rijksuniversiteit groningen

faculteit Wiskunde en Natuurwetenschappen

Eenhedengroep van de ring $\mathbb{Z}[\sqrt[3]{m}]$

Bacheloronderzoek Wiskunde

Juli 2012

Student: E.J. Van Timmeren

Eerste Begeleider: Prof. dr. J. Top

Tweede Begeleider: Prof. dr. H. Waalkens

Samenvatting

In deze scriptie wordt de eenhedengroep bekeken van $\mathbb{Z}[\sqrt[3]{m}]$. Hierbij wordt gekeken of de theorie voor de eenhedengroep van $\mathbb{Z}[\sqrt{m}]$, $m > 0$ ook kan worden gebruikt bij het vinden van de eenhedengroep van $\mathbb{Z}[\sqrt[3]{m}]$. Er zal een bewijs voor het speciale geval van Dirichlets eenhedenstelling worden gegeven. Als laatste zal een voorbeeld worden gegeven voor het vinden van de eenheden van $\mathbb{Z}[\sqrt[3]{m}]$.

Inhoudsopgave

1 Introductie **4**

2 De norm van $\mathbb{Z}[\sqrt{m}]$ **5**

3 Het oplossen van de vergelijking van Pell met behulp van kettingbreuken **7**

3.1 Kettingbreuken 8

3.2 Vergelijking van Pell en kettingbreuken 12

4 Bewijs dat de vergelijking van Pell altijd een niet-triviale oplossing heeft **15**

4.1 Voortbrengers van de eenhedengroep 21

5 De norm van $\mathbb{Z}[\sqrt[3]{m}]$ **24**

6 Inbeddingen **26**

6.1 Inbeddingen van $\mathbb{Z}[\sqrt{m}]$ in $\mathbb{R}$ 26

6.2 Inbeddingen van $\mathbb{Z}[\sqrt[3]{m}]$ in $\mathbb{R}$ of $\mathbb{C}$ 28

7 Dirichlets Eenhedenstelling **35**

8 Eenhedengroep $\mathbb{Z}[\sqrt[3]{m}]^*$ **41**

8.1 De eenhedengroep $\mathbb{Z}[\sqrt[3]{5}]^*$ 41

9 Eenhedengroep van $\mathbb{Z}[\sqrt{m}]$ en Dirichlets eenhedenstelling. **45**

10 Conclusie **48**

11 Dankwoord **49**

A Met behulp van Mathematica eenheden bepalen van $\mathbb{Z}[\sqrt{m}]$ **51**

B Met behulp van Mathematica eenheden bepalen van $\mathbb{Z}[\sqrt[3]{m}]$ **53**

Hoofdstuk 1

Introductie

In deze scriptie wordt de eenhedengroep van $\mathbb{Z}[\sqrt[3]{m}]$ bekeken. We zullen de groepsstructuur van de eenhedengroep $\mathbb{Z}[\sqrt[3]{m}]^*$ bepalen. Voor het vinden van de eenhedengroep in $\mathbb{Z}[\sqrt[3]{m}]$ zal eerst worden gekeken naar de theorie over de eenhedengroep van $\mathbb{Z}[\sqrt{m}]$, waarbij m geen kwadraat is en $m > 0$. Hiervoor zal eerst de norm worden gegeven in het geval $\mathbb{Z}[\sqrt{m}]$. We zullen zien dat deze norm handig is bij het vinden van eenheden in $\mathbb{Z}[\sqrt{m}]^*$. Daarna zullen we een link geven tussen de vergelijking van Pell en de norm. We zullen een methode geven om de vergelijking van Pell op te lossen, met behulp van kettingbreuken. Daartoe zullen we eerst de theorie van kettingbreuken weergeven. Door het oplossen van de vergelijking van Pell kunnen we eenheden vinden van $\mathbb{Z}[\sqrt{m}]$. Tevens zullen een aantal voorbeelden worden gegeven zodat een duidelijk beeld wordt verkregen van de theorie. Bovendien zal een Mathematica script worden gegeven, zodat eenheden in $\mathbb{Z}[\sqrt{m}]$ kunnen worden gevonden.

In hoofdstuk 5 gaan we over tot de ring $\mathbb{Z}[\sqrt[3]{m}]$. Daartoe zullen we eerst opnieuw kijken naar $\mathbb{Z}[\sqrt{m}]$. We zullen de norm vinden met een andere methode dan in hoofdstuk 2 is gebruikt. Deze methode is handiger voor het vinden van de norm in $\mathbb{Z}[\sqrt[3]{m}]$. Om iets te kunnen zeggen over de structuur van de eenhedengroep van $\mathbb{Z}[\sqrt[3]{m}]$ maken we gebruik van inbeddingen. Ook deze zullen we proberen beter te begrijpen met behulp van $\mathbb{Z}[\sqrt{m}]$. Vervolgens zal een bewijs van Dirichlets eenhedenstelling worden gegeven in het geval van $\mathbb{Z}[\sqrt[3]{m}]$.

Als laatste zal met behulp van het computerprogramma Mathematica gekeken worden of er op een gemakkelijker manier dan het simpelweg proberen, eenheden kunnen worden gevonden in $\mathbb{Z}[\sqrt[3]{m}]$. De daarbij gebruikte methode passen we tenslotte ook toe op het vinden van eenheden in $\mathbb{Z}[\sqrt{m}]$.

Hoofdstuk 2

De norm van $\mathbb{Z}[\sqrt{m}]$

Dit hoofdstuk gaat over het bepalen van eenheden in $\mathbb{Z}[\sqrt{m}]$. We beperken ons hier tot $m \in \mathbb{Z}_{>0}$ die geen kwadraat zijn. In het eerste deel zal worden gekeken welke elementen uit deze ring een eenheid zouden kunnen zijn. Bovendien zullen we de norm bepalen en zien hoe we met behulp van die norm eenheden van $\mathbb{Z}[\sqrt{m}]$ kunnen vinden.

Zoals bekend is een element van een ring R een eenheid, als het voldoet aan de volgende eigenschap:

Definitie 1 *Zij R een ring met 1, een element $a \in R$ is een eenheid, als er een $b \in R$ bestaat zodanig dat:*

$$ab = ba = 1$$

(Voor achtergrondinformatie over ringen en eenheden, zie [2]). De verzameling van alle eenheden is de eenhedengroep van R, genoteerd als R^*.

De ring $\mathbb{Z}[\sqrt{m}]$ wordt gedefinieerd door: $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$, met m geen kwadraat, $m \neq 0$.
We kunnen een afbeelding als volgt definiëren:

Definitie 2 $N : \mathbb{Z}[\sqrt{m}] \to \mathbb{Z}$,

$$N(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2$$

Deze afbeelding N wordt de norm genoemd.

De norm voldoet aan de volgende eigenschappen:

- $N(\alpha)$ is de determinant van de $\mathbb{Z}$-lineaire afbeelding "vermenigvuldigen met α": $\mathbb{Z}[\sqrt{m}] \to \mathbb{Z}[\sqrt{m}]$
- $N(\alpha\beta) = N(\alpha)N(\beta)$
- $N(0) = 0$
- $N(1) = 1$

De tweede eigenschap volgt onmiddellijk uit de eerste eigenschap, vanwege de lineaire afbeelding.
Voor het vinden van eenheden in $\mathbb{Z}[\sqrt{m}]^*$ blijkt de norm een handig hulpmiddel, daarvoor gebruiken we stelling 1. Deze stelling is erg belangrijk in de rest van deze scriptie.

Stelling 1

$$\alpha \in \mathbb{Z}[\sqrt{m}]^* \Leftrightarrow N(\alpha) = \pm 1$$

Bewijs
($\Leftarrow$) $\alpha = a + b\sqrt{m}$ en we weten $N(\alpha) = \pm 1$. Daaruit volgt $(a + b\sqrt{m})(a - b\sqrt{m}) = \pm 1$. Dus $\pm(a - b\sqrt{m})$ is een inverse van α en dus $\alpha \in \mathbb{Z}[\sqrt{m}]^*$
($\Rightarrow$) $\alpha \in \mathbb{Z}[\sqrt{m}]^*$, dus er is een $\beta \in \mathbb{Z}[\sqrt{m}]^*$, zodat $\alpha\beta = 1$. Gebruik makend van de eigenschappen van de norm volgt $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$.
Omdat $N(\alpha), N(\beta) \in \mathbb{Z}$, volgt $N(\alpha) = N(\beta) = \pm 1$.

□

We zullen kort het geval bekijken dat m negatief is. In het geval $m = -1$ hebben we te maken met de ring van gehele getallen van Gauss, namelijk: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.
Voor het vinden van eenheden in $\mathbb{Z}[\sqrt{m}]$ met m negatief, levert:

$$a^2 - mb^2 = a^2 + |m|b^2 = \pm 1$$

Dit geeft $a = \pm 1$ en $b = 0$, en in het geval $|m| = 1$ ook nog $a = 0, b = \pm 1$. Zo verkrijgen we de volgende eenhedengroepen voor $m < 0$ en $m = -1$ respectievelijk:

$$\mathbb{Z}[\sqrt{m}]^* = \{1, -1\}$$
$$\mathbb{Z}[i]^* = \{1, i, -1, -i\}$$

We zijn verder niet in deze eenhedengroepen geïnteresseerd, omdat deze maar twee of vier elementen bevatten. We zullen in de rest van de scriptie aannemen dat $m > 0$ tenzij anders vermeld.

Hoofdstuk 3

Het oplossen van de vergelijking van Pell met behulp van kettingbreuken

In dit hoofdstuk zal het verband tussen de eenhedengroep van $\mathbb{Z}[\sqrt{m}]$ en de vergelijking van Pell worden bekeken. Vervolgens zullen we de vergelijking van Pell oplossen met behulp van kettingbreuken. Daartoe zullen we eerst de theorie van kettingbreuken behandelen.

De **Vergelijking van Pell** wordt gegeven door:

$$x^2 - my^2 = 1,\ m \in \mathbb{Z}_{\geq 1},\ m \text{ is geen kwadraat.} \tag{3.1}$$

We zagen in stelling 1, dat voor een eenheid α in $\mathbb{Z}[\sqrt{m}]$ geldt dat de norm gelijk is aan ± 1. Als $N(\alpha) = a^2 - mb^2 = 1$, dan is deze precies gelijk aan de vergelijking van Pell. Hieruit volgt onmiddelijk:

$$P := \{x + y\sqrt{m} : x^2 - my^2 = 1\} \subseteq \mathbb{Z}[\sqrt{m}]^*$$

Als we dus een niet-triviale oplossing voor de vergelijking van Pell kunnen vinden, dan zijn we in staat eenheden te vinden van $\mathbb{Z}[\sqrt{m}]$. We zien dus dat, als $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ een oplossing is van de vergelijking van Pell, dan is $x + y\sqrt{m} \in \mathbb{Z}[\sqrt{m}]^*$ een eenheid met norm 1. De eenheden met norm 1 vormen een ondergroep van $\mathbb{Z}[\sqrt{m}]^*$

De vergelijking van Pell heeft oneindig veel oplossingen (zoals zal worden bewezen in stelling 3 en stelling 5). We kunnen de vergelijking van Pell oplossen met behulp van kettingbreuken. Om dit te kunnen doen, zullen we eerst bekijken welke regels we nodig hebben omtrent kettingbreuken.

3.1 Kettingbreuken

Kettingbreuken worden gebruikt om irrationale reële getallen α te benaderen door breuken. We zullen de meeste bewijzen bij onderstaande stellingen weglaten, omdat dit niet het hoofddoel van deze scriptie is. De stellingen met bijbehorende bewijzen zijn te vinden in [4].

Een algemene eindige kettingbreuk heeft de vorm:

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cdots + \cfrac{1}{q_n}}}}. \tag{3.2}$$

Met $q_0 \in \mathbb{Z}$ en $q_j \in \mathbb{Z}_{\geq 1}$, $j \geq 1$
Om deze kettingbreuk als één breuk te kunnen schrijven, definiëren we het volgende:

- $[\emptyset] = 1$
- $[q_0] = q_0$
-

$$[q_0, q_1, \ldots, q_n] = q_n[q_0, \ldots, q_{n-1}] + [q_0, \ldots, q_{n-2}] \tag{3.3}$$

Deze definitie geldt ook voor reële getallen.
Een algemene eindige kettingbreuk is dan als volgt te schrijven:

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cdots + \cfrac{1}{q_n}}}} = \frac{[q_0, \ldots, q_n]}{[q_1, \ldots, q_n]}. \tag{3.4}$$

Om de notatie wat te vergemakkelijken, definiëren we het volgende:

$$\begin{aligned} A_n &= [q_0, \cdots q_n] \\ B_n &= [q_1, \cdots q_n] \end{aligned} \tag{3.5}$$

We zien hierbij onmiddellijk dat A_n en B_n gehele getallen zijn.

Het opbouwen van $\alpha \in \mathbb{R}$ met behulp van een kettingbreuk gaat als volgt:

$$\begin{aligned}
\alpha &= q_0 + \alpha' \ (\alpha' \text{ is het niet-gehele deel van } \alpha,\ \alpha' = \frac{1}{\alpha_1}) \\
\alpha &= q_0 + \frac{1}{\alpha_1} \ (\alpha_1 > 1) \\
\alpha_1 &= q_1 + \frac{1}{\alpha_2} \ (\alpha_2 > 1) \\
\alpha_n &= q_n + \frac{1}{\alpha_{n+1}} \ (\alpha_{n+1} > 1)
\end{aligned}$$

Hierbij is q_0 het grootste gehele getal kleiner gelijk α en q_j is het grootste gehele getal kleiner gelijk α_j, $j \geq 1$.
Daaruit volgt:

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cdots + \cfrac{1}{q_n + \cfrac{1}{\alpha_{n+1}}}}} = \frac{[q_0, q_1, \cdots, q_n, \alpha_{n+1}]}{[q_1, q_2, \cdots, q_n, \alpha_{n+1}]}$$

Nu volgt uit 3.3 en 3.5: $[q_0, \cdots, q_n, \alpha_{n+1}] = \alpha_{n+1}[q_0, \cdots q_n] + [q_0, \cdots, q_{n-1}] = \alpha_{n+1}A_n + A_{n-1}$. Zo kunnen we α dus op de volgende manier schrijven:

$$\alpha = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}}$$

Er is een relatie tussen A_n en B_n die we nog nodig zullen hebben, namelijk:

Lemma 1 $A_nB_{n-1} - B_nA_{n-1} = (-1)^{n-1}$

Bewijs
We kunnen de volgende formules afleiden voor A_n en B_n met behulp van 3.3.

$$\begin{aligned}
A_n &= [q_0, \cdots q_n] = q_n[q_0, \ldots, q_{n-1}] + [q_0, \ldots, q_{n-2}] = q_nA_{n-1} + A_{n-2} \\
B_n &= [q_1, \cdots q_n] = q_n[q_1, \ldots, q_{n-1}] + [q_1, \ldots, q_{n-2}] = q_nB_{n-1} + B_{n-2}
\end{aligned}$$

Deze formules kunnen we invullen:

$$\begin{aligned}
A_nB_{n-1} - B_nA_{n-1} &= (q_nA_{n-1} + A_{n-2})B_{n-1} - (q_nB_{n-1} + B_{n-2})A_{n-1} \\
&= -(A_{n-1}B_{n-2} - B_{n-1}A_{n-2})
\end{aligned}$$

Hier zien we dat $f(n) = A_nB_{n-1} - B_nA_{n-1}$ gelijk is aan $-f(n-1)$. Daarbij kunnen we de volgende vergelijking opstellen: $f(n) = -f(n-1) = +f(n-2) = \ldots = \pm f(1)$ waarbij

$$f(n) = \begin{cases} +f(1) & \text{als } n \text{ is oneven} \\ -f(1) & \text{als } n \text{ is even} \end{cases}$$

Nu rest nog om de waarde van $f(1)$ te berekenen: $f(1) = A_1B_0 - B_1A_0 = [q_0, q_1]\cdot 1 - q_1 \cdot q_0 = (q_0q_1 + 1) - q_0q_1 = 1$

□

We kunnen nu iets zeggen over de benadering van

$$\alpha = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}} \text{ door } \frac{A_n}{B_n}$$

namelijk het verschil wordt gegeven door:

$$\alpha - \frac{A_n}{B_n} = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}} - \frac{A_n}{B_n} = \frac{A_{n-1}B_n - B_{n-1}A_n}{B_n(\alpha_{n+1}B_n + B_{n-1})} = \frac{\pm 1}{B_n(\alpha_{n+1}B_n + B_{n-1})}$$

Waar het laatste gelijkteken volgt uit lemma 1. We weten: $\alpha_{n+1} > q_{n+1}$, dus verkrijgen we de volgende afschatting:

$$\left|\alpha - \frac{A_n}{B_n}\right| < \frac{1}{B_nB_{n+1}} \tag{3.6}$$

We weten dat B_n en B_{n+1} gehele getallen zijn die monotoon stijgen, dus B_n wordt groter naarmate n stijgt. Hieruit volgt:

$$\lim_{n\to\infty} \frac{A_n}{B_n} = \alpha$$

Bovendien zien we:

$$\left|\alpha - \frac{A_n}{B_n}\right| < \frac{1}{B_n^2}$$

Zo zien we dus dat kettingbreuken een hele goede benadering kunnen geven van een $\alpha \in \mathbb{R}$,

Een kettingbreuk is puur periodiek, als na een bepaalde q_n de reeks weer opnieuw wordt begonnen met q_0. Dus een getal β heeft een puur periodieke kettingbreuk, als het geschreven kan worden als:

$$\beta = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cdots + \cfrac{1}{q_n + \cfrac{1}{q_0 + \cfrac{1}{q_1 + \cdots}}}}}$$

Stelling 2 *Een kwadratisch irrationaal getal α heeft een puur periodieke kettingbreuk als α groter dan 1 is en als zijn geconjugeerde tussen -1 en 0 ligt.*

Voor het oplossen van de vergelijking van Pell hebben we de kettingbreuk van een wortel nodig. Zeg $\sqrt{m}$, m geen kwadraat. De geconjugeerde van $\sqrt{m} = q_0 + \ldots$ is $-\sqrt{m} = -q_0 + \ldots$. Hier zien we dus dat de geconjugeerde niet tussen 0 en 1 ligt. Nemen we nu de wortel $\sqrt{m} + q_0$, dan is de geconjugeerde $0 < -\sqrt{m} + q_0 < 1$. Uit stelling 2 volgt nu dat de kettingbreuk van $\sqrt{m} + q_0$ puur periodiek is. Dus

$$\sqrt{m} + q_0 = 2q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cdots + \cfrac{1}{q_n + \cfrac{1}{2q_0 + \cfrac{1}{q_1 + \cdots}}}}}$$

Daaruit volgt dat elke willekeurige wortel uit de natuurlijke getallen, die geen kwadraat zijn, te schrijven is als:

$$\sqrt{m} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cdots + \cfrac{1}{q_n + \cfrac{1}{2q_0 + \cfrac{1}{q_1 + \cdots}}}}}$$

We zullen hieronder twee voorbeelden van kettingbreuken bekijken, omdat we deze breuken nog vaker terug zullen zien.

