# Lecture 4: Imaginary Quadratic Fields

*Lecturer: Jean-François Biasse* *TA: R. Erukulangara and W. Youmans*



## 4.1 Quadratic number fields

An integer $\Delta$ is a quadratic discriminant if it is not a perfect integral square and $\Delta \equiv 0, 1 \bmod 4$. The quadratic order of discriminant $\Delta$ is defined as the $\mathbb{Z}$-module

$$\mathcal{O}_\Delta = \left[\mathbb{Z} + \frac{\Delta + \sqrt{\Delta}}{2}\mathbb{Z}\right].$$

If $\Delta < 0$, we call $\mathcal{O}_\Delta$ an imaginary quadratic order and if $\Delta > 0$ we call it as real quadratic order. A quadratic order $\mathcal{O}_\Delta$ is called a maximal order if it is not contained in a larger quadratic order. The discriminant of a maximal order is called fundamental discriminant. Let $\Delta$ be a fundamental discriminant. Then, the quadratic field of discriminant $\Delta$ is defined as the $\mathbb{Q}$-module $\mathbb{Q}(\sqrt{\Delta}) = [\mathbb{Q} + \sqrt{\Delta}\mathbb{Q}]$.

It can be shown [1, 2] that every integral ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ can be uniquely represented by

$$\mathfrak{a} = m\left[a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z}\right],$$

where $a, b, m \in \mathbb{Z}$, $a, m > 0$, $b^2 \equiv \Delta \mod 4a$, $\gcd(a, b, (b^2 - \Delta)/4a) = 1$, and $b$ is uniquely determined modulo $2a$. The fractional ideals are the subsets $\mathfrak{a}$ of $\mathbb{Q}(\sqrt{\Delta})$ such that there exists $d$ where $d\mathfrak{a}$ is an integral ideal of $\mathcal{O}_\Delta$. They can be uniquely represented by

$$\mathfrak{a} = q\left[a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z}\right],$$

where $q = \frac{m}{d(\mathfrak{a})}$ and $d(\mathfrak{a})$ is the minimal denominator of $\mathfrak{a}$ defined by $m, a, b$, that is to say the minimal positive $d$ such that $d\mathfrak{a}$ is integral. In addition, $a, b, m$ satisfy the same properties as for the integral ideals. This representation allows us to compute the inverse of a fractional ideal of $\mathcal{O}_\Delta$. Let $\mathfrak{a}$ be a fractional ideal represented by $(q, a, b)$, then its inverse is given by

$$\mathfrak{a}^{-1} = \frac{q}{\mathrm{N}(\mathfrak{a})}\left[a\mathbb{Z} + \frac{-b + \sqrt{\Delta}}{2}\mathbb{Z}\right].$$

The expression of the norm of an ideal can also be made explicit.

**Proposition 4.1** *Let $\mathfrak{a}$ be a fractional ideal represented by $(m/d, a, b)$, then its norm is given by*

$$\mathrm{N}(\mathfrak{a}) = am^2/d^2.$$

To compute the group structure of $\mathrm{Cl}_\Delta$, we will use a sieving algorithm that requires the enumeration of non inert primes of norm lower than a certain bound. To this end, we need to find a way to decide whether a prime is inert, ramified or split, which can be done by using Kummer's theorem.

**Proposition 4.2** *Let $p$ be a prime and let $\left(\frac{\Delta}{p}\right)$ be the Kronecker symbol of $\Delta$ and $p$. We know from Kummer's theorem that:*

- *$p$ splits completely, that is $p\mathcal{O}_\Delta = \mathfrak{p}_1\mathfrak{p}_2$, if $\left(\frac{\Delta}{p}\right) = 1$.*
- *$p$ is inert, that is $p\mathcal{O}_\Delta = \mathfrak{p}_1$, if $\left(\frac{\Delta}{p}\right) = -1$.*
- *$p$ is ramified, that is $p\mathcal{O}_\Delta = \mathfrak{p}_1^2$, if $\left(\frac{\Delta}{p}\right) = 0$.*

These considerations allow us to compute the norm of a given prime ideal $\mathfrak{p} \mid p$. Indeed, if it splits completely or if it is ramified, then $\mathrm{N}(\mathfrak{p}) = p$ whereas if $p$ is inert then $\mathrm{N}(\mathfrak{p}) = p^2$.

The group of units in quadratic extensions is much simpler than in the general case. Recall that in the imaginary case $r_1 = 0$ and $r_2 = 1$ whereas in the real case $r_1 = 2$ and $r_2 = 0$. In the imaginary case, there is no torsion-free subgroup of $\mathcal{O}_\Delta^*$. The units are simply the roots of unity in $\mathcal{O}_\Delta$, that is to say

- $\pm 1$ if $\Delta < -4$
- $\pm 1$, $\pm i$ if $\Delta = -4$
- $\pm 1$, $\pm i$, $\frac{1 \pm \sqrt{-3}}{2}$ if $\Delta = -3$.

