

Eenheden van orders van getalenvelden

Hoofdstuk 1

Orders

1.1 Definities

Definitie 1.1. Een order is een subring O van een ring A zodat

1. A is een ring die een eindig dimensionele algebra is over \mathbb{Q} .
2. O is een vrije abelse groep voortgebracht door een basis van A over \mathbb{Q} .

1.2 Voorbeelden

- Neem een eindige groep G . Dan is $\mathbb{Q}G$ een eindig dimensionele algebra over \mathbb{Q} . Verder is $\mathbb{Z}G$ een deelring van $\mathbb{Q}G$ en is G een basis voor $\mathbb{Q}G$, + en $\mathbb{Z}G$, + zodat $\mathbb{Z}G$, + een vrije abelse groep is voortgebracht door een basis van $\mathbb{Q}G$ over \mathbb{Q} .

$\mathbb{Z}G$ is een order van $\mathbb{Q}G$

- $M_n(\mathbb{Q})$ is een eindig dimensionele algebra over \mathbb{Q} en $M_n(\mathbb{Z})$ is een deelring van $M_n(\mathbb{Q})$. De verzameling $\{E_{ij} \text{ met } 1 \leq i, j \leq n\}$ is een basis voor $M_n(\mathbb{Q})$ en $M_n(\mathbb{Z})$. Dus :

$M_n(\mathbb{Z})$ is een order van $M_n(\mathbb{Q})$

- $\mathbb{Q}(\epsilon_n)$ is een eindig dimensionele algebra over \mathbb{Q} en $\mathbb{Z}(\epsilon_n)$ is een deelring van $\mathbb{Q}(\epsilon_n)$. Veronderstel dat de graad van de uitbreiding $\mathbb{Q}(\epsilon_n)$ gelijk

is aan k . De verzameling $\{1, \epsilon_n, \epsilon_n^2, \dots, \epsilon_n^{k-1}\}$ is een basis voor $\mathbb{Z}(\epsilon_n)$ en $\mathbb{Q}(\epsilon_n)$. Dus

$\mathbb{Z}(\epsilon_n)$ is een order van $\mathbb{Q}(\epsilon_n)$

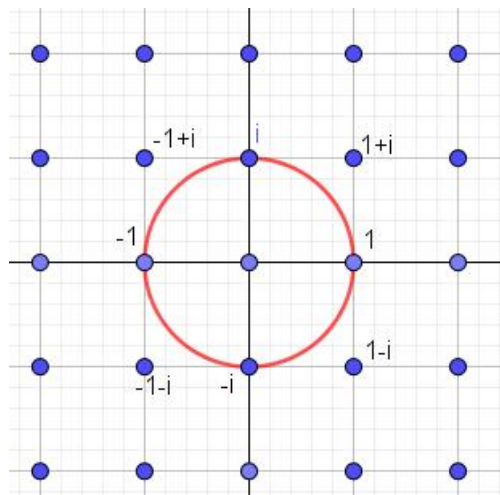
Hoofdstuk 2

Eenheden in orders

2.1 Eenheden van $\mathbb{Z}(i)$

- $\mathbb{Z}(i) = \{a + bi \text{ met } a, b \in \mathbb{Z}\}$ is een order van $\mathbb{Q}(i)$ met als \mathbb{Q} -basis $\{1, i\}$. Ook \mathbb{Z} is een order van $\mathbb{Q}(i)$.
- We zoeken nu naar de eenheden van $\mathbb{Z}(i)$:

$$\begin{aligned} u \text{ is een eenheid van } \mathbb{Z}(i) &\iff \exists v \in \mathbb{Z} : u.v = 1 \\ &\iff |u|.|v| = 1 \\ &\iff |u| \leq 1 \text{ of } |v| \leq 1 \end{aligned}$$



u of v liggen binnen de eenheidscirkel en dus zijn enkel $\pm 1, \pm i$ eenheden.