Voorbeeld 1 We zullen nu de kettingbreuk van $\sqrt{5}$ uitrekenen.

$$\sqrt{5} = 2 + (\sqrt{5} - 2) = 2 + \frac{1}{\frac{1}{\sqrt{5}-2}} = 2 + \frac{1}{\frac{\sqrt{5}+2}{(\sqrt{5}-2)(\sqrt{5}+2)}} = 2 + \frac{1}{\sqrt{5}+2}$$

$$= 2 + \frac{1}{2 + 2 + (\sqrt{5} - 2)} = 2 + \cfrac{1}{4 + \cfrac{1}{\cfrac{1}{\sqrt{5} - 2}}} = 2 + \cfrac{1}{4 + \cfrac{1}{\sqrt{5} + 2}}$$

$$= 2 + \cfrac{1}{4 + \cfrac{1}{4 + \cdots}}$$

We zien hier dus $q_0 = 2$ en $2q_0 = 4$.

Voorbeeld 2 Op dezelfde manier als in voorbeeld 1 kunnen we de kettingbreuk van $\sqrt{3}$ bepalen. Deze wordt gegeven door:

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cdots}}}}$$

Hier zien we $q_0 = 1$, $q_1 = 1$ en $2q_0 = 2$.

3.2 Vergelijking van Pell en kettingbreuken

We zullen nu verder gaan met het oplossen van de vergelijking van Pell (zie vergelijking 3.1), $x^2 - my^2 = 1,\ m \in \mathbb{N}$, m geen kwadraat met behulp van kettingbreuken. Allereerst zullen we $\sqrt{m}$ schrijven als kettingbreuk:

$$\begin{aligned}\sqrt{m} &= q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cdots + \cfrac{1}{q_n + \cfrac{1}{2q_0 + \cfrac{1}{q_1 + \cdots}}}}} \\ &= q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cdots + \cfrac{1}{q_n + \cfrac{1}{m_{n+1}}}}}\end{aligned}$$

Daaruit volgt:

$$m_{n+1} = 2q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cdots}} = \sqrt{m} + q_0$$

We kunnen $\sqrt{m}$ dus schrijven als volgt:

$$\sqrt{m} = \frac{(\sqrt{m} + q_0)A_n + A_{n-1}}{(\sqrt{m} + q_0)B_n + B_{n-1}}$$

Daaruit volgt:

$$\begin{aligned}\sqrt{m}(\sqrt{m}+q_0)B_n+\sqrt{m}B_{n-1}&=(\sqrt{m}+q_0)A_n+A_{n-1}\\ mB_n+\sqrt{m}q_0B_n+\sqrt{m}B_{n-1}&=\sqrt{m}A_n+q_0A_n+A_{n-1}\\ mB_n+(q_0B_n+B_{n-1})\sqrt{m}&=q_0A_n+A_{n-1}+\sqrt{m}A_n\end{aligned}$$

We weten dat $\sqrt{m}$ irrationaal is en dat $q_0, B_n, B_{n-1}, A_n, A_{n-1}$ gehele getallen zijn. Daarom kunnen we de volgende paar vergelijkingen opstellen:

$$\begin{aligned}mB_n&=q_0A_n+A_{n-1}\text{ en}\\ q_0B_n+B_{n-1}&=A_n\end{aligned}$$

Dit kunnen we oplossen voor A_{n-1} en B_{n-1}.

$$\begin{aligned}A_{n-1}&=mB_n-q_0A_n\text{ en}\\ B_{n-1}&=A_n-q_0B_n\end{aligned}$$

We gebruiken nu lemma 1 voor de relatie tussen A_n en B_n, waarbij we de gevonden formules voor A_{n-1} en B_{n-1} invullen.

$$\begin{aligned}A_nB_{n-1}-B_nA_{n-1}&=(-1)^{n-1}\\ A_n(A_n-q_0B_n)-B_n(mB_n-q_0A_n)&=(-1)^{n-1}\\ An^2-q_0A_nB_n-mB_n^2+q_0A_nB_n&=(-1)^{n-1}\\ A_n^2-mB_n^2&=(-1)^{n-1}\end{aligned}$$

Als we nu $x=A_n$ en $y=B_n$ nemen, hebben we een oplossing voor de vergelijking van Pell gevonden, in het geval dat n is oneven. Maar we weten dat, voor het vinden van de eenheden in $\mathbb{Z}[\sqrt{m}]$, het genoeg was, dat de norm gelijk was aan ±1, dus: $a^2-mb^2=\pm1$. We zien dus dat, met deze methode en het nemen van $x=A_n$ en $y=B_n$, we een eenheid hebben gevonden voor elke positieve $\sqrt{m}$ die geen kwadraat is. Het is een stelling dat deze methode altijd de kleinste oplossing groter dan 1 voor de vergelijking van Pell geeft. In stelling 3 en 5 zal worden bewezen dat er voor de vergelijking van Pell een kleinste, niet-triviale, oplossing bestaat. Ook zal blijken dat alle andere eenheden met behulp van deze kleinste eenheid gevonden kunnen worden.

Vervolg voorbeeld 1 We hebben voor $\sqrt{5}$ de volgende kettingbreuk gevonden:

$$\sqrt{5}=2+\cfrac{1}{4+\cfrac{1}{4+\cfrac{1}{\cdots}}}$$

We zagen: $q_0 = 2$. Hieruit volgt dat $A_n = [q_0] = [2] = 2$ en $B_n = [\emptyset] = 1$, dus $x = 2$, $y = 1$. Zo vinden we dus dat de norm wordt gegeven door $2^2 - 5 \cdot 1^2 = -1$. De kleinste eenheid in $\mathbb{Z}[\sqrt{5}]^*$ is dus: $2 + \sqrt{5}$. Een inverse voor $2 + \sqrt{5}$ wordt gegeven door: $-2 + \sqrt{5}$. Voor een oplossing van de vergelijking van Pell, kunnen we deze eenheid kwadrateren, zo verkrijgen we een x en y die voldoen aan $x^2 - my^2 = 1$. Zo vinden we $(2+\sqrt{5})^2 = 9+4\sqrt{5}$, dus $x = 9$ en $y = 4$.

Vervolg voorbeeld 2 We weten

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cdots}}}}$$

Dus $A_n = [1, 1] = 1[1] + 1 = 1 \cdot 1 + 1 = 2$ en $B_n = [1] = 1$. Hieruit volgt dat $2^2 - 3 \cdot 1^2 = 1$. De kleinste eenheid in $\mathbb{Z}[\sqrt{3}]^*$ wordt dus gegeven door: $2 + \sqrt{3}$.

In bijlage A is een mathematica script te vinden die eenheden voor elke willekeurige m, m geen kwadraat en m positief, de kleinste eenheid berekent van de ring $\mathbb{Z}[\sqrt{m}]$ en enkele machten daarvan. Zo kunnen we dus zonder "trial and error"de kleinste eenheid berekenen. Vervolgens kunnen we dan met stelling 6 de complete structruur van $\mathbb{Z}[\sqrt{m}]^*$ bepalen, zoals we aan het einde van hoofdstuk 4 zullen zien voor $\sqrt{3}$ en $\sqrt{5}$.

Hoofdstuk 4

Bewijs dat de vergelijking van Pell altijd een niet-triviale oplossing heeft

In deze pargraaf werken we toe naar een bewijs dat de vergelijking van Pell altijd een niet-triviale oplossing heeft. In het vorige hoofdstuk hebben we dit al gezien, namelijk door het oplossen van de vergelijking van Pell met behulp van kettingbreuken. We zullen in dit hoofdstuk, met een bewijs gegeven door Dirichlet, bewijzen dat de vergelijking van Pell altijd een niet-triviale oplossing heeft, dit is terug te vinden in [7]. Om dit te kunnen bewijzen hebben we eerst wat voorkennis nodig, die zal worden genoemd in onderstaande stellingen en lemma's (uit [7]).

Lemma 2 *Beschouw de verzameling gehele getallen van de vorm: $x \pm y\sqrt{m}$, waarbij x, y een niet negatieve gehele oplossing (mag triviaal zijn) voor de vergelijking van Pell (3.1) is (m is positief en geen kwadraat). Deze verzameling vormt een ondergroep van de vermenigvuldigingsgroep van positieve reële getallen.*

Bewijs
De verzameling $H = x \pm y\sqrt{m}$ is een ondergroep als voldaan is aan:
i) $e = 1 + 0\sqrt{m} \in H$. Om te laten zien dat $e \in H$, moeten we laten zien dat $(1, 0)$ een oplossing is van de vergelijking van Pell. Dus $1 - m * 0 = 1$. Dit is zeker waar, dus $e \in H$.

ii) $\forall x_1 \pm y_1\sqrt{m},\ x_2 \pm y_2\sqrt{m} \in H$ geldt $x \cdot y \in H$.
We gebruiken nu de volgende vermenigvuldigingen: $(x_1 + y_1\sqrt{m})(x_2 + y_2\sqrt{m}) = (x_1x_2 + y_1y_2m) + (x_1y_2 + x_2y_1)\sqrt{m}$ en $(x_1 - y_1\sqrt{m})(x_2 - y_2\sqrt{m}) = (x_1x_2 + y_1y_2m) - (x_1y_2 + x_2y_1)\sqrt{m}$.
Als we nu controleren dat $x = x_1x_2 + y_1y_2m$ en $y = x_1y_2 + x_2y_1$ een oplossing van de vergelijking van Pell is, dan $x \cdot y \in H$.

$x^2 = (x_1x_2 + y_1y_2m)(x_1x_2 + y_1y_2m) = x_1^2x_2^2 + 2x_1x_2y_1y_2m + y_1^2y_2^2m^2$,
$y^2 = (x_1y_2 + x_2y_1)(x_1y_2 + x_2y_1) = x_1^2y_2^2 + x_2^2y_1^2 + 2x_1y_2x_2y_1$.
Dit vullen we in in de vergelijking van Pell:
$x^2 - my^2 = x_1^2x_2^2 + 2x_1x_2y_1y_2m + y_1^2y_2^2m^2 - x_1^2y_2^2m - x_2^2y_1^2m - 2x_1y_2x_2y_1m = x_1^2x_2^2 + y_1^2y_2^2m^2 - x_1^2y_2^2m - x_2^2y_1^2m = (x_1^2 - my_1^2)(x_2^2 - my_2^2) = 1 \cdot 1 = 1$

iii) $\forall x + y\sqrt{m}$ geldt $x^{-1} \in H$. Dit volgt onmiddellijk uit $1 + 0\sqrt{m} = 1 = x^2 - my^2 = (x + y\sqrt{m})(x - y\sqrt{m})$. Daaruit volgt onmiddellijk dat $x^{-1} \in H$.

□

Stelling 3 *Als de vergelijking van Pell een niet-triviale oplossing heeft, dan zijn er oneindig veel. Namelijk stel dat (x_1, y_1) de kleinste oplossing is, dat wil zeggen $x_1 > 1, y_1 > 0$ met een zo klein mogelijke x_1 en y_1. $x_1 + y_1\sqrt{m}$ is dan een eenheid is met norm 1. Dan worden de andere positieve eenheden met norm 1 berekend door: $(x_1 + y_1\sqrt{m})^n = x_n + y_n\sqrt{m}$, $n \in \mathbb{Z}_{\geq 0}$. Waarbij (x_n, y_n) een oplossing voor de vergelijking van Pell is.*

Bewijs
De vergelijking van Pell wordt gegeven door: $x^2 - my^2 = 1$, herschrijven we dit, dan verkrijgen we: $x^2 = 1 + my^2$. We zien door de vorm van deze vergelijking dat x groeit op het moment dat y groeit. Dus als er een niet-triviale oplossing is, dan volgt hieruit dat er een kleinste is met $x_1 > 1$ en $y_1 > 0$. We noemen voor het gemak deze kleinste oplossing $\delta = x_1 + y_1\sqrt{m}$. Dus $1 = \delta^0 < \delta < \delta^2 < \cdots$. Stel nu dat (x, y) een oplossing voor de vergelijking van Pell is. Door gebruik van de Archimedische eigenschap van de reële getallen te maken, weten we dat er een $n \in \mathbb{N}$ is, zodat:

$$\delta^n \leq x + y\sqrt{m} < \delta^{n+1}. \tag{4.1}$$

Als we nu kunnen aantonen dat $x + y\sqrt{m} = \delta^n$, dan zien we dat er tussen δ^n en δ^{n+1} geen andere oplossing voor de vergelijking van Pell bestaat, en is het bewijs geleverd.
Vergelijking 4.1 kunnen we als volgt schrijven:

$$x_n + y_n\sqrt{m} \leq x + y\sqrt{m} < x_{n+1} + y_{n+1}\sqrt{m}, \text{ en dus volgt}$$
$$1 \leq (x + y\sqrt{m})(x_n - y_n\sqrt{m}) < x_1 + y_1\sqrt{m}.$$

Het laatste volgt uit: $x_{n+1} + y_{n+1}\sqrt{m} = (x_n + y_n\sqrt{m})(x_1 + y_1\sqrt{m})$. We weten dat $x_1 + y_1\sqrt{m}$ minimaal is. Uit lemma 2 volgt dat een product van twee oplossingen nog steeds een oplossing van de vergelijking van Pell is. Daaruit volgt dat:

$$(x + y\sqrt{m})(x_n - y_n\sqrt{m}) = 1, \text{ en daarom}$$
$$x + y\sqrt{m} = x_n + y_n\sqrt{m}.$$

We zien hieruit dat tussen δ^n en δ^{n+1} geen andere oplossing van de vergelijking van Pell ligt. Dus worden alle oplossingen gegeven door een veelvoud van de kleinste oplossing, mits er een niet triviale oplossing bestaat.

□

Voordat we verder gaan, zullen we eerst het Ladenprincipe geven, zie [1]. We zullen dit niet bewijzen, omdat de stelling triviaal is. We hebben het Ladenprincipe nodig bij lemma 3. Bovendien zullen we het Ladenprincipe nog nodig hebben om aan te tonen dat $\mathbb{Z}[\sqrt[3]{m}]^* \neq \{\pm 1\}$.

