Yleisesti jos $K = \mathbb{Q}(\theta)$ ja θ:n minimipolynomi on $x^n + c_{n-1}x^{n-1} + \cdots + c_0$, silloin $Tr_{K/\mathbb{Q}}(\theta) = -c_{n-1}$ ja $N_{K/\mathbb{Q}}(\theta) = (-1)^n c_0$. Erityisesti tästä huomataan, että koska minimipolynomin kertoimet ovat $\mathbb{Q}$:ssa, myös jälki ja normi ovat $\mathbb{Q}$:n alkioita.

Lemma 2.19. *Jos $\alpha \in O_K$, silloin $Tr(\alpha), Norm(\alpha) \in \mathbb{Z}$.*

Todistus. Olkoon $\alpha \in O_K$, ja m sen minimipolynomi. Minimipolynomi hajoaa jossain kunnassa L lineaarisiksi tekijöiksi. Olkoot $\alpha_1, \ldots, \alpha_n$ sen juuret. Nämä ovat myös α:n K-konjugaatit ja ne kuuluvat renkaaseen O_L. (Juuret kuuluvat L:ään ja jokainen lineaarinen tekijä $(x - \alpha_i)$ on kokonaislukukertoiminen, näin ollen $\alpha_i \in O_L$. Koska kokonaisluvut muodostavat renkaan, myös $Tr_{K/\mathbb{Q}}(\alpha) = \alpha_1 + \cdots + \alpha_n \in O_L$ ja $N_{K/\mathbb{Q}}(\alpha) = \alpha_1 \ldots \alpha_n \in O_L$. Toisaalta juuri todettiin, että $Tr_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$, näin ollen $Tr(\alpha), N(\alpha) \in \mathbb{Q} \cap O_L = \mathbb{Z}$. □

Määritelmä 2.20. $\alpha \in O_K$ on yksikkö, jos ja vain jos $\alpha^{-1} \in O_K$.

Propositio 2.21. *$\alpha \in O_K$ on yksikkö, jos ja vain jos $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Todistus. Olkoon α yksikkö. Silloin

$$N(\alpha)N(\alpha)^{-1} = N(\alpha\alpha^{-1}) = N(\alpha) = 1.$$

Ylläolevan nojalla $N(\alpha), N(\alpha)^{-1} \in Z$, joten molemmat ovat ± 1.

Toisaalta, oletetaan, että $N(\alpha) = \pm 1$. Olkoot $\alpha_1, \ldots, \alpha_n$ K-konjugaatit alkiolle $\alpha = \alpha_1$. Nyt $\alpha(\alpha_2 \ldots \alpha_n) = \pm 1$. Näin ollen $\alpha^{-1} = \pm(\alpha_2 \ldots \alpha_n)$, joka on renkaassa O_L. Toisaalta tiedämme, että $\alpha^{-1} \in K$, joten $\alpha^{-1} \in O_L \cap K = O_K$. □

Vielä diskriminantista ja kannoista pari asiaa. Näitä tarvitaan, jotta pystymme määrittelemään kunnan diskriminantin.

Lemma 2.22. *$\Delta^2(w) = \det(Tr_{K/\mathbb{Q}}(w_i w_j))$, joten $\Delta^2(w) \in \mathbb{Q}$.*

Todistus. Merkitään $A = (\sigma_i(w_j))$. Silloin

$$\begin{aligned}\Delta^2(w) &= \det(AA^T) = \det(\sum_k \sigma_k(w_i)\sigma_k(w_j)) \\ &= \det(\sum_k \sigma_k(w_i w_j)) = \det(Tr_{K/\mathbb{Q}}(w_i w_j)).\end{aligned}$$

□

Korollaari 2.23. *Jos $v = \{v_1, \ldots, v_n\} \subseteq O_K$ silloin $\Delta^2(v) \in \mathbb{Z}$.*

Lemma 2.24. *Jos $v = \{v_1, \ldots, v_n\}$ ja $w = \{w_1, \ldots, w_n\}$ ovat kaksi kantaa kunnalle $K/\mathbb{Q}$, ja $v_i = \sum_j c_{ij} w_j$, missä $c_{ij} \in \mathbb{Q}$, silloin $\Delta(v) = \det(C)\Delta(w)$, missä $C = (c_{ij})$.*

2.5 Ideaalit, jakoideaalit, ideaaliluokkaryhmä, luokkaluku

Tarkastellaan nyt kokonaislukujen rengasta uudelta kantilta.