$$U(\mathbb{Z}(i)) = \{\pm 1, \pm i\}$$

- Een andere manier om dit resultaat te vinden, werkt met de normafbeelding: $N : \mathbb{Q}(i) \rightarrow \mathbb{Q} : a + bi \mapsto a^2 + b^2$. Omdat $N(x.y) = N(x).N(y)$, induceert dit een groepshomomorfisme tussen $U(\mathbb{Z}(i))$ en $U(\mathbb{Z}) = \{1, -1\}$. Dan is $a + bi \in U(\mathbb{Z}(i)) \iff a^2 + b^2 = \pm 1$. Dit geeft hetzelfde resultaat als hierboven.
- Nog anders kan als volgt: $a + bi$ is een eenheid in $\mathbb{Z}(i)$ als er gehele getallen c en d bestaan zo dat $(a + bi)(c + di) = 1$. Dit geeft het stelsel:

$$\begin{cases} ac - bd = 1 \\ ad + bc = 0 \end{cases}$$

De oplossing van dit stelsel is $c = \frac{a}{a^2 + b^2}$ en $d = -\frac{b}{a^2 + b^2}$. Omdat c en d geheel zijn moet $a^2 + b^2 = \pm 1$. Hieruit volgt hetzelfde resultaat.

2.2 Eenheden van $\mathbb{Z}(\sqrt{2})$

- $\mathbb{Q}(\sqrt{2})$ is een kwadratische velduitbreiding van \mathbb{Q} .
- $\mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is een order van $\mathbb{Q}(\sqrt{2})$ met als basis $\{1, \sqrt{2}\}$. Het is ook de deelring van alle algebraïsche gehele van $\mathbb{Q}(\sqrt{2})$.
- Om de eenheden van $\mathbb{Z}(\sqrt{2})$ te berekenen, definiëren we een normafbeelding: $N : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q} : a + b\sqrt{2} \mapsto a^2 - 2b^2$. Omdat $N(x.y) = N(x).N(y)$, induceert dit een groepshomomorfisme tussen $U(\mathbb{Z}(\sqrt{2}))$ en $U(\mathbb{Z}) = \{1, -1\}$. Dan is $a + b\sqrt{2} \in U(\mathbb{Z}(\sqrt{2})) \iff a^2 - 2b^2 = \pm 1$. Dit is een Diophantische vergelijking. Er is steeds een triviale oplossing voor de vergelijking $a^2 - 2b^2 = 1$, namelijk $a = 1, b = 0$. Maar er zijn ook steeds niet-triviale oplossingen. Een oplossing (p, q) van de Diophantische vergelijking coderen we als $p + q\sqrt{2}$. Als (p, q) een minimale oplossing is van $a^2 - 2b^2 = 1$, dan zijn alle andere oplossingen van de vorm $(p + q\sqrt{2})^n$ met $n \in \mathbb{N}$. De vergelijking $a^2 - 2b^2 = -1$ heeft niet noodzakelijk oplossingen, maar als er zijn dan zijn ze van de vorm $(p + q\sqrt{2})^{2n+1}$, waarbij $p + q\sqrt{2}$ een minimale oplossing is. De oplossingen van $a^2 - 2b^2 = 1$ kunnen uit de minimale oplossing van $a^2 - 2b^2 = -1$ gevonden worden via $(p + q\sqrt{2})^{2n}$. Het is duidelijk dat $1 + \sqrt{2}$ een minimale oplossing is van $a^2 - 2b^2 = -1$ Dus geldt:

