_1 ja luku $c > 0$, joille $|x_n|_p \geq c$ kaikilla $n \geq N$. Toisaalta (x_n) on Cauchy-jono, joten on olemassa sellainen kokonaisluku N_2, että $|x_n - x_{n'}|_p < c$ kaikilla $n, n' \geq N_2$. Olkoot $N = \max\{N_1, N_2\}$ ja $n, n' \geq N$. Tällöin $|x_n - x_{n'}|_p < c$ ja $c \leq \max\{|x_n|_p, |x_{n'}|_p\}$. Siis

$$|x_n - x_{n'}|_p < \max\{|x_n|_p, |x_{n'}|_p\}.$$

Todistetaan, että $|x_n|_p = |x_{n'}|_p$.

Tehdään vastaoletus, että $|x_n|_p \neq |x_{n'}|_p$ jollain $n, n' \geq N$. Näytetään, että $|x_n + x_{n'}|_p = \max\{|x_n|_p, |x_{n'}|_p\}$. Symmetrian nojalla voidaan olettaa, että $|x_n|_p > |x_{n'}|_p$. Voidaan kirjoittaa $|x_n|_p = |x_n + x_{n'} - x_{n'}|_p$. Täten lauseen 2.25 mukaan $|x_n|_p \leq \max\{|x_n + x_{n'}|_p, |x_{n'}|_p\}$. Ei voi olla

$$\max\{|x_n + x_{n'}|_p, |x_{n'}|_p\} = |x_{n'}|_p,$$

sillä tällöin saataisiin ristiriita oletuksen $|x_n|_p > |x_{n'}|_p$ kanssa. Siis

$$\max\{|x_n + x_{n'}|_p, |x_{n'}|_p\} = |x_n + x_{n'}|_p.$$

Toisaalta lauseen 2.25 mukaan

$$|x_n + x_{n'}|_p \leq \max\{|x|_p, |x_{n'}|_p\} = |x_n|_p.$$

Täten $|x_n + x_{n'}|_p = \max\{|x_n|_p, |x_{n'}|_p\}$. Edellisessä kappaleessa kuitenkin todistettiin, että $|x_n - x_{n'}|_p < \max\{|x_n|_p, |x_{n'}|_p\}$. Näin ollen on oltava $|x_n|_p = |x_{n'}|_p$ kaikilla $n, n' \geq N$. □

Määritelmä 2.36. Olkoon $\lambda \in \mathbb{Q}_p$ ja $\lambda = (x_n)$. Tällöin $|\lambda|_p = \lim_{n\to\infty} |x_n|_p$.

Lause 2.37. Määritelmässä 2.36 esiintyvä kuvaus $|\cdot|_p$ on avaruuden $\mathbb{Q}_p$ normi.

Todistus. Lauseen 2.35 nojalla jokaiselle jonolle $(x_n) \in \mathcal{C}$ ja $(x_n) \notin \mathcal{N}$ on määritelty $\lim_{n\to\infty} |x_n|_p$. Todistetaan, että kuvaus $|\cdot|_p$ on hyvinmääritelty. Olkoon $\lambda = (x_n) + (y_n) = (x'_n) + (y'_n)$, missä $(x_n), (x'_n) \in \mathcal{C}$, $(x_n), (x'_n) \notin \mathcal{N}$

ja $(y_n), (y'_n) \in \mathcal{N}$. Jokaista $\lambda \in \mathbb{Q}_p$ kohti löytyy ainakin yksi tällainen esitys kunnan $\mathbb{Q}_p$ määritelmän mukaan. Nyt $(x_n) - (x'_n) = (y'_n) - (y_n) \in \mathcal{N}$. Täten jokaista $\epsilon > 0$ kohti löytyy sellainen luonnollinen luku N, että $|x_n - x'_n|_p < \epsilon$ kaikilla $n \geq N$. Koska $(x_n) - (x'_n) \in \mathcal{C}$, niin lemman 2.27 todistuksen mukaan $||x_n|_p - |x'_n|_p| \leq |x_n - x'_n|_p$. Täten

$$|x'_n|_p - \epsilon < |x_n|_p < \epsilon + |x'_n|_p, \text{ kun } n \geq N.$$

Siis $\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |x'_n|_p$. Näin ollen kuvaus $|\cdot|_p$ on hyvinmääritelty.

Todistetaan vielä, että avaruudessa $\mathbb{Q}_p$ määritelty kuvaus $|\cdot|_p$ on normi. Koska avaruudessa $\mathbb{Q}$ pätee $|x_n|_p \geq 0$ kaikilla rationaaliluvuilla x_n, niin $\lim_{n\to\infty} |x_n|_p \geq 0$ kaikilla $(x_n) \in \mathbb{Q}_p$. Lisäksi $\lim_{n\to\infty} |x_n|_p = 0$ jos ja vain jos $(x_n) \in \mathcal{N}$. Olkoot $(x_n), (y_n) \in \mathbb{Q}_p$. Tällöin lauseen 2.25 mukaan

$$\lim_{n\to\infty} |x_n + y_n|_p \leq \lim_{n\to\infty} \max\{|x_n|_p, |y_n|_p\}.$$

Koska $\lim_{n\to\infty} \max\{|x_n|_p, |y_n|_p\} = \max\{\lim_{n\to\infty} |x_n|_p, \lim_{n\to\infty} |y_n|_p\}$, niin

$$|(x_n) + (y_n)|_p \leq \max\{|(x_n)|_p, |(y_n)|_p\}.$$

Vastaavasti todistetaan, että $|(x_n y_n)|_p = |(x_n)|_p |(y_n)|_p$, kun otetaan huomioon, että $\lim_{n\to\infty} |x_n| \neq 0$ ja $\lim_{n\to\infty} |x_n| \neq 0$, kun (x_n) ja (y_n) eivät ole nollajonoja. Jos taas jompikumpi on nollajono, niin edellinen väite on selvä. Siis $\mathbb{Q}_p$ on normiavaruus kuvauksen $|\cdot|_p$ suhteen. □

Kun tulkitaan jokainen rationaaliluku q vakiojonona (q), niin havaitaan, että avaruuden $\mathbb{Q}_p$ normi on avaruuden $\mathbb{Q}$ normin $|\cdot|_p$ laajennus. Näin ollen merkinnän $|\cdot|_p$ käyttö kummassakin avaruudessa $\mathbb{Q}$ ja $\mathbb{Q}_p$ on perusteltua. Vastaavalla tavalla voidaan laajentaa kuvaus v_p avaruuteen $\mathbb{Q}_p$. Olkoon $\lambda \in \mathbb{Q}_p$ ja $\lambda = (x_n)$. Tällöin $v_p(\lambda) = \lim_{n\to\infty} v_p(x_n)$. Tämä voidaan todistaa hyvinmääritellyksi samoin kuin $|\cdot|_p$ todistettiin hyvinmääritellyksi. On myös huomattava, että avaruudessa $\mathbb{Q}_p$ pätee $|\lambda|_p = p^{-v_p(\lambda)}$.

Seuraavana päämääränä on todistaa, että $\mathbb{Q}_p$ on täydellinen avaruus normin $|\cdot|_p$ indusoiman metriikan suhteen. Tätä varten otetaan käyttöön muutamia apumääritelmiä ja -lauseita.

Määritelmä 2.38. Olkoon $\lambda \in \mathbb{Q}_p$ ja $\lambda = \lim_{n\to\infty} x_n$, missä $(x_n) \in \mathcal{C}$ ja $(x_n) \notin \mathcal{N}$. Kutsutaan jonoa (x_n) alkion λ *edustajaksi*.

Lemma 2.39. Olkoon $\lambda \in \mathbb{Q}_p$ ja $r > 0$. Tällöin jokainen pallo

$$B(\lambda, r) = \{\lambda' \in \mathbb{Q}_p : |\lambda - \lambda'|_p < r\}$$

sisältää vähintään yhden vakiojonon (x).

Todistus. Olkoot $\lambda \in \mathbb{Q}_p$ mielivaltainen, (x_n) sen edustaja ja $r > 0$ mielivaltainen. On olemassa luku r', jolle $0 < r' < r$. Koska (x_n) on Cauchy-jono, niin voidaan löytää sellainen luonnollinen luku N, että $|x_n - x_{n'}|_p < r'$ kaikilla kokonaisluvuilla $n, n' \geq N$. Olkoon $x = x_N$. Todistetaan, että $(x) \in B(\lambda, r)$. Metriikan $|\cdot|_p$ määritelmän mukaan $|\lambda - (x)|_p = \lim_{n\to\infty} |x_n - x|_p$. Lisäksi luvun x määritelmän nojalla $|x_n - x|_p < r'$ kaikille $n \geq N$. Täten

$$\lim_{n\to\infty} |x_n - x|_p \leq r' < r.$$

Siis $(x) \in B(\lambda, r)$. □

Lause 2.40. Joukko $\mathbb{Q}_p$ on täydellinen normin $|\cdot|_p$ indusoiman metriikan suhteen.

Todistus. Olkoon (λ_n) Cauchy-jono avaruudessa $\mathbb{Q}_p$. Päämääränä on löytää avaruuden $\mathbb{Q}_p$ alkio, jotka kohti jono (λ_n) suppenee. Lemman 2.39 mukaan jokaista λ_n kohti löytyy rationaaliluku $y^{(n)}$, jolle $|\lambda_n - (y^{(n)})|_p < \frac{1}{n}$. Olkoot $y^{(1)}, y^{(2)}, y^{(3)}, \cdots$ tämän ehdon toteuttavia rationaalilukuja. Tällöin $\lim_{n\to\infty} |\lambda_n - (y^{(n)})|_p = 0$. Todistetaan, että luvut $y^{(n)}$ muodostavat Cauchy-jonon avaruuden $\mathbb{Q}$ normin $|\cdot|_p$ indusoiman metriikan suhteen.

Olkoon $(x_j^{(n)})$ alkion λ_n edustaja ja $\epsilon > 0$ mielivaltainen. Koska (λ_n) on Cauchy-jono avaruudessa $\mathbb{Q}_p$, niin on olemassa sellainen luonnollinen luku N_1, että

$$\lim_{j\to\infty} |x_j^{(n)} - x_j^{(n')}|_p = |\lambda_n - \lambda_{n'}|_p < \frac{\epsilon}{3} \text{ kaikilla } n, n' \geq N_1. \tag{8}$$

Lukujen $y^{(n)}$ valinnan perusteella löytyy sellainen luonnollinen luku N_2, että

$$\lim_{j\to\infty} |x_j^{(n)} - y^{(n)}|_p = |\lambda_n - (y^{(n)})|_p < \frac{\epsilon}{3} \text{ kaikilla kokonaisluvuilla } n \geq N_2. \tag{9}$$

Olkoon $N = \max\{N_1, N_2\}$. Lauseen 2.25 nojalla

$$|y^{(n)} - y^{(n')}|_p \leq |y^{(n)} - x_j^{(n)}|_p + |x_j^{(n)} - x_j^{(n')}|_p + |x_j^{(n)} - y^{(n')}|_p. \tag{10}$$

Epäyhtälöiden (8), (9) ja (10) nojalla saadaan

$$\lim_{j\to\infty} |y^{(n)} - y^{(n')}|_p < 3\frac{\epsilon}{3} = \epsilon, \text{ kun } n, n' \geq N.$$

Siis $|y^{(n)} - y^{(n')}|_p < \epsilon$, kun $n, n' \geq N$. Täten luvut $y^{(n)}$ muodostavat Cauchy-jonon. Siis jono $y^{(1)}, y^{(2)}, y^{(3)}, \cdots$ kuuluu renkaaseen $\mathcal{C}$. Merkitään tätä Cauchy-jonoa symbolilla λ.

Todistetaan aiempien tietojen avulla, että jonolla (λ_n) on raja-arvo avaruudessa $\mathbb{Q}_p$. Tarkastellaan ensin tapausta $\lambda \in \mathcal{N}$. Tällöin $\lim_{n\to\infty} y^{(n)} = 0$. Näin ollen $0 = \lim_{n\to\infty} |\lambda_n - (y^{(n)})|_p = \lim_{n\to\infty} |\lambda_n|_p$. Siis $\lim_{n\to\infty} \lambda_n - (y^{(n)}) = (0)$. Täten (λ_n) suppenee kohti avaruuden $\mathbb{Q}_p$ lukua. Tarkastellaan vielä tapausta $\lambda \notin \mathcal{N}$. Todistetaan, että $\lim_{n\to\infty} \lambda_n = \lambda$. Koska

$$\lambda_n - \lambda = \lambda_n - (y^{(n)}) + (y^{(n)}) - \lambda,$$

niin lauseen 2.37 nojalla

$$|\lambda_n - \lambda|_p \leq |\lambda_n - (y^{(n)})|_p + |(y^{(n)}) - \lambda|_p. \tag{11}$$

Luvun $y^{(n)}$ valinnan mukaan $\lim_{n\to\infty} |\lambda_n - (y^{(n)})|_p = 0$. Lisäksi

$$|(y^{(n)}) - \lambda|_p = \lim_{j\to\infty} |y^{(n)} - y^{(j)}|_p.$$

Koska luvut $y^{(n)}$ muodostavat Cauchy-jonon, niin $\lim_{n\to\infty} \lim_{j\to\infty} |y^{(n)} - y^{(j)}|_p = 0$. Siis epäyhtälön (11) nojalla $\lim_{n\to\infty} |\lambda_n - \lambda|_p = 0$. Näin ollen tässäkin tapauksessa (λ_n) suppenee kohti avaruuden $\mathbb{Q}_p$ lukua. Siis $\mathbb{Q}_p$ on täydellinen normin $|\cdot|_p$ suhteen.

□

2.2.2 Kunta $\mathbb{Q}_p(\zeta_p)$

Edellisessä luvussa konstruoitiin p-adisten lukujen joukko ja todistetettiin se täydelliseksi metriseksi avaruudeksi. Seuraavaksi tarkoituksena on tutkia p-adisten lukujen kunnan laajennusta $\mathbb{Q}_p(\zeta_p)$. Ennen tämän kunnan tarkastelua tutustutaan p-adisten kokonaislukujen renkaaseen, sillä sitä voidaan käyttää apuna kunnan $\mathbb{Q}_p(\zeta_p)$ rakenteen tutkimisessa.

Määritelmä 2.41. $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$

Lause 2.42. Joukko $\mathbb{Z}_p$ on kommutatiivinen rengas. Rengasta $\mathbb{Z}_p$ kutsutaan *p-adisten kokonaislukujen renkaaksi* ja sen alkioita *p-adisiksi kokonaisluvuiksi*.

Todistus. Koska lauseen 2.33 mukaan $\mathbb{Q}_p$ on kunta, niin todistetaan väite alirengaskriteerin avulla. Joukon $\mathbb{Z}_p$ määritelmän mukaan $\mathbb{Z}_p \subseteq \mathbb{Q}_p$. Lisäksi $(0) \in \mathbb{Z}_p$, joten $\mathbb{Z}_p$ on epätyhjä. Riittää enää todistaa, että $\mathbb{Z}_p$ on suljettu yhteen- ja kertolaskun suhteen. Olkoot $x, y \in \mathbb{Z}_p$ mielivaltaisia. Koska lauseen 2.37 mukaan $|\cdot|_p$ on avaruuden $\mathbb{Q}_p$ normi, niin $|xy|_p = |x|_p|y|_p$. Täten

$|xy|_p \leq 1$. Siis $xy \in \mathbb{Z}_p$. Lisäksi $|x+y|_p \leq \max\{|x|_p, |y|_p\}$, sillä näiden lukujen edustajille $(x_n), (y_n)$ pätee $|x_n + y_n|_p \leq \max\{|x_n|_p, |y_n|_p\}$ kaikilla $n \in \mathbb{N}$. Täten $|x+y|_p \leq 1$ eli $x + y \in \mathbb{Z}_p$. Siis $\mathbb{Z}_p$ on suljettu myös yhteenlaskun suhteen. Täten $\mathbb{Z}_p$ on rengas. □

Edellisessä lauseessa huomataan, että normin $|\cdot|_p$ määrittelyssä oli oleellista, että se toteuttaa ehdon $|x+y|_p \leq \max\{|x|_p, |y|_p\}$. Jos tämä ehto ei olisi voimassa, niin $\mathbb{Z}_p$ ei olisi suljettu yhteenlaskun suhteen.

Tarkastellaan seuraavaksi polynomien jaollisuutta yli renkaan $\mathbb{Z}_p$ ja yli kunnan $\mathbb{Q}_p$. Näitä tietoja tarvitaan, kun määritetään kunnan $\mathbb{Q}_p(\zeta_p)$ rakenne ja lasketaan kuntalaajennuksen $[\mathbb{Q}_p(\zeta_p) : \mathbb{Q}_p]$ aste. Saadut tulokset ovat hyvin samankaltaiset kuin polynomien jaollisuutta tarkasteltaessa rationaali- ja kokonaislukukertoimisten polynomien renkaissa. Rationaalilukukertoimiselle polynomille pätee, että jos se on jaollinen yli kunnan $\mathbb{Q}$, niin se on jaollinen myös yli renkaan $\mathbb{Z}$. Seuraavaksi todistetaan vastaava tulos kunnalle $\mathbb{Q}_p$ ja renkaalle $\mathbb{Z}_p$.

