Lecture XLIX: Quadratic integer rings III

§49.1 Summary:

So far, we worked out some examples of rings of quadratic integers $\mathcal{O}(\sqrt{D})$ where $D \in \mathbb{Z} \smallsetminus \{0,1\}$ is square free.

Recall: $\mathcal{O}(\sqrt{D}) = \mathbb{Z}[\omega]$ with $\omega = \begin{cases} \sqrt{D} & \text{if } D \equiv 2,3 \bmod 4 \\ \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \bmod 4 \end{cases}$

D	-1	-2	-3	-5	-7	-11
ω	$\sqrt{-1}$	$\sqrt{-2}$	$\frac{1+\sqrt{-3}}{2}$	$\sqrt{-5}$	$\frac{1+\sqrt{-7}}{2}$	$\frac{1+\sqrt{-11}}{2}$
$\mathcal{O}(\sqrt{D}) = \mathbb{Z}[\omega] \cap \mathbb{Q}(\sqrt{D}) \subseteq \mathbb{C}$	Euclidean (hence PID)	Euclidean (hence PID)	Euclidean (hence PID)	NOT PID (hence not Euclidean)	Euclidean (hence PID)	Euclidean (hence PID)

TODAY If $D = -19$, we get a PID that is not a Euclidean domain.

§49.2 The Case $D = -19$:

Theorem 1: The ring $R = \mathcal{O}(\sqrt{-19})$ is not a Euclidean domain.

Note: $-19 \equiv 1 \bmod 4$, so $\mathcal{O}(\sqrt{-19}) = \mathbb{Z}[\omega]$ for $\omega = \frac{1+\sqrt{-19}}{2}$

Before we prove the Theorem, we need the following fact, which we already discussed in Corollary §48.1.

Lemma 1: If $R = \mathcal{O}(\sqrt{-19})$, then $R^{\times} = \{\pm 1\}$.

Pf/ Recall that $D<0 \Rightarrow N(\alpha) = |\alpha|^2 \;\; \forall\, \alpha \in \mathbb{Q}(\sqrt{D}) \supseteq \mathcal{O}(\sqrt{D})$.

Corollary §48.1 says $R^{\times} = \{\alpha \in \mathcal{O}(\sqrt{-19}) : |\alpha|^2 = 1\}$

Now, for $\alpha = a + b\omega$ $a,b \in \mathbb{Z}$ we have $1 = |\alpha|^2 = \left(a+\frac{b}{2}\right)^2 + \frac{19}{4}b^2 \geq \frac{19}{4}b^2 \geq b^2$

Thus $|\alpha|^2 = 1 \iff \left(a+\frac{b}{2}\right)^2 = 1$ & $b^2 = 0 \iff a = \pm 1$ & $b = 0$.

Proof of Theorem 1: We show R is not Euclidean arguing by contradiction. Assume R is Euclidean with respect to some function $\mathcal{N}: R \longrightarrow \mathbb{Z}_{\geq 0}$. (not necessarily $N = |\,|^2$)

Claim 1: R is not a field

Pf/ $\omega \notin R^\times$ since $\omega \neq \pm 1$ & $R^\times = \{\pm 1\}$ by Lemma 1

By Claim 1, we can consider the set $X = \{a \in R : a \neq 0, a \notin R^\times\}$

Note: $X \neq \emptyset$ since $\omega \in X$.

Let $u \in X$ so that $N(u) = \min\{N(x) : x \in X\}$

Thus, for any $x \in R$, the Euclidean property of $N : R \longrightarrow \mathbb{Z}_{\geq 0}$ implies that

$x = qu + r$ where $q, r \in R$ and $(r = 0$ or $(r \neq 0$ & $N(r) < N(u))$

The definition of u then implies $r = 0$ or $r \in R^\times$.

Claim 2: There is not $u \in R$ with this property.

