Seuraavana tavoitteena on laskea neliökuntien luokkalukuja ja luokkaryhmiä. Käydään kuitenkin muutama tulos ennen tätä erityisesti yksikäsitteisestä ideaaleihin jaosta.

Ideaaliluokkaryhmä on Abelin ryhmä ja sen kertaluku on aina äärellinen.

Palataan vielä joihinkin tuloksiin, joita tarvitsemme jatkossa, mutta joitten todistaminen tällä kurssilla on liian teknistä ja työlästä.

Lemma 2.47. *Jos A ja B ovat nollasta eroavia ideaaleja kokonaislukujen renkaassa O_K, silloin $N(AB) = N(A)N(B)$.*

Jos $N(I) = p$, missä p on tavallinen alkuluku, silloin I on alkuideaali. Toisin päin tämä ei välttämättä ole totta. Kuitenkin jokaiselle alkuideaalille P on totta, että $N(P) = p^n$.

Vaikka seuraavaa lausettakaan emme ehdi todistaa, käydään seuraavaksi läpi esimerkki, joka osoittaa tekijöihin jaon.

Lause 2.48. *Olkoon K lukukunta, jonka kokonaislukujen rengas on O_K. Mikä tahansa aito ideaali $I \subset O_K$ voidaan kirjoittaa alkuideaalien tulona $I = P_1P_2 \dots P_r$. Tämä tekijöihinjako on yksikäsitteinen lukuunottamatta tekijöiden järjestystä.*

Vielä tarvitsemme Dedekindin lauseen alkuideaalien (p) hajoamisesta laajennuksissa.

Lause 2.49. *Olkoon $K = \mathbb{Q}(\alpha)$, missä $\alpha \in O_K$ ja α:n minimipolynomi on $m(x) \in \mathbb{Z}[x]$, ja sen aste on n. Jos p ei jaa $[O_K : \mathbb{Z}[\alpha]]$ ja $\bar{m}(x) := m(x) \mod p$ hajoaa*

$$\bar{m}(x) = \prod_{i=1}^{r} \bar{g}_i(x)^{e_i}$$

missä kaikki $\bar{g}_i$ ovat erillisiä ja jaottomia, silloin

1. *$P_i = (p, g_i(\alpha))$ on O_K:n alkuideaali.*
2. *Kaikki alkuideaalit P_1 ovat erisuuria.*
3. *Alkuideaalin normi $N(P_i) = p^{f_i}$ missä f_i on $\bar{g}_i$:n aste.*
4. *$(p) = \prod_{i=1}^{r} P_i^{e_i}$.*

Esimerkki 2.50. Olemme jo moneen kertaan nähneet, että renkaassa $\mathbb{Z}[\sqrt{-5}]$ ei ole yksikäsitteistä tekijöihinjakoa, sillä

$$6 = 2 \times 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}).$$

Ideaalien tasolla kirjoitetaan sama

$$(6) = (2)(3) = (1 - \sqrt{-5})(1 + \sqrt{-5}).$$

Olkoon $P_1 = (2, 1 + \sqrt{-5}), P_2 = (2, 1 - \sqrt{-5}), Q_1 = (3, 1 + \sqrt{-5}), Q_2 = (3, 1 - \sqrt{-5})$, missä $(\alpha, \beta) := \{r\alpha + s\beta : r, s \in O_K\}$. Nyt

$$(2) = (4, 6) \subseteq P_1P_2 \subseteq (2, 6) = (2),$$

joten $P_1P_2 = (2)$. Myös $N((2)) = N_{K/\mathbb{Q}}(2) = 4$, joten $N(P_1)N(P_2) = 4$. Lisäksi helppo lasku osoittaa, että $a \equiv b \mod 2$ silloin kun $a + b\sqrt{-5} \in P_i$, kunhan $P_i \neq O_K$. Päättelemme siis, että $N(P_1) = N(P_2) = 2$. Samalla lailla $(3) = (9, 6) \subseteq Q_1Q_2 \subseteq (3, 6) = (3)$, joten $Q_1Q_2) = (3)$ ja $N(Q_1) = N(Q_2) = 3$. Tästä seuraa, että P_1, P_2, Q_1, Q_2 ovat kaikki alkuideaaleja. (Itse asiassa $P_1 = P_2$, esimerkiksi $1 - \sqrt{-5} = 2 \cdot 1 - 1(1 + \sqrt{-5})$).

