Lecture XLVIII: Quadratic integer rings II

Recall: Last time we proved the following results for $D \in \mathbb{Z} \smallsetminus \{0,1\}$ square-free.

Theorem 1: $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$

Any $z \in \mathbb{Q}(\sqrt{D})$ can be written uniquely as $z = a + b\sqrt{D}$ with $a, b \in \mathbb{Q}$.

- We defined:

$$\begin{aligned} \mathbb{Q}(\sqrt{D}) &\xrightarrow{N} \mathbb{Q} \\ a+b\sqrt{D} &\longmapsto a^2 - b^2 D = (a+b\sqrt{D})(a-b\sqrt{D}) \end{aligned}$$

Definition: Assume $D \in \mathbb{Z} \smallsetminus \{0,1\}$ is square free. We define the <u>quadratic ring of integers</u> of $\mathbb{Q}(\sqrt{D})$ as the ring $\mathcal{O}(\sqrt{D}) := \mathbb{Z}[\omega] := \{a + b\omega : a, b \in \mathbb{Z}\}$, where

$$\omega = \begin{cases} \dfrac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \bmod 4 \\ \sqrt{D} & \text{if } D \equiv 2, 3 \bmod 4 \end{cases}$$

Theorem 2:

$$\begin{aligned} \mathcal{O}(\sqrt{D}) &= \{\alpha \in \mathbb{Q}(\sqrt{D}) : N(\alpha) \in \mathbb{Z}\} \\ &= \{\alpha \in \mathbb{Q}(\sqrt{D}) : \alpha \text{ is integral}\} \end{aligned}$$

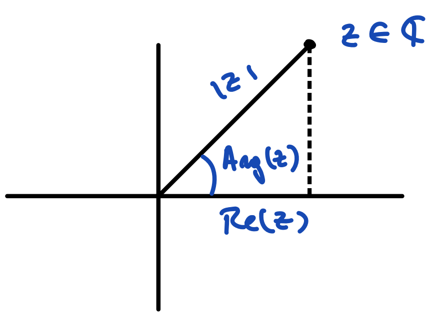
(integral $= \alpha$ is the root of a monic polynomial in $\mathbb{Z}[x]$)

Remark

$$N(a+b\omega) = \begin{cases} a^2 - b^2 D & \text{if } \omega = \sqrt{D} \\ a^2 + ab + b^2\left(\dfrac{1-D}{4}\right) & \text{if } \omega = \dfrac{1+\sqrt{D}}{2} \end{cases}$$

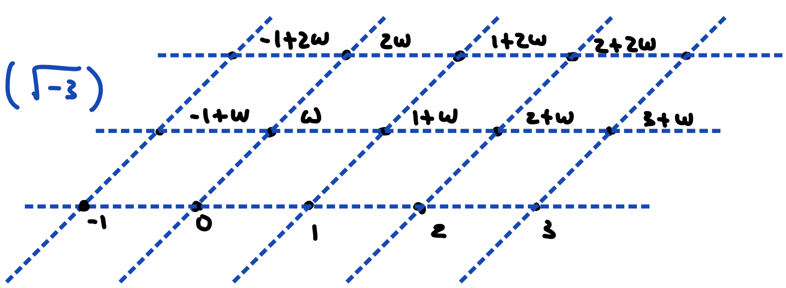
TODAY'S GOAL: Study some values of $D<0$ making $\mathcal{O}(\sqrt{D})$ a Euclidean domain

Lemma: $D < 0 \implies N(a+b\sqrt{D}) = |a+b\sqrt{D}|^2$ ($|\ | =$ norm as a complex number)



$-\pi \leq \arg(z) \leq \pi$

Example: $D = -3 \rightsquigarrow \mathcal{O}(\sqrt{-3})$



$\omega = \frac{1}{2} + \frac{\sqrt{3}}{2} i$

§48.1 Some remarks for general D square-free $D \neq 0,1$:

- Issue 1: $z \in \mathcal{O}(\sqrt{D})$, $N(z) \in \mathbb{Z}$. To get a non-negative integer, we need to take $|\ |$

$\rightsquigarrow \tilde{N} : \mathcal{O}(\sqrt{D}) \longrightarrow \mathbb{Z}_{\geq 0}$ with $\tilde{N}(z) = |N(z)|$.

- We know $\mathcal{O}(\sqrt{-1}) \underset{\substack{\uparrow \\ -1 \equiv 3 \bmod 4}}{=} \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ is a Euclidean domain (Lecture 39).

Let's review how we proved this. Here, $\tilde{N}(z) = N(z) \geq 0$

- We used the following properties of N:
  - $N(a+bi) = a^2+b^2 = a^2 - b^2(-1)$ is multiplicative
  - $N(a+bi) \geq 0 \ \forall a,b$ & $N(a+bi) = 0 \iff a+bi = 0$.
  - $N(a+bi) = 1 \iff (a+bi) \in (\mathbb{Z}[i])^\times$
- Given $w, z \in \mathbb{Z}[i]$ $z \neq 0$ we take the quotient $\frac{w}{z} = c+di \in \mathbb{C}$.