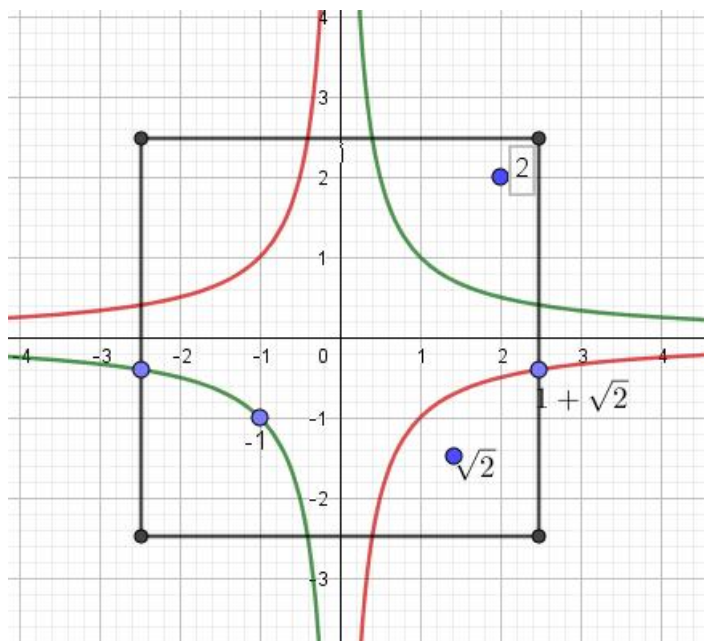
$$U(\mathbb{Z}(\sqrt{2})) = \langle -1 \rangle \langle 1 + \sqrt{2} \rangle$$

- Het kan ook als volgt: $a + b\sqrt{2}$ is een eenheid in $\mathbb{Z}(\sqrt{2})$ als er gehele getallen c en d bestaan zo dat $(a + b\sqrt{2})(c + d\sqrt{2}) = 1$. Dit geeft het stelsel:

$$\begin{cases} ac + 2bd = 1 \\ ad + bc = 0 \end{cases}$$

De oplossing van dit stelsel is $c = \frac{a}{a^2 - 2b^2}$ en $d = -\frac{b}{a^2 - 2b^2}$. Omdat c en d geheel zijn moet $a^2 - 2b^2 = \pm 1$. Hieruit volgt hetzelfde resultaat.

- We kunnen $\mathbb{Z}(\sqrt{2})$ ook inbedden in \mathbb{R}^2 via $\Phi : a + b\sqrt{2} \mapsto (a + b\sqrt{2}, a - b\sqrt{2})$. Elke eenheid van $\mathbb{Z}(\sqrt{2})$ wordt afgebeeld op één van de hyperbolen $xy = 1$ of $xy = -1$.

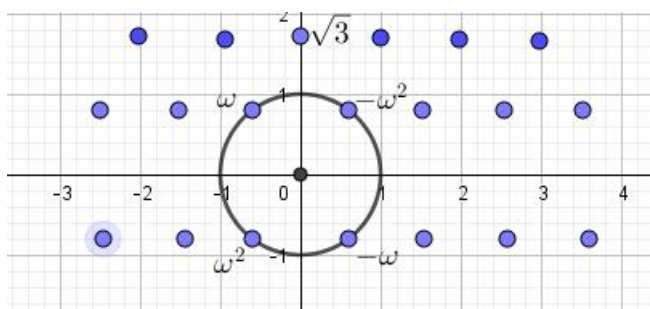


Neem $u = 1 + \sqrt{2}$, dan is u een eenheid van $\mathbb{Z}(\sqrt{2})$, want $u \cdot (\sqrt{2} - 1) = 1$. Construeer het vierkant $K = \{(x, y) \in \mathbb{R}^2 : |x|, |y| \leq u\}$. Er zijn exact 11 punten in K die corresponderen met elementen van $\mathbb{Z}(\sqrt{2})$. Dit zijn $0, \pm 1, \pm\sqrt{2}, \pm 2, \pm(1 + \sqrt{2}), \pm(1 - \sqrt{2})$. Hieruit vinden we 6 eenheden: $\pm 1, \pm(1 + \sqrt{2}), \pm(1 - \sqrt{2})$. Stel nu dat v een willekeurige andere eenheid is van $\mathbb{Z}(\sqrt{2})$, dan proberen we te bewijzen dat $v \in \langle -1, u \rangle$ en zo bekomen we het gewenste resultaat. We kunnen altijd veronderstellen dat $v > 0$. Want als $v < 0$, nemen we $-v$ in plaats van v . Zo kunnen we ook veronderstellen dat $v \geq 1$, want als $v < 1$ zou zijn, vervangen we v door v^{-1} . Welnu, er bestaat een $k \geq 0$ zodat $u^k \leq v < u^{k+1}$. Hieruit

