Compositie van kwadratische en kubische vormen

Bachelorscriptie

Tom van Overbeeke
Studentnummer 3806588
Universiteit Utrecht
Onder begeleiding van Prof. dr. Frits Beukers

4 juli 2014

Inleiding

Als je je een beetje in de getaltheorie verdiept hebt, dan ben je waarschijnlijk ook beroemde problemen tegengekomen, zoals de vraag welke gehele getallen wel en niet representeerbaar zijn als de som van twee kwadraten. Misschien ken je de stelling dat elk geheel getal groter dan nul te schrijven is als de som van vier kwadraten. Maar er wordt natuurlijk ook met hogere machten gewerkt. De beroemde laatste stelling van Fermat zegt dat er geen oplossingen zijn voor de vergelijking $x^n + y^n = z^n$ met $n \geq 3$. Gauss deed in 1801 onderzoek naar het probleem van de som van twee kwadraten, in algemene vorm. Hij onderzocht welke gehele getallen representeerbaar waren door polynomen van de vorm $ax^2 + bxy + cy^2$. Hij publiceerde zijn resultaten in zijn 'Disquisitiones Arithmeticae' [5], een boek dat zijn tijd ver vooruit was. Het was Gauss namelijk gelukt om dit probleem niet alleen op te lossen, maar de polynomen te classificeren aan de hand van hun discriminant $\Delta = b^2 - 4ac$ en een vermenigvuldiging op de polynomen te definiëren, waardoor een groepstructuur ontstond. Bijzonder was hierbij dat de notie van groepen op dat moment nog niet bestond. Hij vond bijvoorbeeld dat m representeerbaar is door een polynoom van discriminant Δ dan en slechts dan als de vergelijking $\xi^2 \equiv \Delta \pmod{4m}$ oplosbaar is. Met behulp van zijn vermenigvuldiging vond hij dat als $f_1(x, y)$ en $f_2(x, y)$ het getal m_1, respectievelijk m_2 representeerde, dan representeerde $(f_1 \circ f_2)(x, y)$ het getal $m_1 m_2$. Een nadeel van de vermenigvuldiging was dat deze slechts existentieel was. Gegeven f_1 en f_2 was het niet makkelijk om $f_1 \circ f_2$ te berekenen. Dirichlet specificeerde deze vermenigvuldiging en dit leidde uiteindelijk tot het compositiealgoritme van Arndt, waardoor het berekenen van een compositie een stuk makkelijk werd. Dirichlet deed echter nog meer, hij bewees dat er een isomorfisme bestond tussen de groep van kwadratische vormen en de groep van idealen van kwadratische ringen. Dit deed hij in 1838 en het was voor beide velden een grote stap vooruit.
166 jaar later, in 2004, publiceert Bhargava vier artikelen, waarin hij kijkt naar het verband tussen vormen van hogere orde en ringen van hogere orde. Dit doet hij aan de hand van (later naar hem vernoemde) Bhargava-kubussen. Hij eindigt met niet minder dan veertien nieuwe composities. Een bijzonder grote stap voor de getaltheorie.
In deze bachelorscriptie bekijk ik in hoofdstuk 1 en 2 de kwadratische vormen en hun compositie, zoals deze door Gauss en Dirichlet behandeld zijn. In hoofdstuk 3 nemen we de grote stap van Bhargava en we eindigen met één van zijn veertien composities: die van de kubische vormen, polynomen van de vorm $ax^3 + 3bx^2y + 3cxy^2 + dy^3$.

Inhoudsopgave

1 Kwadratische vormen

Definitie 1.1. *Een binaire integrale kwadratische vorm is een polynoom in twee variabelen van de vorm* $f(x,y) = ax^2 + bxy + cy^2$ *met* $a, b, c \in \mathbb{Z}$.

Omdat in deze scriptie alleen met binaire integrale vormen (vormen in twee variabelen met gehele coëfficiënten) wordt gewerkt, zullen deze simpelweg worden aangeduid als kwadratische of kubische vormen. Het moge duidelijk zijn wat daarmee bedoeld wordt.

Een andere notatie voor een kwadratische vorm $ax^2 + bxy + cy^2$ is de matrixnotatie $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$. Bedenk hierbij dat geldt dat $\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = (ax^2 + bxy + cy^2)$. Als de variabelen x en y niet van belang zijn, wordt ook de notatie (a, b, c) gebruikt.

Definitie 1.2. *Een kwadratische vorm* (a, b, c) *is primitief als* $ggd(a, b, c) = 1$.
Een kwadratische vorm (a, b, c) *representeert een integer* m *als er* $x, y \in \mathbb{Z}$, *zodat* $m = ax^2 + bxy + cy^2$.
Een representatie is primitief als $ggd(x, y) = 1$.

Merk op dat als een kwadratische vorm niet primitief is, we deze factor uit het polynoom kunnen delen en het eindresultaat weer met deze factor kunnen vermenigvuldigen. In deze scriptie zal daarom alleen met primitieve vormen gewerkt worden. Ook geldt dat als een kwadratische vorm f de integer m representeert, dus $f(x, y) = m$, dan $f(ax, ay) = a^2 m$. Als m kwadraatvrij is, dan geldt dat x en y relatief priem zijn.

Een belangrijke invariant geassocieerd met deze kwadratische vormen is de discriminant Δ. Deze wordt belangrijk als je equivalentieklassen op de kwadratische vormen gaat definiëren.

Definitie 1.3. *Zij* (a, b, c) *een kwadratische vorm. Zijn discriminant* Δ *wordt dan gegeven door* $\Delta = b^2 - 4ac$.

Merk op dat $\Delta \equiv b^2 \pmod 4$, oftewel $\Delta \equiv 0 \pmod 4$ als b even is en $\Delta \equiv 1 \pmod 4$ als b oneven is. Verder geldt ook dat $\mathrm{Det}\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} = -\frac{\Delta}{4}$.
Op dit moment is het goed om een paar opmerkingen te maken over de vormen en zijn discriminant. Als $m = ax^2 + bxy + cy^2$, dan geldt dat $4am = 4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 - \Delta y^2$. Hieruit volgt dat als $\Delta < 0$ een polynoom van discriminant Δ alleen positieve of negatieve getallen kan representeren, afhankelijk van het teken van a. Zo'n polynoom heet positief, dan wel negatief, definiet. Als $\Delta > 0$ geldt dit niet. Dit maakt het makkelijk om te werken met $\Delta < 0$. Dit verschil zal je volgend hoofdstuk ook tegen komen.
In de inleiding werd opgemerkt dat m representeerbaar is door een polynoom van discriminant Δ dan en slechts dan als de vergelijking $\xi^2 \equiv \Delta \pmod m$ oplosbaar is. De ene kant op is dit makkelijk te bewijzen. Als $\xi^2 \equiv \Delta \pmod{4m}$, dan geldt $\Delta = \xi^2 - 4mz$ voor een $z \in \mathbb{Z}$. Het polynoom $mx^2 + \xi xy + zy^2$ heeft dus discriminant Δ en representeert m (met $x = 1, y = 0$). De andere kant op volgt het uit stelling 1.3, die we dit hoofdstuk bewijzen.

1.1 Equivalentieklassen

Definitie 1.4. *Gegeven 2 kwadratische vormen* $f = ax^2 + bxy + cy^2$ *en* $f' = a'x'^2 + b'x'y' + c'y'^2$.
Definieer $f \sim f'$ *als* $f(x, y) = f'(\alpha x + \gamma y, \beta x + \delta y)$, *zó dat* α, β, γ, $\delta \in \mathbb{Z}$, $\alpha\delta - \beta\gamma = 1$.

Merk op dat dit equivalent is met het zeggen dat $f \sim f'$ als er een (andere) 2×2 matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is, zó dat α, β, γ, $\delta \in \mathbb{Z}$, $\alpha\delta - \beta\gamma = 1$ en $\begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$.

Deze relatie is een equivalentierelatie:

- De relatie is reflexief. Voor alle f geldt $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- De relatie is symmetrisch. Voor alle f,f' geldt dat als $f \sim f'$ met $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, dan $f' \sim f$. Er geldt dan namelijk $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} = \begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ en $\delta\alpha - (-\beta)(-\gamma) = \alpha\delta - \beta\gamma = 1$ en $\alpha, -\beta, -\gamma, \delta \in \mathbb{Z}$.
- De relatie is transitief. Voor alle f,f',f'' geldt dat als $f \sim f'$ met $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ en $f' \sim f''$ met $\begin{pmatrix} \epsilon & \zeta \\ \eta & \theta \end{pmatrix}$, dan $f \sim f''$. Er geldt dan namelijk dat

$$\begin{aligned} \begin{pmatrix} a'' & \frac{b''}{2} \\ \frac{b''}{2} & c'' \end{pmatrix} &= \begin{pmatrix} \epsilon & \eta \\ \zeta & \theta \end{pmatrix} \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \epsilon & \zeta \\ \eta & \theta \end{pmatrix} \\ &= \begin{pmatrix} \alpha\epsilon + \beta\eta & \gamma\epsilon + \delta\eta \\ \alpha\zeta + \beta\theta & \gamma\zeta + \delta\theta \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} \alpha\epsilon + \beta\eta & \alpha\zeta + \beta\theta \\ \gamma\epsilon + \delta\eta & \gamma\zeta + \delta\theta \end{pmatrix}. \end{aligned}$$

  Deze coëfficiënten zijn duidelijk geheelwaardig en hebben determinant 1, omdat determinanten vermenigvuldigen.

Er kunnen een aantal dingen worden opgemerkt over de equivalentieklassen.
Ten eerste geldt dat als twee kwadratische vormen equivalent zijn, ze gelijke discriminant hebben. Dit volgt uit het feit dat de determinant van hun transformatiematrix 1 is. Omdat determinanten vermenigvuldigen, is de determinant van hun respectievelijke matrixvorm gelijk. Daarmee is hun discriminant gelijk.
Een ander punt is dat equivalente vormen gelijke getallen representeren. Dit volgt rechtstreeks uit de definitie van equivalentie. Als je (x, y) kunt transformeren naar (x', y') en terug, zodat de kwadratische vormen in elkaar over gaan, moeten ze wel dezelfde getallen representeren. Het omgekeerde geldt ook: als twee vormen van gelijke discriminant dezelfde getallen representeren, dan zijn ze equivalent. Dit zal in deze scriptie echter niet bewezen worden.
Gauss liet overigens nog een belangrijk eigenschap zien van equivalentieklassen. Hij bewees dat iedere vaste discriminant Δ een eindig aantal equivalentieklassen had. Dit betekent dus dat de groep die we dit hoofdstuk proberen te definiëren een eindige groep is.

1.2 Enkele belangrijke equivalenties

In deze paragraaf worden enkele transformaties berekend die nuttig zijn voor het bewijzen van de komende stellingen. Allereerst de meest algemene transformatie. Er geldt dat

$$\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\alpha^2 + b\alpha\gamma + c\gamma^2 & a\alpha\beta + c\gamma\delta + \frac{b(\alpha\delta+\beta\gamma)}{2} \\ a\alpha\beta + c\gamma\delta + \frac{b(\alpha\delta+\beta\gamma)}{2} & a\beta^2 + b\beta\delta + c\delta^2 \end{pmatrix}.$$

Hieruit volgt dat $f = (a, b, c) \sim (a', b', c')$ met

$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2 = f(\alpha, \gamma)$$
$$b' = b(\alpha\delta + \beta\gamma) + 2(a\alpha\beta + c\gamma\delta)$$
$$c' = a\beta^2 + b\beta\delta + c\delta^2 = f(\beta, \delta)$$

Gebruik deze transformatie nu met de volgende matrices:

- Uit de transformatie onder $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ volgt dat $(a, b, c) \sim (c, -b, a)$.
- Uit de transformatie onder $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ volgt dat $(a, b, c) \sim (a, 2a + b, a + b + c)$.
- Uit de transformatie onder $S^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ volgt dat $(a, b, c) \sim (a, 2na + b, n^2a + nb + c)$.

Er geldt dat matrices S en T de groep $\Gamma = \{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} | \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \alpha\delta - \beta\gamma = 1\}$ onder matrixvermenigvuldiging voortbrengen. Hieruit volgt dat twee equivalente vormen onder een eindig aantal transformaties door S en T in elkaar over gaan.

1.3 Compositie van kwadratische vormen

Het blijkt dat er een vermenigvuldiging op equivalantieklassen gedefinieerd kan worden. Gauss definieerde dit als volgt:

Definitie 1.5. *Zij $f_1 = (a_1, b_1, c_1)$ en $f_2 = (a_2, b_2, c_2)$ twee kwadratische vormen van gelijke discriminant. Definieer $f_1 \circ f_2 = F$, waarbij $F = (A, B, C)$ een kwadratische vorm van dezelfde discriminant is, zó dat*

- $f_1(x_1, y_1)f_2(x_2, y_2) = F(X, Y)$,
  waarbij $\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 & \delta_1 \\ \alpha_2 & \beta_2 & \gamma_2 & \delta_2 \end{pmatrix} \begin{pmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{pmatrix}$ *met* $\alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{Z}$.
- $\alpha_1\beta_2 - \alpha_2\beta_1 = a_1$.
- $\alpha_1\gamma_2 - \alpha_2\gamma_1 = a_2$.

Deze definitie is niet handelbaar, omdat niet duidelijk is of deze F bestaat. Daarnaast geeft de definitie geen manier geeft om de compositie te berekenen. Dirichlet gaf aanzet tot een meer bruikbare definitie, die uiteindelijk uitmondde in het compositiealgoritme van Arndt. Dit zullen we in de volgende paragrafen behandelen. Hierbij volgen we de aanpak van Buell [3]. Dirichlet begon met de onderstaande uitdrukking en veralgemeniseerde dit vervolgens voor equivalentieklassen. Er geldt dat

$$(a_1x_1^2 + Bx_1y_1 + a_2Cy_1^2)(a_2x_2^2 + Bx_2y_2 + a_1Cy_2^2) = a_1a_2X^2 + BXY + CY^2,$$

waarbij $\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -C \\ 0 & a_1 & a_2 & B \end{pmatrix} \begin{pmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{pmatrix}$.

Definieer daarom $(a_1, B, a_2C) \circ (a_2, B, a_1C) \sim (a_1a_2, B, C)$. Merk op dat deze vrij specifieke

compositie voldoet aan de voorwaarden van Gauss. Met de volgende stellingen kan dit worden veralgemeniseerd tot compositie van equivalentieklassen.

Stelling 1.1. *Zij* (a_1, b_1, c_1) *en* (a_2, b_2, c_2) *kwadratische vormen van discriminant* Δ*, zó dat* $ggd(a_1, a_2, \frac{b_1+b_2}{2}) = 1$*. Dan zijn er* B *en* C*, zó dat* $(a_1, b_1, c_1) \sim (a_1, B, a_2C)$ *en* $(a_2, b_2, c_2) \sim (a_2, B, a_1C)$*.*

Bewijs
Door (a, b, c) te transformeren onder de matrix S^n, vind je dat $(a, b, c) \sim (a, b+2an, c+bn+an^2)$. Het doel is nu om (a_1, b_1, c_1) te transformeren onder S^{n_1} en (a_2, b_2, c_2) te transformeren onder S^{n_2}, zó dat daaruit de gevraagde vormen komen. Dit betekent dat het probleem gereduceerd wordt tot het oplossen van een stelsel van vergelijkingen $B \equiv b_1 \pmod{2a_1}$ en $B \equiv b_2 \pmod{2a_2}$ voor B en C, zó dat $C = \frac{B^2-\Delta}{4a_1a_2}$ geheel is.

Uit de eerste vergelijking volgt dat $B = b_1 + 2a_1x$ met $x \in \mathbb{Z}$, waardoor $b_1 + 2a_1x \equiv b_2 \pmod{2a_2}$ en $\frac{b_1-b_2}{2} \equiv -a_1x \pmod{a_2}$. Dit is dan en slechts dan oplosbaar als $\text{ggd}(a_1, a_2) | \frac{b_1-b_2}{2}$. Omdat $\Delta = b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2$, geldt dat $a_1c_1 - a_2c_2 = \frac{b_1^2-b_2^2}{4} = \frac{b_1+b_2}{2}\frac{b_1-b_2}{2}$. De linkerkant is deelbaar door $\text{ggd}(a_1, a_2)$, dus de rechterkant is dit ook. Omdat $\text{ggd}(a_1, a_2, \frac{b_1+b_2}{2}) = 1$, moet wel gelden dat $\text{ggd}(a_1, a_2) | \frac{b_1-b_2}{2}$. We concluderen dus dat het stelsel van vergelijkingen oplosbaar is, met als algemene oplossing $B = B_0 + \frac{2a_1a_2}{\text{ggd}(a_1,a_2)}t$ voor zekere B_0 en $t \in \mathbb{Z}$.

Het doel is nu om t zo te kiezen, dat C een geheel getal is. Merk hierbij op dat het voldoende is om t zo te kiezen dat $B^2 \equiv \Delta \pmod{4a_1a_2}$. Stel namelijk dat $B^2 = \Delta + 4a_1a_2x$ met $x \in \mathbb{Z}$. Dan geldt dat $B^2 - 4a_1a_2x = \Delta = B^2 - 4a_1a_2C$, dus $C = x \in \mathbb{Z}$. Definieer verder $k = \frac{a_1a_2}{\text{ggd}(a_1,a_2)}$ en merk op dat $k^2 = a_1a_2\frac{a_1}{\text{ggd}(a_1,a_2)}\frac{a_2}{\text{ggd}(a_1,a_2)}$.
Stel nu dat $B^2 = (B_0 + 2kt)^2 = B_0^2 + 4kB_0t + 4k^2t^2 \equiv \Delta \pmod{4a_1a_2}$. Dan is

$$B_0^2 - \Delta \equiv -4B_0kt \pmod{4a_1a_2}.$$

Merk op dat $4k | B_0^2 - \Delta$, want $\Delta = B_0^2 - 4a_1C_1 = B_0^2 - 4a_2C_2$ (met C_1, C_2 onbekende integers, die verkregen worden door S een aantal maal op (a_1, b_1, c_1), respectievelijk (a_2, b_2, c_2) toe te passen). Hierdoor geldt dat $\Delta - B_0^2 \equiv 0 \pmod{4a_1}$ en $\Delta - B_0^2 \equiv 0 \pmod{4a_2}$, wat betekent dat $\Delta - B_0^2 \equiv 0 \pmod{\frac{4a_1\dot{4}a_2}{\text{ggd}(4a_1,4a_2)}} \equiv 0 \pmod{4k}$.
Bovenstaande vergelijking reduceert daarom tot

$$\frac{B_0^2 - \Delta}{4k} \equiv -B_0t \pmod{\text{ggd}(a_1, a_2)}.$$

Deze vergelijking is op te lossen voor t, omdat $\text{ggd}(B_0, \text{ggd}(a_1, a_2)) = 1$. Er geldt namelijk dat $B = b_1 + 2a_1n_1 = b_2 + 2a_2n_2 = B_0 + 2kt$, dus $B = \frac{b_1+b_2}{2} + a_1n_1 + a_2n_2 = B_0 + 2kt$. Er geldt dus dat $B_0 = \frac{b_1+b_2}{2} + a_1n_1 + a_2n_2 - 2kt$. Omdat $\text{ggd}(a_1, a_2) | a_1$, $\text{ggd}(a_1, a_2) | a_2$, $\text{ggd}(a_1, a_2) | k$, maar $\text{ggd}(\text{ggd}(a_1, a_2), \frac{b_1+b_2}{2}) = 1$, volgt met het Euclidisch algoritme dat $\text{ggd}(B_0, \text{ggd}(a_1, a_2)) = 1$.

We concluderen dat we t zó kunnen kiezen dat C geheel is en daarmee is de stelling bewezen. □

Bovenstaande stelling werkt alleen als $\text{ggd}(a_1, a_2, \frac{b_1+b_2}{2}) = 1$. Daarom de twee volgende stellingen. Deze garanderen dat twee willekeurige kwadratische vormen getransformeerd kunnen worden in twee kwadratische vormen waarvoor $\text{ggd}(a_1, a_2, \frac{b_1+b_2}{2}) = 1$.