Lause 2.43. Oletetaan, että $f(x) \in \mathbb{Z}_p[x]$ on jaollinen yli kunnan $\mathbb{Q}_p$. Tällöin se on jaollinen myös yli renkaan $\mathbb{Z}_p$.

Todistus. Määritellään ensin todistusta helpottava apufunktio. Olkoon

$$r(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}_p[x].$$

Tällöin määritellään $k(r(x)) = \min\limits_{0 \leq i \leq n} v_p(a_i)$. Jos $r(x) \in \mathbb{Z}_p[x]$, niin on voimassa $k(r(x)) \geq 0$. Toisaalta, jos $k(r(x)) < 0$, niin jokin polynomin $r(x)$ kerroin a_i ei kuulu renkaaseen $\mathbb{Z}_p$. Siis $r(x) \in \mathbb{Z}_p[x]$ on yhtäpitävää ehdon $k(r(x)) \geq 0$ kanssa. Koska $f(x)$ on jaollinen yli kunnan $\mathbb{Q}_p$, niin voidaan olettaa $f(x) = g(x)h(x)$, missä $g(x), h(x) \in \mathbb{Q}_p[x]$, eikä kumpikaan polynomeista $g(x)$ tai $h(x)$ ole vakiopolynomi.

Todistetaan ensin, että väite pätee, kun $k(f(x)) = 0$. Oletetaan, että $k(f(x)) = 0$. Kuvauksen k määritelmän nojalla $k(g(x)) = v_p(b)$ jollain $b \in \mathbb{Q}_p$ ja täten $k(g(x)) = -v_p(b^{-1})$. Koska $\mathbb{Q}_p$ on kunta, niin $b^{-1} \in \mathbb{Q}_p$. Saadaan $k(b^{-1}g(x)) = v_p(b^{-1}) + k(g(x)) = 0$. Vastaavasti löydetään luku $c \in \mathbb{Q}_p$, jolle pätee $k(c^{-1}h(x)) = 0$. Tavoitteena on todistaa, että $bc \in \mathbb{Z}_p$. Tämän tiedon avulla saadaan, että polynomi $f(x)$ on jaollinen yli renkaan $\mathbb{Z}_p$.

Merkitään $g_1(x) = b^{-1}g(x)$, $h_1(x) = c^{-1}h(x)$ ja $f_1(x) = b^{-1}g(x)c^{-1}h(x)$. Tällöin $f_1(x) = g_1(x)h_1(x)$. Tiedetään, että $g_1(x), h_1(x), f_1(x) \in \mathbb{Z}_p[x]$. Redusoidaan polynomit $g_1(x), h_1(x)$ ja $f_1(x)$ modulo p, jolloin saadaan vastaavasti polynomit $\overline{g_1}(x)$, $\overline{h_1}(x)$ ja $\overline{f_1}(x)$. Koska $k(g_1(x)) = k(h_1(x)) = 0$, niin $\overline{g_1}(x)$ ja $\overline{h_1}(x)$ eivät ole nollapolynomeja. Täten myöskään $\overline{f_1}(x)$ ei ole nollapolynomi. Koska lisäksi on voimassa $f_1(x) \in \mathbb{Z}_p[x]$, niin on oltava $k(f_1(x)) = 0$.

Lisäksi $k(f_1(x)) = k(b^{-1}c^{-1}f(x))$ ja $k(b^{-1}c^{-1}f(x)) = k(b^{-1}c^{-1}) + k(f(x))$, joten $v_p(b^{-1}c^{-1}) = 0$. Näin ollen $b^{-1}c^{-1}$ on renkaan $\mathbb{Z}_p$ yksikkö. Siis polynomi $bcg_1(x) \in \mathbb{Z}_p[x]$. Merkitään $g_0(x) = bcg_1(x)$ ja $h_0(x) = h_1(x)$. Tällöin $f(x) = g_0(x)h_0(x)$ eli jaollinen yli renkaan $\mathbb{Z}_p$.

Todistetaan vielä, että väite pätee yleisessä tapauksessa. Koska $f(x) \in \mathbb{Z}_p[x]$, niin $k(f(x)) \geq 0$. Samalla tavalla kuin edellä löydetään luku $a \in \mathbb{Q}_p$, jolle $k(af(x)) = 0$. Merkitään $f_1(x) = af(x)$. Polynomi $f_1(x)$ on jaollinen yli kunnan $\mathbb{Q}_p$, koska $f_1(x) = ag(x)h(x)$ ja $ag(x), h(x) \in \mathbb{Q}_p[x]$. Täten edellä olevan todistuksen mukaan $f_1(x) = g_0(x)h_0(x)$, missä $g_0(x), h_0(x) \in \mathbb{Z}_p[x]$ ja kumpikaan polynomeista $g_0(x), h_0(x)$ ei ole vakiopolynomi. Luvun a valinnasta nähdään, että $a^{-1} \in \mathbb{Z}_p$. Täten $a^{-1}g_0(x) \in \mathbb{Z}_p[x]$. Näin ollen polynomi $f(x) = a^{-1}g_0(x)h_0(x)$ on jaollinen yli renkaan $\mathbb{Z}_p$. □

Laajennetaan seuraavaksi rationaalilukujen kuntaan liittyvä Eisensteinin jaottomuuskriteeri kuntaan $\mathbb{Q}_p$. Lauseen väite ja todistus ovat hyvin samantapaiset kuin rationaalilukujen yhteydessä voidaan tehdä.

Lause 2.44 (Eisensteinin jaottomuuskriteeri)**.** Olkoon

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x].$$

Oletetaan, että polynomi $f(x)$, joka toteuttaa seuraavat ehdot

- $|a_n|_p = 1$
- $|a_i|_p < 1$ kaikilla $0 \leq i < n$ ja
- $|a_0|_p = \frac{1}{p}$.

Tällöin $f(x)$ on jaoton yli kunnan $\mathbb{Q}_p$.

Todistus. Tehdään vastaoletus, että $f(x)$ on jaollinen yli kunnan $\mathbb{Q}_p$. Lauseen 2.43 mukaan $f(x)$ on jaollinen myös yli renkaan $\mathbb{Z}_p$. Olkoot $g(x), h(x) \in \mathbb{Z}_p[x]$ vähintään astetta 1 olevia polynomeja, joille $f(x) = h(x)g(x)$. Voidaan kirjoittaa

$$g(x) = b_r x^r + \cdots + b_1 x + b_0$$

ja

$$h(x) = c_m x^r + \cdots + c_1 x + c_0,$$

missä $r + m = n$. Koska $|a_0|_p = \frac{1}{p}$, niin tismalleen toinen luvuista b_0, c_0 ei ole jaollinen luvulla p renkaassa $\mathbb{Z}_p$. Oletetaan, että $p|b_0$ ja $p \nmid c_0$. Lisäksi on voimassa $|a_n|_p = 1$, $a_n = b_r c_m$ ja $a_n, b_r, c_m \in \mathbb{Z}_p$, joten $|b_r|_p = |c_m|_p = 1$. Näin ollen kumpikaan luvuista b_r, c_m ei ole jaollinen luvulla p renkaassa $\mathbb{Z}_p$. Löydetään siis pienin indeksi i, $0 < i \leq r < n$, jolle $p \nmid b_i$ renkaassa $\mathbb{Z}_p$.

Suoraan laskemalla saadaan $a_i = b_i c_0 + \cdots + b_1 c_{i-1} + b_0 c_i$. Voidaan laskea a_i modulo p renkaassa $\mathbb{Z}_p$ ja saadaan $a_i \equiv b_i c_0 \bmod p$. Oletusten mukaan $a_i \equiv 0 \bmod p$ eli $b_i c_0 \equiv 0 \bmod p$. Nyt kuitenkin vähintään toisen luvuista b_i tai c_0 on oltava jaollinen luvulla p renkaassa $\mathbb{Z}_p$. Tämä on ristiriita. Siis $f(x)$ ei ole jaollinen yli kunnan $\mathbb{Q}_p$. □

Edellisten apulauseiden avulla voidaan laskea laajennuksen $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ aste. Samalla saadaan selville tämän laajennuksen kanta.

Lause 2.45. $[\mathbb{Q}_p(\zeta_p) : \mathbb{Q}_p] = p - 1$

Todistus. Todistetaan väite etsimällä luvun ζ_p minimaalipolynomi yli kunnan $\mathbb{Q}_p$. Olkoon $\phi(x) = \sum_{k=0}^{p-1} x^k$. Tavoitteena on todistaa, että $\phi(x)$ on luvun ζ_p minimaalipolynomi yli kunnan $\mathbb{Q}_p$. Tunnetusti $\phi(\zeta_p) = 0$ ja lauseen 2.34 mukaan $\phi(x) \in \mathbb{Q}_p[x]$. Polynomin $\phi(x)$ jaottomuus yli kunnan $\mathbb{Q}_p$ todistetaan tutkimalla polynomia $g(x) = \phi(x+1)$. Lasketaan, mitä $g(x)$ on modulo p renkaassa $\mathbb{Z}_p$. Saadaan $g(x) = \frac{(x+1)^p - 1}{x+1-1}$ ja tästä suoraan laskemalla

$$\frac{(x+1)^p - 1}{x+1-1} \equiv \frac{x^p + 1 - 1}{x} \bmod p.$$

Siis $g(x) \equiv x^{p-1} \bmod p$. Näin ollen kaikki polynomin $g(x)$ kertoimet johtavaa kerrointa lukuun ottamatta ovat jaollisia luvulla p. Lisäksi polynomin $g(x)$ vakiotermi on $g(0) = \phi(1) = p$. Täten lauseen 2.44 mukaan polynomi $g(x)$ on jaoton yli kunnan $\mathbb{Q}_p$. Näin ollen myös $\phi(x)$ on jaoton yli kunnan $\mathbb{Q}_p$. Siis $\phi(x)$ on luvun ζ_p minimaalipolynomi yli kunnan $\mathbb{Q}_p$ ja $[\mathbb{Q}_p(\zeta_p) : \mathbb{Q}_p] = p - 1$. □

Edellisestä todistuksesta nähdään, että $\{1, \zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-2}\}$ muodostaa laajennuksen $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ kannan. Seuraavaksi todistetaan, että laajennus $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ on Galois'n laajennus ja tutkitaan sen automorfismien ryhmää. Automorfismeja tarvitaan, kun lasketaan luvussa 2.1 määriteltyä normeja yli Galois'n laajennusten.

Lause 2.46. Laajennus $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ on Galois'n laajennus ja

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) = \{\sigma_1, \sigma_2, \cdots, \sigma_{p-1}\}, \text{ missä } \sigma_k(\zeta_p) = \zeta_p^k.$$

Todistus. Todistetaan ensin, että $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ on Galois'n laajennus. Lauseen 2.45 mukaan laajennus $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ on äärellinen. Lisäksi polynomi

$$\phi(x) = x^{p-1} + x^{p-2} + \cdots + 1 = \prod_{j=1}^{p-1} (x - \zeta_p^j) \in \mathbb{Q}_p$$

hajoaa kunnassa $\mathbb{Q}_p(\zeta_p)$. Toisaalta, jos $\phi(x)$ hajoaa jossain kunnan $\mathbb{Q}_p$ laajennuksessa $K \subseteq \mathbb{Q}_p(\zeta_p)$, niin $\zeta_p \in K$. Näin ollen $K = \mathbb{Q}_p(\zeta_p)$. Siis $\mathbb{Q}_p(\zeta_p)$ on polynomin $\phi(x) \in \mathbb{Q}_p[x]$ hajoamiskunta ja täten laajennus $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ on normaali. Olkoon $\lambda \in \mathbb{Q}_p$ mielivaltainen ja (x_n) sen edustaja. Jos jollain positiivisella kokonaisluvulla pätee $n(x_n) = (0)$, niin $nx_n = 0$ kaikilla n. Koska luvut x_n ovat rationaalilukuja, niin $n = 0$ tai $x_n = 0$. Täten ei ole olemassa positiivista kokonaislukua n, jolle $n\lambda = (0)$ kaikilla $\lambda \in \mathbb{Q}_p$. Siis $\mathrm{char}(\mathbb{Q}_p) = 0$. Näin ollen $\mathbb{Q}_p$ on separoituva. Täten $\mathbb{Q}_p$ on Galois'n laajennus.

On enää todistettava, että ryhmä $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ sisältää halutut alkiot. Tämä voidaan tehdä täysin vastaavasti kuin lauseessa 2.14 tehty vastaava todistus ryhmälle $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. □

Tutustutaan vielä kahteen laajennuksen $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ ominaisuuteen, jotka muistuttavat laajennuksen $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ ominaisuuksia.

Lause 2.47. Olkoon

$$\mathcal{O} = \{\lambda \in \mathbb{Q}_p(\zeta_p) : f(\lambda) = 0 \text{ jollain pääpolynomilla } f(x) \in \mathbb{Z}_p[x]\}.$$

Tällöin jokaiselle $\lambda \in \mathcal{O}$ pätee $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(\lambda) \in \mathbb{Z}_p$.

Todistus. Väite voidaan todistaa samoin kuin lauseessa 2.11 todistettiin, että kaikille $\beta \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ pätee $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta) \in \mathbb{Z}$. Laajennuksen $\mathbb{Q}(\alpha)/\mathbb{Q}$ ja renkaan $\mathbb{Z}$ sijasta vain tarkastellaan laajennusta $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ ja rengasta $\mathbb{Z}_p$. □

Lause 2.48. Olkoon $\mathcal{O}$ kuten lauseessa 2.47. Tällöin $\mathbb{Z}_p[\zeta_p] = \mathcal{O}$.

Todistus. Vastaavasti kuin lauseessa 2.4 todistettiin, että kunnan kokonaislukujen joukko on rengas, voidaan todistaa, että $\mathcal{O}$ on rengas. Väite voidaan todistaa samoin kuin lauseessa 2.15 todistettiin, että $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$. Nyt vain tarkastellaan laajennusta $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ ja rengasta $\mathbb{Z}_p[\zeta_p]$ laajennuksen $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ ja renkaan $\mathbb{Z}[\zeta_p]$ sijasta. □

Laajennetaan seuraavaksi normi $|\cdot|_p$ avaruuteen $\mathbb{Q}_p(\zeta_p)$. Tavoitteena on, että avaruus $\mathbb{Q}_p(\zeta_p)$ olisi täydellinen tämän normin suhteen.

Lause 2.49. Määritellään kuvaus $|\cdot|_p : \mathbb{Q}_p(\zeta_p) \to \mathbb{R}$. Olkoon

$$x = \sum_{j=0}^{p-2} a_j \zeta_p^j \in \mathbb{Q}_p(\zeta_p).$$

Määritellään $|x|_p = \sup_j |a_j|_p$, missä oikean puolen $|\cdot|_p$ on avaruuden $\mathbb{Q}_p$ normi. Näin määritelty $|\cdot|_p$ on avaruuden $\mathbb{Q}_p(\zeta_p)$ normi.

Todistus. Määritelty kuvaus $|\cdot|_p$ on hyvinmääritelty, sillä $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ muodostaa laajennuksen $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ kannan. Lisäksi $\mathbb{Q}_p(\zeta_p)$ on vektoriavaruus, jonka kerroinkuntana on $\mathbb{Q}_p$. Todistetaan muut ehdot tarkastamalla, että normin määritelmän ehdot ovat voimassa.

