Chapter 13

Quadratic fields and quadratic number rings

12.1 Quadratic number fields

Definition 12.1. *A quadratic number field is a number field of degree 2.*

The integer $d \in \mathbb{Z}$ is said to be *square-free* if it has no square factor, ie

$$a^2 \mid d \implies a = \pm 1.$$

Thus the square-free integers are

$$\pm 1, \pm 2, \pm 3, \pm 5, \ldots.$$

Proposition 12.1. *Suppose $d \neq 1$ is square-free. Then the numbers*

$$x + y\sqrt{d} \quad (x, y \in \mathbb{Q})$$

form a quadratic number field $\mathbb{Q}(\sqrt{d}$.

Moreover, every quadratic number field is of this form; and different square-free integers $d, d' \neq 1$ give rise to different quadratic number fields.

Proof. Recall the classic proof that $\sqrt{d}$ is irrational;

$$\sqrt{d} = \frac{m}{n} \implies n^2 d = m^2,$$

and if any prime factor $p \mid d$ divides the left hand side to an odd power, and the right to an even power.

It is trivial to see that the numbers $x + y\sqrt{d}$ form a commutative ring, while

$$\begin{aligned} \frac{1}{x + y\sqrt{d}} &= \frac{x - y\sqrt{d}}{(x - y\sqrt{d})(x + y\sqrt{d})} \\ &= \frac{x - y\sqrt{d}}{x^2 - dy^2}, \end{aligned}$$

where $x^2 - dy^2 \neq 0$ since $\sqrt{d} \notin \mathbb{Q}$.

It follows that these numbers form a field; and the degree of the field is 2 since $1, \sqrt{d}$ form a basis for the vector space.

Conversely, suppose F is a quadratic number field. Let $1, \theta$ be a basis for the vector space. Then $1, \theta, \theta^2$ are linearly independent, ie θ satisfies a quadratic equation

$$a\theta^2 + b\theta + c = 0 \quad (a, b, c \in \mathbb{Q}).$$

Since F is of degree 2, $a \neq 0$, and we can take $a = 1$. Thus

$$\theta = \frac{-b \pm \sqrt{D}}{2},$$

with $D = b^2 - 4c$.

Now

$$D = a^2 d,$$

where d is a square-free integer (with $a \in \mathbb{Q}$). It follows easily that

$$F = \mathbb{Q}(\sqrt{d}).$$

Finally if $d \neq d'$ then $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(\sqrt{d'})$. For otherwise

$$\sqrt{d'} = x + y\sqrt{d}$$

for some $x, y \in \mathbb{Q}$; and so, on squaring,

$$d'^2 = x^2 + dy^2 + 2xy\sqrt{d}.$$

But this implies that $\sqrt{d} \in \mathbb{Q}$ if $xy \neq 0$; while $y = 0 \implies \sqrt{d} = x \in \mathbb{Q}$, and

$$x = 0 \implies d' = dy^2,$$

which is easily seen to be incompatible with d, d' being square-free. □

12.2 Conjugacy

We suppose in the rest of the Chapter that we are working in a specific quadratic number field $\mathbb{Q}(\sqrt{d})$.

Definition 12.2. *We define the* conjugate *of*

$$z = x + y\sqrt{d}$$

to be

$$\bar{z} = x - y\sqrt{d}$$

If $d < 0$ then this coincides with the complex conjugate; but if $d > 0$ then both z and $\bar{z}$ are real; and

$$z = \bar{z} \iff z \in \mathbb{Q}.$$

Proposition 12.2. *The map*

$$z \mapsto \bar{z} : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$$

is an automorphism of $\mathbb{Q}(\sqrt{d})$*. In fact it is the only such automorphism apart from the trivial map* $z \mapsto z$*.*

The proof is identical to that we gave for gaussian numbers.

Definition 12.3. *The* norm *of* $z = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ *is*

$$\mathcal{N}(z) = z\bar{z} = x^2 - dy^2.$$

Proposition 12.3. *1.* $\mathcal{N}(z) \in \mathbb{Q}$*;*

2. $\mathcal{N}(z) = 0 \iff z = 0$*;*

3. $\mathcal{N}(zw) = \mathcal{N}(z)\mathcal{N}(w)$*;*

4. If $a \in \mathbb{Q}$ *then* $\mathcal{N}(a) = a^2$*;*

Again, the proof is identical to that we gave for the corresponding result for gaussian numbers.

12.3 Quadratic number rings

We want to determine the number ring

$$A = \mathbb{Q}(\sqrt{d}) \cap \bar{\mathbb{Z}}$$

associated to the number field $\mathbb{Q}(\sqrt{d})$, ie we want to find which numbers $x + y\sqrt{d}$ are algebraic integers.