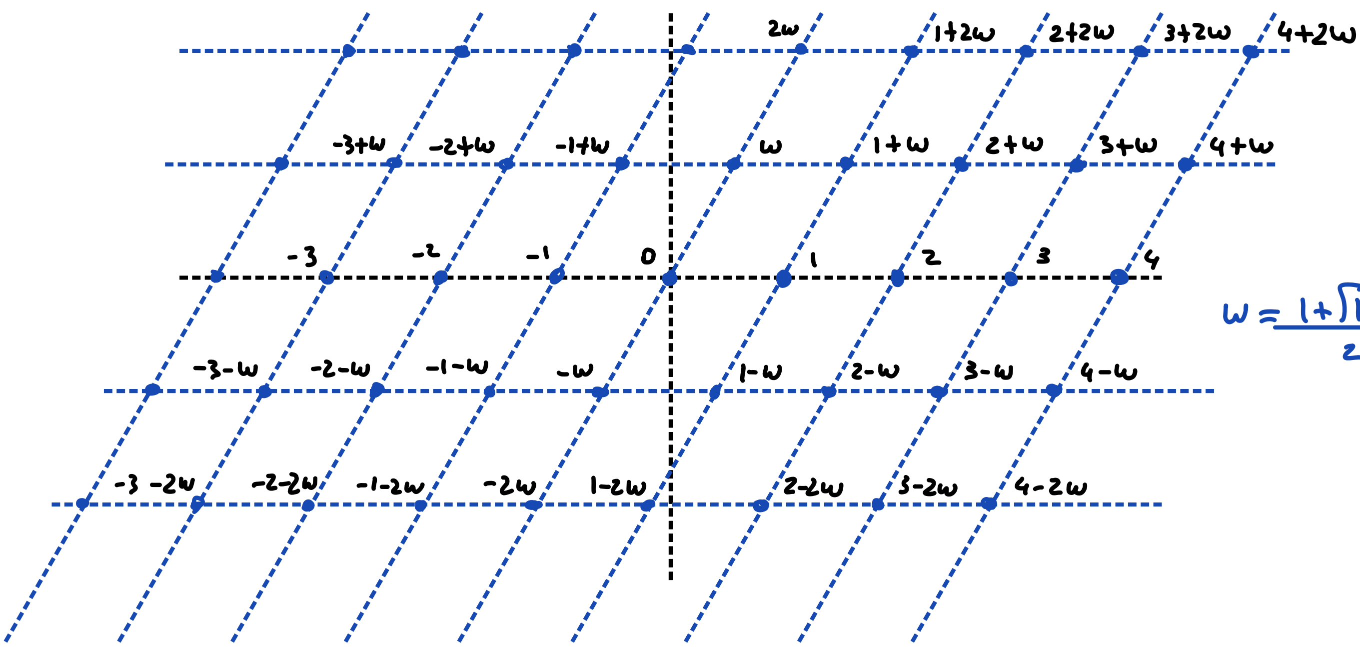
Pf/ By Lemma 1 (above), we conclude our remainders have only 3 options $r = 0, 1, -1$.

Thus, $\boxed{\forall x \in R \ \exists r \in \{0, 1, -1\} \text{ such that } u \text{ divides } x - r \text{ in } R}$ (*)

- In particular, for $x = 2 \in R$, we must have $u \mid 2, 1$ or 3 in R.

Since $u \in X$, we have $u \notin R^\times$, so $u \nmid 1$. This leaves 2 options: $u \mid 2$ or $u \mid 3$.

Next, we draw $\mathbb{Z}[\omega]$ & try to determine the location of u.



$\omega = \dfrac{1+\sqrt{19}\,i}{2}$

We treat the two possibilities: $u \mid 2$ or $u \mid 3$ in R and conclude none are possible.

CASE 1: u divides 2 in R, ie $\exists v \in R$ with $2 = uv$

$\implies |u|^2 |v|^2 = |2|^2 = 4$.

Note: If $a + b\omega \in R$, we have $|a + b\omega|^2 = \left|\left(a + \frac{b}{2}\right) + \frac{b}{2}\sqrt{-19}\right|^2 = \left(a + \frac{b}{2}\right)^2 + \frac{19}{4} b^2$

so $|a+b\omega|^2 \geq 5$ if $b \neq 0$ (because $a, b \in \mathbb{Z}$)

Then, $|u|^2 |v|^2 = 4 \implies u, v \in \mathbb{Z}$, so ($|u|^2 = 4$ & $|v|^2 = 1$) or ($|u|^2 = 1$ & $|v|^2 = 4$)

The second option is not possible by Lemma, since $|u|^2 = 1 \Rightarrow u \in R^\times$ <u>Contr!</u>

Thus: $u = \pm 2$ & $v \in R^\times$.

Then, taking $x = \omega$ in (*) we get $u = \pm 2 \mid \omega$, $\omega - 1$ or $\omega + 1$ in R.

Thus $|\pm 2|^2 = 4 \mid |\omega|^2, |\omega - 1|^2$ or $|\omega + 1|^2$ in $\mathbb{Z}$. This is impossible since $|\omega|^2 = |\omega - 1|^2 = 5$ & $|\omega + 1|^2 = 7$ & these are all prime numbers.

<u>CASE 2:</u> u divides 3 in R, ie $\exists\, v \in R$ with $3 = uv$

$\implies |u|^2 |v|^2 = |3|^2 = 9$.

