2 Kuntalaajennukset

Kerrataan kuntalaajennusten teoriaa.

Määritelmä 2.1. Olkoon L kunta, ja K sen osajoukko. Silloin K on L:n alikunta, jos $K \neq \varnothing$ ja se on suljettu kertolaskun, yhteenlaskun ja käänteisalkioitten ottamisen suhteen. Jos kunta L sisältää tällaisen alikunnan K, kutsumme L:ää kunnan K laajennukseksi, ja merkitsemme tätä $K \leq L$.

Määritelmä 2.2. Olkoon $K \leq L$ kuntalaajennus, ja olkoon $\alpha \in L$. Kutsumme alkiota α algebralliseksi kunnan K yli, jos on olemassa sellainen nollasta poikkeava $f \in K[x]$, jolle $f(\alpha) = 0$ kunnassa L. Jos tämä kirjoitetaan auki, on olemassa $a_0, \ldots, a_n \in K$, jolle pätee $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$.

Olkoon α nyt algebrallinen kunnan K ylitse. Tarkastellaan polynomien joukkoa $J = \{f \in K[x] : f(\alpha) = 0\}$. Tämä on ideaali, ja koska kaikki $K[x]$:n ideaalit ovat pääideaaleja $J = (m)$, missä m on jaoton pääpolynomi, jonka aste on suurempi kuin 1.

Voidaan luoda kuvaus $\theta : K[x] \longrightarrow L$, jossa $g \mapsto g(\alpha)$. Tämä kuvaus θ on rengashomomorfismi, ja sen ydin on $\ker\theta = J = (m)$. Ensimmäisen isomorfialauseen nojalla, $K[x]/(m)$ ja $Im\theta$ ovat kuntia. Kunta

$$K[x]/(m) = \{g+(m) : g = 0, \text{ tai } deg f < deg\, g\} = \{b_0+b_1x+b_{n-1}x^{n-1}+(m)\},$$

missä $n = deg\ m$.

Tästä seuraa, että $Im\ \theta = \{b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}\}$

Kootaan ylläoleva yhteen:

Lause 2.3. *Olkoon $K \leq L$ kuntalaajennus, ja $\alpha \in L$ algebrallinen K:n yli, ja kutsutaan α:n minimipolynomia m:llä. Silloin $K(\alpha) = \{b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} : b_i \in K\}$, jossa $n = deg\ m$, on kunta. Lisäksi $K(\alpha) \geq K$, $\alpha \in K(\alpha)$ ja $K(\alpha)$ on pienin sellainen L:n alikunta, joka sisältää K:n ja α:n.*

Esimerkki 2.4.

1. $\mathbb{R}(i) = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{C}$. Edellisessä merkintätavassa $(K = \mathbb{R}, L = \mathbb{C}, \alpha = i)$. Tälle pätee $i^2 + 1 = 0$, joten $x^2 + 1$ on minimipolynomi.

2. $K = \mathbb{Q}$, $L = \mathbb{R}$, $\alpha = \sqrt{2}$, minimipolynomi on $x^2 - 2$, sen aste on 2, joten $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

3. $K = \mathbb{Q}, L = \mathbb{R}, \alpha = 2^{1/4}$. Minimipolynomi on $x^4 - 2$, tämä on jaoton, joten $\mathbb{Q}(2^{1/4}) = \{b_0 + b_1 2^{1/4} + b_2 2^{1/2} + b_3 2^{3/4} : b_i \in \mathbb{Q}\}$. Tehtävä: laske kunkin $\mathbb{Q}(2^{1/4})$ nollasta eroavan alkion multiplikatiivinen käänteisalkio.

Kuntalaajennuksia voidaan ajatella myös vektoriavaruuksina, ja näin ollen niille voidaan antaa kanta. Tarkemmin sanoen, olkoon $K \leq L$ kuntalaajennus. Kunnan L alkioita voidaan tarkastella vektoreina, ja kunnan K alkioita skalaareina. Määritellään skalaaritulo $a \in K, \beta \in L$ olemaan $a\beta := a\beta$, jossa jälkimmäinen kertolasku tapahtuu kunnassa L. Näin L on vektoriavaruus kunnan K yli.

