MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

AN $L(1/3)$ ALGORITHM FOR IDEAL CLASS GROUP AND REGULATOR COMPUTATION IN CERTAIN NUMBER FIELDS

JEAN-FRANÇOIS BIASSE

Abstract. We analyze the complexity of the computation of the class group structure, regulator, and a system of fundamental units of an order in a certain class of number fields. Our approach differs from Buchmann's, who proved a complexity bound under the generalized Riemann hypothesis of $L(1/2, O(1))$ when the discriminant tends to infinity with fixed degree. We achieve a heuristic subexponential complexity in $O(L(1/3, O(1)))$ under the generalized Riemann hypothesis when both the discriminant and the degree of the extension tend to infinity by using techniques due to Enge, Gaudry and Thomé in the context of algebraic curves over finite fields. We also address rigorously the problem of the precision of the computation of the regulator.

1. Introduction

Let $\mathbb{K} = \mathbb{Q}(\theta)$ be a number field of degree n and discriminant Δ. The ideal class group of its maximal order $\mathcal{O}_\mathbb{K}$ is a finite abelian group that can be decomposed as

$$\mathrm{Cl}(\mathcal{O}_\mathbb{K}) = \bigoplus_i \mathbb{Z}/d_i\mathbb{Z},$$

with $d_i \mid d_{i+1}$. Computing the structure of $\mathrm{Cl}(\mathcal{O}_\mathbb{K})$, along with the regulator and a system of fundamental units of $\mathcal{O}_\mathbb{K}$ is a major task in computational number theory. In addition, the structure of $\mathrm{Cl}(\mathcal{O}_\mathbb{K})$ can be used to solve the discrete logarithm problem, as in [15, Chap. 13].

In 1968, Shanks [23, 24] proposed an algorithm relying on the baby-step giant-step method to compute the class number and the regulator of a quadratic number field in time $O\left(|\Delta|^{1/4+\epsilon}\right)$, or $O\left(|\Delta|^{1/5+\epsilon}\right)$ under the extended Riemann hypothesis [17]. Then, a subexponential strategy for the computation of the group structure of the class group of an imaginary quadratic extension was described in 1989 by Hafner and McCurley [14]. The expected running time of this method is

$$L_\Delta(1/2, \sqrt{2} + o(1)) = e^{\left(\sqrt{2}+o(1)\right)\sqrt{\log|\Delta|\log\log|\Delta|}}.$$

Buchmann [5] generalized this result to the case of an arbitrary extension, thus obtaining a heuristic complexity bounded by $L_\Delta(1/2, 1.7 + o(1))$. This complexity is valid for fixed degree n and Δ tending to infinity. This technique was first used by Adleman, Huang and DeMarrais to compute discrete logarithms in the Jacobian of hyperelliptic curves, and then by Enge [10] who later developed with Gaudry and

2000 *Mathematics Subject Classification.* Primary 54C40, 14E20; Secondary 46E25, 20C20.
Key words and phrases. Number fields, ideal class group, regulator, units, index calculus, subexponentiality.
The author was supported by a DGA grant.

Thomé [11] an algorithm for computing the group structure of the Jacobian and solving the discrete logarithm problem for a certain class of curves in time

$$L_{q^g}\left(1/3, O(1)\right) = e^{O(1)\left(\log(q^g)^{1/3}\log\log(q^g)^{2/3}\right)}.$$

In this paper, we adapt the $L(1/3)$ algorithm of Enge, Gaudry and Thomé to the computation of the group structure of the ideal class group, the regulator, and a system of fundamental units of $\mathcal{O}_{\mathbb{K}}$. We deal with the case where both the discriminant and the degree of the extension grow to infinity under certain restrictions, whereas in [5] the degree is assumed to be fixed. We also provide bounds on the loss of precision during the computation of the regulator.

2. Main idea

Let $\kappa > 0$ be a constant. We define a class $\mathcal{C}_\kappa$ of number fields $\mathbb{K} = \mathbb{Q}(\theta)$ for which we can compute the ideal class group, the regulator and a system of fundamental units of $\mathbb{Z}[\theta]$ in heuristic expected time bounded by $L_{\Delta_f}(1/3, O(1))$, where $f := [\mathcal{O}_{\mathbb{K}}, \mathbb{Z}[\theta]]$ is the index of $\mathbb{Z}[\theta]$, and Δ_f is its discriminant and

$$L_N(\alpha, \beta) := e^{\beta(\log|N|)^\alpha(\log\log|N|)^{1-\alpha}}.$$

Note that for number fields of $\mathcal{C}_\kappa$ satisfying $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta]$, our algorithm computes these invariants for the maximal order in heuristic subexponential complexity $L_\Delta(1/3, O(1))$.

Let $\mathbb{K} := \mathbb{Q}(\theta)$ be a number field of discriminant Δ such that

$$\mathbb{K} = \mathbb{Q}[X]/T(X),$$

with $T(X) = t_n X^n + t_{n-1}X^{n-1} + \ldots + t_0 \in \mathbb{Z}[X]$, $n := [\mathbb{K} : \mathbb{Q}]$ and d be a bound on the size of the coefficients of T, that is

$$d := \log H_T,$$

where $H_T := \max_i |t_i|$. The number field $\mathbb{K}$ belongs to $\mathcal{C}_\kappa$ if

$$n \leq n_0 \log\left(|\Delta_f|\right)^\alpha (1 + o(1)) \tag{1}$$

$$d \leq d_0 \log\left(|\Delta_f|\right)^{1-\alpha} (1 + o(1)), \tag{2}$$

for some $\alpha \in \left]\frac{1}{3}, \frac{2}{3}\right[$, and some constants n_0 and d_0 such that $n_0 d_0 = \kappa$. To the best of our knowledge, estimating the proportion of integer polynomials satisfying (1) and (2) is an open problem. However, we can easily provide bounds on Δ_f involving n and d to verify that our conditions are not absurd. First, Minkowski's bound on the discriminant of a number field allows us to state that

$$|\Delta_f| \geq |\Delta| \geq \frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^n.$$