Stelling 1.2. *Zij (a, b, c) een primitieve kwadratische vorm en zij m een integer. Dan is er een $n \in \mathbb{Z}$ zó dat $ggd(m, n) = 1$ en (a, b, c) n primitief vertegenwoordigt.*

Bewijs
Zij (a, b, c) en m zoals hierboven beschreven. Als $\text{ggd}(a, m) = 1$ of $\text{ggd}(c, m) = 1$, voldoet $n = a$, respectievelijk $n = c$. Met $(x, y) = (1, 0)$ of $(x, y) = (0, 1)$ worden namelijk zowel a als c primitief vertegenwoordigd.
Neem daarom aan dat $\text{ggd}(a, m) \neq 1$ en $\text{ggd}(c, m) \neq 1$. Zij p het product van de priemdelers die a, c en m gemeen hebben. Zij q het product van de priemdelers die a en m, maar niet c gemeen hebben. Zij r het product van de priemdelers die c en m, maar niet a gemeen hebben. Zij s tot slot het product van de overige priemdelers van m. Merk op dat al deze getallen relatief priem zijn. Definieer nu $n = aq^2 + bqrs + cr^2s^2$. Dan wordt n primitief vertegenwoordigd door $(x, y) = (q, rs)$. Verder geldt dat $\text{ggd}(n, p) = \text{ggd}(bqrs, p) = \text{ggd}(b, p) = 1$, omdat $\text{ggd}(a, b, c) = 1$. Ook geldt dat $\text{ggd}(n, q) = \text{ggd}(cr^2s^2, q) = 1$; $\text{ggd}(n, r) = \text{ggd}(aq^2, r) = 1$ en $\text{ggd}(n, s) = \text{ggd}(aq^2, s) = 1$. We concluderen daarom dat $\text{ggd}(m, n) = 1$. □

Stelling 1.3. *Zij (a, b, c) een primitieve kwadratische vorm die $m \in \mathbb{Z}$ primitief vertegenwoordigt. Dan geldt dat $(a, b, c) \sim (m, b', c')$ met $b', c' \in \mathbb{Z}$*

Bewijs
Omdat m primitief vertegenwoordigd is, zijn er α, γ met $\text{ggd}(\alpha, \gamma) = 1$, zodat $a\alpha^2 + b\alpha\gamma + c\gamma^2 = m$. Er geldt dat $\text{ggd}(\alpha, \gamma) = 1 \Leftrightarrow \exists \beta, \delta \in \mathbb{Z} : \alpha\delta - \beta\gamma = 1$. Nu geldt dat

$$\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\alpha^2 + b\alpha\gamma + c\gamma^2 & a\alpha\beta + c\gamma\delta + \frac{b(\alpha\delta+\beta\gamma)}{2} \\ a\alpha\beta + c\gamma\delta + \frac{b(\alpha\delta+\beta\gamma)}{2} & a\beta^2 + b\beta\delta + c\delta^2 \end{pmatrix} = \begin{pmatrix} m & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix}.$$

We concluderen dat $(a, b, c) \sim (m, b', c')$. □

Het gevolg van deze twee stelling is de volgende: Zij (a_1, b_1, c_1), (a_2, b_2, c_2) twee kwadratische vormen van discriminant Δ. Gebruik dan stelling 1.2 met $m = a_1$ om een n met $\text{ggd}(a_1, n) = 1$ te vinden die de tweede vorm representeert. Met stelling 1.3 transformeer je nu de tweede vorm tot (n, b', c'). We kunnen dus twee vormen transformeren te twee equivalente vormen met $\text{ggd}(a_1, a_2) = 1$, dus in het bijzonder $\text{ggd}(a_1, a_2, \frac{b_1+b_2}{2}) = 1$.
Daarmee is de compositie rond. Gegeven twee willekeurige kwadratische vormen f, f' van gelijke discriminant, transformeer je ze eerst in equivalente vormen (a_1, b_1, c_1), respectievelijk (a_2, b_2, c_2), zodat $\text{ggd}(a_1, a_2, \frac{b_1+b_2}{2}) = 1$. Vervolgens transformeer je ze in equivalente vormen (a_1, B, a_2C), respectievelijk (a_2, B, a_1C). Nu geldt dat $f \circ f' = (a_1a_2, B, C)$.
Wat echter nog niet bewezen is, is dat deze compositie welgedefinieerd is. Het zou kunnen dat de compositie afhangt van de representant van de equivalentieklasse of van de transformatie die je gedaan hebt voordat je de compositie gebruikt. Daarom de volgende stelling. Deze zegt als f_1 en f_2 van bovenstaande vorm zijn (dus (a_1, B, a_2C), respectievelijk (a_2, B, a_1C)), evenals f_3 en f_4, zodat $f_1 \sim f_3$ en $f_2 \sim f_4$, dat dan de compositie van f_1 en f_2 equivalent is aan de compositie van f_3 en f_4. Merk op dat dit voldoende is om de welgedefinieerdheid te bewijzen. Stel namelijk dat f_1, f_3 willekeurig equivalent zijn, evenals f_2 en f_4. Dan transformeer je deze eerst in vormen van bovenstaande vorm. Ze zitten nu nog steeds in dezelfde equivalentieklassen. Volgens de stelling zijn hun composities nu gelijk.
Er wordt echter eerst een lemma bewezen, wat nodig is om de stelling te bewijzen.

Lemma 1.4. *Twee vormen (a_1, b_1, c_1) en (a_2, b_2, c_2) met dezelfde discriminant Δ zijn equivalent*

dan en slechts dan als er $\alpha, \gamma \in \mathbb{Z}$ zijn, zó dat

$$\begin{aligned} a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 &= a_2, \\ 2a_1\alpha + (b_1 + b_2)\gamma &\equiv 0 \ (mod\ 2a_2), \\ (b_1 - b_2)\alpha + 2c_1\gamma &\equiv 0 \ (mod\ 2a_2). \end{aligned}$$

Bewijs "⇒"
Stel dat ze equivalent zijn. Dan is er matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, die (a_1, b_1, c_1) in (a_2, b_2, c_2) transformeert. Dat betekent dat $a_2 = a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2$, dus aan de eerste vergelijking is voldaan. Verder geldt dat $\alpha\delta - \beta\gamma = 1$ en $(b_1\gamma + 2a_1\alpha)\beta + (b_1\alpha + 2c_1\gamma)\delta = b_2$.
Eliminatie van δ leidt tot $2b_1\alpha\gamma\beta + 2a_1\alpha^2\beta + b_1\alpha + 2c_1\gamma + 2c_1\gamma^2\beta = b_2\alpha$, waardoor

$$(b_1 - b_2)\alpha + 2c_1\gamma = -2\beta(a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2) \equiv 0 \ (\text{mod } 2a_2).$$

Eliminatie van β leidt tot $2b_1\alpha\gamma\delta - b_1\gamma + 2a_1\alpha^2\delta - 2a_1\alpha + b_1\alpha\gamma\delta + 2c_1\gamma^2\delta = b_2\gamma$, waardoor

$$(b_1 + b_2)\gamma + 2a_1\alpha = 2\delta(a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2) \equiv 0 \ (\text{mod } 2a_2).$$

□

Bewijs "⇐"
Stel dat aan de vergelijkingen wordt voldaan. Dan zijn er $\beta, \delta \in \mathbb{Z}$, zodat $(b_1+b_2)\gamma+2a_1\alpha = 2a_2\delta$ en $(b_1 - b_2)\alpha + 2c_1\gamma = -2a_2\beta$. Nu geldt dat

$$\alpha\delta - \beta\gamma = \frac{1}{2a_2}((b_1 + b_2)\alpha\gamma + 2a_1\alpha^2 + (b_1 - b_2)\alpha\gamma + 2c_1\gamma^2) = \frac{a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2}{a_2} = 1.$$

Ook geldt dat

$$(b_1\gamma + 2a_1\alpha)\beta + (b_1\alpha + 2c_1\gamma)\delta = \frac{b_2(a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2)}{a_2} = b_2.$$

$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ transformeert (a_1, b_1, c_1) dus in (a_2, b_2, c'). Omdat $\alpha\delta - \beta\gamma = 1$, is de discriminant van deze twee vormen gelijk. Daarom geldt dat $c' = \frac{\Delta - b_2^2}{4a_2} = c_2$. We concluderen dat $(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$. □

Stelling 1.5. *Zij $f_1 = (a_1, B, a_2C)$, $f_2 = (a_2, B, a_1C)$, $f_3 = (m_1, N, m_2L)$ en $f_4 = (m_2, N, m_1L)$ kwadratische vormen van gelijke discriminant Δ, zó dat $ggd(a_1, a_2, B) = 1$, $ggd(m_1, m_2, N) = 1$, $f_1 \sim f_3$ en $f_2 \sim f_4$. Dan geldt dat $f_1 \circ f_2 \sim f_3 \circ f_4$.*

Bewijs Zij f_1, f_2, f_3, f_4 zoals hierboven gedefinieerd. Volgens bovenstaand lemma, zijn er $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ te definiëren, zodat

$$\begin{aligned} a_1x_1^2 + Bx_1y_1 + a_2Cy_1^2 &= m_1 \\ 2a_1x_1 + (B+N)y_1 &\equiv 0 \pmod{2m_1} \\ (B-N)x_1 + 2a_2Cy_1 &\equiv 0 \pmod{2m_1} \end{aligned}$$

$$\begin{aligned} a_2x_2^2 + Bx_2y_2 + a_1Cy_2^2 &= m_2 \\ 2a_2x_2 + (B+N)y_2 &\equiv 0 \pmod{2m_2} \\ (B-N)x_2 + 2a_1Cy_2 &\equiv 0 \pmod{2m_2} \end{aligned}$$

Definieer nu $X = x_1x_2 - Cy_1y_2$ en $Y = a_1x_1y_2 + a_2x_2y_1 + By_1y_2$. Zoals aan het begin van dit hoofdstuk geconstateerd, geldt nu dat

$$a_1a_2X^2 + BXY + CY^2 = (a_1x_1^2 + Bx_1y_1 + a_2Cy_1^2)(a_2x_2^2 + Bx_2y_2 + a_1Cy_2^2) = m_1m_2.$$

Merk op dat $B^2 - 4a_1a_2C = \Delta = N^2 - 4m_1m_2L$, dus $N^2 = B^2 - 4a_1a_2C + 4m_1m_2L$. Hierdoor geldt dat

$$\begin{aligned} &2(a_1x_1+(B+N)\frac{y_1}{2})(a_2x_2 + (B+N)\frac{y_2}{2}) \\ &\qquad = 2a_1a_2x_1x_2 + (B+N)(a_2x_2y_1 + a_1x_1y_2) + \frac{y_1y_2}{2}(2B^2 + 2BN + 4m_1m_2L - 4a_1a_2C) \\ &\qquad = 2a_1a_2X + (B+N)Y + 2m_1m_2Ly_1y_2. \end{aligned}$$

Door deze vergelijking nu modulo $2m_1m_2$ te bekijken, zie je dat $2a_1a_2X + (B+N)Y \equiv 0 \pmod{2m_1m_2}$.

Definieer $U = (B-N)X + 2CY$. Dan geldt er dat

$$\begin{aligned} 2((B-N)\frac{x_1}{2} + a_2Cy_1)(a_2x_2 + (B+N)\frac{y_2}{2}) - a_2U &= 2Lm_1m_2x_1x_2 \\ 2(a_1x_1 + (B+N)\frac{y_1}{2})((B-N)\frac{x_2}{2} + a_1Cy_2) - a_1U &= 2Lm_1m_2x_1x_2 \\ 2((B-N)\frac{x_1}{2} + a_2Cy_1)((B-N)\frac{x_2}{2} + a_1Cy_2) - \frac{B-N}{2}U &= -2CLm_1m_2y_1y_2 \\ 2C(a_1x_1 + (B+N)\frac{y_1}{2})(a_2x_2 + (B+N)\frac{y_2}{2}) - \frac{B+N}{2}U &= -2Lm_1m_2y_1y_2 \end{aligned}$$

Door deze vergelijkingen nu modulo $2m_1m_2$ te bekijken en de laatste twee vergelijkingen op te tellen, zie je dat $a_2U \equiv 0 \pmod{2m_1m_2}$, $a_1U \equiv 0 \pmod{2m_1m_2}$ en $BU \equiv 0 \pmod{2m_1m_2}$. Omdat $\text{ggd}(a_1, a_2, B) = 1$, moet nu wel gelden dat $U \equiv 0 \pmod{2m_1m_2}$.

Er geldt dus dat

$$\begin{aligned} a_1a_2X^2 + BXY + CY^2 &= m_1m_2 \\ 2a_1a_2X + (B+N)Y &\equiv 0 \pmod{2m_1m_2} \\ (B-N)X + 2CY &\equiv 0 \pmod{2m_1m_2} \end{aligned}$$

Volgens het bovenstaande lemma volgt nu dat $f_1 \circ f_2 = (a_1a_2, B, C) \sim (m_1m_2, N, L) = f_3 \circ f_4$. $\square$

1.4 De groep van kwadratische vormen van vaste discriminant

Het blijkt dat de compositie die in de vorige paragraaf gedefinieerd is een groepsstructuur vastlegt om de kwadratische vormen van vaste discriminant.

Stelling 1.6. *De equivalentieklassen van kwadratische vormen met vaste discriminant Δ vormen een groep onder compositie. Deze groep heet de klassegroep van discriminant Δ. Notatie: $\mathcal{C}(\Delta)$*

Bewijs

- Vanwege de definitie van de compositie wordt aan **geslotenheid** voldaan.
- Omdat compositie niets meer is dan vermenigvuldiging en matrixtransformatie, is deze compositie **associatief**. Vermenigvuldiging en matrixtransformatie zijn dit immers ook.
- De equivalentieklasse met daarin het element $(1, b', c')$, waarbij b', c' geheel, is het **identiteitselement**. Er geldt namelijk dat voor alle vormen (a, b, c): $(1, b', c') \circ (a, b, c) \sim (1, b, c'') \circ (a, b, c)$ door matrix S $\frac{1}{2}(b - b')$ maal toe te passen op $(1, b', c')$. Omdat de discriminant niet verandert, geldt dat $b^2 - 4ac = \Delta = b^2 - 4c''$, waardoor $c'' = ac$. Er geldt dus dat $(1, b', c') \circ (a, b, c) \sim (1, b, ac) \circ (a, b, c) \sim (a, b, c)$. Merk op dat $(1, b', c') \sim (1, b''', c''')$, waardoor we daadwerkelijk maar één identiteitsklasse hebben.
- Zij (a, b, c) een kwadratische vorm van discriminant Δ. Dan is $(a, -b, c)$ dit ook en dit is de **inverse** van (a, b, c). Door matrix T toe te passen vinden we $(a, -b, c) \sim (c, b, a)$, waardoor $(a, b, c) \circ (a, -b, c) \sim (a, b, c) \circ (c, b, a) \sim (ac, b, 1) \sim (1, -b, ac)$.

□

Merk op dat de compositie commutatief is, dus dat de equivalentieklassen zelfs een Abelse groep vormen.

1.5 Het compositiealgoritme van Arndt

De compositie van kwadratische vormen is nu gedefinieerd. Het probleem is echter dat deze definitie existentieel is. Er is bewezen dat er voor twee willekeurige kwadratische vormen een compositie is, maar het is lastig om deze te geven met behulp van de voorgaande stellingen. Daarvoor geeft Arndt een algoritme.

Stelling 1.7. *Zij $f_1 = (a_1, b_1, c_1)$ en $f_2 = (a_2, b_2, c_2)$ kwadratische vormen van gelijke discriminant Δ. Zij $\beta = \frac{b_1+b_2}{2}$, $n = ggd(a_1, a_2, \beta)$ en kies $t, u, v \in \mathbb{Z}$ zó dat $a_1 t + a_2 u + \beta v = n$. Definieer nu $A = \frac{a_1 a_2}{n^2}$ en $B = \frac{2a_1 b_2 t + 2a_2 b_1 u + v(b_1 b_2 + \Delta)}{2n}$. Dan geldt $f_1 \circ f_2 = (A, B, \frac{B^2 - \Delta}{4A})$.*

Bewijs

Het is duidelijk dat A een geheel getal is. Daarnaast geldt dat $b_1 b_2 + \Delta = 2\beta^2 + \frac{\Delta - b_1^2}{2} + \frac{\Delta - b_2^2}{2} = 2\beta^2 + 2a_1 c_1 + 2a_2 c_2$, waardoor elke term in B deelbaar is door $2n$ en B dus ook geheel is.

Nu geldt dat

$$(a_1 x_1^2 + b_1 x_1 y_1 + c_1 y_1^2)(a_2 x_2^2 + b_2 x_2 y_2 + c_2 y_2^2) = AX^2 + BXY + \frac{B^2 - \Delta}{4A} Y^2, \tag{1}$$

waarbij

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} n & \frac{(b_2 - B)n}{2a_2} & \frac{(b_1 - B)n}{2a_1} & \frac{(b_1 b_2 + \Delta - B(b_1 + b_2))n}{4a_1 a_2} \\ 0 & \frac{a_1}{n} & \frac{a_2}{n} & \frac{b_1 + b_2}{2n} \end{pmatrix} \begin{pmatrix} x_1 x_2 \\ x_1 y_2 \\ y_1 x_2 \\ y_1 y_2 \end{pmatrix}.$$

Merk op dat ook deze vermenigvuldiging aan de eisen van Gauss-compositie voldoet. Als we bewijzen dat deze substitutie gehele coëfficiënten heeft, dan volgt uit de welgedefinieerdheid van de compositie dat $f_1 \circ f_2 = (A, B, \frac{B^2-\Delta}{4A})$.
Omdat $n = \text{ggd}(a_1, a_2, \beta)$ is duidelijk dat de coëfficiënten van Y geheel zijn.
Verder geldt dat

$$\begin{aligned}(b_2 - B)n &= b_2(a_1t + a_2u + \beta v) - (a_1b_2t + a_2b_1u + v\frac{b_1b_2 + \Delta}{2}) \\ &= ua_2(b_2 - b_1) + v\frac{(b_2^2 - \Delta)}{2} = ua_2(b_2 - b_1) + 2va_2c_2 \equiv 0 \pmod{2a_2}.\end{aligned}$$

Bedenk voor deze laatste equivalentie dat $b_2 \equiv b_1 \pmod 2$. Analoog vind je dat $(b_1 - B)n \equiv 0 \pmod{2a_1}$.
Als laatste geldt dat

$$\begin{aligned}(b_1b_2 + \Delta - B(b_1 + b_2))n &= (b_1b_2 + \Delta)(a_1t + a_2u + \beta v) - (a_1b_2t + a_2b_1u + v\frac{b_1b_2 + \Delta}{2})(b_1 + b_2) \\ &= -a_1b_2^2t - a_2b_1^2u + \Delta a_1t + \Delta a_2u = (\Delta - b_2^2)a_1t + (\Delta - b_1^2)a_2u \\ &= 4a_1a_2(t + u) \equiv 0 \pmod{4a_1a_2}.\end{aligned}$$

We zien dus dat de coëfficiënten geheel zijn. We concluderen dat de stelling is bewezen. □

1.6 Bijvoorbeeld

In de laatste paragraaf van elk hoofdstuk wordt een voorbeeld bekeken, waarbij de theorie van dat hoofdstuk wordt behandeld. Neem $\Delta = -23$ als vaste discriminant van onze kwadratische vormen. Deze heeft drie equivalentieklassen, gegeven door de representanten $(1, 1, 6)$, $(2, 1, 3)$ en $(2, -1, 3)$. Uit de theorie van dit hoofdstuk blijkt dat deze equivalentieklassen een groep moeten vormen, waarbij $(1, 1, 6)$ het identiteitselement is. Verder hebben we gezien dat de inverse van (a, b, c) gegeven wordt door $(a, -b, c)$. In dit geval zouden dus $(2, 1, 3)$ en $(2, -1, 3)$ elkaars inverse moeten zijn. Merk op dat er (op isomorfie na) maar één groep van drie elementen bestaat, waardoor $\mathcal{C}(-23) \simeq (\mathbb{Z}/3\mathbb{Z}, +)$. Hierbij wordt $(1, 1, 6)$ naar 0 afgebeeld en $(2, 1, 3)$ en $(2, -1, 3)$ naar 1 en 2. Dit is conform onze verwachting dat de laatste twee elkaars inverse zijn. Om er echt zeker van te zijn, zullen we de compositie ook op twee manieren expliciet berekenen, zowel met behulp van de Dirichletcompositie, als met het compositiealgoritme van Arndt.

Voordat de Dirichletcompositie kan gebruikt worden, moeten $(2, 1, 3)$ en $(2, -1, 3)$ worden getransformeerd tot kwadratische vormen van de vorm (a_1, B, a_2C) en (a_2, B, a_1C). Er geldt dat

$$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}2 & -\frac{1}{2}\\ -\frac{1}{2} & 3\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} = \begin{pmatrix}3 & \frac{1}{2}\\ \frac{1}{2} & 2\end{pmatrix},$$

waardoor $(2, -1, 3) \sim (3, 1, 2)$. Hieruit volgt dat $(2, 1, 3) \circ (2, -1, 3) \sim (2, 1, 3) \circ (3, 1, 2) \sim (6, 1, 1)$.
Als laatste geldt dat

$$\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}\begin{pmatrix}6 & \frac{1}{2}\\ \frac{1}{2} & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix} = \begin{pmatrix}1 & \frac{1}{2}\\ \frac{1}{2} & 6\end{pmatrix}.$$

We concluderen dat $(2, 1, 3) \circ (2, -1, 3) \sim (1, 1, 6)$.