volgt dat $1 \leq u^{-k} \cdot v < u$. We weten dat $w = u^{-k} \cdot v$ een eenheid is van $\mathbb{Z}(\sqrt{2})$, maar we weten nu ook dat $\Phi(w)$ in het getekende vierkant K ligt en $1 \leq w < u$. Bijgevolg is $w = 1$ en dus is $v = u^k$, net wat we wilden bewijzen.

2.3 Eenheden van $\mathbb{Z}(\omega)$

- $\mathbb{Q}(\omega)$ is een kwadratische velduitbreiding van \mathbb{Q} , omdat $\omega^2 = -1 - \omega$.
Verder is $\omega = \frac{-1 + \sqrt{3}}{2}$
- $\mathbb{Z}(\omega) = \{a + b\omega : a, b \in \mathbb{Z}\}$ is een order van $\mathbb{Q}(\omega)$ met als basis $\{1, \omega\}$. Het is ook de deelring van alle algebraïsche gehele van $\mathbb{Q}(\omega)$.
- In onderstaande tekening is het duidelijk dat $\mathbb{Z}(\omega)$ geen element bevat met een modulus kleiner dan 1. Bijgevolg hebben de eenheden modulus 1.



- $|a + b\omega| = \left| \frac{2a - b}{2} + \frac{b\sqrt{3}}{2}i \right|$. De modulus is 1 als $(2a - b)^2 + 3b^2 = 4$. Stel $2a - b = x$, dan krijgen we $x^2 + 3b^2 = 4$. De oplossingen hiervan zijn $(x, b) = (\pm 2, 0), (\pm 1, \pm 1)$ of $(a, b) = (\pm 1, 0), (1, 1), (0, \pm 1), (-1, -1)$.
- Bijgevolg is $U(\mathbb{Z}(\omega)) = \{\pm 1, \pm \omega, \pm \omega^2\}$.

2.4 Eenheden van $\mathbb{Z}(\epsilon_8)$

- $\mathbb{Q}(\epsilon_8) = \mathbb{Q}(i, \sqrt{2})$ is een velduitbreiding van \mathbb{Q} van graad 4. Verder is $\epsilon_8 = \frac{\sqrt{2}}{2}(1 + i)$ en $\epsilon_8^2 = i$. Verder rekenwerk leert ons dat $(\epsilon_8 + \epsilon_8^{-1})^2 = 2$ zodat $\epsilon_8 + \epsilon_8^{-1} = \sqrt{2}$.

- $\mathbb{Z}(\epsilon_8) = \{a + b\epsilon_8 + c\epsilon_8^2 + d\epsilon_8^3 : a, b, c, d \in \mathbb{Z}\}$ is een order van $\mathbb{Q}(\epsilon_8)$ met als basis $\{1, \epsilon_8, \epsilon_8^2, \epsilon_8^3\}$. Het is ook de deelring van alle algebraïsche gehelen van $\mathbb{Q}(\epsilon_8)$.
- Omdat $\mathbb{Z}(\sqrt{2}) \subset \mathbb{Z}(\epsilon_8)$ is $u = 1 + \sqrt{2}$ een eenheid van $\mathbb{Z}(\epsilon_8)$.
- Andere eenheden die we al zeker kunnen berekenen, zijn de cyclotomische eenheden. Zo is $\eta_3(\epsilon_8) = 1 + \epsilon_8 + \epsilon_8^2 = (1 + \frac{\sqrt{2}}{2})(1 + i) = \frac{\sqrt{2}}{2}(\sqrt{2} + 1)(1 + i) = u \cdot \epsilon_8$.
- We berekenen nu $|x|^2$ met $x = a + b\epsilon_8 + c\epsilon_8^2 + d\epsilon_8^3 : a, b, c, d \in \mathbb{Z}$.

