Math 71: Principal Ideal Domains, Quadratic Integer Rings, and Euclidean Domains

Lily McBeath*

November 7, 2023

Contents

*This LaTeX template is courtesy of Lucy Knight.

1 Principal Ideal Domains

In a previous lecture we defined principal ideals and observed that in some rings, every ideal can be generated by a single element.

Definition 1.1. A **principal ideal domain (PID)** is an integral domain in which every ideal is principal.

Examples include $\mathbb{Z}$ and $F[x]$, the ring of polynomials with coefficients in F a field. In fact, any field F is a principal ideal domain, since its only ideals are (0) and $(1) = F$.
One non-example is $\mathbb{Z}[x]$, the polynomials with integral coefficients. As we saw in a previous lecture, the ideal $(2, x) \subset \mathbb{Z}[x]$ is not principal.
To summarize, so far we have defined the following classes of commutative rings with multiplicative identity:

$$\{\text{fields}\} \subset \{\text{principal ideal domains}\} \subset \{\text{integral domains}\}.$$

All of the inclusions are proper: $\mathbb{Z}$ is an example of a PID which is not a field, and $\mathbb{Z}[x]$ is an example of an integral domain which is not a PID.

2 Quadratic Integer Rings

Recall the **quadratic field**

$$\mathbb{Q}(\sqrt{D}) = \{x + y\sqrt{D} : x, y \in \mathbb{Q}\},$$

for D a squarefree integer. For the remainder of this section, we will characterize subrings of $\mathbb{Q}(\sqrt{D})$ which share certain properties analogous to the properties of the subring $\mathbb{Z}$ of $\mathbb{Q}$.

2.1 Introduction to Quadratic Integers

Consider the subset

$$\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} : a, b \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{D}).$$

One can check that $\mathbb{Z}[\sqrt{D}]$ is a subring of $\mathbb{Q}(\sqrt{D})$ under the addition and multiplication defined on $\mathbb{Q}(\sqrt{D})$. Can we find a larger subring of $\mathbb{Q}(\sqrt{D})$? Consider the subset

$$\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] := \left\{a + b\left(\frac{1+\sqrt{D}}{2}\right) : a, b \in \mathbb{Z}\right\} \subset \mathbb{Q}(\sqrt{D}).$$

It is straightforward to check that $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ is closed under addition.
Is it closed under multiplication? Let $\alpha, \beta \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$, where

$$\alpha := a + b\left(\frac{1+\sqrt{D}}{2}\right) \quad \text{and} \quad \beta := c + d\left(\frac{1+\sqrt{D}}{2}\right).$$

Then

$$\begin{aligned}
\alpha\beta &= \left(a + b\left(\frac{1+\sqrt{D}}{2}\right)\right)\left(c + d\left(\frac{1+\sqrt{D}}{2}\right)\right) \\
&= ac + (ad + bc)\left(\frac{1+\sqrt{D}}{2}\right) + bd\left(\frac{1+2\sqrt{D}+D}{4}\right) \\
&= ac + (ad + bc)\left(\frac{1+\sqrt{D}}{2}\right) + bd\left(\frac{1+\sqrt{D}}{2} + \frac{D-1}{4}\right) \\
&= ac + bd\left(\frac{D-1}{4}\right) + (ad + bc + bd)\left(\frac{1+\sqrt{D}}{2}\right),
\end{aligned}$$

so $\alpha\beta \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ if $4 \mid D-1$. That is, $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ is a subring of $\mathbb{Q}(\sqrt{D})$ if $D \equiv 1 \bmod 4$.
In fact, this is an "if and only if" statement.

Proposition 2.1. *Let $\mathbb{Q}(\sqrt{D})$ be a quadratic field for D squarefree. Then $\mathbb{Z}[\frac{1+\sqrt{D}}{2}] \subset \mathbb{Q}(\sqrt{D})$ is a subring if and only if $D \equiv 1 \bmod 4$.*

Proof. ($\Longleftarrow$) Since $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ is closed under addition as a subset of $\mathbb{Q}(\sqrt{D})$, is nonempty (contains 1), and is closed under multiplication if $D \equiv 1 \bmod 4$, this direction holds.
($\Longrightarrow$) We will prove the contrapositive: if $D \not\equiv 1 \bmod 4$, then $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ is not a subring.
Let $\frac{1+\sqrt{D}}{2} \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. Then by the calculation given above, the square of $\frac{1+\sqrt{D}}{2}$ is

$$\left(\frac{1+\sqrt{D}}{2}\right)^2 = \left(\frac{D-1}{4}\right) + \left(\frac{1+\sqrt{D}}{2}\right).$$

Let $a := \frac{D-1}{4}$, then $(\frac{1+\sqrt{D}}{2})^2 = a + \frac{1+\sqrt{D}}{2}$. If $D \not\equiv 1 \bmod 4$, then $4 \nmid D-1$, so $a \notin \mathbb{Z}$. So $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ is not closed under multiplication, and therefore is not a subring of $\mathbb{Q}(\sqrt{D})$. □

These observations motivate the following definition.