Voor het compositiealgoritme van Arndt berekenen we $\beta = \frac{b_1+b_2}{2} = 0$, $n = \text{ggd}(a_1, a_2, \beta) = 2$ en t, u, v, zodat $2t + 2u = 2$, waardoor $t = 1$ en $u = v = 0$. Hieruit volgt dat $A = \frac{a_1 a_2}{n^2} = 1$ en $B = \frac{2a_1 b_2 t + 2a_2 b_1 u + v(b_1 b_2 + \Delta)}{2n} = -1$. Hieruit volgt dat $C = \frac{B^2 - \Delta}{4A} = 6$. Nu geldt dat

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 6 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 6 \end{pmatrix},$$

waardoor $(2, 1, 3) \circ (2, -1, 3) \sim (1, -1, 6) \sim (1, 1, 6)$.

2 Algebraïsche getaltheorie

In dit hoofdstuk bekijken we een heel ander veld in de wiskunde: de algebraïsche getaltheorie. Het blijkt namelijk dat er een een-op-een relatie is tussen de kwadratische vormen uit het vorige hoofdstuk en idealen van kwadratische uitbreidingen van $\mathbb{Q}$. Er worden een aantal resultaten uit de algebraïsche getaltheorie gebruikt die wegens de lengte en het niveau van deze scriptie niet bewezen zullen worden. In dit hoofdstuk volgen we weer in grote lijnen de aanpak van Buell [3].

2.1 Kwadratische uitbreidingen

Definitie 2.1. *Een kwadratisch algebraïsch getal is een complex getal α dat $f(x) = 0$ oplost, waarbij f een kwadratisch polynoom met coëfficiënten in $\mathbb{Z}$ is.*
Een kwadratisch algebraïsche gehele (of integer) is een complex getal α dat $f(x) = 0$ oplost, waarbij f een monisch kwadratisch polynoom met coëfficiënten in $\mathbb{Z}$ is.

Merk op dat, met behulp van de abc-formule, alle kwadratische algebraïsche getallen te schrijven zijn als $\alpha = \frac{-b\pm\sqrt{b^2-4ac}}{2a} = \frac{-b+e\sqrt{d}}{2a}$ met $a, b, c, d, e \in \mathbb{Z}$, waarbij d geen kwadratische factoren heeft. We zeggen dat d de radicand is van α. Het is duidelijk dat $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d}) = \{t + u\sqrt{d} \mid t, u \in \mathbb{Q}\}$.

Stelling 2.1. *Zij d een kwadraatvrij geheel getal. De ring van gehelen van $\mathbb{Q}(\sqrt{d})$, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, kortweg $\mathcal{O}(\sqrt{d})$, wordt gegeven door:*

$$\mathcal{O}(\sqrt{d}) = \begin{cases} \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} & \text{als } d \equiv 2, 3 \ (mod\ 4) \\ \{\frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \ (mod\ 2)\} & \text{als } d \equiv 1 \ (mod\ 4) \end{cases}$$

Bewijs
Uit bovenstaande opmerkingen volgt dat α een kwadratische algebraïsche gehele is, d.e.s.d.a. $\alpha = \frac{-b+e\sqrt{d}}{2}$ met $b^2 - 4c = e^2 d$. Bekijk deze vergelijking modulo 4 en bedenk dat $a^2 \equiv 0, 1 \pmod 4$, als a even, respectievelijk oneven is. Als $d \equiv 2, 3 \pmod 4$, dan moet dus gelden dat b en e even zijn, waaruit het gevraagde volgt. Als $d \equiv 1 \pmod 4$, dan volgt hieruit dat b en e van dezelfde pariteit zijn.
Merk ook op dat dit een ring is. Dit volgt uit het feit dat deze verzameling gesloten is onder vermenigvuldiging en optelling en uit de gebruikelijke eigenschappen van vermenigvuldiging en optelling. □

Definieer nu de discriminant Δ van een kwadratische uitbreiding als

$$\Delta = \begin{cases} 4d & \text{als } d \equiv 2, 3 \pmod 4 \\ d & \text{als } d \equiv 1 \pmod 4 \end{cases}$$

Merk hierbij op dat $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\Delta})$. Definieer verder de geconjugeerde van $\alpha = a + b\sqrt{d}$ als $\bar{\alpha} = a - b\sqrt{d}$. De norm van een element α wordt gedefinieerd door $N(\alpha) = \alpha\bar{\alpha} = \left(\frac{-b+e\sqrt{d}}{2a}\right)\left(\frac{-b-e\sqrt{d}}{2a}\right) = \frac{b^2-e^2 d}{4a^2}$. Merk op dat, wegens dezelfde argumenten als in bovenstaand bewijs, voor een algebraïsche gehele α geldt dat $N(\alpha) \in \mathbb{Z}$. Daarnaast geldt dat als $d < 0$, dan $N(\alpha) > 0$ voor alle $\alpha \in \mathbb{Q}(\sqrt{d})$. Definieer verder de Trace-functie als $\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha}$. De Trace-functie stuurt $\alpha = a + b\sqrt{d}$ dus naar $2a$.

2.2 Idealen in $\mathcal{O}(\sqrt{d})$

In deze paragraaf worden veel definities en resultaten gegeven over de idealen in $\mathcal{O}(\sqrt{d})$. Uiteindelijk heb je ze allemaal nodig voor de belangrijke stelling uit de volgende paragraaf. Begin met de gebruikelijke definities voor idealen, die je al zult kennen.

Definitie 2.2. *Gegeven R een ring. Dan is $I \subset R$ een ideaal in R als $\forall i_1, i_2 \in I, r_1, r_2 \in R$: $r_1 i_1 + r_2 i_2 \in I$.*
I is een hoofdideaal in R als $I = \{r\alpha \mid r \in R\} = (\alpha)$ met $\alpha \in R$.
Zij I, J twee idealen in R. Dan wordt het productideaal gegeven door $IJ = \{i_1 j_1 + \ldots + i_n j_n \mid i_1, \ldots, i_n \in I, j_1, \ldots, j_n \in J\}$.

Nu definiëren we wat een gebroken ideaal is voor $\mathcal{O}(\sqrt{d})$.

Definitie 2.3. *Een gebroken ideaal I is een verzameling $I \subset \mathbb{Q}(\sqrt{d})$, zodat*

- $\forall i_1, i_2 \in I, r_1, r_2 \in \mathcal{O}(\sqrt{d}) : r_1 i_1 + r_2 i_2 \in I$.
- $\exists r \in \mathcal{O}(\sqrt{d}) : \forall i \in I, ri \in \mathcal{O}(\sqrt{d})$

De volgende stellingen zijn specifieke gevallen van algemene stellingen in de algebraïsche getaltheorie. Ze zullen niet bewezen worden in deze scriptie.

Stelling 2.2. *Zij I een ideaal in $\mathcal{O}(\sqrt{d})$. Dan zijn er $\alpha, \beta \in \mathcal{O}(\sqrt{d})$, zodat elk element van I geschreven kan worden als $\alpha x + \beta y$ met $x, y \in \mathbb{Z}$. Schrijf $I = [\alpha, \beta]$.*

Merk op dat uit deze stelling volgt dat een gebroken ideaal te schrijven is als $I = [\frac{\alpha}{r}, \frac{\beta}{r}]$ met $\alpha, \beta \in \mathcal{O}(\sqrt{d})$. Daarnaast geldt dat, gegeven $I = [i_1, i_2]$, $J = [j_1, j_2]$ twee idealen in $\mathcal{O}(\sqrt{d})$, IJ bestaat uit alle $\mathbb{Z}$-lineaire combinaties van $i_1 j_1$, $i_1 j_2$, $i_2 j_1$ en $i_2 j_2$.
Bovenstaande stelling kan echter nog sterker. Stel namelijk dat $I = [\alpha, \beta]$, dan geldt er duidelijk dat $I = [\alpha, \alpha + \beta]$. Schrijf $\alpha = a_1 + a_2\sqrt{d}$ en $\beta = b_1 + b_2\sqrt{d}$ met a_1, a_2, b_1, b_2 geheel of een geheel getal gedeeld door twee, afhankelijk van d. Dan kunnen we nu het Euclidisch algoritme toepassen op a_2 en b_2, waardoor een van de twee wegvalt. We kunnen I dus schrijven als $I = [a, b + g\sqrt{d}]$. Het blijkt nu zelfs zo te zijn dat g zowel a als b deelt. Dit geeft de volgende stelling:

Stelling 2.3. *Zij I een ideaal in $\mathcal{O}(\sqrt{d})$. Dan is $I = [a, b + g\sqrt{d}]$, met $a, b, g \in \mathbb{Z}$ als $d \equiv 2, 3 \pmod 4$ en $a, 2b, 2g \in \mathbb{Z}$ als $d \equiv 1 \pmod 4$. Verder geldt dat $g|a$ en $g|b$.*

Wanneer je deze basis hebt aangenomen, kun je bewijzen dat er een c bestaat, zodat $d = (b')^2 - a'c$ als $d \equiv 2, 3 \pmod 4$, met $b' = \frac{b}{g}$ en $a' = \frac{a}{g}$. Er geldt namelijk dat $[a, b + g\sqrt{d}] = (g)[a', b' + \sqrt{d}]$ een ideaal is in $\mathcal{O}(\sqrt{d})$, waardoor $[a', b' + \sqrt{d}]$ ook een ideaal in $\mathcal{O}(\sqrt{d})$ is. Dit betekent dat $(b')^2 - d = (b' + \sqrt{d})(b' - \sqrt{d})$ een element is van dit ideaal. Er zijn dus $c, e \in \mathbb{Z}$, zodat $a'c + (b' + \sqrt{d})e = (b')^2 - d$. Omdat in de laatste term geen factoren $\sqrt{d}$ zitten, moet gelden dat $e = 0$, waardoor $d = (b')^2 - a'c$. Als $d \equiv 1 \pmod 4$, dan geldt dat $[a, \frac{b+g\sqrt{d}}{2}] = (g)[a', \frac{b'+\sqrt{d}}{2}]$ een ideaal is in $\mathcal{O}(\sqrt{d})$, waardoor $[a', \frac{b'+\sqrt{d}}{2}]$ dit ook is. Nu geldt dat $\frac{(b')^2 - d}{4} = \frac{b'+\sqrt{d}}{2}\frac{b'-\sqrt{d}}{2}$ een element is van dit ideaal. Wegens een hetzelfde argument als hierboven geldt dat $\frac{(b')^2 - d}{4} = a'c$, waardoor $d = (b')^2 - 4a'c$. Deze feiten hebben we in de volgende paragraaf nodig.

Nu we idealen kunnen schrijven als $I = [\alpha, \beta]$, kunnen we een norm-functie op deze idealen definiëren. Doe dit als volgt.

Definitie 2.4. *Zij $I = [\alpha, \beta]$ een ideaal. Door α en β te verwisselen, kunnen we eisen dat $\frac{\alpha\bar{\beta}-\bar{\alpha}\beta}{\sqrt{\Delta}} > 0$. Noem dit ideaal georiënteerd. Definieer de norm van het georiënteerde ideaal I als $N(I) = \frac{\alpha\bar{\beta}-\bar{\alpha}\beta}{\sqrt{\Delta}}$.*

De volgende stelling wordt nuttig als we equivalentieklassen gaan definiëren op gebroken idealen. Deze equivalentieklassen worden gebruikt om een groepstructuur op de gebroken idealen te definiëren, welke isomorf blijkt te zijn aan de groep op de kwadratische vormen.

Stelling 2.4. *Zij I een ideaal in $\mathcal{O}(\sqrt{d})$. Dan is er een ideaal J in $\mathcal{O}(\sqrt{d})$, zó dat het productideaal IJ een hoofdideaal is.*

Definitie 2.5. *Gegeven twee gebroken idealen I, J in $\mathcal{O}(\sqrt{d})$. Dan zijn ze equivalent als er een hoofdideaal (α) bestaat met $\alpha \in \mathbb{Q}(\sqrt{d}), \alpha \neq 0$, zó dat $I = (\alpha)J$.*

Dit is duidelijk een equivalentie relatie:

- De relatie is reflexief, want $I = (1)I$
- De relatie is symmetrisch, want als $I = (\alpha)J$, $(\alpha \neq 0)$, dan $J = (\frac{1}{\alpha})I$. Bedenk hierbij dat $\mathbb{Q}(\sqrt{d})$ een lichaam is.
- De relatie is transitief, want als $I = (\alpha)J$ en $J = (\beta)K$, dan $I = (\alpha\beta)K$.

Verder geldt dat als I, J equivalent zijn, dan zijn IK en JK dat ook. Ook de omgekeerde implicatie geldt, als je er daarbij vanuit gaat dat K niet het nulideaal is. Deze opmerking, samen met stelling 3, is voldoende om de volgende conclusie te trekken.

Stelling 2.5. *De equivalentieklassen van gebroken idealen in $\mathcal{O}(\sqrt{d})$, zonder het nulideaal, vormen een groep onder de vermenigvuldiging van idealen. Hierbij is de identiteit de klasse met alle hoofdidealen. De inverse van een ideaal I is het ideaal J, zó dat IJ een hoofdideaal is. Deze groep, $\mathcal{C}(\mathcal{O}(\sqrt{\Delta}))$, heet de ideaal-klassegroep van discriminant Δ.*

2.3 Het verband met kwadratische vormen

We bewijzen nu dat $\mathcal{C}(\Delta)$, de klassegroep van discriminant Δ en $\mathcal{C}(\mathcal{O}(\sqrt{\Delta}))$, de ideaal-klassegroep (van dezelfde discriminant Δ) isomorf zijn. Dit doen we voor het geval dat $\Delta < 0$. Op het moment dat $\Delta > 0$, blijkt dat er (in bepaalde gevallen) geen isomorfisme is tussen $\mathcal{C}(\Delta)$ en $\mathcal{C}(\mathcal{O}(\sqrt{\Delta}))$. Je kunt dan echter een strikte equivalentie tussen de gebroken idealen in $\mathcal{O}(\sqrt{\Delta})$ definiëren, die hetzelfde is als de vorige equivalentie, maar waarbij ook nog wordt geëist dat $N(\alpha) > 0$, dus $I \sim J$ als $I = (\alpha)J$ en $N(\alpha) > 0$. De klassegroep die je dan krijgt, $\mathcal{C}^+(\mathcal{O}(\sqrt{\Delta}))$, is weer isomorf aan $\mathcal{C}(\Delta)$ en het isomorfisme is hetzelfde. Dit geval zullen we echter niet bewijzen in deze scriptie.

Stelling 2.6. *Zij $\Delta \in \mathbb{Z}_{<0}$. De afbeelding $\phi : \mathcal{C}(\Delta) \to \mathcal{C}(\mathcal{O}(\sqrt{\Delta}))$, gegeven door $[(a, b, c)] \mapsto \left[[a, \frac{-b+\sqrt{\Delta}}{2}]\right]$, is een groepsisomorfisme.*

Bewijs
Allereerst bewijzen we dat deze afbeelding welgedefinieerd is. Herinner je uit hoofdstuk 1 dat twee equivalente vormen altijd in een eindig aantal transformaties onder matrix S, T in elkaar over gaan. Dit betekent dat het voldoende is om te bewijzen dat ϕ kwadratische vormen equivalent onder matrix S, respectievelijk T naar equivalente idealen stuurt. Matrix S transformeert (a, b, c) naar $(a, b + 2a, a + b + c)$. Er geldt dat

$$\phi\left([(a, b + 2a, a + b + c)]\right) = \left[[a, \frac{-b + \sqrt{\Delta}}{2} - a]\right] = \left[[a, \frac{-b + \sqrt{\Delta}}{2}]\right] = \phi\left([(a, b, c)]\right).$$

Onder matrix T gaat (a,b,c) over in $(c,-b,a)$. Hiervoor geldt dat

$$\phi\left([(c,-b,a)]\right) = \left[[c, \frac{b+\sqrt{\Delta}}{2}]\right] = \left[[\frac{b^2-\Delta}{4a}, \frac{b+\sqrt{\Delta}}{2}]\right] = \left[[-\frac{b+\sqrt{\Delta}}{2a}\frac{-b+\sqrt{\Delta}}{2}, \frac{b+\sqrt{\Delta}}{2}]\right]$$
$$= \left[\left(\frac{b+\sqrt{\Delta}}{2a}\right)[a, \frac{-b+\sqrt{\Delta}}{2}]\right] = \left[[a, \frac{-b+\sqrt{\Delta}}{2}]\right] = \phi\left([(a,b,c)]\right).$$

We concluderen dat ϕ equivalente kwadratische vormen naar dezelfde equivalentieklasse van gebroken idealen in $\mathcal{O}(\sqrt{\Delta})$ stuurt en dus welgedefinieerd is.

Zij $I = [\alpha, \beta]$ een ideaal. Door α en β eventueel te verwisselen, kunnen we eisen dat I een georiënteerd ideaal is. De inverse van ϕ wordt nu gegeven door $\psi : \mathcal{C}(\mathcal{O}(\sqrt{\Delta})) \to \mathcal{C}(\Delta), [I] = [[\alpha,\beta]] \mapsto \left[\frac{N(\alpha)x^2+\mathrm{Tr}(\alpha\bar{\beta})xy+N(\beta)y^2}{N(I)}\right]$. We bewijzen allereerst dat equivalente idealen naar dezelfde kwadratische vorm worden afgebeeld. Vervolgens bewijzen we dat het polynoom een element is van $\mathcal{C}(\Delta)$, door te bewijzen dat zijn coëfficiënten geheel zijn en zijn discriminant gelijk is aan Δ. Als laatste bewijzen we dat ψ daadwerkelijk de inverse is van ϕ.
Stel dat $I = [\alpha,\beta]$, $J = [\alpha',\beta']$ en $I \sim J$. Dan is er een $\lambda \in \mathbb{Q}(\sqrt{\Delta})$, zodat $I = (\lambda)J$, dus $J = [\lambda\alpha, \lambda\beta]$. Merk nu op dat $N(J) = N(\lambda)N(I)$, waardoor J naar $\left[\frac{N(\lambda)N(\alpha)x^2+\mathrm{Tr}(N(\lambda)\alpha\bar{\beta})xy+N(\lambda)N(\beta)y^2}{N(\lambda)N(I)}\right]$ wordt afgebeeld. De factor $N(\lambda)$ kunnen we boven en onder de deelstreep wegstrepen. We concluderen dat de afbeeldingen van I en J gelijk zijn. Wat we ook moeten bewijzen is dat de $\psi([I])$ onafhankelijk is van de basis van I. Stel namelijk $I = [\alpha,\beta]$, dan is niet gegeven dat α, β uniek zijn. Stel daarom dat $I = [\alpha,\beta] = [\tilde{\alpha},\tilde{\beta}]$. Er moet nu wel gelden dat $\tilde{\alpha} = r\alpha + s\beta$ en $\tilde{\beta} = t\alpha + u\beta$, met $r,s,t,u \in \mathbb{Z}$, omdat ze allebei element van I zijn. Omdat deze transformatie inverteerbaar moet zijn (er zijn ook $r',s',t',u' \in \mathbb{Z}$, zodat $\alpha = r'\tilde{\alpha} + s'\tilde{\beta}$ en $\beta = t'\tilde{\alpha} + u'\tilde{\beta}$), moet gelden dat $ru - st = \pm 1$. Omdat beide idealen georiënteerd zijn, volgt dat $ru - st = 1$. Berekenen we nu $N(\tilde{\alpha})$, $\mathrm{Tr}(\tilde{\alpha}\bar{\tilde{\beta}})$ en $N(\tilde{\beta})$, dan vinden we dat $N(\tilde{\alpha}) = r^2N(\alpha) + rs\mathrm{Tr}(\alpha\bar{\beta}) + s^2N(\beta)$, $\mathrm{Tr}(\tilde{\alpha}\bar{\tilde{\beta}}) = 2(rtN(\alpha) + (ru+st)\mathrm{Tr}(\alpha\bar{\beta}) + suN(\beta))$ en $N(\tilde{\beta}) = t^2N(\alpha) + tu\mathrm{Tr}(\alpha\bar{\beta}) + u^2N(\tilde{\beta})$. Dit betekent dat $[\tilde{\alpha},\tilde{\beta}]$ naar de kwadratische vorm $\left[\frac{N(\tilde{\alpha})x^2+\mathrm{Tr}(\tilde{\alpha}\bar{\tilde{\beta}})xy+N(\tilde{\beta})y^2}{N(I)}\right] = \left[\frac{N(\alpha)(rx+ty)^2+\mathrm{Tr}(\alpha\bar{\beta})(rx+ty)(sx+uy)+N(\beta)(sx+uy)^2}{N(I)}\right]$ wordt gestuurd. Deze kwadratische vorm is via de matrix $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ equivalent aan de kwadratische vorm waar $[\alpha,\beta]$ heen wordt gestuurd. De afbeelding $\psi(I)$ is dus onafhankelijk van de basis van I.