$$\begin{aligned} |x|^2 &= \left| a + b\frac{\sqrt{2}}{2}(1+i) + ci + d\frac{\sqrt{2}}{2}(i-1) \right|^2 \\ &= \left(a + b\frac{\sqrt{2}}{2} - d\frac{\sqrt{2}}{2} \right)^2 + \left(\frac{\sqrt{2}}{2}b + c + \frac{\sqrt{2}}{2}d \right)^2 \\ &= a^2 + b^2 + c^2 + d^2 + (ab + bc + cd - ad)\sqrt{2} \end{aligned}$$

- De afbeelding $N : U(\mathbb{Z}(\epsilon_8)) \rightarrow U(\mathbb{Z}(\sqrt{2})) : x \mapsto |x|^2$ is een groeps-homomorfisme. De kern van N bestaat uit de elementen x waarvoor $a^2 + b^2 + c^2 + d^2 = 1$ en $ab + bc + cd - ad = 0$. Het is duidelijk dat $\ker N = \langle \epsilon_8 \rangle$. Verder geldt ook dat $N(u) = u^2$. Omdat $v = u \cdot \epsilon_8$ zal dan ook $N(v) = u^2$.
- Nu ligt u niet in het beeld van N , net zomin als u^{-1} . Dus is $\text{Bld}N = \langle u^2 \rangle$ en bijgevolg is $U(\mathbb{Z}(\epsilon_8)) = \langle \epsilon_8 \rangle \times \langle 1 + \sqrt{2} \rangle = \langle \epsilon_8 \rangle \times \langle 1 + \epsilon_8 + \epsilon_8^2 \rangle$.

2.5 Eenheden van $\mathbb{Z}(i\sqrt{d})$ met d een kwadraatvrij positief geheel getal

- $\mathbb{Q}(i\sqrt{d})$ is een kwadratische velduitbreiding van \mathbb{Q} . Het is het ontbindingsveld van de veelterm $x^2 + d$
- $\mathbb{Z}(i\sqrt{d}) = \{a + bi\sqrt{d} : a, b \in \mathbb{Z}\}$ is een order van $\mathbb{Q}(i\sqrt{d})$ met als basis $\{1, i\sqrt{d}\}$. Het is ook de deelring van alle algebraïsche gehelen van $\mathbb{Q}(i\sqrt{d})$ op voorwaarde dat d bij deling door 4 niet als rest 1 heeft. Als $d \equiv 1 \pmod{4}$, dan is de ring der gehele gegeven door $\mathbb{Z}\left(\frac{1+i\sqrt{d}}{2}\right) = \left\{ \frac{a+bi\sqrt{d}}{2} \text{ met } a \equiv b \pmod{2} \right\}$.

- Om de eenheden van $\mathbb{Z}(i\sqrt{d})$ te berekenen, definiëren we een normafbeelding: $N : \mathbb{Q}(i\sqrt{d}) \rightarrow \mathbb{Q} : a + bi\sqrt{d} \mapsto a^2 + d.b^2$. Omdat $N(x.y) = N(x).N(y)$, induceert dit een groepshomomorfisme tussen $U(\mathbb{Z}(i\sqrt{d}))$ en $U(\mathbb{Z}) = \{1, -1\}$. Dan is $a + bi\sqrt{d} \in U(\mathbb{Z}(i\sqrt{d})) \iff a^2 + db^2 = \pm 1$. Omdat $d > 0$ heeft deze vergelijking enkel $a = \pm 1, b = 0$ als oplossingen. Dus geldt:

