Quadratic fields

Qiangru Kuang

Let $d \in \mathbb{Z}$ be square-free and $d \neq 0, 1$. Then

$$L = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[x]/(x^2 - d)$$

is a degree 2 extension over $\mathbb{Q}$. It is called a quadratic field. If $d > 0$ then there are two real embeddings, in which case we call $L$ a real quadratic field. Otherwise $L$ is an imaginary quadratic field. Note that in using this notation, we implicitly assume that there is a complex embedding $\sigma : L \to \mathbb{C}$.

**Ring of integers** A particularly nice characterisation of algebraic integers in a quadratic field is $\alpha \in \mathcal{O}_L$ if and only if $N_{L/\mathbb{Q}}(\alpha), \text{tr}_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Suppose $\alpha = \frac{u}{2} + \frac{v}{2}\sqrt{d} \in \mathcal{O}_L$ where $u, v \in \mathbb{Q}$. Then multiplication by $\alpha$ has with respect to the basis $\{1, \sqrt{d}\}$ matrix representation

$$\begin{pmatrix} 1 & v \\ \frac{u}{2} & u \end{pmatrix}$$

so

$$N_{L/\mathbb{Q}}(\alpha) = \frac{1}{4}(u^2 - v^2 d) \in \mathbb{Z}$$

$$\text{tr}_{L/\mathbb{Q}}(\alpha) = u \in \mathbb{Z}$$

so $v^2 d \in \mathbb{Z}$. Suppose $v = \frac{r}{s}$ is an expression in coprime integers. Then $d^2 r^2 \in s^2 \mathbb{Z}$ so $s^2 \mid d^2 r^2$. If $p$ is a prime dividing $s$ then $p^2 \mid d^2$. As $d$ is square-free, $p \mid d$. Absurd. Thus $v \in \mathbb{Z}$ and

$$\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_L \subseteq \mathbb{Z} + \mathbb{Z}[\sqrt{d}]$$.

- If $d = 2, 3 \pmod{4}$ then $u^2 = 0, 1 \pmod{4}, v^2 = 0, 1 \pmod{4}$. As $u^2 = v^2 d \pmod{4}$, $u, v \in 2\mathbb{Z}$ so $\alpha \in \mathbb{Z}[\sqrt{d}]$. Thus $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$.  

- If $d = 1 \pmod{4}$ then $u^2 = v^2 \pmod{4}$ so $u = v \pmod{2}$. Thus

$$\mathcal{O}_L \subseteq \left\{ \frac{u}{2} + \frac{v}{2}\sqrt{d} : u = v \pmod{2} \right\} = \mathbb{Z} \oplus \mathbb{Z} \frac{1 + \sqrt{d}}{2}.$$  

Now check that $\frac{1 + \sqrt{d}}{2} \in \mathcal{O}_L$ so we conclude that $\mathcal{O}_L = \mathbb{Z}[\frac{1 + \sqrt{d}}{2}]$. 

1
**Discriminant**  Recall that

\[ D_L = \det(\sigma_i(\alpha_j))^2 = \det(\text{tr}_{L/Q}(\alpha_i\alpha_j)) = (-1)^{(\frac{d}{2})}N_{L/Q}(f'(\alpha)) \]

where \( \{\alpha_i\} \) is an integral basis, \( \{\sigma_i\} \) are the complex embeddings, \( \alpha \) is a generator of \( \mathcal{O}_L \) as a \( \mathbb{Z} \)-algebra and \( f \) is the minimal polynomial whereof.

- If \( d = 2, 3 \pmod{4} \) then \( \alpha = \sqrt{d}, f(x) = x^2 - d \). Thus
  \[ D_L = -N_{L/Q}(2\sqrt{d}) = 4d. \]
  Alternatively, since \( \text{tr}_{L/Q}(1) = 2, \text{tr}_{L/Q}(\sqrt{d}) = 0 \), we can easily compute the matrix \( \text{tr}_{L/Q}(\alpha_i\alpha_j) \).