We bewijzen nu dat de coëfficiënten geheel zijn. Zij I een gebroken ideaal in $\mathcal{O}(\sqrt{\Delta}) = \mathcal{O}(\sqrt{d})$. Volgens een stelling uit de vorige paragraaf geldt dat $I = [a, b+g\sqrt{d}] = (a)[1, \frac{b+g\sqrt{d}}{a}] = (a)[1, \frac{b'+\sqrt{d}}{a'}]$, waarbij $a' = \frac{a}{g}$ en $b' = \frac{b}{g}$ geheel zijn. In de vorige paragraaf zagen we ook dat als $d \equiv 2,3 \pmod 4$, er een $c \in \mathbb{Z}$ bestond, zodat $d = (b')^2 - a'c$. Dan is $\Delta = 4d = (2b')^2 - 4a'c$ en $I = (a)[1, \frac{b'+\sqrt{d}}{a'}] = (a)[1, \frac{2b'+\sqrt{\Delta}}{2a'}] = (a)[1,\tau]$. Er geldt dat $N(\tau) = N(\frac{2b'+\sqrt{\Delta}}{2a'}) = \frac{(2b')^2-(2b')^2+4a'c}{(2a')^2} = \frac{c}{a'}$, $\mathrm{Tr}(\tau) = \mathrm{Tr}(\frac{2b'+\sqrt{\Delta}}{2a'}) = \frac{2b'}{a'}$ en $N([1,\tau]) = N([1, \frac{2b'+\sqrt{\Delta}}{2a'}]) = \frac{1}{a'}$. Als $d \equiv 1 \pmod 4$, dan geldt dat $\Delta = d = b'^2 - 4a'c$ met $c \in \mathbb{Z}$. Dat betekent dat $I = (a)[1, \frac{b'+\sqrt{\Delta}}{2a'}] = (a)[1,\tau]$, waarbij $N(\tau) = N(\frac{b'+\sqrt{\Delta}}{a'}) = \frac{(b')^2-(b')^2+4a'c}{(2a')^2} = \frac{c}{a'}$, $\mathrm{Tr}(\tau) = \mathrm{Tr}(\frac{b'+\sqrt{\Delta}}{2a'}) = \frac{b'}{a'}$ en $N([1,\tau]) = N([1, \frac{b'+\sqrt{\Delta}}{2a'}]) = \frac{1}{a'}$. I wordt dus afgebeeld op het polynoom $\left[\frac{x^2+\mathrm{Tr}(\tau)xy+N(\tau)y^2}{N([1,\tau])}\right]$, welke gehele coëfficiënten heeft.

Merk ook op dat een willekeurig gebroken ideaal in $\mathcal{O}(\sqrt{\Delta})$ ook daadwerkelijk naar een kwadratisch polynoom van discriminant Δ wordt gestuurd. Er geldt namelijk dat $\mathrm{Tr}(\alpha\beta)^2 - 4N(\alpha)N(\beta) = (\alpha^2\bar{\beta}^2 + 2\alpha\bar{\alpha}\beta\bar{\beta} + \bar{\alpha}^2\beta^2) - 4\alpha\bar{\alpha}\beta\bar{\beta} = (\alpha\bar{\beta} - \bar{\alpha}\beta)^2 = N([\alpha,\beta])^2\Delta$, waardoor $B^2 - 4AC = \left(\frac{\mathrm{Tr}(\alpha\beta)}{N([\alpha,\beta])}\right)^2 - \frac{4N(\alpha)N(\beta)}{N([\alpha,\beta])^2} = \Delta$

We bewijzen nu dat de functies daadwerkelijk elkaars inverse zijn. $[(a,b,c)]$ wordt door ϕ naar $[a, \frac{-b+\sqrt{b^2-4ac}}{2}] \sim [1, \frac{-b+\sqrt{b^2-4ac}}{2a}]$ gestuurd. Er geldt dat $N(\frac{-b+\sqrt{b^2-4ac}}{2a}) = \frac{c}{a}$, $\mathrm{Tr}(\frac{-b+\sqrt{b^2-4ac}}{2a}) = -\frac{b}{a}$ en $N([1, \frac{-b+\sqrt{b^2-4ac}}{2a}]) = \frac{1}{a}$. Het ideaal moet worden geordend als $[\frac{-b+\sqrt{b^2-4ac}}{2a}, 1]$, waardoor deze naar $[(c,-b,a)] = [(a,b,c)]$ gestuurd wordt. ψ stuurt een ideaal $[\alpha,\beta]$ naar de kwadratische vorm $\left[\frac{N(\alpha)x^2+\mathrm{Tr}(\alpha\bar{\beta})xy+N(\beta)y^2}{N([\alpha,\beta])}\right]$. Deze wordt door ϕ juist afgebeeld op $\left[[\frac{N(\alpha)}{N([\alpha,\beta])}, \frac{-\frac{\mathrm{Tr}(\alpha\bar{\beta})}{N([\alpha,\beta])}+\sqrt{\Delta}}{2}]\right] = \left[[\frac{\alpha\bar{\alpha}}{N([\alpha,\beta])}, \frac{\left(1-\frac{\alpha\bar{\beta}+\bar{\alpha}\beta}{\alpha\bar{\beta}-\bar{\alpha}\beta}\right)\sqrt{\Delta}}{2}]\right] = \left[[\frac{\alpha\bar{\alpha}}{N([\alpha,\beta])}, \frac{\bar{\alpha}\beta}{N([\alpha,\beta])}]\right] = \left[\left(\frac{\bar{\alpha}}{N([\alpha,\beta])}\right)[\alpha,\beta]\right]$. We concluderen dat $\phi(\psi([[\alpha,\beta]])) = [[\alpha,\beta]]$ en dat ϕ en ψ elkaars inverse zijn.

Tot nu toe hebben we bewezen dat ϕ welgedefinieerd is. Daarnaast volgt uit de welgedefinieerdheid van de inverse ψ dat de afbeelding ϕ zowel injectief (anders waren er twee idealen met dezelfde kwadratische vorm), als surjectief (anders was er een ideaal zonder kwadratische vorm) is. Om van een groepsisomorfisme te mogen spreken moet nog gelden dat $\phi(x) \circ \phi(y) = \phi(x \circ y)$. Vanwege onze definitie van de compositie van kwadratische vormen is het voldoende om twee kwadratische vormen van de vorm (a_1, B, Ca_2), respectievelijk (a_2, B, Ca_1) (met $\mathrm{ggd}(a_1, a_2, B) = 1$) te vermenigvuldigen en te laten zien dat de bijbehorende idealen gelijk zijn. We hebben gedefinieerd dat $(a_1, B, Ca_2) \circ (a_2, B, Ca_1) = (a_1a_2, B, C)$. We moeten dus bewijzen dat $[a_1, \frac{-B+\sqrt{\Delta}}{2}][a_2, \frac{-B+\sqrt{\Delta}}{2}] = [a_1a_2, \frac{-B+\sqrt{\Delta}}{2}]$. Volgens de definitie van ideaalvermenigvuldiging geldt dat $[a_1, \frac{-B+\sqrt{\Delta}}{2}][a_2, \frac{-B+\sqrt{\Delta}}{2}] = [a_1a_2, a_1\frac{-B+\sqrt{\Delta}}{2}, a_2\frac{-B+\sqrt{\Delta}}{2}, \frac{-B+\sqrt{\Delta}}{2}\frac{-B+\sqrt{\Delta}}{2}]$. Omdat $\frac{-B+\sqrt{\Delta}}{2}\frac{-B+\sqrt{\Delta}}{2} = \frac{B^2-2B\sqrt{\Delta}+\Delta}{4} = \frac{2B^2-2B\sqrt{\Delta}-4a_1a_2C}{4} = -B\frac{-B+\sqrt{\Delta}}{2} - a_1a_2C$ en $\mathrm{ggd}(a_1, a_2, B) = 1$, is het duidelijk dat de gelijkheid geldt. Er is immers een $\mathbb{Z}$-lineaire combinatie zodat $a_1t + a_2u + Bv = 1$. Hiermee is het bewijs geleverd dat de compositie behouden blijft onder ϕ. ϕ is een groepsisomorfisme en $\mathcal{C}(\Delta)$ en $\mathcal{C}(\mathcal{O}(\sqrt{\Delta}))$ zijn isomorf voor $\Delta < 0$. □

Een laatste opmerking gaat over het compositiealgoritme van Arndt binnen deze idealen. Dit is niet meer noodzakelijk voor het bovenstaande bewijs, maar hebben we nodig voor het laatste hoofdstuk van deze scriptie. Herinner je dat, gegeven $f_1 = (a_1, b_1, c_1)$ en $f_2 = (a_2, b_2, c_2)$, geldt dat $f_1 \circ f_2 = (A, B, \frac{\Delta - B^2}{4A})$. Hierbij is $A = \frac{a_1a_2}{n^2}$ en $B = \frac{2a_1b_2t + 2a_2b_1u + v(b_1b_2+\Delta)}{2n}$, waarbij $\beta = \frac{b_1+b_2}{2}$, $n = \mathrm{ggd}(a_1, a_2, \beta)$ en $t, u, v \in \mathbb{Z}$ zó dat $a_1t + a_2u + \beta v = n$. We bewijzen nu dat $[a_1, \frac{-b_1+\sqrt{\Delta}}{2}][a_2, \frac{-b_2+\sqrt{\Delta}}{2}] = [\frac{a_1a_2}{n}, n\frac{-B+\sqrt{\Delta}}{2}]$. Merk op dat hierbij een $=$-teken staat en niet een $\sim$-teken. We bewijzen dus gelijkheid en niet equivalentie. Equivalentie volgt namelijk al uit het compositiealgoritme van Arndt samen met het feit dat $[\frac{a_1a_2}{n}, n\frac{-B+\sqrt{\Delta}}{2}] = (n)[\frac{a_1a_2}{n^2}, \frac{-B+\sqrt{\Delta}}{2}]$. Er geldt dat $N\left(\frac{a_1a_2}{n}, n\frac{-B+\sqrt{\Delta}}{2}]\right) = a_1a_2 = N\left([a_1, \frac{-b_1+\sqrt{\Delta}}{2}]\right) N\left([a_2, \frac{-b_2+\sqrt{\Delta}}{2}]\right) = N\left([a_1, \frac{-b_1+\sqrt{\Delta}}{2}][a_2, \frac{-b_2+\sqrt{\Delta}}{2}]\right)$. Het is daarom voldoende om te bewijzen dat $[a_1, \frac{-b_1+\sqrt{\Delta}}{2}][a_2, \frac{-b_2+\sqrt{\Delta}}{2}] \subseteq [\frac{a_1a_2}{n}, n\frac{-B+\sqrt{\Delta}}{2}]$. Dit kunnen we expliciet uitrekenen. Zo geldt er duidelijk dat $a_1a_2 = \frac{a_1a_2}{n}n$. Merk verder op dat $\frac{a_1}{n}\frac{b_1b_2+\Delta}{2n} = \frac{a_1}{n}\frac{b_1b_2+b_2^2-4a_2c_2}{2n} \equiv$

$\frac{b_1+b_2}{2n}\frac{a_1}{n}b_2 \pmod{\frac{2a_1a_2}{n^2}}$, waardoor

$$\frac{a_1}{n}B = \frac{2a_1^2b_2t}{2n^2}+\frac{2a_1a_2b_1u}{2n^2}+\frac{a_1}{n}\frac{v(b_1b_2+\Delta)}{2n} \equiv \left(\frac{a_1}{n}t+\frac{a_2}{n}u+\frac{b_1+b_2}{2n}v\right)\frac{a_1}{n}b_2 \equiv \frac{a_1}{n}b_2 \pmod{\frac{2a_1a_2}{n^2}}.$$

Zij $m_1 \in \mathbb{Z}$ nu zodat $\frac{a_1}{n}B = \frac{a_1}{n}b_2 + \frac{2a_1a_2}{n^2}m_1$ en $m_2 = \frac{a_1}{n}$. Dan geldt dat $m_1\frac{a_1a_2}{n} + m_2 n\frac{-B+\sqrt{\Delta}}{2} = m_1\frac{a_1a_2}{n} + a_1\frac{-b_2+\sqrt{\Delta}}{2} - \frac{n}{2}\frac{2a_1a_2}{n^2}m_1 = a_1\frac{-b_2+\sqrt{\Delta}}{2}$. Analoog is er een $\mathbb{Z}$-lineaire combinatie van $\frac{a_1a_2}{n}$ en $n\frac{-B+\sqrt{\Delta}}{2}$, zodat deze gelijk is aan $a_2\frac{-b_1+\sqrt{\Delta}}{2}$ of $\frac{-b_1+\sqrt{\Delta}}{2}\frac{-b_2+\sqrt{\Delta}}{2}$. Gebruik hierbij voor de laatste gelijkheid dat $a_1\Delta \equiv a_1b_2^2 \pmod{\frac{2a_1a_2}{n^2}}$ en $a_2\Delta \equiv a_2b_1^2 \pmod{\frac{2a_1a_2}{n^2}}$. Hiermee is dus bewezen dat $[a_1, \frac{-b_1+\sqrt{\Delta}}{2}][a_2, \frac{-b_2+\sqrt{\Delta}}{2}] \subseteq [\frac{a_1a_2}{n}, n\frac{-B+\sqrt{\Delta}}{2}]$ en omdat de normen gelijk zijn, hebben we dat $[a_1, \frac{-b_1+\sqrt{\Delta}}{2}][a_2, \frac{-b_2+\sqrt{\Delta}}{2}] = [\frac{a_1a_2}{n}, n\frac{-B+\sqrt{\Delta}}{2}]$.

2.4 Bijvoorbeeld

In de laatste paragraaf van elk hoofdstuk wordt een voorbeeld bekeken, waarbij de theorie van dat hoofdstuk wordt behandeld. Neem $\Delta = -23$ als vaste discriminant van onze kwadratische vormen. Deze heeft drie equivalentieklassen, gegeven door de representanten $(1,1,6)$, $(2,1,3)$ en $(2,-1,3)$. Deze worden door ϕ naar de gebroken idealen $[1, \frac{-1+\sqrt{-23}}{2}]$,$[2, \frac{-1+\sqrt{-23}}{2}]$ en $[2, \frac{1+\sqrt{-23}}{2}]$ van $\mathcal{O}(\sqrt{-23})$ gestuurd. We berekenen $[2, \frac{-1+\sqrt{-23}}{2}][2, \frac{1+\sqrt{-23}}{2}]$ en laten zien dat deze equivalent is aan $[1, \frac{-1+\sqrt{-23}}{2}]$. Dit is dus dezelfde berekening als we vorig hoofdstuk gedaan hebben, maar dan in de ideaaltheorie. Er geldt dat

$$\begin{aligned}[2, \frac{-1+\sqrt{-23}}{2}][2, \frac{1+\sqrt{-23}}{2}] &= [4, 1+\sqrt{-23}, -1+\sqrt{-23}, -6] = [-2, 1+\sqrt{-23}, -2, -6] \\ &= [2, 1+\sqrt{-23}] = (2)[1, \frac{1+\sqrt{-23}}{2}].\end{aligned}$$

Merk op dat we dit ook vinden als we het compositiealgoritme van Arndt gebruiken om een gelijk ideaal te vinden. We hadden dat $\beta = \frac{b_1+b_2}{2} = 0$, $n = \text{ggd}(a_1, a_2, \beta) = 2$ en t, u, v, zodat $2t + 2u = 2$, waardoor $t = 1$ en $u = v = 0$, dus $B = \frac{2a_1b_2t+2a_2b_1u+v(b_1b_2+\Delta)}{2n} = -1$. We hebben laten zien dat $[a_1, \frac{-b_1+\sqrt{\Delta}}{2}][a_2, \frac{-b_2+\sqrt{\Delta}}{2}] = [\frac{a_1a_2}{n}, n\frac{-B+\sqrt{\Delta}}{2}]$, dus daaruit volgt inderdaad dat

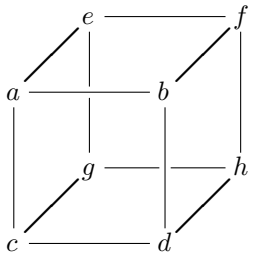
$$[2, \frac{-1+\sqrt{-23}}{2}][2, \frac{1+\sqrt{-23}}{2}] = [2, 1+\sqrt{-23}]$$

.

3 Bhargavakubussen

3.1 Introductie tot de kubus

Zoals we in hoofdstuk 1 2×2 matrices aan kwadratische vormen associeerde, is het doel van dit en het volgende hoofdstuk om $2 \times 2 \times 2$ kubussen aan kubische vormen te associëren. We bekijken daarom de ruimte $\mathcal{C}_2 = \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. Deze kunnen we representeren door kubussen met gehele coëfficiënten op de hoekpunten:



Zoals we in hoofdstuk 1 aannamen dat de niet-diagonaal elementen gelijk waren en daardoor de matrix associeerde met een kwadratische vorm, zo zullen we in hoofdstuk 4 aannemen dat $b = c = e$ en $d = f = g$ en daarmee de kubus associëren met een kubische vorm. Merk op dat in hoofdstuk 1 de niet-diagonaal elementen gegeven waren door $\frac{b}{2}$. In hoofdstuk 4 zullen we blijven aannemen dat we in $\mathcal{C}_2$ werken (dus met gehele getallen op de hoekpunten), waardoor we alleen uitspraken kunnen doen over de kubische vormen van de vorm $ax^3 + 3bx^2y + 3cxy^2 + dy^3$. Voor het echter zover is, zullen we in dit hoofdstuk algemene eigenschappen van de zogeheten Bhargavakubus bewijzen en zullen we dus nog niet aannemen dat $b = c = e$ en $d = f = g$. Bhargava introduceerde deze kubussen in een paper in 2004 [1] en scheen hiermee een nieuw licht op verschillende composities, waarbij wij dus geïnteresseerd zijn in de compositie van kubische vormen. Daarvoor moeten echter eerst de algemene Bhargavakubussen en zijn verschillende eigenschappen geïntroduceerd worden. In dit hoofdstuk volgen we logischerwijs de ideeën en bewijzen van Bhargava [1], maar daarbij gebruik ik ook de iets gedetailleerdere aanpak van Bouyer [2].

3.2 Equivalentieklassen

Gegeven een kubus $A \in \mathcal{C}_2$. Dan kun je deze kubus op drie verschillende manieren opsplitsen in twee 2×2 matrices. Zo kun je de boven- en onderkant scheiden, evenals de voor- en achterkant en de linker- en rechterkant. Dit geeft de volgende drie partities in matrices:

- $M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$
- $M_2 = \begin{pmatrix} a & c \\ e & g \end{pmatrix}, N_2 = \begin{pmatrix} b & d \\ f & h \end{pmatrix}$
- $M_3 = \begin{pmatrix} a & e \\ b & f \end{pmatrix}, N_3 = \begin{pmatrix} c & g \\ d & h \end{pmatrix}$

Zij $\Gamma = SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$. Definieer nu een actie van Γ op $\mathcal{C}_2$ als volgt: in de i-de factor, $1 \leq i \leq 3$, stuurt de matrix $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})$ het paar $\begin{pmatrix} M_i \\ N_i \end{pmatrix}$ naar het paar

$\begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} M_i \\ N_i \end{pmatrix} = \begin{pmatrix} rM_i + sN_i \\ tM_i + uN_i \end{pmatrix}$. Je vervangt dus eerst de voor- en achterkant. Vervolgens vervang je de linker- en rechterkant, waarbij je de nieuwe waarden van de hoekpunten gebruikt die je bij de eerste vervanging gevonden hebt. Als laatste vervang je de boven- en onderkant. De acties van de aparte factoren van Γ commuteren met elkaar. Het maakt niet uit of je eerst de voor- en achterkant vervangt en vervolgens de linker- en rechterkant of andersom. Dit is analoog aan feit dat lineaire operaties op rijen en kolommen van matrices met elkaar commuteren. Gegeven $\gamma = \gamma_1 \times \gamma_2 \times \gamma_3 \in \Gamma$ en $A \in \mathcal{C}_2$, schrijf $\gamma(A) = A^\gamma$.