$$U(\mathbb{Z}(i\sqrt{d})) = \{\pm 1\}$$

2.6 Eenheden van $\mathbb{Z}(\sqrt{3})$

- $\mathbb{Q}(\sqrt{3})$ is een kwadratische velduitbreiding van \mathbb{Q} .
- $\mathbb{Z}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$ is een order van $\mathbb{Q}(\sqrt{3})$ met als basis $\{1, \sqrt{3}\}$. Het is ook de deelring van alle algebraïsche gehelen van $\mathbb{Q}(\sqrt{3})$.
- Om de eenheden van $\mathbb{Z}(\sqrt{3})$ te berekenen, definiëren we een normafbeelding: $N : \mathbb{Q}(\sqrt{3}) \rightarrow \mathbb{Q} : a + b\sqrt{3} \mapsto a^2 - 3b^2$. Omdat $N(x.y) = N(x).N(y)$, induceert dit een groepshomomorfisme tussen $U(\mathbb{Z}(\sqrt{3}))$ en $U(\mathbb{Z}) = \{1, -1\}$. Dan is $a + b\sqrt{3} \in U(\mathbb{Z}(\sqrt{3})) \iff a^2 - 3b^2 = \pm 1$.
- Dit is een Diophantische vergelijking. Er is steeds een triviale oplossing voor de vergelijking $a^2 - 3b^2 = 1$, namelijk $a = 1, b = 0$. Maar er zijn ook steeds niet-triviale oplossingen. Een oplossing (p, q) van de Diophantische vergelijking coderen we als $p + q\sqrt{3}$. Als (p, q) een minimale oplossing is van $a^2 - 3b^2 = 1$, dan zijn alle andere oplossingen van de vorm $(p + q\sqrt{3})^n$ met $n \in \mathbb{N}$. De minimale oplossing is $(2, 1)$. De vergelijking $a^2 - 3b^2 = -1$ heeft geen oplossingen. Want we kunnen de vergelijking herleiden tot $a^2 + 1 = 3b^2$. Het linkerlid kan nooit een drievoud zijn. Dus geldt:

$$U(\mathbb{Z}(\sqrt{3})) = \langle -1 \rangle \langle 2 + \sqrt{3} \rangle$$

2.7 Eenheden van $\mathbb{Z}(\sqrt{5})$

- $\mathbb{Q}(\sqrt{5})$ is een kwadratische velduitbreiding van \mathbb{Q} .
- $\mathbb{Z}(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$ is een order van $\mathbb{Q}(\sqrt{5})$ met als basis $\{1, \sqrt{5}\}$. Het is niet de deelring van alle algebraïsche gehelen van $\mathbb{Q}(\sqrt{5})$. Deze wordt gegeven door $\mathbb{Z}(\frac{1+\sqrt{5}}{2})$.

- Om de eenheden van $\mathbb{Z}(\sqrt{5})$ te berekenen, definiëren we een normafbeelding: $N : \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{Q} : a + b\sqrt{5} \mapsto a^2 - 5b^2$. Omdat $N(x.y) = N(x).N(y)$, induceert dit een groepshomomorfisme tussen $U(\mathbb{Z}(\sqrt{5}))$ en $U(\mathbb{Z}) = \{1, -1\}$. Dan is $a + b\sqrt{5} \in U(\mathbb{Z}(\sqrt{5})) \iff a^2 - 5b^2 = \pm 1$.
- Dit is een Diophantische vergelijking. Er is steeds een triviale oplossing voor de vergelijking $a^2 - 3b^2 = 1$, namelijk $a = 1, b = 0$. Maar er zijn ook steeds niet-triviale oplossingen. Een oplossing (p, q) van de Diophantische vergelijking coderen we als $p + q\sqrt{5}$. Als (p, q) een minimale oplossing is van $a^2 - 5b^2 = -1$, dan zijn alle andere oplossingen van de vorm $(p + q\sqrt{5})^n$ met $n \in \mathbb{N}$. De minimale oplossing is $(2, 1)$. Dus geldt:

$$U(\mathbb{Z}(\sqrt{5})) = \langle -1 \rangle \left\langle 2 + \sqrt{5} \right\rangle$$