Määritelmä 2.5. Laajennuksen *aste*, jota merkitään $[L : K]$, on L:n dimensio vektoriavaruutena kunnan K yli, jos tämä on äärellinen. Muuten määritellään asteeksi ääretön.

Tarkastellaan kuntaa $K(\alpha)$ kunnan K yli, missä α on algebrallinen K:n yli. Kuten jo aiemmin totesimme $K(\alpha) = \{b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} : b_i \in K\}$, jossa $n = deg\ m$. Tässä $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ on virittäjäjoukko avaruudelle $K(\alpha)$, kunnan K yli. Koska m on minimipolynomi, on tämä joukko myös lineaarisesti riippumaton, joten se on kanta. Näin ollen

$$[K(\alpha) : K] = deg\ m,$$

missä m on α:n minimipolynomi kunnan K yli.

Määritelmä 2.6. *Lukukunta* K on rationaalilukujen $\mathbb{Q}$ äärellinen laajennus. Lukukunnan asteeksi kutsutaan indeksiä $[K : \mathbb{Q}]$.

Lause 2.7. *Jos K on lukukunta, on se muotoa $K = \mathbb{Q}(\theta)$, jollekin algebralliselle luvulle $\theta \in K$.*

Todistus. Koska K on lukukunta, on $[K : \mathbb{Q}] = n$, jollekin n. Valitaan $\alpha \in K$, ja tarkastellaan alkioita $1, \alpha, \ldots, \alpha^n \in K$. Nämä ovat $n + 1$ alkiota vektoriavaruudessa K, jonka dimensio on n, joten väistämättä ne ovat lineaarisesti riippuvia $\mathbb{Q}$:n yli. Joten on olemassa sellaiset $a_0, \ldots, a_n \in \mathbb{Q}$, jotka kaikki eivät ole identtisesti nollia siten, että $a_0 1 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Tämän vuoksi α on algebrallinen luku kunnan $\mathbb{Q}$ yli. Näin on todistettu, että K on algebrallinen laajennus. Vielä ei ole todistettu, että yksi ainoa alkio θ virittää tämän laajennuksen.

Väite Jos α, β ovat algebrallisia lukuja kunnassa K, silloin on olemassa algebrallinen luku θ, jolle $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$.

Olkoon f, g alkioitten α, β minimipolynomit. Halutaan osoittaa, että voidaan löytää $\lambda \in \mathbb{Q}$, jolle pätee $\theta = \alpha + \lambda\beta$ ja $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$. Selvästikin $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha, \beta)$.

Määritellään $\phi(x) = f(\theta - \lambda x) \in \mathbb{Q}(\theta)[x]$. Nyt $\phi(\beta) = f(\theta - \lambda\beta) = f(\alpha) = 0$, joten β on ϕ:n juuri. Valitaan λ siten, että β on ainoa ϕ:n ja g:n yhteinen juuri. Tämä voidaan tehdä, sillä ainoastaan äärellinen määrä λ:ja ei kelpaa.

Joten $syt(\phi(x), g(x)) = c(x - \beta)$, missä $c \in \mathbb{C}^*$. Nyt $c(x - \beta) \in \mathbb{Q}(\theta)[x]$, mikä tarkoittaa $c, c\beta \in \mathbb{Q}(\theta)$ ja $\beta \in \mathbb{Q}(\theta)$. Koska $\theta = \alpha + \lambda\beta \in \mathbb{Q}(\theta)$, tästä seuraa, että $\alpha \in \mathbb{Q}(\theta)$, joten $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\theta)$, joten $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$.

Lopputulos seuraa tästä induktiolla. Se on suhteellisen pitkä, joten luotan siihen, että ylläoleva ajatus riittää. □

2.1 Kokonaisluvut

Määritelmä 2.8. Algebrallinen luku α on *algebrallinen kokonaisluku* kunnassa $\mathbb{Q}(\alpha)$, jos α:n minimipolynomin kertoimet ovat kaikki renkaassa $\mathbb{Z}$. Merkitään näitä kokonaislukuja O_k.

Propositio 2.9. *Olkoon K algebrallinen lukukunta. Jos $\alpha, \beta \in O_k$ silloin $\alpha + \beta, \alpha\beta \in O_k$.*

Ennen kuin voimme todistaa tämän lauseen, pitää meidän määritellä modulit. Modulit ovat algebrallisessa mielessä jossain määrin vektoriavaruuksien kanssa analogisia. Tässä vain skalaareina ei ole kunta vaan joku kokonaisalue.