Stelling 4 ***Ladenprincipe*** *Als n objecten worden verdeeld in m niet-lege verzamelingen, met $n > m$, dan is er minstens één m die meer dan één object bevat.*

Als (x, y) een oplossing van de vergelijking van Pell is, dan vormt $\frac{x}{y}$ een goede benadering van $\sqrt{m}$.

$$\begin{aligned} x^2 - my^2 &= 1 \\ \frac{x^2}{y^2} - m &= \frac{1}{y^2} \\ \frac{x^2}{y^2} &= m + \frac{1}{y^2} \\ \frac{x}{y} &= \sqrt{m + \frac{1}{y^2}} = \sqrt{m} + \frac{\theta}{y},\ 0 < \theta < 1 \end{aligned}$$

Dit is precies wat we ook zagen bij de kettingbreuken. We konden een oplossing van de vergelijking van Pell vinden met behulp van $x = A_n$ en $y = B_n$. We zagen daarbij dat $|\sqrt{m} - \frac{A_n}{B_n}| < \frac{1}{B_n B_{n-1}}$ (zie formule 3.6).

Lemma 3 *Zij q een irrationaal getal. Er zijn oneindig veel rationale getallen $\frac{x}{y}$ (met x, y relatief priem, dat is $ggd(x, y) = 1$), zodat:*
$0 < |q - \frac{x}{y}| < \frac{1}{y^2}$

Bewijs
We zullen eerst bewijzen dat het volgende geldt:
Voor een getal $n \in \mathbb{N}_{>1}$ geldt: er zijn gehele getallen x, y met $0 < y \leq n$, zodat:
$0 < |q - \frac{x}{y}| < \frac{1}{ny}$

We nemen $n + 1$ getallen: $\{0q\}, \{1q\}, \cdots \{nq\}$. Waarbij $\{\alpha\} = a - \lfloor a \rfloor$, (met $\lfloor a \rfloor$ de floor functie) dus het niet-gehele deel van α. Deze $n + 1$ getallen zijn paarsgewijs disjunct, namelijk stel dat er twee hetzelfde zijn, zeg: $\{iq\} = \{jq\}$, dan volgt: $iq - \lfloor iq \rfloor = jq - \lfloor jq \rfloor$. Hieruit volgt dat $q = \frac{\lfloor iq \rfloor - \lfloor jq \rfloor}{i-j}$. Dit is een rationaal getal. Hieruit volgt een tegenstelling, want q is een irrationaal getal en dus volgt $i = j$.

We hebben dus $n+1$ paarsgewijs disjuncte getallen.
We kunnen het interval $[0,1)$ opdelen in n gelijke stukken op de volgende manier: $[0,\frac{1}{n}),[\frac{1}{n},\frac{2}{n}),\cdots,[\frac{n-1}{n},1)$. We maken nu een afbeelding die $\{iq\}$ stuurt naar het deelinterval dat $\{iq\}$ bevat. We zien dat we n deelintervallen hebben en dat we $n+1$ getallen hebben. Nu volgt uit het Ladenprincipe (stelling 4) dat er twee disjuncte getallen zich in hetzelfde interval bevinden, zeg $\{iq\}$ en $\{jq\}$ met $i>j$. Dus

$$\begin{aligned} 0 < |\{iq\} - \{jq\}| &< \frac{1}{n} \\ 0 < |(i-j)q - (\lfloor iq \rfloor - \lfloor jq \rfloor)| &< \frac{1}{n} \\ 0 < |yq - x| &< \frac{1}{n} \end{aligned}$$

De laatste vergelijking volgt uit het hernoemen van variabelen: $x = \lfloor iq \rfloor - \lfloor jq \rfloor$ en $y = i-j$.
Delen door y geeft het gewenste resultaat:
$0 < |q - \frac{x}{y}| < \frac{1}{ny}$.
Vanwege onze keuze van y, namelijk $0 < y \leq n$, volgt $\frac{1}{ny} \leq \frac{1}{y^2}$.
En hieruit volgt het bewijs van lemma 3: $0 < |q - \frac{x}{y}| < \frac{1}{y^2}$.

□

Stelling 5 *De vergelijking van Pell, $x^2 - my^2 = 1$, m geen kwadraat, heeft een niet-triviale oplossing.*

Bewijs
Allereerst passen we lemma 3 toe op de vergelijking:

$$x^2 - my^2 = k \tag{4.2}$$

Voor een geheel getal k dat voldoet aan: $|k| < 1 + 2\sqrt{m}$, laten we zien dat vergelijking 4.2 oneindig veel oplossingen heeft. Laat x, y voldoen aan:

$$\begin{aligned} |\sqrt{m} - \frac{x}{y}| &< \frac{1}{y^2} \\ |y\sqrt{m} - x| &< \frac{1}{y} \end{aligned}$$

De eerste regel volgt uit lemma 3. Hieruit kunnen we de restrictie voor k afleiden, namelijk:

$$
\begin{aligned}
|k| = |x^2 - my^2] &= |x - y\sqrt{m}| \cdot |x + y\sqrt{m}| \\
&= |x - y\sqrt{m}| \cdot |x - y\sqrt{m} + 2y\sqrt{m}| \\
&\leq |x - y\sqrt{m}| \cdot (|x - y\sqrt{m}| + 2y\sqrt{m}) \\
&< \frac{1}{y}(\frac{1}{y} + 2y\sqrt{m}) \\
&= \frac{1}{y^2} + 2\sqrt{m} \\
&\leq 1 + 2\sqrt{m}
\end{aligned}
$$

De ongelijkheid $|x^2 - my^2] < 1 + 2\sqrt{m}$ heeft oneindig veel gehele oplossingen x, y en dus heeft $x^2 - my^2 = k$ oneindig veel oplossingen voor een bepaalde k.
Volgens lemma 2 geeft het vermenigvuldigen van twee oplossingen van de vergelijking van Pell een nieuwe oplossing van de vergelijking van Pell. Nu volgt dat het vermenigvuldigen van een oplossing van de vergelijking van Pell met een oplossing van de vergelijking 4.2 een nieuwe oplossing geeft voor vergelijking 4.2. Daaruit volgt dat, als we twee oplossingen van vergelijking 4.2 delen, die dezelfde waarde voor $x^2 - my^2$ hebben, we een oplossing van de vergelijking van Pell verkrijgen. Het nadeel hieraan is dat deze oplossing niet geheel hoeft te zijn. Toch kunnen we hiermee bewijzen dat er altijd een niet-triviale gehele oplossing is.

Stel x_1, y_1 en x_2, y_2 zijn twee oplossingen van 4.2, dan:

$$
\begin{aligned}
\frac{x_1 + y_1\sqrt{m}}{x_2 + y_2\sqrt{m}} &= \frac{x_1 + y_1\sqrt{m}}{x_2 + y_2\sqrt{m}} \cdot \frac{x_1 - y_1\sqrt{m}}{x_2 - y_2\sqrt{m}} \\
&= \frac{(x_1x_2 - y_1y_2m) - (x_1y_2 - x_2y_1)\sqrt{m}}{k} \\
&= \frac{x_1x_2 - y_1y_2m}{k} - \frac{x_1y_2 - x_2y_1}{k}\sqrt{m} \\
&= x + y\sqrt{m}
\end{aligned}
$$

Waarbij de laatste vergelijking volgt uit het hernoemen van variabelen. Het blijkt handig om de volgende berekening uit te voeren:

$$
\begin{aligned}
k^2(x^2 - my^2) &= (kx)^2 - m(ky)^2 \\
&= (x_1x_2 - y_1y_2m)^2 - m(x_1y_2 - x^2y_1)^2 \\
&= x_1^2(x_2^2 - my_2^2) + my_1^2(my_2^2 - x_2^2) \\
&= x_1^2k - kmy_1^2 \\
&= k(x_1^2 - my_1^2) \\
&= k^2
\end{aligned}
$$

Daaruit volgt dus dat $x^2 - my^2 = 1$, met

$$x = \frac{|x_1x_2 - y_1y_2m|}{|k|} \text{ en } y = \frac{|x_1y_2 - x_2y_1|}{|k|}$$

Nu rest ons nog om te laten zien dat (x_1, y_1) en (x_2, y_2) zo gekozen kunnen worden, dat de oplossing (x, y) voor de vergelijking van Pell geheel is en dat $x \neq 1$ en $y \neq 0$.

We kunnen een equivalentierelatie opbouwen, namelijk twee oplossingen voor 4.2 zijn equivalent, als geldt:
$(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow x_1 \equiv x_2 \bmod k$ en $y_1 \equiv y_2 \bmod k$
Door de oneindigheid van het aantal oplossing van 4.2 kunnen we altijd een klasse vinden die twee verschillende paren getallen heeft, die voldoen aan deze equivalentierelatie. Zeg dat die twee paren (x_1, x_2) en (y_1, y_2) zijn. We gaan nu aantonen dat $x_1x_2 - y_1y_2m \equiv 0 \bmod k$ en $x_1y_2 - x_2y_1 \equiv 0 \bmod k$:

$$x_1x_2 - y_1y_2m \equiv x_1^2 - my_1^2 \equiv 0 \bmod k \tag{4.3}$$

$$x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \bmod k \tag{4.4}$$

Waarbij 4.3 volgt uit het feit dat $x_1 \equiv x_2 \bmod k$ en $y_1 \equiv y_2 \bmod k$. Hieruit volgt dat x en y geheel zijn. Dus er bestaan oplossingen waarvoor x en y geheel zijn.

Nu rest ons nog aan te tonen dat $x \neq 1$ en $y \neq 0$. Stel nu dat $x = 1$ en $y = 0$. Dan volgt daaruit $x_1x_2 - y_1y_2m = \pm k$ en $x_1y_2 - x_2y_1 = 0 \Rightarrow x_1y_2 = x_2y_1$. We vermenigvuldigen de eerste vergelijking met x_1 en vullen dan $x_1y_2 = x_2y_1$ in:

$$\pm x_1k = x_1^2x_2 - y_1y_2x_1m = x_1^2x_2 - mx_2y_1^2 = x_2(x_1^2 - my_1^2) = x_2k$$

Daaruit volgt: $x_1 = \pm x_2$. We weten dat beide positief zijn, dus $x_1 = x_2$. Daaruit volgt $y_1 = y_2$. Maar onze aanname was dat (x_1, y_1) en (x_2, y_2) verschillende oplossingen waren voor 4.2. Dus dit is een tegenstelling, dus $x \neq 1$ en $y \neq 0$.

□

4.1 Voortbrengers van de eenhedengroep

We kunnen nu bewijzen dat de eenhedengroep $\mathbb{Z}[\sqrt{m}]^*$ uit de voortbrengers van de kleinste eenheid bestaat.

Stelling 6 $\mathbb{Z}[\sqrt{m}]^* = \{\pm\beta^q : q \in \mathbb{Z}\}$, *waarbij* $\beta > 1$ *de kleinste eenheid is.*

Bewijs
Voor het vinden van eenheden in $\mathbb{Z}[\sqrt{m}]$ moeten we de vergelijking: $x^2 - my^2 = \pm 1$ oplossen. Uit stelling 5 weten we dat de vergelijking van Pell, $x^2 - my^2 = 1$, altijd een niet-triviale oplossing heeft. Hebben we een oplossing (x, y) voor $x^2 - my^2 = -1$, dan kunnen we daarvan wel een oplossing voor de vergelijking van Pell maken, namelijk op de volgende manier:

$$N(x + y\sqrt{m}) = -1, \text{ dan volgt } N((x + y\sqrt{m})^2) = 1.$$

Hiermee vinden we dus dat de $N(\alpha) = x^2 - my^2 = \pm 1$ altijd een niet-triviale oplossing heeft.
Uit het bewijs van stelling 3 volgt dat, omdat de vergelijking van Pell een niet-triviale oplossing heeft, deze een minimum oplossing heeft. Deze 'kleinste' eenheid noemen we β. Verder volgt uit stelling 3 dat alle andere oplossingen een macht zijn van de kleinste oplossing. Daaruit volgt dus dat de verzameling $\{\beta^q : q \in Z_{>0}\} \subset \mathbb{Z}[\sqrt{m}]^*$.
Als we $m = 0$ nemen, dan verkrijgen we de triviale eenheid: $1 + 0\sqrt{m}$.
Uit stelling 1 volgt dat $\alpha \in \mathbb{Z}[\sqrt{m}]^* \Leftrightarrow N(\alpha) = \pm 1$. Waarbij de norm gegeven wordt door: $N(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2$. Dus een $a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$, als $(a + b\sqrt{m})(a - b\sqrt{m}) = \pm 1$. Hieruit volgt onmiddellijk dat als β een eenheid is, dat $-\beta$ ook een eenheid is. Het feit dat β^{-m} ook een eenheid is volgt uit het feit dat de eenheden een groep vormen. Vanwege de norm zijn ook $a - b\sqrt{m}$ en $-a + b\sqrt{m}$ eenheden. Dus volgt: $\mathbb{Z}[\sqrt{m}]^* = \{\pm\beta^q : q \in \mathbb{Z}\}$.

□

Vervolg voorbeeld 1 We hebben voor $\sqrt{5}$ de volgende kleinste eenheid gevonden: $2+\sqrt{5}$ met norm -1. Zo vinden we dus:

$$\mathbb{Z}[\sqrt{5}]^* = \{\pm(2 + \sqrt{5})^q : q \in \mathbb{Z}\}$$

Hieronder staat een tabel met de eerste tien eenheden van $\mathbb{Z}[\sqrt{5}]$. Deze zijn gevonden met behulp van Mathematica. De methode daarvoor is beschreven in Appendix A.

Eenheid	**Norm**
$2+\sqrt{5}$	-1
$9+4\sqrt{5}$	1
$38+17\sqrt{5}$	-1
$161+72\sqrt{5}$	1
$682+305\sqrt{5}$	-1
$2889+1292\sqrt{5}$	1
$12238+5473\sqrt{5}$	-1
$51841+23184\sqrt{5}$	1
$219602+98209\sqrt{5}$	-1
$930249+416020\sqrt{5}$	1

Vervolg voorbeeld 2 De kleinste eenheid in $\mathbb{Z}[\sqrt{3}]^*$ wordt gegeven door: $2+\sqrt{3}$ met norm 1. Zo zien we:

$$\mathbb{Z}[\sqrt{3}]^* = \{\pm(2+\sqrt{3})^q : q \in \mathbb{Z}\}$$

Tabel met de eerste tien eenheden van $\mathbb{Z}[\sqrt{3}]$ is de volgende:

Eenheid	**Norm**
$2+\sqrt{3}$	1
$7+4\sqrt{3}$	1
$26+15\sqrt{3}$	1
$97+56\sqrt{3}$	1
$362+209\sqrt{3}$	1
$1351+780\sqrt{3}$	1
$5042+2911\sqrt{3}$	1
$18817+10864\sqrt{3}$	1
$70226+40545\sqrt{3}$	1
$262087+151316\sqrt{3}$	1

Voorbeeld 3 Niet alle eenheden zijn zo klein als bij de ringen $\mathbb{Z}[\sqrt{5}]$ en $\mathbb{Z}[\sqrt{3}]$. In dit voorbeeld bekijken we de eerste tien eenheden van $\mathbb{Z}[\sqrt{31}]$. Met behulp van Mathematica vinden we dat daar de kleinste eenheid de volgende is: $1520+273\sqrt{31}$, met norm 1. Zo zien we dus dat de eenhedengroep $\mathbb{Z}[\sqrt{31}]^*$ wordt gegeven door:

$$\mathbb{Z}[\sqrt{31}]^* = \{\pm(1520+273\sqrt{31})^q : q \in \mathbb{Z}\}$$

Voor de eerste tien eenheden verkrijgen we dan de volgende tabel:

Eenheid	**Norm**
$1520 + 273\sqrt{31}$	1
$4620799 + 829920\sqrt{31}$	1
$14047227440 + 2522956527\sqrt{31}$	1
$42703566796801 + 7669787012160\sqrt{31}$	1
$129818829015047600 + 23316149994009873\sqrt{31}$	1
$394649197502177907199 + 70881088312003001760\sqrt{31}$	1
$1199733430587791822837360 + 215478485152339131340527\sqrt{31}$	1
$364718923433768963924766720 1 + 65505452398202264727220032 0\sqrt{31}$	1
$1108745407265314591552108545368 0 + 199136553742686369536835763227 3\sqrt{31}$	1
$337058567336763292454944605315199 99 + 605375057872314165189715992990960 0\sqrt{31}$	1

Hoofdstuk 5

De norm van $\mathbb{Z}[\sqrt[3]{m}]$

In de komende hoofdstukken gaan we eenheden proberen te vinden in $\mathbb{Z}[\sqrt[3]{m}]$, waarbij $m \in \mathbb{Z}$ geen derde macht van een geheel getal is en $m > 0$. In onderstaande hoofdstukken zullen β_1, β_2, β voortdurend worden genoemd, dit zijn eenheden van $\mathbb{Z}[\sqrt[3]{m}]$, tenzij anders vermeld. De ring $\mathbb{Z}[\sqrt[3]{m}]$ ziet er als volgt uit:

$$\mathbb{Z}[\sqrt[3]{m}] = \{a + b\sqrt[3]{m} + c\sqrt[3]{m}^2 : a, b, c \in \mathbb{Z}\} \tag{5.1}$$

We zagen in hoofdstuk 2 dat we eenheden konden vinden in $\mathbb{Z}[\sqrt{m}]$, m geen kwadraat, doormiddel van het oplossen van de normvergelijking $N(\alpha) = \pm 1$, $\alpha \in \mathbb{Z}[\sqrt{m}]$. Bij $\mathbb{Z}[\sqrt[3]{m}]$ gaat dit op dezelfde manier. Ook hier zijn eenheden te vinden door het oplossen van $N(\alpha) = \pm 1$, met $\alpha \in \mathbb{Z}[\sqrt[3]{m}]$. Het vinden van deze norm kan nog op een andere manier dan we in hoofdstuk 2 zagen. We zullen dit eerst doen voor de ring $\mathbb{Z}[\sqrt{m}]$, om het vervolgens uit te breiden naar $\mathbb{Z}[\sqrt[3]{m}]$

We starten met een basis voor $\mathbb{Z}[\sqrt{m}]$, we kiezen de basis $1, \sqrt{m}$. We vermenigvuldigen een element $a + b\sqrt{m}$ met de twee elementen van de basis. Namelijk:

$$1 \cdot (a + b\sqrt{m}) = a + b\sqrt{m} \tag{5.2}$$

$$\sqrt{m} \cdot (a + b\sqrt{m}) = bm + a\sqrt{m} \tag{5.3}$$

We kunnen dit als volgt in matrix vorm schrijven:

$$\begin{bmatrix} 1 & \sqrt{m} \end{bmatrix} \begin{bmatrix} a & bm \\ b & a \end{bmatrix} = \begin{bmatrix} a + b\sqrt{m} \\ bm + a\sqrt{m} \end{bmatrix}^T$$

De determinant van de tweede matrix geeft de norm: $\begin{vmatrix} a & bm \\ b & a \end{vmatrix} = a^2 - mb^2$.