Koska lauseen 2.37 mukaan $\mathbb{Q}_p$ on normiavaruus varustettuna normilla $|\cdot|_p$, niin avaruudessa $\mathbb{Q}_p(\zeta_p)$ pätee $|x|_p \geq 0$ kaikilla $x \in \mathbb{Q}_p(\zeta_p)$. Lisäksi

$$|x|_p = \sup_j |a_j|_p = 0, \text{ kun } |a_j|_p = 0 \text{ kaikilla } j.$$

Täten $|x|_p = 0$ jos ja vain jos $x = 0$. Olkoot $x, y \in \mathbb{Q}_p(\zeta_p)$ mielivaltaisia. Merkitään $x = \sum_{j=0}^{p-2} a_j \zeta_p^j$ ja $y = \sum_{j=0}^{p-2} b_j \zeta_p^j$, missä $a_j, b_j \in \mathbb{Q}_p$ kaikilla j. Lisäksi olkoon $c \in \mathbb{Q}_p$ mielivaltainen. Nyt $cx = \sum_{j=0}^{p-2} ca_j \zeta_p^j$. Täten on voimassa $|cx|_p = \sup_j |ca_j|_p$. Koska c on vakio indeksin j suhteen ja $|\cdot|_p$ normi avaruudessa $\mathbb{Q}_p$, niin $\sup_j |ca_j|_p = |c|_p \sup_j |a_j|_p$. Siis $|cx|_p = |c|_p |x|_p$ avaruudessa $\mathbb{Q}_p(\zeta_p)$. Koska $x + y = \sum_{j=0}^{p-2} (a_j + b_j)\zeta_p^j$, niin $|x+y|_p = \sup_j |a_j + b_j|_p$. Lauseen 2.37 mukaan $|a_j + b_j|_p \leq \max\{|a_j|_p, |b_j|_p\}$. Lisäksi

$$\sup_j \max\{|a_j|_p, |b_j|_p\} = \max\{\sup_j |a_j|_p, \sup_j |b_j|_p\},$$

joten $|x + y|_p \leq \max\{|x|_p, |y|_p\}$. Näin ollen $|\cdot|_p$ on avaruuden $\mathbb{Q}_p(\zeta_p)$ normi. □

Edellisessä lauseessa määritellyn normin $|\cdot|_p$ restriktio avaruuteen $\mathbb{Q}_p$ on määritelmässä 2.36 määritelty avaruuden $\mathbb{Q}_p$ normi. Näin ollen edellisessä lauseessa määritelty normi on määritelmän $\mathbb{Q}_p$ laajennus. Todistetaan vielä, että avaruus $\mathbb{Q}_p$ on täydellinen normin $|\cdot|_p$ indusoiman metriikan suhteen.

Lause 2.50. Avaruus $\mathbb{Q}_p(\zeta_p)$ on täydellinen normin $|\cdot|_p$ indusoiman metriikan suhteen.

Todistus. Olkoon (x_n) on Cauchy-jono avaruudessa $\mathbb{Q}_p(\zeta_p)$ ja $x_n = \sum_{j=0}^{p-2} a_j^{(n)} \zeta_p^j$. Voidaan tulkita x_n pistejonona (y_n), missä $y_n = (a_1^{(n)}, a_2^{(n)}, \cdots, a_{p-2}^{(n)})$. Tällöin (y_n) on Cauchyn-jono. Täten jokainen jokaisella j jono $(a_j^{(n)})$ on Cauchyn-jono. Lauseen 2.40 mukaan jokainen jono $(a_j^{(n)})$ suppenee. Oletetaan, että jono $(a_j^{(n)})$ suppenee kohti lukua a_j. Tällöin jono (y_n) suppenee kohti lukua $(a_1, a_2, \cdots, a_{p-2})$. Saadaan, että jono (x_n) suppenee kohti lukua $\sum_{j=0}^{p-2} a_j \zeta_p^j$. Siis avaruus $\mathbb{Q}_p(\zeta_p)$ on täydellinen normin $|\cdot|_p$ indusoiman metriikan suhteen □

3 Catalanin yhtälö, kun $\min\{p, q\} < 43$

Tässä luvussa tarkastellaan Catalanin yhtälöä, kun p ja q ovat parittomia alkulukuja. Luvun lopussa todistetaan, ettei tällöin Catalanin yhtälöllä ole nollasta eroavia ratkaisuja luvuilla x, y, kun vähintään toinen luvuista p, q on pienempi kuin 43. Tämän todistamiseksi osoitetaan ensin, että $q \equiv 1 \bmod p$. Käsittely perustuu Schoofin kirjassa [12] esitettyihin todistuksiin.

Symbolilla ζ_p tarkoitetaan edelleen p:nnettä primitiivistä ykkösenjuurta, missä p on pariton alkuluku. Merkitään $\pi = \zeta_p - 1$. Luvun kompleksikonjugoinnista käytetään merkintää ι. Lauseen 2.14 mukaan ι kuuluu ryhmään $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Otetaan myös tässä luvussa käyttöön merkinnät $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ ja $G_p = \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$. Renkaan R alkion α generoimasta ihanteessa käytetään edelleen merkintää $[\alpha]$. Jos $K/\mathbb{Q}$ on Galois'n laajennus, $\alpha \in K$ ja $a = \sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} a_\sigma \sigma \in \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$, niin merkinnällä α^a tarkoitetaan lukua $\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(\alpha)^{a_\sigma}$. Vastaavasti merkinnällä $a\alpha$ tarkoitetaan lukua $\sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} a_\sigma \sigma(\alpha)$.

Tutustutaan aluksi muutamaan Catalanin yhtälön toteuttavien kokonaislukujen ominaisuuteen. Todistetaan ensin, että jos Catalanin yhtälöllä on nollasta eroavia ratkaisuja ja $\min\{p, q\} \geq 2$, niin $p \neq q$. Tällöin riittää tarkastella seuraavan ehdon toteuttavia lukuja:

Olkoot $x, y, p, q \in \mathbb{Z}$, $xy \neq 0$, $p \neq q$, p ja q ovat parittomia alkulukuja sekä $x^p - y^q = 1$. $(*)$

Lemma 3.1. Olkoot x, y, p ja q kokonaislukuja, jotka toteuttavat Catalanin yhtälön $x^p - y^q = 1$. Oletetaan lisäksi, että $xy \neq 0$ ja $\min\{p, q\} \geq 2$. Tällöin $p \neq q$.

Todistus. Tehdään vastaoletus, että $p = q$. Tällöin Catalanin yhtälö saadaan muotoon $x^p - y^p = 1$. Voidaan olettaa, että $x \neq y$, sillä jos $x = y$, niin $x^p - y^p = 0$, mikä on vastoin oletusta $x^p - y^p = 1$.

Tutkitaan ensin tapausta $|x| > |y|$. Kolmioepäyhtälön nojalla

$$|x^p - y^p| \geq |x|^p - |y|^p.$$

Otetaan erotuksesta $|x|^p - |y|^p$ luku $|x|^{p-1}$ yhteiseksi tekijäksi, jolloin saadaan

$$|x|^p - |y|^p = |x|^{p-1}(|x| - \frac{|y|^p}{|x|^{p-1}}).$$

Koska $|x| > |y|$, niin

$$|x|^{p-1}(|x| - \frac{|y|^p}{|x|^{p-1}}) > |x|^{p-1}(|x| - \frac{|y|^p}{|y|^{p-1}}).$$

Sieventämällä ja käyttämällä tietoa $|x| > |y|$ saadaan, että

$$|x|^{p-1}(|x| - \frac{|y|^p}{|y|^{p-1}}) \geq |x|^{p-1}.$$

Siis $|x^p - y^p| > |x|^{p-1}$. Koska oletuksen mukaan $x \neq 0$, niin $|x| \geq 1$, joten $|x^p - y^p| > 1$. Siis ei voi päteä $x^p - y^p = 1$, kun $|x| > |y|$.

Koska $|x^p - y^p| = |y^p - x^p|$, niin edellisen kappaleen laskuissa voidaan vaihtaa luvut y ja x toisin päin, jolloin saadaan vastaava todistus tapaukselle $|y| > |x|$. Myöskään tapauksessa $|y| > |x|$ ei voi siis päteä, että $x^p - y^p = 1$. Näin ollen vastaoletus $p = q$ oli väärin ja on pädettävä $p \neq q$. □

Jo 1960-luvulla Cassels todisti, että Catalanin yhtälön toteuttaville kokonaisluvuille pätee tietynlaisia jaollisuusominaisuuksia. Yksi niistä esitetään seuraavaksi.

Lause 3.2. Olkoot p ja q parittomia alkulukuja sekä x ja y nollasta eroavia kokonaislukuja, joille $x^p - y^q = 1$. Tällöin on olemassa kokonaisluku a, jolle $x - 1 = p^{q-1}a^q$.

Todistus. Todistus on esitetty artikkelissa [2]. □

Erityisesti on huomioitava, että edellisen lauseen mukaan $x \equiv 1 \bmod p^{q-1}$. Tästä taas edelleen seuraa, että $x \equiv 1 \bmod p$.

3.1 $q \equiv 1 \bmod p$

Tässä luvussa todistetaan, että Catalanin yhtälössä on voimassa kongruenssi $q \equiv 1 \bmod p$. Tulosta käytetään myöhemmin hyödyksi luvussa 3.2 todistettaessa, ettei ehtoa $(*)$ toteuttavia lukuja ole, kun $\min\{p, q\} < 43$. Väitteen $q \equiv 1 \bmod p$ todistamiseksi tutustutaan sopiviin kunnan $\mathbb{Q}(\zeta_p)$ lukuihin ja niiden ominaisuuksiin.

Seuraavassa lauseessa tutustutaan myöhemmin useissa todistuksissa esiintyvien lukujen ω ja ω' määritelmiin. Muistettakoon, että merkintä ι tarkoittaa kompleksikonjugointia.

Lause 3.3. Olkoot x, y, p ja q ehdon $(*)$ toteuttavia lukuja. Oletetaan, että $(x - \zeta_p)^{1-\iota} = \alpha^q$ jollain $\alpha \in \mathbb{Q}(\zeta_p)^*$. Olkoon $\omega \in \overline{\mathbb{Q}}$, jolle $\omega^q = \frac{x-\zeta_p}{1-\zeta_p}$. Lisäksi olkoon $\omega' = \frac{\omega}{\alpha}$. Tällöin $(\omega')^q = \frac{x-\iota(\zeta_p)}{1-\zeta_p}$.

Todistus. Lasketaan luku $(\omega')^q$. Luvun ω' määritelmän mukaan $(\omega')^q = (\frac{\omega}{\alpha})^q$. Sijoitetaan tähän ω^q ja α^q. Saadaan

$$(\frac{\omega}{\alpha})^q = \frac{\frac{x-\zeta_p}{1-\zeta_p}}{(x-\zeta_p)^{1-\iota}}.$$

Sieventämällä saadaan

$$\frac{\frac{x-\zeta_p}{1-\zeta_p}}{(x-\zeta_p)^{1-\iota}} = \frac{(x-\zeta_p)(x-\zeta_p)^\iota}{(1-\zeta_p)(x-\zeta_p)}.$$

Supistamalla ja sieventämällä $(x-\zeta_p)^\iota = x - \iota(\zeta_p)$ saadaan

$$\frac{(x-\zeta_p)(x-\zeta_p)^\iota}{(1-\zeta_p)(x-\zeta_p)} = \frac{x-\iota(\zeta_p)}{1-\zeta_p}.$$

Siis $(\omega')^q = \frac{x-\iota(\zeta_p)}{1-\zeta_p}$. □

Tästä lähtien α, ω ja ω' on määritelty kuten lauseessa 3.3. Lisäksi merkitään $\mu = \frac{x-1}{1-\zeta_p}$ ja $\eta = (\omega-\omega')^q$. Luvun η määritelmän mukaan $\eta = (\omega-\omega')^q = \omega^q(1-\frac{1}{\alpha})^q$ ja edelleen $\omega^q(1-\frac{1}{\alpha})^q = \frac{x-\iota(\zeta_p)}{1-\zeta_p}(1-\frac{1}{\alpha})^q$ jokaisella mahdollisella luvun ω valinnalla. Siis luvun η arvo ei ole riippuvainen luvun ω valinnasta.

Tavoitteena on ilmaista ω ja ω' kunnassa $\mathbb{Q}_p(\zeta_p)$ sarjaesityksenä. Tätä varten todistetaan, että η on renkaan $\mathbb{Z}[\zeta_p]$ yksikkö.

Lause 3.4. Olkoot x, y, p ja q ehdon $(*)$ toteuttavia lukuja. Tällöin luku η on renkaan $\mathbb{Z}[\zeta_p]$ yksikkö.

Todistus. Todistetaan ensin, että $\eta \in \mathbb{Q}(\zeta_p)$. Aiempien laskujen mukaan $\eta = \omega^q(1-\frac{1}{\alpha})^q$. Luvun ω^q määritelmän mukaan $\omega^q \in \mathbb{Q}(\zeta_p)$. Lisäksi luvun α määritelmän mukaan $\alpha \in \mathbb{Q}(\zeta_p)$. Näin ollen $\eta \in \mathbb{Q}(\zeta_p)$.

On vielä todistettava, että $\eta \in \mathbb{Z}[\zeta_p]$ ja on todella renkaan $\mathbb{Z}[\zeta_p]$ yksikkö. Hyödynnetään tämän todistamisessa lausetta 2.15, jonka mukaan $\mathbb{Z}[\zeta_p]$ on kunnan $\mathbb{Q}(\zeta_p)$ kokonaislukujen rengas. Lisäksi käytetään todistuksessa apuna kuntaa $L = \mathbb{Q}(\zeta_p, \omega, \omega')$ jä tämän kunnan kokonaislukujen rengasta. On voimassa $[L : \mathbb{Q}(\zeta_p)] < \infty$, sillä $\omega^q, \omega'^q \in \mathbb{Q}(\zeta_p)$. Merkitään $n = [L : \mathbb{Q}(\zeta_p)]$.

Väitteen todistamiseksi tutkitaan lukua $\omega^q - \omega'^q$. Sievennetään tätä ensin. Sijoittamalla saadaan $\omega^q - \omega'^q = \frac{x-\zeta_p}{1-\zeta_p} - \frac{x-\iota(\zeta_p)}{1-\zeta_p}$. Sievennetään tätä ja otetaan ζ_p^{-1} yhteiseksi tekijäksi. Tällöin

$$\frac{x-\zeta_p}{1-\zeta_p} - \frac{x-\iota(\zeta_p)}{1-\zeta_p} = \frac{\zeta_p^{-1}(1-\zeta_p^2)}{1-\zeta_p}.$$

Koska $\frac{\zeta_p^{-1}(1-\zeta_p^2)}{1-\zeta_p} = \zeta_p^{-1} + 1$, niin $\omega^q - \omega'^q = \zeta_p^{-1} + 1$. Selvästi $\omega^q - \omega'^q \in \mathbb{Q}(\zeta_p)$. Lauseen 2.14 mukaan $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1 + \zeta_p^{-1}) = \prod_{k=1}^{p-1}(1 + \zeta_p^{-k})$. Koska on voimassa $\prod_{k=1}^{p-1}(1 + \zeta_p^{-k}) = \prod_{k=1}^{p-1}(1 + \zeta_p^{k})$, niin esimerkin 2.16 nojalla $1 + \zeta_p^{-1}$ on renkaan $\mathbb{Z}[\zeta_p]$ yksikkö ja sen normi on $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1+\zeta_p^{-1}) = 1$. Käytetään näitä tietoja apuna todistuksessa.

Tarkastellaan nyt laajennusta $L/\mathbb{Q}$ ja erityisesti luvun $\omega^q - \omega'^q$ ominaisuuksia tässä laajennuksessa. Lasketaan ensin $N_{L/\mathbb{Q}}(\omega^q - \omega'^q)$. Koska on voimassa $\mathbb{Q}(\zeta_p) \subseteq L$, niin lauseen 2.8 nojalla

$$N_{L/\mathbb{Q}}(\omega^q - \omega'^q) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(N_{L/\mathbb{Q}(\zeta_p)}(\omega^q - \omega'^q)).$$

Koska $\omega^q, \omega'^q \in \mathbb{Q}(\zeta_p)$, niin $N_{L/\mathbb{Q}(\zeta_p)}(\omega^q - \omega'^q) = (\omega^q - \omega'^q)^n$. Saadaan

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(N_{L/\mathbb{Q}(\zeta_p)}(\omega^q - \omega'^q)) = (N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\omega^q - \omega'^q))^n.$$

Edellisen kappaleen nojalla $(N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\omega^q - \omega'^q))^n = 1$. Siis $N_{L/\mathbb{Q}}(\omega^q - \omega'^q) = 1$.