Definition 2.2. The **ring of integers** of the quadratic field $\mathbb{Q}(\sqrt{D})$ (also referred to as the **quadratic integer ring**) is the subring $\mathbb{Z}[\omega] \subset \mathbb{Q}(\sqrt{D})$ where

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

We will denote $\mathbb{Z}[\omega] \subset \mathbb{Q}(\sqrt{D})$ by $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ or $\mathcal{O}_D$, and we will call elements of $\mathcal{O}_D$ **quadratic integers**.

Example 2.3. Let $D = -1$. Then since $-1 \equiv 3 \bmod 4$,

$$\mathcal{O}_{-1} = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Elements of this ring are referred to as the **Gaussian integers**.

Example 2.4. Let $D = -3$. Then since $-3 \equiv 1 \bmod 4$,

$$\mathcal{O}_{-3} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{-3}}{2}\right) : a, b \in \mathbb{Z}\right\}.$$

Elements of this ring are referred to as the **Eisenstein integers**.
Recall Euler's formula

$$e^{i\theta} = \cos\theta + i\sin\theta,$$

then we see that

$$e^{i2\pi/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = -1 + \frac{1+\sqrt{-3}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right].$$

In fact,

$$\mathbb{Z}[e^{i2\pi/3}] = \{a + be^{i2\pi/3} : a, b \in \mathbb{Z}\} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right].$$

2.2 The Norm on $\mathcal{O}_D$

In calculus we use functions such as the absolute-value norm

$$\begin{array}{rccc} |\cdot|: & \mathbb{R} & \to & \mathbb{R}_{\geqslant 0} \\ & x & \mapsto & |x| \end{array}$$

and the Euclidean norm

$$\begin{array}{rccc} \|\cdot\|_2: & \mathbb{R}^n & \to & \mathbb{R}_{\geqslant 0} \\ & v & \mapsto & \sqrt{v \cdot v} \end{array}$$

to capture the "size" of real numbers and vectors. For a complex number $z = x + yi \in \mathbb{C}$, where $x, y \in \mathbb{R}$, its absolute value (or modulus) $|z|$ is given by the function

$$\begin{array}{rccc} |\cdot|: & \mathbb{C} & \to & \mathbb{R}_{\geqslant 0} \\ & z & \mapsto & \sqrt{z \cdot \overline{z}} = \sqrt{x^2 + y^2}, \end{array}$$

where $\overline{z} = x - yi$ is the complex conjugate of z. In this section, we will use an algebraic definition of norm to similarly capture the "size" of quadratic integers.

Definition 2.5. The **field norm** on $\mathbb{Q}(\sqrt{D})$ is the map

$$\begin{array}{rccc} N: & \mathbb{Q}(\sqrt{D}) & \to & \mathbb{Q} \\ & x + y\sqrt{D} & \mapsto & (x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - Dy^2. \end{array}$$

Proposition 2.6. *The field norm on $\mathbb{Q}(\sqrt{D})$ is multiplicative. That is, for all $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$,*

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Proof. Let $\alpha = x + y\sqrt{D}$ and $\beta = x' + y'\sqrt{D}$. Then

$$\alpha\beta = (x + y\sqrt{D})(x' + y'\sqrt{D}) = xx' + yy'D + (xy' + yx')\sqrt{D}.$$

We calculate that

$$\begin{aligned} N(\alpha\beta) &= (xx' + yy'D)^2 - D(xy' + yx')^2 \\ &= (xx')^2 + 2xx'yy'D + (yy'D)^2 - D(xy')^2 - 2Dxy'yx' - D(yx')^2 \\ &= (xx')^2 - D(yx')^2 - D(xy')^2 + (Dyy')^2 \\ &= (x^2 - Dy^2)(x'^2 - Dy'^2) \\ &= N(\alpha)N(\beta), \end{aligned}$$

as desired. □

The field norm can be restricted to $\mathcal{O}_D = \mathbb{Z}[\omega]$ in the following way.

