Isogeny-based Cryptography School **Summer 2021**

Lecture 3: Class Groups and Unit Groups

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

3.1 Ideal class group

Definition 3.1 *Let $\mathcal{O}$ be an order of K. We denote by*

- *$\mathcal{I}_\mathcal{O}$ the group of invertible fractional ideals of $\mathcal{O}$*
- *$\mathcal{P}_\mathcal{O}$ the group of fractional principal invertible ideals of $\mathcal{O}$, that is, invertible fractional ideals of the form $\alpha\mathcal{O}$ for $\alpha \in K$.*

Definition 3.2 (Ideal class group) *Let $\mathcal{O}$ be an order of K. Its ideal class group is defined as*

$$\mathrm{Cl}_\mathcal{O} = \mathcal{I}_\mathcal{O}/\mathcal{P}_\mathcal{O}.$$

Given a fractional ideal $\mathfrak{a} \in \mathcal{I}_\mathcal{O}$, we denote by $[\mathfrak{a}]$ its equivalence class in $\mathrm{Cl}_\mathcal{O}$. We emphasize here that if $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}_\mathcal{O}$, then $[\mathfrak{a}] = [\mathfrak{b}]$ if and only if $\exists \alpha \in K,\ \mathfrak{b} = (\alpha)\mathfrak{a}$.

The finiteness of the ideal class group of an order $\mathcal{O}$ of K can be proved by the means of Minkowski theory. Following [4, Chap. 6], we present here the proof of the special case $\mathcal{O} = \mathcal{O}_K$. To construct the Euclidean lattice on which we will use Minkowski's theorem, we first have to define the set

$$K_\mathbb{R} = \left\{ (z_\sigma) \in \prod_\sigma \mathbb{C} \mid z_\rho \in \mathbb{R},\ z_{\overline{\sigma}} = \overline{z}_\sigma \right\},$$

where the σ are the n embeddings of K into $\mathbb{C}$ and ρ are the r_1 real embeddings where $n = r_1 + 2r_2$. We then define the mapping $\Psi : K \to K_\mathbb{R}$ by

$$\begin{array}{rccc} & K & \longrightarrow & K_\mathbb{R} \\ \Psi : & x & \longmapsto & (\sigma_1(x), \ldots, \sigma_n(x)), \end{array}$$

We can prove the following proposition by using the definitions of volume and discriminant as determinants of matrices. We refer to [4] Proposition 5.2 for a full proof.

Proposition 3.3 *If $\mathfrak{a} \neq 0$ is an ideal of $\mathcal{O}$, then $\Gamma = \Psi(\mathfrak{a})$ is a complete lattice in $K_\mathbb{R}$. Its fundamental mesh has volume*

$$\mathrm{vol}(\Gamma) = \sqrt{|d(\mathcal{O})|}\mathrm{N}(\mathfrak{a}),$$

where $d(\mathcal{O})$ is the discriminant of $\mathcal{O}$.

This allows us to prove the existence of elements in an ideal $\mathfrak{a}$ of $\mathcal{O}$ of bounded norm.

Corollary 3.4 *Let $\mathfrak{a} \subset \mathcal{O}$ be an ideal of $\mathcal{O}$, and let $c_\sigma > 0$ for every embedding σ of K in $\mathbb{C}$ be real numbers such that $c_\sigma = c_{\overline{\sigma}}$ and*

$$\prod_\sigma c_\sigma > \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d(\mathcal{O})|}\mathrm{N}(\mathfrak{a}).$$

Then there exists $a \in \mathfrak{a}$, $a \neq 0$ such that $|\sigma(a)| < c_\sigma$ for every embedding σ of K.