- If \( d = 1 \pmod{8} \) then \( \alpha = \frac{1+\sqrt{d}}{2} \), \( f(x) = x^2 + x + \frac{1-d}{4} \). Thus
  \[ D_L = -N_{L/Q}(\sqrt{d}) = d. \]

**Factorisation of ideals**  Recall that Dedekind’s criterion says that subject to certain divisibility condition, given \( L = \mathbb{Q}(\alpha) \) and \( \alpha \in \mathcal{O}_L \) with minimal polynomial \( f(x) \) and \( p \) prime, if

\[ \overline{f}(t) = \prod_{i=1}^{r} \overline{g}_i(t)^{e_i} \in \mathbb{F}_p[x] \]

is a factorisation into irreducibles then

\( (p) = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \)

is a factorisation into prime ideals.

- If \( p = 2 \),
  - if \( d = 2, 3 \pmod{4} \) then let \( \alpha = \sqrt{d} \) so
    \[ \overline{f}(x) = x^2 - d = (x - \sqrt{d})^2 \in \mathbb{F}_2[x] \]
    so \( (2) = \mathfrak{p}^2 \), i.e. ramifies.
  - if \( d = 1 \pmod{8} \) then let \( \alpha = \frac{1+\sqrt{d}}{2} \) so
    \[ \overline{f}(x) = x^2 + x + \frac{1-d}{4} = x^2 + x = x(x+1) \in \mathbb{F}_2[x] \]
    so \( (2) = \mathfrak{p}\mathfrak{q} \), i.e. splits completely.
  - if \( d = 5 \pmod{8} \) then \( \overline{f}(x) \in \mathbb{F}_2[x] \) is irreducible so \( 2 \) is inert.

- If \( p \) is odd, let \( \alpha = \sqrt{d} \) and \( f(x) = x^2 - d \) so
  - if \( (\frac{d}{p}) = 0 \) then \( (p) = \mathfrak{p}^2 \), i.e. ramifies.
  - if \( (\frac{d}{p}) = 1 \) then \( (p) = \mathfrak{p}\mathfrak{q} \), i.e. splits completely.
  - if \( (\frac{d}{p}) = -1 \) then \( p \) is inert.
Lattice  Recall that the covolume of a lattice formed by an ideal of the ring of integers is the volume of the parallelepiped spanned by its \( \mathbb{Z} \)-basis.

Given an imaginary quadratic field \( \mathcal{L} \), claim that

\[
A(I) = \frac{1}{2} \sqrt{|\text{disc}(I)|} = \frac{N(I)}{2} \sqrt{|D_\mathcal{L}|}
\]

for \( I \subseteq \mathcal{O}_\mathcal{L} \).

Proof. Let \( \alpha_1 = x_1 + iy_1, \alpha_2 = x_2 + iy_2 \) be an integral basis for \( I \). Then

\[
A(I) = \left| \det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} \right|.
\]

Meanwhile

\[
\text{disc}(I) = \det \begin{pmatrix} x_1 + iy_1 & x_2 + iy_2 \\ x_1 - iy_1 & x_2 - iy_2 \end{pmatrix}^2 = (2i)^2 \det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}^2.
\]

By Minkowski’s theorem and multiplicativity of norm, we can deduce that for any number field \( \mathcal{L} \), the ideal class group \( \text{Cl}(\mathcal{O}_\mathcal{L}) \) is finite and can be generated by the class of prime ideals \( \mathfrak{p} \) with \( N(\mathfrak{p}) \leq c_\mathcal{L} \) where \( c_\mathcal{L} = \frac{2}{\pi} \sqrt{|D_\mathcal{L}|} \).

Example.

1. \( d = -7 \). As \( d = 1 \pmod{4} \), \( D_\mathcal{L} = -7 \). Thus

\[
c_\mathcal{L} = \frac{2}{\pi} \sqrt{7} < \frac{2}{3} \sqrt{7} < 2
\]

so \( \text{Cl}(\mathcal{O}_\mathcal{L}) \) is generated by ideals of norm \( < 2 \). There are none except \( \mathcal{O}_\mathcal{L} \). Thus \( \text{Cl}(\mathcal{O}_\mathcal{L}) \) is trivial. Hence \( \mathcal{O}_\mathcal{L} = \mathbb{Z}[\frac{1+i\sqrt{-7}}{2}] \) is a UFD.