Lause 2.25. *Lukukunnan K kokonaislukujen renkaalla O_K on kokonaislukukanta. Eli on olemassa $w_1, \ldots, w_n \in O_K$ joille pätee $O_K = \{\sum_j c_j w_j : c_j \in \mathbb{Z}\}$.*

Todistuksen saatte käydä itse läpi keskiviikon tunnilla olemisen sijaan. Huomaa, että kanta ei ole yksikäsitteinen. Yksikäsitteisyys menetetään siinä, että skalaarit muodostavat renkaan eivätkä kuntaa.

Esimerkki 2.26. $K = \mathbb{Q}(\sqrt{D})$, silloin O_K:lla on kokonaislukukanta

$$\begin{cases} \{1, \sqrt{D}\} & , D \equiv 2, 3 \mod 4 \\ \{1, \frac{1+\sqrt{D}}{2}\} & , D \equiv 1 \mod 4. \end{cases}$$

Seuraavaksi määrittelemme kunnan diskriminantin.

Olkoot $v = \{v_1, \ldots, v_n\}$ ja $w = \{w_1, \ldots, w_n\}$ ovat kaksi $\mathbb{Q}$-kantaa lukukunnalle K. Tarkastellaan $\mathbb{Z}$-alimoduleita $M = \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}}$ ja $M = \langle w_1, \ldots, w_n \rangle_{\mathbb{Z}}$. Oletetaan, että $v, w \subset O_K$, silloin $\Delta^2(v), \Delta^2(w) \in \mathbb{Z}$, koska $\Delta^2(v) = \det(Tr_{K/\mathbb{Q}}(v_i v_j)$. Oletetaan, että $N \subseteq M$. Silloin on olemassa $c_{ij} \in \mathbb{Z}$, joille $v_i = \sum_j c_{ij} w_j$. Merkitään $C = (c_{ij})$. Silloin

$$|\det(C)| = [M : N] = m,$$

additiivisina Abelin ryhminä. Joten Lemman nojalla

$$\Delta^2(w) = (\det(C))^2 \Delta^2(v) = m^2 \Delta^2(v).$$

Jos $M = N$, tästä seuraa, että $\det(C) = \pm 1$ ja $\Delta^2(w) = \Delta^2(v)$.

Diskriminantti ei siis riipu $\mathbb{Z}$-modulin kannasta.

Määritelmä 2.27. Olkoon $M = \langle w_1, \ldots, w_n \rangle$ joku $\mathbb{Z}$-moduli. Olkoon $\Delta^2(M) = \Delta^2(w)$ mille tahansa M:n kannalle w. Kunnan diskriminantti $\Delta^2(K)$ olemaan $\Delta^2(O_K)$.

Lemma 2.28. *Olkoon O_K lukukunnan K kokonaisluvut, ja $\alpha \in O_K$. Jos $N_{K/\mathbb{Q}}(\alpha)$ on alkuluku $\mathbb{Z}$:ssa, silloin α on jaoton alkio renkaassa O_K.*

Todistus. Olkoon $\alpha = \gamma\delta$. Silloin $N(\alpha) = p = N(\gamma)N(\delta)$ jollekin alkuluvulle p. Tästä seuraa, että joko $N(\gamma)$ tai $N(\delta) = 1$, joten toinen niistä on yksikkö. □

Huomaa, että jaottoman alkion normi ei aina ole alkuluku! Esimerkiksi renkaassa $\mathbb{Z}[\sqrt{-5}]$ alkio $1+\sqrt{-5}$ on jaoton, mutta sen normi on $1^2+5\times 1^2 = 6$.