Edellistä normia hyödynnetään, kun todistetaan, että η on renkaan $\mathbb{Z}[\zeta_p]$ yksikkö. Todistetaan seuraavaksi, että $\omega, \omega' \in \mathcal{O}_L$. Tehdään tämä todistamalla, että $\omega^q, \omega'^q \in \mathcal{O}_L$. Kirjoitetaan ω^q muodossa $\frac{x-1}{1-\zeta_p} + \frac{1-\zeta_p}{1-\zeta_p} \in \mathbb{Q}(\zeta_p)$. Esimerkin 2.21 ja lauseen 2.20 nojalla $p \in [1 - \zeta_p]$ renkaassa $\mathbb{Z}[\zeta_p]$. Lisäksi lauseen 3.2 mukaan $x - 1 \equiv 0 \bmod p^{q-1}$, joten $x - 1 = \beta(1 - \zeta_p)^{a(q-1)}$ jollain kokonaisluvulla a ja alkiolla $\beta \in \mathbb{Z}[\zeta_p]$. Saadaan

$$\frac{x-1}{1-\zeta_p} + \frac{1-\zeta_p}{1-\zeta_p} = \beta(1-\zeta_p)^{a(q-1)} + 1.$$

Tästä esitysmuodosta nähdään, että lauseen 2.4 mukaan $\frac{x-\iota(\zeta_p)}{1-\zeta_p}$ on kunnan $\mathbb{Q}(\zeta_p)$ kokonaisluku. Siis ω^q on kunnan $\mathbb{Q}(\zeta_p)$ kokonaisluku. Näin olen ω^q on myös kunnan L kokonaisluku. Vastaavasti voidaan tarkastella lukua ω'^q muodossa $\frac{x-1}{1-\zeta_p} + \frac{1-\iota(\zeta_p)}{1-\zeta_p}$. Koska on voimassa $\frac{1-\iota(\zeta_p)}{1-\zeta_p} = \sum_{k=0}^{p-2} \zeta_p^k$, niin

$$\frac{x-1}{1-\zeta_p} + \frac{1-\iota(\zeta_p)}{1-\zeta_p} = \beta(1-\zeta_p)^{a(q-1)} + \sum_{k=0}^{p-2} \zeta_p^k.$$

Siis lauseen 2.4 mukaan myös ω'^q on kunnan $\mathbb{Q}(\zeta_p)$ kokonaisluku. Täten ω'^q on myös kunnan L kokonaisluku. Lauseen 2.6 mukaan $\omega, \omega' \in \mathcal{O}_L$.

Yhdistetään saadut tiedot luvuista $\omega^q - \omega'^q$, ω ja ω'. Suoraan laskemalla nähdään, että

$$\frac{\omega^q - \omega'^q}{\omega - \omega'} = \omega^{q-1} + \omega^{q-2}\omega' + \ldots + \omega'^{q-1}.$$

Koska edellisen kappaleen mukaan $\omega, \omega' \in \mathcal{O}_L$, niin lauseen 2.4 nojalla

$$\omega^{q-1} + \omega^{q-2}\omega' + \ldots + \omega'^{q-1} \in \mathcal{O}_L \text{ ja } \omega - \omega' \in \mathcal{O}_L.$$

Lauseen 2.11 mukaan $N_{L/\mathbb{Q}}(\omega - \omega') \in \mathbb{Z}$. Koska $N_{L/\mathbb{Q}}(\omega - \omega')$ jakaa normin $N_{L/\mathbb{Q}}(\omega^q - \omega'^q) = 1$, niin on oltava $|N_{L/\mathbb{Q}}(\omega - \omega')| = 1$. Näin ollen lauseen 2.12 mukaan $\omega - \omega'$ on renkaan $\mathcal{O}_L$ yksikkö.

Koska $\eta = (\omega - \omega')^q$ ja $\omega - \omega'$ on renkaan $\mathcal{O}_L$ yksikkö, niin myös η on renkaan $\mathcal{O}_L$ yksikkö. Toisaalta ensimmäisessä kappaleessa todettiin, että $\eta \in \mathbb{Q}(\zeta_p)$. Täten myös $\eta^{-1} \in \mathbb{Q}(\zeta_p)$ ja lukujen η, η^{-1} on oltava kunnan $\mathbb{Q}(\zeta_p)$ kokonaislukuja. Siis η on renkaan $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ yksikkö.

□

Edellisessä todistuksessa on huomattava, että luvun η normi on yksi jokaisella mahdollisella luvun ω valinnalla. Nimittäin jo aiemmin todettiin, ettei luku η ole riippuvainen luvun ω valinnasta.

Edeltävien lauseiden tiedot voidaan nyt kerätä yhteen ja saada luvulle ω sarjaesitys kunnassa $\mathbb{Q}_p(\zeta_p)$. Myöhemmin sarjaesitystä tullaan hyödyntämään laskettaessa tietyn luvun u normia $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(u) \bmod \mu^2$ renkaassa $\mathbb{Z}_p[\zeta_p]$. Tätä lukua käytetään väitteen $q \equiv 1 \bmod p$ todistuksessa. Kuten tavallisesti, merkinnällä $\binom{\frac{1}{q}}{j}$ tarkoitetaan lukua $\frac{\frac{1}{q}(\frac{1}{q}-1)\ldots(\frac{1}{q}-(j-1))}{j!}$.

Lause 3.5. Olkoot x, y, p ja q ehdon $(*)$ toteuttavia lukuja. Tällöin kunnassa $\mathbb{Q}_p(\zeta_p)$

$$\omega = \sqrt[q]{1+\mu} = \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \mu^j.$$

Todistus. Todistetaan ensin, että sarja $\sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \mu^j$ suppenee kunnassa $\mathbb{Q}_p(\zeta_p)$ ja $1+\mu = (\sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \mu^j)^q$. Lauseen 2.49 mukaan $\mathbb{Q}_p(\zeta_p)$ on normiavaruus normin $|\cdot|_p$ suhteen. Edelleen lauseen 2.50 mukaan avaruus $\mathbb{Q}_p(\zeta_p)$ on täydellinen normin $|\cdot|_p$ indusoiman metriikan suhteen. Lisäksi lauseen 3.2 nojalla $\mu \equiv 0 \bmod p$, joten $|\mu|_p \leq p^{-1} < 1$. Näin ollen

$$\lim_{j\to\infty} \left| \frac{\binom{\frac{1}{q}}{j+1} \mu^{j+1}}{\binom{\frac{1}{q}}{j} \mu^j} \right|_p = |\mu|_p < 1.$$

Siis edellisen kaavan ja avaruuden $\mathbb{Q}_p(\zeta_p)$ täydellisyyden nojalla $\sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \mu^j$ suppenee normiavaruudessa $\mathbb{Q}_p(\zeta_p)$.

Formaalisten potenssisarjojen renkaassa $(\sum_{j=0}^{\infty}\binom{\frac{1}{q}}{j}\mu^j)^q = 1+\mu$. Koska $(\sum_{j=0}^{\infty}\binom{\frac{1}{q}}{j}\mu^j)^q$ suppenee avaruudessa $\mathbb{Q}_p(\zeta_p)$, niin $(\sum_{j=0}^{\infty}\binom{\frac{1}{q}}{j}\mu^j)^q = 1+\mu$ avaruudessa $\mathbb{Q}_p(\zeta_p)$. Koska aiemmin luvun η määrittelyn yhteydessä todettiin, ettei sen arvo riipu luvun ω valinnasta, niin voidaan valita

$$\omega = \sqrt[q]{1+\mu} = \sum_{j=0}^{\infty}\binom{\frac{1}{q}}{j}\mu^j \in \mathbb{Q}_p(\zeta_p).$$

□

Luvulle ω' saadaan samantapainen sarjaesitys kuin luvulle ω. Samoin kuin luvun ω sarjaesitystä, myös luvun ω' sarjaesitystä käytetään luvun tietyn luvun u normin $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(u)$ mod μ^2 laskemiseksi renkaassa $\mathbb{Z}_p[\zeta_p]$. Ennen kuin kuitenkaan voidaan laskea luvulle ω' sarjaesitystä, tarkastellaan sen todistuksessa käytettäviin kolmeen lemmaan.

Lemma 3.6. Olkoon p pariton alkuluku. Tällöin kaikki kunnan $\mathbb{Q}(\zeta_p)$ ykkösenjuuret ovat muotoa $\pm\zeta_p^j$, missä ζ_p on p:nnes primitiivinen ykkösenjuuri ja j kokonaisluku väliltä $[1,p]$.

Todistus. Todistetaan ensin, että kunnassa $\mathbb{Q}(\zeta_p)$ on vain äärellinen määrä ykkösenjuuria. Jos ζ_k on ykkösenjuuri ja on voimassa $\zeta_k \in \mathbb{Q}(\zeta_p)$, niin saadaan $\varphi(k) = [\mathbb{Q}(\zeta_k) : \mathbb{Q}] \leq p-1$. Tällaisia lukuja ζ_k on vain äärellisen monta kappaletta, joten kunnassa $\mathbb{Q}(\zeta_p)$ on vain äärellinen määrä ykkösenjuuria. Näiden generoima multiplikatiivinen ryhmä on siis syklinen.

Merkitään kunnan $\mathbb{Q}(\zeta_p)$ ykkösenjuurten ryhmän generaattoria symbolilla ζ_k. Tällöin $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_k)$. Siis $\varphi(k) = p-1$. Näin ollen $k = p$ tai $k = 2p$. Koska kaikki luvut $\pm\zeta_p^j$ kuuluvat kuntaan $\mathbb{Q}(\zeta_p)$ ja ovat ykkösenjuuria, niin $k = 2p$, eikä edellä mainittujen ykkösenjuurten lisäksi kunnassa $\mathbb{Q}(\zeta_p)$. Näin on saatu väite todistettua. □

Lemma 3.7. Renkaassa $\mathbb{Z}[\zeta_p]$ on voimassa $\alpha \equiv -1 \bmod \pi$.

Todistus. Lasketaan ensiksi, mitä on α^q modulo π ja sen avulla lasketaan α modulo π. Merkitään $t = \frac{x-\zeta_p}{\pi}$. Tällöin $\alpha^q = (\frac{x-\zeta_p}{\pi})^{1-\iota}\pi^{1-\iota}$. Sievennetään $\iota(\pi)$ muotoon $-\zeta_p^{-1}\pi$ ja sijoitetaan $t = \frac{x-\zeta_p}{\pi}$, jolloin saadaan

$$(\frac{x-\zeta_p}{\pi})^{1-\iota}\pi^{1-\iota} = -t^{1-\iota}\zeta_p.$$

Koska $\zeta_p \equiv 1 \bmod \pi$, niin $\alpha^q \equiv -t^{1-\iota} \bmod \pi$. Tarkastellaan lukua $t = \frac{x-\zeta_p}{\pi}$. Luku $\frac{x-\zeta_p}{\pi}$ voidaan kirjoittaa muodossa $\frac{x-1}{\pi} - 1$. Koska lauseen 3.2 mukaan

$x-1 \equiv 0 \bmod p$, niin $\frac{x-1}{\pi} - 1 \equiv -1 \bmod \pi$. Siis $t \equiv -1 \bmod \pi$. Tarkastellaan nyt lukua $\iota(t)$. Kuten aiemmin on jo todettu $\iota(\pi) = -\zeta_p^{-1}\pi$, joten saadaan $\iota(t) = -\zeta_p \frac{x-1}{\pi} - 1$. Siis myös $\iota(t) \equiv -1 \bmod \pi$. Näin ollen

$$t^{1-\iota} \equiv 1 \bmod \pi,$$

joten $\alpha^q \equiv -1 \bmod \pi$. Väitteen todistamiseksi verrataan lukuja α^2 modulo π ja α^q modulo π. Lasketaan tätä varten α^2 modulo π.

Määritelmän mukaan $\alpha^q = (x-\zeta_p)^{1-\iota}$. Kerrotaan se kompleksikonjugaatillaan, jolloin saadaan, että $(\alpha\iota(\alpha))^q = 1$. Koska q on pariton alkuluku, joka on erisuuri kuin p, niin lemman 3.6 nojalla kunnassa $\mathbb{Q}(\zeta_p)$ ei ole luvun yksi lisäksi mitään muita q:nnensia ykkösenjuuria. Täten saadaan $\alpha\iota(\alpha) = 1$. Todetaan seuraavaksi, että $\alpha\iota(\alpha) \equiv \alpha^2 \bmod \pi$. Koska $\alpha \in \mathbb{Q}(\zeta_p)$, niin α on muotoa $\sum_{k=1}^{p-1} a_k \zeta_p^k$, missä luvut a_k ovat rationaalilukuja. Lisäksi $\zeta_p^k \equiv 1 \bmod \pi$ kaikilla kokonaisluvuilla k. Siis $\alpha \equiv \sum_{k=1}^{p-1} a_k \bmod \pi$, joten $\alpha \equiv \iota(\alpha) \bmod \pi$. Näin ollen $1 = \alpha\iota(\alpha) \equiv \alpha^2 \bmod \pi$.

Nyt on saatu, että $\alpha^q \equiv -1 \bmod \pi$ ja $\alpha^2 \equiv 1 \bmod \pi$. Koska q on pariton luku, on voimassa $\alpha \equiv -1 \bmod \pi$. □

Lemma 3.8. Olkoot p ja q parittomia alkulukuja sekä $p \neq q$. Jos $\zeta \neq 1$ on q:nnes ykkösenjuuri kunnassa $\mathbb{Q}_p(\zeta_p)$, niin $\zeta \in \mathbb{Z}_p[\zeta_p]$ ja $\zeta \not\equiv 1 \bmod \pi$.

Todistus. Oletetaan, että $\zeta \neq 1$ on q:nnes ykkösenjuuri kunnassa $\mathbb{Q}_p(\zeta_p)$. Todistetaan ensin, että $\zeta \in \mathbb{Z}_p[\zeta_p]$. Merkitään $f(x) = \sum_{k=0}^{q-1} x^k$. Tällöin $f(\zeta) = 0$, $f(x)$ on pääpolynomi ja $f(x) \in \mathbb{Z}_p[x]$. Lauseen 2.48 mukaan $\zeta \in \mathbb{Z}_p[\zeta_p]$. Todistetaan vielä, että $\zeta \not\equiv 1 \bmod \pi$.

Tehdään vastaoletus, että $\zeta \equiv 1 \bmod \pi$. Tällöin voidaan kirjoittaa luku ζ muodossa $\zeta = \beta\pi + 1$, missä $\beta \in \mathbb{Z}_p[\zeta_p]$. Korotetaan tämä lauseke potenssiin q, jolloin saadaan $1 = 1 + \sum_{j=1}^{q} \binom{q}{j} (\beta\pi)^j$. Siis $\sum_{j=1}^{q} \binom{q}{j} (\beta\pi)^j = 0$. Koska $\zeta \neq 1$, niin $\beta\pi \neq 0$ ja $\sum_{j=1}^{q} \binom{q}{j} (\beta\pi)^{j-1} = 0$. Tämä voidaan kirjoittaa muodossa

$$\sum_{j=1}^{q} \binom{q-1}{j-1} (\beta\pi)^{j-1} + \sum_{j=1}^{q} \binom{q-1}{j} (\beta\pi)^{j-1} = 0. \tag{12}$$

Koska $\binom{q-1}{j} = \frac{1}{q}\binom{q}{j}$, kun $0 \leq j \leq q-1$, niin

$$\sum_{j=1}^{q} \binom{q-1}{j} (\beta\pi)^{j-1} = \frac{1}{q} \sum_{j=1}^{q} \binom{q}{j} (\beta\pi)^{j-1} - \frac{1}{q} (\beta\pi)^{q-1}. \tag{13}$$

Koska $\sum_{j=1}^{q} \binom{q}{j} (\beta\pi)^{j-1} = 0$, niin lausekkeet (12) ja (13) yhdistämällä saadaan $\sum_{j=1}^{q} \binom{q-1}{j-1} (\beta\pi)^{j-1} - \frac{1}{q}(\beta\pi)^{q-1} = 0$. Kun tämä kirjoitetaan luvun ζ avulla, saadaan

$$q\zeta^{q-1} = (\beta\pi)^{q-1}. \tag{14}$$

Todistetaan laajennuksen $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ normeja laskemalla, että tämä on mahdotonta.

Tarkastellaan ensin normia

$$N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(q\zeta^{q-1}) = N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(q)N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(\zeta)^{q-1}.$$

Olkoon $f(x)$ sama polynomi kuin tämän todistuksen ensimmäisessä kappaleessa. Luvun ζ minimaalipolynomi $g(x)$ yli kunnan $\mathbb{Q}_p$ jakaa polynomin $f(x)$. Koska $f(x) = \prod_{k=1}^{q-1}(x-\zeta^k)$, niin $g(x) = \prod_{j=1}^{m}(x-\zeta^{k_j})$, missä luvut k_j ovat erisuuria ja $k_j \in \{1,2,\ldots,q-1\}$ kaikilla j. Siis lauseen 2.10 mukaan on voimassa $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(\zeta) = \pm\zeta^k$ jollain kokonaisluvulla k. Laskemalla saadaan, että $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(\zeta)^{q-1} = \pm\zeta^{-k}$. Lauseiden 2.46, 2.34 ja 2.45 nojalla $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(q) = q^{p-1}$. Siis

$$N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(q\zeta^{q-1}) = \pm q^{p-1}\zeta^{-k}. \tag{15}$$

Tarkastellaan seuraavaksi normia

$$N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}\left((\beta\pi)^{q-1}\right) = \left(N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(\beta)N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(\pi)\right)^{q-1}.$$

Lauseen 2.46 ja lauseen 2.15 toiseksi viimeisen kappaleen mukaan

$$N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(\pi)^{q-1} = p^{q-1}. \tag{16}$$

Lauseiden 2.47 ja 2.48 nojalla $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(\beta)^{q-1} \in \mathbb{Z}_p$. Näin ollen kaavojen (14), (15) ja (16) nojalla $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(\beta)^{q-1} = \frac{\pm q^{p-1}\zeta^{-k}}{p^{q-1}} \in \mathbb{Z}_p$. Kuitenkin $|\frac{\pm q^{p-1}\zeta^{-k}}{p^{q-1}}|_p = p^{q-1} > 1$, joten $\frac{\pm q^{p-1}\zeta^{-k}}{p^{q-1}} \notin \mathbb{Z}_p$. Siis vastaoletuksen $\zeta \equiv 1 \bmod \pi$ on oltava väärin.