Op dezelfde manier kunnen we een norm bepalen voor $\mathbb{Z}[\sqrt[3]{m}]$. Hier kunnen we de basis als volgt kiezen: $1, \sqrt[3]{m}, \sqrt[3]{m}^2$. Vermenigvuldigen we ook hier een element $\alpha = a + b\sqrt[3]{m} + c\sqrt[3]{m}^2 \in \mathbb{Z}[\sqrt[3]{m}]$ met de basis verkrijgen we het volgende:

$$\begin{aligned} 1 \cdot (a + b\sqrt[3]{m} + c\sqrt[3]{m}^2) &= a + b\sqrt[3]{m} + c\sqrt[3]{m}^2 \\ \sqrt[3]{m}(a + b\sqrt[3]{m} + c\sqrt[3]{m}^2) &= a\sqrt[3]{m} + b\sqrt[3]{m}^2 + cm \\ \sqrt[3]{m}^2(a + b\sqrt[3]{m} + c\sqrt[3]{m}^2) &= a\sqrt[3]{m}^2 + bm + cm\sqrt[3]{m} \end{aligned}$$

Zetten we dit opnieuw in een matrix vorm dan verkrijgen we het volgende:

$$\begin{bmatrix} 1 & \sqrt[3]{m} & \sqrt[3]{m}^2 \end{bmatrix} \begin{bmatrix} a & cm & bm \\ b & a & cm \\ c & b & a \end{bmatrix} = \begin{bmatrix} a + b\sqrt[3]{m} + c\sqrt[3]{m}^2 \\ cm + a\sqrt[3]{m} + b\sqrt[3]{m}^2 \\ bm + cm\sqrt[3]{m} + a\sqrt[3]{m}^2 \end{bmatrix}^T$$

Bereken we ook hier de determinant dan wordt de norm gegeven door:

$$N[\alpha] = \begin{vmatrix} a & cm & bm \\ b & a & cm \\ c & b & a \end{vmatrix} = a^3 + b^3m + c^3m^2 - 3abcm \tag{5.4}$$

Eenheden van $\mathbb{Z}[\sqrt[3]{m}]$, waarbij m geen derdemachtswortel en $m > 0$, voldoen aan: $a^3 + b^3m + c^3m^2 - 3abcm = \pm 1$. De kettingbreuk van $\sqrt[3]{m}$ is niet puur periodiek, daarom kunnen we zonder generalisatie van de kettingbreuken de vergelijking $a^3 + b^3m + c^3m^2 - 3abcm = \pm 1$ niet oplossen. Daarom gaan we proberen met een 'speciaal geval' van Dirichlets eenhedenstelling eenheden te vinden. Daartoe hebben we de theorie in komende hoofdstukken nodig.

Hoofdstuk 6

Inbeddingen

6.1 Inbeddingen van $\mathbb{Z}[\sqrt{m}]$ in $\mathbb{R}$

Om een beter begrip van de eenheden in $\mathbb{Z}[\sqrt[3]{m}]$ te krijgen, zullen we nogmaals de eenheden van de ring $\mathbb{Z}[\sqrt{m}]$, $m > 0$, m geen kwadraat, bekijken. We zullen een deel van de bewijzen weglaten, omdat die in de volgende subsectie zullen worden gegeven in het geval van $\mathbb{Z}[\sqrt[3]{m}]$. De bewijzen zijn in het geval van $\mathbb{Z}[\sqrt{m}]$ eenvoudiger.
We kunnen bij $\mathbb{Z}[\sqrt{m}]$ twee inbeddingen maken. Een inbedding is een injectief ringhomomorfisme van een ring $R \subset F$ naar F, $\sigma : R \to F$. We maken gebruik van de nulpunten van $X^2 - m$, namelijk $\alpha_1 = \sqrt{m},\ \alpha_2 = -\sqrt{m}$. De twee inbeddingen worden gegeven door:

$$\begin{aligned} \sigma_{1.0} : \mathbb{Z}[\sqrt{m}] &\to \mathbb{R} \qquad (6.1)\\ a + b\sqrt{m} &\mapsto a + b\alpha_1 = a + b\sqrt{m} \\ \sigma_{2.0} : \mathbb{Z}[\sqrt{m}] &\to \mathbb{R} \qquad (6.2)\\ a + b\sqrt{m} &\mapsto a + b\alpha_2 = a - b\sqrt{m} \end{aligned}$$

We zien dat $\sigma_{1.0}$ en $\sigma_{2.0}$ injectieve ringhomomorfismen zijn. We kunnen een afbeelding maken van de eenhedengroep naar een beeld $L_2 \subset \mathbb{R}^2$.

$$\begin{aligned} f_1 : \mathbb{Z}[\sqrt{m}]^* &\to L_2 \subset \mathbb{R}^2 \qquad (6.3)\\ \beta &\mapsto (\log|\sigma_{1.0}(\beta)|, \log|\sigma_{2.0}(\beta)|) \end{aligned}$$

Lemma 4 *De norm $N(\beta)$ kan worden gegeven door: $N(\beta) = \sigma_{1.0}(\beta)\sigma_{2.0}(\beta)$, waarbij $N(\beta) = a^2 - mb^2$*

Bewijs

$$N(\beta) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2$$

□

Lemma 5 *Het beeld van f_1 ligt op de lijn $x + y = 0$.*

Bewijs

$$\begin{aligned} 1 = |N(\beta)| &= \prod_{i=1}^{2} |\sigma_{i.0}(\beta)|, \text{ en dus} \\ 0 = \sum_{i=1}^{2} \log|\sigma_{i.0}(\beta)| &= \log|\sigma_{1.0}(\beta)| + \log|\sigma_{2.0}(\beta)| \\ &= x + y \end{aligned}$$

□

Lemma 6 *Een eenheid $\beta \in \mathbb{Z}[\sqrt{m}]$ voldoet aan $\prod_{i=1}^{2}(X - \sigma_{i.0}(\beta))$, met coëfficiënten in $\mathbb{Z}$.*

Bewijs

$$\begin{aligned} \prod_{i=1}^{2}(X - \sigma_{i.0}(\beta)) &= (X - \sigma_{1.0}(\beta))(X - \sigma_{2.0}(\beta)) \\ &= X^2 - (\sigma_{1.0}(\beta) + \sigma_{2.0}(\beta))X + \sigma_{1.0}(\beta)\sigma_{2.0}(\beta) \\ &= X^2 - (a + b\sqrt{m} + a - b\sqrt{m})X + a^2 - mb^2 \\ &= X^2 - 2aX + a^2 - mb^2 \\ &= X^2 - 2aX \pm 1 \end{aligned}$$

De afbeelding $\sigma_{1.0}$ is de identiteitsafbeelding en dus volgt hieruit onmiddellijk dat een eenheid β hieraan voldoet.

□

Stelling 7 *Het beeld van f_1 is van de vorm $\mathbb{Z} \cdot \gamma$, voor vaste $\gamma \in L_2$*

Bewijs
Uit stelling 6 weten we dat de eenhedengroep bestaat uit: $\mathbb{Z}[\sqrt{m}]^* = \{\pm\beta^{\pm p} : p \in \mathbb{Z}_{\geq 0}\}$. De afbeelding f_1 stuurt een eenheid β naar $(\log|\sigma_{1.0}|, \log|\sigma_{2.0}|)$. We onderscheiden nu 3 gevallen: $\beta^{\pm p}, -\beta^{\pm p}$ $(p \in \mathbb{Z}_{>0})$ en $\pm\beta^0$.

We zullen laten zien dat het beeld dan exact van de vorm $\mathbb{Z} \cdot \gamma$ is:

$$\begin{aligned} f_1(\beta^{\pm p}) &= (\log|\sigma_{1.0}(\beta^{\pm p})|, \log|\sigma_{2.0}(\beta^{\pm p})|) \\ &= (\log|\sigma_{1.0}(\beta)|^{\pm p}, \log|\sigma_{2.0}(\beta)|^{\pm p}) \\ &= (\pm p \log|\sigma_{1.0}(\beta)|, \pm p \log|\sigma_{2.0}(\beta)|) \\ &= \pm p(\log|\sigma_{1.0}(\beta)|, \log|\sigma_{2.0}(\beta)|) \end{aligned}$$

$$f_1(-\beta^{\pm p}) = -f_1(\beta^{\pm p}) = \mp p(\log|\sigma_{1.0}(\beta)|), \log|\sigma_{2.0}(\beta)|))$$

$$f_1(\pm\beta^0) = f_1(\pm 1) = (log|\pm 1|, log|\pm 1|) = (0,0) = \pm 0(\log|\sigma_{1.0}(\beta)|), \log|\sigma_{2.0}(\beta)|))$$

Hieruit volgt onmiddellijk dat het beeld van f_1 van de vorm $\mathbb{Z} \cdot \gamma$ is, voor vaste $\gamma \in L_2$, waarbij $\gamma = f_1(\beta)$, met β de kleinste eenheid groter dan één.

□

Hieruit volgt dus dat het beeld van f_1 discreet is, dus dat het aantal $f_1(\beta)$ met $\beta \in \mathbb{Z}[\sqrt{m}]^*$ in een begrensd gebied kleiner dan oneindig is. Als we nu in het geval van de ring $\mathbb{Z}[\sqrt[3]{m}]$ kunnen laten zien dat het beeld van $f:\ \mathbb{Z}[\sqrt[3]{m}]^* \to H \subset \mathbb{R}^2$ discreet is, dus dat het aantal $f(\beta)$ met $\beta \in \mathbb{Z}[\sqrt[3]{m}]^*$ in een begrensd gebied kleiner dan oneindig is, dan zijn we een stap dichter bij een oplossing hoe de eenhedengroep $\mathbb{Z}[\sqrt[3]{m}]^*$ eruit ziet. Daarvoor zullen we eerst inbeddingen van $\mathbb{Z}[\sqrt[3]{m}]$ in $\mathbb{R}$ of $\mathbb{C}$ bekijken. In stelling 12 zal worden bewezen dat het beeld van $f:\ \mathbb{Z}[\sqrt[3]{m}]^* \to H \subset \mathbb{R}^2$ discreet is.

6.2 Inbeddingen van $\mathbb{Z}[\sqrt[3]{m}]$ in $\mathbb{R}$ of $\mathbb{C}$

Om een beeld te krijgen van de eenhedengroep $\mathbb{Z}[\sqrt[3]{m}]$ maken we ook hier gebruik van inbeddingen. Voor het maken van deze inbeddingen, maken we gebruik van de nulpunten van het polynoom: $X^3 - m = 0$, deze heeft drie nulpunten in $\mathbb{C}$. We noemen ze: $\alpha_1 \in \mathbb{R}$, $\alpha_2 \in \mathbb{C}$ en $\alpha_3 = \overline{\alpha_2} \in \mathbb{C}$. De nulpunten worden gegeven door:

$$\alpha_1 = \sqrt[3]{m} \tag{6.4}$$

$$\alpha_2 = e^{\frac{2\pi i}{3}} \sqrt[3]{m} = -\frac{1}{2}\sqrt[3]{m} + \frac{1}{2}\sqrt{3}\sqrt[3]{m}i \tag{6.5}$$

$$\alpha_2 = e^{\frac{4\pi i}{3}} \sqrt[3]{m} = -\frac{1}{2}\sqrt[3]{m} - \frac{1}{2}\sqrt{3}\sqrt[3]{m}i \tag{6.6}$$

We weten dat $\mathbb{Z}[\sqrt[3]{m}] \subset \mathbb{R} \subset \mathbb{C}$. We gebruiken nu de volgende drie inbeddingen, waarbij we $\alpha = \sqrt[3]{m}$ gebruiken:

$$\sigma_1 : \mathbb{Z}[\alpha] \to \mathbb{R} \tag{6.7}$$
$$n + m\alpha + k\alpha^2 \mapsto n + m\alpha_1 + k\alpha_1^2$$
$$\sigma_2 : \mathbb{Z}[\alpha] \to \mathbb{C} \tag{6.8}$$
$$n + m\alpha + k\alpha^2 \mapsto n + m\alpha_2 + k\alpha_2^2$$
$$\sigma_3 : \mathbb{Z}[\alpha] \to \mathbb{C} \tag{6.9}$$
$$n + m\alpha + k\alpha^2 \mapsto n + m\alpha_3 + k\alpha_3^2$$

We zien dat $\sigma_3 = \overline{\sigma_2}$.

Stelling 8 *σ_1, σ_2 en σ_3 zijn inbeddingen.*

Bewijs
Een ringhomomorfisme voldoet aan de volgende drie eigenschappen:

$$1. f(1) = 1$$
$$2. f(a+b) = f(a) + f(b)$$
$$3. f(ab) = f(a) \cdot f(b)$$

σ_1 is de identiteitsafbeelding. Dit is dus zeker een ringhomomorfisme.
$\sigma_2 :\ \mathbb{Z}[\alpha] \to \mathbb{C}, n + m\alpha + k\alpha^2 \mapsto n + m\alpha_2 + k\alpha_2^2$

$$\begin{aligned}
\sigma_2(1) &= 1 \\
\sigma_2(\beta_1 + \beta_2) &= \sigma_2(a + b\alpha + c\alpha^2 + n + m\alpha + k\alpha^2) \\
&= \sigma_2(a + n + (b+m)\alpha + (c+k)\alpha^2) \\
&= a + n + (b+m)\alpha_2 + (c+k)\alpha_2^2 \\
&= a + b\alpha_2 + c\alpha_2^2 + n + m\alpha_2 + k\alpha_2^2 \\
&= \sigma_2(\beta_1) + \sigma_2(\beta_2)
\end{aligned}$$

$\sigma_2(\beta_1\beta_2) = \sigma_2(\beta_1) \cdot \sigma_2(\beta_2)$ volgt op dezelfde manier. Hieruit volgt dat σ_2 en daarmee ook σ_3 ringhomomorfismen zijn. Nu rest nog te laten zien dat σ_1, σ_2 en σ_3 injectief zijn.
Een afbeelding f is injectief $\Leftrightarrow Ker(f) = \{a : f(a) = 0\} = 0$

$$\begin{aligned}
Ker(\sigma_1) &= \{a + b\alpha + c\alpha^2 : a + b\alpha_1 + c\alpha_1^2 = 0\} \\
&= \{a + b\alpha + c\alpha^2 : a + b\sqrt[3]{m} + c\sqrt[3]{m}^2 = 0\}
\end{aligned}$$

Gegeven is dat m geen derdemachtswortel is en dat $m > 0$, daaruit volgt: $\sqrt[3]{m} \notin \mathbb{Z}$ en $a, b, c \in \mathbb{Z}$. Dus volgt dat $Ker(\sigma_1) = 0$, dus σ_1 is injectief.

$$\begin{aligned}
Ker(\sigma_2) &= \{a + b\alpha + c\alpha^2 : a + b\alpha_2 + c\alpha_2^2 = 0\} \\
&= \{a + b\alpha + c\alpha^2 : a + b(-\frac{1}{2}\sqrt[3]{m} + \frac{1}{2}\sqrt{3}\sqrt[3]{mi}) + c(-\frac{1}{2}\sqrt[3]{m} + \frac{1}{2}\sqrt{3}\sqrt[3]{mi})^2 = 0\}
\end{aligned}$$

Ook hier volgt onmiddellijk uit dat $Ker(\sigma_2) = 0$ (omdat $a, b, c \in \mathbb{Z}$) en dus is σ_2 injectief. Omdat σ_3 de toegevoegde waarde is van σ_2 volgt dat σ_3 ook injectief is.