Proposition 2.7. *Let $\alpha = a + b\omega \in \mathbb{Z}[\omega] \subset \mathbb{Q}(\sqrt{D})$. Then*

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

where

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

Proof. Let $\alpha \in \mathbb{Z}[\omega]$. In the case where $D \equiv 2, 3 \bmod 4$, we can write $\alpha = a + b\sqrt{D}$, so

$$N(\alpha) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2.$$

Else, $D \equiv 1 \bmod 4$, so $\omega = \frac{1+\sqrt{D}}{2}$ and $\alpha = a + b\frac{1+\sqrt{D}}{2}$ for $a, b \in \mathbb{Z}$. First, observe that we can rewrite α in the form

$$\alpha = x + y\sqrt{D},$$

where $x := a + b/2$ and $y := b/2$. Then, applying the field norm, we get

$$\begin{aligned} N(\alpha) &= x^2 - Dy^2 \\ &= \left(a + \frac{b}{2}\right)^2 - D\left(\frac{b}{2}\right)^2 \\ &= a^2 + ab + \frac{b^2}{4} - D\frac{b^2}{4} \\ &= a^2 + ab + b^2\left(\frac{1-D}{4}\right), \end{aligned}$$

and this agrees with our definition

$$\begin{aligned} N(\alpha) &= (a + b\omega)(a + b\overline{\omega}) \\ &= \left(a + b\left(\frac{1+\sqrt{D}}{2}\right)\right)\left(a + b\left(\frac{1-\sqrt{D}}{2}\right)\right) \\ &= \left(a + \frac{b}{2} + \frac{b}{2}\sqrt{D}\right)\left(a + \frac{b}{2} - \frac{b}{2}\sqrt{D}\right) \\ &= a^2 + \frac{ab}{2} - \frac{ab}{2}\sqrt{D} + \frac{ab}{2} + \frac{b^2}{4} - \frac{b^2}{4}\sqrt{D} + \frac{ab}{2}\sqrt{D} + \frac{b^2}{4}\sqrt{D} - \frac{b^2}{4}D \\ &= a^2 + ab + b^2\left(\frac{1-D}{4}\right), \end{aligned}$$

as desired. □

Observe that unlike the norms discussed at the beginning of this section, the field norm is not necessarily positive. On the other hand, when restricted to the quadratic integer ring, the field norm is actually integer-valued.

Proposition 2.8. *If $\alpha \in \mathcal{O}_D$, then $N(\alpha) \in \mathbb{Z}$.*

Proof. Let $\alpha \in \mathcal{O}_D$ and consider the case where $D \equiv 2, 3 \bmod 4$, then $\alpha = a + b\sqrt{D}$ for some $a, b \in \mathbb{Z}$. So by Proposition 2.7,

$$N(\alpha) = a^2 - Db^2 \in \mathbb{Z},$$

as desired.
For the case where $D \equiv 1 \bmod 4$, we have $\alpha = a + b\frac{1+\sqrt{D}}{2}$ for $a, b \in \mathbb{Z}$. Then again from Proposition 2.7, we have

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

which is an integer since $4 \mid D - 1$. □

Note that we can also define the field norm on $\mathbb{Q}(\sqrt{D})$ (and the restriction to the ring of integers $\mathcal{O}_D$) without coordinates in the following way.

Proposition 2.9. *The map*

$$\begin{array}{rccc} \sigma: & \mathbb{Q}(\sqrt{D}) & \to & \mathbb{Q}(\sqrt{D}) \\ & x+y\sqrt{D} & \mapsto & x-y\sqrt{D} \end{array}$$

is a ring isomorphism.

Proof. Exercise. □

Then for all $\alpha \in \mathbb{Q}(\sqrt{D})$, $N(\alpha) = \alpha \cdot \sigma(\alpha)$, with σ as defined above.

Example 2.10. The field norm on $\mathbb{Q}(i)$ (and on the subring of Gaussian integers) is given by

$$N(x+yi) = x^2 + y^2.$$

Observe that for any $\alpha \in \mathbb{Q}(i)$, $N(\alpha) = |\alpha|^2$, where $|\alpha|$ is the complex absolute value.

In general, the field norm is the square of the complex absolute value when $\mathbb{Q}(\sqrt{D})$ is an **imaginary quadratic field**, i.e., when $D < 0$.

