3.3 Luokkaryhmä

Seuraavana tavoitteena on osoittaa, että binääristen neliömuotojen ekvivalenssiluokat muodostavat ryhmän.

Määritelmä 3.39. Määritellään operaatio kahden samaa diksriminanttia olevan binäärisen neliömuodon $f_1(a_1, b_1, c_1)$ ja $f_2(a_2, b_2, c_2)$ välillä seuraavalla tavalla. Olkoot $s = (b_1 + b_2)/2, n = (b_1 - b_2)/2$, ja u, v, w ja D sellaisia

$$ua_1 + va_2 + ws = d = syt(a_1, a_2, s),$$

ja

$$d_0 = syt(d, c_1, c_2, n).$$

Nyt f_1 ja f_2 yhdiste tuottaa neliömuodon

$$(a_3, b_3, c_3) = \left(d_0 \frac{a_1 a_2}{d^2}, b_2 + \frac{2a_2}{d}(v(s - b2) - wc_2), \frac{b_3^2 - D}{4a_3} \right).$$

Propositio 3.40. *Ekvivalenssiluokat, ja ylläoleva operaatio muodostavat äärellisen Abelin ryhmän, jonka koko on h_D, eli luokkaluku.*

3.4 Yhteys neliökuntien luokkalukuihin

Kuten huomattiin, definiittien ja epädefiniittien neliömuotojen teorialla oli eronsa. Samalla lailla imaginääristen neliökuntien teoria oli helpompi kuin reaalisten neliökuntien. Yksi ero imaginäärisillä neliökunnilla ja reaalisilla neliökunnilla on se, että imaginäärisessä kunnassa $N(\alpha) > 0$ kaikille $\alpha \in K = \mathbb{Q}(\sqrt{-D})$. Reaalisen neliökunnan tapauksessa $N(\alpha)$ voi olla positiivinen tai negatiivinen.

Ideaaliluokkien joukossa määriteltiin ideaalit I ja J ekvivalenteiksi, jos oli olemassa $\alpha, \beta \in O_K$, joille $(\alpha)I = (\beta)J$. Tästä seuraa, että I ja J ovat ekvivalentteja, jos $I = (\alpha/\beta)J$. Ei kuitenkaan tiedetä, onko $\alpha/\beta \in O_K$. Tämän vuoksi määritellään nyt murtoideaali.

Määritelmä 3.41. Ideaali I on murtoideaali, jos on olemassa määrätty $\nu \in O_K$, jolle pätee, että jokaista $\alpha \in I$, aina $\nu\alpha \in O_K$

Jokainen ideaali on murtoideaali. Lisäksi murtoideaaleille sallitaan "yhteinen nimittäjä".

Kuten kunnalle $K = \mathbb{Q}(\sqrt{D})$ ja sen kokonaislukujen renkaalle O_K voidaan antaa kannat. Voidaan antaa kanta myös ideaalille $I \lhd O_K$. Sillä on kanta $\{\alpha_1, \alpha_2\}$, joten jokainen $\beta \in I$ voidaan kirjoittaa muotoon $\beta = x\alpha_1 + y\alpha_2$, missä $x, y \in \mathbb{Z}$.

Lisäksi kullekin ideaalille voidaan antaa kanoninen kanta, joka on yksikäsitteinen $\{a, b + g\delta\}$, missä $a, b, g \in \mathbb{Z}$, $\delta \in O_K$, $a > 0$, $0 \leq b < a$, $0 \leq g \leq a$ ja $g \mid a, b$. Kun ideaalille on löydetty kanta $\{\alpha_1, \alpha_2\}$ on sille helppo laskea normi, nimittäin $N(I) = |\alpha_1\bar{\alpha_2} - \bar{\alpha_1}\alpha_2|/\sqrt{D}$.

Jos ideaalilla on kanoninen kanta $\{a, b + g\delta\}$, on vastaavan murtoideaalin kanta muotoa $\{a/\nu, (b + g\delta)/\nu\}$

Edellisissä luvuissa määriteltiin ideaalit I ja J ekvivalenteiksi, jos oli olemassa $\alpha, \beta \in O_K$, joille $(\alpha)I = (\beta)J$.