Proof: We first define the centrally symmetric convex set

$$X := \{(z_\sigma) \in K_{\mathbb{R}} \mid |z_\sigma| < c_\sigma\}.$$

Its volume is given by $\mathrm{vol}(X) = 2^{r_1+r_2}\pi^{r_2}\prod_\sigma c_\sigma$. We thus have from the previous proposition that

$$\mathrm{vol}(X) > 2^{r_1+r_2}\pi^{r_2}\left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d(\mathcal{O})|}\mathrm{N}(\mathfrak{a}) = 2^n \,\mathrm{vol}(\Gamma).$$

We conclude by Minkowski's first theorem that there exists a lattice point $\Psi(a) \in X$ $a \neq 0$, $a \in \mathfrak{a}$. ■

Theorem 3.5 *The ideal class group $\mathrm{Cl}_\mathcal{O}$ is a finite group. Its order $h_\mathcal{O}$ is called the class number .*

Proof: Using Corollary 3.4, we show that for every fractional ideal $\mathfrak{a}$, there is $a \in \mathfrak{a}$ such that

$$|\mathrm{N}(a)| \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d(\mathcal{O})|}\mathrm{N}(\mathfrak{a}).$$

Then we prove that the class of every fractional ideal $\mathfrak{b}$ contains $\mathfrak{b}_0$ such that $\mathrm{N}(\mathfrak{b}_0) \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d(\mathcal{O})|}$ by applying the above inequality to $\mathfrak{a} := \mathfrak{b}^{-1}$ and defining $\mathfrak{b}_0 := (a)\mathfrak{b}$ which satisfies the desired bound on the norm, as well as $[\mathfrak{b}_0] = [\mathfrak{b}]$. Now from the properties of prime ideal decomposition of ideals, there can only be a finite number of ideals $\mathfrak{b}_0$ that satisfy $\mathrm{N}(\mathfrak{b}_0) \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d(\mathcal{O})|}$ thus proving the finiteness of $\mathrm{Cl}_\mathcal{O}$. ■

To compute $\mathrm{Cl}_\mathcal{O}$, we need to identify a generating set $\mathcal{B} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_N\}$ for $\mathrm{Cl}_\mathcal{O}$. We take the prime ideals satisfying $\mathrm{N}(\mathfrak{p}) \leq B$ for a bound B large enough to ensure that we generate the whole class group. The proof of the finiteness of $\mathrm{Cl}_\mathcal{O}$ showed that we could take the exponential bound $B = \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d(\mathcal{O})|}$. Unfortunately, we have to rely on an unproven assumption to exhibit a moderate bound, namely the *Generalized Riemann Hypothesis*. It states that the zeros of the Hecke L-function

$$L(s, \chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\mathrm{N}(\mathfrak{a})^s},$$

satisfy $\mathrm{Re}(s) > 1/2$ for any Hecke character χ. The idea of Bach's theorem [1, 3] is to look at a character χ defined modulo $\mathfrak{f} := (f)$ where f the conductor of the order we work with over the ideals of $\mathcal{O}_K$ and to study the difference between $L(s, \chi)$ and $\zeta(s) = L(s, \chi_0)$ (where χ_0 is the trivial character). They differ by a large term coming from the pole of $L(s, \chi_0)$ and by terms coming from zeros ρ of $L(s, \chi_0)$ satisfying $0 < \mathrm{Re}(\rho) < 1$. Under GRH, one only has to care about the pole $L(s, \chi_0)$, whose study allows one to derive Bach's bounds.

Theorem 3.6 (Bach) *Let K be a number field of degree greater than 1, and let Δ be the discriminant of K. Let χ be a non principal character of the ideals of K that is defined modulo $\mathfrak{f}$, then*

- $\chi(\mathfrak{p}) \neq 1$ *occurs for* $\mathrm{N}(\mathfrak{p}) \leq 3\log^2\left(\Delta^2\mathrm{N}(\mathfrak{f})\right)$
- $\chi(\mathfrak{p}) \neq 0, 1$ *occurs for* $\mathrm{N}(\mathfrak{p}) \leq 12\log^2\left(\Delta^2\mathrm{N}(\mathfrak{f})\right)$

- $\chi(\mathfrak{p}) \neq 0, 1$ *and* $\deg(\mathfrak{p}) = 1$ *occurs for* $\mathrm{N}(\mathfrak{p}) \leq 18 \log^2\left(\Delta^2 \mathrm{N}(\mathfrak{f})\right)$