2. \( d = -5 \), \( D_\mathcal{L} = -20 \) so

\[
c_\mathcal{L} = \frac{2}{\pi} \sqrt{20} = \frac{4}{\pi} \sqrt{5} < \frac{4}{3} \sqrt{5} < 3
\]

so \( \text{Cl}(\mathcal{O}_\mathcal{L}) \) is generated by prime ideals \( \mathfrak{p} \subseteq \mathcal{O}_\mathcal{L} \) of norm \( N(\mathfrak{p}) = 2 \). We know by Dedekind’s criterion that \( 2\mathcal{O}_\mathcal{L} = \mathfrak{p}^2 \). Thus \( \text{Cl}(\mathcal{O}_\mathcal{L}) \) is generated by \( [\mathfrak{p}] \) and \( [\mathfrak{p}]^2 = [2\mathcal{O}_\mathcal{L}] = [\mathcal{O}_\mathcal{L}] \) is the trivial class. Hence there are two possibilities:

(a) if \( \mathfrak{p} \) is principal then \( \text{Cl}(\mathcal{O}_\mathcal{L}) \) is trivial.

(b) if \( \mathfrak{p} \) is not principal then \( \text{Cl}(\mathcal{O}_\mathcal{L}) \cong \mathbb{Z}/2\mathbb{Z} \).

But we already knew that \( \mathcal{O}_\mathcal{L} \) is not a UFD so \( \text{Cl}(\mathcal{O}_\mathcal{L}) \) is not trivial so must have

\( \text{Cl}(\mathcal{O}_\mathcal{L}) \cong \mathbb{Z}/2\mathbb{Z} \).

For real quadratic fields \( \mathcal{L} = \mathbb{Q}(\sqrt{d}) \), it is instructive as an exercise to derive the baby Minkowski constant, which should be \( c_\mathcal{L} = \frac{1}{2} \sqrt{|D_\mathcal{L}|} \).
Example. \(d = 10\). Then \(c_L = \frac{1}{2}\sqrt{4 \cdot 10} < 4\). By Dedekind’s criterion,

\[
(2) = p_2^2 \\
(3) = p_3p_3'
\]

What we can do at this stage is to compute the norm of some elements. For example \(N(2 + \sqrt{10}) = 6\) so \((2 + \sqrt{10}) = p_2p_3'\) or \(p_2p_3'\). In either case, \([p_2]\)

\[
\text{generates } \text{Cl}(O_L).
\]

If \(p_2\) is principal then there exists \(a, b \in \mathbb{Z}\) such that

\[
a^2 - 10b^2 = \pm 2.
\]

Reduce modulo 5, \(\pm 2\) is not a quadratic residue so impossible. Thus \(\text{Cl}(O_L) \cong \mathbb{Z}/2\mathbb{Z}\).

**Exercise.** Find the class group of ring of integers of \(\mathbb{Q}(\sqrt{-17})\).

**Dirichlet’s unit theorem**  
Dirichlet’s unit theorem states that there is an isomorphism

\[
O_L^\times \cong \mu_L \times \mathbb{Z}^{r+s-1}
\]

where \(\mu_L\) is the group of roots of unity in \(O_L^\times\).

Thus \(O_L^\times\) is finite if and only if

1. \(r = 1, s = 0\), so \(L = \mathbb{Q}\), or
2. \(r = 0, s = 1\), so \(L = \mathbb{Q}(\sqrt{d})\) for some \(d \in \mathbb{Z}\) negative square-free.