Murtoideaalien tapauksessa määritellään $I \sim J$, jos $I = (\gamma)J$. Ekvivalenssia kutsutaan kapeaksi ekvivalenssiksi, jos $N(\gamma) > 0$. Kun K on imaginäärinen neliökunta, kapea ekvivalenssi on sama kuin ekvivalenssi. Jos kyseessä on reaalinen neliökunta, ekvivalenssiluokka saattaa hajota kahteen kapeaan ekvivalenssiluokkaan.

Ideaalista neliömuotoon ja neliömuodosta ideaaliin.

Osoitetaan, että jokaista ideaalia vastaa muoto, ja jokaista muotoa vastaa ideaali, ja että ekvivalentit ideaalit vastaavat ekvivalentteja muotoja ja päin vastoin.

Millä tahansa ideaalilla I on kahden alkion kanta $\{\alpha_1, \alpha_2\}$, missä $\alpha_1, \alpha_2 \in O_K$. Siis $I = \{x\alpha_1 + y\alpha_2 : x, y \in I\}$.

Jotta erotetaan kannat $\{\alpha_1, \alpha_2\}$ ja $\{\alpha_2, \alpha_1\}$ toisistaan, luodaan järjestys kannoille. Kantaa $\{\alpha_1, \alpha_2\}$ sanotaan järjestetyksi, jos $\alpha_1\bar{\alpha_2} - \bar{\alpha_1}\alpha_2 = N(I)\sqrt{D}$ on positiivinen tai positiivinen imaginäärinen, eli $-i(\alpha_1\bar{\alpha_2} - \bar{\alpha_1}\alpha_2) > 0$..

Tähän ideaaliin liitämme neliömuodon,

$$Q_I := \frac{N(\alpha_1 x + \alpha_2 y)}{N(I)} = \frac{\alpha_1\bar{\alpha_1}x^2 + (\alpha_1\bar{\alpha_2} + \bar{\alpha_1}\alpha_2)xy + \alpha_2\bar{\alpha_2}y^2}{N(I)},$$

jonka diskriminantti on D. Tämä on binäärinen neliömuoto, jonka kertoimet ovat rationaalisia kokonaislukuja. (Tehtävä: laske!). Jos diskriminantti on negatiivinen, tämä on positiivinen definiitti muoto. Sanotaan, että tämä muoto kuuluu ideaalille I. Ideaalin I luokkaa vastaa binäärimuotojen Q_I luokka.

Seuraavaksi todistetaan, että tämä neliömuoto ei riipu ideaalin kannasta.

Lemma 3.42. *Neliömuoto $Q_I := \frac{N(\alpha_1 x + \alpha_2 y)}{N(I)}$ ei riipu ideaalin I kannasta.*

Todistus. Olkoon $\{\beta_1, \beta_2\}$ joku toinen kanta ideaalille I. Kannasta toiseen pääsee matriisin

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

avulla. Ja koska kantoja voi vaihtaa puoleen ja toiseen, on tämä matriisi kääntyvät. Seuraavaksi osoitamme, että $\sigma \in \mathrm{SL}_2(\mathbb{Z})$

Lasketaan kannan determinantti.

$$\det(\beta_1, \beta_2) = \det \begin{pmatrix} \beta_1 & \beta_2 \\ \bar{\beta_1} & \bar{\beta_2} \end{pmatrix} = \beta_1\bar{\beta_2} - \bar{\beta_1}\beta_2 > 0$$

Toisaalta

$$\det(\beta_1, \beta_2) = \det \begin{pmatrix} a\alpha_1 + b\alpha_2 & c\alpha_1 + d\alpha_2 \\ a\bar{\alpha_1} + b\bar{\alpha_2} & c\bar{\alpha_1} + d\bar{\alpha_2} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha_1 & \alpha_2 \\ \bar{\alpha_1} & \bar{\alpha_2} \end{pmatrix} > 0$$

Koska kantojen determinantit ovat molemmat positiivisia ja determinantit ovat riippumattomia kannoista, väistämättä $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$ ja matriisi kuuluu ryhmään $\mathrm{SL}_2(\mathbb{Z})$. Näin ollen $\sigma Q_I(x, y) = Q'_I(x, y)$, eli neliömuoto ei riipu kannasta ideaalille I. □

Voidaan myös osoittaa, että muoto $Q_I(x, y)$ on primitiivinen.