We pick $a, b \in \mathbb{Z}[i]$ such that (shift to bound $N(w - z(a+bi))$)

$$\left.\begin{aligned} -\tfrac{1}{2} &\leq \overbrace{c-a}^{=:\alpha} < \tfrac{1}{2} \\ -\tfrac{1}{2} &\leq \underbrace{d-b}_{\beta} < \tfrac{1}{2} \end{aligned}\right\} \Rightarrow w = \underbrace{z(a+bi)}_{\in \mathbb{Z}[i]} + (\alpha+\beta i)z$$

with $r = (\alpha+\beta i)z \in \mathbb{Z}[i]$ ($= w - z(a+bi)$ & $\mathbb{Z}[i]$ is a ring) and

$$-\tfrac{1}{2} \leq \alpha < \tfrac{1}{2}, \quad -\tfrac{1}{2} \leq \beta < \tfrac{1}{2} \Rightarrow N(\alpha+\beta i) \leq \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2}$$

$$\Rightarrow N((\alpha+\beta i)z) = N(\alpha+\beta i)N(z) \leq \tfrac{1}{2}N(z) < N(z)$$

Q: What can we extend to $\mathcal{O}(\sqrt{D})$ for D square-free, $D \neq 0,1$?

Lemma 2: $\tilde{N}$ is multiplicative

Proof: $N(a+b\sqrt{D}) = (a+b\sqrt{D})(a-b\sqrt{D})$ for $a, b \in \mathbb{Q}$.

$$\begin{aligned} N((a+b\sqrt{D})(c+h\sqrt{D})) &= N((ac+bhD) + (ah+cb)\sqrt{D}) \\ &= ((ac+bhD) + (ah+cb)\sqrt{D})((ac+bhD) - (ah+cb)\sqrt{D}) \\ &= (a+b\sqrt{D})(c+h\sqrt{D})(a-b\sqrt{D})(c-h\sqrt{D}) \\ &= (a+b\sqrt{D})(a-b\sqrt{D})(c+h\sqrt{D})(c-h\sqrt{D}) = N(a+b\sqrt{D})\,N(c+h\sqrt{D}) \end{aligned}$$

Since $|\ |$ is multiplicative on $\mathbb{Q}$, we conclude that $\tilde{N}$ is multiplicative $\square$

Lemma 3: $N(a+b\sqrt{D}) = 0 \iff a = b = 0$. Thus $\tilde{N}(z) = 0$ for $z \in \mathcal{O}(\sqrt{D}) \iff z = 0$.

Proof: If $a+b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ has $N(a+b\sqrt{D}) = 0$, then $(a+b\sqrt{D})(a-b\sqrt{D}) = 0$

in $\mathbb{Q}$. Then, $a+b\sqrt{D}=0$ (so, $a=b=0$) or $a-b\sqrt{D}=0$ (so $a=b=0$).

Corollary: $\mathcal{O}(\sqrt{D})^\times = \{ z \in \mathcal{O}(\sqrt{D}) : \tilde{N}(z)=1 \}$

Proof: ($\subseteq$) $\tilde{N}(1)=1$, $\tilde{N}$ is multiplicative & $\mathbb{Z}^\times = \{\pm 1\}$. This ensures ($\subseteq$) holds.

($\supseteq$) If $z \in \mathcal{O}(\sqrt{D})$ & $\tilde{N}(z)=1$ then $z = a+b\sqrt{D}$ with $a,b\in\mathbb{Q}$. We get

$|(a+b\sqrt{D})(a-b\sqrt{D})| = 1$

Claim: $a+b\sqrt{D} \in \mathcal{O}(\sqrt{D}) \implies a-b\sqrt{D} \in \mathcal{O}(\sqrt{D})$ by construction

Pf/. If $D \equiv 2,3 \mod 4$ then $\mathcal{O}(\sqrt{D}) = \mathbb{Z}[\sqrt{D}]$, so $a+b\sqrt{D} \in \mathcal{O}(\sqrt{D}) \iff a,b\in\mathbb{Z}$

- If $D\equiv 1 \mod 4$ then $\mathcal{O}(\sqrt{D}) = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$, so

$$a+b\sqrt{D} \in \mathcal{O}(\sqrt{D}) \iff a+b\sqrt{D} = c + h\left(\frac{1+\sqrt{D}}{2}\right) \quad \text{with } c,h\in\mathbb{Z}$$