Proposition 2.11. *Let $\alpha \in \mathbb{Q}(\sqrt{D})$ with $D < 0$. Then $N(\alpha) = |\alpha|^2$.*

Proof. Let $\alpha = x + y\sqrt{D} = x + iy\sqrt{-D}$, where $-D > 0$. Then x and $y\sqrt{-D}$ are real numbers and we have

$$\begin{aligned} |\alpha|^2 &= |x + iy\sqrt{-D}|^2 \\ &= \left(\sqrt{x^2 + (y\sqrt{-D})^2}\right)^2 \\ &= x^2 - Dy^2 \\ &= N(\alpha), \end{aligned}$$

as desired. □

Example 2.12. The field norm on $\mathbb{Q}(\sqrt{-3})$ is given by

$$N(x+y\sqrt{-3}) = x^2 + 3y^2.$$

For an Eisenstein integer $\alpha = a + b\frac{1+\sqrt{-3}}{2} \in \mathcal{O}_{-3}$, the restriction of the field norm is

$$N(\alpha) = a^2 + ab + b^2.$$

That being said, in a **real quadratic field** $\mathbb{Q}(\sqrt{D})$ with $D > 0$, Proposition 2.11 does not hold. In fact, any $\alpha \in \mathbb{Q}(\sqrt{D}) \subset \mathbb{R}$ has $|\alpha| = \alpha$, so to show that $N(\alpha) \neq |\alpha|^2$ it suffices to find α such that $N(\alpha) \neq \alpha^2$. Let $\alpha = \sqrt{D} \in \mathcal{O}_D \subset \mathbb{Q}(\sqrt{D})$, then

$$N(\alpha) = -D \neq D = \alpha^2 = |\alpha|^2,$$

since $D > 0$ is a nonzero integer.

2.3 Units in $\mathcal{O}_D$

Now we consider which elements of the quadratic integer ring $\mathcal{O}_D$ are invertible. Recall that $\mathcal{O}_D^\times$ denotes the multiplicative group of units in the ring $\mathcal{O}_D$.

Proposition 2.13. *Let $\alpha \in \mathcal{O}_D$ be a quadratic integer. Then $\alpha \in \mathcal{O}_D^\times$ if and only if $N(\alpha) \in \{\pm 1\}$.*

Proof. ($\Longrightarrow$) Let $\alpha \in \mathcal{O}_D^\times$. Then by definition, there exists $\beta \in \mathcal{O}_D$ such that $\alpha\beta = 1$. Then applying the norm to both sides, $N(\alpha\beta) = N(1) = 1$. By Proposition 2.6, this implies $N(\alpha)N(\beta) = 1$. But since the norm is integer-valued for elements of $\mathcal{O}_D$, this implies that $N(\alpha)$ is an integer dividing 1, so $N(\alpha) \in \{\pm 1\}$, as desired.
($\Longleftarrow$) Assume $N(\alpha) \in \{\pm 1\}$ for $\alpha \in \mathcal{O}_D$, and write $\alpha = a + b\omega \in \mathbb{Z}[\omega]$. Then

$$N(\alpha) = N(a + b\omega) = (a + b\omega)(a + b\overline{\omega}) \in \{\pm 1\}.$$

If $N(\alpha) = 1$, then $(a + b\omega)(a + b\overline{\omega}) = 1$, so $\alpha^{-1} = a + b\overline{\omega}$. So $\alpha \in \mathcal{O}_D^\times$ by definition.
On the other hand, if $N(\alpha) = -1$, then $\alpha^{-1} = -(a + b\overline{\omega})$, and $\alpha \in \mathcal{O}_D^\times$. □

This characterization of the units in $\mathcal{O}_D$ as the elements of norm ± 1 is very useful.

Example 2.14. By Proposition 2.13 the units in $\mathbb{Z}[i]$ are the elements $a + bi \in \mathbb{Z}[i]$ such that

$$N(a + bi) = a^2 + b^2 \in \{\pm 1\}.$$

Since $a^2 + b^2 \geqslant 0$, to determine the units in $\mathbb{Z}[i]$ it suffices to find all integers $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = 1$. But these are exactly

$$(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\},$$

which correspond to

$$a + bi \in \{1, -1, i, -i\}.$$

So $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Another way of seeing this is that in the complex plane, the units in the Gaussian integers are the points (a, b) with integer coordinates that lie on the unit circle $a^2 + b^2 = 1$, i.e., those that have complex absolute value 1.

In general, the following theorem from algebraic number theory tells us how many units we expect to find in $\mathcal{O}_D$.