On the other hand, there is a one dimensional torsion-free subgroup of $\mathcal{O}_\Delta^*$ in the real case. The group of units has the form

$$\mathcal{O}_\Delta^* \simeq \langle -1 \rangle \times \langle \varepsilon_\Delta \rangle ,$$

for some $\varepsilon_\Delta$ called a *fundamental unit* of $\mathcal{O}_\Delta$. As $r = 1$, the regulator of $\mathcal{O}_\Delta$ has the simple form

$$R_\Delta = \log|\varepsilon_\Delta|.$$

Let us now define the notions of normal ideal and reduced ideal in the context of quadratic number fields.

**Definition 4.3** *Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_\Delta$ represented by $(q, a, b)$, then $\mathfrak{a}$ is normal if*

- *$-a < b \leq a$ if ($\Delta < 0$) or ($\Delta > 0$ and $a \geq \sqrt{\Delta}$)*
- *$\sqrt{\Delta} - 2a < b \leq \sqrt{\Delta}$ if $\Delta > 0$ and $a < \sqrt{\Delta}$.*

*We say that it is reduced if it is normal, $q = 1/a$, and*

- *$|b| \leq a \leq c$, and ($b \geq 0$ if $a = c$) in the imaginary case*
- *$|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}$ in the real case,*

*where $c = (\Delta - b^2)/(4a)$.*

## 4.2 Quadratic forms

To represent ideals with binary quadratic forms, we use the map between primitive ideals of $\mathcal{O}_\Delta$ and binary quadratic forms of discriminant $\Delta$

$$a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z} \longmapsto aX^2 + bXY + cY^2.$$

If we restrict to normal ideals and normal forms, which are the preimages of normal ideals, this map is actually a bijection. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two normal ideals of $\mathcal{O}_\Delta$. The quadratic form corresponding to $\mathfrak{ab}$ is the composition of the normal quadratic form $\phi_\mathfrak{a}$ representing $\mathfrak{a}$ and the normal quadratic form $\phi_\mathfrak{b}$ representing $\mathfrak{b}$. In the following, we manipulate primitive representatives of classes of ideals, thus allowing ourselves to consider arithmetic operations on quadratic forms. The composition is described in Algorithm 1.

**Algorithm 1** Composition of quadratic forms

**Require:** $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ with $a_1 > a_2$
**Ensure:** The composition $f_3 = (a_3, b_3, c_3)$ of $f_1$ and $f_2$
$s \leftarrow \frac{1}{2}(b_1 + b_2)$
$n \leftarrow b_2 - s$.
Compute $(u, v, d)$ such that $ua_2 + va_1 = d = \gcd(a_2, a_1)$, $y_1 \leftarrow u$
Compute $(u, v, d_1)$ such that $us + vd = d_1 = \gcd(s, d)$, $x_2 \leftarrow u$, $y_2 \leftarrow -v$
$v_1 \leftarrow a_1/d_1$, $v_2 \leftarrow a_2/d_1$
$r \leftarrow (y_1 y_2 n - x_2 c_2 \mod v_1)$
$b_3 \leftarrow b_2 + 2v_2 r$, $a_3 \leftarrow v_1 v_2$
$c_3 \leftarrow (c_2 d_1 + r(b_2 + v_2 r))/v_1$
**return** $(a_3, b_3, c_3)$

The composition of quadratic forms is the same whether $\Delta$ is positive or negative. On the other hand, the reduction step differs. In the imaginary case, we always consider the unique reduced representative of a class. We describe in Algorithm 2 the reduction step of a primitive ideal for $\Delta < 0$. This procedure can be applied independently to the unique reduced ideal of a given class or to the corresponding quadratic form.

**Algorithm 2** Reduction of primitive ideals in the imaginary case

**Require:** $\mathfrak{a} = (a, b, c)$ of negative discriminant
**Ensure:** Reduced ideal equivalent to $\mathfrak{a}$.
$k \leftarrow$ false
**while** $k =$ false **do**
  **if** not $(-a < b \leq a)$ **then**
    $b \leftarrow 2aq + r$ with $0 \leq r < 2a$ by Euclidean division of $b$ by $2a$
    $c \leftarrow c - bq + aq^2$
  **end if**
  $k \leftarrow$ true
  **if** $a > c$ **then**
    $b \leftarrow -b$, exchange $a$ and $c$, $k \leftarrow$ false
  **end if**
  **if** $a = c$ and $b < 0$ **then**
    $b \leftarrow -b$, $k \leftarrow$ false
  **end if**
**end while**
**return** $(a, b, c)$

Both composition and reduction of quadratic forms can be done in $O(\log^2|\Delta|)$ bit operations. Reduced ideals have the property that $a, b < \sqrt{|\Delta|}$. So the reduced ideals gives reasonably small representative for each element of $\mathrm{Cl}_{\mathcal{O}_\Delta}$. Moreover, there is only one reduced ideal in the ideal class of an imaginary quadratic order. This allows us to identify elements of $\mathrm{Cl}_{\mathcal{O}_\Delta}$ with reduced binary quadratic forms of discriminant $\Delta$.

## References

[1] J. Buchmann, C.Thiel, and H.C. Williams. Short representation of quadratic integers. *Computational Algebra and Number Theory, Mathematics and its Applications*, 325:159–185, 1995.

[2] H.K. Lenstra. On the calculation of regulators and class numbers of quadratic felds. *London Math. Soc. Lecture Note Series*, 56:123–150, 1982.