Thus, $a+b\sqrt{D} = \left(c+\frac{h}{2}\right) + \frac{h}{2}\sqrt{D}$ & $a-b\sqrt{D} = c+\frac{h}{2} - \frac{h}{2}\sqrt{D} = c+h-\frac{h}{2}-\frac{h}{2}\sqrt{D}$

$$= \underbrace{a+h}_{\in\mathbb{Z}} + (-1)\left(\frac{1+\sqrt{D}}{2}\right) \in \mathbb{Z}[\omega] = \mathcal{O}(\sqrt{D})$$

Then, if $a+b\sqrt{D} \in \mathcal{O}(\sqrt{D})$ has $\tilde{N}(a+b\sqrt{D})=1$, then $\varepsilon = N(a+b\sqrt{D}) = \pm 1$

$\Rightarrow (a+b\sqrt{D})^{-1} = \varepsilon\,(a-b\sqrt{D}) \in \mathcal{O}(\sqrt{D})$. □

Remark: Using $\mathcal{O}(\sqrt{D}) = \{\alpha \in \mathbb{Q}(\sqrt{D}) : N(\alpha)\in\mathbb{Z}\}$, the statement is obvious.

Next: We take several examples of $D<0$ & see if the shifting method we used for $\mathbb{Z}[i]$ applies or not.

§48.2 The case $D=-2$:

Theorem: $R = \mathcal{O}(\sqrt{-2})$ is a Euclidean domain with $\tilde{N}(z) = N(z)$ $\forall z\in R$

Note: $D=-2 \equiv 2 \mod 4$, so $\mathcal{O}(\sqrt{-2}) = \mathbb{Z}[\sqrt{-2}]$.

$D<0 \Rightarrow N(z) = |z|^2$ viewing $z\in\mathbb{C}$.

Proof: The same proof technique used for $\mathbb{Z}[i]$ works in this example.

We want to show (R,N) satisfies the Euclidean property, namely given $\alpha,\beta\in R$ with $\beta\neq 0$, $\exists\, q,r\in R$ with $\alpha = q\beta + r$ such that $r=0$ or $r\neq 0$ and $N(r)<N(\beta)$.

We write $\frac{\alpha}{\beta} \in \underset{\text{field}}{\mathbb{Q}(\sqrt{-2})} \subseteq \mathbb{C}$ as $\frac{\alpha}{\beta} = \rho_1 + \rho_2\sqrt{-2}$ with $\rho_1,\rho_2\in\mathbb{Q}$.

we can find $q_1,q_2\in\mathbb{Z}$ s.t $-\frac{1}{2} \leq \rho_1 - q_1 \leq \frac{1}{2}$ & $-\frac{1}{2}\leq \rho_2 - q_2 \leq \frac{1}{2}$

Take $q = q_1 + q_2\sqrt{-2} \in R$ & $r = (\rho_1 + \rho_2\sqrt{-2} - q)\beta$

Then $r, q \in R$ & $N(r) = N((\rho_1+\rho_2\sqrt{-2}) - q)\, N(\beta)$ (by Lemma 2)

By construction $\gamma = (\rho_1 + \rho_2\sqrt{-2}) - q = (\rho_1 - q_1) + (\rho_2 - q_2)\sqrt{-2} \in \mathbb{Q}(\sqrt{-2})$

satisfies $N(\gamma) = (\rho_1 - q_1)^2 + 2(\rho_2 - q_2)^2 \leq \left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2 = \frac{1}{4} + \frac{1}{2} = \frac{3}{4} < 1$

Thus, if $r \neq 0$ we get $N(r) = N(\gamma)N(\beta) < 1\, N(\beta) = N(\beta)$

$\beta \neq 0 \Rightarrow N(\beta) \neq 0$ (Lemma 3) $\square$

§48.3 The case $D=-3$:

Theorem: $R = \mathcal{O}(\sqrt{-3})$ is a Euclidean domain with $\tilde{N}(z) = N(z)\ \forall z \in R$

Note: $D = -3 \equiv 1 \mod 4$, so $\mathcal{O}(\sqrt{-3}) = \mathbb{Z}[\omega]$ with $\omega = \frac{1}{2} + \frac{\sqrt{-3}}{2}$

$D < 0 \Rightarrow N(z) = |z|^2$ viewing $z \in \mathbb{C}$.