Theorem 2.15 (Dirichlet's unit theorem)**.** *Let $\mathcal{O}_D$ be the ring of integers of a quadratic field $\mathbb{Q}(\sqrt{D})$. Then $\mathcal{O}_D^\times$ is finitely generated as an abelian group. In particular,*

(a) If $D < 0$, then $\mathcal{O}_D^\times$ has rank zero as a finitely generated abelian group. That is, $\mathcal{O}_D^\times$ is finite.

(b) If $D > 0$, then $\mathcal{O}_D^\times$ has rank one as a finitely generated abelian group, and for all $\alpha \in \mathcal{O}_D^\times$,

$$\alpha = \pm\varepsilon^n$$

*where $\varepsilon \in \mathcal{O}_D^\times$ is a **fundamental unit** and $n \in \mathbb{Z}$. That is, $\mathcal{O}_D^\times$ is infinite.*

Example 2.16. Recall the Eisenstein integers $\mathcal{O}_{-3} \subset \mathbb{Q}(\sqrt{-3})$, which are also contained in an imaginary quadratic field. Then, to find α such that $\alpha \in \mathcal{O}_{-3}^\times$, we need to find α such that $N(\alpha) = |\alpha|^2 = 1$. Since the complex absolute value is nononegative, it suffices to consider α with $|\alpha| = 1$. By Theorem 2.15, there are only finitely many such α.
Exercise (related to Problem Set #5 5(a)): Find all of the units in $\mathcal{O}_{-3}$. This can be done algebraically by letting $\alpha = a + b\frac{1+\sqrt{-3}}{2}$ and finding all integer solutions to

$$N(\alpha) = a^2 + ab + b^2 = \pm 1.$$

For a geometric perspective, consider elements $\alpha \in \mathcal{O}_{-3}$ as complex numbers and plot them in the complex plane. They should form a triangular lattice. Which ones are on the unit circle (have complex absolute value 1)?

Example 2.17. Let $\mathcal{O}_2 \subset \mathbb{Q}(\sqrt{2})$, then since $2 > 0$ by Theorem 2.15 we expect $\mathcal{O}_2^\times$ to be infinite.
Observe that $1+\sqrt{2} \in \mathcal{O}_2$ has norm -1, so $\varepsilon := 1+\sqrt{2} \in \mathcal{O}_2^\times$ and

$$\varepsilon^{-1} = (1+\sqrt{2})^{-1} = -1+\sqrt{2} \in \mathcal{O}_2^\times.$$

Further, $N(-\varepsilon) = N(-1-\sqrt{2}) = -1$ and $N(-\varepsilon^{-1}) = N(1-\sqrt{2}) = -1$. So

$$\{\pm\varepsilon, \pm\varepsilon^{-1}\} \subset \mathcal{O}_2^\times.$$

Moreover, since the norm is multiplicative,

$$N(\varepsilon^a) = N(\varepsilon)^a = (-1)^a \in \{\pm 1\}$$

and

$$N((\varepsilon^{-1})^a) = N(\varepsilon^{-1})^a = (-1)^a \in \{\pm 1\}$$

for all $a \in \mathbb{Z}_{>0}$. Further, $\varepsilon^0 = 1$ and $-\varepsilon^0 = -1$ both clearly have norm 1, and

$$N(-\varepsilon^n) = N(-1)N(\varepsilon^n) = N(\varepsilon^n)$$

for all $n \in \mathbb{Z}$. So altogether, we have shown that

$$\{\pm(1+\sqrt{2})^n : n \in \mathbb{Z}\}$$

is an infinite set of units in $\mathcal{O}_2$. By Theorem 2.15, these are all of them.

2.4 Diophantine Equations

Quadratic integers are used in the study of Diophantine equations in number theory.

Definition 2.18. A **Diophantine equation** is an equation in two or more variables (usually polynomial or exponential) with integer coefficients and integer unknowns.

Example 2.19. The **Pythagorean equation**

$$x^2 + y^2 = z^2$$

is a Diophantine equation whose solutions are Pythagorean triples such as $(3,4,5)$ and $(5,12,13)$. In fact, this equation has infinitely many integer solutions! Assume that z is nonzero (otherwise we would just have the trivial solution), divide both sides by z^2, so that

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = \left(\frac{x}{z} + \frac{y}{z}i\right)\left(\frac{x}{z} - \frac{y}{z}i\right) = 1.$$

Now we can find solutions to the Pythagorean equation by finding elements of $\mathbb{Q}(i)$ with norm 1. On the complex plane, this is equivalent to finding rational points on the unit circle. From these rational points, one can then use stereographic projection to derive Euclid's formula for solutions to the Pythagorean equation.
On the other hand, the Diophantine equation

$$x^n + y^n = z^n$$

for $n \geqslant 3$ has been shown to have no solutions in the positive integers. This is the content of **Fermat's Last Theorem**.