Definitie 3.1. *Gegeven twee kubussen $A, B \in \mathcal{C}_2$. Definieer $A \sim B$ als er een $\gamma \in \Gamma$ bestaat, zó dat $A^\gamma = B$.*

Dit is een equivalentierelatie. Merk verder de anologie op met de equivalentierelaties van kwadratische vormen, zoals we die in hoofdstuk 1 gedefiniëerd hebben.

3.3 Kwadratische vormen in de kubus

Nu de kubussen en hun equivalentieklassen gedefinieerd zijn, kunnen we aan de hand van de matrices M_i en N_i drie kwadratische vormen definiëren. Waarom dit nuttig is, zal snel blijken. Er geldt namelijk dat als we deze kwadratische vormen vermenigvuldigen, we de identiteit vinden. Dit betekent dat we een nieuwe manier hebben om de Dirichlet-compositie te berekenen. Dit zien we verderop in deze paragraaf.

Definitie 3.2. *Gegeven een kubus $A \in \mathcal{C}_2$ en M_i,N_i zoals boven gedefinieerd, waarbij $1 \leq i \leq 3$. Definieer de kwadratische vorm $Q_i^A(x, y)$ als*

$$Q_i^A(x, y) = -\det(M_i x + N_i y).$$

Je kunt deze expliciet uitrekenen. Dit geeft

$$\begin{aligned} Q_1^A &= x^2(-ad + bc) + xy(ah - bg - cf + de) + y^2(-eh + fg), \\ Q_2^A &= x^2(-ag + ce) + xy(ah + bg - cf - de) + y^2(-bh + df), \\ Q_3^A &= x^2(-af + be) + xy(ah - bg + cf - de) + y^2(-ch + dg). \end{aligned}$$

Het blijk dat de discriminant van de drie kwadratische vormen allemaal gelijk is. Daarom geeft dit een logische definitie van de discriminant van de kubus.

Definitie 3.3. *Gegeven een kubus $A \in \mathcal{C}_2$ en $Q_i^A(x, y)$, zoals boven gedefinieerd. Definieer de discriminant van A als*

$$\begin{aligned} Disc(A) &= Disc(Q_i^A) \\ &= a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 - 2(abgh + cdef + acfh + bdeg + aedh + bfcg) \\ &\quad + 4(adfg + bceh). \end{aligned}$$

Een andere definitie volgt ook logisch uit de kwadratische vormen van een kubus. De definitie van primitiviteit.

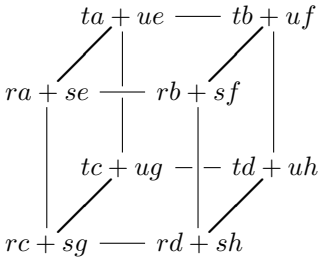
Definitie 3.4. *Een kubus $A \in \mathcal{C}_2$ is primitief als zijn geassocieerde kwadratische vormen Q_i^A dit ook zijn.*

Het blijkt dat er een verband is tussen de equivalentie van de kubussen en de equivalentie van hun kwadratische vormen.

Stelling 3.1. *Gegeven een kubus* $A \in \mathcal{C}_2$ *en* $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \times id \times id \in \Gamma$. *Dan geldt dat* $Q_1^{(A^\gamma)}(x,y) = Q_1^A(rx-ty,-sx+uy)$, $Q_2^{(A^\gamma)}(x,y) = Q_2^A(x,y)$, $Q_3^{(A^\gamma)}(x,y) = Q_3^A(x,y)$. *Hieruit volgt dat equivalente kubussen* A *en* B, *equivalente kwadratische vormen* Q_i^A *en* Q_i^B *hebben.*

Merk op dat $\begin{pmatrix} rx-ty \\ -sx+uy \end{pmatrix} = \begin{pmatrix} r & -t \\ -s & u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix}^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$. Je vind $Q_1^{(A^\gamma)}$ dus door γ op de matrixvorm van Q_1^A te laten werken.

Bewijs
Een explicite berekening levert de volgende kubus op voor A^γ:



Vullen we dit in voor Q_1, dan vinden we dat

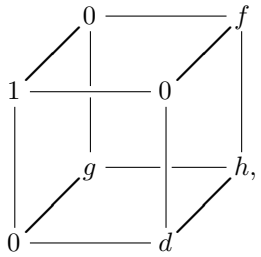
$$\begin{aligned}
Q_1^{(A^\gamma)} &= x^2(-(ra+se)(rd+sh)+(rb+sf)(rc+sg)) \\
&\quad + xy((ra+se)(td+uh)-(rb+sf)(tc+ug)-(rc+sg)(tb+uf)+(rd+sh)(ta+ue)) \\
&\quad + y^2(-(ta+ue)(td+uh)+(tb+uf)(tc+ug)) \\
&= x^2(bcr^2-adr^2-ders+cfrs+bgrs-ahrs+fgs^2-ehs^2) \\
&\quad + xy(-2bcrt+2adrt+dest-cfst-bgst+ahst+deru-cfru-bgru+ahru-2fgsu+2ehsu) \\
&\quad + y^2(bct^2-adt^2-detu+cftu+bgtu-ahtu+fgu^2-ehu^2) \\
&= (rx-ty)^2(-ad+bc)+(rx-ty)(-sx+uy)(ah-bg-cf+de)+(-sx+uy)^2(-eh+fg) \\
&= Q_1^A(rx-ty,-sx+uy).
\end{aligned}$$

We zouden Q_2 en Q_3 ook expliciet kunnen uitrekenen en daarmee de stelling kunnen bewijzen. Merk echter op dat bij M_2 en N_2 alleen kolomoperaties zijn uitgevoerd. Bekijk bijvoorbeeld specifiek M_2 (de linkerkant van de kubus) en noteer daarbij de oude kolommen als c_1 en c_2 en de nieuwe kolommen als $\tilde{c}_1$ en $\tilde{c}_2$. Dan geldt dat $\tilde{c}_1 = rc_1 + sc_2$ en $\tilde{c}_2 = \frac{s\tilde{c}_1+(-st+ru)c_2}{r}$. Hierdoor wordt de determinant van M_2 door γ geschaald met $r\frac{-st+ru}{r} = ru - st = 1$. Dit zie je door de kolommen te vermenigvuldigen en bij elkaar op te tellen. Alleen de vermenigvuldiging heeft effect op de determinant. Op dezelfde manier wordt N_2 ook met een factor 1 geschaald, waardoor $Q_2 = -\det(M_2x - N_2y)$ gelijk blijft. Eenzelfde argument kunnen we geven voor Q_3. Er is gebleken dat $\gamma = \gamma_1 \times \mathrm{id} \times \mathrm{id} \in \Gamma$ Q_1 transformeert en Q_2 en Q_3 onveranderd laat. Verder transformeert hij Q_1 door γ_1 op de matrixvorm van Q_1 te laten werken. Hieruit volgt dat $\gamma = \gamma_1 \times \gamma_2 \times \gamma_3 \in \Gamma$ Q_i transformeert door γ_i op de matrixvorm van Q_i te laten werken. Dit bewijst het laatste punt van de stelling. Equivalente kubussen hebben equivalente kwadratische vormen. Er geldt overigens ook dat als twee kubussen equivalente vormen hebben, ze equivalent zijn. We kunnen namelijk het vormen met een matrix γ_i naar elkaar transformeren, dus dan wordt de ene kubus via $\gamma_1 \times \gamma_2 \times \gamma_3$ in de andere kubus getransformeerd.□

We sluiten de paragraaf af met de stelling waarmee begonnen. Deze zegt dat het product van de kwadratische vormen van (primitieve) kubussen gelijk is aan de identiteit. Dit feit kun je bijvoorbeeld gebruiken om de compositie van twee kwadratische vormen te berekenen. Gegeven twee kwadratische vormen is het namelijk mogelijk om een (primitieve) kubus te maken, zó dat de twee kwadratische vormen aan de kubus geassocieerd worden. De derde kwadratische vorm is dan de inverse van het product van de eerste twee en daarmee is het product bekend.

Stelling 3.2. *Zij A een primitief element van $\mathcal{C}_2$. Dan geldt dat $Q_1 \circ Q_2 = Q_3^{-1}$.*

Zij A een primitieve kubus. Dan is A equivalent met een kubus van de vorm



waarbij $d, f, g, h \in \mathbb{Z}$. Merk op dat als A primitief is, dat dan $G = \text{ggd}(a, b, c, d, e, f, g, h) = 1$. Dit komt omdat $G|\text{ggd}(bc - ad, ed + ah - bg - fc, gf - eh)$ en deze laatste grote gemene deler is gelijk aan 1, wegens de primitiviteit van Q_1. We bewijzen nu dat we A kunnen transformeren tot bovenstaande kubus. Herinner je de matrices $S^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ en $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Merk op dat $T \times \text{id} \times \text{id}$, $\text{id} \times T \times \text{id}$ en $\text{id} \times \text{id} \times T$ de zijkanten omwisselen, waarbij één zijkant een min-teken krijgt. Door deze drie elementen van Γ op A uit te voeren, kun je ervoor zorgen dat a absoluut gezien het kleinste element is, dat niet nul is. Als a relatief priem is met b, c of e, dan kunnen we (met behulp van het uitgebreide Euclidische algoritme) een matrix vinden die a naar 1 transformeert. Als b, c en e allen een veelvoud zijn van a, dan kunnen we $S^n \times \text{id} \times \text{id}$, $\text{id} \times S^n \times \text{id}$ en $\text{id} \times \text{id} \times S^n$ gebruiken om deze modulo a te reduceren. Deze matrices laten namelijk één zijkant onveranderd, terwijl ze bij de andere zijkant n maal de eerste zijkant optellen. Nu vervangen we a weer door de absoluut kleinste waarde, die niet nul is. Herhaal dit proces totdat $a = 1$ of $b = c = e = 0$. Merk in dit laatste geval op dat $\text{ggd}(bc - ad, ed + ah - bg - fc, gf - eh) = \text{ggd}(ad, ah, fg) = 1$, dus er zijn $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}$, zodat $a(\lambda_1 d + \lambda_2 h) + f(\lambda_3 g) = 1$, waardoor $\text{ggd}(a, f) = 1$. Door nu nogmaals S toe te passen, vinden we een kubus met $\text{ggd}(a, e) = 1$, waardoor we deze kunnen transformeren tot een kubus met $a = 1$. Deze $a = 1$ kunnen we nu gebruiken om b, c en e tot 0 te reduceren en daarmee is bewezen dat A equivalent is met een bovenstaande kubus. De kwadratische vormen die bij deze kubus horen, worden gegeven door

$$\begin{aligned} Q_1(x, y) &= -dx^2 + hxy + fgy^2, \\ Q_2(x, y) &= -gx^2 + hxy + dfy^2, \\ Q_3(x, y) &= -fx^2 + hxy + dgy^2. \end{aligned}$$

Merk nu op dat met Dirichlet-compositie geldt dat $Q_1 \circ Q_2 = (-d, h, fg) \circ (-g, h, fd) = (dg, h, -f) \sim (-f, -h, dg) = Q_3^{-1}$. We zien dus met Dirichlet-compositie dat het product van de drie kwadratische vormen gelijk is aan de identiteit. □

3.4 Idealen en kubussen

In deze paragraaf bewijzen we dat er een bijectie is tussen drietallen idealen in $\mathbb{Q}(\sqrt{d})$ en de kubussen uit dit hoofdstuk. Merk op dat het natuurlijk is om het over drietallen idealen te hebben. We hebben immers ook drie kwadratische vormen aan de kubus geassocieerd. Deze bijectie geeft meer inzicht in de structuur van de kubussen. Zo kunnen we een natuurlijke vermenigvuldiging op de kubussen definiëren die uit deze bijectie volgt. Dit doen we in de volgende paragraaf.

We werken opnieuw in de ring van gehelen van $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\Delta})$, de kwadratische uitbreiding van $\mathbb{Q}$ van radicand d en discriminant Δ. Daarnaast nemen we opnieuw aan dat $\Delta < 0$. We definiëren voor het gemak een aantal nieuwe schrijfwijzen. Schrijf

$$\tau = \begin{cases} \frac{\sqrt{\Delta}}{2} = \sqrt{d} & \text{als } \Delta \equiv 0 \pmod 4 \\ \frac{1+\sqrt{\Delta}}{2} = \frac{1+\sqrt{d}}{2} & \text{als } \Delta \equiv 1 \pmod 4 \end{cases}$$

Merk op dat bij deze notatie geldt dat $\mathcal{O}(\sqrt{d}) = [1, \tau]$. Definieer verder $\pi : \mathcal{O}(\sqrt{d}) \to \mathbb{Z}$ door $\pi(\alpha) = \frac{\alpha - \bar{\alpha}}{\sqrt{\Delta}}$. Hierdoor geldt dat, als je schrijft $\alpha = a + b\tau \in \mathcal{O}(\sqrt{d})$, dan $\pi(\alpha) = b$. Schrijf als laatste

$$\epsilon = \begin{cases} 0 & \text{als } \Delta \equiv 0 \pmod 4 \\ 1 & \text{als } \Delta \equiv 1 \pmod 4 \end{cases}$$

Met deze definities kunnen we aan de slag. Begin met het definieren van de drietallen idealen waar we geïnteresseerd in zijn.

Definitie 3.5. *Het drietal gebroken idealen (I_1, I_2, I_3) van $\mathcal{O}(\sqrt{d})$ is gebalanceerd als $I_1 I_2 I_3 \subset \mathcal{O}(\sqrt{d})$ en als geldt dat $N(I_1)N(I_2)N(I_3) = 1$.*

Op drietallen idealen kunnen we verder eenzelfde equivalentie definieren als op enkele idealen.

Definitie 3.6. *Twee gebalanceerde drietallen gebroken idealen (I_1, I_2, I_3) en (I_1', I_2', I_3') zijn equivalent als er $\kappa_1, \kappa_2, \kappa_3 \in \mathbb{Q}(\sqrt{d})$ bestaan, zó dat $I_i = (\kappa_i) I_i'$ voor $1 \leq i \leq 3$.*

In het bijzonder geldt nu dat $N(\kappa_1\kappa_2\kappa_3) = 1$. Deze relatie is wegens dezelfde argumenten als in hoofdstuk 2 een equivalentierelatie. Als je vermenigvuldiging op deze drietallen definieerd als $(I_1, I_2, I_3) \circ (I_1', I_2', I_3') = (I_1 I_1', I_2 I_2', I_3 I_3')$ vormen de equivalentieklassen van de drietallen gebroken idealen een groep, opnieuw wegens dezelfde argumenten als in hoofdstuk 2. Noteer deze groep als $\mathcal{C}^3(\mathcal{O}(\sqrt{\Delta}))$

Stelling 3.3. *Er bestaat een bijectie tussen $\mathcal{C}_2(\Delta)$ en $\mathcal{C}^3(\mathcal{O}(\sqrt{\Delta}))$.*

Bewijs
Zij (I_1, I_2, I_3) een representant van een equivalentieklasse in $\mathcal{C}^3(\mathcal{O}(\sqrt{\Delta}))$. Schrijf $I_1 = [\alpha_1, \alpha_2]$, $I_2 = [\beta_1, \beta_2]$ en $I_3 = [\gamma_1, \gamma_2]$, zó dat I_1, I_2, I_3, juist georienteerd zijn. Omdat I_1, I_2, I_3 gebalanceerd zijn, geldt dat $I_1 I_2 I_3 \subset \mathcal{O}(\sqrt{d})$, waardoor we de volgende set van acht vergelijkingen hebben:

$$\alpha_i \beta_j \gamma_k = c_{i,j,k} + a_{i,j,k}\tau \quad \text{waarbij } i, j, k \in \{1, 2\},\ c_{i,j,k}, a_{i,j,k} \in \mathbb{Z}. \tag{2}$$

Stuur nu het drietal (I_1, I_2, I_3) naar de kubus A met op de hoekpunten de getallen $a_{i,j,k} = \pi(\alpha_i \beta_j \gamma_k)$. Dus

$$A = \begin{array}{ccc} a_{2,1,1} & \text{---} & a_{2,2,1} \\ | & & | \\ a_{1,1,1} & \text{---} & a_{1,2,1} \\ | & & | \\ & a_{2,1,2} \text{---} & a_{2,2,2}. \\ | & & | \\ a_{1,1,2} & \text{---} & a_{1,2,2} \end{array}$$

We bewijzen dat dit een bijectie is. Daartoe bewijzen we eerst dat deze afbeelding welgedefinieerd is.
Stel dat we in plaats $[\alpha_1, \alpha_2]$ een andere basis van I_1 genomen hadden, $[\tilde{\alpha}_1, \tilde{\alpha}_2]$. Dan geldt dat $\tilde{\alpha}_1 = r\alpha_1 + s\alpha_2$ en $\tilde{\alpha}_2 = t\alpha_1 + u\alpha_2$, met $r, s, t, u \in \mathbb{Z}$ en $ru - st = 1$, wegens dezelfde argumenten als in het vorige hoofdstuk. Er geldt nu dat $\tilde{\alpha}_1\beta_j\gamma_k = r\alpha_1\beta_j\gamma_k + s\alpha_2\beta_j\gamma_k = (rc_{1,j,k} + sc_{2,j,k}) + (ra_{1,j,k} + sa_{2,j,k})\tau$ met $j, k \in \{1, 2\}$. Evenzo geldt dat $\tilde{\alpha}_2\beta_j\gamma_k = (tc_{1,j,k} + uc_{2,j,k}) + (ta_{1,j,k} + ua_{2,j,k})\tau$. We zien dat dit drietal idealen naar de kubus $A^{\gamma_1 \times \mathrm{id} \times \mathrm{id}}$ wordt afgebeeld met $\gamma_1 = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$, waardoor $\gamma_1 \times \mathrm{id} \times \mathrm{id} \in \Gamma$. Het drietal wordt met een verschillende basis naar dezelfde equivalentieklasse gestuurd. Dit gaat analoog voor basistransformaties van I_2 en I_3.
Stel dat we in plaats van (I_1, I_2, I_3) een equivalent drietal $(\kappa_1 I_1, \kappa_2 I_2, \kappa_3 I_3)$ hadden genomen. Dan wordt elk element op de kubus met $\kappa_1\kappa_2\kappa_3$ vermenigvuldigd, waardoor we de volgende vergelijking vinden:

$$\kappa_1\kappa_2\kappa_3\alpha_i\beta_j\gamma_k = c_{i,j,k} + a_{i,j,k}\tau \quad \text{waarbij } i, j, k \in \{1, 2\},\ c_{i,j,k}, a_{i,j,k} \in \mathbb{Z}.$$

Dit is dus gelijk aan de kubus die we verkrijgen door de basistransformatie $[\alpha_1, \alpha_2] \to [\kappa_1\kappa_2\kappa_3\alpha_1, \kappa_1\kappa_2\kappa_3\alpha_2]$. Merk op dat $\kappa_1\kappa_2\kappa_3$ een eenheid is in $\mathcal{O}(\sqrt{d})$, waardoor het inderdaad een simpele basistransformatie is. We hebben al bewezen dat een basistransformatie de kubus naar een equivalente kubus stuurt, dus we concluderen dat de equivalente idealen naar equivalente kubussen worden afgebeeld. Overigens zou kunnen gelden dat je door deze transformatie de orientatie van het ideaal I_1 verliest, (bijvoorbeeld als $\kappa_1\kappa_2\kappa_3 = -1$). Dit is echter niet erg, omdat de elementen van de kubus dan worden gegeven door $-a_{i,j,k}$ in plaats van $a_{i,j,k}$. Deze kubussen zijn echter equivalent, omdat ze dezelfde kwadratische vormen hebben. De welgedefinieerdheid is hiermee bewezen.