□

We maken nu een afbeelding die met behulp van de inbeddingen σ_1, σ_2 de eenheden van $\mathbb{Z}[\sqrt[3]{m}]$ afbeeld op $\mathbb{R}^2$.

$$\begin{aligned} f : \mathbb{Z}[\sqrt[3]{m}]^* &\to H \subset \mathbb{R}^2 \\ \beta &\mapsto (\log|\sigma_1(\beta)|, \log|\sigma_2(\beta)|) \end{aligned} \tag{6.10}$$

Stelling 9 *f is een homomorfisme.*

Bewijs
Een afbeelding is een homomorfisme als aan de volgende eigenschap is voldaan:

$$f(a \cdot b) = f(a) * f(b)$$

$$\begin{aligned} f(\beta_1\beta_2) &= (\log|\sigma_1(\beta_1\beta_2)|, \log|\sigma_2(\beta_1\beta_2)|) \\ &= (\log|\sigma_1(\beta_1)\sigma_1(\beta_2)|, \log|\sigma_2(\beta_1)\sigma_2(\beta_2)|) \\ &= (\log|\sigma_1(\beta_1)||\sigma_1(\beta_2)|, \log|\sigma_2(\beta_1)||\sigma_2(\beta_2)|) \\ &= (\log|\sigma_1(\beta_1)| + \log|\sigma_1(\beta_2)|, \log|\sigma_2(\beta_1)| + \log|\sigma_2(\beta_2)|) \\ &= (\log|\sigma_1(\beta_1)|, \log|\sigma_2(\beta_1)|) + (\log|\sigma_1(\beta_2)|, \log|\sigma_2(\beta_2)|) \\ &= f(\beta_1) + f(\beta_2) \end{aligned}$$

De tweede regel volgt uit het feit dat σ_1 en σ_2 ringhomomorfismen zijn.

□

Stelling 10 *De norm kan worden gegeven door: $N(\beta) = \sigma_1(\beta)\sigma_2(\beta)\sigma_3(\beta)$, waarbij de norm wordt gegeven door: $N(\beta) = a^3 + b^3m + c^3m^2 - 3abcm$.*

Bewijs
Een $\beta \in \mathbb{Z}[\sqrt[3]{m}]$ is van de vorm: $a + b\sqrt[3]{m} + c\sqrt[3]{m}^2$.

$$\begin{aligned} \sigma_1(\beta) &= a + b\sqrt[3]{m} + c\sqrt[3]{m}^2 \\ \sigma_2(\beta) &= a + b\sqrt[3]{m}e^{\frac{2\pi i}{3}} + c\sqrt[3]{m}^2e^{\frac{4\pi i}{3}} \\ \sigma_2(\beta) &= a + b\sqrt[3]{m}e^{\frac{4\pi i}{3}} + c\sqrt[3]{m}^2e^{\frac{2\pi i}{3}} \end{aligned}$$

Hierbij is gebruikt gemaakt van: $e^{\frac{8\pi i}{3}} = e^{\frac{2\pi i}{3}}$. We zullen nu door simpelweg het uitrekenen van $\sigma_1(\beta)\sigma_2(\beta)\sigma_3(\beta)$ laten zien dat de norm hieraan voldoet.

$$\begin{aligned}
N(\beta) &= \sigma_1(\beta)\ [a^2 + ab\sqrt[3]{m}e^{\frac{4\pi i}{3}} + ca\sqrt[3]{m}^2 e^{\frac{2\pi i}{3}} + ab\sqrt[3]{m}e^{\frac{2\pi i}{3}} + b^2\sqrt[3]{m}^2 + bcme^{\frac{4\pi i}{3}} \\
&+ ac\sqrt[3]{m}^2 e^{\frac{4\pi i}{3}} + bcme^{\frac{2\pi i}{3}} + c^2 m\sqrt[3]{m}] \\
&= \sigma_1(\beta)\ [a^2 + b^2\sqrt[3]{m}^2 + c^2 m\sqrt[3]{m} + (ca\sqrt[3]{m}^2 + ab\sqrt[3]{m} + bcm)e^{\frac{2\pi i}{3}} \\
&+ (ab\sqrt[3]{m} + bcm + ac\sqrt[3]{m}^2)e^{\frac{4\pi i}{3}}]
\end{aligned}$$

We weten dat $e^{\frac{4\pi i}{3}} = \overline{e^{\frac{2\pi i}{3}}}$ en aangezien dezelfde termen staan voor $e^{\frac{4\pi i}{3}}$ en $e^{\frac{2\pi i}{3}}$ kunnen we hiervan de reële delen bij elkaar optellen, het complexe deel valt weg. Zo houden we het volgende over:

$$\begin{aligned}
N(\beta) &= \sigma_1(\beta)\ [a^2 + b^2\sqrt[3]{m}^2 + c^2 m\sqrt[3]{m} - ca\sqrt[3]{m}^2 - ab\sqrt[3]{m} - bcm] \\
&= \sigma_1(\beta)\ [a^2 - bcm + (b^2 - ca)\sqrt[3]{m}^2 + (c^2 m - ab)\sqrt[3]{m}] \\
&= a^3 + (ab^2 - ca^2)\sqrt[3]{m}^2 + (c^2 ma - a^2 b)\sqrt[3]{m} - bcma + a^2 b\sqrt[3]{m} \\
&+ (b^3 - cab)m + (c^2 mb - ab^2)\sqrt[3]{m} - b^2 cm\sqrt[3]{m} \\
&+ a^2 c\sqrt[3]{m}^2 + (b^2 c - c^2 a)m\sqrt[3]{m} + (c^3 m - abc)m - bc^2\sqrt[3]{m}^2 \\
&= a^3 - bcma + b^3 m - cabm + c^3 m^2 - abcm \\
&+ (c^2 ma - a^2 b + a^2 b - b^2 cm + b^2 cm - c^2 ma)\sqrt[3]{m} \\
&+ (ab^2 - ca^2 + c^2 mb - ab^2 + a^2 c - bc^2 m)\sqrt[3]{m}^2 \\
&= a^3 + b^3 m + c^3 m^2 - 3mabc
\end{aligned}$$

□

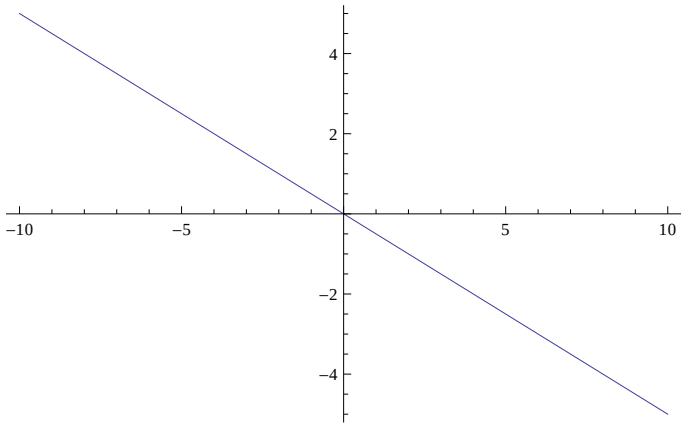
We weten dat eenheden β in $\mathbb{Z}[\sqrt[3]{m}]$ voldoen aan $N(\beta) = a^3 + b^3 m + c^3 m^2 - 3abcm = \pm 1$. Daarmee kunnen we de volgende stelling bewijzen:

Stelling 11 *Het beeld van* $f : \mathbb{Z}[\sqrt[3]{m}]^* \to \mathbb{R}^2,\ \beta \mapsto (\log|\sigma_1(\beta)|, \log|\sigma_2(\beta)|)$ *ligt op de lijn:* $H = \{(x_1, x_2) \in \mathbb{R}^2 : x_1 + 2x_2 = 0\}$, *waarbij* $x_1 = \log|\sigma_1(\beta)|,\ x_2 = \log|\sigma_2(\beta)|$.

Bewijs

$$\begin{aligned}
1 = |N(\beta)| &= \prod_{i=1}^{3} |\sigma_i(\beta)| \\
0 = \sum_{i=1}^{3} \log|\sigma_i(\beta)| &= \log|\sigma_1(\beta)| + 2\log|\sigma_2(\beta)| \\
&= x + 2y
\end{aligned}$$

Hierbij wordt gebruikt gemaakt van het feit dat $\sigma_3(\beta) = \overline{\sigma_2(\beta)}$, daaruit volgt: $|\sigma_3(\beta)| = |\sigma_2(\beta)|$.



Figuur 6.1: De lijn H

□

De meeste stellingen en bewijzen die hieronder worden genoemd en gebruikt komen uit [8]. Wij zullen ze toepassen voor de ring $\mathbb{Z}[\sqrt[3]{m}]$, waarbij het aantal reeële inbeddingen $r = 1$ is, en het aantal complexe inbeddingen $s = 1$ (waarbij de complex geconjugeerde wordt genegeerd).

Lemma 7 *De kern van f is de eindige cylische groep $\{\pm 1\}$.*

Bewijs

$$\begin{aligned}\mathrm{Ker} f &= \{\alpha \in \mathbb{Z}[\sqrt[3]{m}] : \log|\sigma_i(\alpha)| = 0 \ \forall i \leq 2\} \\ &= \{\alpha \in \mathbb{Z}[\sqrt[3]{m}] : |\sigma_i(\alpha)| = 1 \ \forall i \leq 2\} \\ &= \{\pm 1\}\end{aligned}$$

□

Lemma 8 *Een eenheid $\beta \in \mathbb{Z}[\sqrt[3]{m}]^*$ voldoet aan $\prod_{i=1}^{3}(X - \sigma_i(\beta)) = 0$, met coefficiënten in $\mathbb{Z}$.*

Bewijs We laten hier de afhankelijkheid van β in het bewijs weg, dit scheelt veel schrijfwerk.

$$\begin{aligned}\prod_{i=1}^{3}(X - \sigma_i) &= (X - \sigma_1)(X - \sigma_2)(X - \sigma_3) \\ &= (X^2 - \sigma_2 X - \sigma_1 X + \sigma_1\sigma_2)(X - \sigma_3) \\ &= X^3 - \sigma_2 X^2 - \sigma_1 X^2 + \sigma_1\sigma_2 X - \sigma_3 X^2 + \sigma_2\sigma_3 X + \sigma_1\sigma_3 X - \sigma_1\sigma_2\sigma_3 \\ &= X^3 - (\sigma_1 + \sigma_2 + \sigma_3)X^2 + (\sigma_1\sigma_3 + \sigma_2\sigma_3 + \sigma_1\sigma_2)X - \sigma_1\sigma_2\sigma_3\end{aligned}$$

We weten hierbij dat $\sigma_1\sigma_2\sigma_3 = N(\beta) = \pm 1$. Nu rest ons om te laten zien dat $(\sigma_1 + \sigma_2 + \sigma_3) \in \mathbb{Z}$ en $(\sigma_1\sigma_3 + \sigma_2\sigma_3 + \sigma_1\sigma_2) \in \mathbb{Z}$.

$$\begin{aligned}\sigma_1 + \sigma_2 + \sigma_3 &= a + b\sqrt[3]{m} + c\sqrt[3]{m} + a + b\sqrt[3]{m}e^{\frac{2\pi i}{3}} + c\sqrt[3]{m}^2e^{\frac{4\pi i}{3}} + a + b\sqrt[3]{m}e^{\frac{4\pi i}{3}} + c\sqrt[3]{m}^2e^{\frac{2\pi i}{3}} \\ &= 3a + b\sqrt[3]{m} + c\sqrt[3]{m} + (b\sqrt[3]{m} + c\sqrt[3]{m}^2)e^{\frac{2\pi i}{3}} + (b\sqrt[3]{m} + c\sqrt[3]{m}^2)e^{\frac{4\pi i}{3}} \\ &= 3a + b\sqrt[3]{m} + c\sqrt[3]{m}^2 - (b\sqrt[3]{m} + c\sqrt[3]{m}^2) = 3a \in \mathbb{Z}\end{aligned}$$

Hier wordt gebruikt gemaakt van: $\overline{e^{\frac{4\pi i}{3}}} = e^{\frac{2\pi i}{3}} = e^{\frac{8\pi i}{3}}$.

$$\begin{aligned}\sigma_2\sigma_3 &= a^2 - bcm + (b^2 - ca)\sqrt[3]{m}^2 + (c^2m - ab)\sqrt[3]{m} \\ \sigma_1\sigma_2 &= (a + b\sqrt[3]{m} + c\sqrt[3]{m}^2)(a + b\sqrt[3]{m}e^{\frac{2\pi i}{3}} + c\sqrt[3]{m}^2e^{\frac{4\pi i}{3}}) \\ &= a^2 + ab\sqrt[3]{m}e^{\frac{2\pi i}{3}} + ac\sqrt[3]{m}^2e^{\frac{4\pi i}{3}} + b^2\sqrt[3]{m}^2e^{\frac{2\pi i}{3}} + bcme^{\frac{4\pi i}{3}} + ab\sqrt[3]{m} + ac\sqrt[3]{m}^2 \\ &\quad + bcme^{\frac{2\pi i}{3}} + c^2m\sqrt[3]{m}e^{\frac{4\pi i}{3}} \\ &= a^2 + ab\sqrt[3]{m} + ac\sqrt[3]{m}^2 + (ab\sqrt[3]{m} + b^2\sqrt[3]{m} + bcm)e^{\frac{2\pi i}{3}} + (ab\sqrt[3]{m} + b^2\sqrt[3]{m} + bcm)e^{\frac{2\pi i}{3}} \\ \sigma_1\sigma_3 &= a^2 + ab\sqrt[3]{m} + ac\sqrt[3]{m} + (ab\sqrt[3]{m} + b^2\sqrt[3]{m} + bcm)e^{\frac{2\pi i}{3}} + (ab\sqrt[3]{m} + b^2\sqrt[3]{m} + bcm)e^{\frac{2\pi i}{3}}\end{aligned}$$

$$\begin{aligned}\sigma_1\sigma_3 + \sigma_2\sigma_3 + \sigma_1\sigma_2 &= \sigma_2\sigma_3 + 2a^2 - ab\sqrt[3]{m} - b^2\sqrt[3]{m}^2 - bcm - ac\sqrt[3]{m}^2 - bcm - c^2m\sqrt[3]{m} \\ &\quad + 2ab\sqrt[3]{m} + 2ac\sqrt[3]{m} \\ &= a^2 + 2a^2 - bcm - 2bcm + (b^2 + ca)\sqrt[3]{m}^2 + (c^2m + ab)\sqrt[3]{m} \\ &\quad + (-ab - c^2m)\sqrt[3]{m} + (-b^2 - ac)\sqrt[3]{m}^2 \\ &= 3a^2 - 3bcm \in \mathbb{Z}\end{aligned}$$

Zo verkrijgen we dus de polynoom waaraan $\beta \in \mathbb{Z}[\sqrt[3]{m}]^*$ voldoet:

$$X^3 - 3aX^2 + (3a^2 - 3bcm)X \mp 1 = 0 \tag{6.11}$$

De afbeelding σ_1 is de identiteitsafbeelding en dus volgt hieruit onmiddellijk dat een eenheid β hieraan voldoet.

□

Stelling 12 *Het beeld van f is discreet in $\mathbb{R}^2$. Dat wil zeggen in een begrensd gebied bevinden zich maar eindig veel $f(\beta)$ met $\beta \in \mathbb{Z}[\sqrt[3]{m}]^*$*

Bewijs

Stel we nemen een gebied waarbij de $|x - \text{coördinaat}| \leq g$ en $|y - \text{coördinaat}| \leq g$.

