Lecture XLVII: Quadratic integer rings

Recall: A **Euclidean domain** is an integral domain R such that there exists a function

$$N : R \longrightarrow \mathbb{Z}_{\geq 0} \quad (\text{optional: } N(0)=0 \text{ or define } N: R\setminus\{0\} \longrightarrow \mathbb{Z}_{\geq 0})$$

such that for every $a, b \in R$, $b \neq 0$ we can find $q, r \in R$ such that:

$$a = qb + r \quad \text{AND} \quad N(r) < N(b) \text{ if } r \neq 0$$

Lemma: Euclidean domains are PIDs.

Examples: $\mathbb{Z}$, $K[x]$ with K a field, $\mathbb{Z}[i]$

TODAY'S GOAL: Introduce another family of examples, namely Quadratic Integers.

§47.1 Quadratic integer rings:

Definition: Consider $D \in \mathbb{Z}\setminus\{0,1\}$ with $\sqrt{D} \notin \mathbb{Z}$. A **quadratic field extension of $\mathbb{Q}$** is a field of the form $R = \mathbb{Q}(\sqrt{D}) \subseteq \mathbb{C}$ Here $\mathbb{Q}(\sqrt{D})$ is the smallest subfield of $\mathbb{C}$ containing $\sqrt{D} \in \mathbb{C}$

Remark: We can assume D is square-free

Q: What do elements of $\mathbb{Q}(\sqrt{D})$ look like?

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

Proof: We show the double inclusion:

($\supseteq$) $\mathbb{Q}, \{\sqrt{D}\} \subseteq \mathbb{Q}(\sqrt{D})$ ring $\Rightarrow$ $a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ $\forall a, b \in \mathbb{Q}$.

($\subseteq$) Enough to show $R = (\text{RHS})$ is a field (a subfield of $\mathbb{C}$) It is a subset of $\mathbb{C}$, so we need to check fewer things (closed under $+, \cdot$, $0 \in R$, $1 \in R$ & $R^\times = R\setminus\{0\}$)

$(R, +, 0)$ is an abelian group, $1 = 1 + 0\sqrt{D} \in R$

$$(a + b\sqrt{D})(c + f\sqrt{D}) = \underbrace{(ac + bfD)}_{\in \mathbb{Q}} + \underbrace{(af + bc)}_{\in \mathbb{Q}}\sqrt{D} \in R$$

Claim: $q + b\sqrt{D} = 0 \iff a = 0$ & $b = 0$

PF/ $0 = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D = 0 \Rightarrow b^2 D = a^2$

Write $a = \frac{r}{s}$ $(r,s)=1$, $b = \frac{m}{n}$ $(m,n)=1$ to get $(ms)^2 D = (rn)^2$ in $\mathbb{Z}$.

If $r \neq 0 \Rightarrow m \neq 0$ Then $(ms)^2 D = (rn)^2 \neq 0$ in $\mathbb{Z}$ and D is square free, which cannot happen!

Then $r = 0$ (i.e. $a = 0$) & so $a + b\sqrt{D} = b\sqrt{D} = 0$ in $\mathbb{C}$ forces $b = 0$.

Then, pick $a+b\sqrt{D} \in R \setminus \{0\}$ $\Rightarrow$ $(a+b\sqrt{D})(a-b\sqrt{D}) = a^2-b^2D \in \mathbb{Q} \setminus \{0\}$

(because both $a+b\sqrt{D}$ & $a-b\sqrt{D} \in \mathbb{C}$ and are non-zero by the claim).

Hence: $(a+b\sqrt{D})^{-1} = \frac{a}{a^2-b^2D} - \frac{b}{a^2-b^2D}\sqrt{D} \in R$. □

Remark: Quadratic integers are subrings of $\mathbb{Q}(\sqrt{D})$.

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

Proof: Direct consequence of the claim made in the proof of Lemma 1.

As a consequence of the proof of Lemma 1 we can define a function:

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

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

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

Remark: The name comes from the following definition: we say $\alpha \in \mathbb{C}$ is **integral** if we can find $p \in \mathbb{Z}[x] \setminus \{0\}$ monic with $p(\alpha) = 0$.