As with case 1, we know $|x| = 0, 1$ or ≥ 5 if $x \in R$, so $|u|^2 = 9$ & $|v|^2 = 1$ is the only valid option because $u \notin R^\times$. Thus, $u = \pm 3$

As before, taking $x = \omega$ in (*) yields $u = \pm 3 \mid \omega, \omega - 1$ or $\omega + 1$ in R, thus $9 = |u|^2 \mid |\omega|^2, |\omega - 1|^2$ or $|\omega + 1|^2$ in $\mathbb{Z}$. Since $|\omega|^2 = |\omega - 1|^2 = 5$ & $|\omega + 1|^2 = 7$, the last divisibility statement cannot occur. $\square$

<u>Theorem 2:</u> The ring $R = \mathcal{O}(\sqrt{-19})$ is a PID.

In order the prove the statement, we need an auxilliary result.

<u>Definition:</u> Let R be an integral domain and $N : R \longrightarrow \mathbb{Z}_{\geq 0}$ a function with $N(0) = 0$. We call such a function a <u>norm</u>.

We say the norm is <u>positive</u> if $N(x) = 0 \iff x = 0$.

A positive norm $N : R \longrightarrow \mathbb{Z}_{\geq 0}$ is called a <u>Dedekind-Hasse norm</u> if for every nonzero $a, b \in R$ either $a \in (b)$ or $\exists\, c \in (a, b)$ with $N(c) < N(b)$. That is, either $b \mid a$ in R or $\exists\, s, t \in R$ with $0 < N(sa - tb) < N(b)$.

<u>Remark:</u> For a Euclidean domain with respect to a positive norm, we take $s = 1$.

<u>Lemma 2:</u> Let R be an integral domain. If R has a positive Dedekind-Hasse norm, then R is a PID

⚠ The result is stronger: the converse is also True. However, we will not need it here.

Proof: Let $I \subsetneq R$ be a non-zero ideal & let $b \in I$ with $N(b) = \min\{N(x) : x \in I \setminus \{0\}\}$

Assume $a \in I \setminus \{0\}$, so $(a,b) \subseteq I$. The minimality of $N(b)$ together with the D-H norm property implies $b \mid a$, so $a \in (b)$. Thus $I = (b)$, as we wanted □

Proof of Theorem 2: By Lemma 2, it is enough to show that $R = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ has a positive D-H norm, namely $N(a+b\omega) = (a+\frac{b}{2})^2 + 19\frac{b^2}{4} = a^2+ab+\frac{b^2}{4}+19\frac{b^2}{4} = a^2+ab+5b^2$

- We know $N(a+b\omega) = |a+b\omega|^2$ so N is a positive norm on R.
- N is a multiplicative norm.
- Let $\alpha, \beta \in R \setminus \{0\}$ with $\frac{\alpha}{\beta} \notin R$. We must find $s, t \in R$ with $0 < N(s\alpha - t\beta) < N(\beta)$

Since N is multiplicative, this is equivalent to requiring $0 < N(\frac{\alpha}{\beta}s - t) < 1$.

Since $\frac{\alpha}{\beta} \in \mathbb{Q}(\sqrt{-19})$, we write $\frac{\alpha}{\beta} = \frac{a+b\sqrt{-19}}{c}$ with $a,b,c \in \mathbb{Z}$ with no common divisor & $c > 1$ (because $\frac{\alpha}{\beta} \notin R$)

The condition $\gcd(a,b,c) = 1 \Rightarrow \exists\, x,y,z \in \mathbb{Z}$ with $ax+by+cz = 1$

We treat 5 cases for $c > 1$ in $\mathbb{Z}$ & find suitable $s,t \in R$ with $N(\frac{\alpha}{\beta}s - t) < 1$ for each case

CASE 1: Assume $c \geq 5$

Let $N = ay - 19bx \in \mathbb{Z}$ & apply the division algorithm by c in $\mathbb{Z}$ to get

$$ay - 19bx = cq + r \quad \text{with} \quad |r| \leq c/2 \quad (\text{instead of } r \in [0,c))$$

Take $s = y + x\sqrt{-19}$ & $t = q - z\sqrt{-19}$. We have:

- $s, t \in R$
- $\frac{\alpha}{\beta}s - t = \frac{a+b\sqrt{-19}}{c}(y+x\sqrt{-19}) - (q - z\sqrt{-19}) = \frac{(ay-19bx-cq)}{c} + \frac{(ax+by+cz)\sqrt{-19}}{c}$

$= \frac{r}{c} + \frac{(ax+by+cz)}{c}\sqrt{-19} = \frac{r}{c} + \frac{1}{c}\sqrt{-19}$

$\Rightarrow 0 < N(\frac{\alpha}{\beta}s - t) = \left(\frac{r}{c}\right)^2 + \frac{19}{c^2} \leq \left(\frac{1}{2}\right)^2 + \frac{19}{c^2} = \frac{1}{4} + \frac{19}{c^2}$

Claim: Since $c \geq 5$ we get the desired condition $0 < N(\frac{\alpha}{\beta}s - t) < 1$.