We moeten dus nu laten zien:

$$\#\{\alpha \in \mathbb{Z}[\sqrt[3]{m}] : f(\alpha) \in G \times G\} < \infty$$
$$\#\{\alpha \in \mathbb{Z}[\sqrt[3]{m}] : \log|\sigma_1(\alpha)| \leq G \text{ en } \log|\sigma_2(\alpha)| \leq G\} < \infty$$
$$\#\{\alpha \in \mathbb{Z}[\sqrt[3]{m}] : |\sigma_1(\alpha)| \leq e^G \text{ en } |\sigma_2(\alpha)| \leq e^G\} < \infty$$

Als we nu aan kunnen tonen dat

$$\{\text{polynomen} \prod_{i=1}^{3}(X - \sigma_i(\alpha)) : u \in \mathbb{Z}[\sqrt[3]{m}]^*, |\sigma_1(\alpha)| \leq e^G \text{ en } |\sigma_2(\alpha)| \leq e^G\}$$

een eindige verzameling polynomen is, dan is het bewijs rond.

Uit lemma 8 weten we:

$$\prod_{i=1}^{3}(X - \sigma_i(\alpha)) = X^3 - (\sigma_1 + \sigma_2 + \sigma_3)X^2 + (\sigma_1\sigma_3 + \sigma_2\sigma_3 + \sigma_1\sigma_2)X - \pm 1 \tag{6.12}$$
$$= X^3 + aX^2 + bX \pm 1 \tag{6.13}$$

Met $a, b \in \mathbb{Z}$. We zien hier:

$$|a| = |\sigma_1 + \sigma_2 + \sigma_3| \leq \sum_{i=1}^{3}|\sigma_i| \leq 3e^G < \infty$$

en

$$|b| = |\sigma_1\sigma_3 + \sigma_2\sigma_3 + \sigma_1\sigma_2| \leq |\sigma_1\sigma_3| + |\sigma_2\sigma_3| + |\sigma_1\sigma_2| \leq 3e^{2G} < \infty$$

Dus is deze verzameling polynomen eindig, dus is het beeld van f discreet.

□

De meeste bovenstaande stellingen en lemma's hebben we nodig om in hoofdstuk 7 een speciaal geval van Dirichlets Eenhedenstelling te bewijzen.

Hoofdstuk 7

Dirichlets Eenhedenstelling

Een algemene versie van Dirichlets eenhedenstelling is te vinden in [9], stelling 5.13. In deze scriptie zullen we deze stelling formuleren en bewijzen in het geval van de ring $\mathbb{Z}[\sqrt[3]{m}]$.

Stelling 13 ***Dirichlets Eenhedenstelling; speciaal geval.*** *De eenhedengroep* $\mathbb{Z}[\sqrt[3]{m}]^* \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*, waarbij* m *geen derde macht.*

Om stelling 13 te kunnen bewijzen hebben we de stelling van Minkowski nodig (In het engels ook wel: Minkowski's theorem) deze stelling is te vinden in [9].

Stelling 14 ***Stelling van Minkowski.*** *Laat* L *een volledig rooster in een* $n-$*dimensionale Euclidische ruimte* V *en* $X \subset V$ *een gesloten, begrensd, convex, symmetrische deelverzameling die voldoet aan:*

$$Vol(X) \geq 2^n \, Vol(V/L) \tag{7.1}$$

Dan bevat X *een roosterpunt ongelijk aan nul.*

Waarbij convex betekent dat voor alle $x, y \in X$ en alle $\lambda \in [0,1]$, $\lambda x + (1-\lambda)y \in X$.
Symmetrisch betekent dat voor alle $x \in X$, $-x \in X$.
We zullen nu met onderstaande stellingen proberen een bewijs te vinden voor Dirichlets eenhedenstelling. Dit is terug te vinden in [8].

Lemma 9 *De discriminant van de ring* $R = \mathbb{Z}[\sqrt[3]{m}]$*,* m *geen derde macht, wordt gegeven door:* $-27m^2$*.*

Bewijs
Neem $A = (a_{ij}) = \sigma_j(\alpha_i)$.
$\text{disc}(\mathbb{Z}[\sqrt[3]{m}]) = \det(A \cdot A^T) = \det(A) \cdot \det(A^T) = \det(A) \cdot \det(A) = \det(A)^2$.

$$
\begin{aligned}
\det(A) &= \begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt[3]{m}) & \sigma_1(\sqrt[3]{m}) \\ \sigma_2(1) & \sigma_2(\sqrt[3]{m}) & \sigma_2(\sqrt[3]{m}) \\ \sigma_3(1) & \sigma_3(\sqrt{m}) & \sigma_3(\sqrt[3]{m}) \end{vmatrix} \\
&= \begin{vmatrix} 1 & \sqrt[3]{m} & \sqrt[3]{m}^2 \\ 1 & \sqrt[3]{m}e^{\frac{2\pi i}{3}} & \sqrt[3]{m}^2 e^{\frac{4\pi i}{3}} \\ 1 & \sqrt[3]{m}e^{\frac{4\pi i}{3}} & \sqrt[3]{m}^2 e^{\frac{2\pi i}{3}} \end{vmatrix} \\
&= 1 \cdot \begin{vmatrix} \sqrt[3]{m}e^{\frac{2\pi i}{3}} & \sqrt[3]{m}^2 e^{\frac{4\pi i}{3}} \\ \sqrt[3]{m}e^{\frac{4\pi i}{3}} & \sqrt[3]{m}^2 e^{\frac{2\pi i}{3}} \end{vmatrix} - 3\sqrt{m} \begin{vmatrix} 1 & \sqrt[3]{m}^2 e^{\frac{4\pi i}{3}} \\ 1 & \sqrt[3]{m}^2 e^{\frac{2\pi i}{3}} \end{vmatrix} + 3\sqrt[3]{m} \begin{vmatrix} 1 & \sqrt[3]{m}e^{\frac{2\pi i}{3}} \\ 1 & \sqrt[3]{m}e^{\frac{4\pi i}{3}} \end{vmatrix} \\
&= me^{\frac{4\pi i}{3}} - me^{\frac{2\pi i}{3}} - me^{\frac{2\pi i}{3}} + me^{\frac{4\pi i}{3}} + me^{\frac{4\pi i}{3}} - me^{\frac{2\pi i}{3}} \\
&= 3me^{\frac{4\pi i}{3}} - 3me^{\frac{2\pi i}{3}} \\
&= 3m(-\frac{1}{2} - \frac{1}{2}\sqrt{3}i) - 3m(-\frac{1}{2} + \frac{1}{2}\sqrt{3}i) \\
&= -\frac{3}{2}m\sqrt{3}i - \frac{3}{2}m\sqrt{3}i \\
&= -3m\sqrt{3}i
\end{aligned}
$$

$\text{disc}(\mathbb{Z}[\sqrt[3]{m}]) = \det(A)^2 = 9m^2 \cdot 3 \cdot i^2 = -27m^2.$

□

Om stelling 13 te kunnen bewijzen, definiëren we het volgende:

$$A = \sqrt{|\text{disc}(\mathbb{Z}[\sqrt[3]{m}])|} \cdot \frac{2}{\pi} \in \mathbb{R}_{>0} \tag{7.2}$$

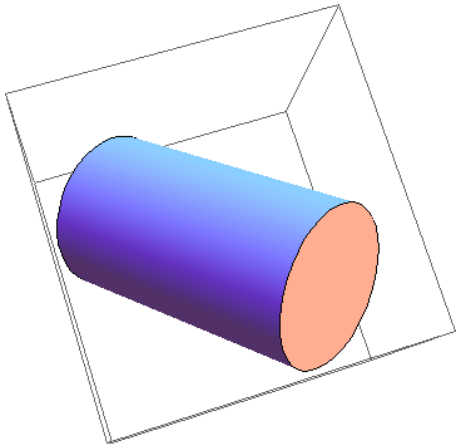
We kiezen $c_1, c_2^2 \in \mathbb{R}_{>0}$ zodat:

$$c_1 \cdot c_2^2 = A \tag{7.3}$$

Maak hierbij een S zodat:

$$S = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : |x_1| \leq c_1, |x_2^2 + x_3^2| \leq c_2^2\} \subset \mathbb{R}^3. \tag{7.4}$$

Uit deze definitie voor S kunnen we zien dat S gesloten, begrensd, convex en symmetrisch is ten opzicht van de oorsprong. Dit komt, omdat S het product is van één interval en één cirkel. Het interval en de cirkel hebben beide ook deze eigenschappen, daaruit volgt onmiddellijk dat S deze eigenschappen heeft. We zien uit deze definitie voor S dat in dit geval S een cilinder vorm heeft.



Figuur 7.1: De cilinder S.

We zien hierbij dat

$$\text{Vol } S = 2c_1 \cdot \pi c_2^2 = 2\pi A = \sqrt{|\text{disc}(R)|} \cdot \frac{2}{\pi} \cdot 2\pi = 2^2\sqrt{|\text{disc}(R)|}$$

We maken vervolgens gebruik van de afbeelding:

$$\varphi : \mathbb{Z}[\sqrt[3]{m}] \to \mathbb{R}^3 \text{ door } \varphi(x) = (\sigma_1(x), \text{Re}(\sigma_2(x)), \text{Im}(\sigma_2(x)))$$

We nemen vervolgens als rooster:

$$L = \varphi(\mathbb{Z}[\sqrt[3]{m}]) \subset \mathbb{R}^3$$

$$\text{Vol}(\mathbb{R}^3/L) = \frac{1}{2}\sqrt{|\text{disc}(R)|}$$

Nu maken we gebruik van de stelling van Minkowski, zie stelling 14. Namelijk:

$$\text{Vol } S = 2^2\sqrt{|\text{disc}(R)|} = 2^3\text{Vol}(\mathbb{R}^3/L). \tag{7.5}$$

We zien dat aan de voorwaarden van de stelling van Minkowski is voldaan. S bevat een roosterpunt ongelijk aan nul. We hebben nu een cilinder S gemaakt, die een punt bevat van het rooster. Dat wil zeggen er is een $a \in \mathbb{Z}[\sqrt[3]{m}]$, zodat $|\sigma_i| \leq c_i$ voor $i \in \{1, 2\}$. Hieruit volgt:

$$|N(a)| = |\prod_{i=1}^{3} \sigma_i(a)| = |\sigma_1(a)| \cdot |\sigma_2(a)|^2 \leq c_1 c_2^2 = A$$

Hierbij gebruiken we stelling 10.
Nu maken we een verzameling V, met $V := \{b \in \mathbb{Z}[\sqrt[3]{m}] : |N(b)| \leq A\}$.

Lemma 10 *De verzameling* $V = \{b \in \mathbb{Z}[\sqrt[3]{m}] : |N(b)| \leq A\}$ *is oneindig.*

Bewijs

We nemen een $v \in V$ met: $\varphi(v) = (\sigma_1(v), \mathrm{Re}(\sigma_2(v)), \mathrm{Im}(\sigma_2(v))) \in \mathbb{R}^3$. Vervolgens kunnen we een cilinder $S_1 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : |x_1| \leq c_1, |x_2^2 + x_3^2| \leq c_2^2\} \subset \mathbb{R}^3$ maken met hoogte $< |\sigma_1(v)|$ we kunnen dan c_2 zodanig kiezen dat nog steeds geldt: $c_1 c_2^2 = A$. Deze cilinder S_1 kunnen we zodanig maken dat hij een groot genoeg volume heeft, zodat hij aan de stelling van Minkowski voldoet. S_1 bevat een roosterpunt ongelijk aan nul. Dit roosterpunt kan niet gelijk zijn aan v omdat we de hoogte van de cilinder beperkt hebben, zodat $v \notin S_1$. We vinden dus een $v_1 \neq v$.

$$N(v_1) = |\prod_{i=1}^{3} \sigma_i(v_1)| = |\sigma_1(v_1)| \cdot |\sigma_2(v_1)|^2 \leq c_1 c_2^2 = A.$$

Dus volgt $v_1 \in V$. Zo kunnen we de hoogte en straal van de cilinder telkens variëren waardoor we oneindig veel punten vinden die in V zitten.

□

Vervolgens nemen we de verzameling: $W := \{\text{de hoofdidealen } (b) \subset \mathbb{Z}[\sqrt[3]{m}] : |N(b)| \leq A\}$.

Lemma 11 *De verzameling* $W = \{$*de hoofdidealen* $(b) \subset \mathbb{Z}[\sqrt[3]{m}] : |N(b)| \leq A\}$ *is eindig.*

Bewijs

We kunnen dit ook als volgt bekijken: We nemen $\mathbb{Z}[\sqrt[3]{m}]$ als optelgroep. Dat wil zeggen dat $\mathbb{Z}[\sqrt[3]{m}] -$ optelgroep $\cong \mathbb{Z}^3$. We nemen nu de lineaire afbeelding vermenigvuldigen met b. Als we van deze afbeelding de determinant nemen, dan verkrijgen we de norm van b. Dus

$$\mathbb{Z}[\sqrt[3]{m}] - \text{optelgroep} \xrightarrow{\text{“vermenigvuldigen met } b\text{”}} b\mathbb{Z}[\sqrt[3]{m}]$$

We zagen dat $\mathbb{Z}[\sqrt[3]{m}] -$ optelgroep $\cong \mathbb{Z}^3$, en dus:

$$\mathbb{Z}^3 \xrightarrow{\text{“vermenigvuldigen met } b\text{”}} (\text{beeld van } \mathbb{Z}^3) \subset \mathbb{Z}^3$$

Uit de analyse weten we dat

$$\det(\text{“vermenigvuldigen met } b\text{”}) = \pm \frac{vol(b(x))}{vol(x)} = N(b)$$

Daaruit volgt:

$$\#\mathbb{Z}[\sqrt[3]{m}]/b\mathbb{Z}[\sqrt[3]{m}] = \#\mathbb{Z}^3/\text{beeld van } \mathbb{Z}^3 = |\det(\text{“vermenigvuldigen met } b\text{”})| = |N(b)|$$

De verzameling W is dan gelijk aan het volgende: $W = \{\text{de hoofdidealen } (b) \subset \mathbb{Z}[\sqrt[3]{m}] : \#\mathbb{Z}[\sqrt[3]{m}]/(b) \leq A\}$. Deze verzameling ligt bevat in:

$$W_1 = \{\text{de idealen } I \subset \mathbb{Z}[\sqrt[3]{m}] : \#\mathbb{Z}[\sqrt[3]{m}]/I \leq A\}$$

Als we nu aan kunnen tonen dat W_1 eindig is, dan volgt daaruit dat W ook eindig is. Stel $\#\mathbb{Z}[\sqrt[3]{m}]/I \leq A$. Daaruit volgt dat $\#\mathbb{Z}[\sqrt[3]{m}]/I \in \{1, 2, 3, \ldots \lfloor A \rfloor\}$. Waarbij $\lfloor A \rfloor$ de floor functie is. We definiëren nu: $n := \lfloor A \rfloor!$ dan: $\#\mathbb{Z}[\sqrt[3]{m}]/I \mid n$. De ring $\mathbb{Z}[\sqrt[3]{m}]/I$ is een optelgroep (zie [2]). $\#\mathbb{Z}[\sqrt[3]{m}]/I$ is het aantal elementen van die groep. Dus $\forall r + I \in \mathbb{Z}[\sqrt[3]{m}]/I$ geldt: $(\#\mathbb{Z}[\sqrt[3]{m}]/I) \cdot (r + I) = 0 + I$. Dus geldt zeker $nr + I = n \cdot (r + I) = 0 + I$. Daaruit volgt onmiddellijk: $nr - 0 = nr \in I \ \forall r \in \mathbb{Z}[\sqrt[3]{m}]$. Dus $n\mathbb{Z}[\sqrt[3]{m}] \subset I$.

Als het aantal idealen I, die de eigenschap $n\mathbb{Z}[\sqrt[3]{m}] \subset I$ hebben, eindig is, dan is het bewijs rond. We kijken nu naar de ring $\mathbb{Z}[\sqrt[3]{m}]/n\mathbb{Z}[\sqrt[3]{m}]$. We willen weten wat de idealen in $\mathbb{Z}[\sqrt[3]{m}]/n\mathbb{Z}[\sqrt[3]{m}]$ zijn. Daartoe weten we dat er een bijectie (een bijectieve afbeelding) is tussen de idealen

$$\{\overline{I} \subset \mathbb{Z}[\sqrt[3]{m}]/n\mathbb{Z}[\sqrt[3]{m}]\} \leftrightarrow \{I \subset \mathbb{Z}[\sqrt[3]{m}] \text{ zodat } n\mathbb{Z}[\sqrt[3]{m}] \subset I\}$$

We zien hier dat we $\mathbb{Z}[\sqrt[3]{m}]/n\mathbb{Z}[\sqrt[3]{m}]$ als optelgroep kunnen zien als $\mathbb{Z}^3/n\mathbb{Z}^3 \cong (\mathbb{Z}/n\mathbb{Z})^3$. Waarbij we weten dat $(\mathbb{Z}/n\mathbb{Z})^3$ eindig veel ondergroepen (zelfs: deelverzamelingen) heeft. Daaruit volgt dat er eindig veel hoofdidealen van $\mathbb{Z}[\sqrt[3]{m}]$ zijn met norm hooguit A.