Määritelmä 2.10. Olkoon R kokonaisalue. R-moduli M on Abelin ryhmä, jossa on kuvaus $R \times M \longrightarrow M$ joka kuvaa $(r, m) \mapsto rm$ ja toteuttaa seuraavat ehdot:

1. $(r_1 + r_2)m = r_1m + r_2m$
2. $(r_1r_2)m = r_1(r_2m)$
3. $r(m_1 + m_2) = rm_1 + rm_2$
4. $1m = m$

kaikille $r, r_1, r_2 \in R$ ja $m, m_1, m_2 \in M$.

Esimerkki 2.11. Jos R on kunta ja M on vektoriavaruus R:n yli, silloin M on R-moduli. Jos $R = \mathbb{Z}$ ja M on mikä tahansa additiivinen Abelin ryhmä, silloin M on $\mathbb{Z}$-moduli.

Sanomme, että M on äärellisesti viritetty, jos on olemassa $m_1, \ldots, m_k \in M$ joille pätee

$$M = \{r_1m_1 + \cdots + m_kr_k : r_i \in R\}.$$

Todistetaan lemma ennen itse proposition todistusta.

Lemma 2.12. *Luku $\alpha \in K$ on algebrallinen kokonaisluku, jos ja vain jos on olemassa nollasta eroava äärellisesti viritetty $\mathbb{Z}$-moduli $M \subseteq K$, jolle $\alpha M \subseteq M$.*

Todistus. Olkoon $\alpha \in O_K$, ja se toteuttaa $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0$, missä $a_i \in \mathbb{Z}$. Olkoon $M = \mathbb{Z}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{Z}[x]\} \subset K$. Silloin $M = \langle 1, \alpha, \ldots, \alpha^{d-1} \rangle$ ja $\alpha M \subseteq M$, koska $\alpha(\alpha^{d-1}) = \alpha^d = -\sum_{i=0}^{d-1} a_i \alpha^i \in M$. Toisin päin, olkoon $M \subseteq K$ äärellisesti viritetty moduli, jolle pätee $\alpha M \subseteq M$. Valitaan $w_1, \ldots, m_n$ virittäjäjoukoksi ja olkoon

$$\alpha w_i = \sum_j c_{ij} w_j, \ c_{ij} \in \mathbb{Z}.$$

Jos asetetaan $C = (c_{ij})$ näemme, että $(\alpha I - C)(w_1, \ldots, w_n)^t = (0, \ldots, 0)^t$ joten α toteuttaa yhtälön $\det(xI - C) = 0$, mikä on pääpolynomi, jolla on kokonaislukukertoimet. Näin ollen $\alpha \in O_K$. □

Viimein pystymme todistamaan proposition.

Todistus. Olkoot $\alpha, \beta \in O_K$. Ja $M, N \subseteq K$ äärellisesti viritettyjä $\mathbb{Z}$-moduleja, jonka virittäjät ovat $\{v_1, \ldots, v_d\}$ ja $\{w_1, \ldots, w_e\}$ ja joille pätee $\alpha M \subseteq M$ ja $\beta N \subseteq N$. Tarkastellaan

$$MN := \left\{ \sum_{i=1}^{k} m_i n_i : m_i \in M, n_i \in N \right\}.$$

Moduli MN on äärellisesti viritetty, sen virittäjät ovat $\{v_i m_j : 1 \leq i \leq d, 1 \leq j \leq e\}$, lisäksi se kuuluu K:n. Valittujen modulien nojalla on totta, että

$$\begin{aligned} (\alpha + beta)MN \subseteq (\alpha M)N + M(\beta N) \subseteq MN \\ (\alpha\beta)MN \subseteq (\alpha M)(\beta N) \subseteq MN. \end{aligned}$$

Edellisen lemman perusteella tästä seuraa, että $\alpha + \beta, \alpha\beta \in O_K$. □

Näin ollen voimme todistaa, että kokonaisluvut O_K muodostavat renkaan, sillä yhteen- ja kertolasku ovat normaalit ja O_K on suljettu tämän operaation suhteen. Nolla ja ykkönen kuuluvat myös renkaaseen, ja se on kommutatiivinen.