We thus have $n \leq O\left(\log|\Delta_f|(1 + o(1))\right)$. From the definition of the discriminant of a polynomial, we can also derive an upper bound of $|\Delta_f|$. Indeed, the discriminant

of T is the resultant of T and its derivative, which is given by

$$\Delta_f = (-1)^{n(n-1)/2} \begin{vmatrix} 1 & t_{n-1} & t_{n-2} & \dots & t_0 & 0 & \dots \\ 0 & t_n & t_{n-1} & \dots & t_1 & t_0 & \dots \\ \vdots & & & & \vdots & & \\ 0 & \dots & \dots & 0 & t_n & \dots & t_0 \\ n & (n-1)t_{n-1} & (n-2)t_{n-2} & \dots & t_0 & 0 & \dots \\ 0 & nt_n & (n-1)t_{n-1} & \dots & t_1 & 0 & \dots \\ \vdots & & & & \vdots & & \\ 0 & \dots & \dots & 0 & nt_n & \dots & t_1 \end{vmatrix}.$$

The $(2n-1) \times (2n-1)$ matrix whose determinant gives us Δ_f has the absolute value of its entries bounded by nH_T. By using Hadamard's inequality, we can thus bound $|\Delta_f|$ from above by

$$|\Delta_f| \leq \left(\left(\sqrt{2n-1}\right) nH_T\right)^{2n-1}.$$

This implies that in general, $\log|\Delta_f| \leq (2n-1)(d+1+o(1))$. Note here that the restrictions given by (1) and (2) are asymptotic, and that they only make sense for infinite families of number fields. In the following example, we exhibit such an infinite family constructed as Kummer extensions of $\mathbb{Q}$, thus proving that our class of number fields is not empty.

Example. Let $D \in \mathbb{Z}$, and $\mathbb{K}_{n,K}$ be an extension of $\mathbb{Q}$ defined by an irreducible polynomial of the form

$$T(X) = X^n - K,$$

with

$$K := \left\lfloor e^{\log(|D|)^{1-\alpha}} \right\rfloor$$
$$n := \left\lfloor \log\left(|D|\right)^{\alpha} \right\rfloor,$$

for some $\alpha \in \left]\frac{1}{3}, \frac{2}{3}\right[$. Then, T has discriminant satisfying

$$\log(|\Delta_f|) = \log(n^n K^{n-1}) = \log(|D|)(1+o(1)).$$

This way, we can construct an infinite family of number fields belonging to $\mathcal{C}_1$ since every $D \neq 0$ yields a polynomial T satisfying (1) and (2). In Table 1, we illustrate numerically for small values of n and K that this family of number fields belongs to $\mathcal{C}_1$. We restricted ourselves to $\alpha = 1/2$. We observe in Table 1 that our construction ensures that $n \sim (\log|\Delta_f|)^{1/2}$ and $\log K \sim (\log|\Delta_f|)^{1/2}$.

TABLE 1. Fields defined by polynomials of the form $X^n - K$ in $\mathcal{C}_1$

Δ_f	n	K	$n/(\log\lvert\Delta_f\rvert)^{1/2}$	$\log(K)/(\log\lvert\Delta_f\rvert)^{1/2}$
52	2	13	1.006	1.290
-22707	3	29	0.947	1.063
-42592000	4	55	0.954	0.956
1712441503125	5	153	0.942	0.948
1791002197851656256	6	521	0.925	0.965

If in addition we restrict ourselves to n and K being the largest prime numbers below their respective bounds such that

$$n^2 \nmid K^{n-1} - 1,$$

then by using Dedekind's criterion whose proof can be found in [8, 6.1.2], we have an infinite family of number fields lying in $\mathcal{C}_1$ satisfying $\mathbb{Z}[\theta] = \mathcal{O}_{\mathbb{K}_{n,K}}$, where $\mathcal{O}_{\mathbb{K}_{n,K}}$ is the maximal order of $\mathbb{K}_{n,K}$.

We proceed by analogy with the approach of [11] in the context of algebraic curves, where the authors examined curves of the form

$$\mathcal{C} : Y^n + X^d + f(X, Y),$$

such that any monomial $X^i Y^j$ occurring in f satisfies $ni + dj < nd$. The genus g is assumed to tend to infinity and

$$\begin{aligned} n &\approx g^{\alpha} \\ d &\approx g^{1-\alpha}. \end{aligned}$$