Lause 2.29. *Jos p on alkuluku, ja $p \equiv 1 \mod 4$, silloin on olemassa $a, b \in \mathbb{Z}$, joille $p = a^2 + b^2$. Kaiken lisäksi tämä hajotelma on yksikäsitteinen.*

Yllä oleva lause on todistettu syksyn 2009 lukuteorian kurssilla. Todistetaan nyt vastaava lause toisen kokonaislukujen renkaan avulla. Valitaan $K = \mathbb{Q}(\sqrt{-2})$, joten $O_K = \mathbb{Z}[\sqrt{-2}]$. Tehtäväpaperissa todistettiin, että $\mathbb{Z}[\sqrt{2}]$ on Eukleideen alue, samalla tavalla voidaan todistaa, että $\mathbb{Z}[\sqrt{-2}]$ on Eukleideen alue. Näin ollen sillä on yksikäsitteinen tekijöihinjako. Normi on $N_{K/\mathbb{Q}}(a + b\sqrt{-2}) = a^2 + 2b^2$, joten ainoat yksiköt ovat ± 1.

Lause 2.30. *Yhtälön $y^2 + 2 = x^3$ kokonaislukuratkaisut ovat $x = 3, y = \pm 5$.*

Todistus. Aloitetaan parillinen/pariton tarkastelulla. Jos y on parillinen, silloin x on myös parillinen, mistä seuraa, että $8 \mid x^3 = y^2 + 2$. Mutta koska $4 \mid y^2$, on mahdotonta, että $8 \mid y^2 + 2$. Joten y on pariton.

Yhtälö voidaan hajottaa $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$. Oletetaan, että on olemassa jaoton alkio α joka jakaa sekä $y + \sqrt{-2}$ että $y - \sqrt{-2}$:n. Silloin α jakaa näiden erotuksen $2\sqrt{-2} = -(\sqrt{-2})^3$. Toisaalta, $\sqrt{-2}$ on itse jaoton alkio, sillä sen normi on alkuku 2. Joten $\alpha = \pm\sqrt{-2}$. Nyt

$$\alpha \mid y + \sqrt{-2} \Rightarrow \sqrt{-2} \mid y \Rightarrow 2 \mid y^2,$$

mikä on ristiriita, sillä alussa pääteltiin y:n olevan pariton. Näin ollen oletus siitä, että $y+\sqrt{-2}$:llä ja $y-\sqrt{-2}$:llä olisi yhteinen jaoton tekijä, ei ole totta. Yksikäsitteinen tekijöihinjako tarkoittaa, että sekä $y + \sqrt{-2}$ että $y - \sqrt{-2}$ ovat kuutioita, tai ainakin yksikköä vaille kuutioita. Koska ainoat yksiköt ovat ± 1, ja ne ovat kuutioita, ovat $y \pm \sqrt{-2}$ kumpikin kuutioita. Näin ollen

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3,$$

joten

$$a^3 + 3a^2b\sqrt{-2} + 3ab^2(-2) + b^3(-2)\sqrt{-2} = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2},$$

ja näin ollen $b(3a^2 - 2b^2) = 1$, jonka ainoat ratkaisut ovat $b = \pm 1$ ja $a = \pm 1$, mistä seuraa, että

$$y = a^3 - 6ab^2 = a(a^2 - 6b^2) = \pm 5 \text{ ja } x = 3.$$

□

Lause 2.31. *Olkoon K lukukunta, jonka kokonaislukujen rengas on O_K. Mikä tahansa aito ideaali $I \subset O_K$ voidaan kirjoittaa alkuideaalien tulona $I = P_1 P_2 \dots P_r$. Tämä tekijöihinjako on yksikäsitteinen lukuunottamatta tekijöiden järjestystä.*

Jos $u \in O_K$ on yksikkö, silloin $(u) = O_K$, ja näin ollen $(u)I = I$ mille tahansa ideaalille $I \lhd R$. Näin ollen tekijöihinjaossa ideaalit nielaisevat yksiköitä, eikä tarvitse puhua yksiköitä vaille määritellystä tekijöihinjaosta jos ajatellaan sitä ideaalien avulla.

Jos O_K on pääideaalialue, silloin ylläoleva ideaalien tekijöihinjako suoraan antaa alkioille yksikäsitteisen tekijöihinjaon. Mutta yleisesti ottaen, O_K ei välttämättä ole pääideaali. Seuraavaksi tarkastellaan tätä tapausta.

Määritelmä 2.32. Jos I ja J ovat nollasta eroavia ideaaleja O_K:ssa, kirjoitamme $I \sim J$ (ja sanomme, että I on ekvivalentti J:n kanssa), jos on olemassa sellaiset $\alpha, \beta \in O_K$, joille pätee $I(\alpha) = J(\beta)$.