2.2 Neliökunnat

Nyt voimme siirtyä tarkastelemaan tarkemmin neliökuntia. Nämä ovat helpoimpia kuntalaajennuksia, mutta millään tavalla näiden teoriaa ei voi pitää triviaalina. Itseasiassa, on olemassa vielä useita avoimia ongelmia, jopa näille pienimmille mahdollisille kuntalaajennuksille.

Neliökunnat ovat rationaalilukujen $\mathbb{Q}$ astetta kaksi olevia laajennuksia, ja ne voidaan kirjoittaa muotoon $\mathbb{Q}(\sqrt{D})$, missä $D \in \mathbb{Q}$, ja $\sqrt{D}$ toteuttaa

polynomin $x^2 - D \in \mathbb{Q}[x]$. Jos $\sqrt{D} \notin \mathbb{Q}$, silloin $\sqrt{D}$ on algebrallinen luku $\mathbb{Q}$:n yli, jonka aste on 2. Kunta on $\mathbb{Q}(\sqrt{D}) := \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$.

Jos $D = a^2 d$, jollekin a, huomataan, että minimipolynomi $x^2 - a^2 d = (x - a\sqrt{d})(x + a\sqrt{d})$, mutta tässä $a \in \mathbb{Q}$, joten riittää liittää kuntaan luku $\sqrt{d}$, jotta polynomi hajoaa.

Tästä lähtien käsittelemme tapausta $\mathbb{Q}(\sqrt{D})$, missä $D \neq 0, 1$ ja D on neliövapaa kokonaisluku.

Kokonaisluvut neliökunnissa ovat siis niitä algebrallisia lukuja, joiden minimipolynomin kertoimet ovat (rationaalisia) kokonaislukuja. Ne ovat joko muotoa $\mathbb{Z}(\sqrt{D})$, tapauksessa, että $D \equiv 3 \mod 4$, tai sitten

$$\{m + n\sqrt{D}\} \cup \{ (m + \frac{1}{2}) + (n + \frac{1}{2})\sqrt{D}\}$$

tapauksessa $D \equiv 1 \mod 4$.

Näillä renkaissa on astefunktio ϕ, joka joskus toimii myös Eukleideen astefunktiona. Huom. nämä kokonaisalueet eivät aina ole Eukleideen alueita!

$\phi(a + b\sqrt{D}) = |a^2 - db^2| \in \mathbb{Z}$. Luonnollisesti tämä funktio on multiplikatiivinen, mutta Eukleideen algoritmi ei välttämättä toimi.

2.3 Kokonaisluvut neliökunnissa

Kuten yllä totesimme, neliökunnalla $K = \mathbb{Q}(\sqrt{D})$ on $\mathbb{Q}$-kanta $\{1, \sqrt{D}\}$. Näin ollen mikä tahansa alkio $\alpha = a + b\sqrt{D} \in K$. Tämän alkion minimipolynomi on $m_\alpha(x) = x^2 - 2ax + (a^2 - Db^2)$, jos $b \neq 0$ ja $(x - a)$ jos $b = 0$. Määritelmän mukaan kokonaislukuja ovat ne, joiden minimipolynomin kertoimet ovat kokonaislukuja. Näin olle, jos $b = 0$, kokonaislukuja ovat $\alpha = a \in \mathbb{Z}$. Tapaus $b \neq 0$ on tietysti kiinnostavampi. Vaadimme, että $2a, a^2 - Db^2 \in \mathbb{Z}$. Ensimmäisestä seuraa, että $a \in \mathbb{Z}$ tai $a \in \mathbb{Z} + \frac{1}{2}$.

Tapaus I: $a \in \mathbb{Z}$ ja $a^2 - Db^2 \in \mathbb{Z}$. Tästä seuraa, että $Db^2 \in \mathbb{Z}$, mistä seuraa, että $b \in \mathbb{Z}$.