The idea in [11] is to look for functions $\phi(X, Y) \in \mathbb{F}_q[X, Y]$ satisfying

$$\deg_Y \phi \approx g^{\alpha - 1/3} \quad \text{and} \quad \deg_X \phi \approx g^{2/3-\alpha},$$

with $\mathcal{N}(\phi)$ splitting into polynomials of degree bounded by $B = \log\left(L_{q^g}(1/3, \rho)\right)$ for some number ρ determined in the complexity analysis. Each time such a decomposition occurs, the ideal (ϕ) is necessarily a product of primes belonging to the set $\mathcal{B}$ of the totally split prime ideals of degree bounded by B

$$(\phi) = \prod_{\mathfrak{p}_i \in \mathcal{B}} \mathfrak{p}_i^{e_i}.$$

Such a decomposition of a principal ideal is called a *relation*. In the following, we will also denote the vector (e_i) itself a relation. Every time we find a relation, we add the row vector (e_i) to a matrix $M \in \mathbb{Z}^{m \times N}$ called the *relation matrix*, where $N := |\mathcal{B}|$, and $m \geq k$ is the number of relations collected. A linear algebra step is performed on this matrix. It consists in computing its Smith Normal Form, that is to say integers $d_1, \ldots, d_N$, with $d_N | d_{N-1} | \ldots | d_1$, such that there exist two unimodular matrices $U \in \mathbb{Z}^{m \times m}$ and $V \in \mathbb{Z}^{N \times N}$ satisfying

$$M = U \begin{pmatrix} d_1 & & (0) & \\ & \ddots & & (0) \\ (0) & & d_k & \\ \hline & & (0) & \end{pmatrix} V.$$

The SNF of M provides us with the group structure of the Jacobian of the curve $\mathcal{C}$. Indeed, if $\mathcal{L}_{\mathbb{Z}}$ is the lattice spanned by all the possible relations, and if $\mathcal{J}$ denotes the Jacobian of $\mathcal{C}$, then we have

$$\mathcal{J} \simeq \mathbb{Z}^N / \mathcal{L}_{\mathbb{Z}}.$$

Provided that m is large enough to ensure that with high probability the rows of M generate $\mathcal{L}_\mathbb{Z}$, and provided the classes of the elements of $\mathcal{B}$ generate $\mathcal{J}$, we have

$$\mathcal{J} \simeq \bigoplus_i \mathbb{Z}/d_i\mathbb{Z}.$$

In our context, we need the group structure of $\mathrm{Cl}(\mathbb{Z}[\theta])$, along with the regulator R, and a system of fundamental units of $\mathbb{Z}[\theta]$. In the following, we denote by f the index of $\mathbb{Z}[\theta]$, by $\mathfrak{f}$ its conductor, and by Δ_f its discriminant. The computation of the group structure of $\mathrm{Cl}(\mathbb{Z}[\theta])$ is done using methods similar to those used for the computation of the structure of $\mathcal{J}$. We look for relations of the form

$$(\phi) = \prod_i \mathfrak{p}_i^{e_i},$$

where $\phi \in \mathbb{K}$, and where the $\mathfrak{p}_i$ are prime ideals of norm bounded by $L_{\Delta_f}(1/3, \rho)$. Every time we find such a relation, we add the row vector $(e_i)_{i \leq N}$ to the relation matrix denoted by $M_\mathbb{Z} \in \mathbb{Z}^{m \times N}$. To continue the analogy with [11], we require that ϕ be of the form

$$\phi = A(\theta),$$

where $A \in \mathbb{Z}[X]$ of degree k. During the analysis, we will provide bounds on k and on the coefficients of A, that delimit the search space. Providing the rows of $M_\mathbb{Z}$ generate the lattice $\mathcal{L}_\mathbb{Z}$ of all the possible row vectors $(e_i)_{i \leq N} \in \mathbb{Z}^N$ representing a relation, and providing B is large enough to ensure that the classes of the prime ideals in $\mathcal{B}$ generate $\mathrm{Cl}(\mathbb{Z}[\theta])$, we have

$$\mathrm{Cl}(\mathbb{Z}[\theta]) \simeq \mathbb{Z}^N/\mathcal{L}_\mathbb{Z} \simeq \bigoplus_{i \leq N} \mathbb{Z}/d_i\mathbb{Z},$$

where the d_i are the diagonal coefficients of the SNF of $M_\mathbb{Z}$. The main difference with the context of algebraic curves is the computation of R and of a system of fundamental units. The group of units of $\mathbb{Z}[\theta]$ is of the form

$$U(\mathbb{K}) \simeq \mu(\mathbb{K}) \times \mathbb{Z}^r,$$

where $\mu(\mathbb{K})$ is the multiplicative group of the roots of unity in $\mathbb{Z}[\theta]$. A system of fundamental units (γ_i), $i \leq r$, is a set of elements of $\mathbb{Z}[\theta]$ satisfying

$$U(\mathbb{K}) = \mu(\mathbb{K}) \times \langle \gamma_1 \rangle \times \ldots \times \langle \gamma_r \rangle .$$

Once such a system is found, we use the logarithm map:

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

where the $|.|_j$ are the Archimedian valuations on $\mathbb{K}$, to construct a matrix $A_r \in \mathbb{R}^{r \times (r+1)}$ whose rows are the vectors $\mathrm{Log}(\phi_i)$, for $i \leq r$. The regulator is defined as the determinant of any $r \times r$ minor of A_r. To construct A_r and a system of fundamental units, we augment the row vectors by columns containing the Archimedian valuations, and add the row

$$(e_1, \ldots, e_k, \log|\phi|_1, \ldots, \log|\phi|_{r+1}) \in \mathbb{Z}^N \times \mathbb{R}^{r+1}$$

to a relation matrix M whenever a relation $(\phi) = \prod_i \mathfrak{p}_i^{e_i}$ is found. A linear algebra step performed on M provides us with the group structure, the regulator, and a system of fundamental units. It is described in detail in § 4. The following theorem summarizes the main result of this paper.