Lemma 2.33. *Relaatio $\sim$ on ekvivalenssirelaatio nollasta eroavien O_K:n ideaalien joukossa.*

Todistus. Harjoitustehtävä IV/4. □

Määritelmä 2.34. Relaation $\sim$ tuottamia ekvivalenssiluokkia joukossa O_K, kutsutaan ideaaliluokiksi. Merkitään ideaaliluokkien joukkoa C_K:lla. Ideaaliluokkien mahtavuus $h_K = |C_K|$ on kunnan K luokkaluku.

Propositio 2.35. *Luokkaluku $h_K = 1$ jos ja vain jos O_K on pääideaalialue.*

Todistus. Olkoon O_K pääideaalialue. Silloin mille tahansa nollasta eroavalle $I \lhd O_K$, on olemassa $\alpha \in O_K$, jolle $I = (\alpha)$. Silloin $I(1) = O_K(\alpha)$, joten $I \sim O_K$, ja ideaaliluokkia on vain yksi.

Toiseen suuntaan, oletetaan $h_K = 1$. Tämä tarkoittaa, että jokaiselle $I \lhd O_K$ on olemassa $\alpha, \beta \in O_K$, joille

$$I(\alpha) = O_K(\beta).$$

Yhtälön oikea puoli antaa (β):n. Koska $\beta \in (\beta)$, nähdään, että $\beta = a\alpha$, jollekin $a \in I$. Näin ollen $\beta/\alpha \in I \lhd O_K$. Väite: $I = (\alpha/\beta)$. Ilman muuta $(\beta/\alpha) \subseteq I$. Toisaalta, myös $I \subseteq (\beta/\alpha)$, joten I on pääideaali. □

Lemma 2.36. *Olkoon $I \subset O_K$ nollasta eroava ideaali. Silloin $I \cap \mathbb{Z} \neq \{0\}$.*

Todistus. Valitaan mikä tahansa nollasta eroava $\alpha \in I$. Oletetaan, että $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0$, missä $a_0 \neq 0$. Silloin $a_0 = -\alpha(a_1 + \cdots + \alpha^{d-1}) \in I \cap \mathbb{Z}$. □

Lemma 2.37. *O_K/I on äärellinen rengas.*

Todistus. Valitaan mikä tahansa nollasta eroava $a \in I \cap \mathbb{Z}$. Silloin $(a) \subseteq I \subseteq O_K$. Kuvaus $O_K/(a) \longrightarrow O_K/I$ joka kuvaa $\alpha + (a) \mapsto \alpha + I$ on hyvinmääritelty surjektio. On siis tarpeeksi, jos osoitetaan, että $O_K/(a)$ on äärellinen. Olkoon $w = \{w_1, \ldots, w_n\}$ kokonaislukukanta renkaalle O_K. Silloin $O_K/(a)$ on isomorfinen $\mathbb{Z}/(a)^n$ kanssa, missä $n = [K : \mathbb{Q}]$. Joten $|O_K/(a)| = a^n < \infty$. □

Määritelmä 2.38. Ideaalin I normi on $N(I) = |O_K/I|$.

Huomautus 2.39. Ideaalien normi on multiplikatiivinen, mutta tämän todistus siirretään myöhempään ajankohtaan.

Erityisesti pääideaalien normit on helppo laskea.

Lemma 2.40. *Jos $I = (\alpha)$, silloin $N(I) = |N_{K/\mathbb{Q}}(\alpha)|$*

Todistus. Olkoon $w = \{w_1, \ldots, w_n\}$ kokonaislukukanta renkaalle O_K. Silloin $\alpha w = \{\alpha w_1, \ldots, \alpha w_n\}$ on $\mathbb{Z}$-kanta ideaalille $I = (\alpha)$. Tämän kannan determinantti on $\Delta(\alpha w) = \prod_{i=1}^{n} \sigma_i(\alpha)\Delta(w) = N_{K/\mathbb{Q}}(\alpha)\Delta(w)$. Tosin I on O_K:n additiivinen aliryhmä, jonka indeksi on määritelmän mukaan $N(I)$. Joten jos αw_i voidaan ilmaista w:n avulla tapaan $\alpha w_i = \sum c_{ij} w_j$, missä $c_{ij} \in \mathbb{Z}$, sitten $N(I) = |\det(c_{ij})|$. Toisaalta Lemman perusteella $\Delta(\alpha w) = \det(c_{ij})\Delta(w)$, joten $|\Delta(\alpha w)/\Delta(w)| = |N_{K/\mathbb{Q}}(\alpha)| = N(I)$. □