Pf/ • $\frac{1}{4} + \frac{19}{c^2} < 1 \iff c^2 + 19\cdot 4 < 4c^2$
$76 < 3c^2$
$\frac{76}{3} < c^2$

$(\lceil \frac{76}{3} \rceil = 26)$ so the statement is true for $c \geq 6$.

- If $c = 5$, then $|r| \leq 5/2$ & $r \in \mathbb{Z} \Rightarrow |r| \leq 2 \Rightarrow r^2 + 19 \leq 23 < 25$. □

Thus, it remains to treat the cases $c = 2, 3$ or 4. We do this by hand.

CASE 2: Assume $c=2$

The conditions $\gcd(a,b,c)=1$ and $\frac{\alpha}{\beta} \notin R$ implies that one of a or b is even and the other one is odd.

Taking $s=1$ and $t = \frac{(a-1)+b\sqrt{-19}}{2}$ we get

- $s, t \in R$
- $\frac{\alpha}{\beta}s - t = \frac{a+b\sqrt{-19}}{2} - \frac{(a-1)+b\sqrt{-19}}{2} = \frac{1}{2}$ satisfies

$0 < N\left(\frac{\alpha}{\beta}s-t\right) = \frac{1}{4} < 1$, as we wanted

CASE 3: Assume $c=3$

Since $\gcd(a,b,3)=1$, the integer $N(a+b\sqrt{-19}) = a^2+19b^2$ is not divisible by 3 (because $a^2+b^2 \equiv 0 \bmod 3 \iff a \equiv b \equiv 0 \bmod 3$)

Write $a^2+19b^2 = 3q+r$ for $q, r \in \mathbb{Z}$ with $r = 1, 2$.

Taking $s = a-b\sqrt{-19}$ and $t = q$ we get:

- $s, t \in R$
- $\frac{\alpha}{\beta}s - t = \frac{a+b\sqrt{-19}}{3}(a-b\sqrt{-19}) - q = \frac{a^2+19b^2}{3} - q = \frac{r}{3} = \frac{1}{3}$ or $\frac{2}{3}$

In both cases: $0 < N\left(\frac{\alpha}{\beta}s-t\right) \leq \left(\frac{2}{3}\right)^2 = \frac{4}{9} < 1$

CASE 4: Assume $c=4$

Since $\gcd(a,b,4)=1$, we see that a and b are not both even. We have 2 options.

(1) If a & b have different parity (one even & one odd), then $N(a+b\sqrt{-19}) = a^2+19b^2$ is odd. Then, dividing a^2+19b^2 by 4 in $\mathbb{Z}$ we get

$$a^2+19b^2 = 4q+r$$

for some $q, r \in \mathbb{Z}$ with $r = 1, 3$.

Taking $s = a-b\sqrt{-19}$ and $t = q$ we get:

- $s, t \in R$
- $\frac{\alpha}{\beta}s - t = \frac{a+b\sqrt{-19}}{4}(a-b\sqrt{-19}) - q = \frac{a^2+19b^2-4q}{4} = \frac{r}{4} = \frac{1}{4}$ or $\frac{3}{4}$

In both cases, $0 < N\left(\frac{\alpha}{\beta}s-t\right) \leq \left(\frac{3}{4}\right)^2 = \frac{9}{16} < 1$.

(2) If both a & b are odd, then $a^2+19b^2 \equiv 1+19 \equiv 4 \mod 8$ $\quad (x = \pm 1, \pm 3 \mod 8 \Rightarrow x^2 \equiv 1 \mod 8)$

Thus, $a^2+19b^2 = 8\cdot q + 4$ for some $q \in \mathbb{Z}$.

Taking $s = \dfrac{a-b\sqrt{-19}}{2}$ and $t = q$ we get:

- $s, t \in R$
- $\dfrac{\alpha}{\beta}s - t = \dfrac{a+b\sqrt{-19}}{4}\left(\dfrac{a-b\sqrt{-19}}{2}\right) - q = \dfrac{a^2+19b^2}{8} - q = \dfrac{8q+4}{8} - q = \dfrac{1}{2}$

Then: $0 < N\left(\dfrac{\alpha}{\beta}s - t\right) = \left(\dfrac{1}{2}\right)^2 = \dfrac{1}{4} < 1.$

§49.3 Summary:

We have proven the following

Theorem: We have strict inclusions

$$\text{Fields} \subsetneq \text{Euclidean domains} \subsetneq \text{Principal Ideal domains} \subsetneq \text{Noetherian domains}$$

$\not\ni \mathbb{Z} \in$ $\qquad$ $\not\ni \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \in$ $\qquad$ $\not\ni \mathbb{Z}[x] \in$, $\not\ni \mathbb{Z}[\sqrt{-5}] \in$, $\not\ni K[x,y] \in$

Q: What next? Unique Factorization Domains (next time)