Lemma 3.43. *Jos $I_1 = (\gamma)I_2$, jollekin $\gamma \in O_K$, ja $N(\gamma) > 0$, silloin $Q_1 \equiv Q_2$*

Todistus. Olkoon $\{\alpha, \beta\}$ kanta ideaalille I_2, silloin I_1:llä on kanta $\{\gamma\alpha, \gamma\beta\}$, ja koska normi on multiplikatiivinen $N(I_1) = N(\gamma)N(I_2)$. Näin ollen

$$Q_{I_1}(x, y) = N(\gamma\alpha x + \gamma\beta y)/N(\gamma)N(I_2) = N(\alpha x + \beta y)/N(I_2) = Q_{I_2}(x, y).$$

□

Liitetään nyt binäärimuotoon ideaali.

Mihin tahansa primitiiseen binääriseen neliömuotoon (A, B, C), jonka diskriminantti on D, voidaan liittää ideaali

$$M = \{1, \frac{B - \sqrt{D}}{2A}\}$$

jos $A > 0$. Koska $N(M) = |\frac{B-\sqrt{D}}{2A} - \frac{b+\sqrt{D}}{2A}|/\sqrt{D} = \frac{1}{A}$, niin tähän ideaaliin liittyy muoto

$$\frac{1}{N(M)} N(x + \frac{B - \sqrt{D}}{2A} y) = ax^2 + bxy + cy^2.$$

Ja jos $A < 0$, silloin $D > 0$, ja muoto on epädefiniitti. Tässä tapauksessa liitetään ideaalin

$$M = \sqrt{D}\{1, \frac{B - \sqrt{D}}{2A}\},$$

jonka normi on

$$N(M) = |N(\sqrt{D})|N(\{1, \frac{B-\sqrt{D}}{2A}\}) = \frac{D}{|A|},$$

ja neliömuodoksi saadaan

$$\frac{1}{N(M)}N(\sqrt{D}x+\sqrt{D}\frac{B-\sqrt{D}}{2A}y) = -\frac{D}{N(M)}N(x+\frac{B-\sqrt{D}}{2A}y) = ax^2+bxy+cy^2.$$

Kumpikin kanta on myös järjestetty, sillä

$$\frac{B+\sqrt{D}}{2A} - \frac{B-\sqrt{D}}{2A} = \frac{\sqrt{D}}{A}, A > 0,$$

ja

$$\sqrt{D}\frac{-BD+\sqrt{D}}{2A} - \sqrt{D}\frac{-BD-\sqrt{D}}{2A} = \frac{\sqrt{D}}{A}, A < 0, D > 0.$$

Lopulta osoitetaan, että jos kaksi neliömuotoa ovat ekvivalentit, niin silloin myös niiden tuottamat ideaalit ovat (kapeasti) ekvivalentit.

Oletetaan, että $f_1 = f_2(rx + sy, tx + uy)$, missä $ru + st = 1$. Missä ensimmäiseen neliömuotoon liittyy ideaali M_1 ja toiseen M_2. Oletetaan, että näillä ideaaleilla on järjestetyt kannat $\{\alpha_1, \beta_1\}$ ja $\{\alpha_2, \beta_2\}$. Koska neliömuoto ei riippunut ideaalin kannasta

$$f_{M_1}(rx + sy, tx + uy) = f_{\{r\alpha_1+t\beta_1, s\alpha_1+u\beta_1\}}(x, y).$$

Lisäksi, koska $ru - st = 1$, on $\{r\alpha_1 + t\beta_1, s\alpha_1 + u\beta_1\}$ on myös järjestetty kanta ideaalille M_1. Näin ollen $f_{M_1} = f_{M_1}$.

