**Isogeny-based Cryptography School** **Summer 2021**

# Lecture 2: Ideals in Number Fields

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

**Disclaimer**: *These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.*

## 2.1 Fractional ideals

To construct the ideal class group, we need to define the notion of *fractional ideal*. We will list a few properties relative to these objects without demonstrations. Complete proofs can be found in Chapter 1, §3 of Neukirch's book on the subject [3]. There are different equivalent definitions of a fractional ideal of an order $\mathcal{O}$ of a number field $K$. They naturally extend the notion of ideal of $\mathcal{O}$ when we define them as subsets $\mathfrak{a}$ of $K$ such that there is an integer $d > 0$ with $d\mathfrak{a}$ an ideal of $\mathcal{O}$. To differentiate fractional ideals from ideals of $\mathcal{O}$, we often refer to the latter as *integral ideals* of $K$. We now provide an alternative definition of a fractional ideal of $\mathcal{O}$.

**Definition 2.1 (Fractional ideal)** *A fractional ideal of an order $\mathcal{O}$ of $K$ is a finitely generated $\mathcal{O}$-submodule of $K$.*

The above definition emphasizes the module structure of a fractional ideal of $\mathcal{O}$. In particular, a fractional ideal $\mathfrak{a}$ is both an $\mathcal{O}$-module and a $\mathbb{Z}$-module. As an $\mathcal{O}$-module, $\mathfrak{a}$ is defined by 2 elements (we often call this the 2-element representation), while $\mathfrak{a}$ can also be viewed as a $\mathbb{Z}$ module, i.e. there exist $a_1, \ldots, a_n$ (where $n = \deg(K)$) such that

$$\mathfrak{a} = \mathbb{Z}a_1 + \mathbb{Z}a_2 + \ldots + \mathbb{Z}a_n.$$

Therefore fractional ideals are Euclidean lattices. Fractional ideals can be added and multiplied. If $\mathfrak{a} = \bigoplus_{i \leq n} \mathbb{Z}a_i$ and $\mathfrak{b} = \bigoplus_{i \leq n} \mathbb{Z}b_i$, then we have

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} &= \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n + \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n \\ \mathfrak{a}\mathfrak{b} &= \mathbb{Z}a_1b_1 + \ldots + \mathbb{Z}a_nb_1 + \mathbb{Z}a_1b_2 + \ldots + \mathbb{Z}a_nb_2 + \ldots \end{aligned}$$

Note that the generating sets presented above are not bases. Standard linear algebra techniques are required to compute the basis of $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{a} + \mathfrak{b}$, which run in polynomial time. Certain fractional ideals are *invertible.* Let $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}}$. The inverse of $\mathfrak{a}$ is given by

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}.$$

Invertible fractional ideals of $\mathcal{O}$ form a multiplicative group.

## 2.2 Prime ideals

**Proposition 2.2** *An order $\mathcal{O}$ of $K$ is a one-dimensional noetherian integral domain, that is to say that every prime ideal $\mathfrak{p} \in \mathcal{O}$ is maximal.*

Let $\mathfrak{p}$ be a prime ideal of the order $\mathcal{O}$ of $K$. As it is a maximal ideal, $\mathcal{O}/\mathfrak{p}$ is a field called *the residue class field* of $\mathfrak{p}$. For every prime ideal $\mathfrak{p}$ there exists a prime number $p$ such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. We say that $\mathfrak{p}$ lies over $p$ and we denote this property by $\mathfrak{p} \mid p$. Furthermore, for every prime $p$ we have the following unique decomposition

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}, \tag{2.1}$$

where the $\mathfrak{p}_i$ are prime ideals of $\mathcal{O}_K$. For every $i$, the exponent $e_i$ is called the *ramification index*, and the degree of the field extension

$$f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p]$$

is called the *inertia degree* of $\mathfrak{p}_i$ over $p$. As $K/\mathbb{Q}$ is separable, we have the identity

$$\sum_{i=1}^{g} e_i f_i = n.$$

**Definition 2.3** *Using the above notations, we say that*

- *$p$ splits completely if $g = n$. Hence $\forall i, e_i = f_i = 1$.*
- *$p$ is inert if $g = e_1 = 1$. In that case $p\mathcal{O}_K = \mathfrak{p}_1$ and $f_1 = [K : \mathbb{Q}]$.*
- *$p$ ramifies (or $K$ is ramified at $p$) if $\exists i,\ e_i \geq 2$.*

We can compute the prime ideals occurring in (2.1) for most of the primes in the case $\mathbb{Z}[\theta] \subseteq \mathcal{O}$ from Kummer's theorem. For a proof of this theorem we refer to [1, Theorem 4.8.13].