Tapaus II: $a \in \mathbb{Z} + \frac{1}{2}$, eli $a = m + \frac{1}{2}$. Näin ollen $a^2 - Db^2 = m^2 + m + \frac{1}{4} - Db^2 \in \mathbb{Z}$. Tästä seuraa $\frac{1}{4} - Db^2 \in \mathbb{Z}$. Kerrotaan yhtälö neljällä, ja saadaan $1 - D(2b)^2 \in \mathbb{Z}$, eli $D(2b)^2 \in \mathbb{Z}$, joten $2b \in \mathbb{Z}$ ja edelleen joko $b \in \mathbb{Z}$ tai $b \in \mathbb{Z} + \frac{1}{2}$. Ensimmäinen tapaus on mieletön, sillä $\frac{1}{4} - Db^2 \in \mathbb{Z}$ ei voi toteutua, kun $b \in \mathbb{Z}$. Jäljelle jää tapaus $b = n + \frac{1}{2}$, jollekin n. Tässä tapauksessa $b^2 = n^2 + n + \frac{1}{4}$ ja yhtälöksi jää $\frac{1}{4} - \frac{D}{4} \in \mathbb{Z}$, joten $D \equiv 1 \mod 4$.

2.4 Diskriminantti, normi ja jälki

Määritelmä 2.13. Kunnan K upotus kuntaan L on injektiivinen (rengas)homomorfismi $K \hookrightarrow L$

Tarkastellaan $\mathbb{Q}$:n mahdollisia upotuksia kuntaan K, ja merkitään näitä $\sigma : \mathbb{Q} \longrightarrow K$. Nyt $\sigma(1) \neq 0$, koska σ on injektio. Edelleen $\sigma(a) = \sigma(1 \cdot a) = \sigma(1)\sigma(a)$, mistä seuraa, että $\sigma(1) = 1$. Koska σ (rengashomomorfismina) on additiivinen, tämä määrittää yksikäsitteisesti σ:n arvot kaikille $\mathbb{Z}$. Tämä voidaan helposti laajentaa nyt rationaaliluvulle $r = m/n$, jossa $m, n \in \mathbb{Z}$. Tästä saadaan $\sigma(r) = \sigma(m)(\sigma(n))^{-1}$. Näin ollen σ on yksikäsitteisesti määritelty myös kaikille $\mathbb{Q}$:n arvoille, joten $\mathbb{Q}$ voidaan lopulta upottaa ainoastaan yhdellä tavalla kuntaan K. Jos kunnan K karakteristika on 0, silloin kuvaus, joka kuvaa $1 \in \mathbb{Q}$ alkioon $1 \in K$ määrittää tämän ainoan upotuksen. Erityisesti $\mathbb{Q}$ kunnan $\mathbb{C}$ alikuntana on ainoa tapa upottaa $\mathbb{Q}$ kuntaan $\mathbb{C}$.

Lause 2.14. *Olkoon $K = \mathbb{Q}(\theta)$ algebrallinen lukukunta, jonka aste on n. Silloin on olemassa täsmälleen n erillistä upotusta $\sigma_i : K \longrightarrow \mathbb{C}$. $i = 1, \ldots, n$. Alkiot $\sigma_i(\theta)$ ovat täsmälleen θ:n minimipolynomin erilliset nollakohdat $\mathbb{C}$:ssä.*

Todistus. Olemme todistaneet aiemmin, että kaikki lukukunnat ovat muotoa $\mathbb{Q}(\theta)$, jollekin θ, missä θ:n minimipolynomi $f(x)$ on jaoton ja sen aste on n. Merkitään $f(x)$:n juuria $\mathbb{C}$:ssä $\theta_1, \theta_2, \ldots, \theta_n$. Nämä juuret ovat keskenään erisuuria, koska polynomi $f(x)$ on jaoton. Kaikille $i = 1, \ldots, n$ määritellään kuvaus $\sigma_i : \mathbb{Q}(\theta) \longrightarrow \mathbb{C}$, joka kuvaa θ:n alkioksi θ_i. Edellisen kappaleen nojalla kuvauksen σ_i pitää kuvata $\mathbb{Q}$ itselleen, joten riittää määritellä, minne θ kuvautuu.