We bewijzen nu dat de discriminant van A gelijk is aan Δ. Begin met drietal $I_1 = I_2 = I_3 = \mathcal{O}(\sqrt{d})$, $\alpha_1 = \beta_1 = \gamma_1 = 1$ en $\alpha_2 = \beta_2 = \gamma_2 = \tau$. Merk op dat met de definities van τ en ϵ geldt dat $\tau^2 = \epsilon\tau + \frac{\Delta - \epsilon}{4}$ en $\tau^3 = \frac{\Delta + 3\epsilon}{4}\tau + \frac{\epsilon(\Delta - \epsilon)}{4}$. De kubus A_{id} die we met dit drietal idealen associëren is dus

$$A_{\mathrm{id}} = \begin{array}{ccc} 1 & \text{---} & \epsilon \\ | & & | \\ 0 & \text{---} & 1 \\ | & & | \\ & \epsilon \text{---} & \frac{\Delta+3\epsilon}{4} \\ | & & | \\ 1 & \text{---} & \epsilon \end{array}$$

We hebben deze kubus A_{id} gedoopt, omdat dit de identiteit blijkt te zijn bij compositie van kubussen, welke we in de volgende paragraaf zullen definiëren. Een directe berekening van zijn

discriminant geeft dat $\mathrm{Disc}(A_{\mathrm{id}}) = 3\epsilon^2 - 2(3\epsilon^2) + 4\frac{\Delta+3\epsilon}{4} = \Delta$. Nu transformeren we I_1 in een gebroken ideaal $[\alpha_1, \alpha_2]$. Er geldt dat $\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix} = \begin{pmatrix}r & s\\ t & u\end{pmatrix}\begin{pmatrix}1\\ \tau\end{pmatrix} = T\begin{pmatrix}1\\ \tau\end{pmatrix}$, maar nu zijn $r, s, t, u \in \mathbb{Q}$ en de determinant van de transformatiematrix hoeft niet gelijk te zijn aan 1. We weten dat het elementen van $\mathbb{Q}$ zijn, omdat we in $\mathbb{Q}(\sqrt{d})$ werken. Merk wel op dat geldt dat

$$N(I_1) = \frac{1}{\sqrt{\Delta}}\left|\begin{pmatrix}\alpha_1 & \bar{\alpha}_1\\ \alpha_2 & \bar{\alpha}_2\end{pmatrix}\right| = \frac{1}{\sqrt{\Delta}}\left|\begin{pmatrix}r & s\\ t & u\end{pmatrix}\begin{pmatrix}1 & 1\\ \tau & \bar{\tau}\end{pmatrix}\right| = \left|\begin{pmatrix}r & s\\ t & u\end{pmatrix}\right|\frac{\tau-\bar{\tau}}{\sqrt{\Delta}} = \left|\begin{pmatrix}r & s\\ t & u\end{pmatrix}\right| = \det(T).$$

We hebben net gezien dat een verandering van basis door een matrixvermenigvuldiging $T \times \mathrm{id} \times \mathrm{id}$ de geassocieerde kubus A transformeert in de kubus $A^{T\times\mathrm{id}\times\mathrm{id}}$. Uit het werk van de vorige paragraaf volgt dat Q_1^{id} wordt getransformeerd door matrix T. Q_2^{id} en Q_3^{id} gaan over in $\det(T)Q_2^{\mathrm{id}}$, respectievelijk $\det(T)Q_3^{\mathrm{id}}$. In het bijzonder volgt nu dat de basisverandering naar I_1 de discriminant van de kubus schaalt met een factor $\det(T)^2 = N(I_1)^2$. Als we nu I_2 en I_3 ook transformeren in willekeurige gebroken idealen, dan vinden we (met dezelfde argumenten) dat de discriminant van de bijbehorende kubus A gegeven wordt door $\mathrm{Disc}(A) = N(I_1)^2N(I_2)^2N(I_3)^2\mathrm{Disc}(A_{\mathrm{id}})$. Voor een gebalanceerd drietal (I_1, I_2, I_3) geldt dat $N(I_1)N(I_2)N(I_3) = 1$. Daarnaast geldt dat $\mathrm{Disc}(A_{\mathrm{id}}) = \Delta$, dus we concluderen dat $\mathrm{Disc}(A) = \Delta$.

De volgende stap in het bewijs is om de bijectiviteit te bewijzen. Neem daartoe een kubus A met discriminant Δ en hoekpunten $a_{i,j,k}$. Vul deze in in de verzameling vergelijkingen (2). In deze set van acht vergelijkingen staan nu veertien onbekenden, $\alpha_i, \beta_j, \gamma_k$ en $c_{i,j,k}$. Dit lijkt dus te weinig om deze op te lossen, maar we hebben nog meer aannamen over de vergelijkingen. We weten bijvoorbeeld, omdat $\alpha_i, \beta_j, \gamma_k \in \mathbb{Q}(\sqrt{d})$, dat er commutativiteit geldt. Dat betekent dat

$$(\alpha_i\beta_j\gamma_k)(\alpha_{i'}\beta_{j'}\gamma_{k'}) = (\alpha_{i'}\beta_j\gamma_k)(\alpha_i\beta_{j'}\gamma_{k'}) = (\alpha_i\beta_{j'}\gamma_k)(\alpha_{i'}\beta_j\gamma_{k'}) = (\alpha_i\beta_j\gamma_{k'})(\alpha_{i'}\beta_{j'}\gamma_k),$$

waarbij $i, i', j, j', k, k' \in \{1, 2\}$. Hieruit volgen negen verschillende vergelijkingen in $a_{i,j,k}$ en $c_{i,j,k}$. Deze negen vergelijkingen kun je uitvermenigvuldigen, gebruikmakend van $\tau^2 = \epsilon\tau + \frac{\Delta-\epsilon}{4}$ en de definitie van de discriminant. Door vervolgens iedere vergelijking op te splitsen in twee vergelijkingen, één van de coëfficiënten van 1 en één van de coëfficiënten van τ, vind je achttien onafhankelijke lineaire en kwadratische vergelijkingen van $c_{i,j,k}$. Als je nu eist dat $N(I_1)N(I_2)N(I_3) > 0$ wegens de oriëntatie, dan vind je een unieke oplossing voor iedere $c_{i,j,k}$:

$$\begin{aligned} c_{i,j,k} =& (i'-i)(j'-j)(k'-k)\\ &\left(a_{i',j,k}a_{i,j',k}a_{i,j,k'} + \frac{1}{2}a_{i,j,k}(a_{i,j,k}a_{i',j',k'} - a_{i',j,k}a_{i,j',k'} - a_{i,j',k}a_{i',j,k'} - a_{i,j,k'}a_{i',j',k})\right)\\ &- \frac{1}{2}a_{i,j,k}\epsilon, \end{aligned} \tag{3}$$

waarbij $\{i, i'\} = \{j, j'\} = \{k, k'\} = \{1, 2\}$. Het blijkt dus dat $c_{i,j,k}$ uniek wordt bepaald door de kubus A. Nu moeten we op zoek naar de factoren $\alpha_i, \beta_j, \gamma_k \in \mathbb{Q}(\sqrt{d})$. Merk op dat je deze nooit uniek kunt bepalen, omdat we op zoek zijn naar gebroken idealen en we al gezien hebben dat $I_1' = \kappa I_1$ dezelfde kubus opleveren (als I_2 en I_3 ook geschaald worden). Wel volgen γ_1 en γ_2 uit vergelijkingen (2), als we $\alpha_1, \alpha_2, \beta_1$ en β_2 bepaald hebben. Merk verder op dat, opnieuw wegens commutativiteit, $\alpha_1(\alpha_2, \beta_j, \gamma_k) = \alpha_2(\alpha_1, \beta_j, \gamma_k)$, waardoor de verhouding $\frac{\alpha_1}{\alpha_2} = \frac{c_{1,j,k}+a_{1,j,k}\tau}{c_{2,j,k}+a_{2,j,k}\tau}$ uniek bepaald is. Evenzo is de verhouding $\frac{\beta_1}{\beta_2} = \frac{c_{i,1,k}+a_{i,1,k}\tau}{c_{i,2,k}+a_{i,2,k}\tau}$ uniek bepaald. Dit is voldoende om (de equivalentieklasse van) het drietal idealen (I_1, I_2, I_3) te bepalen. Kies $\alpha_i = c_{i,1,1} + a_{i,1,1}\tau$ en $\beta_j = c_{2,j,2} + a_{2,j,2}\tau$, waardoor uit (2) volgt dat $\gamma_1 = \beta_1^{-1}$ en $\gamma_2 = \alpha_2^{-1}$.

We moeten nu bewijzen dat $[\alpha_1, \alpha_2]$ een (gebroken) ideaal is. Evenzo voor $[\beta_1, \beta_2]$ en $[\gamma_1, \gamma_2]$. $[\alpha_1, \alpha_2]$ en $[\beta_1, \beta_2]$ zijn al deelverzamelingen van $\mathcal{O}(\sqrt{d})$. Door $[\gamma_1, \gamma_2]$ te vermenigvuldigen met de factor $\beta_1\alpha_2 \in \mathcal{O}(\sqrt{d})$ wordt dit ook een deelverzameling van $\mathcal{O}(\sqrt{d})$, waardoor het 'gebroken' gedeelte duidelijk is. Om te bewijzen dat het een ideaal is, is het voldoende om te bewijzen dat $\tau\alpha_i \in [\alpha_1, \alpha_2]$, $\tau\beta_j \in [\beta_1, \beta_2]$ en $\tau\gamma_k \in [\gamma_1, \gamma_2]$. Dit volgt uit het feit dat $\mathcal{O}(\sqrt{d}) = [1, \tau]$. Zij $Q_i^A = p_i x^2 + q_i xy + r_i y^2$ de geassocieerde kwadratische vorm van de kubus A. Dan blijkt dat

$$\begin{aligned}\tau\alpha_1 &= \frac{q_1+\epsilon}{2}\alpha_1 + p_1\alpha_2\\ -\tau\alpha_2 &= r_1\alpha_1 + \frac{q_1-\epsilon}{2}\alpha_2\end{aligned}$$

Dit is expliciet uit te rekenen door de definities van Δ, Q_1, vergelijkingen (3) en $\tau^2 = \epsilon\tau + \frac{\Delta-\epsilon}{4}$ in te vullen. Op dezelfde manier volgt dat

$$\begin{aligned}\tau\beta_1 &= \frac{q_2+\epsilon}{2}\beta_1 + p_2\beta_2\\ -\tau\beta_2 &= r_2\beta_1 + \frac{q_2-\epsilon}{2}\beta_2\\ \tau\gamma_1 &= \frac{q_3+\epsilon}{2}\gamma_1 + p_3\gamma_2\\ -\tau\gamma_2 &= r_3\gamma_1 + \frac{q_3-\epsilon}{2}\gamma_2\end{aligned}$$

Hieruit volgt dat het inderdaad idealen zijn. We hebben nu bewezen dat bij iedere kubus een unieke equivalentieklasse hoort (wegens de uniciteit van $c_{i,j,k}$). Hiermee is surjectiviteit bewezen. Stel dat je twee verschillende drietallen idealen (I_1, I_2, I_3) en (I_1', I_2', I_3') hebt die naar twee equivalente kubussen A en A^γ worden afgebeeld. Dan kunnen we nu (I_1', I_2', I_3') door een basistransformatie met γ^{-1} naar A laten afbeelden. Uit de uniciteit die we net bewezen hebben volgt dan dat (I_1, I_2, I_3) en (I_1', I_2', I_3') ook equivalent zijn, waarmee ook de injectiviteit bewezen is. We concluderen dat de afbeelding bijectief is en daarmee is de stelling bewezen. □

Interessant is om nog even te kijken naar de primitieve kubussen. Zoals we in de vorige paragraaf bewezen hebben is een primitieve kubus equivalent aan een kubus met $a = 1$ en $b = c = e = 0$. Gebruik de vorige stelling om een I_1, I_2 en bijbehorende I_3 te vinden die naar deze kubus afbeelden. Neem

$$I_1 = [\alpha_1, \alpha_2] = [c_{1,1,1}+\alpha_{1,1,1}\tau, c_{2,1,1}+\alpha_{2,1,1}\tau] = [\frac{h-\epsilon}{2}+1\frac{\sqrt{\Delta}+\epsilon}{2}, -fg+0\frac{\sqrt{\Delta}+\epsilon}{2}] = [fg, \frac{h+\sqrt{\Delta}}{2}]$$

en

$$I_2 = [\beta_1, \beta_2] = [c_{1,1,1}+\alpha_{1,1,1}\tau, c_{1,2,1}+\alpha_{1,2,1}\tau] = [\frac{h-\epsilon}{2}+1\frac{\sqrt{\Delta}+\epsilon}{2}, -df+0\frac{\sqrt{\Delta}+\epsilon}{2}] = [df, \frac{h+\sqrt{\Delta}}{2}].$$

De afbeelding ψ die we in hoofdstuk 2 hebben gedefinieerd stuurt nu I_1 naar $(fg, -h, \frac{h^2-\Delta}{4fg}) = (fg, -h, -d) \sim (-d, h, fg) = Q_1$, waarbij we de definitie van de discriminant Δ hebben gebruikt. Evenzo stuurt ψ het gebroken ideaal I_2 naar $(df, -h, -g) \sim (-g, h, df) = Q_2$. Omdat de equivalenties die we in hoofdstuk 2 op idealen en in hoofdstuk 3 op drietallen idealen hebben gedefinieerd gelijk zijn, zien we dat de afbeeldingen ϕ en ψ uit het vorige hoofdstuk de kwadratische vorm Q_i van een primitieve kubus en het gebroken ideaal I_i van bijbehorend drietal idealen aan elkaar relateren. Dit is een erg nuttige constatering. Merk ook op dat, omdat het product van de kwadratische vormen de identiteit is en omdat de identiteit wordt gerelateerd aan $[1, \tau] = \mathcal{O}(\sqrt{d})$, geldt dat $I_1I_2I_3$ equivalent is aan $\mathcal{O}(\sqrt{d})$ voor deze drietallen idealen. Omdat het drietal (I_1, I_2, I_3) gebalanceerd is, geldt daarom dat $I_1I_2I_3 = \mathcal{O}(\sqrt{d})$.

3.5 Compositie van kubussen

In deze paragraaf bewijzen we twee grote stellingen. Het bewijzen hiervan is echter erg simpel, omdat we de bijectie uit het vorige hoofdstuk zullen gebruiken. Verder zullen we er vanuit gaan dat de kubussen vanaf nu primitief zijn. Hiermee kunnen we de opmerking gebruiken, waarmee we de vorige paragraaf afsloten.

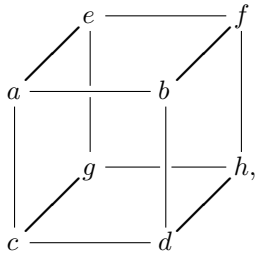
Stelling 3.4. *Gegeven f_1, f_2, f_3 drie primitieve kwadratische vormen van discriminant Δ, zó dat $f_1 \circ f_2 \circ f_3 = id$. Dan is er een primitieve kubus $A \in \mathcal{C}_2$, zó dat $Q_1^A = f_1$, $Q_2^A = f_2$ en $Q_3^A = f_3$. Deze kubus is op equivalentie na uniek.*

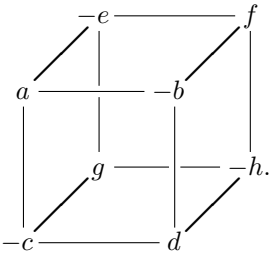
Bewijs
Dit volgt rechtstreeks uit de stelling van de vorige paragraaf. Zij $I_i = \phi(f_i)$. Dan volgt uit het feit dat $f_1 \circ f_2 \circ f_3 = \mathrm{id}$ dat $I_1 I_2 I_3 = \mathcal{O}(\sqrt{d})$, waardoor het drietal gebalanceerd is. Er is dus een kubus $A \in \mathcal{C}_2$ die we met dit drietal associëren. Uit ons werk in de vorige paragraaf volgt dat $Q_1^A = f_1$, $Q_2^A = f_1$ en $Q_3^A = f_3$ en we weten zelfs dat deze kubus primitief is. □

Definitie 3.7. *Zij $A, B \in \mathcal{C}_2$ primitieve kubussen en zij Q_i^A, respectievelijk Q_i^B hun geassocieerde kwadratische vormen. Laat nu $C \in \mathcal{C}_2$, zó dat $Q_i^C = Q_i^A \circ Q_i^B$ voor $1 \leq i \leq 3$. Definieer dan $[A] \circ [B] = [C]$.*

Stelling 3.5. *Deze definitie plaatst een groepstructuur op de primitieve kubussen van C_2.*

Bewijs
Merk op dat $Q_1^C \circ Q_2^C \circ Q_3^C = \left(Q_1^A \circ Q_2^A \circ Q_3^A\right) \circ \left(Q_1^B \circ Q_2^B \circ Q_3^B\right) = \mathrm{id} \circ \mathrm{id} = \mathrm{id}$, wegens de primitiviteit van A en B. Wegens de vorige stelling geldt dat C ook primitief is. De groepstructuur is nu duidelijk. Er geldt duidelijk dat er geslotenheid is en de associativiteit volgt uit de associativiteit van de compositie van kwadratische vormen. De kubus A_{id} is, zoals eerder aangegeven, de identiteit. Dat dit de identiteit is, is nu ook duidelijk: zijn geassocieerde kwadratische vormen zijn gegeven door $Q_i^{A_{\mathrm{id}}} = (1, -\epsilon, \frac{\epsilon - \Delta}{4})$, wat de identiteit is van kwadratische vormen, zoals we in hoofdstuk 1 zagen. De inverse wordt gegeven door onderstaande kubus. Merk namelijk op dat $Q_i^{\left(A^{-1}\right)}$ inderdaad gelijk is aan $\left(Q_i^A\right)^{-1}$.

als $A =$ 

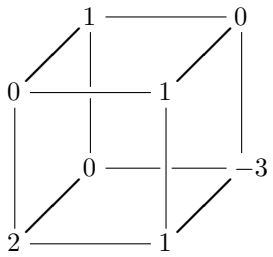
dan $A^{-1} =$ 

□

Logischerwijs is dit dezelfde groepsstructuur als op de drietallen gebroken idealen die we in het vorige hoofdstuk bekeken hebben, waarbij we wel moeten eisen dat $I_1 I_2 I_3 = \mathcal{O}(\sqrt{d})$. Volgens onze definitie is $Q_i^C = Q_i^A \circ Q_i^B$ en die komt overeen met de vermenigvuldiging die we op de drietallen idealen gedefinieerd hebben, namelijk $(I_1, I_2, I_3) \circ (I_1', I_2', I_3') = (I_1 I_1', I_2 I_2', I_3 I_3')$. Merk daarbij op dat $I_1 I_1', I_2 I_2', I_3 I_3' = I_1 I_2 I_3 I_1' I_2' I_3' = \mathcal{O}(\sqrt{d})\mathcal{O}(\sqrt{d}) = \mathcal{O}(\sqrt{d})$.

3.6 Bijvoorbeeld

In de laatste paragraaf van elk hoofdstuk wordt een voorbeeld bekeken, waarbij de theorie van dat hoofdstuk wordt behandeld. Neem $\Delta = -23$ als vaste discriminant van onze kwadratische vormen. Deze heeft drie equivalentieklassen, gegeven door de representanten $(1, 1, 6)$, $(2, 1, 3)$ en $(2, -1, 3)$. Opnieuw berekenen we $(2, 1, 3) \circ (2, -1, 3)$, maar nu door de volgende kubus te bekijken:



Uit de formules van dit hoofdstuk volgt dat

$$Q_1^A = x^2(-ad + bc) + xy(ah - bg - cf + de) + y^2(-eh + fg) = 2x^2 + xy + 3 = (2, 1, 3),$$
$$Q_2^A = x^2(-ag + ce) + xy(ah + bg - cf - de) + y^2(-bh + df) = 2x^2 - xy + 3 = (2, -1, 3),$$
$$Q_3^A = x^2(-af + be) + xy(ah - bg + cf - de) + y^2(-ch + dg) = x^2 - xy + 6 = (1, -1, 6).$$

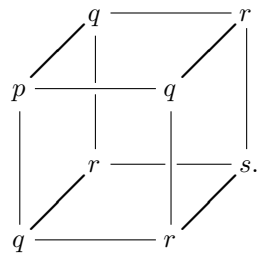
Hieruit volgt dat $(2, 1, 3) \circ (2, -1, 3) \circ (1, -1, 6) = \mathrm{id}$. Omdat $(a, -b, c)$ de inverse is van (a, b, c), vinden we nu dat $(2, 1, 3) \circ (2, -1, 3) = (1, 1, 6)$.

Hoe hebben we deze kubus nu gevonden? Uit het vorige hoofdstuk volgt dat $(2, 1, 3)$ aan $[2, \frac{-1+\sqrt{-23}}{2}] = [2, \tau - 1]$ wordt gerelateerd. Evenzo wordt $(2, -1, 3)$ aan $[2, \frac{1+\sqrt{-23}}{2}] = [2, \tau]$ wordt gerelateerd. Nu geldt dat $[2, \tau - 1][2, \tau] = (2)[1, \tau]$, waardoor $[2, \tau - 1][2, \tau](\frac{1}{2})[1, \tau] = \mathcal{O}(\sqrt{-23})$. We nemen nu dus $I_1 = [2, \tau - 1]$, $I_2 = [2, \tau]$ en $I_3 = (\frac{1}{2})[1, \tau]$. Als we nu de afbeelding gebruiken die in dit hoofdstuk is gegeen, dan vinden we bovenstaande kubus.