Theorem 1. *Let $\kappa > 0$ be a constant, and $\mathbb{K}$ be a number field of the form $\mathbb{K} = \mathbb{Q}(\theta)$ in $\mathcal{C}_\kappa$. Then under the Generalized Riemann Hypothesis (GRH) and other heuristics specified in the next sections, the expected time for computing $\mathrm{Cl}(\mathbb{Z}[\theta])$, the regulator, and a system of fundamental units of $\mathbb{Z}[\theta]$ lies in*

$$L_{\Delta_f}(1/3, O(1)),$$

where f is the index of $\mathbb{Z}[\theta]$ in the maximal order $\mathcal{O}_\mathbb{K}$, and Δ_f is its discriminant.

The rest of the paper is devoted to the proof of Theorem 1. We specify the parts of this proof that depend of the validity of the generalized Riemann hypothesis (GRH).

3. The relation matrix

Let ρ be a constant to be determined later, and B a smoothness bound defined by

$$B := \lceil L_{\Delta_f}(1/3, \rho) \rceil.$$

We define the factor base $\mathcal{B}$ as the set of prime ideals of norm bounded by B. This factor base has cardinality

$$N := |\mathcal{B}| = L_{\Delta_f}(1/3, \rho + o(1)).$$

In addition, as we assume GRH, the classes of the elements of $\mathcal{B}$ generate $\mathrm{Cl}(\mathbb{Z}[\theta])$. Indeed, $\mathrm{Cl}(\mathbb{Z}[\theta])$ is isomorphic to a subgroup of the ray class group of $\mathrm{Cl}(\mathcal{O}_\mathbb{K})$ of conductor $\mathfrak{f}$. By using [2, Theorem 4], we can show that under GRH, the primes of norm up to $12(\log((\Delta^2)\mathcal{N}(\mathfrak{f}))^2$ generate this ray class group. Therefore, it suffices that $B > 48(\log(\Delta_f))^2$, which is satisfied. In the following, we need to test the smoothness of principal ideals of the form (ϕ), where $\phi = A(\theta)$ and $A \in \mathbb{Z}[X]$. We use and recall in Lemma 2 the well-known result that is proved in [8, Lemma 3.3.4]

Lemma 2. *The norm of ϕ satisfies*

$$\mathcal{N}(\phi) = Res\ (T(X), A(X)),$$

where Res denotes the resultant.

Computing $\mathcal{N}(\phi)$ for $\phi \in \mathbb{K}$ allows us to decide whether ϕ is a product of prime ideals $\mathfrak{p} \in \mathcal{B}$. Indeed, it suffices to check if $\mathcal{N}(\phi) \in \mathbb{Z}$ is B-smooth which can be done by using the number field sieve (NFS) in heuristic expected time

$$L_{\mathcal{N}(\phi)}(1/3, \sqrt[3]{64/9} + o(1)).$$

During the relation search, we restrict ourselves to polynomials A having the logarithm of their coefficients a_i bounded by an integer a such that there exist two constants δ and ν to be determined later satisfying

$$a \leq \left\lceil \delta \frac{\kappa \log|\Delta_f|/n}{(\log|\Delta_f|/\log\log|\Delta_f|)^{1/3}} \right\rceil \tag{3}$$

$$k \leq \left\lceil \nu \frac{n}{(\log|\Delta_f|/\log\log|\Delta_f|)^{1/3}} \right\rceil. \tag{4}$$

Using Lemma 2 and Hadamard's inequality, we deduce an upper bound on $\log \mathcal{N}(\phi)$:

$$\log \mathcal{N}(\phi) \leq na + dk + n\log k + k\log n \tag{5}$$

$$\leq \kappa\,(\log|\Delta_f|)^{2/3}\,(\log\log|\Delta_f|)^{1/3}\,(\delta + \nu + o(1)). \tag{6}$$

Therefore, factoring the norms of the ϕ that are drawn during the relation collection can be done in heuristic expected time bounded by $L_{\Delta_f}(1/3, o(1))$. In the following, we will also need a bound on the real coefficients $\log|\phi|_i$ occurring in the relation matrix. By the following proposition, we derive a bound on the $\log|\theta|_i$ from the imposed bounds on the coefficients of T.

Proposition 3. *Let σ_i be the n complex embeddings of $\mathbb{K}$ such that we have $T = \prod_i (X - \sigma_i(\theta))$ whose coefficients satisfy (2), then the $\sigma_i(\theta)$ satisfy*

$$\log(|\theta|_i) = \log(|\sigma_i(\theta)|) = O\left((\log|\Delta_f|)^{1-\alpha}\right).$$

Proof. Landau-Mignotte's theorem [18] states that if $D \mid T$ with $\deg D = m$, then the coefficients d_j of D satisfy

$$|d_j| \leq 2^{m-1}(|T| + t_n),$$

where $|T|$ is the Euclidean norm of the vector of the coefficients of T. Applying this to $D = X - \sigma_i(\theta)$ and $m = 1$ allows us to obtain:

$$\log(|\theta|_i) \leq \log(|T| + t_n) \leq O\left((\log|\Delta_f|)^{1-\alpha}\right),$$

the second inequality being due to (2). □

Corollary 4. *With $\phi = A(\theta)$, and a and k respectively bounded by (3) and (4), we have*

$$\log|\phi|_i \leq (\log|\Delta_f|)^{2/3} (\log\log|\Delta_f|)^{1/3} (1 + o(1)).$$

Proof. From (3) and proposition 3, we have

$$\begin{aligned}
\log|\phi|_i &= \log|A(\theta)|_i \\
&\leq n\log(a) + \log|\theta_i| \\
&\leq \kappa\delta (\log|\Delta_f|)^{2/3} (\log\log|\Delta_f|)^{1/3} + O(\log(|\Delta_f|)^{2/3}) \\
&\leq (\log|\Delta_f|)^{2/3} (\log\log|\Delta_f|)^{1/3} (1 + o(1)).
\end{aligned}$$

□

To evaluate the probability of smoothness of ideals with respect to $\mathcal{B}$, we need to refer to some unproven heuristics. Let $P(\iota, \mu)$ be the probability that a principal ideal $\mathfrak{a}$ of $\mathcal{O}_\mathbb{K}$ such that $\log(\mathcal{N}(\mathfrak{a})) \leq \iota$ is smooth with respect to the set of prime ideals $\mathfrak{p}$ satisfying $\log(\mathcal{N}(\mathfrak{p})) \leq \mu$. We assume that these smoothness probabilities are the same as the probability of smoothness of integers proved in [6].