On myös niin, että $(1 + \sqrt{-5}) \subseteq P_1, Q_1$ ja $(1 - \sqrt{-5}) \subseteq P_2, Q_2$. Normien tarkastelu osoittaa, että $(1 + \sqrt{-5}) = P_1Q_1$ ja $(1 - \sqrt{-5}) = P_2Q_2$. Näin ollen

$(2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$ onkin alkuideaalien tulona $P_1P_2Q_1Q_2 = P_1Q_1P_2Q_2$,

mikä osoittaa, että vaikka hajotelma jaottomiin alkioihin on eri, alkuideaalien tulo on sama.

Koska normeja on yleensä tavattoman hankala laskea ideaaleille, yleensä riittää etsiä niille joku hyvä yläraja.

2.7 Minkowskin raja

Tässä käsittelemme Minkowskin rajaa, ja miten sen avulla voidaan laskea luokkalukuja. Kappaleen tärkein anti on itse tulos, mutta yritän myös hahmotella, mistä raja tulee, sillä se antaa tärkeän esimerkin "lukujen geometriasta". Lukujen geometria on ollut hyödyllinen tapa hahmottaa kokonaislukujen joukkoa, vähän niin kuin teimme Eukleideen alueen todistuksissa.

Määritellään ensin hila, perusalue, ja tilavuus.

Olkoon $\{v_1, v_2, \ldots v_n\}$, mikä tahansa kanta $\mathbb{R}^n$:lle. Tämä kanta virittää hilan $L = \{a_1v_1 + a_2v_2 + \cdots + a_nv_n : a_i \in \mathbb{Z}\}$. Hila on $\mathbb{R}^n$:n additiivinen aliryhmä. Hilan perualue on $D = \{a_1v_1 + a_2v_2 + \cdots + a_nv_n : a_i \in [0, 1)\}$, ja jokainen $v \in \mathbb{R}^n$ voidaan yksikäsitteisesti kirjoittaa muotoon $v = u + w$, jossa $u \in L$ ja $w \in D$.

Oletetaan, että $v_i = \sum_{j=1}^{n} a_{ij}e_j$, jossa $\{e_1, \ldots, e_n\}$ on $\mathbb{R}^n$ standardi kanta, tällöin voimme määritellä perusalueen tilavuuden $Vol(D) := |\det(a_{ij})|$. Huomaa myös, että $Vol((D)^2) = \det(v_i \cdot v_j)$, koska se on matriisin $(a_{ij})(a_{ij})^t$ determinantti.

Tehtävä 1. Todista, että $Vol(D)$ ei riipu $\mathbb{Z}$-kannan valinnasta hilalle L.

Lemma 2.51 (Blichfeldt)**.** *Olkoon L hila $\mathbb{R}^n$:ssä, ja olkoon S rajoitettu ja mitallinen $\mathbb{R}^n$:n osajoukko, jolle pätee $Vol(S) > Vol(L)$. Silloin on olemassa $x, y \in S$, missä $x \neq y$ ja $x - y \in L$.*

Määritelmä 2.52. Kutsumme $S \subseteq \mathbb{R}^n$ kuperaksi, jos

$$x, y \in S, 0 \leq \lambda \leq 1 \Rightarrow \lambda x + (1 - \lambda)y \in S.$$

S on symmetrinen origon suhteen, jos $x \in S \Rightarrow -x \in S$.

Nyt voimme esittää Minkowskin kuperan alueen lauseen.