Tämän näkee seuraavasti. Kunta $\mathbb{Q}(\theta_i) \cong \mathbb{Q}[x]/(f)$, ja jotta saadaan σ_i, yhdistetään isomorfismi $\mathbb{Q}(\theta) \longrightarrow \mathbb{Q}[x]/(f)$:n joka kuvaa $\theta \mapsto x$, isomorfismin $\mathbb{Q}[x]/(f) \longrightarrow \mathbb{Q}(\theta_i)$:n kanssa, joka kuvaa $x \mapsto \theta_i$.

Nyt kasassa on ainakin n kuvausta $\mathbb{Q}(\theta) \longrightarrow \mathbb{C}$. Oletetaan, että on olemassa vielä uusi upotus $\tau : \mathbb{Q}(\theta) \longrightarrow \mathbb{C}$. Silloin $\tau(f(\theta)) = \tau(0) = 0$. Mutta koska τ kiinnittää $\mathbb{Q}$:n ja τ on homomorfismi, $\tau(f(\theta)) = f(\tau(\theta))$, joten θ:n kuvan pitää kuin pitääkin olla f:n juuri, eli lopulta τ on muotoa σ_i, jollekin i, joten upotuksia on tasan n kappaletta. □

Jos $\sigma_i(K) \subseteq \mathbb{R}$, silloin kyseessä on reaalinen upotus, muussa tapauksessa upotusta kutsutaan kompleksiseksi.

Määritelmä 2.15. Olkoon $K/\mathbb{Q}$ algebrallinen lukukunta, jonka aste on n, ja olkoon $\alpha \in K$. Olkoot $\sigma_i : K \longrightarrow \mathbb{C}$ kunnan K yhteensä n upotusta. Alkioita $\sigma_i(\alpha)$ kutsutaan α:n K-konjugaateiksi. Määrittelemme alkion α jäljen $Tr_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$, ja normin $N_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha)$.

Helposti nähdään, että

$$N(\alpha\beta) = N(\alpha)N(\beta),$$

ja että $N(\alpha) = 0$ jos ja vain jos $\alpha = 0$ sekä $N(a) = a^n$ kun $a \in \mathbb{Q}$.

Katsotaan näitä heti tapauksessa, jossa lukukunta on neliökunta.

Upotuksia on kahdenlaisia. Jos D on positiivinen kokonaisluku, silloin on vain reaaliupotukset $\mathbb{Q}(\sqrt{D}) \longrightarrow \mathbb{R}$, missä $a + b\sqrt{D} \mapsto a + b\sqrt{D}$ ja $a + b\sqrt{D} \mapsto a - b\sqrt{D}$.

Tapauksessa D on negatiivinen kokonaisluku, on kaksi kompleksikonjugaattiupotusta $a+i\sqrt{D} \mapsto a+i\sqrt{D}$ ja $a+i\sqrt{D} \mapsto a-i\sqrt{D}$. Joka tapauksessa, kokonaislukujen rengas on kaksiulotteinen.

Näin saadaan alkiolle normi ja jälki. Normin ja jäljen perusteella on helppo laskea myös minimipolynomit.

Määritelmä 2.16. Olkoon $w = \{w_1, \ldots, w_n\}$ joku n-jono K:n alkiota, missä $n = [K : \mathbb{Q}]$. Determinantti on $\Delta(w) := \det(\sigma_i(w_j))$. Diskriminantti on $\Delta^2(w)$.

Lemma 2.17 (van der Monden determinantti)**.** *Jos $K = \mathbb{Q}(\alpha)$ ja $v = \{1, \alpha, \ldots, \alpha^{n-1}\}$, silloin*

$$\Delta^2(v) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Tässä $\alpha_1, \ldots, \alpha_n$ ovat α:n konjugaatteja.

Korollaari 2.18. *$\Delta(w_1, \ldots, w_n) \neq 0$ jos ja vain jos $w_1, \ldots, w_n$ on $K/\mathbb{Q}$:n kanta.*

Olkoon $K = \mathbb{Q}(\sqrt{D})$, missä D on neliövapaa kokonaisluku. Näin ollen $[K : \mathbb{Q}] = 2$, ja O_K:n kokonaislukukanta on $\{1, \sqrt{d}\}$ jos $d \equiv 2, 3 \mod 4$ ja kanta on $\{1, \frac{1+\sqrt{d}}{2}\}$ kun $d \equiv 1 \mod 4$. Nämä voi lukea suoraan kokonaislukujen renkaasta.