Theorem 12.1. *Suppose*

$$z = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d}).$$

Then

1. *If* $d \not\equiv 1 \bmod 4$
$$z \in \bar{\mathbb{Z}} \iff z = m + n\sqrt{d},$$
where $m, n \in \mathbb{Z}$*.*

2. *If* $d \equiv 1 \bmod 4$ *then*
$$z \in \bar{\mathbb{Z}} \iff z = \frac{m + n\sqrt{d}}{2},$$
where $m, n \in \mathbb{Z}$ *and* $m \equiv n \bmod 2$*.*

Proof. If
$$z = x + y\sqrt{d} \in \bar{\mathbb{Z}}$$
then
$$\bar{z} = x \in y\sqrt{d} \in \bar{\mathbb{Z}}$$
since z and $\bar{z}$ satisfy the same polynomials over $\mathbb{Q}$. Hence
$$z + \bar{z} = 2x \in \bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}.$$

Also
$$\mathcal{N}(z) = z\bar{z} = x^2 - dy^2 \in \mathbb{Z}.$$
It follows that
$$4dy^2 = d(2y)^2 \in \mathbb{Z} \implies 2y \in \mathbb{Z}$$
since d is square-free. (For suppose $2y = m/n$, where $\gcd(m, n) = 1$. Then $dm^2/n^2 \in \mathbb{Z}$. If the prime $p \mid n$ then
$$p^2 \mid dm^2 \implies p^2 \mid d,$$
which is impossible since d is square-free.)

Thus
$$z = \frac{m + n\sqrt{d}}{2},$$
where $m, n \in \mathbb{Z}$. Now
$$\mathcal{N}(z) = \frac{m^2 - dn^2}{4} \in \mathbb{Z},$$
ie
$$m^2 \equiv dn^2 \bmod 4.$$

If n is even then so is m; and if m is even then so is n, since $4 \nmid d$. On the other hand if m, n are both odd then
$$m^2 \equiv n^2 \equiv 1 \bmod 4.$$
It follows that
$$d \equiv 1 \bmod 4.$$

In other words, if $d \not\equiv 1 \bmod 4$ then m, n are even, and so
$$z = a + b\sqrt{d},$$
with $a, b \in \mathbb{Z}$.

On the other hand, if $d \equiv 1 \bmod 4$ then m, n are both even or both odd.

It only remains to show that if $d \equiv 1 \bmod 4$ and m, n are both odd then
$$z = \frac{m + n\sqrt{d}}{2} \in \bar{\mathbb{Z}},$$

It is sufficient to show that

$$\theta = \frac{1+\sqrt{d}}{2} \in \bar{\mathbb{Z}},$$

since

$$z = (a + b\sqrt{d}) + \theta,$$

where

$$a = (m-1)/2,\ b = (n-1)/2 \in \mathbb{Z}.$$

But

$$(\theta - 1/2)^2 = d/4,$$

ie

$$\theta^2 - \theta + (1-d)/4.$$

But $(1-d)/4 \in \mathbb{Z}$ if $d \equiv 1 \bmod 4$. Hence

$$\theta \in \bar{\mathbb{Z}}.$$

□

12.4 Units I: Imaginary quadratic fields

Suppose F is a number field, with associated number ring A (the algebraic integers in F). By 'abuse of language', as the French say, we shall speak of the units of F when we are really referring to the units in A.

Proposition 12.4. *Suppose $z \in \mathbb{Q}(\sqrt{d})$ is an algebraic integer. Then*

$$z \textit{ is a unit } \iff \mathcal{N}(z) = \pm 1.$$

Proof. Suppose z is a unit, say

$$zw = 1,$$

where w is also an integer. Then

$$\mathcal{N}(zw) = \mathcal{N}(z)\mathcal{N}(w) = \mathcal{N}(1) = 1^2 = 1.$$

Since $\mathcal{N}(z), \mathcal{N}(w) \in \mathbb{Z}$ it follows that

$$\mathcal{N}(z) = \mathcal{N}(w) = \pm 1.$$

On the other hand, if

$$\mathcal{N}(z) = z\bar{z} = \pm 1$$

then

$$z^{-1} = \pm\bar{z} \in \bar{\mathbb{Z}}.$$

□

Theorem 12.2. *Suppose d is square-free and $d < 0$. Then the group of units is finite. More precisely,*

1. *If $d = -1$ there are 4 units: $\pm 1, \pm i$;*
2. *if $d = -3$ there are 6 units: $\pm 1, \pm\omega, \pm\omega^2$, where $\omega = (1+\sqrt{-3})/2$;*
3. *in all other cases, there are just 2 units: ± 1.*

Proof. Suppose ϵ is a unit.

If $d \not\equiv 1 \bmod 4$ then

$$\epsilon = m + n\sqrt{d} \quad (m, n \in \mathbb{Z}).$$

Thus

$$\mathcal{N}(\epsilon) = m^2 + dn^2 = 1,$$

If $d < -1$ then it follows that $m = \pm 1,\ n = 0$. If $d = -1$ then there are the additional solutions $m = 0,\ n = \pm 1$, as we know.

If $d \equiv 1 \bmod 4$ then

$$\epsilon = \frac{m + n\sqrt{d}}{2},$$

where $m, n \in \mathbb{Z}$ with $m \equiv n \bmod 2$. In this case,

$$\mathcal{N}(\epsilon) = \frac{m^2 - dn^2}{4} = 1,$$

ie

$$m^2 - dn^2 = 4.$$

If $d \leq -7$ then this implies that $m = \pm 1,\ n = 0$. This only leaves the case $d = -3$, where

$$m^2 + 3n^2 = 4.$$

This has 6 solutions: $m = \pm 2,\ n = 0$, giving $\epsilon = \pm 1$; and $m = \pm 1,\ n = \pm 1$, giving $\epsilon = \pm\omega, \pm\omega^2$. □

Units in real quadratic fields (where $d > 0$) have a very different character, requiring a completely new idea from the theory of *diophantine approximation*; we leave this to another Chapter.