Lause 2.53. *Olkoon L hila $\mathbb{R}^n$:ssä. Ja S rajoitettu, mitallinen $\mathbb{R}^n$:n osajoukko, joka on sekä kupera että symmetrinen. Jos $Vol(S) > 2^n Vol(L)$, silloin on olemassa $v \in L \setminus \{0\}$, missä $v \in S$.*

Huomaa, että jos S on suljettu, ja näin ollen kompakti, riittää, että $Vol(S) \geq 2^n Vol(L)$.

Esimerkki 2.54. Todistetaan toisella tapaa, että jos $p \equiv 1 \mod 4$, silloin on olemassa $x, y \in \mathbb{Z}$, joille pätee $p = x^2 + y^2$. Tiedämme, että $\left(\frac{-1}{p}\right) = 1$, joten on olemassa s, jolle pätee $s^2 \equiv -1 \mod p$. Jos $p = x^2 + y^2$, silloin $x^2 + y^2 \equiv 0 \mod p$, joten $(x/y)^2 \equiv -1 \mod p$. Näin ollen $x \equiv \pm sy \mod p$. Etsimme siis pientä kokonaislukuratkaisua kongruenssiin $x \equiv sy \mod p$. Tällaiset pisteet muodostavat hilan L avaruudessa $\mathbb{R}^2$. Saamme

$$x \equiv sy \mod p \Leftrightarrow x = sy + pz, z \in \mathbb{Z} \Leftrightarrow (x, y) = y(s, 1) + z(p, 0).$$

Siispä $\{(s, 1), (p, 0)\}$ on kanta hilalle L, ja

$$Vol(L) = \left|\det \begin{pmatrix} s & p \\ 1 & 0 \end{pmatrix}\right| = p.$$

Olkoon C kiekko $x^2 + y^2 < 2p$, jonka säde on $\sqrt{2p}$. Joukko C on selvästikin kupera ja symmetrinen origon suhteen ja sen tilavuus on

$$Vol(C) = \pi(\sqrt{2p})^2 = 2\pi p > 2^2 p = 2^2 Vol(L).$$

Näin ollen Minkowskin lauseen perusteella on olemassa nollasta poikkeava $v \in L$, joka on myös $v \in C$. Oletetaan, että $v = (x, y)$. Koska $v \in L$, saamme $x \equiv sy \mod p$, ja näin ollen $x^2 + y^2 \equiv 0 \mod p$. Toisaalta $v \in C$ tarkoittaa sitä, että $x^2 + y^2 < 2p$, joten $x^2 + y^2 = 0, p$. Koska $v \neq 0$, on pakko olla $x^2 + y^2 = p$.

Sovelletaan nyt näitä algebrallisiin lukukuntiin. Olkoon $[K : \mathbb{Q}] := n = r + 2s$, jossa r on reaaliupotusten $\sigma_i : K \longrightarrow \mathbb{R}$ määrä ja s kompleksikonjugaatti upotusparien määrä $\sigma_j, \bar{\sigma}_j : K \longrightarrow \mathbb{C}$.

Jos $K = \mathbb{Q}(\sqrt{D})$, olemme jo nähneet, että on olemassa joko kaksi reaaliupotusta tai yksi kompleksikonjugaattipari.

Lause 2.55. *Olkoon $I \lhd O_K$ nollasta eroava ideaali. Silloin on olemassa nollasta eroava $\alpha \in I$, jolle pätee*

$$|Norm_{K/\mathbb{Q}}(\alpha)| \leq c_K N(I),$$

missä

$$c_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta^2(K)|}$$

on Minkowskin vakio lukukunnalle K.