Example 2.20. The Diophantine equation

$$x^2 - Dy^2 = 1,$$

where $x, y \in \mathbb{Z}$ and $D > 0$ is a squarefree integer, is called **Pell's equation**. Notice that if (x, y) is a solution to Pell's equation, then since

$$x^2 - Dy^2 = (x + y\sqrt{D})(x - y\sqrt{D}) = 1,$$

the integral point (x, y) corresponds to a unit $x + y\sqrt{D} \in \mathcal{O}_D^\times$. More specifically, solutions to Pell's equation correspond to units with norm 1. Further, Theorem 2.15 implies that solutions to Pell's equation are of the form $\pm\varepsilon^n$ for some $\varepsilon \in \mathcal{O}_D^\times$ and $n \in \mathbb{Z}$.
For example, let $D = 2$, then from Example 2.17 we know that all solutions to Pell's equation are of the form $\pm(1+\sqrt{2})^n$ for $n \in \mathbb{Z}$. We calculated that $N(1+\sqrt{2}) = -1 \neq 1$, so $(1, 1)$ is not a solution to Pell's equation. However,

$$N(3 + 2\sqrt{2}) = N((1 + \sqrt{2})^2) = N(1 + \sqrt{2})^2 = (-1)^2 = 1,$$

so $(3, 2)$ is a solution. Similarly, one can show that any element of the form $\pm(1+\sqrt{2})^{2n} \in \mathcal{O}_2^\times$, $n \in \mathbb{Z}$ has norm 1 and is therefore a solution. Thus, we have found infinitely many solutions to Pell's equation using the theory of units in a quadratic integer ring!

2.5 Quadratic Integer Rings that are PIDs

For which integers D is $\mathcal{O}_D$ a principal ideal domain? This question has not been completely answered in general! However, for imaginary quadratic fields the question is resolved.

Theorem 2.21 (Baker-Heegner-Stark)**.** *Let $\mathcal{O}_D$ be the ring of integers of a quadratic field $\mathbb{Q}(\sqrt{D})$ with $D < 0$. Then $\mathcal{O}_D$ is a principal ideal domain if and only if*

$$D \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

We know of many examples of real quadratic fields that are PIDs, and we will see examples in Section 3. It is expected that there are infinitely many, but it has not been proven!

Conjecture 2.22 (Gauss)**.** *There are infinitely many quadratic fields $\mathbb{Q}(\sqrt{D})$ with $D > 0$ such that $\mathcal{O}_D$ is a principal ideal domain.*

Computational evidence suggests that out of all real quadratic fields of the form $\mathbb{Q}(\sqrt{p})$, where p is a prime, just over $3/4$ of them are PIDs.

3 Euclidean Domains

3.1 Introduction

We define yet another class of commutative rings.

Definition 3.1. A **Euclidean domain (ED)** is an integral domain with a **Euclidean norm**; that is, with a map $N : R \to \mathbb{Z}_{\geqslant 0}$ such that $N(0) = 0$ and for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that

$$a = qb + r,$$

where either $r = 0$ or $N(r) < N(b)$. We call q and r the **quotient** and **remainder**, respectively.

Example 3.2.

1. Any field F is a Euclidean domain with the zero norm $N : F \to \{0\}$. For any $a, b \in F$ with $b \neq 0$, we have $a = qb + r$ with $q := a/b$ and $r = 0$.
2. The ring $\mathbb{Z}$ is a Euclidean domain with norm given by the absolute value.
3. The ring $F[x]$ of polynomials with coefficients in a field F is a Euclidean domain with norm $N : F[x] \to \mathbb{Z}_{\geqslant 0}$ given by the degree map $f(x) \mapsto \deg(f(x))$.

One might ask how Euclidean domains are related to principal ideal domains.