□

Omdat de verzameling V oneindig is en de verzameling W eindig, zijn er $b_1, b_2, b_3, b_4, \ldots$ met $(b_1) = (b_2) = (b_3) = (b_4) = \ldots$. Dat wil zeggen dat ze een eenheid verschillen, dus vinden we: $\frac{b_2}{b_1}, \frac{b_3}{b_1}, \frac{b_4}{b_1}, \ldots \in \mathbb{Z}[\sqrt[3]{m}]$. Zo vinden we altijd een niet-triviale eenheid van $\mathbb{Z}[\sqrt[3]{m}]$.
Het beeld van f is discreet en we vinden dus altijd een niet-triviale eenheid. Er kan dus een eenheid u gekozen worden waarvoor $f(u) \neq (0, 0)$ is en bovendien $||f(u)||$ minimaal is. Net als bij het hoofdstuk over de vergelijking van Pell volgt dan voor elke eenheid v, dat $f(v) = nf(u)$ voor een $n \in \mathbb{Z}$. En dus $f(v) = f(u^n)$, waaruit volgt dat $v = \pm u^n$. Daarmee is het speciale geval van de eenhedenstelling van Dirichlet bewezen. Dus $\mathbb{Z}[\sqrt[3]{m}]^*$ is isomorf met $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

We zien dat de eenhedengroep ook bij de ring $\mathbb{Z}[\sqrt[3]{m}]$ op vermenigvuldigen met ± 1 na, wordt voortgebracht door één element. De eenhedengroep ziet er als volgt uit:

$$\mathbb{Z}[\sqrt[3]{m}]^* = \{\pm(a + b\sqrt[3]{m} + c\sqrt[3]{m}^2)^q : q \in \mathbb{Z}\}$$

Nu is het nog interessant om te weten wanneer een eenheid groter dan 1 van $\mathbb{Z}[\sqrt[3]{m}]$ daadwerkelijk de voortbrenger is van de eenhedengroep. Daarvoor hebben we eerste de volgende stelling nodig:

Stelling 15 ***Artin.*** *Neem de ring $\mathbb{Z}[\sqrt[3]{m}]$, en neem $u \in \mathbb{Z}[\sqrt[3]{m}]^*$ de voortbrenger > 1 van de eenhedengroep, dan $|disc(\mathbb{Z}[\sqrt[3]{m}])| < 4u^3 + 24$.*

Dit bewijs laten we achterwege, het is te vinden in [11]. Met stelling 15 kunnen we de volgende stelling bewijzen, die heel nuttig is om te kijken of een eenheid groter dan 1 ook daadwerkelijk een voortbrenger van de eenhedengroep is:

Stelling 16 *We nemen een $u \in \mathbb{Z}[\sqrt[3]{m}]^*$ met $u > 1$. Dan is u een voortbrenger van de eenhedengroep als: $4u^{\frac{3}{2}} + 24 < |disc(\mathbb{Z}[\sqrt[3]{m}])|$.*

Bewijs
We weten door het speciale geval van Dirichlets eenhedenstelling dat de eenhedengroep $\mathbb{Z}[\sqrt[3]{m}]^*$ één voortbrenger groter dan 1 heeft, noem deze voortbrenger ϵ. Dus $u = \epsilon^n$ voor een positief geheel getal n. Als we nu laten zien dat $n = 1$ dan is de stelling bewezen. Als zou gelden dat $n > 1$, dan was

$$|\text{disc}(\mathbb{Z}[\sqrt[3]{m}])| \leq 4\epsilon^3 + 24 = 4u^{3/n} + 24 \leq 4u^{3/2} + 24.$$

Dit is een tegenspraak.

□

Hoofdstuk 8

Eenhedengroep $\mathbb{Z}[\sqrt[3]{m}]^*$

In dit hoofdstuk zullen we voor een aantal m de eenheden proberen te vinden van de ring $\mathbb{Z}[\sqrt[3]{m}]$. Het script waarmee deze eenheden zijn gevonden staat beschreven in bijlage B.

8.1 De eenhedengroep $\mathbb{Z}[\sqrt[3]{5}]^*$

We zullen beginnen met het geval $m = 5$. We praten dus over de ring $\mathbb{Z}[\sqrt[3]{5}] := \{a+b\sqrt[3]{5}+c\sqrt[3]{5}^2 : a, b, c \in \mathbb{Z}\}$. De discriminant van de ring $\mathbb{Z}[\sqrt[3]{5}]$ wordt gegeven door: $disc(\mathbb{Z}[\sqrt[3]{5}]) = -27 \cdot 5^2 = -675$ (zie stelling 9). Vervolgens kunnen we A bepalen (zie vergelijking 7.2). Deze wordt gegeven door:

$$A = \sqrt{|\text{disc}(\mathbb{Z}[\sqrt[3]{5}])|} \cdot \frac{2}{\pi} = \sqrt{675} \cdot \frac{2}{\pi}$$

Vervolgens gaan we proberen een c_1, c_2 zodanig te kiezen, dat $c_1 \cdot c_2^2 = A$. We beginnen met $c_2 = \frac{4}{5}$ en met $c_1 = \frac{A}{c_2^2}$. Daarna gaan we voor i, j, k, elk lopent van -5 tot 5, elementen $a = i+j\sqrt[3]{5}+k\sqrt[3]{5}^2 \in \mathbb{Z}[\sqrt[3]{5}]$ zoeken die voldoen aan $|\sigma_1(a)| < c_1$ en $|\sigma_2(a)| < c_2$.

Voor $c_2 = \frac{4}{5}$ en $c_1 = \frac{A}{c_2^2}$ vinden we de volgende i, j, k die voldoen aan deze eis.

$$\begin{aligned} -5, -3, -2 \\ -3, -2, -1 \\ 0, 0, 0 \\ 3, 2, 1 \\ 5, 3, 2 \end{aligned}$$

Vervolgens bereken we de norm van de onderste twee elementen:

$$N(3 + 2\sqrt[3]{5} + \sqrt[3]{5}^2) = 2$$
$$N(5 + 3\sqrt[3]{5} + 2\sqrt[3]{5}^2) = 10$$

We zien dat deze beide elementen niet een norm ± 1 hebben en dus geen eenheid zijn. We proberen nu of we voor andere waarden van c_1 en c_2 wel een eenheid van $\mathbb{Z}[\sqrt[3]{5}]$ kunnen vinden. We nemen nu $c_1 = 9$ en $c_2 = \frac{A}{c_1}$. Vervolgens herhalen we het proces weer, maar nu met deze nieuwe waarden voor c_1 en c_2. Dan verkrijgen we de volgende elementen:

$$-3, -1, -1$$
$$-2, -2, -1$$
$$-2, -1, -1$$
$$-1, 0, 0$$
$$0, 0, 0$$
$$1, 0, 0$$
$$2, 1, 1$$
$$2, 2, 1$$
$$3, 1, 1$$

Weer gaan we de norm berekenen, om te kijken of er nu een eenheid tussen zit.

$$N(2 + 1\sqrt[3]{5} + 1\sqrt[3]{5}^2) = 8$$

We zien dat de eenheden $a = 2 + 1\sqrt[3]{5} + 1\sqrt[3]{5}^2$ en $b = (3 + 2\sqrt[3]{5} + \sqrt[3]{5}^2)^3$ dezelfde norm hebben en dus hetzelfde hoofdideaal voortbrengen. Als we deze elementen op elkaar delen dan krijgen we wel een eenheid.
Zo verkrijgen we de volgende eenheden:

$$\alpha_1 = \frac{b}{a} = 1 - 4\sqrt[3]{5} + 2\sqrt[3]{5}^2 \tag{8.1}$$
$$\alpha_2 = \frac{a}{b} = 41 + 24\sqrt[3]{5} + 14\sqrt[3]{5}^2 \tag{8.2}$$

Waarbij $N(\alpha_1) = 1$ en $N(\alpha_2) = 1$. Bovendien weten we dat de eenhedengroep $\mathbb{Z}[\sqrt[3]{m}]$ wordt voortgebracht door één element, en hier zien we:

$$\alpha_2 = (\alpha_1)^{-1}$$

Om een beter beeld te krijgen van de eenhedengroep $\mathbb{Z}[\sqrt[3]{5}]^*$ kunnen we de machten nemen van deze twee eenheden, om zo meer eenheden te vinden. Dit is weergegeven in de volgende tabellen.

Voor α_1 is dit de volgende tabel:

Eenheid	**Norm**
$1 - 4\ 5^{1/3} + 2\ 5^{2/3}$	1
$-79 + 12\ 5^{1/3} + 20\ 5^{2/3}$	1
$-359 + 528\ 5^{1/3} - 186\ 5^{2/3}$	1
$8641 + 104\ 5^{1/3} - 3016\ 5^{2/3}$	1
$70001 - 64620\ 5^{1/3} + 13850\ 5^{2/3}$	1
$-853199 - 206124\ 5^{1/3} + 412332\ 5^{2/3}$	1
$-11161079 + 7329992\ 5^{1/3} - 469570\ 5^{2/3}$	1
$71530241 + 47278608\ 5^{1/3} - 52111696\ 5^{2/3}$	1
$1586550241 - 759959316\ 5^{1/3} - 98165646\ 5^{2/3}$	1
$-4049729999 - 8087816740\ 5^{1/3} + 6114772100\ 5^{2/3}$	1

En voor α_2:

Eenheid	**Norm**
$41 + 24\ 5^{1/3} + 14\ 5^{2/3}$	1
$5041 + 2948\ 5^{1/3} + 1724\ 5^{2/3}$	1
$619921 + 362532\ 5^{1/3} + 212010\ 5^{2/3}$	1
$76235201 + 44582616\ 5^{1/3} + 26072072\ 5^{2/3}$	1
$9375075001 + 5482577120\ 5^{1/3} + 3206230550\ 5^{2/3}$	1
$1152906139441 + 674223600444\ 5^{1/3} + 394288353444\ 5^{2/3}$	1
$141779406161441 + 82913099705868\ 5^{1/3} + 48487874854034\ 5^{2/3}$	1
$17435417614513921 + 10196294075597552\ 5^{1/3} + 5962828948216400\ 5^{2/3}$	1
$2144132181272867401 + 1253896106222981736\ 5^{1/3} + 733282891294408542\ 5^{2/3}$	1
$263676093823125310001 + 154198715096299666740\ 5^{1/3} + 90175955630242455500\ 5^{2/3}$	1

In paragraaf 6.2 hebben we de volgende afbeelding gedefinieerd:

$$\begin{aligned} f : \mathbb{Z}[\sqrt[3]{m}]^* &\to H \subset \mathbb{R}^2 \\ \beta &\mapsto (\log|\sigma_1(\beta)|, \log|\sigma_2(\beta)|) \end{aligned} \tag{8.3}$$

Waarbij het beeld wordt afgebeeld op de lijn: $H = \{(x_1, x_2) \in \mathbb{R}^2 : x_1 + 2x_2 = 0\}$, waarbij $x = \log|\sigma_1(\beta)|,\ y = \log|\sigma_2(\beta)|$ (zie stelling 11). We zien hier dat dat precies gebeurt, namelijk:

$$\log|\sigma_1(\alpha_1)| + 2 \cdot \log|\sigma_2(\alpha_1)| = 0$$

Bovendien zien we dat

$$f(\alpha_1) = \frac{1}{2} \cdot f(\alpha_1^2) = -1 \cdot f(\alpha_2)$$

We gaan nu met behulp van stelling 15 de voortbrenger $u > 1$ van $\mathbb{Z}[\sqrt[3]{5}]^*$ bepalen. Er geldt dat $\sigma_1(\alpha_2) = 122.9756711\ldots$, dus dit is een eenheid > 1.

Noemen we de voortbrenger > 1 weer u, dan geldt dus $\alpha_2 = u^n$ voor een $n \geq 1$, dus ook $u = \alpha_2^{1/n}$ en $u > \sqrt[3]{\frac{675-24}{4}} = 5.459761425\ldots$ (zie stelling 15). Dus volgt

$$122.9756711\ldots > (5.459761425\ldots)^n,$$

en daarom is $n \leq 2$. Zou $n = 2$ gelden, dan zou α_2 een kwadraat zijn in $\mathbb{Z}[\sqrt[3]{5}]$. Met het Maple-commando

```
alias(beta=RootOf(x^3-5)):
factor(x^2-(41+24*beta+14*beta^2),beta);
```

zie je dat dit niet het geval is. Dus geldt $n = 1$ en $u = \alpha_2$.
Dus de structuur van de eenhedengroep $\mathbb{Z}[\sqrt[3]{5}]^*$ is als volgt:

$$\mathbb{Z}[\sqrt[3]{5}]^* = \{\pm(41 + 24\sqrt[3]{5} + 14\sqrt[3]{5}^2)^q : q \in \mathbb{Z}\}.$$

Op dezelfde manier hebben we geprobeerd in $\mathbb{Z}[\sqrt[3]{23}]^*$ niet-triviale elementen te vinden. In dit geval is bekend, dat de kleinste eenheid > 1 vrij grote coefficienten heeft (zie [12]). Hoewel theoretisch gezien, de methode zeker zo'n eenheid zou moeten vinden, is dat in de praktijk niet gelukt.

Hoofdstuk 9

Eenhedengroep van $\mathbb{Z}[\sqrt{m}]$ en Dirichlets eenhedenstelling.

We hebben in paragraaf 4.1 de eenheden bekeken van de ringen: $\mathbb{Z}[\sqrt{5}], \mathbb{Z}[\sqrt{3}]$ en $\mathbb{Z}[\sqrt{31}]$. We hebben in deze drie gevallen de voortbrenger van de eenhedengroep gevonden met behulp van kettingbreuken.
We hebben in hoofdstuk 7 een methode gevonden om eenheden te vinden met behulp van Dirichlets eenhedenstelling. Dit zullen we nu ook doen voor de bovenstaande ringen. Het mathematica script dat hiervoor gebruikt is, is op hetzelfde gebaseerd als de code voor het vinden van eenheden in $\mathbb{Z}[\sqrt[3]{m}]$. Voor het vinden van eenheden in de ring $\mathbb{Z}[\sqrt{m}]$ hebben we eerst de discriminant van de ring $\mathbb{Z}[\sqrt{m}]$ nodig:

Stelling 17 *De discriminant van de ring $\mathbb{Z}[\sqrt{m}]$ wordt gegeven door: $4m$.*

Bewijs
Neem $A = (a_{ij}) = \sigma_j(\alpha_i)$.
$\text{disc}(\mathbb{Z}[\sqrt{m}]) = \det(A \cdot A^T) = \det(A) \cdot \det(A^T) = \det(A) \cdot \det(A) = \det(A)^2$.

$$\begin{aligned}\det(A) &= \begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt{m}) \\ \sigma_2(1) & \sigma_2(\sqrt{m}) \end{vmatrix} \\ &= \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix} \\ &= -2\sqrt{m}\end{aligned}$$

$\text{disc}(\mathbb{Z}[\sqrt{m}]) = (-2\sqrt{m})^2 = 4m$

□

De methode van hoofdstuk 7 wordt in het geval van de ring $\mathbb{Z}[\sqrt{m}]$ als volgt:

$$A = \sqrt{|\text{disc}(\mathbb{Z}[\sqrt{m}])|} = 2\sqrt{m}$$

Vervolgens kiezen we c_1, c_2 zodanig dat:

$$c_1 \cdot c_2 = A$$

De verzameling S_1 definiëren we als volgt:

$$S_1 = \{(x_1, x_2) \in \mathbb{R}^2 : |x_1| \leq c_1, |x_2| \leq c_2\} \subset \mathbb{R}^2. \tag{9.1}$$

We zien dat S_1 begrensd, gesloten, convex en symmetrische is. Hij voldoet ook weer aan de stelling van Minkowski. Hij bevat dus een roosterpunt $a \in \mathbb{Z}[\sqrt{m}]$ met de eigenschap: $|\sigma_1(a)| \leq c_1, |\sigma_2(a)| \leq c_2$. Dit is alle theorie die we nodig hebben om eenheden te kunnen vinden in de ring $\mathbb{Z}[\sqrt{m}]$.
Voor deze ringen kunnen we ook resultaten uit hoofdstuk 4 gebruiken. Daar zagen we, dat

$$\{\alpha \in \mathbb{Z}[\sqrt{m}] \ : \ |N(\alpha)| < 1 + 2\sqrt{m}\}$$

een oneindige verzameling is. Net als in hoofdstuk 7 zie je dat deze elementen slechts eindig veel hoofdidealen in $\mathbb{Z}[\sqrt{m}]$ voortbrengen. Dat levert opnieuw een bewijs voor het bestaan van niet-triviale eenheden in $\mathbb{Z}[\sqrt{m}]$.