To simplify the analysis, let us state the consequence of this theorem for the generators of $\mathrm{Cl}(\mathcal{O}_K)$. In this case, we can use a character defined modulo $f = 1$. Let $\langle \mathcal{B} \rangle \subseteq \mathrm{Cl}_{\mathcal{O}_K}$ be the set generated by the primes in $\mathcal{B}$ for a bound $B \geq 12 \log^2\left(\Delta^2\right)$ (note that here $\mathrm{N}(\mathfrak{f}) = 1$ since $\mathcal{O} = \mathcal{O}_K$). If $\langle \mathcal{B} \rangle \neq \mathrm{Cl}_{\mathcal{O}_K}$, then there is a non-trivial character $\mathrm{Cl}_{\mathcal{O}_K} \to \mathbb{C}^*$ which is trivial on $\langle \mathcal{B} \rangle$, which is a contradiction since by Bach's theorem, the ideals $\mathfrak{a}$ for which $\chi(\mathfrak{a}) \neq 1$ have to be in $\langle \mathcal{B} \rangle$.

3.2 Unit group

Definition 3.7 *We say that $x \in \mathcal{O}$ is a unit if*

$$\mathrm{N}(x) = \pm 1.$$

For every unit x, we have $\mathrm{N}(x) \in \mathbb{Z}$ and consequently $x \in \mathcal{O}$. In addition, by multiplicativity of the norm, the units form a multiplicative group that we denote by $\mathcal{O}^*$. We denote by $\mu(K)$ the multiplicative group of the roots of unity.

$$\forall x \in \mu(K)\ \exists k \in \mathbb{N},\ \mathrm{N}(x)^k = \mathrm{N}(x^k) = \mathrm{N}(1) = 1.$$

As $\mathrm{N}(x) \in \mathbb{Q}$, we know that $\mathrm{N}(x) = \pm 1$ and thus

$$\mu(K) \subseteq \mathcal{O}^*.$$

We quote here the main result concerning the group of units of a number field. For a detailed proof of this theorem, we refer to [4, Chap I §7] .

Theorem 3.8 *Let r_1 be the number of real embeddings of K and r_2 the number of classes of complex embeddings of K under the complex involution. $\mathcal{O}_K^*$ can be decomposed as*

$$\mathcal{O}^* \simeq \mu(K) \times \mathbb{Z}^{r_1 + r_2 - 1}.$$

Let $r := r_1 + r_2 - 1$. The previous result implies that there are units $\varepsilon_1, \ldots, \varepsilon_r$ such that every unit ε can be uniquely decomposed as $\varepsilon = \xi \varepsilon_1^{\nu_1} \ldots \varepsilon_r^{\nu_r}$, with $\xi \in \mu(K)$ and integers ν_i. Any r-tuple of elements $\varepsilon_1, \ldots, \varepsilon_r$ of $\mathcal{O}^*$ satisfying this property is called a *system of fundamental units* of K.

The Archimedian valuations generalize the notion of absolute value on $\mathbb{R}$. They are used to define the regulator of K and the notion of reduced ideal.

Definition 3.9 (Archimedian valuation) *Let $i \leq r + 1$ and $x \in K$. We define the i-th Archimedian valuation of x by*

$$|x|_i := |\sigma_i(x)|.$$

We use the Archimedian valuations to define the logarithm function

$$\begin{array}{rccc} & K & \longrightarrow & \mathbb{R}^{r+1} \\ \mathrm{Log}: & x & \longmapsto & (\log|x|_1, \ldots, \log|x|_{r+1}), \end{array}$$

which extends the notion of logarithm on the real numbers. We notice here that the logarithm vectors of units form a lattice in $\mathbb{R}^{r+1}$ since $\forall x, y \in K$, and $\forall e \in \mathbb{Z}$

$$\begin{aligned} \mathrm{Log}(x) + \mathrm{Log}(y) &= \mathrm{Log}(xy) \\ e\mathrm{Log}(x) &= \mathrm{Log}(x^e). \end{aligned}$$