Heuristic 1. *We assume that under GRH, the probability $P(\iota, \mu)$ that a principal ideal of $\mathcal{O}_\mathbb{K}$ of norm bounded by e^ι is e^μ-smooth satisfies*

$$P(\iota, \mu) \geq e^{(-u\log u(1+o(1)))}, \tag{7}$$

for $u = \iota/\mu$.

A similar assertion on the smoothness of ideals can be proved in the quadratic case [22] under GRH, but remains conjectural for arbitrary n, even under GRH [5]. In the context of curves, Enge, Gaudry and Thomé used a theorem due to Hess to derive the smoothness probability of divisors, but had to use a similar heuristic as (7) for the smoothness of principal ideals.

Proposition 5. *Let*

$$\iota = \left\lfloor \log L_{\Delta_f}(\zeta, c) \right\rfloor = \left\lfloor c \left(\log |\Delta_f|\right)^{\zeta} \left(\log\log |\Delta_f|\right)^{1-\zeta} \right\rfloor$$
$$\mu = \left\lceil \log L_{\Delta_f}(\beta, d) \right\rceil = \left\lceil d \left(\log |\Delta_f|\right)^{\beta} \left(\log\log |\Delta_f|\right)^{1-\beta} \right\rceil,$$

then assuming Heuristic 1, we have

$$P(\iota, \mu) \geq L_{\Delta_f}\left(\zeta - \beta, \frac{-c}{d}(\zeta - \beta) + o(1)\right).$$

Proof. When $f = 1$ (that is $\mathbb{Z}[\theta] = \mathcal{O}_{\mathbb{K}}$), the result is a direct substitution of

$$u = \frac{\iota}{\mu} = \frac{c}{d}\left(\frac{\log |\Delta|}{\log\log |\Delta_f|}\right)^{\zeta-\beta}$$

in (7). On the other hand, when $f > 1$ the prime ideals dividing the prime numbers p satisfying $p \mid f$ do not occur in $\mathrm{Cl}(\mathbb{Z}[\theta])$. Therefore, the probability of smoothness with respect to the prime ideals of norm bounded by e^{μ} is less than the value given by (7) since the p such that $p \mid f$ cannot occur in the decomposition of $\mathcal{N}(\phi)$. Thus, we need to show that this loss does not affect the asymptotic expression of $P(\iota, \mu)$.

In the worst case scenario, the conductor is of the same size as $\sqrt{\Delta_f}$, and is a product of all the smallest primes. From [21], we know that there exist constants c and e such that:

$$e^{cx} \leq \prod_{p \leq x} p \leq e^{ex}.$$

Thus, an integer x such that $f = \prod_{p \leq x} p$ has to satisfy:

$$x = O\left(\log \Delta_f\right).$$

For every prime p dividing the conductor, the smoothness probability given by Heuristic 1 has to be multiplied by $(p-1)/p$ since we do not take into account prime ideals divisible by p. The cofactor multiplied to the smoothness probability given by Heuristic 1 to take into account the primes $p \mid f$ in the worst case scenario satisfies

$$\prod_{p \leq x}\left(\frac{p-1}{p}\right) \sim \frac{C}{\log x},$$

for some constant C (see [21]). Therefore, in the worst case scenario we have

$$\begin{aligned} P(\iota, \mu) &\geq L_{\Delta_f}\left(\zeta - \beta, \frac{-c}{d}(\zeta - \beta) + o(1)\right) \cdot \frac{1}{\log\log |\Delta_f|(1 + o(1))} \\ &= L_{\Delta_f}\left(\zeta - \beta, \frac{-c}{d}(\zeta - \beta) + o(1)\right). \end{aligned}$$

□

Proposition 5 allows us to derive the expected time for the relation collection phase. We need to make the following heuristic on the number of relations that are required to generate the whole lattice of relations.

Heuristic 2. *We assume that there is a constant K_1 such that collecting $N + K_1 N$ allows us to generate the full lattice of relations with a probability close to 1.*

Unlike in [5], we cannot randomize our relations since it requires ideal reduction, which is exponential in the degree. Heuristic 2 allows us to bound the time required to compute the relation matrix in a conservative way. Indeed, K_1 can be as large as we need provided that it remains constant.

Corollary 6. *The complexity of the relation collection is bounded by*

$$L_{\Delta_f}\left(1/3, \frac{\kappa(\nu+\delta)}{3\rho} + \rho + o(1)\right).$$

Proof. Direct application of Proposition 5 with the parameters

$$\beta = \frac{1}{3},\ d = \rho$$
$$\zeta = \frac{2}{3},\ c = \kappa(\delta + \nu + o(1)),$$

shows that the expected number of trials to obtain a relation is at most

$$L_{\Delta_f}\left(1/3, \frac{\kappa(\nu+\delta)}{3\rho} + o(1)\right).$$

We know that the factor base has size $N = L_{\Delta_f}(1/3, \rho + o(1))$, thus the complexity of the search for $N + K_1 N$ relations is bounded by

$$L_{\Delta_f}\left(1/3, \frac{\kappa(\nu+\delta)}{3\rho} + \rho + o(1)\right).$$

□

We postpone to §6 the study of the constraints on the parameters deriving from the size of the search space. Indeed, we need to verify that we draw sufficiently many ϕ of the form $A(\theta)$ given the constraints we have on the size of the coefficients of A and on its degree.