**Theorem 2.4 (Kummer)** *Let $\mathcal{O}$ be an order of $K$ satisfying $\mathbb{Z}[\theta] \subseteq \mathcal{O}$, and $f = [\mathcal{O} : \mathbb{Z}[\theta]]$ the index of $\theta$ in $\mathcal{O}$. Then for any prime $p \nmid f$ we can obtain the prime decomposition as follows. Let*

$$T(X) \equiv \prod_{i=1}^{g} T_i(X)^{e_i} \mod p$$

*be the decomposition of $T$ into monic irreducible factors in $\mathbb{F}_p[X]$. Then*

$$p\mathcal{O} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i},$$

*where*

$$\mathfrak{p}_i = p\mathcal{O} + T_i(\theta)\mathcal{O}.$$

*Furthermore $f_i = \deg(T_i(X))$.*

When $p$ divides the index, the situation is more difficult, but there are methods to deal with it [1, Chap. 6]. As only a finite number of $p$ divide the index, we already cover almost all prime ideals with the above method.

**Example 1** *If $d \equiv 2, 3 \bmod 4$, the order $\mathcal{O} = \mathbb{Z}[\sqrt{d}]$ is the maximal order, and in this case, the index of $\sqrt{d}$ is 1. Let us choose $d = 10$ for example. In this case, $T(X) = X^2 - d$.*

- *$T(X) \equiv X^2 - 1 = (X-1)(X+1) \bmod 3$. Therefore $p = 3$ is totally split, and the two primes above 3 are $\mathfrak{p}_1 = 3\mathcal{O} + (\sqrt{10}+1)\mathcal{O}$ and $\mathfrak{p}_2 = 3\mathcal{O} + (\sqrt{10}-1)\mathcal{O}$. Moreover, $\mathcal{O}/\mathfrak{p}_1 \simeq \mathcal{O}/\mathfrak{p}_2 \simeq \mathbb{F}_3$.*

- $T(X) \equiv X^2 \bmod 5$. *Therefore* $p = 5$ *ramifies, and the only prime above* $p = 5$ *is* $\mathfrak{p} = 5\mathcal{O} + \sqrt{10}\mathcal{O}$. *Moreover,* $\mathcal{O}/\mathfrak{p} \simeq \mathbb{F}_5$.
- $T(X) \equiv X^2 + 4 \bmod 7$ *is irreducible. Therefore* $p = 7$ *is inert, and the only prime above* $p = 7$ *is* $\mathfrak{p} = 7\mathcal{O} + 14\mathcal{O} = 7\mathcal{O}$. *Moreover,* $\mathcal{O}/\mathfrak{p} \simeq \mathbb{F}_{7^2}$.

This algorithmic construction of almost of of the prime ideals allows us to derive the construction of ideals $\mathfrak{a}$.

**Proposition 2.5** *Let* $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}}$*, then there exist a unique integer* $k$ *and unique prime ideals* $\mathfrak{p}_i$ *satisfying*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}.$$

## 2.3 Norm of an ideal

Now, let us extend the notion of norm to fractional ideals of an order $\mathcal{O}$. Let $\mathfrak{a}$ be a fractional ideal of an order $\mathcal{O}$ of $K$. We define its norm by

$$\mathrm{N}(\mathfrak{a}) := |\mathcal{O}/\mathfrak{a}|\,.$$

The norms of $\mathfrak{a}$ and $\mathfrak{a}\mathcal{O}_K$ correspond when $\mathfrak{a}$ is coprime with $(f)$. Indeed, in that case, the multiplication by $f$ induces an isomorphism between $\mathcal{O}_K/\mathfrak{a}\mathcal{O}_K$ and $\mathcal{O}/\mathfrak{a}$ (see [2]), and we thus have $|\mathcal{O}/\mathfrak{a}| = |\mathcal{O}_K/\mathfrak{a}\mathcal{O}_K|$. We can verify that the norm on ideals is multiplicative and that furthermore for $\alpha \in K$

$$\mathrm{N}\left((\alpha)\right) = \mathrm{N}(\alpha),$$

that is to say that the two notions correspond for elements of $K$ and principal ideals generated by them. In particular, if $p$ is a prime such that $p = \prod_i \mathfrak{p}_i^{e_i}$, then for every $i$ we have $\mathrm{N}(\mathfrak{p}_i) = p^{f_i}$ where $f_i = [\mathcal{O}/\mathfrak{p}_i : \mathbb{Z}/p]$. The notion of norm of fractional ideals is useful to determine which primes divide a certain fractional ideal $\mathfrak{a}$. We extend norms to fractional ideals naturally with the rule $\mathrm{N}(\mathfrak{a}/\mathfrak{b}) = \mathrm{N}(\mathfrak{a})/\mathrm{N}(\mathfrak{b})$.

## References

[1] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, 1991.

[2] D. A. Cox. *Primes of the form* $x^2 + ny^2$. John Wiley & Sons, 1989.

[3] J. Neukirch. *Algebraic number theory*. Comprehensive Studies in Mathematics. Springer-Verlag, 1999. ISBN 3-540-65399-6.