Example:
- $\sqrt{2}$, $\sqrt[3]{3}$ are integral ($p = x^2-2$, $p = x^3-3$)
- $\frac{1+\sqrt{5}}{2}$ is integral ($p = (x-(\frac{1+\sqrt{5}}{2}))(x+\frac{1-\sqrt{5}}{2}) = x^2 - \frac{2}{2}x + \frac{1-5}{4}$
$= x^2-x-1 \in \mathbb{Z}[x]$)

The following statements explain our choice of $\mathcal{O}(\sqrt{D})$.

Proposition: $\mathcal{O}(\sqrt{D}) = \{\alpha \in \mathbb{Q}(\sqrt{D}) : N(\alpha) \in \mathbb{Z}\}$ for $D \in \mathbb{Z} \setminus \{0,1\}$ square-free

Proof: $\mathbb{Z}[\omega] \subseteq \mathcal{O}(\sqrt{D})$ is easy: we just need to check that $N(a+b\omega) \in \mathbb{Z}$.

We check both options for ω separately:

CASE 1: Assume $D \equiv 2, 3 \bmod 4$, so $\omega = \sqrt{D}$. Then $N(a+b\omega) = N(a+b\sqrt{D}) = a^2-b^2D \in \mathbb{Z}$

because $a, b, D \in \mathbb{Z}$

CASE 2: Assume $D \equiv 1 \bmod 4$, so $\omega = \frac{1+\sqrt{D}}{2}$. Then $N(a+b\omega) = N\left(a + b\frac{(1+\sqrt{D})}{2}\right) =$

$$= N\left(\left(a+\tfrac{b}{2}\right) + \tfrac{b}{2}\sqrt{D}\right) = \frac{(2a+b)^2}{4} - \frac{b^2}{4}D = \frac{4a^2}{4} + \frac{b^2}{4} + ab - \frac{b^2}{4}D = \underbrace{a^2+ab+b^2\frac{(1-D)}{4}}_{\in \mathbb{Z}}$$

since $D \equiv 1 \bmod 4 \Rightarrow \frac{1-D}{4} \in \mathbb{Z}$.

Thus $N(a+b\omega) \in \mathbb{Z}$.

The converse requires some results we still don't have

The proof shows some relevant computation.

Corollary: $N(a+b\omega) = \begin{cases} a^2 - b^2 D & \text{if } D \equiv 2,3 \bmod 4 \\ a^2 + ab + b^2\left(\frac{1-D}{4}\right) & \text{if } D \equiv 1 \bmod 4 \end{cases}$

Theorem: $\mathcal{O}_{(\sqrt{D})} = \{ a+b\sqrt{D} \in \mathbb{Q}(\sqrt{D}) : a+b\sqrt{D} \text{ is integral} \}$

Proof: It is easy to see $\alpha \in \mathbb{Z}[\omega]$ is integral for all α, so we get ($\subseteq$)

- If $D \equiv 2,3 \bmod 4$, we get $\mathcal{O}(\sqrt{D}) = \mathbb{Z}[\sqrt{D}]$ so the polynomial

$$P(x) = (x - (a+b\sqrt{D}))(x-(a-b\sqrt{D})) = x^2 - 2ax + (a^2 - b^2 D) \in \mathbb{Z}[x]$$

is monic and $P(a+b\sqrt{D}) = 0 \quad \forall\, a, b \in \mathbb{Z}$

- If $D \equiv 1 \bmod 4$, we get $\mathcal{O}(\sqrt{D}) = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$, and the polynomial

$$P(x) = \left(x - \left(a + b\frac{1+\sqrt{D}}{2}\right)\right)\left(x - \underbrace{\left(a+\tfrac{b}{2} - b\frac{\sqrt{D}}{2}\right)}_{\left(a+b - b\left(\frac{1+\sqrt{D}}{2}\right)\right)}\right)$$

$$= x^2 - (2a+b)x + \left(\left(a+\tfrac{b}{2}\right)^2 - \frac{b^2 D}{4}\right) = x^2 - (2a+b)x + \left(a^2 + ab + b^2\left(\frac{1-D}{4}\right)\right)$$

lies in $\mathbb{Z}[x]$, is monic and $P\left(a + b\frac{1+\sqrt{D}}{2}\right) = 0$.

For the converse, we will need some more facts.

