Isogeny-based Cryptography School **Summer 2021**

Lecture 1: Number Fields and Orders

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.*

1.1 First definitions

Let T be an irreducible polynomial degree n. We say that K is the *number field* defined by T if it satisfies

$$K \simeq \mathbb{Q}[X]/(T(X)).$$

We denote by $\theta \in \mathbb{C}$ a root of T such that $K = \mathbb{Q}(\theta)$. In particular, a number field K always satisfies two things:

- $K \subset \mathbb{C}$.
- $[K : \mathbb{Q}] = \deg(T)$.

Let $n = [K : \mathbb{Q}]$, there are n different complex embeddings $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$. These different ways to embed K into $\mathbb{C}$ correspond to a choice of an injective morphism $K \to \mathbb{C}$ where θ gets mapped to a different root of T in $\mathbb{C}$. While the embeddings themselves are different, they preserve the structure of K as a whole. Let r_1 be the number of embeddings satisfying $\sigma_i(K) \subseteq \mathbb{R}$, namely the real embeddings. We refer to the others as the complex embeddings and denote by r_2 the number of equivalence classes of such embeddings under the complex involution $x \mapsto \overline{x}$. Therefore r_1 and r_2 satisfy $n = r_1 + 2r_2$.

Example 1 (Real quadratic fields) *To illustrate these notions, let us start with real quadratic fields. Let $d > 0$ be a square free integer. Then $K = \mathbb{Q}(\sqrt{d})$ is the number field corresponding to $T = X^2 - d$. Its elements have the form $x = a + b\sqrt{d}$ for $a, b \in \mathbb{Q}$. Its embedding are all real:*

- $\sigma : \alpha \mapsto \sqrt{d}$.
- $\sigma : \alpha \mapsto -\sqrt{d}$.

Therefore, its signature is $r_1 = 2$ and $r_2 = 0$.

Example 2 (Imaginary quadratic fields) *Our next example is the other kind of quadratic fields, namely the imaginary ones. Let $d > 0$ be a square free integer. Then $K = \mathbb{Q}(\sqrt{-d})$ is the number field corresponding to $T = X^2 + d$. Its elements have the form $x = a + b\sqrt{-d}$ for $a, b \in \mathbb{Q}$. Its embedding are all complex:*

- $\sigma : \alpha \mapsto i\sqrt{d}$.
- $\sigma : \alpha \mapsto -i\sqrt{d}$.

Therefore, its signature is $r_1 = 0$ and $r_2 = 1$. In particular, the two complex embeddings are conjugates*: i.e. one is obtained from the other one by complex conjugation.*

Example 3 (Cyclotomic fields) *Of less relevance to isogenies, the cyclotomic fields are nonetheless a very important family of number fields. Let $n \geq 1$, and let ζ_n be a primitive n-th root of unity (i.e. $\zeta_n^n = 1$, but $\zeta_n^k \neq 1$ for $k < n$). The cyclotomic field of conductor n is $K = \mathbb{Q}(\zeta_n)$. Its defining polynomial is the n-th cyclotomic polynomial*

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \gcd(n,k)=1}} \left(X - e^{2i\pi k/n}\right).$$

For $n > 1$, its embeddings are all complex and given by $\zeta_n \mapsto e^{2ik\pi/n}$ for $1 \leq k \leq n$ and $\gcd(n,k) = 1$. In particular, the signature of the field is then $r_1 = 0$, $r_2 = \varphi(n)/2$ where $\varphi(n)$ is the degree of $\mathbb{Q}(\zeta_n)$.

1.2 Norm and trace

The first notion that immediately derives from the calculation of the embeddings of an element in $\mathbb{C}$ is the algebraic norm. Many algorithms related to class group computation require us to understand which primes divide the norm of a given element.

Definition 1.1 (Norm and Trace) *Let K be a number field of degree n, σ_i be the n distinct embeddings of K in $\mathbb{C}$, and $\alpha \in K$. We define the norm and trace maps by*

$$\mathrm{N}(\alpha) = \prod_{i \leq n} \sigma_i(\alpha)$$
$$\mathrm{Tr}(\alpha) = \sum_{i \leq n} \sigma_i(\alpha).$$

The norm and trace maps satisfy: $\forall \alpha, \beta \in K$

$$\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$$
$$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$

The norm map can be extended to ideals which will be useful in the following since it will allow us to decide whether an element of the class group is smooth. We thus need an explicit formula to compute $\mathrm{N}(\alpha)$ for $\alpha \in K$. Any element $\alpha \in K$ can be decomposed as

$$\alpha = \frac{1}{d}\left(\sum_{i=0}^{n} a_i \theta^i\right),$$

where $a_i, d \in \mathbb{Z}$. Let $A(X) = \sum_i a_i X^i \in \mathbb{Z}[X]$, then we can prove by using [1, Proposition 4.3.4] that

$$\mathrm{N}(\alpha) = \frac{1}{d^n} Res(T(X), A(X)), \tag{1.1}$$

where $Res(T, A)$ denotes the resultant of the polynomials T and A.