□

Edellisiä lemmoja käyttäen saadaan muodostettua luvulle ω' samantapainen sarjaesitys kuin luvulle ω lauseessa 3.5. Tarkastellaan tätä seuraavaksi.

Lause 3.9. Olkoot x, y, p ja q ehdon $(*)$ toteuttavia lukuja. Tällöin kunnassa $\mathbb{Q}_p(\zeta_p)$

$$\omega' = -\zeta_p^r\sqrt[q]{1+\iota(\mu)} = -\zeta_p^r\sum_{j=0}^{\infty}\binom{\frac{1}{q}}{j}\iota(\mu)^j,$$

missä r on kokonaisluku, jolle on voimassa $qr \equiv -1 \bmod p$.

Todistus. Todistetaan väite kahdessa erässä sen mukaan, sisältääkö kunta $\mathbb{Q}_p(\zeta_p)$ jonkin muun kuin triviaalin q:nnen ykkösenjuuren vai ei. Tarkastellaan ensin tapausta, ettei kunta $\mathbb{Q}_p(\zeta_p)$ sisällä muita q:nnensia ykkösenjuuria kuin luvun 1. Näin ollen kunnassa $\mathbb{Q}_p(\zeta_p)$ on olemassa yksikäsitteinen alkio ω', jolle $\omega'^q = -\iota(\zeta_p)(1+\iota(\mu))$. Tällöin $\omega' = -\zeta_p^r \sqrt[q]{1+\iota(\mu)}$ ja $qr \equiv -1 \bmod p$. Siis ensimmäinen yhtäsuuruus on todistettu. Samalla tavoin kuin lauseessa 3.5 voidaan todistaa, että $\sqrt[q]{1+\iota(\mu)} = -\zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j$ kunnassa $\mathbb{Q}_p(\zeta_p)$. Lause 3.9 pitää täten paikkansa, kun kunta $\mathbb{Q}_p(\zeta_p)$ ei sisällä muita q:nnensia ykkösenjuuria kuin luvun 1.

Tarkastellaan nyt tapausta, että $\mathbb{Q}_p(\zeta_p)$ sisältää vähintään yhden epätriviaalin q:nnen ykkösenjuuren. Samoin kuin edellisessä tapauksessa, voidaan todeta, että $-\zeta_p^r \sqrt[q]{1+\iota(\mu)} = -\zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j$, missä $qr \equiv -1 \bmod p$. Näin ollen jälkimmäinen yhtäsuuruus on todistettu. Ensimmäisen yhtäsuuruuden todistamiseksi tutkitaan kunnan $\mathbb{Q}_p(\zeta_p)$ q:nnensia ykkösenjuuria.

Tarkastellaan sarjaa $-\zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j$. Korottamalla se potenssiin q voidaan todeta, että ω' on luku $-\zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j$ kerrottuna jollain q:nnellä ykkösenjuurella ζ. Tavoitteena on todistaa, että

$$\omega' \equiv -\zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j \bmod \pi.$$

Lemman 3.8 nojalla tästä nimittäin seuraisi, että $\omega' = -\zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j$ ja väite olisi todistettu. Lasketaan ensin, mitä on $-\zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j \bmod \pi$. Lauseen 3.2 nojalla $\mu \equiv 0 \bmod \pi$, joten $\iota(\mu) = -\zeta_p \mu \equiv 0 \bmod \pi$. Näin saadaan, että $-\zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j \equiv -\zeta_p^r \bmod \pi$. Lisäksi $\pi | (\zeta_p^r - 1)$, joten $-\zeta_p^r \equiv -1 \bmod \pi$. Täten $-\zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j \equiv -1 \bmod \pi$.

Lasketaan vielä ω' modulo π. Käytetään sen laskemiseksi esitystä $\omega' = \frac{\omega}{\alpha}$. Lauseen 3.5 mukaan $\omega = \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \mu^j$, joten $\omega \equiv 1 \bmod \pi$. Lemman 3.7 mukaan $\alpha \equiv -1 \bmod \pi$, joten $\omega' \equiv -1 \bmod \pi$. Siis $\omega' = -\zeta_p^r \sqrt[q]{1+\iota(\mu)}$ kunnassa $\mathbb{Q}_p(\zeta_p)$. □

Lauseissa 3.5 ja 3.9 on saatu luvuille ω ja ω' sarjaesitykset kunnassa $\mathbb{Q}_p(\zeta_p)$. Olkoon $u = \omega - \omega'$, missä ω ja ω' ovat lauseissa 3.5 sekä 3.9 määritellyt luvut. Tämän esityksen avulla saadaan luvulle u sarjaesitys kunnassa $\mathbb{Q}_p(\zeta_p)$. Saadun sarjaesityksen avulla voidaan laskea $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(u) \bmod \mu^2$ renkaassa $\mathbb{Z}_p[\zeta_p]$ kahdella eri tavalla. Tämä tehdään seuraavissa lauseissa.

Lause 3.10. Normit $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\eta)$ ja $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(u)$ ovat yhtäsuuria kuin 1.

Todistus. Lasketaan ensin luvun η normi ja tämän avulla saadaan luvun u normi. Lauseen 3.4 mukaan η on renkaan $\mathbb{Z}[\zeta_p]$ yksikkö. Näin ollen lauseista 2.4 ja 2.12 seuraa, että $\mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}$ sekä $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\eta) = \pm 1$. Todistetaan, ettei -1 ole normin $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\eta)$ arvo.

Koska η on renkaan $\mathbb{Z}[\zeta_p]$ alkio, niin voidaan kirjoittaa $\eta = \sum_{k=1}^{p-1} a_k \zeta_p^k$, missä luvut a_k ovat kokonaislukuja. Lauseen 2.14 mukaan

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\eta) = \prod_{j=1}^{p-1}(\sum_{k=1}^{p-1} a_k \zeta_p^{kj}).$$

Ryhmitellään tulo yhdistämällä termit, joiden potensseissa on luvut j ja $p-j$. Saadaan

$$\prod_{j=1}^{p-1}(\sum_{k=1}^{p-1} a_k \zeta_p^{kj}) = \prod_{j=1}^{\frac{p-1}{2}}((\sum_{k=1}^{p-1} a_k \zeta_p^{kj})(\sum_{k=1}^{p-1} a_k \zeta_p^{-kj})).$$

Nyt kerrottavana on luku ja sen kompleksikonjugaatti. Kirjoitetaan

$$\sum_{k=1}^{p-1} a_k \zeta_p^{kj} = x_j + iy_j, \text{ missä } x_j, y_j \in \mathbb{R}.$$

Näin saadaan tuloksi

$$\prod_{j=1}^{\frac{p-1}{2}}((\sum_{k=1}^{p-1} a_k \zeta_p^{kj})(\sum_{k=1}^{p-1} a_k \zeta_p^{-kj})) = \prod_{j=1}^{\frac{p-1}{2}}(x_j^2 + y_j^2).$$

Tämä on selvästi vähintään nolla. Siis $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\eta) \geq 0$ eli se ei voi olla -1.

On vielä todistettava, että $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(u) = 1$. Lukujen ω ja ω' valintojen takia $u = \omega - \omega' \in \mathbb{Q}(\zeta_p)$, joten lauseen 2.10 mukaan $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(u) \in \mathbb{Q}$. Toisaalta tämän todistuksen alun mukaan $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(u)^q = 1$. Koska q on pariton alkuluku, niin $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(u) = 1$. □

Lause 3.11. Olkoot x, y, p ja q ehdon $(*)$ toteuttavia lukuja. Tällöin renkaassa $\mathbb{Z}_p[\zeta_p]$ on voimassa

$$N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(u) \equiv 1 + \frac{x-1}{q} \sum_{k=1}^{p-1} \frac{1 - \zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)} \bmod \mu^2.$$

Todistus. Käytetään normista $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}$ lyhennysmerkintää N. Lauseiden 2.14, 2.46 ja 2.34 mukaan $N(z) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(z)$ kaikilla luvuilla $z \in \mathbb{Q}(\zeta_p)$. Tarkastellaan ensin lukua u ja käytetään sen sopivaa esitysmuotoa luvun $N(u)$ laskemiseksi.

Lauseiden 3.5 ja 3.9 mukaan $u = \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \mu^j + \zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j$. Koska $\iota(\mu) = -\zeta_p \mu$, niin

$$\sum_{j=2}^{\infty} \binom{\frac{1}{q}}{j} \mu^j + \zeta_p^r \sum_{j=2}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j = \mu^2 (\sum_{j=2}^{\infty} \binom{\frac{1}{q}}{j} \mu^{j-2} + \zeta_p^r \sum_{j=2}^{\infty} \binom{\frac{1}{q}}{j} (-\zeta_p)^j \mu^{j-2}).$$

Näin ollen renkaassa $\mathbb{Z}_p[\zeta_p]$ on voimassa

$$\sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \mu^j + \zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j \equiv 1 + \frac{\mu}{q} + \zeta_p^r (1 + \frac{\iota(\mu)}{q}) \bmod \mu^2.$$

Otetaan luku $1 + \zeta_p^r$ yhteiseksi tekijäksi, jolloin saadaan

$$1 + \frac{\mu}{q} + \zeta_p^r (1 + \frac{\iota(\mu)}{q}) = (1 + \zeta_p^r)(1 + \frac{\mu + \zeta_p^r \iota(\mu)}{(1 + \zeta_p^r) q}). \tag{17}$$

Koska $\mu = \frac{x-1}{1-\zeta_p}$ ja $\iota(\mu) = \frac{x-1}{1-\zeta_p^{-1}}$, niin

$$\frac{\mu + \zeta_p^r \iota(\mu)}{(1 + \zeta_p^r) q} = \frac{x-1}{(1 + \zeta_p^r) q} \frac{1 - \zeta_p^{r+1}}{1 - \zeta_p}.$$

Täten saadaan lauseke (17) sievennettyä muotoon

$$(1 + \zeta_p^r)(1 + \frac{\mu + \zeta_p^r \iota(\mu)}{(1 + \zeta_p^r) q}) = (1 + \zeta_p^r)(1 + \frac{(x-1)(1 - \zeta_p^{r+1})}{(1 + \zeta_p^r) q (1 - \zeta_p)}).$$

Näin ollen $u \equiv (1 + \zeta_p^r)(1 + \frac{(x-1)(1-\zeta_p^{r+1})}{(1+\zeta_p^r) q (1-\zeta_p)}) \bmod \mu^2$ renkaassa $\mathbb{Z}_p[\zeta_p]$.

Tutkitaan nyt luvun u normia käyttäen apuna edellisessä kappaleessa löydettyä esitysmuotoa modulo μ^2. Lauseen 2.46 mukaan

$$N(u) = \prod_{k=1}^{p-1} \left(\sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \mu_k^j + \zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu_k)^j \right),$$

missä $\mu_k = \frac{x-1}{1-\zeta_p^k}$. Luku μ_k voidaan myös ilmaista luvun μ avulla. Laskemalla nimittäin nähdään, että $\mu_k = \mu \sum_{t=0}^{s-1} \zeta_p^{kt}$, missä s on kokonaisluku, jolle $ks \equiv 1 \bmod p$. Näin ollen edellisessä kappaleessa laskettujen kongruenssien nojalla renkaassa $\mathbb{Z}_p[\zeta_p]$ on voimassa kongruenssi

$$\begin{aligned} &\prod_{k=1}^{p-1} \left(\sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \mu_k^j + \zeta_p^r \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu_k)^j \right) \\ &\equiv N(1 + \zeta_p^r) N(1 + \frac{(x-1)(1 - \zeta_p^{r+1})}{(1 + \zeta_p^r) q (1 - \zeta_p)}) \bmod \mu^2. \end{aligned}$$

Esimerkin 2.16 mukaan $N(1+\zeta_p^r)=1$, joten ryhmän G_p automorfismeja käyttäen

$$N(1+\zeta_p^r)N(1+\frac{(x-1)(1-\zeta_p^{r+1})}{(1+\zeta_p^r)q(1-\zeta_p)})=\prod_{k=1}^{p-1}\left(1+\frac{x-1}{q}\frac{1-\zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)}\right).$$

Tarkastellaan lukujen $\frac{x-1}{q}\frac{1-\zeta_p^{k_1(r+1)}}{(1+\zeta_p^{rk_1})(1-\zeta_p^{k_1})}$ ja $\frac{x-1}{q}\frac{1-\zeta_p^{k_2(r+1)}}{(1+\zeta_p^{rk_2})(1-\zeta_p^{k_2})}$ tuloa. Lukujen tulo on $\mu^2\frac{(1-\zeta_p^{k_1(r+1)})(1-\zeta_p^{k_2(r+1)})(1-\zeta_p)^2}{(1+\zeta_p^{rk_1})(1-\zeta_p^{k_1})(1+\zeta_p^{rk_2})(1-\zeta_p^{k_2})q^2}$. Näin ollen renkaassa $\mathbb{Z}_p[\zeta_p]$ on voimassa kongruenssi

$$\prod_{k=1}^{p-1}\left(1+\frac{x-1}{q}\frac{1-\zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)}\right)\equiv 1+\frac{x-1}{q}\sum_{k=1}^{p-1}\frac{1-\zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)} \bmod \mu^2.$$

Siis $N(u)\equiv 1+\frac{x-1}{q}\sum_{k=1}^{p-1}\frac{1-\zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)} \bmod \mu^2$. □

Edellisessä lauseessa esiintyy vielä melko hankala summa $\sum_{k=1}^{p-1}\frac{1-\zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)}$. Seuraavan lauseen tarkoituksena on yksinkertaistaa sitä. Huomionarvoista tässä on, että lukua $\frac{1-\zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)}$ tarkastellaan modulo π, eikä modulo μ^2. Ajatuksena nimittäin on, että myöhemmin, kun todistetaan $q\equiv 1 \bmod p$ käytetään lukua $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(u) \bmod (x-1)\pi$ apuna. Koska $(x-1)\pi$ jakaa luvun μ^2 renkaassa $\mathbb{Z}_p[\zeta_p]$, niin edellisen lauseen laskuja voidaan käyttää apuna.

Lemma 3.12. Olkoon r lauseessa 3.9 määritelty luku. Tällöin renkaassa $\mathbb{Z}_p[\zeta_p]$ on voimassa

$$\frac{1-\zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)}\equiv\frac{r+1}{2} \bmod \pi$$

kaikilla kokonaisluvuilla $k\in[1,p-1]$.