Theorem 3.3. *Let R be a ring. If R is a Euclidean domain, then R is a principal ideal domain.*

Proof. Let R be a Euclidean domain, and let $I \subset R$ be an ideal.
If $I = (0)$ is the zero ideal, then I is generated by 0 and therefore principal.
Else, if $I \neq (0)$, then there exists a nonzero element $d \in I$ such that $N(d) \leqslant N(a)$ for all $a \in I$, where $N : R \to \mathbb{Z}_{\geqslant 0}$ is the Euclidean norm. In other words, there exists a nonzero element of minimal norm in I. Then the (d) is contained in I. We claim that $I \subset (d)$.
Let $a \in I$ be arbitrary. Then since R is a Euclidean domain, there exist $q, r \in R$ such that $a = qd + r$ with $r = 0$ or $N(r) < N(d)$. Since $r = a - qd$ and $a, d \in I$, we have that $r \in I$, so if $N(r) < N(d)$ then this contradicts our assumption that d is of minimal norm in I. Thus, $r = 0$, so $a = qd$ and $a \in (d)$. Since $a \in I$ was taken arbitrarily, we conclude that $I \subset (d)$.
So we have shown that $I = (d)$ is principal. Since $I \subset R$ was chosen arbitrarily, R is a principal ideal domain, as desired. □

Is the converse to Theorem 3.3 true? We will answer this in Section 3.2.

3.2 Quadratic Integer Rings that are EDs

Notice that in order for $\mathcal{O}_D \subset \mathbb{Q}(\sqrt{D})$ to be a Euclidean domain, we must define a Euclidean norm that is nonnegative. In general, the field norm on $\mathbb{Q}(\sqrt{D})$ and its restriction to $\mathcal{O}_D$ are not necessarily nonnegative. This leads us to consider the absolute value of the field norm.

Definition 3.4. The quadratic integer ring $\mathcal{O}_D \subset \mathbb{Q}(\sqrt{D})$ is **norm-Euclidean** if it is a Euclidean domain with Euclidean norm given by

$$\alpha \mapsto |N(\alpha)|,$$

where $\alpha \in \mathcal{O}_D$ and $N : \mathcal{O}_D \to \mathbb{Z}$ is the restriction of the field norm to $\mathcal{O}_D$.

The question of which quadratic integer rings are norm-Euclidean has been solved completely, and more is true for the imaginary quadratic field case.

Theorem 3.5. *Let $\mathcal{O}_D$ be the ring of integers of a quadratic field $\mathbb{Q}(\sqrt{D})$.*

(a) If $D < 0$, then $\mathcal{O}_D$ is norm-Euclidean if and only if

$$D \in \{-1, -2, -3, -7, -11\}.$$

Further, $\mathcal{O}_D$ is a Euclidean domain if and only if it is norm-Euclidean.

(b) If $D > 0$, then $\mathcal{O}_D$ is norm-Euclidean if and only if

$$D \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Example 3.6. By Theorem 2.21 and Theorem 3.5, $\mathcal{O}_{-19} = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}] \subset \mathbb{Q}(\sqrt{-19})$ is an example of a principal ideal domain that is not a Euclidean domain.

After reading Theorem 3.5, one might ask whether there exist quadratic integer rings $\mathcal{O}_D$ with $D > 0$ that are Euclidean domains with respect to some other norm. The answer is yes!

Theorem 3.7 (Clark, 1994). *The quadratic integer ring $\mathcal{O}_{69} = \mathbb{Z}[\frac{1+\sqrt{69}}{2}]$ is a Euclidean domain that is not norm-Euclidean.*

In fact, we have the following theorem.

Theorem 3.8 (Weinberger, 1973). *Let $\mathcal{O}_D$ be the ring of integers of a quadratic field $\mathbb{Q}(\sqrt{D})$ with $D > 0$. Assuming the generalized Riemann hypothesis, $\mathcal{O}_D$ is a Euclidean domain if and only if it is a principal ideal domain.*

So, if you believe Conjecture 2.22 and the generalized Riemann hypothesis, then we expect that there are infinitely many real quadratic fields such that $\mathcal{O}_D$ is a Euclidean domain.
We can now add Euclidean domains to our inclusion diagram of classes of commutative rings with identity:

$$\{\text{fields}\} \subset \{\text{Euclidean domains}\} \subset \{\text{principal ideal domains}\} \subset \{\text{integral domains}\}.$$

We have $\mathbb{Z}$ as an example of a Euclidean domain that is not a field, $\mathcal{O}_{-19}$ as a principal ideal domain that is not a Euclidean domain, and $\mathbb{Z}[x]$ as an integral domain that is not a principal ideal domain.

4 Irreducible and Prime Elements

We often think about prime integers as numbers that cannot factor any further: the only possible integer factors of a prime number $p \in \mathbb{Z}$ are ± 1 and $\pm p$. How do we reconcile this definition with the definition of a prime ideal?