Example 4 *Suppose $\alpha = a + b\sqrt{d}$ is an element of $\mathbb{Q}(\sqrt{d})$ for $d > 0$ squarefree, then*

- $\mathrm{N}(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d.$
- $\mathrm{Tr}(\alpha) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a.$

1.3 Orders and the ring of integers

The notion of order is really important, in particular because of its connection with the computation of isogenies. Indeed, it will be shown in future modules of this summer school that orders in a quadratic field defined by the characteristic polynomial of the Frobenius endomorphism are isomorphic to the ring of endomorphisms of ordinary elliptic curves. More generally, the maximal order generalizes the notion of integers in number fields. In particular, ideals in number fields are understood to be ideals of orders (which have a ring structure).

Definition 1.2 (Order) *$\mathcal{O}$ is said to be an order of K if it is a subring of K which is an n-dimensional $\mathbb{Z}$-module.*

A $\mathbb{Z}$-basis of a module $\mathcal{O}$ is called an *integral basis*. It has n elements where $n = [K : \mathbb{Q}]$. This means that for any order $\mathcal{O}$ of K there are n linearly independent elements $a_1, \ldots, a_n \in K$ such that

$$\mathcal{O} = \mathbb{Z}a_1 + \mathbb{Z}a_2 + \ldots + \mathbb{Z}a_n.$$

This means that orders have the structure of a *Euclidean lattice*. Orders are (partially) ordered by inclusion. If $\mathcal{O}$ and $\mathcal{O}'$ are orders of K with $\mathcal{O} \subseteq \mathcal{O}'$, then *the index* of $\mathcal{O}$ in $\mathcal{O}'$ is $[\mathcal{O}' : \mathcal{O}]$. We denote by $\mathcal{O}_K$ the maximal order of K.

Example 5 *The order $\mathcal{O} = \mathbb{Z}[\zeta_n]$ is an order of $\mathbb{Q}(\zeta_n)$. It is in fact its maximal order. Let $a_k = \zeta_n^k$ for $1 \leq k \leq n$ and $\gcd(n, k) = 1$. Then we have*

$$\mathbb{Z}[\zeta_n] = \bigoplus_{\substack{1\leq k\leq n \\ \gcd(n,k)=1}} \mathbb{Z}a_k.$$

Note that there are many examples of fields $\mathbb{Q}(\theta)$ whose maximal order is strictly larger than $\mathbb{Z}[\theta]$.

Definition 1.3 (Discriminant) *Let $\mathcal{O}$ be an order of K of integral basis $b_1, \ldots, b_n$, the discriminant $d(\mathcal{O})$ of $\mathcal{O}$ is defined by*

$$d(\mathcal{O}) = \det(\sigma_i(b_j))^2 = \det\left(\mathrm{Tr}(b_i b_j)\right).$$

The notion of discriminant is important since we need it to measure the hardness of problems such as class group computation and the discrete logarithm problem whose complexities are taken as functions of the bit size of the discriminant. As the elements of an order $\mathcal{O}$ have a minimal polynomial with coefficients in $\mathbb{Z}$, we thus know that $d(\mathcal{O}) \in \mathbb{Z}$. More generally, one can define the discriminant $d(\alpha_1, \ldots, \alpha_n)$ of an arbitrary n-tuple of points in K as $\det(\sigma_i(\alpha_j)) \in \mathbb{Q}$. In particular, $\mathbb{Z}[\theta]$ is an order of K satisfying

$$d(\mathbb{Z}[\theta]) = d(T) = d(\mathcal{O}_K)f^2,$$

where $d(T)$ denotes the discriminant of the polynomial T and $f = [\mathcal{O}_K : \mathbb{Z}[\theta]]$. In general, $f \neq 1$ and thus $\mathbb{Z}[\theta] \subsetneq \mathcal{O}_K$. When $\mathcal{O} \subsetneq \mathcal{O}_K$, $f := [\mathcal{O}_K, \mathcal{O}]$ is called the *conductor* of $\mathcal{O}$.

Example 6 *The discriminant of $\mathbb{Z}[\zeta_n]$ for $n \geq 2$ is given by*

$$d(\mathbb{Z}[\zeta_n]) = (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)(p-1)}}.$$

References

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

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