4. The linear algebra phase

In this section, we start with an overview of the linear algebra phase, and then we address its complexity. The computation of R and of a system of fundamental units is developed in § 5.

4.1. **Overview.** We denote by M the relation matrix whose rows lie in $\mathbb{Z}^N \times \mathbb{R}^{r+1}$, and by $M_\mathbb{Z}$ and $M_\mathbb{R}$ the matrices formed respectively by the first N and the last $r+1$ columns of M. The matrix M thus has the following shape

$$M = \left(\begin{array}{c:c} M_\mathbb{Z} & M_\mathbb{R} \end{array}\right).$$

In the following, we assume that Heuristic 2 is satisfied. If we do not obtain the full lattice of relations (which can be tested easily as we will see at the end of this section), we start all over again and construct other relations. The matrix $M_\mathbb{R}$ contains fixed point rational approximations of the $\log|\phi_i|_j$ for $i \leq N + K_1 N$ and $j \leq r+1$: the discussion of precision issues when we add or multiply two fixed point rational approximations of real numbers is postponed to § 5.2. As the rows of M are assumed to generate the full lattice of the relations, the determinant of

the lattice $\mathcal{L}_\mathbb{Z}$ spanned by the rows of $M_\mathbb{Z}$ gives us the class number $h(\mathbb{Z}[\theta])$, and its Smith Normal Form $\mathrm{diag}(d_1, \ldots, d_N)$ gives us the decomposition

$$\mathrm{Cl}(\mathbb{Z}[\theta]) \simeq \mathbb{Z}^N/\mathcal{L}_\mathbb{Z} \simeq \bigoplus_i \mathbb{Z}/d_i\mathbb{Z}.$$

On the other hand, we need to construct r relations of the form

$$(0, \ldots, 0, \log|\gamma|_1, \ldots, \log|\gamma|_{r+1}),$$

along with the corresponding values of γ (that are necessarily units), such that these relations generate the lattice $\mathcal{L}_\mathbb{R}$ of relations whose integer part contains only zero coefficients. To do this, we compute the Hermite Normal Form $H_\mathbb{Z}$ of $M_\mathbb{Z}$ with its unimodular transformation matrix $U_\mathbb{Z} \in \mathbb{Z}^{(N+K_1N)\times(N+K_1N)}$ satisfying $U_\mathbb{Z}M_\mathbb{Z} = H_\mathbb{Z}$. A full rank-matrix $H \in \mathbb{Z}^{s_1\times s_2}$ is said to be in HNF if it has the shape

$$H = \begin{pmatrix} h_{1,1} & 0 & \ldots & 0 \\ \vdots & h_{2,2} & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ * & * & \ldots & h_{s_2,s_2} \\ \hline & & (0) & \end{pmatrix},$$

with $\forall j < i : 0 \leq h_{ij} < h_{jj}$ and $\forall j > i : h_{ij} = 0$. The last K_1N rows of $U_\mathbb{Z}$ denoted by $(\vec{u}_j)_{j\leq K_1N}$ generate the kernel of $M_\mathbb{Z}$ under Heuristic 2. On the other hand, the Smith Normal Form of the essential part of $H_\mathbb{Z}$ gives us the structure of $\mathrm{Cl}(\mathbb{Z}[\theta])$, still under Heuristic 2. We recall that the essential part of a matrix $H \in \mathbb{Z}^{m\times N}$ in Hermite Normal Form is the upper left $l \times l$ submatrix such that the entries $h_{i,i}$ for $l + 1 \leq i \leq N$ satisfy $h_{i,i} = 1$. Then, we apply the $\vec{u}_j$ to $M_\mathbb{R}$, thus obtaining a matrix $A_\mathbb{R} \in \mathbb{R}^{K_1N\times(r+1)}$ whose rows correspond to the Archimedian valuations of units $(\beta_j)_{j\leq K_1N}$. To compute the regulator R, we need to find r combinations of rows of $A_\mathbb{R}$, along with the corresponding units $(\gamma_i)_{i\leq r}$, that span the lattice of units $\mathcal{L}_\mathbb{R}$. This procedure is described in § 5.

At the end of the linear algebra phase, we have to check a posteriori that $N+K_1N$ relations were enough to generate $\mathcal{L}_\mathbb{Z}$ and $\mathcal{L}_\mathbb{R}$. The analytic class number formula allows us to compute an approximation of $h(\mathcal{O}_\mathbb{K})R(\mathcal{O}_\mathbb{K})$ in polynomial time under the generalized Riemann hypothesis [3]. We also know from [19, Theorem 12.12] that

$$\frac{h(\mathbb{Z}[\theta])R(\mathbb{Z}[\theta])}{h(\mathcal{O}_\mathbb{K})R(\mathcal{O}_\mathbb{K})} = \frac{\#(\mathcal{O}_\mathbb{K}/\mathfrak{f})^*}{\#(\mathbb{Z}[\theta]/\mathfrak{f})^*},$$

where G^* denotes the multiplicative group of G, $h(\mathcal{O})$ denotes the class number of the order $\mathcal{O}$ and $R(\mathcal{O})$ its regulator. This allows us to derive a number h^* such that

$$h^* \leq R(\mathbb{Z}[\theta])h(\mathbb{Z}[\theta]) < 2h^*.$$

Before going into more details on the linear algebra phase, we recall the main steps of this process in Algorithm 1.