Lause 2.41. *Luokkaluku h_K on aina äärellinen lukukunnalle K.*

2.6 Ideaaliluokat muodostavat ryhmän

Lemma 2.42. *Olkoot $I, J \subseteq O_K$ nollasta eroavia ideaaleja ja $JI = I$, silloin $J = O_K$. (O_K toimii eräänlaisena identiteettialkiona ideaalien ekvivalenssiluokkien joukossa).*

Todistus. Olkoon $\{\alpha_1, \ldots, \alpha_n\}$ ideaalin I kokonaislukukanta. Koska $I = JI$ on olemassa $b_{ij} \in J$, joille $\alpha_i = \sum b_{ij}\alpha_j$, joten $\det(b_{ij} - \delta_{ij}) = 0$. Jos kerrotaan determinantti auki, kaikki termit lukuunottamatta identiteettimatriisin ykkösiä kuuluvat J:hin. Koska $0 \in J$, lopulta myös determinanttiyhtälön perusteella $1 \in J$ ja näin ollen $J = (1) = O_K$. □

Lemma 2.43. *Jos $\{0\} \neq I \lhd O_K$ ja $w \in K$ on sellainen, jolla $wI \subseteq I$, silloin $w \in O_K$.*

Todistus. Lemma 2.12 todistaa tämän suoraan, kun valitaan $M = I$. □

Lemma 2.44. *Jos* $\{0\} \neq I, J \lhd O_K$ *ja* $w \in O_K$ *on sellainen, että* $(w)I = JI$, *silloin* $(w) = J$.

Todistus. Valitaan mielivaltainen $\beta \in J$. Nyt $(\beta)I \subseteq (w)I$, joten $(\beta/w)I \subseteq I$. Edellisen lemman perusteella $(\beta/w) \in O_K$, joten $\beta \in (w)$. Koska β oli mielivaltainen $J \subseteq (w)$, joten $w^{-1}J \lhd O_K$. Nyt $I = (w^{-1}J)I$, joten kahden lemman takaa saadaan $w^{-1}J = O_K$, siispä $J = (w)$. □

Propositio 2.45. *Kaikille* $\{0\} \neq I \lhd O_K$, *on olemassa* k *joka on* $1 \leq k \leq h_K$ *ja* I^k *on pääideaali.*

Todistus. Tarkastellaan $h_K + 1$ ideaalin joukkoa $\{I^i : 1 \leq i \leq h_K + 1\}$. Luokkaluvun määritelmän mukaan jotkut kaksi näistä ovat ekvivalentteja. On siis olemassa $\alpha, \beta \in O_K$, joille $(\alpha)I^i = (\beta)I^j$, ja joten $I^i \sim I^j$, missä $i < j$. Olkoon $k = j - i$, ja $J = I^k$. Silloin $(\alpha)I^i = (\beta)I^iJ \subseteq \beta I^i$. Joten $(\alpha/\beta)I^i \subseteq I^k$. Tämä tarkoittaa, että $\alpha/\beta \in O_K$, ja $(\alpha/\beta)I^i = JI^i$, joten $(\alpha/\beta) = J$ ja näin ollen $J = I^k$ on pääideaali. □

Propositio 2.46. *Ideaaliluokat* C_K *muodostavat ryhmän. Sen nimi on luokkaryhmä, ja sen koko on luokkaluku* h_K.

Todistus. Kahden ideaaliluokan tulo määritellään $[I] \cdot [J] := [IJ]$. Tämä on hyvin määritelty. Ideaaliluokka $[O_K]$ toimii identiteettialkiona, ja assosiatiivisuus on myös helppo tarkistaa. Lopuksi riittää tarkistaa käänteisalkioitten olemassaolo. Olkoon $[I]$ ideaalin I luokka, ja $[O_K] = [(1)]$ identiteettialkio. Edellisen lemman nojalla $[I] \in C_K$. Jos I^k on pääideaali, silloin $[I^{k-1}]$ on ideaaliluokan $[I]$ käänteisalkio. □