Todistus. Tarkastellaan lukua $\frac{1-\zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)}$ modulo π. Luvun ζ_p tilalle voidaan kirjoittaa luku $1+\pi$, joten

$$\frac{1-\zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)}=\frac{1-(1+\pi)^{k(r+1)}}{(1+(1+\pi)^{rk})(1-(1+\pi)^k)}.$$

Otetaan käyttöön merkintä $O(\pi^j)$. Merkinnällä tarkoitetaan summaa, joka on jaollinen luvulla π^j. Näin ollen siis symbolit $O(\pi^3)$ ja $O(\pi^2)$ tarkoittavat summia, jotka ovat jaollisia luvuilla π^3 ja π^2. Tällöin

$$\frac{1-(1+\pi)^{k(r+1)}}{(1+(1+\pi)^{rk})(1-(1+\pi)^k)}=\frac{-k(r+1)\pi+O(\pi^2)}{1-(1+\pi)^k+(1+\pi)^{rk}-(1+\pi)^{k(r+1)}}.$$

Sieventämällä nimittäjän potensseja käyttämällä potenssiin korotuksen summaesitystä saadaan

$$\frac{-k(r+1)\pi + O(\pi^2)}{1-(1+\pi)^k + (1+\pi)^{rk} - (1+\pi)^{k(r+1)}} = \frac{-k(r+1)\pi + O(\pi^2)}{-2k\pi + \pi^2(-\binom{k}{2} + \binom{rk}{2} - \binom{k(r+1)}{2}) + O(\pi^3)}.$$

Otetaan nimittäjässä π yhteiseksi tekijäksi kaikista muista termeistä paitsi termistä $O(\pi^3)$. Näin sieventämällä saadaan

$$\frac{-k(r+1)\pi + O(\pi^2)}{-2k\pi + \pi^2(-\binom{k}{2} + \binom{rk}{2} - \binom{k(r+1)}{2}) + O(\pi^3)} = \frac{-k(r+1)\pi + O(\pi^2)}{\pi(-2k + k\pi(-k(r+1)+1)) + O(\pi^3)}.$$

Tarkastellaan erotusta $\frac{-k(r+1)\pi+O(\pi^2)}{\pi(-2k+k\pi(-k(r+1)+1))+O(\pi^3)} - \frac{r+1}{2}$. Tarkoituksena on todistaa, että se on jaollinen luvulla π, sillä tällöin väite olisi saatu todistettua. Sieventämällä saadaan

$$\frac{-k(r+1)\pi + O(\pi^2)}{\pi(-2k + k\pi(-k(r+1)+1)) + O(\pi^3)} - \frac{r+1}{2} = \frac{O(\pi^2) + O(\pi^3)}{\pi(-2k + k\pi(-k(r+1)+1)) + O(\pi^3)}.$$

Tästä esityksestä nähdään, että luvun

$$\frac{-k(r+1)\pi + O(\pi^2)}{\pi(-2k + k\pi(-k(r+1)+1)) + O(\pi^3)} - \frac{r+1}{2}$$

osoittaja on jaollinen yhdellä luvun π korkeammalla potenssilla kuin nimittäjä, sillä osoittaja on $O(\pi^2)$, mutta nimittäjä ei ole jaollinen luvulla π^2. Näin ollen

$$\frac{-k(r+1)\pi + O(\pi^2)}{\pi(-2k + k\pi(-k(r+1)+1)) + O(\pi^3)} - \frac{r+1}{2} \equiv 0 \bmod \pi.$$

Siis $\frac{1-\zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)} \equiv \frac{r+1}{2} \bmod \pi$. □

Seuraavassa lauseessa todistetaan väite $q \equiv 1 \bmod p$ hyödyntäen edellisiä lauseita. On huomionarvoista, että todistuksessa oletetaan ryhmässä $\mathbb{Q}(\zeta_p)^*$ olevan alkion α, jolle $\alpha^q = (x-\zeta_p)^{1-\iota}$. Jos tällaista alkiota ei ole ryhmässä $\mathbb{Q}(\zeta_p)^*$, niin väite ei ole välttämättä voimassa.

Lause 3.13. Olkoot x, y, p ja q ehdon $(*)$ toteuttavia lukuja. Tällöin

$$q \equiv 1 \bmod p.$$

Todistus. Todistetaan väite normin $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(u)$ avulla. Ilmoitetaan se kahdella eri tavalla modulo $(x-1)\pi$. Tällä tavoin nimittäin saadaan jokin luvulla $q-1$ jaollinen luku, joka on myös jaollinen luvulla $(x-1)\pi$, josta väite seuraa. Merkitään $N = N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}$. Lauseiden 2.14, 2.46 ja 2.34 mukaan $N(z) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(z)$ kaikilla $z \in \mathbb{Q}(\zeta_p)$. Näin ollen lauseen 3.10 mukaan $N(u) = 1$ eli $N(u) \equiv 1 \bmod (x-1)\pi$. Nyt on löydetty luvulle $N(u)$ yksi esitystapa modulo $(x-1)\pi$ ja on vielä löydettävä toinen esitystapa. Käytetään tähän edellä olevia lauseita.

Lemman 3.12 mukaan

$$N(u) \equiv 1 + \frac{x-1}{q} \sum_{k=1}^{p-1} \frac{1-\zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)} \bmod \mu^2.$$

Koska $(x-1)\pi | \mu^2$, niin

$$N(u) \equiv 1 + \frac{x-1}{q} \sum_{k=1}^{p-1} \frac{1-\zeta_p^{k(r+1)}}{(1+\zeta_p^{rk})(1-\zeta_p^k)} \bmod (x-1)\pi.$$

Lemman 3.12 nojalla $N(u) \equiv 1 + \frac{x-1}{q}\frac{(r+1)(p-1)}{2} \bmod (x-1)\pi$.

Nyt $N(u)$ on laskettu kahdella eri tavalla ja

$$1 \equiv 1 + \frac{x-1}{q}\frac{(r+1)(p-1)}{2} \bmod (x-1)\pi.$$

Siis $\frac{x-1}{q}\frac{(r+1)(p-1)}{2} \equiv 0 \bmod (x-1)\pi$. Näin ollen $\pi|(p-1)(r+1)$. Koska $\pi|p$, niin $\pi|(r+1)$ eli $r \equiv -1 \bmod \pi$. Lisäksi r on kokonaisluku, joten $r \equiv -1 \bmod p$. Luvun r määritelmän mukaan $rq \equiv -1 \bmod p$ eli $q \equiv 1 \bmod p$.

□

3.2 Obstruktioryhmä ja lause IV

Tässä luvussa todistetaan, ettei ehdon $(*)$ toteuttavia lukuja ole, kun on voimassa $\min\{p,q\} < 43$. Tämän väitteen todistuksessa käytetään apuna erästä ryhmän $\mathbb{Q}(\zeta_p)^*$ aliryhmää, jota kutsutaan obstruktioryhmäksi. Seuraavissa määritelmissä ja lauseissa tutustutaan tähän ryhmään.

Määritelmä 3.14. Olkoon $\mathfrak{r}$ renkaan $\mathbb{Z}[\zeta_p]$ alkuihanne ja $\gamma \in \mathbb{Q}(\zeta_p)$. Olkoon $a = \operatorname{ord}_{\mathfrak{r}} \gamma$, missä a on suurin kokonaisluku, jolle $\mathfrak{r}^a | \gamma$. Merkinnällä $\mathfrak{r}^a | \gamma$ tarkoitetaan, että on olemassa $\beta \in \mathbb{Z}[\zeta_p]$, jolle $\beta\gamma \in \mathfrak{r}^a$.

Määritelmä 3.15. Olkoot p ja q ehdossa $(*)$ määriteltyjä lukuja sekä $\mathfrak{p}$ esimerkissä 2.21 määritelty alkuihanne. Olkoon H seuraava joukko:

$$\{\gamma \in \mathbb{Q}(\zeta_p)^* : \operatorname{ord}_{\mathfrak{r}} \gamma \equiv 0 \bmod q \text{ kaikille renkaan } \mathbb{Z}[\zeta_p] \text{ alkuihanteille } \mathfrak{r} \neq \mathfrak{p}\}/\mathbb{Q}(\zeta_p)^{*q}.$$

On huomattava, että edellinen määritelmä voidaan kirjoittaa myös toisella tavalla. Nimittäin $\gamma \in H$ on yhtäpitävää muodon $[\gamma] = \mathfrak{f}^q\mathfrak{p}^k$ kanssa. Tässä k on kokonaisluku ja $\mathfrak{f} = \{\frac{a}{b} : a \in \mathfrak{a}\}$, missä $b \in \mathbb{Z}[\zeta_p]$ ja $\mathfrak{a}$ on renkaan $\mathbb{Z}[\zeta_p]$ ihanne.

Lause 3.16. Määritelmässä 3.15 oleva H on ryhmä. Kutsutaan sitä *obstruktioryhmäksi*.

Todistus. Todistetaan, että joukko H täyttää ryhmän ehdot. Ensinnäkin joukko H on epätyhjä, sillä $1 \in H$. Näin ollen sillä on myös neutraalialkio, koska luku 1 on sen neutraalialkio. Lisäksi joukon H alkiot ovat kompleksilukuina assosiatiivisia. Seuraavaksi todistetaan, että joukko H on suljettu. Tämän todistamiseksi käytetään määritelmästä 3.15 muotoa alkio $\gamma \in H$ on yhtäpitävää sen kanssa, että $[\gamma] = \mathfrak{f}^q\mathfrak{p}^k$. Tässä k on kokonaisluku ja $\mathfrak{f} = \{\frac{a}{b} : a \in \mathfrak{a}\}$, missä $b \in \mathbb{Z}[\zeta_p]$ ja $\mathfrak{a}$ on renkaan $\mathbb{Z}[\zeta_p]$ ihanne.

Olkoot γ_1 ja γ_2 kaksi joukon mielivaltaista H alkiota. Voidaan kirjoittaa

$$[\gamma_1] = \mathfrak{f}_1^q\mathfrak{p}^{k_1} \text{ ja } [\gamma_2] = \mathfrak{f}_2^q\mathfrak{p}^{k_2}, \text{ missä } \mathfrak{f}_1 = \{\frac{a}{b_1} : a \in \mathfrak{a}_1\} \text{ ja } \mathfrak{f}_2 = \{\frac{a}{b_2} : a \in \mathfrak{a}_2\}.$$

Merkitään $\mathfrak{f} = \{\frac{a}{b_1 b_2} : a \in \mathfrak{a}_1\mathfrak{a}_2\}$. Koska $\mathbb{Z}[\zeta_p]$ on kommutatiivinen rengas, niin $[\gamma_1\gamma_2] = \mathfrak{f}^q\mathfrak{p}^{k_1+k_2}$. Siis $\gamma_1\gamma_2 \in H$ eli H on suljettu.

On vielä todistettava, että jokaisen joukon H alkion käänteisalkio kuuluu myös joukkoon H. Olkoon $\gamma \in H$. Koska $\mathbb{Q}(\zeta_p)^*$ on ryhmä, niin $\gamma^{-1} \in \mathbb{Q}(\zeta_p)^*$. Koska $\gamma^q = 1$ joukossa H, niin $\gamma^{-1} = \gamma^{q-1}$. Edellisen kappaleen mukaan H on suljettu, joten $\gamma^{q-1} \in H$. Siis $\gamma^{-1} \in H$ ja H on ryhmä.

□

Ennen kuin siirrytään tarkemmin tarkastelemaan obstruktioryhmän alkioiden ominaisuuksia, todistetaan kaksi tarvittavaa apulausetta. Kuten luvussa 3.1, myös tässä luvussa tarkastellaan normia $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(u)$ renkaassa $\mathbb{Z}_p[\zeta_p]$. Luvusta 3.1 eroten kuitenkin normia tarkastellaan modulo μ^3, eikä modulo μ^2. Modulon tarkastelun lähestymistapa on kuitenkin samantapainen kuin aiemmin lauseen 3.11 yhteydessä. Sitä hyödynnetään samanhenkisesti myöhemmin kuin lauseessa 3.13 lukua $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(u) \bmod \mu^2$.

Lause 3.17. Olkoot x, y, p ja q ehdon $(*)$ toteuttavia lukuja. Tällöin renkaassa $\mathbb{Z}_p[\zeta_p]$ on voimassa

$$N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(u) \equiv 1 + \frac{(1-q)(x-1)^2}{2q^2} \sum_{k=1}^{p-1} \frac{\zeta_p^k}{(1-\zeta_p^k)^2} \bmod \mu^3.$$

Todistus. Käytetään normin laskemiseksi samaa ideaa kuin lauseen 3.11 todistuksessa. Merkitään $N = N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}$. Tällöin lauseiden 2.14, 2.46 ja 2.34 mukaan $N(z) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(z)$ kaikilla $z \in \mathbb{Q}(\zeta_p)$. Tehdään kaikki laskut modulo μ^3 renkaassa $\mathbb{Z}_p[\zeta_p]$.

Tarkastellaan ensin lukua u. Koska lauseen 3.13 mukaan $q \equiv 1 \bmod p$, niin $r \equiv -1 \bmod p$, joten lauseiden 3.5 ja 3.9 mukaan

$$u = \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \mu^j + \zeta_p^{-1} \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j.$$

Toisaalta, koska $\iota(\mu) = -\zeta_p \mu$, niin

$$\sum_{j=3}^{\infty} \binom{\frac{1}{q}}{j} \mu^j + \zeta_p^{-1} \sum_{j=3}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j = \mu^3 \left(\sum_{j=3}^{\infty} \binom{\frac{1}{q}}{j} \mu^{j-3} + \zeta_p^{-1} \sum_{j=3}^{\infty} \binom{\frac{1}{q}}{j} (-\zeta_p)^j \mu^{j-3} \right).$$

Laskemalla saadaan

$$\sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \mu^j + \zeta_p^{-1} \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \iota(\mu)^j \equiv 1 + \frac{\mu}{q} + \binom{\frac{1}{q}}{2} \mu^2 + \zeta_p^{-1} (1 + \frac{\iota(\mu)}{q} + \binom{\frac{1}{q}}{2} \iota(\mu^2)) \bmod \mu^3.$$

Koska $\iota(\mu) = -\zeta_p \mu$, niin $\frac{\mu}{q} + \zeta_p^{-1} \frac{\iota(\mu)}{q} = 0$. Otetaan edellisestä lausekkeesta $1 + \zeta_p^{-1}$ yhteiseksi tekijäksi, jolloin saadaan

$$1 + \frac{\mu}{q} + \binom{\frac{1}{q}}{2} \mu^2 + \zeta_p^{-1} (1 + \frac{\iota(\mu)}{q} + \binom{\frac{1}{q}}{2} \iota(\mu^2)) = (1 + \zeta_p^{-1})(1 + \frac{\binom{\frac{1}{q}}{2} \mu^2 + \zeta_p^{-1} \binom{\frac{1}{q}}{2} \iota(\mu^2)}{1 + \zeta_p^{-1}}).$$

Tarkastellaan lukua $\frac{\binom{\frac{1}{q}}{2} \mu^2 + \zeta_p^{-1} \binom{\frac{1}{q}}{2} \iota(\mu^2)}{1 + \zeta_p^{-1}}$, jotta saadaan u esitettyä yksinkertaisemmassa muodossa modulo μ^3. Koska $\iota(\mu) = -\zeta_p \mu$, niin sieventämällä saadaan

$$\frac{\binom{\frac{1}{q}}{2} \mu^2 + \zeta_p^{-1} \binom{\frac{1}{q}}{2} \iota(\mu^2)}{1 + \zeta_p^{-1}} = \frac{(1-q)\mu^2(1+\zeta_p)}{2q^2(1+\zeta_p^{-1})}.$$

Sijoitetaan $\mu = \frac{x-1}{1-\zeta_p}$, jolloin saadaan

$$\frac{(1-q)\mu^2(1+\zeta_p)}{2q^2(1+\zeta_p^{-1})} = \frac{(1-q)(x-1)^2}{2q^2(1-\zeta_p)^2} \frac{1+\zeta_p}{1+\zeta_p^{-1}}.$$

Luku $\frac{1+\zeta_p}{1+\zeta_p^{-1}}$ sievenee muotoon ζ_p, joten tehtyjen luvun $\frac{\binom{\frac{1}{q}}{2} \mu^2 + \zeta_p^{-1} \binom{\frac{1}{q}}{2} \iota(\mu^2)}{1 + \zeta_p^{-1}}$ sievennysten perusteella

$$u \equiv (1 + \zeta_p^{-1})(1 + \frac{(1-q)(x-1)^2}{2q^2} \frac{\zeta_p}{(1-\zeta_p)^2}) \bmod \mu^3.$$

Tarkastellaan nyt luvun $N(u)$ arvoa modulo μ^3 käyttäen apuna edellä laskettua luvun u arvoa modulo μ^3. Lauseen 2.14 mukaan

$$N(u) \equiv \prod_{k=1}^{p-1}(1+\zeta_p^{-k})(1+\frac{(1-q)(x-1)^2}{2q^2}\frac{\zeta_p^k}{(1-\zeta_p^k)^2}) \bmod \mu^3.$$

Toisaalta $N(1+\zeta_p^{-1}) = \prod_{k=1}^{p-1}(1+\zeta_p^{-k})$ ja esimerkin 2.16 mukaan $N(1+\zeta_p^{-1}) = 1$, joten

$$N(u) \equiv \prod_{k=1}^{p-1}\left(1+\frac{(1-q)(x-1)^2}{2q^2}\frac{\zeta_p^k}{(1-\zeta_p^k)^2}\right) \bmod \mu^3.$$

Tarkastellaan termien $\frac{(1-q)(x-1)^2}{2q^2}\frac{\zeta_p^{k_1}}{(1-\zeta_p)^2}$ ja $\frac{(1-q)(x-1)^2}{2q^2}\frac{\zeta_p^{k_2}}{(1-\zeta_p)^2}$ tuloa, missä k_1, k_2 ovat kokonaislukuja väliltä $[1, p-1]$. Tulo on $\mu^3\frac{(x-1)\zeta_p^{k_1+k_2}(1-q)^2(1-\zeta_p)^3}{2q^2(1-\zeta_p^{k_1})^2(1-\zeta_p^{k_2})^2}$, joten

$$\prod_{k=1}^{p-1}\left(1+\frac{(1-q)(x-1)^2}{2q^2}\frac{\zeta_p^k}{(1-\zeta_p^k)^2}\right) \equiv 1+\frac{(1-q)(x-1)^2}{2q^2}\sum_{k=1}^{p-1}\frac{\zeta_p^k}{(1-\zeta_p^k)^2} \bmod \mu^3.$$

Siis $N(u) \equiv 1 + \frac{(1-q)(x-1)^2}{2q^2}\sum_{k=1}^{p-1}\frac{\zeta_p^k}{(1-\zeta_p^k)^2} \bmod \mu^3$. □

Edellisessä lauseessa luvussa $N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(u) \bmod \mu^3$ esiintyy vielä hankalasti käsiteltävä summa. Tätä summaa yksinkertaistetaan seuraavassa lauseessa.