Algorithm 1 Linear algebra phase

Input: M

Output: $h(\mathbb{Z}[\theta])$, the structure of $\mathrm{Cl}(\mathbb{Z}[\theta])$, R, and a system of fundamental units

1: Compute the HNF $H_{\mathbb{Z}}$ of $M_{\mathbb{Z}}$ and the transformation matrix $U_{\mathbb{Z}}$.
2: Compute the SNF of the essential part of $H_{\mathbb{Z}}$ and deduce $h(\mathbb{Z}[\theta])$ and the group structure of $\mathrm{Cl}(\mathbb{Z}[\theta])$.
3: Extract a basis $(\vec{u}_j)_{j\leq K_1 N}$ of $\ker M_{\mathbb{Z}}$ from $U_{\mathbb{Z}}$ and deduce $A_{\mathbb{R}}$
4: By using the methods of § 5, find r independent relations generating $\mathcal{L}_{\mathbb{R}}$ along with the corresponding units.
5: Compute the determinant R of $\mathcal{L}_{\mathbb{R}}$.
6: Compute h^* and check if $h^* \leq h(\mathbb{Z}[\theta])R(\mathbb{Z}[\theta]) < 2h^*$. If not create another M and go back to step one.

Notation 7. *In the following, $\boldsymbol{r}_i^X$ denotes the row number i of the matrix X.*

4.2. **Complexity.** To obtain the matrix $A_{\mathbb{R}}$ and the structure of $\mathrm{Cl}(\mathbb{Z}[\theta])$, we first need to compute the Hermite Normal Form $H_{\mathbb{Z}}$ of $M_{\mathbb{Z}}$. We use the HNF algorithm described and analyzed in [27], which has the best complexity for rectangular matrices whose HNF have an essential part with small dimensions. Its bit complexity is bounded by

$$\tilde{O}\left(l(N+K_1N)N^3\left(\log|M_{\mathbb{Z}}|\right)^2+(N+K_1N)N^2\,\mathrm{M}\left(\log(h(\mathbb{Z}[\theta]))\right)\right), \tag{8}$$

where $\tilde{O}$ denotes the complexity when omitting the logarithm factors, $l \leq N$ is the number of columns of the essential part of the HNF of $M_{\mathbb{Z}}$, $|M_{\mathbb{Z}}| := \max_{i,j}\left\{|M_{\mathbb{Z}}^{i,j}|\right\}$, and $\mathrm{M}(x)$ is the bit complexity of the multiplication of integers of size bounded by x. In the following, we take

$$\mathrm{M}(x) = x\log x\log\log x.$$

We know from the Brauer-Siegel theorem [25] that

$$\log(h(\mathbb{Z}[\theta])) \leq O(\log|\Delta_f|).$$

To evaluate the complexity of the HNF computation, we need a bound on $|M_{\mathbb{Z}}|$ depending on the size of the input.

Proposition 8. *$|M_{\mathbb{Z}}|$ satisfies*

$$|M_{\mathbb{Z}}| = O((\log|\Delta_f|)^{2/3}(\log\log|\Delta_f|)^{1/3}).$$

Proof. We restricted ourselves to ϕ satisfying

$$\log(\mathcal{N}(\phi)) \leq \kappa(\log|\Delta_f|)^{2/3}(\log\log|\Delta_f|)^{1/3}(\delta+\nu+o(1)).$$

If $\mathcal{N}(\phi) = \prod_i \mathcal{N}(\mathfrak{p}_i)^{e_i}$, then we clearly see that the vector (e_i) having the largest coefficient under the previous constraint is the one where e_1 is maximal and all the others are set to zero, providing we set $\mathfrak{p}_1$ to the prime ideal of smallest norm. In that case, e_1 satisfies

$$e_1 = O((\log|\Delta_f|)^{2/3}(\log\log|\Delta_f|)^{1/3}).$$

□

This allows us to determine the expected time taken by the computation of the HNF.

Proposition 9. *The computation of the HNF has bit complexity bounded by*

$$O\left(L(1/3, 5\rho + o(1)\right).$$

The structure of $\mathrm{Cl}(\mathbb{Z}[\theta])$ immediately derives from the computation of the HNF of $M_{\mathbb{Z}}$. Indeed, the essential part of $H_{\mathbb{Z}}$ is a square matrix whose dimensions are bounded by $\log(\Delta_f)^{2+\alpha}(1 + o(1))$ and whose entries have size bounded by $O(\log|\Delta_f|)$. By using the same method as in [14], this can be done in a number of bit operations bounded by

$$O\left(\left(\log|\Delta_f|\right)^3 \left(\log(\Delta_f)^{2+\alpha}(1 + o(1))\right)^4\right),$$

which is polynomial in $\log|\Delta_f|$, and thus negligible compared to the expected time to compute the HNF.