We beginnen met de ring $\mathbb{Z}[\sqrt{5}]$.

A wordt gegeven door: $A = 2\sqrt{5}$.
Neem: $c_1 = 2$, $c_2 = \sqrt{5}$. We vinden dan de volgende elementen: $(-1, 0)$, $(0, 0)$, $(1, 0)$, de eerste en derde daarvan zijn triviale eenheden, dus deze c_1, c_2 voldoen niet.
Neem: $c_1 = 1$, $c_2 = 2\sqrt{5}$. We vinden de volgende elementen: $(-2, 1)$, $(0, 0)$, $(2, -1)$. We berekenen de norm van het laatste element: $N(2 - \sqrt{5}) = 2^2 - 5(-1)^2 = -1$. We zien dat we dus een eenheid hebben gevonden, namelijk: $2 - \sqrt{5} \in \mathbb{Z}[\sqrt{5}]^*$.

Met de kettingbreuken vonden we de eenheid: $2 + \sqrt{5} = -\left(\frac{1}{2-\sqrt{5}}\right)$. We zien dat deze methode niet zo effectief is als de methode met de kettingbreuken. Met de kettingbreuken kun je een eenheid berekenen, met deze methode blijft het toch zoeken; je moet soms een paar keer een c_1, c_2 opnieuw kiezen, voordat je een eenheid vind.

In de ring $\mathbb{Z}[\sqrt{3}]$ was de methode nog wat langzamer door foutieve keuze van c_1, c_2:

- $c_1 = 1,\ c_2 = 2\sqrt{3} : (0,0)$
- $c_1 = 2,\ c_2 = \sqrt{3} : (-1,0),\ (0,0),\ (1,0)$
- $c_1 = 4,\ c_2 = \frac{1}{2}\sqrt{3} : (0,0)$
- $c_1 = \frac{1}{2},\ c_2 = 4\sqrt{3} : (-2,1),\ (0,0),\ (2,-1)$

Vervolgens bereken we de norm van het laatste element: $N(2-\sqrt{3}) = 2^2 - 3(-1)^2 = 1$. We zien dat we hier de eenheid: $2-\sqrt{3}$ hebben gevonden. Dit is de inverse van de eenheid die we met kettingbreuken vonden: $2+\sqrt{3} = \frac{1}{2-\sqrt{3}}$.

Als laatste voorbeeld nemen we $\mathbb{Z}[\sqrt{31}]$. Hier geldt:

$$N(11-2\sqrt{31}) = -3 \text{ en } N(28+5\sqrt{31}) = 9.$$

In dit geval blijkt

$$\frac{(11-2\sqrt{31})^2}{28+5\sqrt{31}} = 1520 - 273\sqrt{31}$$

een voortbrenger van de eenhedengroep te zijn. Het is een eenheid met norm 1. Dus de structuur van de eenhedengroep $\mathbb{Z}[\sqrt{31}]$ is als volgt:

$$\mathbb{Z}[\sqrt{31}]^* = \{\pm(1520 - 273\sqrt{31})^q : q \in \mathbb{Z}\}.$$

Hoofdstuk 10

Conclusie

In deze scriptie hebben we eerst de theorie voor $\mathbb{Z}[\sqrt{m}]$ bekeken, om daar eenheden in te kunnen vinden. We kunnen daarvoor de norm goed gebruiken. Namelijk voor een eenheid $\alpha = x + y\sqrt{m} \in \mathbb{Z}[\sqrt{m}]^*$ geldt: $N(\alpha) = x^2 - my^2 = \pm 1$. Om een oplossing (x, y) voor deze vergelijking te vinden kunnen we gebruik maken van de vergelijking van Pell: $x^2 - my^2 = 1$. Om deze vergelijking op te lossen hebben we gebruik gemaakt van kettingbreuken. Met behulp van kettingbreuken kunnen we een benadering van $\sqrt{m}$ geven en zo de oplossing (x, y) voor de vergelijking van Pell vinden. Met deze oplossing kunnen we de structuur van de eenhedengroep $\mathbb{Z}[\sqrt{m}]^*$ bepalen, namelijk:

$$\mathbb{Z}[\sqrt{m}]^* = \{\pm\beta^q : q \in \mathbb{Z}\}$$

Voor het vinden van eenheden in $\mathbb{Z}[\sqrt[3]{m}]$ kunnen we ook gebruik maken van de norm. Deze norm wordt gegeven door: $N(\alpha) = a^3 + b^3m + c^3m^2 - 3abcm$. Ook hier geldt voor een eenheid $\beta \in \mathbb{Z}[\sqrt[3]{m}]^*$ dat $N(\beta) = \pm 1$. Helaas konden we hier geen gebruik maken van kettingbreuken om deze vergelijking op te lossen. We hebben hier gebruik gemaakt van een reële inbedding van de ring $\mathbb{Z}[\sqrt[3]{m}]$ en twee complexe inbeddingen van de ring $\mathbb{Z}[\sqrt[3]{m}]$. Om de inbeddingen beter te begrijpen hebben we ze ook bekeken in het geval van de ring $\mathbb{Z}[\sqrt{m}]$.
Voor het vinden van eenheden in $\mathbb{Z}[\sqrt[3]{m}]$ hebben we gebruik gemaakt van de afbeelding:

$$\begin{aligned} f : \mathbb{Z}[\sqrt[3]{m}]^* &\to H \subset \mathbb{R}^2 \\ \beta &\mapsto (\log|\sigma_1(\beta)|, \log|\sigma_2(\beta)|) \end{aligned}$$

Het beeld van f wordt weergegeven door: $H = \{(x_1, x_2) \in \mathbb{R}^2 : x_1 + 2x_2 = 0\}$. Met behulp van het bewijs Dirichlets eenhedenstelling in het geval van één reële inbedding en één complexe inbedding waren we in staat eenheden in $\mathbb{Z}[\sqrt[3]{m}]$ te vinden en ook de structuur van de groep te bepalen. Deze bleek van dezelfde structuur te zijn als de eenhedengroep $\mathbb{Z}[\sqrt{m}]^*$, namelijk:

$$\mathbb{Z}[\sqrt[3]{m}]^* = \{\pm(a + b\sqrt[3]{m} + c\sqrt[3]{m}^2)^q : q \in \mathbb{Z}\}$$

Hoofdstuk 11

Dankwoord

Allereerst wil ik graag Prof. dr. J. Top bedanken voor het bedenken van het onderwerp voor deze scriptie en voor het helpen met alle problemen waar ik tegen aan ben gelopen tijdens het maken van deze scriptie. Zonder hem was deze scriptie nooit zo tot stand gekomen.

Graag wil ik ook mijn vrienden en familie bedanken voor alle support die ze mij deze periode hebben gegeven. Vooral Rianne Veenstra voor het dag in dag uit samen werken aan onze scripties. Ook Paul Vermeulen en Herre Kamsma verdienen het om genoemd te worden. Zij waren er altijd wanneer ik het even niet meer zag zitten of hulp nodig had. Natuurlijk mijn ouders en mijn zusje niet te vergeten voor het controleren van mijn scriptie.
Als laatste wil ik graag Prof. dr. H. Waalkens bedanken voor het zijn van mijn tweede begeleider.

Bibliografie

[1] http://mathworld.wolfram.com/DirichletsBoxPrinciple.html.

[2] Dictaat Algebraïsche structuren.

[3] Dictaat groepentheorie.

[4] H. Davenport. *The Higher Arithmetic an introduction to the theory of numbers.* Cambridge University Press, eighth edition, 2008.

[5] Daniel A. Marcus. *Number Fields.* Springer-Verlag, 1977.

[6] Ionica Smeets. *On continued fraction algorithms.* PhD thesis, Universiteit Leiden, 2010. www.math.leidenuniv.nl/scripties/SmeetsThesis.pdf.

[7] Craig Smoryński. *Logical Number Theory 1 An introduction.* Springer-Verlag, 1991.

[8] William Stein. A brief introduction to classical and adelic algebraic number theory. *Course Notes for Math*, Volume 21(May), 2004.

[9] P. Stevenhagen. Number rings.

[10] H.P.F. Swinnerton-Dyer. *A Brief Guide to Algebraic Number Theory.* Cambridge University Press, 2001.

[11] A. Fröhlich & M. J. Taylor. *Algebraic number theory.* Cambridge University Press, 1991.

[12] Hideo Wada. A table of fundamental units of purely cubic fields. *Proceedings of the Japan Academy*, Volume 46(10), 1970.

Bijlage A

Met behulp van Mathematica eenheden bepalen van $\mathbb{Z}[\sqrt{m}]$

In de onderstaande code worden de eerste 10 eenheden van een eenhedengroep $\mathbb{Z}[\sqrt{m}]^*$ berekend. Dit gebeurt op de volgende manier:
In ln[1] wordt de wortel vastgesteld (in dit geval: $m = 5$). In ln[2] wordt de kettingbreuk van $\sqrt{m}$ berekend. In ln[3] en ln[4] wordt deze afgebroken tot het getal $2q_0 = q_n$. Vervolgens wordt in ln[5] de breuk berekend die voor deze kettingbreuk het beste $\sqrt{m}$ benadert. In ln[6] wordt de kleinste eenheid berekend, namelijk $A_n + \sqrt{m}B_n$, waarbij A_n en B_n de teller en noemer van ln[5] zijn. Vervolgens worden in ln[7] de machten 1 t/m 10 berekend van de kleinste eenheid en wordt gecheckt of deze wel een norm van ± 1 hebben. Dat resulteert in de onderste matrix.

```
In[1]:= m=5;
In[2]:= a=ContinuedFraction[Sqrt[m]];
In[3]:= b=Flatten[a];
In[4]:= c=Drop[b,-1];
In[5]:= d=FromContinuedFraction[c];
In[6]:= basis=Numerator[d]+Sqrt[m]*Denominator[d]
Out[6]= 2+Sqrt[5]
In[7]:= Transpose[List[Table[Expand[basis^i],{i,1,10}],
Table[AlgebraicNumberNorm[basis^j],{j,1,10}]]]//MatrixForm
Out[7]//MatrixForm=
(2+Sqrt[5]                -1
9+4 Sqrt[5]                1
38+17 Sqrt[5]             -1
161+72 Sqrt[5]             1
682+305 Sqrt[5]           -1
```

```
2889+1292 Sqrt[5]          1
12238+5473 Sqrt[5]        -1
51841+23184 Sqrt[5]        1
219602+98209 Sqrt[5]      -1
930249+416020 Sqrt[5]      1)
```

Bijlage B

Met behulp van Mathematica eenheden bepalen van $\mathbb{Z}[\sqrt[3]{m}]$

In dit onderstaande Mathematica script wordt met behulp van het bewijs van het speciale geval van Dirichlets eenhedenstelling op een snellere manier dan 'trial and error' eenheden van de ring $\mathbb{Z}[\sqrt[3]{m}]$ gevonden. Uitleg over de uitkomsten van dit script kunnen worden gevonden in hoofdstuk 8.

In ln[1] tot en met ln[6] worden de ring $\mathbb{Z}[\sqrt[3]{m}]$ en de waarde van A vastgelegd en c_1, c_2 gekozen, zodat $c_1 \cdot c_2^2 = A$. In ln[8] wordt voor verschillende waarden van i, j, k de absolute waarden van σ_1 en σ_2 berekend, en wordt gekeken of deze waardes kleiner zijn dan respectievelijk c_1 en c_2. Alle i, j, k die daaraan voldoen worden als output gegeven. Vervolgens wordt in ln[9] de norm van de 'nuttige' $a \in \mathbb{Z}[\sqrt[3]{m}]$ berekend met behulp van de ingebouwde functie AlgebraicNumberNorm van Mathematica ('nuttig' wil zeggen de positieve a ongelijk aan nul). In ln[11] tot en met ln[14] wordt het proces herhaald voor andere waarden van c_1, c_2 (hoe vaak dit proces herhaald moet worden, zal niet voor alle m gelijk zijn). Vervolgens zoeken we met behulp van deze uitkomsten een eenheid in $\mathbb{Z}[\sqrt[3]{m}]$. Deze eenheid zullen we weer tot de macht 10 verheffen (zoals in Appendix A beschreven). Zo kunnen we op een vrij snelle manier eenheden in $\mathbb{Z}[\sqrt[3]{m}]$ vinden, zonder letterlijke alle elementen van de ring $\mathbb{Z}[\sqrt[3]{m}]$ te proberen. Voor grotere eenheden is dit alsnog een methode die lang duurt, maar nog altijd sneller dan 'trial and error'.

```
In[1]:= m=5;
In[2]:= beta=m^(1/3);
In[3]:= disc=-27m^2;
In[4]:= A=Sqrt[Abs[disc]]*2/Pi;
In[5]:= numA=N[A,20]
Out[5]= 16.539866862653761485
```

```
In[6]:= c2=4/5
        c1=A/c2^2
Out[6]= 4/5
Out[7]= (375 Sqrt[3])/(8 \[Pi])

In[8]:= g1=For[i=-5,i<=5,i++,For[j=-5,j<=5,j++,For[k=-5,k<=5,k++,
\[Alpha]=Abs[i+j*5^(1/3)+k*5^(2/3)];
\[Alpha]2=Abs[i+j*5^(1/3)*(-1/2+1/2*Sqrt[-3])
+k*5^(2/3)*(-1/2-1/2 Sqrt[-3])]^2;
If[\[Alpha]<c1&&\[Alpha]2<c2,Print[{i,j,k}]]]]]

During evaluation of In[8]:= {-5,-3,-2}
During evaluation of In[8]:= {-3,-2,-1}
During evaluation of In[8]:= {0,0,0}
During evaluation of In[8]:= {3,2,1}
During evaluation of In[8]:= {5,3,2}

In[9]:= test1=AlgebraicNumberNorm[3+2beta+beta^2]
        test2=AlgebraicNumberNorm[5+3beta+2beta^2]
Out[9]= 2
Out[10]= 10

In[11]:= c3=9
         c4=A/c3
Out[11]= 9
Out[12]= 10/(Sqrt[3] \[Pi])

In[13]:= g2=For[i=-5,i<=5,i++,For[j=-5,j<=5,j++,For[k=-5,k<=5,k++,
\[Alpha]=Abs[i+j*5^(1/3)+k*5^(2/3)];
\[Alpha]2=Abs[i+j*5^(1/3)*(-1/2+1/2*Sqrt[-3])
+k*5^(2/3)*(-1/2-1/2 Sqrt[-3])]^2;
If[\[Alpha]<c3&&\[Alpha]2<c4,Print[{i,j,k}]]]]]

During evaluation of In[13]:= {-3,-1,-1}
During evaluation of In[13]:= {-2,-2,-1}
During evaluation of In[13]:= {-2,-1,-1}
During evaluation of In[13]:= {-1,0,0}
During evaluation of In[13]:= {0,0,0}
During evaluation of In[13]:= {1,0,0}
```

```
During evaluation of In[13]:= {2,1,1}
During evaluation of In[13]:= {2,2,1}
During evaluation of In[13]:= {3,1,1}

In[14]:= test3=AlgebraicNumberNorm[2 + beta + beta^2]
Out[14]= 8
In[15]:= test4=test1^3/test3
Out[15]= 1
In[16]:= a=Expand[(3+2beta+beta^2)^3];
In[17]:= b=2+beta+beta^2;

In[18]:= unit2=FullSimplify[Expand[b/a]]
Out[18]= 1-4 5^(1/3)+2 5^(2/3)

In[19]:= unit3=FullSimplify[Expand[a/b]]
Out[19]= 41+24 5^(1/3)+14 5^(2/3)

In[20]:= AlgebraicNumberNorm[unit2]
Out[20]= 1
In[21]:= AlgebraicNumberNorm[unit3]
Out[21]= 1

In[22]:= Transpose[List[Table[Expand[(unit2)^i],{i,1,10}],
Table[AlgebraicNumberNorm[(unit2)^j],{j,1,10}]]]//MatrixForm
Out[22]//MatrixForm=
(1-4 5^(1/3)+2 5^(2/3)                          1
-79+12 5^(1/3)+20 5^(2/3)                       1
-359+528 5^(1/3)-186 5^(2/3)                    1
8641+104 5^(1/3)-3016 5^(2/3)                   1
70001-64620 5^(1/3)+13850 5^(2/3)               1
-853199-206124 5^(1/3)+412332 5^(2/3)           1
-11161079+7329992 5^(1/3)-469570 5^(2/3)        1
71530241+47278608 5^(1/3)-52111696 5^(2/3)      1
1586550241-759959316 5^(1/3)-98165646 5^(2/3)   1
-4049729999-8087816740 5^(1/3)+6114772100 5^(2/3)   1)
```