Remark: In both cases, the constant term of $P(x)$ is $N(a+b\omega)$.

Thus, to show the missing inclusions, it is enough to show:

$$\{ a+b\sqrt{D} \in \mathbb{Q}(\sqrt{D}) : a+b\sqrt{D} \text{ is integral} \} = \{ a+b\sqrt{D} \in \mathbb{Q}(\sqrt{D}) : N(a+b\sqrt{D}) \in \mathbb{Z} \}$$

This uses three facts:

① $p \in \mathbb{Q}[x]$ monic of smallest degree that has $a+b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ as a root $\Leftrightarrow$ $a-b\sqrt{D}$ is also a root. Then, $q_{(x)} = (x-(a+b\sqrt{D}))(x-(a-b\sqrt{D})) = x^2 - 2ax - (a^2-b^2D) \mid p(x)$ in $\mathbb{Q}[x]$. In particular, if $b \neq 0$ then $q_{(x)} \in \mathbb{Q}[x]$ is the polynomial of smallest degree that has $a+b\sqrt{D}$ as a root.

② Any $p \in \mathbb{Z}[x]$ monic of minimal degree that has $a+b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ as a root with $b \neq 0$ cannot be factored non-trivially in $\mathbb{Q}[x]$ (by Gauss's Lemma, which we see in a future lecture). This shows that $p(x) = q_{(x)} \in \mathbb{Z}[x]$ so

$$N(a+b\sqrt{D}) = a^2 - b^2 D \in \mathbb{Z} \quad \text{and} \quad 2a \in \mathbb{Z}.$$

③ Any $a \in \mathbb{Q}$ is integral if and only if $a \in \mathbb{Z}$.

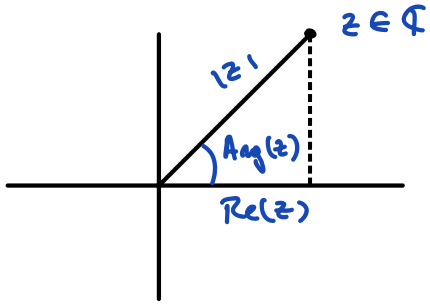
Pf/ ($\Leftarrow$) $p(x) = x - a \in \mathbb{Z}[x]$ is monic and $p(a) = 0$

($\Rightarrow$) If a is integral, then $\exists\, p \in \mathbb{Z}[x]$ monic of minimal degree that has $p(a) = 0$. Then: $p(x) = (x-a) \cdot f_{(x)}$ with $f \in \mathbb{Q}[x]$ (do long division)

$\Rightarrow a \in \mathbb{Z}$ (denominator of a | leading coefficient of p.) (We'll see this in a future lecture)

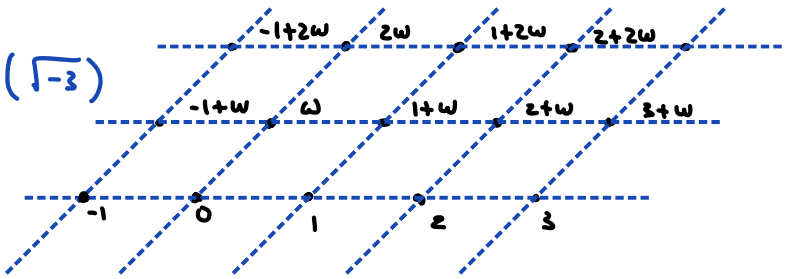
Combining these statements we will get to any $a+b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ integral lies in $\mathcal{O}(\sqrt{D})$, as the Theorem claimed.

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



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

$D = -3 \Rightarrow \mathcal{O}(\sqrt{-3})$



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

Q: For which values of D is $\mathcal{O}(\sqrt{D})$ a Euclidean domain?

A: NOT all!

Here is the precise statement (We will not prove it)

Theorem 2: Let $D \in \mathbb{Z} \setminus \{0,1\}$ be a square-free integer. Then, $\mathcal{O}(\sqrt{D})$ is a Euclidean domain if, and only if:

(i) $(D<0)$ $\quad D = -1, -2, -3, -7, -11$

(ii) $(D>0)$ $\quad D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$

Furthermore, the Euclidean norm on $\mathcal{O}(\sqrt{D})$ equals $\tilde{N}(z) = |N(z)|$.