Lemma 3.18. $\sum_{k=1}^{p-1}\frac{\zeta_p^k}{(1-\zeta_p^k)^2} = \frac{1-p^2}{12}$

Todistus. Kirjoitetaan luku $\frac{\zeta_p^k}{(1-\zeta_p^k)^2}$ toisessa muodossa, jotta saadaan haluttu summa esitettyä kahden eri summan erotuksena. Laskemalla havaitaan, että $\frac{1}{(1-\zeta_p^k)^2} - \frac{1}{1-\zeta_p^k} = \frac{\zeta_p^k}{(1-\zeta_p^k)^2}$. Siis

$$\sum_{k=1}^{p-1}\frac{\zeta_p^k}{(1-\zeta_p^k)^2} = \sum_{k=1}^{p-1}\frac{1}{(1-\zeta_p^k)^2} - \sum_{k=1}^{p-1}\frac{1}{1-\zeta_p^k}. \tag{18}$$

Lasketaan summa $\sum_{k=1}^{p-1}\frac{\zeta_p^k}{(1-\zeta_p^k)^2}$ käyttäen hyödyksi summia $\sum_{k=1}^{p-1}\frac{1}{(1-\zeta_p^k)^2}$ ja $\sum_{k=1}^{p-1}\frac{1}{1-\zeta_p^k}$.

Tarkastellaan ensin summaa $\sum_{k=1}^{p-1}\frac{1}{(1-\zeta_p^k)^2}$. Olkoon $x_k = \frac{1}{1-\zeta_p^k}$. Tällöin

$$\sum_{k=1}^{p-1}\frac{1}{(1-\zeta_p^k)^2} = \sum_{k=1}^{p-1}x_k^2. \tag{19}$$

Lasketaan summan $\sum_{k=1}^{p-1} x_k^2$ arvo käyttämällä Vietan kaavoja. Nimittäin, jos jonkin polynomin kaikki juuret ovat luvut x_k, niin

$$\sum_{k=1}^{p-1} x_k^2 = (\sum_{k=1}^{p-1} x_k)^2 - 2\sum_{k=1}^{p-1}\sum_{j=k+1}^{p-1} x_k x_j$$

ja oikealla puolella olevat summat voidaan laskea Vietan kaavojen avulla. On siis löydettävä polynomi, jonka kaikki nollakohdat ovat luvut x_k yksinkertaisina. Tunnetusti luvut ζ_p^k ovat polynomin $f(x) = \frac{x^p-1}{x-1}$ kaikki juuret. Näin ollen polynomin $f_1(x) = f(1-x)$ kaikki juuret ovat luvut $1-\zeta_p^k$. Olkoon nyt $f_2(x) = f_1(\frac{1}{x})$, jolloin $f_2(x_k) = 0$ kaikilla luvuilla x_k. Toisaalta, tekemällä edellä olevat sijoitukset saadaan $f_2(x) = \frac{(1-\frac{1}{x})^p-1}{-\frac{1}{x}}$. Saadaan siis, että $-x(1-\frac{1}{x})^p + x = 0$ aina, kun $x = x_k$. Edellinen yhtälö voidaan kertoa luvulla x^{p-1}, jolloin saadaan, että $-(x-1)^p + x^p = 0$ kaikilla $x = x_k$. Olkoon $p(x) = -(x-1)^p + x^p$. Koska se on astetta $p-1$ ja sille on löydetty $p-1$ eri juurta, niin sen kaikki juuret ovat luvut x_k. Siis on löydetty halutunlainen polynomi $p(x)$.

Nyt voidaan käyttää Vietan kaavoja apuna. Olkoot a_{p-1}, a_{p-2} ja a_{p-3} polynomin $p(x)$ astetta $p-1$, $p-2$ ja $p-3$ olevien termien kertoimet. Tällöin $a_{p-1} = p$, $a_{p-2} = -\binom{p}{2}$ ja $a_{p-3} = \binom{p}{3}$. Vietan kaavojen mukaan

$$(\sum_{k=1}^{p-1} x_k)^2 - 2\sum_{k=1}^{p-1}\sum_{j=k+1}^{p-1} x_k x_j = (-\frac{a_{p-2}}{a_{p-1}})^2 - 2\frac{a_{p-3}}{a_{p-1}}.$$

Sijoittamalla arvot saadaan $(-\frac{a_{p-2}}{a_{p-1}})^2 - 2\frac{a_{p-3}}{a_{p-1}} = (\frac{\binom{p}{2}}{p})^2 - 2\frac{\binom{p}{3}}{p}$. Sieventämällä tätä saadaan $(\frac{\binom{p}{2}}{p})^2 - 2\frac{\binom{p}{3}}{p} = \frac{(1-p)(p-5)}{12}$. Kaavan (19) nojalla

$$\sum_{k=1}^{p-1} \frac{1}{(1-\zeta_p^k)^2} = \frac{(1-p)(p-5)}{12}.$$

On enää selvitettävä summa $\sum_{k=1}^{p-1} \frac{1}{1-\zeta_p^k}$. Havaitaan, että edellisen kappaleen merkinnöin $\sum_{k=1}^{p-1} \frac{1}{1-\zeta_p^k} = \sum_{k=1}^{p-1} x_k$ ja oikean puoleisen summan arvo laskettiin jo edellisessä kappaleessa. Se on $\frac{\binom{p}{2}}{p} = \frac{p-1}{2}$. Siis

$$\sum_{k=1}^{p-1} \frac{1}{(1-\zeta_p^k)^2} - \sum_{k=1}^{p-1} \frac{1}{1-\zeta_p^k} = \frac{(1-p)(p-5)}{12} - \frac{p-1}{2}.$$

Sieventämällä saadaan $\frac{(1-p)(p-5)}{12} - \frac{p-1}{2} = \frac{1-p^2}{12}$. Siis kaavan (18) nojalla

$$\sum_{k=1}^{p-1} \frac{\zeta_p^k}{(1-\zeta_p^k)^2} = \frac{1-p^2}{12}.$$

□

Edellisen lemman avulla siis saadaan

$$N_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}(u) \equiv 1 + \frac{(1-q)(x-1)^2}{2q^2}\frac{1-p^2}{12} \bmod \mu^3.$$

Tätä muotoa käytetään myöhemmin lauseen 3.21 todistuksessa. Seuraavaksi tutustutaan kahteen määritelmään, joiden avulla voidaan muotoilla obstruktioryhmän alkioita koskeva lauseen 3.21 väite.

Määritelmä 3.19. Olkoon M $\mathbb{Z}[G]$-moduli. Sen miinusosa on

$$M^- = \{(1-\iota)\, m : m \in M\}.$$

On huomattava, että H ja joukko H^- ovat $\mathbb{Z}[G]$-moduleja. Olkoon nimittäin $h \in H$ ja $\sigma \in \mathbb{Z}[G]$. Tällöin ryhmä $\mathbb{Z}[G]$ operointi joukossa H on h^σ. Lauseen 3.16 nojalla H on ryhmä ja tarkemmin abelin ryhmä kertolaskun suhteen sekä $h^\sigma \in H$. Näin modulikertolaskuna toimii käsitelty operointi ja ryhmän H yhteenlaskuna kertolasku. Näin tulkittuna H on $\mathbb{Z}[G]$-moduli. Näin ollen voidaan myös määritellä joukko H^-. Vastaavalla pättelyllä myös joukko H^- on $\mathbb{Z}[G]$-moduli. Tätä tietoa tarvitaan, jotta myöhemmin esitettyjä määritelmiä voidaan soveltaa joukkoihin H ja H^-.

Määritelmä 3.20. Joukon H^- alkio h on *triviaali* alkio, jos on olemassa $\gamma \in \mathbb{Q}(\zeta_p)^*$, jolle $h = \gamma^q$. Alkio h on *epätriviaali*, jos se ei ole triviaali alkio.

Edellisten määritelmien avulla saadaan muotoiltua obstruktioryhmän alkiota $(x-\zeta_p)^{1-\iota}$ koskeva väite. Seuraava lause käytännössä sanoo, että jos ehdon $(*)$ toteuttavat luvut löytyvät, niin obstruktioryhmästä löytyy epätriviaali alkio. Myöhemmin todistetaan, ettei kuitenkaan obstruktioryhmässä voi olla epätriviaaleja alkioita, kun vähintään toinen luvuista p, q on pienempi kuin 43. Näin ollen tällöin ei myöskään voi olla ehtoa $(*)$ toteuttavia lukuja.

Lause 3.21. Olkoot x, y, p ja q ehdon $(*)$ toteuttavia lukuja. Tällöin luku $(x-\zeta_p)^{1-\iota}$ on obstruktioryhmän H epätriviaali alkio.

Todistus. Todistetaan ensin, että $x - \zeta_p \in H$, jolloin $(x-\zeta_p)^{1-\iota} \in H^-$. Tehdään tämä todistamalla, että kaikki luvut $x - \zeta_p^k$, missä kokonaisluku $k \in [1, p]$, kuuluvat ryhmään H. Ensinnäkin, $x - \zeta_p^k \in \mathbb{Q}(\zeta_p)^*$. Koska x, y, p, q toteuttavat Catalanin yhtälön, niin $\prod_{k=1}^{p}(x-\zeta_p^k) = y^q$. Koska yhtälön oikea puoli on luku y potenssiin q, on myös vasemman puolen oltava jokin luku potenssiin q kunnassa $\mathbb{Q}(\zeta_p)^*$. Koska $\frac{1-\zeta_p^k}{1-\zeta_p} = \frac{x-1}{1-\zeta_p} + \frac{1-\zeta_p^k}{1-\zeta_p}$, $1-\zeta_p|(x-1)$ ja $1-\zeta_p|(1-\zeta_p^k)$, niin $\frac{1-\zeta_p^k}{1-\zeta_p} \in \mathbb{Z}[\zeta_p]$. Näin ollen minkä tahansa kahden luvun $1-\zeta_p^{k_1}$ ja $1-\zeta_p^{k_2}$ suurin yhteinen tekijä renkaassa $\mathbb{Z}[\zeta_p]$ jakaa luvun $1-\zeta_p$. Voidaan siis kirjoittaa tulo $\prod_{k=1}^{p}(x-\zeta_p^k)$ muodossa $A\prod_{k=1}^{p}(\frac{x-\zeta_p^k}{A_k})$, missä $A, A_k \in \mathbb{Z}[\zeta_p]$, $A_k|(x-\zeta_p^k)$, $(1-\zeta_p)|A$ ja minkä tahansa kahden termin $\frac{x-\zeta_p^k}{A_k}$ suurin yhteinen tekijä on 1. Täten kaikille renkaan $\mathbb{Z}[\zeta_p]$ alkuihanteille $\mathfrak{r} \neq \mathfrak{p}$ on voimassa

$$\mathrm{ord}_{\mathfrak{r}}(x-\zeta_p^k) \equiv 0 \bmod q.$$

Siis $x - \zeta_p^k \in H$. Näin ollen $(x-\zeta_p)^{1-\iota} \in H^-$.

Todistetaan väite, että $(x-\zeta_p)^{1-\iota}$ on epätriviaali alkio, vastaoletuksen avulla. Oletetaan, että $(x-\zeta_p)^{1-\iota}$ on ryhmän H triviaali alkio eli $\frac{x-\zeta_p}{x-\iota(\zeta_p)} = \gamma^q$ jollain luvulla $\gamma \in \mathbb{Q}(\zeta_p)^*$. Johdetaan tämä ristiriitaan tutkimalla luvun u normia modulo μ^3 renkaassa $\mathbb{Z}_p[\zeta_p]$.

Lauseen 3.17 ja lemman 3.18 mukaan

$$N(u) \equiv 1 + \frac{(1-q)(x-1)^2}{2q^2}\frac{1-p^2}{12} \bmod \mu^3.$$

Koska lauseen 3.10 mukaan $N(u) = 1$, niin $\frac{(1-q)(x-1)^2}{2q^2}\frac{1-p^2}{12} \equiv 0 \bmod \mu^3$. Toisaalta $\mu^3 = (\frac{x-1}{-\pi})^3$, joten $x-1$ jakaa luvun $\frac{1-q}{2q^2}\frac{1-p^2}{12}\pi^3$ renkaassa $\mathbb{Z}_p[\zeta_p]$. Lauseen 3.2 mukaan $x - 1 \equiv 0 \bmod p^{q-1}$, joten p^{q-1} jakaa luvun $\frac{1-q}{2q^2}\frac{1-p^2}{12}\pi^3$. Koska $\mathrm{syt}(p, 1-p^2) = 1$, niin $p^{q-1}|\frac{1-q}{2q^2}\frac{\pi^3}{12}$ ja edelleen $p^{q-1}|\frac{1-q}{3}\pi^3$. Toisaalta $\frac{\pi^3}{3}$ jakaa luvun p, joten $p^{q-2}|(1-q)$. Koska p on pariton alkuluku, niin $p^{q-2} > 2^{q-2} = (1+1)^{q-2}$. Tämä potenssiinkorotus voidaan kirjoittaa summamuodossa $(1+1)^{q-2} = \sum_{k=0}^{q-2}\binom{q-2}{k}1^k$. Koska summassa on $q-1$ termiä ja ne ovat kaikki positiivisia kokonaislukuja, niin $\sum_{k=0}^{q-2}\binom{q-2}{k}1^k \geq q-1$. Siis $p^{q-2} > q-1 > 1-q > -p^{q-2}$, mikä on ristiriidassa tuloksen $p^{q-2}|(1-q)$ kanssa. Näin ollen vastaoletuksen, että $(x-\zeta_p)^{1-\iota}$ on ryhmän H triviaali alkio, täytyy olla väärin ja $(x-\zeta_p)^{1-\iota}$ on ryhmän H epätriviaali alkio. □

Kuten jo aiemmin mainittiin, lauseen IV väite seuraa siitä, ettei obstruktioryhmässä ole epätriviaaleja alkioita. Ennen tämän todistamista tutustutaan muutamaan todistuksessa hyödylliseen määritelmään.

Määritelmä 3.22. Olkoon M renkaan $\mathbb{Z}[G]$ moduli ja q pariton alkuluku. Tällöin määritellään $M[q] = \{m \in M : qm = 0\}$.

Aiemmin on todettu, että joukot H ja H^- ovat $\mathbb{Z}[G]$-moduleja. Näin ollen edellisen määritelmän mukaan voidaan määritellä joukot $H[q]$ ja $H^-[q]$. Lisäksi jokaiselle renkaan $\mathbb{Z}[G]$ modulille M pätee, että myös $M[q]$ on $\mathbb{Z}[G]$-moduli. Modulikertolaskuna toimii sama modulikertolasku kuin $\mathbb{Z}[G]$-modulilla M.

Määritelmä 3.23. Olkoon $b \in \mathbb{Z}[\zeta_p]$ ja $\mathfrak{a}$ renkaan $\mathbb{Z}[\zeta_p]$ ihanne. Tällöin joukkoa $I = \{\frac{a}{b} : a \in \mathfrak{a}\}$ kutsutaan kunnan $\mathbb{Q}(\zeta_p)$ *osamäärä ihanteeksi.*

Määritelmä 3.24. Joukko Cl_p on

$$Cl_p = \{I/P : I \text{ on kunnan } \mathbb{Q}(\zeta_p) \text{ osamäärä ihanne ja } P \text{ pääihanne}\}.$$

Samoin kuin aiemmin joukkojen H ja H^- kohdalla todettiin, myös joukot Cl_p ja Cl_p^- ovat $\mathbb{Z}[G]$-moduleja. Modulikertolaskuna toimii sama laskutoimitus kuin modulien H ja H^- tapauksissa. Näin ollen myös $Cl_p^-[q]$ voidaan määritellä määritelmän 3.22 tavalla. Myös $Cl_p^-[q]$ on $\mathbb{Z}[G]$-moduli. Seuraavassa lauseessa kerrotaan, miten modulin $Cl_p^-[q]$ tunteminen auttaa modulin H^- käsittelyssä.

Lause 3.25. On olemassa moduli-isomorfismi modulilta H^- modulille $Cl_p^-[q]$.