This lattice, which has dimension r in $\mathbb{R}^{r+1}$ is called the *lattice of units*. The regulator of K is defined from the volume of the fundamental mesh of the lattice of units of $\mathcal{O}_K^*$. The most constructive way of defining this notion is to use the matrix

$$M_R := (\mathrm{Log}(\varepsilon_i))_{i \leq r} \in \mathbb{R}^{r \times (r+1)},$$

where the ε_i are a system of fundamental units of $\mathcal{O}_K$.

Definition 3.10 (Regulator) *Let $\mathcal{L}$ be the lattice of units of $\mathcal{O}_K$, and let M_R be a basis of $\mathcal{L}$ as defined above. The absolute value of the determinant of an arbitrary minor of size r of M_R is called the regulator and denoted by R_K or by R if there is no ambiguity.*

3.3 Euler product

The regulator and the class number of $\mathcal{O}_K$ are related via a relation involving Dedekind's zeta function.

Definition 3.11 (Dedekind zeta function) *The Dedekind zeta function is defined over the complex numbers s with $Re(s) > 1$ by*

$$\xi_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})},$$

where the $\mathfrak{a}$ are the integral ideals of $\mathcal{O}_K$.

Proposition 3.12 (Analytic class number formula) *Let h and R be respectively the class number of the maximal order of K and its regulator. These values satisfy the relation*

$$hR = \frac{|\mu(K)|\sqrt{|d(\mathcal{O}_K)|}}{2^{r_1}(2\pi)^{r_2}} \lim_{s \to 1} \left((s-1)\xi_K(s)\right).$$

As $hR \in \mathbb{R}$, we can only hope to compute an approximation of it. In class group computation, if we get h^* such that $h^* \leq hR < 2h^*$, this allows us to stop the computation once the correct class group/unit group has been computed. Note that this means that the best known techniques for the computation of the class group require us to compute the unit group as well. One of the most interesting cases in the study of isogenies is when K is an imaginary quadratic field. Since $r_1 = 0$, the rank of the unit group is 0, and it is only $\{\pm 1\}$. In this special case Proposition 3.12 gives in fact a recipe for the computation of an approximation of h and not hR. Now a good enough estimate need to be computable efficiently. This again requires the Extended Riemann Hypothesis to justify that the truncation of the product gives a good enough precision.

Proposition 3.13 (From [2]) *Under the Extended Riemann Hypothesis, there is a polynomial time algorithm to compute h^* such that $h^* \leq hR < 2h^*$.*

Archimedian valuations also allow us to define the notion of *reduced ideal*. The purpose of the reduction of a fractional ideal $\mathfrak{a}$ is to find an integral ideal $\mathfrak{a}_1$ in the same class in $\mathrm{Cl}_{\mathcal{O}_K}$ with minimal relative generator, that is a minimal $\alpha \in K$ such that $\mathfrak{a} = (\alpha)\mathfrak{a}_1$.

Definition 3.14 (Minimum of an ideal) *Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. We say that $\alpha \in \mathfrak{a}$ is a minimum if*

$$\beta \in \mathfrak{a},\ |\beta|_i < |\alpha|_i\ \forall i \leq r \Rightarrow \beta = 0$$

We say that an ideal $\mathfrak{a}$ is *reduced* if the smallest positive integer in $\mathfrak{a}$ is a minimum in $\mathfrak{a}$.

References

[1] E. Bach. Explicit bounds for primality testing and related problems. *Mathematics of Computation*, 55(191):355–380, 1990.

[2] E. Bach. Improved approximations for Euler products. In *Number Theory: CMS Proc.*, volume 15, pages 13–28. Amer. Math. Soc., Providence, RI, 1995.

[3] K. Belabas, F. Diaz y Diaz, and E. Friedman. Small generators of the ideal class group. *Mathematics of Computation*, 77(262):1185–1197, 2007.

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