Nyt

$$f_{M_1}(x, y) = \frac{1}{N(M_1)}N(\alpha_1 x + \beta_1 y) = \frac{N(\alpha_1)}{N(M_1)}(x + \frac{\beta_1}{\alpha_1}y)(x + \frac{\bar{\beta_1}}{\bar{\alpha_1}}y)$$

ja samalla lailla

$$f_{M_2}(x, y) = \frac{N(\alpha_2)}{N(M_2)}(x + \frac{\beta_2}{\alpha_2}y)(x + \frac{\bar{\beta_2}}{\bar{\alpha_2}}y)$$

Nyt muodon $f_{M_1}(x, 1)$ nollat ovat $-\frac{\beta_1}{\alpha_1}$ ja $-\frac{\bar{\beta_1}}{\bar{\alpha_1}}$ ja samoin $f_{M_2}(x, 1)$ nollat ovat $-\frac{\beta_2}{\alpha_2}$ ja $-\frac{\bar{\beta_2}}{\bar{\alpha_2}}$, joten väistämättä joko

$$\frac{\beta_1}{\alpha_1} = \frac{\beta_2}{\alpha_2}$$

tai

$$\frac{\beta_1}{\alpha_1} = \frac{\bar{\beta_2}}{\bar{\alpha_2}}.$$

Näistä jälkimmäinen ei toimi, sillä $\{\alpha_1, \beta_1\}$ ja $\{\alpha_2, \beta_2\}$ olivat kumpikin järjestettyjä kantoja. Joten pannaan $\gamma = \frac{\beta_1}{\alpha_1}$, joten $\beta_1 = \alpha_1\gamma$ ja $\beta_2 = \alpha_2\gamma$, joten kannat ideaaleille ovat

$$M_1 = \{\alpha_1, \beta_1\} = \{\alpha_1, \alpha_1\gamma\} = \alpha_1\{1, \gamma\}$$

ja

$$M_2 = \{\alpha_2, \beta_2\} = \{\alpha_2, \alpha_2\gamma\} = \alpha_2\{1, \gamma\}.$$

Ja näin ollen

$$M_2 = \frac{\alpha_2}{\alpha_1} M_1.$$

Vielä todetaan, että $N(\alpha_1), N(\alpha_2)$ ovat samaa etumerkkiä (ylläolevien yhtälöitten perusteella), joten $N(\frac{\alpha_2}{\alpha_1}) > 0$, kuten pitääkin ja ideaalit ovat kapeasti ekvivalentteja.

4 Zeeta-funktiot ja luokkalukulause

Dedekindin zeeta-funktio on määritelty

$$\zeta_k(s) = \sum_{\mathfrak{a} \lhd O_k} N(\mathfrak{a})^{-s}.$$

Tämän funktion analyyttisten ominaisuuksien perusteella voidaan määritellä luokkaluku. Yleensä ei kuitenkaan käytännössä, vaan pelkästään teoriassa.

Olkoon $[K : \mathbb{Q}] = n = r + 2s$ lukukunta. Määritellään seuraavat invariantit

1. h_K on kunnan K luokkaluku, eli ideaaliluokkien määrä
2. Reg_K on kunnan regulaattori.
3. ω_K on kunnan K sisältämien ykkösen juurten määrä.
4. D_K on diskriminantti.

Lause 4.1. *Dedekindin zeeta-funktio $\zeta_K(s)$ suppenee absoluuttisesti alueella $\Re(s) > 1$ ja se voidaan jatkaa meromorfiseksi funktioksi koko kompleksi tasolla. Sillä on yksi yksinkertainen napa kohdassa $s = 1$, ja residyy tässä navassa on täsmälleen*

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot h_K \cdot \mathrm{Reg}_K}{w_K \cdot \sqrt{|D_K|}}$$