Todistus. Tarkastellaan kuvausta $\psi : H \to Cl_p[q]$. Olkoon $\gamma \in H$ ja $[\gamma] = \mathfrak{a}^q\mathfrak{p}^k$ jollekin kokonaisluvulle k ja kunnan $\mathbb{Q}(\zeta_p)$ osamäärä ihanteelle $\mathfrak{a}$. Kuvaus ψ kuvaa luvun γ osamäärä ihanteiden $\mathfrak{a}$ luokkaan. Koska $\mathfrak{p}$ on esimerkin 2.21 mukaan alkuihanne, niin ψ on hyvinmääritelty kuvaus. Kuvaus ψ on selvästi homomorfismi. Jokaiselle ihanteelle $\mathfrak{a}$, jolle $\mathfrak{a}^q = [\gamma]$ jollain $\gamma \in \mathbb{Q}(\zeta_p)$, on olemassa alkukuva joukossa H. Siis ψ on surjektio. Kuvauksen ψ ydin muodostuu alkioista $\beta \in H$, joille $[\beta] = \mathfrak{p}^k$, missä k on kokonaisluku.

Rajoitetaan nyt kuvaus ψ kuvaukseksi ψ', jonka lähtöjoukko on ryhmältä H^-. Tällöin $\psi' : H^- \to Cl_p[q]^-$. Koska $Cl_p[q]^- = Cl_p^-[q]$, niin $\psi' : H^- \to Cl_p^-[q]$. Olkoon $\beta \in H$ ja $[\beta] = \mathfrak{p}^k$. Tällöin $\beta = (\beta_1(1-\zeta_p))^k$ jollain yksiköllä $\beta_1 \in \mathbb{Z}[\zeta_p]$. Koska $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\beta_1) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\iota(\beta_1))$, niin lauseen 2.12 mukaan myös $\iota(\beta_1)$ on renkaan $\mathbb{Z}[\zeta_p]$ yksikkö. Siis $\frac{\beta_1}{\iota(\beta_1)} \in \mathbb{Z}[\zeta_p]$. Lisäksi $|\sigma(\frac{\beta_1}{\iota(\beta_1)})| = 1$ kaikilla $\sigma \in G$. Näin ollen myös $|\sigma(\beta)| = 1$ kaikilla $\sigma \in G$. Lauseen 2.17 mukaan β on ykkösenjuuri. Lauseen 3.6 mukaan β on $2p$:nnes ykkösenjuuri. Nämä kaikki ykkösenjuuret voidaan esittää muodossa γ^q, missä $\gamma \in \mathbb{Q}(\zeta_p)^*$. Siis ψ' on isomorfismi. Näin ollen on olemassa isomorfismi modulilta H^- modulille $Cl_p^-[q]$. □

Merkitään joukon Cl_p^- kertalukua symbolilla h_p^-. Tämän kertaluvun laskemiseksi tunnetaan kaava, kun p on pariton alkuluku, ja jo 1800-luvulla Kummer osasi laskea niitä. Tietoa tästä löytyy teoksesta [5]. Taulukossa 1 on listattu luvun h_p^- saamat arvot, kun $p \leq 41$.

Taulukko 1: Luvut h_p^-, kun $p \leq 41$

p	h_p^-	p	h_p^-	p	h_p^-	p	h_p^-
3	1	11	1	19	1	31	9
5	1	13	1	23	3	37	37
7	1	17	1	29	8	41	121

Lause 3.26 (IV)**.** Olkoot p ja q ovat parittomia alkulukuja, joista vähintään toinen on pienempi kuin 43. Tällöin Catalanin yhtälöllä $x^p - y^q = 1$ ei ole yhtään ratkaisua kokonaisluvuilla x, y, jotka ovat erisuuria kuin nolla.

Todistus. Todistetaan ensin, että jos p ei jaa lukua h_q^- tai q ei jaa lukua h_p^-, niin ehdon $(*)$ toteuttavia x ja y ei ole. Tällöin riittää todistaa, että jos $\min\{p, q\} < 43$, niin $p \nmid h_q^-$ tai $q \nmid h_p^-$.

Oletetaan ensin, ettei q jaa lukua h_p^-. Tällöin $Cl_p^-[q]$ on triviaali. Lemman 3.1 ja lauseen 3.25 mukaan $Cl_p^-[q]$ on isomorfinen ryhmän H^- kanssa, joten myös H^- on triviaali. Kuitenkin lauseen 3.21 mukaan, jos Catalanin yhtälöllä on ehdon $(*)$ toteuttava ratkaisu, niin ryhmässä H^- on oltava epätriviaali alkio. Siis Catalanin yhtälöllä ei voi olla ratkaisua $xy \neq 0$. Vastaava todistus voidaan tehdä myös, kun p ei jaa lukua h_q^-.

Todistetaan seuraavaksi, että jos parittomista alkuluvuista p ja q vähintään toinen on pienempi kuin 43, niin ainakaan toinen luvuista h_q^- tai h_p^- ei ole jaollinen luvulla p tai q. Ensinnäkin, lemman 3.1 mukaan $p \neq q$. Oletetaan ensin, että $p < q$. Tällöin $p < 43$. Taulukosta 1 nähdään, että $h_p^- = 1$, kun $p \leq 19$. Siis kun $p \leq 19$, niin q ei voi jakaa lukua h_p^-, koska $q \neq \pm 1$. Lisäksi, kun $p = 29$, niin luvulla h_p^- ei ole yhtään paritonta alkutekijää, joten luku q ei voi jakaa sitä. Tapauksessa $p = 37$ on myös $h_p^- = 37$. Luku q ei voi jakaa lukua h_p^-, koska $p \neq q$. Kun $p = 23, 31, 41$, niin h_p^- on vastaavasti $3, 3^2, 11^2$. Jotta nyt q jakaisi luvun h_p^-, niin $q < p$, mikä on vastoin oletusta $p < q$. Kun siis $p < q$ ja vähintään toinen näistä on pienempi kuin 43, niin q ei jaa lukua h_p^-. Alun todistuksen mukaan tällöin Catalanin yhtälöllä ei voi olla ratkaisua $xy \neq 0$.

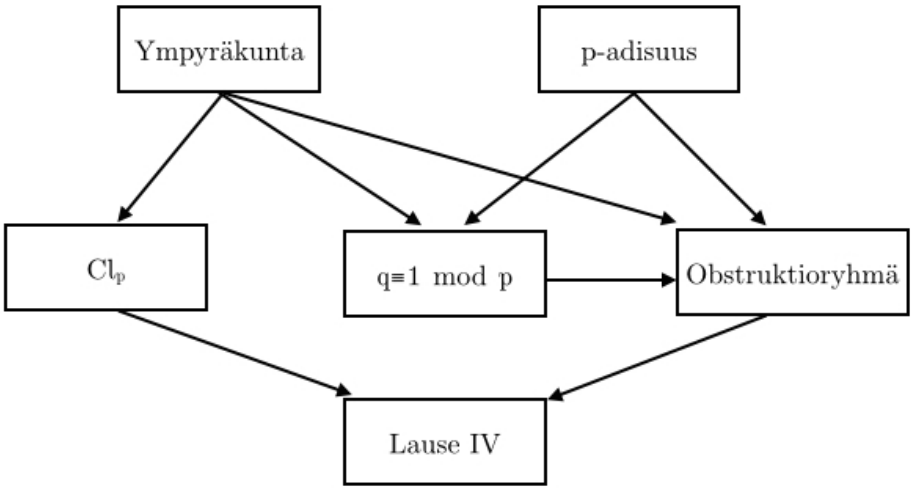
Tarkastellaan vielä tapausta $p > q$. Nyt $q < 43$. Tällöin h_q^- saa vastaavat arvot kuin h_p^- taulukossa 1. Samoin kuin edellisessä kappaleessa, voidaan

todistaa, ettei luku p jaa lukua h_q^-. Siis tällöinkään Catalanin yhtälöllä ei voi olla ratkaisua $xy \neq 0$, joten Catalanin yhtälöllä ei ole ratkaisua $xy \neq 0$, kun vähintään toinen luvuista p tai q on pienempi kuin 43.

□

4 Lopuksi

Tässä tutkielmassa todistettiin, ettei yhtälöllä $x^p - y^q = 1$ ole nollasta eroavia kokonaislukuratkaisuja, kun p ja q ovat parittomia alkulukuja. Todistuksen rakenne näkyy kuvassa 1. Luvussa 3.1 todistettiin, että sopivien alkuehtojen täyttyessä $q \equiv 1 \bmod p$. Todistus tehtiin tarkastelemalla sopivia kunnan $\mathbb{Q}(\zeta_p)$ alkioita ja niiden normeja Galois'n laajennuksessa $\mathbb{Q}_p(\zeta_p)/\mathbb{Z}_p[\zeta_p]$. Kunnan $\mathbb{Q}(\zeta_p)$ alkioiden normeja Galois'n laajennuksessa $\mathbb{Q}_p(\zeta_p)/\mathbb{Z}_p[\zeta_p]$ tutkittiin myös luvussa 3.2. Tässä luvussa määriteltiin obstruktioryhmä ja joukko Cl_p sekä todistettiin näille eri ominaisuuksia. Ominaisuudet saatiin laskemalla sopivien kunnan $\mathbb{Q}(\zeta_p)$ alkioiden normeja Galois'n laajennuksessa $\mathbb{Q}_p(\zeta_p)/\mathbb{Z}_p[\zeta_p]$ ja käyttämällä luvussa 3.1 saatua tulosta $q \equiv 1 \bmod p$. Obstruktioryhmän ja joukon Cl_p ominaisuuksien avulla todistettiin, ettei yhtälöllä $x^p - y^q = 1$ ole nollasta eroavia kokonaislukuratkaisuja, kun p ja q ovat parittomia alkulukuja.



Kuva 1: Todistuksen rakenne

Tarkastellaan vielä, miten lausetta IV voidaan käyttää apuna Catalanin yhtälön ratkaisussa. Jo 1850-luvulla Lebesgue osoitti, ettei yhtälöllä $x^p = y^2 + 1$ ole nollasta eroavia kokonaislukuratkaisuja, kun $p \geq 2$. Myöhemmin 1900-luvulla Chein osoitti, että yhtälön $x^2 = y^q + 1$ nollasta eroavat kokonaislukuratkaisut ovat $(x, y, q) = (\pm 3, 2, 3)$, kun $q > 3$. Nämä todistukset löytyvät lähteistä [6] ja [3]. Näiden todistuksien mukaan Catalanin yhtälön ratkaisemiseksi on tarkasteltava vain parittomia lukujen p ja q arvoja.

Oletetaan, että p ja q ovat alkulukuja, $\min\{p, q\} \geq 7$ sekä jollain nollas-

ta eroavilla kokonaisluvuilla x ja y on voimassa $x^p - y^q = 1$. Kirjassa [12] esitetään seuraaville kolmelle lauseelle todistukset:

Lause 4.1 (I)**.** $p^{q-1} \equiv 1 \bmod q^2$ ja $q^{p-1} \equiv 1 \bmod p^2$

Lause 4.2 (II)**.** $p \equiv 1 \bmod q$ tai $q \equiv 1 \bmod p$

Lause 4.3 (III)**.** $p < 4q^2$ ja $q < 4p^2$

Todistetaan, että näistä lauseista saadaan seuraava tulos.

Lause 4.4. Olkoot x, y, p ja q kokonaislukuja, $xy \neq 0$ ja $\min\{p, q\} \geq 2$. Tällöin yhtälön $x^p - y^q = 1$ ratkaisut ovat $(x, y, p, q) = (\pm 3, 2, 2, 3)$.

Todistus. Todistetaan ensin, että väite on voimassa, kun p ja q ovat alkulukuja. Lebesguen ja Cheinin todistusten nojalla voidaan olettaa, että p ja q ovat parittomia alkulukuja. Lisäksi lemman 3.1 mukaan $p \neq q$. Lauseen IV mukaan voidaan olettaa, että $\min\{p, q\} \geq 7$. Nyt lauseen II mukaan $p \equiv 1 \bmod q$ tai $q \equiv 1 \bmod p$. Oletetaan, että $p \equiv 1 \bmod q$. Tapaus $q \equiv 1 \bmod p$ todistetaan samoin. Todistetaan seuraavaksi aputulos, että $p \equiv 1 \bmod q^2$.

Lauseen I mukaan $p^{q-1} \equiv 1 \bmod q^2$. Näin ollen voidaan kirjoittaa $p - 1 = n_1 q$ ja $p^{q-1} - 1 = n_2 q^2$ joillain kokonaisluvuilla n_1 ja n_2. Tavoitteena on todistaa, että q jakaa luvun n_1. Voidaan kirjoittaa $p^{q-1} - 1 = (p-1)\sum_{j=0}^{q-2} p^j$. Täten $n_2 q^2 = n_1 q \sum_{j=0}^{q-2} p^j$. Siis $q | n_1$ tai $q | \sum_{j=0}^{q-2} p^j$. Koska $p \equiv 1 \bmod q$, niin $\sum_{j=0}^{q-2} p^j \equiv q - 1 \not\equiv 0 \bmod q$. Siis $q | n_1$ ja $p \equiv 1 \bmod q^2$.

Voidaan siis kirjoittaa $p = 1 + nq^2$, missä n on positiivinen kokonaisluku. Lauseen III mukaan $n \leq 3$. Jos $n = 1$ tai $n = 3$, niin $1 + nq^2$ on parillinen luku. Tämä ei kuitenkaan ole mahdollista, koska on oletettu, että p on pariton luku. Siis enää on tarkasteltava tapausta $n = 2$. Koska $\min\{p, q\} \geq 7$, niin $q \neq 3$. Täten $1 + 2q^2 \equiv 0 \bmod 3$. Mutta on oletettu, että $p \geq 7$, joten tämä ei ole mahdollista. Siis yhtälöllä $x^p - y^q = 1$ ei ole ratkaisuja, kun p, q ovat alkulukuja ja $\min\{p, q\} \geq 7$.

Todistetaan vielä, että väite pätee kaikilla kaikilla kokonaisluvuilla p, q, kun $\min\{p, q\} \geq 2$. Oletetaan, että kokonaisluvut x, y, p ja q toteuttavat Catalanin yhtälön. Tällöin on olemassa alkuluvut $p_1 | p$ ja $q_1 | q$. Voidaan kirjoittaa $p = p_1 k_p$ ja $q = q_1 k_q$, missä k_p ja k_q ovat positiivisia kokonaislukuja. Yhtälö $x^p - y^q = 1$ voidaan kirjoittaa muodossa $(x^{k_p})^{p_1} - (y^{k_q})^{q_1} = 1$. Täten jo todistettujen asioiden mukaan $x^{k_p} = 2$ ja $y^{k_q} = \pm 3$. Tämä on mahdollista vain, kun $k_p = k_q = 1$. Tällöin p ja q ovat alkulukuja. Täten Catalanin yhtälön $x^p - y^q = 1$ ratkaisut ovat $(x, y, p, q) = (\pm 3, 2, 2, 3)$. □

Kirjallisuutta

[1] Dennis S. Bernstein. *Matrix mathematics: theory, facts, and formulas with application to linear systems theory.* Princeton University Press, Princeton, 2005.

[2] J. W. S. Cassels. On the equation $a^x - b^y = 1$. II. *Mathematical Proceedings of the Cambridge Philosophical Society*, 56:97–103, 1960.

[3] E. Z. Chein. A note on the equation $x^2 = y^q + 1$. *Proc. Amer. Math. Soc.*, 56, 1976.

[4] Fernando Q. Gouvêa. *p-adic Numbers: An Introduction.* Springer-Verlag Berlin Heidelberg, toinen laitos, 1997.

[5] E. E. Kummer. Über die zerlegung der aus wurzeln der einheit gebildeten complexen zahlen in ihre primfactoren. *J. Reine Angew. Math*, 35, 1847.

[6] V. Lebesgue. Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$. *Nouvelles annales de mathématiques : journal des candidats aux écoles polytechnique et normale*, 9, 1850.

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

[8] M. Mignotte. Catalan's equation just before 2000. Kirjassa Matti Jutila ja Tauno Metsänkylä, toim., *Proceedings of the Turku Symposium on Number Theory in Memory of Kustaa Inkeri May 31-June 4, 1999.* de Gruyter, Berlin, 2001.

[9] Preda Mihăilescu. A class number free criterion for Catalan's conjecture. *J. Number Theory*, 99, 2003.

[10] Preda Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. reine angew. Mathematik*, 572, 2004.

[11] Preda Mihăilescu. On the class groups of cyclotomic extensions in presence of a solution to Catalan's equation. *J. Number Theory*, 118, 2006.

[12] René Schoof. *Catalan's conjecture.* Springer-Verlag, London, 2008.

[13] Joel Spencer. An elementary proof of Kronecker's theorem. *Fibonacci Quart.*, 15, 1977.

[14] Ian Stewart ja David Tall. *Algebraic number theory and Fermat's last theorem.* AK Peters, kolmas laitos, 2002.

[15] R. Tijdeman. On the equation of Catalan. *Acta Arithmetica*, 29, 1976.

[16] Kari Ylinen. *Topologian perusteet.* Turun yliopisto, Luentomoniste, 2011.