Lause 2.56. *Mikä tahansa ideaaliluokka $c \in C_K$ sisältää ideaalin J, jolle pätee $N(J) \leq c_K$, eli*

$$N(J) \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta^2(K)|}.$$

Todistus. Olkoon I mikä tahansa ideaali käänteisideaaliluokassa c^{-1}. Tiedetään, että on olemassa nollasta eroava $\alpha \in I$, jolle $|N_{K/\mathbb{Q}}(\alpha)| \leq c_K N(I)$. Koska $(\alpha) \subseteq I$, väistämättä $I \mid (\alpha)$, joten on olemassa ideaali J, jolle $IJ = (\alpha)$. Suhteet $I \in c^{-1}$ ja $IJ = (\alpha)$ johtavat siihen, että $J \in c$, ja näin ollen $[J] = c$. Edelleen $N(I)N(J) = N(IJ) = |N_{K/\mathbb{Q}}(\alpha)| \leq c_K N(I)$, joten $N(J) \leq c_K$. $\square$

2.8 Luokkaryhmän ja luokkalukujen laskeminen Minkowskin rajan avulla.

Olkoon c mikä tahansa ideaaliluokka. Silloin on olemassa $J \in c$, jolle $N(J) \leq c_K$. Kirjoitetaan J alkuideaalien tulona $J = P_1 \dots P_s$. Koska normi on multiplikatiivinen, $N(P_i) \leq c_K$ jokaiselle i. Tämän lisäksi $c = [J] = [P_1 \dots P_s] = [P_1] \dots [P_s]$. Joten c on ryhmässä, jonka ovat virittäneet alkuideaalit, joiden normi on korkeintaan c_K. Näin ollen, ideaaliluokkaryhmä itse on viritetty alkuideaalien luokilla, joiden normi on korkeintaan c_K.

Tavoitteenamme on siis löytää virittäjät ideaaliluokkaryhmälle. Huomataan, että alkuideaalit, joiden normi on $\leq c_K$ ovat ideaalien (p) tekijöitä, missä $p \in \mathbb{N}$ on alkuluku ja $p \leq c_K$. Dedekindin lauseen perusteella, kaikki tällaiset alkuluvut p, voidaan hajottaa alkuideaaleiksi, jotka sitten antavat

täydellisen virittäjäjoukon ideaaliluokkaryhmälle. Tämä ei kuitenkaan riitä, sillä alkuideaalien välillä voi olla suhteita. Jotkut näistä on helppo löytää alkulukujen alkuideaalihajotelmista, koska nämä ovat aina pääideaaleja. Toiset voidaan löytää hajottamalla pääideaaleja (α), jotka on virittänyt joku $\alpha \in O_K$, jonka normi on pieni.

Osoittaaksemme, että löydetty suhteitten joukko on täydellinen, on syytä todistaa, että sopivat virittäjien yhdistelmät eivät ole pääideaaleja. Yleisesti ottaen, tämä voi olla todella hankalaa, mutta kompleksisille neliökunnilla voidaan todistaa, että ideaali I on ei-pääideaali löytämällä kaikki alkiot $\alpha \in O_K$, joiden $Norm_{K/\mathbb{Q}}(\alpha) = N(I)$, ja tarkistamalla, onko $I = (\alpha)$ vai ei. Jos K on kompleksinen neliökunta, on olemassa vain äärellisen monta vaihtoehtoa sellaisille α:oille, joiten normi on sama kuin I:n normi.

Esimerkki 2.57. Valitaan $K = \mathbb{Q}(\sqrt{-5})$, joten $O_K = \mathbb{Z}[\sqrt{-5}]$. Tiedämme jo, että $h_K > 1$. Nyt todistamme, että $h_K = 2$. Laajennuksen aste on 2, ja kunnasta $\mathbb{Q}(\sqrt{-5})$ on kaksi kompleksikonjugaattiupotusta kuntaan $\mathbb{C}$, joten $s = 1$ ja $r = 0$. Diskriminantti on $\Delta^2(K) = -20$. Näin ollen

$$c_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{20} = \frac{4\sqrt{5}}{\pi} < 3.$$

Joten mikä tahansa ideaaliluokka sisältää ideaalin, jonka normi on korkeintaan 2, ja C_K:n virittävät luokat alkuideaaleja, joitten normi on korkeintaan 2. Nyt $(2) = P_2^2$, missä $P_2 = (2, 1 + \sqrt{-5})$ ja $N(P_2) = 2$. Siis $[P_2]$ virittää C_K:n. Lisäksi $P_2^2 = (2)$, joten $[P_2]^2 = [(2)] = [O_K]$, mikä on C_K:n identiteetti. Näin ollen C_K on syklinen ja sen kertaluku on 2, joten $h_K = 2$.