4 Kubische vormen

Zoals eerder aangekondigd gaan we in dit hoofdstuk kijken naar kubische vormen en zullen we hier een compositie op definiëren. Net zoals in het vorige hoofdstuk volgen we hierbij de ideeën en bewijzen van Bhargava [1] en de iets gedetailleerdere aanpak van Bouyer [2].

We relateren een kubische vorm $C(x,y) = px^3 + 3qx^2y + 3rxy^2 + sy^3 = (p,q,r,s)$ aan de Bhargavakubus

$C =$ 

Noteer de verzameling van zulke kubussen als $\mathrm{Sym}^3\mathbb{Z}^2$. Merk meteen op dat er een natuurlijke inclusie is van deze verzameling naar de verzameling van Bhargavakubussen, namelijk $\iota : \mathrm{Sym}^3\mathbb{Z}^2 \to \mathcal{C}_2$ door $\iota(C) = C$. Met behulp van deze inclusie kunnen we alle definities uit het voorgaande hoofdstuk ook op de symmetrische kubussen en daarmee op de kubische vormen projecteren.

Definitie 4.1. *Zij $C = (p,q,r,s)$ een kubische vorm.*

- *Zijn discriminant wordt gegeven $\Delta = p^2s^2 + 4(pr^3 + q^3s) - 3q^2r^2 - 6pqrs$.*
- *Zijn geassocieerde kwadratische vormen zijn gelijk en worden gegeven door*

$$Q_i^{\iota(C)} = (q^2 - pr)x^2 + (ps - qr)xy + (r^2 - qs)y^2.$$

- *C is primitief als zijn geassocieerde kwadratische vormen dat ook zijn.*

4.1 Equivalentieklassen op kubische vormen

In dit hoofdstuk wordt, evenals in de voorgaande drie hoofdstukken, een equivalentie gedefinieerd op de objecten waar we mee werken, in dit geval de kubische vormen. Als je deze equivalentie analoog wil definiëren aan de vorige hoofdstukken, heb je eigenlijk twee opties. Je zou een relatie kunnen definiëren zoals bij de kwadratische vormen.

Definitie 4.2. *Zij C, C' twee kubische vormen, definieer dan $C \sim C'$ als er een $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, zodat $C(ax + cy, bx + dy) = C'(x,y)$.*

Je zou echter ook een relatie kunnen definiëren aan de hand van hun Bhargavakubussen.

Definitie 4.3. *Zij $C, C' \in Sym^3\mathbb{Z}^2$, definieer dan $C \sim C'$ als er een $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, zodat $\iota(C)^{\gamma\times\gamma\times\gamma} = \iota(C')$.*

Noteer hierbij de subgroep $\{\gamma \times \gamma \times \gamma | \gamma \in \mathrm{SL}_2(\mathbb{Z})\}$ van Γ als $\bar{\Gamma}$. Dan zijn C, C' dus equivalent als er een $\gamma \in \bar{\Gamma}$ bestaat, zodat $\iota(C)^\gamma = \iota(C')$. Gelukkig zijn beide relaties gelijk. Dit kun je expliciet uitrekenen en geeft voor $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dat $C' = (p', q', r', s')$ met

$$\begin{aligned} p' &= a^3p + 3a^2bq + 3ab^2r + b^3s, \\ q' &= a^2cp + (a^2d + 2abc)q + (b^2c + 2abd)r + b^2ds, \\ r' &= ac^2p + (2acd + bc^2)q + (2bcd + ad^2)r + bd^2s, \\ s' &= c^3p + 3c^2dq + 3cd^2r + d^3s. \end{aligned}$$

Deze relatie is een equivalentierelatie, bijvoorbeeld wegens dezelfde argumenten als bij de equivalentie van kwadratische vormen.

4.2 Kubische vormen en idealen

Deze paragraaf zal analoog gaan aan paragraaf 3.4 uit het vorige hoofdstuk. Daar bewezen we dat er een bijectie was tussen een drietal idealen in $\mathbb{Q}(\sqrt{\Delta})$ en de Bhargavakubussen. In deze paragraaf bewijzen we iets soortgelijks, maar dan voor de kubische vormen. Hierdoor kunnen we een compositie definiëren op de kubische vormen, waardoor er vervolgens ook een groepsstructuur ontstaat.

In plaats van dat we naar drietallen gebroken idealen (I_1, I_2, I_3) kijken, kijken we nu naar één gebroken ideaal I, dat we driemaal met zichzelf vermenigvuldigen. Zij $\delta \in \mathbb{Q}(\sqrt{\Delta})$, zó dat $I^3 \subseteq \delta\mathcal{O}(\sqrt{d})$ en $N(I)^3 = N(\delta)$. Definieer een relatie op de paren (I, δ), (I', δ') door $(I, \delta) \sim (I', \delta')$ als er een $\kappa \in \mathbb{Q}(\sqrt{\Delta})$ is, zodat $I' = (\kappa)I$ en $\delta' = \kappa^3\delta$. Dit is opnieuw een equivalentierelatie. De equivalentieklassen van deze paren vormen een groep onder de logische vermenigvuldiging $(I, \delta) \circ (I', \delta') = (II', \delta\delta')$ met als identiteitselement $(\mathcal{O}(\sqrt{d}), 1)$. Noteer deze groep als $\mathcal{C}_1^3(\mathcal{O}(\sqrt{\Delta}))$. Hierbij staat de 1 voor het feit dat we met maar één ideaal werken.

Stelling 4.1. *Er bestaat een bijectie tussen de verzameling kubische vormen met discriminant Δ en de groep van paren (I, δ).*

Bewijs
Dit bewijs is vrijwel analoog met het bewijs uit paragraaf 3.4. Zij $(I, \delta) \in \mathcal{C}_1^3(\mathcal{O}(\sqrt{\Delta}))$. Dan geldt dus dat $I = [\alpha, \beta]$ een gebroken ideaal is in $\mathcal{O}(\sqrt{d})$. Neem aan dat dit een geordend ideaal is. Verder geldt dat $I^3 \subseteq \delta\mathcal{O}(\sqrt{d}) = [\delta, \delta\tau]$ en $N(I)^3 = N(\delta)$. Er geldt nu dat

$$\begin{aligned} \alpha^3 &= \delta(c_0 + a_0\tau), \\ \alpha^2\beta &= \delta(c_1 + a_1\tau), \\ \alpha\beta^2 &= \delta(c_2 + a_2\tau), \\ \beta^3 &= \delta(c_3 + a_3\tau), \end{aligned} \tag{4}$$

waarbij $c_i, a_i \in \mathbb{Z}$. We beelden nu het paar (I, δ) af naar de kubus $C = (a_0, a_1, a_2, a_3)$. We laten

zien dat deze afbeelding welgedefinieerd is. Merk daartoe op dat de volgende gelijkheid geldt.

$$\begin{aligned}\pi\left(\frac{(x\alpha+y\beta)^3}{\delta}\right) &= \frac{\frac{\alpha^3-\bar{\alpha}^3}{\delta}x^3+3\frac{\alpha^2\beta-\bar{\alpha}^2\bar{\beta}}{\delta}x^2y+3\frac{\alpha\beta^2-\bar{\alpha}\bar{\beta}^2}{\delta}xy^2+\frac{\beta^3-\bar{\beta}^3}{\delta}y^3}{\sqrt{\Delta}}\\ &= \frac{(\tau-\bar{\tau})(a_0x^3+3a_1x^2y+3a_2xy^2+a_3y^3)+(1-1)(c_0x^3+3c_1x^2y+3c_2xy^2+c_3y^3)}{\sqrt{\Delta}}\\ &= \frac{(\tau-\bar{\tau})(a_0x^3+3a_1x^2y+3a_2xy^2+a_3y^3)}{\tau-\bar{\tau}}\\ &= C(x,y).\end{aligned}$$

Stel nu dat je de basis van I veranderd naar $\widetilde{\alpha}=a\alpha+b\beta$ en $\widetilde{\beta}=c\alpha+d\beta$, dan wordt $I=[\widetilde{\alpha},\widetilde{\beta}]$ door $\pi\left(\frac{(x\widetilde{\alpha}+y\widetilde{\beta})^3}{\delta}\right)=\pi\left(\frac{((ax+cy)\alpha+(bx+dy)\beta)^3}{\delta}\right)=C'(ax+cy,bx+dy)$ naar een equivalente vorm afgebeeld. Merk hierbij op dat $a,b,c,d\in\mathbb{Z}$ en $ad-bc=1$, omdat de basisverandering inverteerbaar is en het ideaal georiënteerd moet blijven. Andersom geldt ook dat als $C'=C^\gamma$, dan kunnen we de basis met γ veranderen om het ideaal naar C' te sturen. Als je verder het ideaal met een factor κ schaalt, dan wordt δ met een factor κ^3 geschaald, waardoor de factoren er boven en onder de deelstreep uitvallen en het equivalente ideaal naar dezelfde vorm wordt gestuurd. Hiermee hebben we de welgedefinieerdheid bewezen.

Vervolgens bewijzen we dat een kubische vorm C geassocieerd aan een paar (I,δ) daadwerkelijk discriminant Δ heeft. Neem allereerst aan dat $I=[1,\tau]$, $\delta=1$. Dan wordt (I,δ) naar de kubus A_{id} uit het vorige hoofdstuk gestuurd, welke gerelateerd is aan de kubische vorm $C_{\mathrm{id}}=(0,1,\epsilon,\frac{\Delta+3\epsilon}{4})$. Invullen geeft dat $\mathrm{Disc}(C_{\mathrm{id}})=\Delta+3\epsilon-3\epsilon^2=\Delta$. Transformeer nu δ naar $\delta'=a+b\bar{\tau}$, met $a,b\in\mathbb{Q}$. Uit de set vergelijkingen (4) volgt dan dat C_{id} wordt getransformeerd tot de kubische vorm $C=\frac{1}{N(\delta')}\left(b,a+b\epsilon,a\epsilon+b\frac{\Delta+3\epsilon}{4},a\frac{\Delta+3\epsilon}{4}+b\frac{\epsilon(2\Delta+2\epsilon)}{4}\right)$. De discriminant van deze kubische vorm is gelijk aan $\frac{\Delta}{N(\delta')^4}\left((a+\frac{b\epsilon}{2})^2-\Delta(\frac{b}{2})^2\right)^2=\frac{\Delta}{N(\delta')^4}N(\delta')^2=\frac{\Delta}{N(\delta')^2}$. Transformeer nu I tot een willekeurig gebroken ideaal $I'=[\alpha,\beta]$ met behulp van een transformatiematrix $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, waarbij $a,b,c,d\in\mathbb{Q}$ en, net als in het vorige hoofdstuk, $ad-bc=N(I')$. Dit betekent dat de kubische vorm wordt veranderd in $C'(x,y)=C(ax+cy,bx+dy)$ en uit de vorige paragraaf volgen specifieke formules voor p',q',r' en s'. Rekenen we hiermee de discriminant uit, dan blijkt deze geschaald te zijn met een factor $(ad-bc)^6=N(I')^6$. Als nu geldt dat $N(I')^3=N(\delta')$, dan volgt daaruit dat de discriminant van C', de kubische vorm geassocieerd aan het paar (I',δ'), gelijk is aan $\frac{N(I')^6}{N(\delta')^2}\Delta=\Delta$. Voor ieder willekeurige paar (I',δ') met $N(I')^3=N(\delta')$ geldt dat de discriminant van zijn geassocieerde kubische vorm gelijk is aan Δ.

Er rest nu slechts te bewijzen dat de afbeelding zowel surjectief als injectief is. Zij $C=(a_0,a_1,a_2,a_3)$ een kubische vorm van discriminant Δ en beschouw de verzameling vergelijkingen (4). In deze set van vier vergelijkingen staan zeven onbekenden, α, β, δ, c_0, c_1, c_2 en c_3. Net zoals het voorgaande hoofdstuk kunnen we de commutativiteit gebruiken, waarbij ons doel is om te laten zien dat c_0, c_1, c_2 en c_3 uniek bepaald zijn. Er geldt dus dat $(\alpha^2\beta)^2=(\alpha^3)(\alpha\beta^2)$ en $(\alpha\beta^2)=(\alpha^2\beta)(\beta^3)$. Bedenk dat $\tau^2=\epsilon\tau+\frac{\Delta-\epsilon}{4}$. Daarmee kun je deze vergelijkingen uitvermenigvuldigen en splitsen in de coëfficiënten van 1 en van τ, waardoor je de volgende vier

vergelijkingen vindt:

$$\begin{aligned} c_0c_2 + a_0a_2\frac{\Delta-\epsilon}{4} &= c_1^2 + a_1^2\frac{\Delta-\epsilon}{4} \\ c_0a_2 + c_2a_0 + \epsilon a_0a_2 &= 2c_1a_1 + \epsilon a_1^2 \\ c_1c_3 + a_1a_3\frac{\Delta-\epsilon}{4} &= c_2^2 + a_2^2\frac{\Delta-\epsilon}{4} \\ c_1a_3 + c_3a_1 + \epsilon a_1a_3 &= 2c_2a_2 + \epsilon a_2^2 \end{aligned}$$

Als je verder eist dat $[\alpha, \beta]$ georiënteerd is, dan blijkt deze set vergelijkingen een unieke oplossing te hebben. Deze wordt gegeven door

$$\begin{aligned} c_0 &= \frac{1}{2}(2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 - \epsilon a_0), \\ c_1 &= \frac{1}{2}(a_1^2a_2 - 2a_0a_2^2 + a_0a_1a_3 - \epsilon a_1), \\ c_2 &= -\frac{1}{2}(a_1a_2^2 - 2a_1^2a_3 + a_0a_2a_3 + \epsilon a_2), \\ c_3 &= -\frac{1}{2}(2a_2^3 - 3a_1a_2a_3 + a_0a_3^2 + \epsilon a_3). \end{aligned} \tag{5}$$

We zien dat c_i uniek bepaald worden door de kubische vorm (a_0, a_1, a_2, a_3). Nu moeten α en β bepaald worden. Net zoals in het vorige hoofdstuk kunnen deze niet uniek bepaald worden. Worden deze namelijk geschaald met een factor κ (en daarmee wordt δ geschaald met een factor κ^3), dan hebben we al gezien dat deze nieuwe variabelen dezelfde kubus geven. Omdat $\frac{\alpha}{\beta} = \frac{c_0+a_0\tau}{c_1+a_1\tau} = \frac{c_1+a_1\tau}{c_2+a_2\tau} = \frac{c_2+a_2\tau}{c_3+a_3\tau}$, geldt dat de verhouding tussen α en β wel uniek bepaald is. Als je nu α en β kiest, dan volgt δ uit vergelijkingen (4). Neem $\alpha = c_1 + a_1\tau$, $\beta = c_2 + a_2\tau$, dan volgt dat $\delta = \alpha\beta$. We moeten nu laten zien dat $[\alpha, \beta]$ een gebroken ideaal is. Omdat $\alpha, \beta \in \mathcal{O}(\sqrt{d})$, is het 'gebroken' gedeelte bewezen. Om te bewijzen dat het een ideaal is, is het voldoende om te bewijzen dat $\alpha\tau$ en $\beta\tau$ een element zijn van $[\alpha, \beta]$. Het blijkt dat

$$\begin{aligned} \alpha\tau &= \frac{a_0a_3 - a_1a_2 + \epsilon}{2}\alpha + (a_1^2 - a_0a_2)\beta \\ -\beta\tau &= (a_2^2 - a_1a_3)\alpha + \frac{a_0a_3 - a_1a_2 - \epsilon}{2}\beta \end{aligned}$$

Dit is expliciet uit te rekenen door de definitie van Δ, vergelijkingen (5) en $\tau^2 = \epsilon\tau + \frac{\Delta-\epsilon}{4}$ in te vullen. We hebben hiermee bewezen dat bij elke kubische vorm een unieke equivalentieklasse van paren (I, δ) hoort (wegens de uniciteit van de c_i). Daarmee is de surjectiviteit van de afbeelding bewezen. De injectiviteit volgt hier ook uit. Stel dat twee verschillende paren (I, δ) en (I', δ') naar twee equivalente kubische vormen C en C^γ afbeelden. Dan kun je (I', δ') door een basistransformatie met γ^{-1} naar C laten afbeelden. Wegens de uniciteit geldt nu dat (I, δ) en (I', δ') equivalent zijn. Daarmee is ook de injectiviteit van de afbeelding bewezen. We concluderen dat de afbeelding bijectief is en daarmee is de stelling bewezen. □

Ook nu is het interessant om te kijken naar primitieve kubussen. In dit geval zijn dat primitieve kubische vormen. We claimen dat een kubische vorm primitief is dan en slechts dan als $I^3 = \delta\mathcal{O}(\sqrt{d})$, waarbij (I, δ) zijn geassocieerde paar is. De makkelijkste manier om dit te zien is als volgt. Zij $(I, \delta) = ([\alpha, \beta], \delta)$ een paar met $N(I)^3 = N(\delta)$ en $I^3 \subseteq \delta\mathcal{O}(\sqrt{d})$. Zij $C = (a_0, a_1, a_2, a_3)$ zijn geassocieerde kubische vorm en bekijk zijn bijbehorende Bhargava-kubus $\iota(C)$. Als we de

afbeelding uit het vorige hoofdstuk bekijken om te zien aan welk drietal (I_1, I_2, I_3) deze Bhargava-kubus wordt geassocieerd, dan volgt uit vergelijkingen (3) en (5) dat

$$\begin{aligned} c_{1,1,1} &= \frac{1}{2}(2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 - \epsilon a_0) = c_0 \\ c_{1,1,2} = c_{1,2,1} = c_{2,1,1} &= \frac{1}{2}(a_1^2a_2 - 2a_0a_2^2 + a_0a_1a_3 - \epsilon a_1) = c_1 \\ c_{1,2,2} = c_{2,1,2} = c_{2,2,1} &= -\frac{1}{2}(a_1a_2^2 - 2a_1^2a_3 + a_0a_2a_3 + \epsilon a_2) = c_2 \\ c_{2,2,2} &= -\frac{1}{2}(2a_2^3 - 3a_1a_2a_3 + a_0a_3^2 + \epsilon a_3) = c_3 \end{aligned}$$

Volgen we de constructie van I_1, I_2 en I_3 verder, dan vinden we dat

$$\begin{aligned} I_1 &= [c_{1,1,1} + a_{1,1,1}\tau, c_{2,1,1} + a_{2,1,1}\tau] = [c_0 + a_0\tau, c_1 + a_1\tau] = [\frac{\alpha^3}{\delta}, \frac{\alpha^2\beta}{\delta}] = \frac{\alpha^2}{\delta}[\alpha, \beta] = \frac{\alpha^2}{\delta}I, \\ I_2 &= [c_{2,2,1} + a_{2,2,1}\tau, c_{2,2,2} + a_{2,2,2}\tau] = [c_2 + a_2\tau, c_3 + a_3\tau] = [\frac{\alpha\beta^2}{\delta}, \frac{\beta^3}{\delta}] = \frac{\beta^2}{\delta}[\alpha, \beta] = \frac{\beta^2}{\delta}I, \\ I_3 &= [(c_{1,1,1} + a_{1,1,1}\tau)^{-1}, (c_{2,2,2} + a_{2,2,2}\tau)^{-1}] = [\frac{\delta}{\alpha\beta^2}, \frac{\delta}{\alpha^2\beta}] = \frac{\delta}{\alpha^2\beta^2}[\alpha, \beta] = \frac{\delta}{\alpha^2\beta^2}I. \end{aligned}$$

We weten uit het vorige hoofdstuk dat $I_1I_2I_3 = \mathcal{O}(\sqrt{d})$ dan en slechts dan als zijn geassocieerde kubus primitief is. Daarnaast geldt dat C primitief is dan en slechts dan als $\iota(C)$ dat is. Hieruit volgt dat

$$I^3 = \delta\mathcal{O}(\sqrt{d}) \Leftrightarrow I_1I_2I_3 = \frac{I^3}{\delta} = \mathcal{O}(\sqrt{d}) \Leftrightarrow \iota(C) \text{ is primitief} \Leftrightarrow C \text{ is primitief.}$$

4.3 Compositie van kubische vormen

Door de bijectie die we in de vorige paragraaf gevonden hebben, volgt op een natuurlijke manier een vermenigvuldiging op de kubische vormen. Gegeven twee kubische vormen, berekenen we de paren (I, δ) en (I', δ'), die hierbij horen. Deze kunnen vervolgens vermenigvuldigd worden tot $(II', \delta\delta')$, waarna we weer de bijbehorende kubische vorm kunnen berekenen. In deze paragraaf laten we zien hoe dit moet voor twee algemene kubische vormen van discriminant Δ.