For real quadratic fields \(L = \mathbb{Q}(\sqrt{d})\), let \(\sigma : L \to \mathbb{R}\) be the real embedding such that \(\sigma(\sqrt{d}) > 0\). As \(\sigma(\mu_L) \subseteq \mathbb{R}^\times\), must have \(\mu_L = \{\pm 1\}\). Consider the homomorphism

\[
\ell' : O_L^\times \to \mathbb{R}
\]

\[
\alpha \mapsto \log |\sigma(\alpha)|
\]

As \(\ell'(O_L^\times) \subseteq \mathbb{R}\) is a lattice, there is a unique element \(\alpha \in O_L^\times\) such that \(\sigma(\alpha) > 0\), \(\ell'(\alpha)\) generates the lattice. Then

\[
O_L^\times = \{\pm \alpha^n : n \in \mathbb{Z}\}.
\]

This \(\alpha\) is called the fundamental unit. It has the property that \(\log |\sigma(\alpha)|\) is minimal, i.e. \(\sigma(\alpha) > 1\) is minimal. This gives us a way to find fundamental units.

**Lemma 0.1.** Suppose \(d = 2, 3 \mod 4\), \(v \in O_L^\times\) and \(v > 1\). Then \(v = a + b\sqrt{d}\) where \(a \geq b \geq 1\).  

**Proof.** Let \(v' = a - b\sqrt{d}\). Then

\[
v v' = a^2 - db^2 = \pm 1.
\]

As \(v > 1\), \(|v'| < 1\) so

\[
2a = v + v' > 0
\]

\[
2b = v - v' > 0
\]

Also

\[
\left(\frac{a}{b}\right)^2 = d \pm \frac{1}{b^2} > 1.
\]

\(\square\)
There is an entirely analogous result for \( d = 1 \) \((\mod 4)\) which is left as an exercise.

Now suppose \( d = 2, 3 \) \((\mod 4)\). Suppose \( u = a + b\sqrt{d} \in \mathcal{O}_L^\times \) is the fundamental unit. Let \( u^k = a_k + b_k\sqrt{d} \). Then

\[
u^{k+1} = u \cdot u^k = (a_1 + b_1\sqrt{d})(a_k + b_k\sqrt{d}) = (a_1a_k + db_1b_k) + (b_1a_k + a_1b_k)\sqrt{d}
\]

so

\[
b_{k+1} = b_1a_k + a_1b_k \geq 2b_k > b_k
\]

so \((b_k)_{k \in \mathbb{N}}\) is strictly increasing. We can therefore characterise \( u \) as follow: let \( b \in \mathbb{N} \) be the least positive integer such that \( db^2 + 1 \) or \( db^2 - 1 \) is of the form \( a^2 \) for some \( a \in \mathbb{N} \). Then \( u = a + b\sqrt{d} \) is the fundamental unit.

If instead \( d = 1 \) \((\mod 4)\), we get

\[
b_{k+1} = \frac{1}{2}(b_1a_k + a_1b_k) \geq b_k
\]

with equality if and only if \( a_1 = b_1 = 1, a_k = b_k \). In this case

\[
N(u) = \left|\frac{1 - d}{4}\right| = 1
\]

so \( d = 5 \). In this case \( u = \frac{1}{2}(1 + \sqrt{5}) \) is the fundamental unit.

If instead \( d > 5 \), we proceed as before and characterise \( u \) as follow: let \( b \in \mathbb{N} \) be the least positive integer such that \( db^2 + 4 \) or \( db^2 - 4 \) is of the form \( a^2 \) for some \( a \in \mathbb{N} \). Then \( u = \frac{1}{2}(a + b\sqrt{d}) \) is the fundamental unit.

**Example.**

1. \( d = 2 \). Then \( b = 1 \) works since \( 2 - 1 = 1^2 \) so \( 1 + \sqrt{2} \) is a fundamental unit.

2. \( d = 7 \).

\[
\begin{align*}
b &= 1 : 7 \pm 1 \text{ not a square} \\
b &= 2 : 4 \cdot 7 \pm 1 \text{ not a square} \\
b &= 3 : 9 \cdot 7 + 1 = 8^2
\end{align*}
\]

so \( 8 + 3\sqrt{7} \) is a fundamental unit.