Definition 4.1. Let R be an integral domain. A nonzero nonunit element $r \in R$ is **irreducible** if $r = ab$ for $a, b \in R$ implies that either $a \in R^\times$ or $b \in R^\times$. An element that is not irreducible is called **reducible**.

Definition 4.2. Let R be an integral domain. An nonzero element $p \in R$ is **prime** if $(p) \subset R$ is a prime ideal.

In general, prime elements are always irreducible.

Proposition 4.3. *Let R be an integral domain. Then if $p \in R$ is prime then p is irreducible.*

Proof. Assume that $p \in R$ is prime and that $p = ab$ for some $a, b \in R$. Then since (p) is a prime ideal, either $a \in (p)$ or $b \in (p)$.
If $a \in (p)$, then $a = pr$ for some $r \in R$. So $p = ab = (pr)b$, and since R is an integral domain we can conclude by the cancellation law that $1 = rb$. Then $b \in R^\times$ by definition.
If $b \in (p)$, then by a similar argument we conclude that $a \in R^\times$. So by definition, p is irreducible. □

Thankfully, in a principal ideal domain such as $\mathbb{Z}$, these two definitions coincide. So our earlier definition of prime numbers as irreducible lines up with the notion of a prime ideal, at least in this case.

Proposition 4.4. *Let R be a principal ideal domain. Then $p \in R$ is prime if and only if p is irreducible.*

Proof. ($\Longrightarrow$) Apply Proposition 4.3.
($\Longleftarrow$) Let $p \in R$ be irreducible and consider the ideal $(p) \subset R$. Any proper ideal in R is contained in some maximal ideal $M \subset R$, so $(p) \subset M$. Further, since R is a principal ideal domain we have $M = (m)$ for some nonzero $m \in R$. So $p \in (m)$ implies that $p = mr$ for some $r \in R$. But since p is irreducible, either $m \in R^\times$ or $r \in R^\times$. In the first case, M contains a unit, so $M = R$, contradicting the assumption that M is a maximal ideal. Thus, we must have $r \in R^\times$. But then $pr^{-1} = m$, so that $m \in (p)$ and therefore $(m) \subset (p)$. We conclude that $(p) = (m)$ is a maximal ideal. In particular, (p) is prime, so p is prime, as desired. □

Proposition 4.4 implies that one can prove that a ring R is not a PID by exhibiting an irreducible element $r \in R$ that is not prime.

Example 4.5. Consider $\mathcal{O}_{-5} = \mathbb{Z}[\sqrt{-5}]$. Theorem 2.21 asserts that $\mathcal{O}_{-5}$ is not a PID, and we can prove this by showing that $3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible but not prime.
First we claim that 3 is irreducible. Assume that

$$3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$$

for some $a, b, c, d \in \mathbb{Z}$. Then applying the field norm to both sides, we get

$$N(3) = 9 = (a^2 + 5b^2)(c^2 + 5d^2) = N(a + b\sqrt{-5})N(c + d\sqrt{-5}).$$

Since the norm is integer-valued on $\mathbb{Z}[\sqrt{-5}]$, we know that $a^2 + 5b^2$ and $c^2 + 5d^2$ are integers that divide 9. In particular, they must be positive. We divide into cases.
If $a^2 + 5b^2 = 1$, then $a + b\sqrt{-5} \in \mathcal{O}_{-5}^{\times}$.
If $a^2 + 5b^2 = 3$, then $b = 0$ since otherwise $a^2 + 5b^2 \geqslant 5 > 3$. But there is no integer a such that $a^2 = 3$. So this case is impossible.
Finally, if $a^2 + 5b^2 = 9$, then $c^2 + 5d^2 = 1$ and therefore $c + d\sqrt{-5} \in \mathcal{O}_{-5}^{\times}$.
We conclude that 3 is irreducible in $\mathbb{Q}[\sqrt{-5}]$ by definition.
However, we claim that 3 is not prime. Consider the ideal $(3) \subset \mathcal{O}_{-5}$, then $3 \mid 9$ so $9 \in (3)$. But

$$9 = (2 + \sqrt{-5})(2 - \sqrt{-5}),$$

where $3 \nmid 2 + \sqrt{-5}$ and $3 \nmid 2 - \sqrt{-5}$. So (3) is not prime, and therefore 3 is not prime in $\mathcal{O}_{-5}$.

Index