Zij $C = (a_0, a_1, a_2, a_3)$ en $C' = (a_0', a_1', a_2', a_3')$. Bereken de (unieke) bijbehorende c_i en c_i' volgens vergelijkingen (5). Definieer nu $I = [\alpha, \beta] = [c_1 + a_1\tau, c_2 + a_2\tau]$, $I' = [\alpha', \beta'] = [c_1' + a_1'\tau, c_2' + a_2'\tau]$. Dan worden δ en δ' gegeven door $\delta = \alpha\beta$, $\delta' = \alpha'\beta'$. Zoals gezegd is het nu de bedoeling om $(II', \delta\delta')$ te berekenen. Het is duidelijk dat $\delta\delta' = \alpha\alpha'\beta\beta'$. Het berekenen van II' is lastiger dan het in eerste instantie lijkt. Je moet namelijk II' vinden en niet een gebroken ideaal dat daaraan equivalent is, omdat $\delta\delta'$ dan ook geschaald moet worden. In hoofdstuk 2 zagen we dat $[\frac{N(\alpha)}{N([\alpha,\beta])}, \frac{-\frac{\mathrm{Tr}(\alpha\bar{\beta})}{N([\alpha,\beta])} + \sqrt{\Delta}}{2}] = \left(\frac{\bar{\alpha}}{N([\alpha,\beta])}\right)[\alpha, \beta]$ en, met behulp van het compositiealgoritme van Arndt uit hoofdstuk 1, dat $[a_1, \frac{-b_1+\sqrt{\Delta}}{2}][a_2, \frac{-b_2+\sqrt{\Delta}}{2}] = [\frac{a_1a_2}{n}, n\frac{-B+\sqrt{\Delta}}{2}]$. Hierbij is $B = \frac{2a_1b_2t + 2a_2b_1u + v(b_1b_2+\Delta)}{2n}$, waarbij $\beta = \frac{b_1+b_2}{2}$, $n = \mathrm{ggd}(a_1, a_2, \beta)$ en $t, u, v \in \mathbb{Z}$ zó dat $a_1t + a_2u + \beta v = n$. Hieruit volgt dat

$$\begin{aligned} II' &= [\alpha, \beta][\alpha', \beta'] = \left(\frac{N(I)N(I')}{\bar{\alpha}\bar{\alpha'}}\right)[\frac{N(\alpha)}{N(I)}, \frac{-\frac{\mathrm{Tr}(\alpha\bar{\beta})}{N(I)} + \sqrt{\Delta}}{2}][\frac{N(\alpha')}{N(I')}, \frac{-\frac{\mathrm{Tr}(\alpha'\bar{\beta'})}{N(I')} + \sqrt{\Delta}}{2}] \\ &= \left(\frac{N(I)N(I')}{\bar{\alpha}\bar{\alpha'}}\right)[\frac{N(\alpha)N(\alpha')}{N(I)N(I')n}, n\frac{-B+\sqrt{\Delta}}{2}], \end{aligned} \tag{6}$$

waarbij $n = \text{ggd}(\frac{N(\alpha)}{N(I)}, \frac{N(\alpha')}{N(I')}, \frac{\text{Tr}(\alpha\bar{\beta})N(I')+\text{Tr}(\alpha'\bar{\beta}')N(I)}{2N(I)N(I')})$, $t, u, v \in \mathbb{Z}$ zó dat $\frac{N(\alpha)}{N(I)}t + \frac{N(\alpha')}{N(I')}u + \frac{\text{Tr}(\alpha\bar{\beta})N(I')+\text{Tr}(\alpha'\bar{\beta}')N(I)}{2N(I)N(I')}v = n$ en $B = \frac{2N(\alpha)\text{Tr}(\alpha'\bar{\beta}')t+2N(\alpha')\text{Tr}(\alpha\bar{\beta})u+(\text{Tr}(\alpha\bar{\beta})\text{Tr}(\alpha'\bar{\beta}')+N(I)N(I')\Delta)v}{2nN(I)N(I')}$.
Dit kunnen we invullen in vergelijkingen 4. Bedenk hierbij dat $\sqrt{\Delta} = 2\tau - \epsilon$ en $\frac{N(\alpha)}{\bar{\alpha}} = \alpha$. Dan vinden we

$$\begin{aligned}
\widetilde{c_0} + \widetilde{a_0}\tau &= \frac{(\alpha\alpha')^2}{n^3\beta\beta'} \\
\widetilde{c_1} + \widetilde{a_1}\tau &= \frac{(\alpha\alpha')^2}{n\beta\beta'}\left(\frac{N(I)N(I')}{N(\alpha)N(\alpha')}\right)\left(\frac{-B-\epsilon}{2}+\tau\right) \\
\widetilde{c_2} + \widetilde{a_2}\tau &= \frac{n(\alpha\alpha')^2}{\beta\beta'}\left(\frac{N(I)N(I')}{N(\alpha)N(\alpha')}\right)^2\left(\frac{-B-\epsilon}{2}+\tau\right)^2 \\
\widetilde{c_3} + \widetilde{a_3}\tau &= \frac{n^3(\alpha\alpha')^2}{\beta\beta'}\left(\frac{N(I)N(I')}{N(\alpha)N(\alpha')}\right)^3\left(\frac{-B-\epsilon}{2}+\tau\right)^3
\end{aligned} \tag{7}$$

We definiëren dus de compositie als $C \circ C' = \widetilde{C} = (\widetilde{a_0}, \widetilde{a_1}, \widetilde{a_2}, \widetilde{a_3})$.

Stelling 4.2. *De inverse van een kubische vorm $C = (p, q, r, s)$ wordt gegeven door $C' = (p, -q, r, -s)$.*

Bewijs Bereken c_i en c_i' met behulp van vergelijkingen (5). Dan vind je dat

$$\begin{aligned}
c_0' &= \frac{1}{2}(-2q^3 + 3pqr - p^2s - \epsilon p) = -c_0 - \epsilon p, \\
c_1' &= \frac{1}{2}(q_1^2 r - 2pr^2 + pqs + \epsilon q) = c_1 + \epsilon q, \\
c_2' &= -\frac{1}{2}(-qr^2 + 2q^2 s - prs + \epsilon r) = -c_2 - \epsilon r, \\
c_3' &= -\frac{1}{2}(2r^3 - 3qrs + ps^2 - \epsilon s) = c_3 + \epsilon s.
\end{aligned}$$

Kies nu $I = [\alpha, \beta] = [c_0 + p\tau, c_1 + q\tau]$, waardoor $\delta = \alpha^2$. Kies $I' = [\alpha', \beta'] = [c_0' + p\tau, c_1' - q\tau] = [-c_0 + p(\tau - \epsilon), c_1 + q(-\tau + \epsilon)] = [-\bar{\alpha}, \bar{\beta}]$, waardoor $\delta' = \alpha'^2 = \bar{\alpha}^2 = \bar{\delta}$. Er geldt nu dat $N(\alpha') = N(-\bar{\alpha}) = N(\alpha)$, $N(I') = N(I)$ en $\text{Tr}(\alpha'\bar{\beta}') = \text{Tr}(-\bar{\alpha}\beta) = -\text{Tr}(\alpha\bar{\beta})$, waardoor $n = \frac{N(\alpha)}{N(I)}$. Vul dit in in vergelijking (6) en zie dat $II' = [N(I), N(I)\frac{-B+\sqrt{\Delta}}{2}]$. De waarde van B is hierbij niet belangrijk, maar bedenk wel dat deze dezelfde pariteit heeft als Δ en dus dezelfde pariteit als ϵ. Dit betekent dat $II' = [N(I), N(I)\frac{\epsilon+\sqrt{\Delta}}{2}] = (N(I))[1, \tau]$. Verder geldt volgens onze aannamen dat $N(I)^3 = N(\delta) = \delta\bar{\delta} = \delta\delta'$. Door nu het paar $([1, \tau], 1)$ te schalen met $N(I)$ (en dus het δ-gedeelte met $N(I)^3$), zien we dat $([1, \tau], 1)$ en $(II', \delta\delta')$ equivalent zijn en dus geassocieerd worden aan dezelfde kubische vorm: de identiteit. We concluderen dat C en C' elkaars inverse zijn. □

Stelling 4.3. *De primitieve kubische vormen van vaste discriminant Δ vormen een groep onder deze compositie.*

Bewijs

- De **geslotenheid** van deze compositie volgt uit het feit dat de vermenigvuldiging $(I, \delta) \circ (I', \delta') = (II', \delta\delta')$ gesloten is op de paren (I, δ) met $I^3 = \delta\mathcal{O}(\sqrt{d})$. Er geldt namelijk dat $(II')^3 = (I^3)(I'^3) = (\delta\mathcal{O}(\sqrt{d})(\delta'\mathcal{O}(\sqrt{d})) = \delta\delta'\mathcal{O}(\sqrt{d})$.

- De **associativiteit** van deze compositie volgt rechtstreeks uit de associativiteit van de ideaalvermenigvuldiging op gebroken idealen I en de associativiteit van de vermenigvuldiging van elementen $\delta \in \mathbb{Q}(\sqrt{\Delta})$.
- Er is een **identiteitselement**. Zoals gezien, wordt deze gegeven door

$$C_{\text{id}} = \begin{cases} 3x^2y + \frac{\Delta}{4}y^3 & \text{als } \Delta \equiv 0 \pmod 4 \\ 3x^2y + 3xy^2 + \frac{\Delta+3}{4}y^3 & \text{als } \Delta \equiv 1 \pmod 4 \end{cases}$$

- Voor elke primitieve kubische vorm $C = (p, q, r, s)$ is er een **inverse-element**. Deze wordt gegeven door $C^{-1} = (p, -q, r, -s)$ en deze is inderdaad ook primitief. Dit volgt uit de primitiviteit van C.

□

Wat is nu het verschil tussen de compositie van Bhargavakubussen en de compositie van kubische vormen? Opnieuw is dit afhankelijk van de discriminant Δ. Het ligt namelijk aan het aantal eenheden in $\mathcal{O}(\sqrt{d})$. Als je kijkt naar de definitie van equivalentie van paren (I, δ), dan zie je dat $(I, \delta) \sim (I', \delta')$ als er een κ is, zodat $(\kappa)I = I'$ en $\kappa^3\delta = \delta'$. Als ϵ nu een eenheid is in $\mathcal{O}(\sqrt{d})$, die géén derde macht is, dan zijn $([\alpha, \beta], \delta)$ en $([\alpha, \beta], \epsilon\delta)$ niet equivalent aan elkaar, maar worden ze geassocieerd aan de drietallen $(\frac{\alpha^2}{\delta}I, \frac{\beta^2}{\delta}I, \frac{\delta}{\alpha^2\beta^2}I)$ en $(\frac{\alpha^2}{\epsilon\delta}I, \frac{\beta^2}{\epsilon\delta}I, \frac{\epsilon\delta}{\alpha^2\beta^2}I)$, welke wel aan elkaar equivalent zijn. Dit betekent dat hun kubische vormen niet equivalent zijn, terwijl de geassocieerde Bhargavakubussen dit wel zijn. Als $\Delta < 0$ heeft $\mathcal{O}(\sqrt{d})$ geen eenheden, dus is de vermenigvuldiging aan elkaar gelijk. Als $\Delta > 0$ hoeft dit niet zo te zijn en kunnen niet equivalente kubische vormen naar equivalente kubussen worden afgebeeld.

4.4 Bijvoorbeeld

In de laatste paragraaf van elk hoofdstuk wordt een voorbeeld bekeken, waarbij de theorie van dat hoofdstuk wordt behandeld. Neem $\Delta = -23$ als vaste discriminant van onze kwadratische en kubische vormen. In dit voorbeeld berekenen we de compositie van $C = (1, 2, -2, 1)$ en $C' = (29, 6, 0, -1)$. Omdat $\Delta < 0$, verwachten we dat de compositie van de twee equivalent is aan de compositie van hun Bhargavakubussen. Bekijk de geassocieerde kwadratische vormen van deze kubische vormen. Voor C is deze gelijk aan $(6, 5, 2) \sim (2, -1, 3)$ en voor C' is deze gelijk aan $(36, -29, 6) \sim (2, -1, 3)$. We verwachten dus dat de kwadratische vorm van hun compositie equivalent is aan $(2, -1, 3) \circ (2, -1, 3) \sim (2, 1, 3)$.
Als we het compositiealgoritme volgen, vinden we dat $I = [c_1 + a_1\tau, c_2 + a_2\tau] = [-8 + 2\tau, 2 - 2\tau]$ en $\delta = (-8 + 2\tau)(2 - 2\tau) = 8 + 16\tau$. Evenzo vinden we dat $I' = [c_1' + a_1'\tau, c_2' + a_2'\tau] = [-90 + 6\tau, -36]$ en $\delta' = 3240 - 216\tau$. We oriënteren de idealen en gebruiken we vergelijkingen (7), waarbij $\alpha = 2 - 2\tau = 1 - \sqrt{-23}$, $\beta = -8 + 2\tau = -7 + \sqrt{-23}$, $\alpha' = -36$, $\beta' = -90 + 6\tau = -87 + 3\sqrt{-23}$, $N(\alpha) = 24$, $N(\alpha') = 1296$, $N(I) = 12$ en $N(I') = 216$. Verder vinden we $\text{Tr}(\alpha\bar{\beta}) = -60$ en $\text{Tr}(\alpha'\bar{\beta}') = 6264$, waardoor $n = 2$, $t = 1$, $u = 0$, $v = 0$ en $B = 29$. Dit levert uiteindelijk het volgende op:

$$\widetilde{c_0} + \widetilde{a_0}\tau = -2 - \sqrt{-23} = -1 - 2\tau,$$
$$\widetilde{c_1} + \widetilde{a_1}\tau = \frac{27 + 9\sqrt{-23}}{2} = 9 + 9\tau,$$
$$\widetilde{c_2} + \widetilde{a_2}\tau = \frac{-165 - 39\sqrt{-23}}{2} = -63 - 39\tau,$$
$$\widetilde{c_3} + \widetilde{a_3}\tau = \frac{947 + 161\sqrt{-23}}{2} = 393 + 161\tau.$$

We vinden dus dat $(1, 2, -2, 1) \circ (29, 6, 0, -1) = (-2, 9, -39, 161)$. Merk op dat de discriminant van deze vorm inderdaad gelijk is aan $\Delta = -23$ en dat zijn geassocieerde kwadratische vorm wordt gegeven door $(3, 29, 72) \sim (3, -1, 2) \sim (2, 1, 3)$, conform verwachting.

Als laatste geven we een voorbeeld van twee kubische vormen die niet equivalent zijn, maar wel dezelfde geassocieerde kubische vorm hebben (en waardoor hun Bhargavakubussen dus wel equivalent zijn). Volgens het argument uit de vorige paragraaf moet gelden dat $\Delta > 0$ en moeten er eenheden zijn in $O(\sqrt{d})$ (die geen derde macht zijn). Neem $\Delta = 8$. Deze heeft inderdaad eenheden die geen derde macht zijn, bijvoorbeeld $3 + \sqrt{8}$. Bekijk nu de kubische vormen $(0, 1, 4, 14)$ en $(2, 1, 0, -2)$. Deze hebben beide discriminant 8 en hun kwadratische vorm wordt gegeven door $(1, -4, 2)$. Ze zijn echter zeker niet equivalent, omdat $3x^2y + 12xy^2 + 14y^3 = y(3x^2 + 12xy + 14y^2)$, terwijl $2x^3 + 3x^2y - 2y^3$ niet kan worden gefactoriseerd. Ze kunnen dus niet equivalent zijn, omdat anders y naar $bx + dy$ wordt gestuurd en dus $2x^3 + 3x^2y - 2y^3$ gefactoriseerd zou moeten worden.

5 Conclusie en discussie

In deze scriptie is een compositie geconstrueerd op de kubische vormen aan de hand van idealen van de kwadratische uitbreidingen van $\mathbb{Q}$. Hiervoor hebben we allereerst de kwadratische vormen bestudeerd. Er zijn equivalentieklassen en een discriminant op deze kwadratische vormen gedefinieerd en vervolgens hebben we de compositie van Gauss bestudeerd met behulp van de Dirichlet-compositie. Dit werk heeft geleid tot het compositiealgoritme van Arndt. De volgende stap was om de bijectie te bekijken met equivalentieklassen van gebroken idealen van $\mathbb{Q}(\sqrt{\Delta})$. Deze bijectie gaf bijvoorbeeld een makkelijkere manier om kwadratische vormen te vermenigvuldigen, omdat dit makkelijker te doen is in de ideaaltheorie. In hoofdstuk 3 is de Bhargavakubus geïntroduceerd en ook deze structuur gaf een manier om kwadrische vormen te vermenigvuldigen. Belangrijker waren echter de compositie van de kubussen, welke een groepstructuur vastlegde op de primitieve Bhargavakubussen, en het verband tussen drietallen idealen in $\mathbb{Q}(\sqrt{\Delta})$ en de kubussen. Dit verband bracht ons er in hoofdstuk 4 toe om de bijectie tussen kubussen, die we relateerden aan kubische vormen, en idealen, die we driemaal met zichzelf vermenigvuldigen, te bekijken. Aan de hand van dit verband is uiteindelijk de compositie op kubische vormen gedefinieerd, waarbij we opnieuw het compositiealgoritme van Arndt hebben gebruikt.

Het is nu gelukt om een compositie op kubische vormen te definiëren. Net zoals bij de Gauss-compositie is het echter niet duidelijk wat de compositie is van twee willekeurige vormen. Het is wel mogelijk om deze compositie te berekenen, maar er zijn een aantal vragen over deze compositie onbeantwoord. De belangrijkste in mijn optiek is de vraag van de transformatie. Bij de Gauss-compositie was een transformatie van x_1x_2, x_1y_2, y_1x_2, y_1y_2 naar X, Y gegeven. Bij de compositie van kubische vormen is hier niets over bekend, omdat we de compositie zelf uitvoeren 'als het nog idealen zijn'. Vergelijk dit met de compositie van kwadratische vormen in hoofdstuk 2. Daar wordt ook geen woord gerept over deze transformatie, omdat er niets is om te transformeren: het is een simpele ideaalvermenigvuldiging. Een manier om hier achter te komen is om specifiek te gaan kijken naar de elementen van de idealen. We hebben gezien dat een basisverandering van een ideaal gelijk is aan een transformatie van de kwadratische of kubische vorm. Misschien dat als je specifiek gaat kijken welke elementen met welke elementen worden vermenigvuldigd bij de ideaalvermenigvuldiging, dit inzicht geeft in de transformatie van de kwadratische (waar we de transformatie al kennen) en kubische vormen. Een ander idee voor een vervolgonderzoek is om een 'Dirichlet-vermenigvuldiging' te zoeken voor de kubische vormen. Dit is dus een vermenigvuldiging die duidelijk waar is voor twee specifieke, maar niet te specifieke, vormen (inclusief expliciete transformatie) en dit vervolgens veralgemeniseerd kan worden tot vermenigvuldiging op equivalentieklassen. Dit laatste idee zou ook meer inzicht geven in de compositie van kubische vormen. Dit is namelijk iets wat op dit moment gemist wordt. Het is niet duidelijk waarom twee kubische vormen met elkaar vermenigvuldigd juist deze kubische vorm geven, behalve dat we dat zo gedefinieerd hebben. Dit is dan ook de conclusie van deze scriptie. We hebben inzichten opgedaan over de compositie van kwadratische vormen en een eerste stap gedaan om deze inzichten ook te vinden in de compositie van kubische vormen.

Referenties

[1] M. Bhargava. *Higher composition laws I: A new form on Gauss composition, and quadratic generalizations*. Annals of Mathematics, **159**, 217250, 2004. URL `http://annals.math.princeton.edu/wp-content/uploads/annals-v159-n1-p03.pdf`

[2] F. Bouyer. *Composition and Bhargava's Cubes*. URL `http://www2.warwick.ac.uk/fac/sci/maths/people/staff/bouyer/gauss_composition.pdf`

[3] D.A. Buell. *Binary Quadratic Forms*. Springer, New York, 1989.

[4] P. Dirichlet. *Vorlesungen über zahlentheorie*. F. Vieweg und sohn, Braunschweig, 1863. Hoofdstuk 4-5, pag. 138-314. URL `https://archive.org/stream/vorlesungenberz03dedegoog#page/n7/mode/2up`

[5] C. F. Gauss. *Disquisitiones Arithmeticae*. A. G. Fleischer, Leipzig, 1801. Hoofdstuk 5, pag. 120-380. URL `http://gdz.sub.uni-goettingen.de/dms/load/img/?PPN=PPN235993352&IDDOC=137206`