Esimerkki 2.58. Seuraavaksi katsotaan tapausta $K = \mathbb{Q}(\sqrt{-6})$, missä $O_K = \mathbb{Z}[\sqrt{-6}]$, missä $n = 2, r = 0, s = 1$ ja $\Delta^2(K) = -24$. Minkowskin raja on

$$C_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{24} = \frac{4\sqrt{6}}{\pi} \approx 3,1.$$

Näin ollen ideaaliluokkaryhmän virittävät alkuideaalit P, joille $N(P) \leq c_K$, mikä tarkoittaa sitä, että $N(P) = 2$ tai 3.

Minimipolynomi $x^2 + 6 \equiv x^2 \mod 2$, joten $(2) = P_2^2$, missä $P_2 := (2, \sqrt{-6})$. Samalla lailla $x^2 + 6 \equiv x^2 \mod 3$ joten $(3) = P_3^2$, missä $P_3 := (3, \sqrt{-6})$. Nyt $N(P_2) = 2$ ja $N(P_3) = 3$, kummankin haaroittumisindeksi on 2. Tästä seuraa, että ideaaliluokat $[P_2]$ ja $[P_3]$ virittävät ideaaliluokkaryhmän C_K. Vielä on syytä kuitenkin tarkistaa, onko olemassa mitään suhteita, jotka nämä ideaaliluokat toteuttavat, ja tarkistaa myös kummankin aste.

Jos P_2 on pääideaali, silloin $P_2 = (x + y\sqrt{-6})$, missä $x, y \in \mathbb{Z}$. Kun otetaan normi kummaltakin puolelta, saadaan $2 = |x^2 + 6y^2|$, mikä on täysin

mahdoton yhtälö. Samalla tavalla P_3 ei ole pääideaali. Tämä tarkoittaa, että $[P_2], [P_3] \neq [O_K]$ ryhmässä C_K. Koska kuitenkin $P_2^2 = (2)$ tästä seuraa, että $[P_2]^2 = [O_K]$ ja samoin $[P_3]^2 = [O_K]$.

Seuraavaksi huomataan, että $\sqrt{-6} = \sqrt{-6} \cdot 3 - 2\sqrt{-6} \in P_2P_3$. Koska $N_{K/\mathbb{Q}}(\sqrt{-6}) = 6$, päätellään $(\sqrt{-6}) = P_2P_3$, joten $[P_2][P_3] = [O_K]$ ja näin ollen $[P_3] = [P_2]^{-1} = [P_2]$ ja lopulta C_K on syklinen, ja sen kertaluku on 2, virittäjänään $[P_2]$.

Esimerkki 2.59. Etsitään kaikki kokonaislukuratkaisut yhtälöön $y^2 + 54 = x^3$. Tämä on elliptinen käyrä.

Aloitetaan parillinen/pariton tarkastelulla. Olkoon $x, y \in \mathbb{Z}$ ratkaisu. Jos y on parillinen, silloin $x^3 \equiv 54 \equiv 2 \mod 4$, mikä on mahdonta. Jos $3 \mid y$, silloin $3 \mid x$, jos asetetaan $x = 3x_1$ ja $y = 3y_1$, saadaan $y_1^2 + 6 = 3x_1^2$. Joten $3 \mid y_1$, ja kun kirjoitetaan $y_1 = 3y_2$, saadaan $3y_2^2 + 2 = x_1^3$. Mutta $3y_2^2 + 2 \equiv 2 \text{ or } 5 \mod 9$, mistä seuraa, että $x_1^3 \equiv 0, 1 \text{ or } 8 \mod 9$. Tämä on lopulta ristiriita, joten $(y, 3) = 1$.