Proof: We check the Euclidean property is satisfied. Take $\alpha, \beta \in R$ with $\beta \neq 0$

As in §48.2, we write $\frac{\alpha}{\beta} \in \mathbb{Q}(\sqrt{-3})$ as $\frac{\alpha}{\beta} = \rho_1 + \rho_2\sqrt{-3}$ for $\rho_1, \rho_2 \in \mathbb{Q}$

We now pick an appropriate shift in $\mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right)$, a shift of the form $\left(a + \frac{b}{2}\right) + \frac{b}{2}\sqrt{-3}$ with $a, b \in \mathbb{Z}$

$\Rightarrow \exists \left(\left(a+\frac{b}{2}\right) + \frac{b}{2}\sqrt{-3}\right) \in \mathbb{Z}[\omega]$ (for $a, b \in \mathbb{Z}$) such that

$$\gamma = (\rho_1 + \rho_2\sqrt{-3}) - \left(a + b\,\frac{1+\sqrt{-3}}{2}\right) \in \mathbb{Q}(\sqrt{-3}) \text{ satisfies}$$

$$-\frac{1}{4} \leq \rho_2 - \frac{b}{2} \leq \frac{1}{4} \quad \text{and} \quad -\frac{1}{2} \leq \rho_1 - \left(a+\frac{b}{2}\right) = \left(\rho_1 - \frac{b}{2}\right) - a \leq \frac{1}{2}$$

Thus, $N(\gamma) = \left(\rho_1 - \left(a+\frac{b}{2}\right)\right)^2 + 3\left(\rho_2 - \frac{b}{2}\right)^2 \leq \left(\frac{1}{2}\right)^2 + 3\left(\frac{1}{4}\right)^2 = \frac{1}{4} + \frac{3}{16} = \frac{7}{16} < 1$

Conclusion: $q = a + \frac{b}{2} + \frac{b}{2}\sqrt{3} \in R$ & $r = \gamma\beta \in R$ satisfies $\alpha = q\beta + r$

with $r = 0$ or ($r \neq 0$ & $N(r) = N(\gamma)\underbrace{N(\beta)}_{\neq 0} < N(\beta)$). $\square$

Remark: Same arguments work for $D = -7, -11$ (both are $\equiv 1 \mod 4$)

($N(\gamma) \leq \left(\frac{1}{2}\right)^2 + 7\left(\frac{1}{4}\right)^2 = \frac{11}{16} < 1$ for $D = -7$ & $N(\gamma) \leq \left(\frac{1}{2}\right)^2 + 11\left(\frac{1}{4}\right)^2 = \frac{15}{16} < 1$ for $D = -11$.)

§48.4 The case $D=-5$:

Theorem: $R=\mathcal{O}(\sqrt{-5})$ is not a Euclidean domain. Moreover, it is not a PID.

Note: $D=-5\equiv 3 \bmod 4$, so $\mathcal{O}(\sqrt{-5})=\mathbb{Z}[\sqrt{-5}]$

$D<0 \Rightarrow N(z)=|z|^2$ viewing $z\in\mathbb{C}$.

Proof: We show R is NOT a PID, hence it cannot be a Euclidean domain by Lemma §46.5. We do so by building an explicit ideal I of R that is not principal.

Claim: $I=(3, 2+\sqrt{-5})\subseteq R$ is not a principal ideal.

Pf/ We argue by contradiction, and assume $\exists\, \alpha\in R$ with $I=(\alpha)$.

Then, $3\in(\alpha) \Rightarrow 3=\alpha\beta$ for some $\beta\in R$

Taking $N(\ )$, we get $9=|3|^2=|\alpha|^2|\beta|^2$ with $|\alpha|^2, |\beta|^2\in\mathbb{Z}$.

As $|\alpha|^2=a^2+b^2 5$ with $a,b\in\mathbb{Z}$ we know $|\alpha|^2\neq 3$. This gives us 2 options for $|\alpha|^2\in\mathbb{Z}$

CASE 1: $|\alpha|^2=9$. In this case, $|\beta|^2=1$, so by construction, $\beta=\pm1$

Hence, $3=\alpha(\pm1)$ ie $(3, 2+\sqrt{-5})=(3)$. But this means $2+\sqrt{-5}\in(3)$, ie $\exists\, m,n\in\mathbb{Z}$ such that $2+\sqrt{-5}=3(m+n\sqrt{-5})=3m+3n\sqrt{-5}$

$\Rightarrow 2=3m \quad m\in\mathbb{Z}$ Contradiction!

CASE 2: $|\alpha|^2=1$, so $\alpha=\pm1$ hence $I=R$

This means $1\in(3, 2+\sqrt{-5})$ ie $\exists\, \gamma,\delta\in R$ with $1=3\gamma+(2+\sqrt{-5})\delta$

Multiplying both sides by $(2-\sqrt{-5})$ we get:

$$2-\sqrt{-5}=3\gamma(2-\sqrt{5})+\delta\underbrace{(2^2+5\cdot1^2)}_{=9}$$

$$2-\sqrt{-5}=3\underbrace{(\gamma(2-\sqrt{5})+3\delta)}_{\in R}$$

$\Rightarrow \exists\, m,n\in\mathbb{Z}$ with $2-\sqrt{-5}=3(m+n\sqrt{-5})$, so $2=3m$ with $m\in\mathbb{Z}$ Contradiction!