- Analoog kunnen we de eenheden bepalen van $\mathbb{Z}(\frac{1+\sqrt{5}}{2})$. Hierbij geldt:

$$U(\mathbb{Z}(\frac{1+\sqrt{5}}{2})) = \langle -1 \rangle \left\langle \frac{1+\sqrt{5}}{2} \right\rangle$$

- Omdat $2 + \sqrt{5} = \left(\frac{1+\sqrt{5}}{2}\right)^3$ is het duidelijk dat $U(\mathbb{Z}(\sqrt{5})) \subset U(\mathbb{Z}(\frac{1+\sqrt{5}}{2}))$

2.8 Eenheden van $M_2(\mathbb{Z})$

- $M_2(\mathbb{Q})$ is een eindig dimensionale algebra over \mathbb{Q} en $M_2(\mathbb{Z})$ is een deelring van $M_2(\mathbb{Q})$. De verzameling $\{E_{11}, E_{12}, E_{21}, E_{22}\}$ is een basis voor $M_2(\mathbb{Q})$ en $M_2(\mathbb{Z})$.
- Dus is $M_2(\mathbb{Z})$ een order van $M_2(\mathbb{Q})$.
- De groep van de eenheden van $M_2(\mathbb{Z})$ is $GL_2(\mathbb{Z})$, de verzameling 2×2 matrices met determinant ± 1 .
- De verzameling 2×2 matrices met determinant $+1$ noemen we met $SL_2(\mathbb{Z})$. Nu heeft $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ orde twee en een determinant gelijk aan -1 . Dus geldt er dat

$$U(M_2(\mathbb{Z})) = SL_2(\mathbb{Z}) \rtimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- De groep $SL_2(\mathbb{Z})$ is gegeven door volgende representatie:

$$SL_2(\mathbb{Z}) = \{T, V, J : T^2 = V^3 = J \text{ en } J^2 = 1\}$$

Hierbij is $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $V = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ en $J = -I_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

Elk torsie element van $SL_2(\mathbb{Z})$ is toegevoegd aan een element van $\langle T \rangle$ of $\langle U \rangle$. Bijgevolg is de orde van een torsie element van $SL_2(\mathbb{Z})$ een deler van 3 of 4.

2.9 Eenheden van $\mathbb{H}(\mathbb{Z})$

- $\mathbb{H}(\mathbb{Q}) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}\}$ is een 4 dimensionele algebra over \mathbb{Q} en $\mathbb{H}(\mathbb{Z})$ is een deelring van $\mathbb{H}(\mathbb{Q})$. De verzameling $\{1, i, j, k\}$ is een basis voor $\mathbb{H}(\mathbb{Q})$ en $\mathbb{H}(\mathbb{Z})$. De vermenigvuldiging is gedefinieerd volgens de regels $i^2 = j^2 = k^2 = -1$ en $ij = -ji = k$.
- Dus is $\mathbb{H}(\mathbb{Z})$ een order van $\mathbb{H}(\mathbb{Q})$.
- We kunnen $\mathbb{H}(\mathbb{Z})$ bekijken als discrete deelverzameling van \mathbb{R}^4 met als norm $N : \mathbb{H}(\mathbb{Q}) \rightarrow \mathbb{Q}$, gedefinieerd als $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$. Deze normfunctie behoudt de vermenigvuldiging, of met andere woorden $N(xy) = N(x)N(y)$.
- Om de eenheden te bepalen van $\mathbb{H}(\mathbb{Z})$ zoeken we dus naar de elementen $x = a + bi + cj + dk$ waarvoor $a^2 + b^2 + c^2 + d^2 = 1$. Het oplossen van deze Diophantische vergelijkingen geeft dat:

$$U(\mathbb{H}(\mathbb{Z})) = \{\pm 1, \pm i, \pm j, \pm k\}$$