Tästä seuraa ensin, että $(y, 6) = 1$ ja myös $(x, 6) = 1$.

Hajotetaan yhtälö nyt ideaaleihin

$$(y + 3\sqrt{-6})(y - 3\sqrt{-6}) = (x)^3.$$

Osoitetaan seuraavaksi, että vasemman puolen tekijät ovat suhteellisia alkulukuja.

Jos on olemassa alkuideaali P joka jakaa kummankin tekijän, jakaa se myös niiden erotuksen $(y+3\sqrt{-6}) - (y-3\sqrt{-6}) = 6\sqrt{-6}$, joten $6\sqrt{-6} \in P$. Koska $\sqrt{-6} = P_2P_3$, jakaa $P \mid P_2^3P_3^3$, joten P voi olla ainoastaan alkuideaali P_2 tai P_3. Kuitenkin $P \mid (y + 3\sqrt{-6})$ tarkoittaa sitä, että $P \mid (x)^3$ ja kun tarkastelemme normeja $N(P) \mid x^6$, mikä on mahdotonta, sillä $(x, 6) = 1$. Siispä $(y + 3\sqrt{-6})$ ja $(y - 3\sqrt{-6})$ ovat suhteellisia alkuideaaleja renkaassa O_K. Koska ideaaleilla on yksikäsitteinen tekijöihinjako, väistämättä

$$(y + 3\sqrt{-6}) = I^3$$

jollekin ideaalille I. Koska I^3 on pääideaalia, $[I]^3 = [O_K]$, eli identiteettialkio C_K:ssa. Toisaalta tiedetään, että $h_K = 2$, joten $[I] = [O_K]$. Näin ollen I on pääideaali ja $I = (\alpha)$, jollekin $\alpha \in O_K$.

Tästä seuraa, että $(y + 3\sqrt{-6}) = (\alpha)^3$, joten $y + 3\sqrt{-6} = u\alpha^3$, missä u on yksikkö. Toisaalta ainoat yksiköt renkaassa $O_K = \mathbb{Z}[\sqrt{-6}]$ ovat $u = \pm 1$ ja kumpikin näistä on jo kolmansia potensseja, joten

$$y + 3\sqrt{-6} = (u\alpha)^3 = [a + b\sqrt{-6}]^3.$$

Nyt kun kerrotaan oikea puoli yhtälöstä auki, ja verrataan kertoimia kummallakin puolella, saadaan $\sqrt{-6}$:n kerrointen perusteella yhtälö $3 = b(3a^2 - 6b^2)$,

misät seuraa, että $1 = b(a^2 - 2b^2)$ Joten $b = -1$ ja $a^2 = 1$ antaa $y = a^3 - 18b^2a = a(a^2 - 18b^2) = \pm 17$. Kun $y = \pm 17$ ainoa mahdollinen $x = 7$, joten lopullinen ratkaisu on $x = 7, y = \pm 17$.

2.9 Imaginääriset neliökunnat

Imaginääriset neliökunnat ovat niitä, joissa kunnan diskriminantti on negatiivinen luku. Itseasiassa, tässä tapauksessa kaikki sellaiset kunnat, joiden luokkaluku on $h_K = 1$ ja $K = \mathbb{Q}(\sqrt{d})$ ovat

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Jos $d \in \{-19, -43, -67, -163\}$ kokonaislukujen rengas O_K ei ole Eukleideen alue.

2.10 Reaaliset neliökunnat

Yleisesti ottaen uskotaan, että renkaassa O_K on yksikäsitteinen tekijöihinjako äärettömän monelle reaaliselle neliökunnalle. Tämä on kuitenkin toistaiseksi avoin ongelma algebrallisessa lukuteoriassa.