To compute $A_{\mathbb{R}}$, we need to compute the transformation matrix and extract kernel vectors from it. This has expected time bounded by (8). It provides $K_1 N$ vectors $\vec{u}_j \in \mathbb{Z}^{N+K_1N}$ representing linear dependencies between the rows of $M_{\mathbb{Z}}$. Applying those linear combinations to the rows of M yields K_1N relations with zero coefficients on the first N coordinates. We denote by $\mathcal{L}_{\mathbb{R}}$ the lattice of the relations having only zeros on their first N coordinates. As we assume Heuristic 2, these K_1N relations generate $\mathcal{L}_{\mathbb{R}}$. The last r coordinates of each of the K_1N relations created this way are added as a row vector to the matrix $A_{\mathbb{R}}$. Note here that we drop the last Archimedian valuation of our units since we need the determinant of a $r \times r$ minor to compute the regulator. In addition, for every $\vec{u}_j$ of the form

$$\vec{u}_j = (u_j^{(1)}, \ldots, u_j^{(N+K_1N)}),$$

and for all $j \leq K_1N$, the value $\beta_j = \prod_i \phi_i^{u_j^{(i)}}$ is the unit corresponding to the row

$$\mathbf{r}_j^{A_{\mathbb{R}}} = \sum_i u_j^{(i)} \mathbf{r}_i^M.$$

As we will see in §6, the coefficients $u_j^{(i)}$ are too large to allow us to compute directly β_j in subexponential time. We thus give the units β_j in compact representation, that is to say by storing the $\vec{u}_j$.

Corollary 10. *The complexity of the computation of the kernel of $M_{\mathbb{Z}}$ and of the structure of $\mathrm{Cl}(\mathbb{Z}[\theta])$ is bounded by*

$$L_{\Delta_f}\left(1/3, 5\rho + o(1)\right).$$

We postpone the study of the complexity of the computation of $A_{\mathbb{R}}$ to §5.3 since it depends on the precision we choose for the rational approximations of the $\log|\phi_i|_j$, which is discussed in §5.2. In the following, we will need bounds on $|\vec{u}_j|$ and on $|A_{\mathbb{R}}|$. The size of the entries of $U_{\mathbb{Z}}$ derive from the analysis of the HNF algorithm of [14] and is bounded by

$$O\left((N + K_1N)\log\left(\sqrt{N + K_1N}|M_{\mathbb{Z}}|\right)\right),$$

which allows us to state the following lemma.

Lemma 11. *$|\vec{u}_j|$ and $|A_{\mathbb{R}}|$ satisfy:*

$$\log|\vec{u}_j| = L_{\Delta_f}(1/3, \rho + o(1))$$
$$\log|A_{\mathbb{R}}| = L_{\Delta_f}(1/3, \rho + o(1)).$$

Before discussing the computation of R and a system of fundamental units, we address the issue of the complexity of the computation of h^*. This can be done in polynomial time when $f = 1$, but in the general case, it is a non-trivial computation whose bottleneck is the factorization of f.

Proposition 12. *The computation of h^* can be done in expected time bounded by*

$$L_{\Delta_f}(1/3, \sqrt[3]{64/9} + o(1)).$$

Proof. We use the fact that

$$\frac{h(\mathbb{Z}[\theta])R(\mathbb{Z}[\theta])}{h(\mathcal{O}_{\mathbb{K}})R(\mathcal{O}_{\mathbb{K}})} = \frac{\#(\mathcal{O}_{\mathbb{K}}/\mathfrak{f})^*}{\#(\mathbb{Z}[\theta]/\mathfrak{f})^*}.$$

We first compute a factorization of $f \leq \sqrt{\Delta_f}$, which can be achieved in heuristic complexity bounded by

$$L_{\Delta_f}(1/3, \sqrt[3]{64/9} + o(1)),$$

by using the number field sieve. Then we compute the maximal order $\mathcal{O}_{\mathbb{K}}$ in polynomial time [7] from the factorization of f, and an approximation of $h(\mathcal{O}_{\mathbb{K}})R(\mathcal{O}_{\mathbb{K}})$ in polynomial time by the means of [3]. Finally, we use the fact that for an order $\mathcal{O} \subseteq \mathcal{O}_{\mathbb{K}}$,

$$\begin{aligned}(\mathcal{O}/\mathfrak{f})^* &\simeq \prod_{\mathfrak{p}|\mathfrak{f}} (\mathcal{O}_{\mathfrak{p}}/\mathfrak{f}\mathcal{O}_{\mathfrak{p}})^* \\ &\simeq \prod_{\mathfrak{p}|\mathfrak{f}} (\mathcal{O}/\mathfrak{p})^* \times \left((1+\mathfrak{p})/(1+\mathfrak{f}+\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{f})})\right)^+,\end{aligned}$$

where $\mathcal{O}_{\mathfrak{p}}$ denotes the localization at $\mathfrak{p}$, $v_{\mathfrak{p}}(\mathfrak{f})$ denotes the valuation of $\mathfrak{f}$ at $\mathfrak{p}$, and G^+ denotes the additive group G. We can thus state that

$$\#(\mathcal{O}/\mathfrak{f})^* = \prod_{\mathfrak{p}|\mathfrak{f}} \left(\mathcal{N}_{\mathcal{O}/\mathbb{Q}}(\mathfrak{p}) - 1\right) \frac{\mathcal{N}_{\mathcal{O}/\mathfrak{p}}(\mathfrak{f}+\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{f})})}{\mathcal{N}_{\mathcal{O}/\mathbb{Q}}(\mathfrak{p})}.$$

This allows us to compute $\#(\mathcal{O}_{\mathbb{K}}/\mathfrak{f})^*$ and $\#(\mathbb{Z}[\theta]/\mathfrak{f})^*$ in polynomial time since the norms of the $\mathfrak{p}$ and of $\mathfrak{f}$ are bounded by $O(|\Delta_f|)$, $\mathcal{N}_{\mathcal{O}/\mathbb{Q}}(\mathfrak{f}+\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{f})}) \leq \mathcal{N}_{\mathcal{O}/\mathbb{Q}}(\mathfrak{f})$ and the number of $\mathfrak{p}$ dividing $\mathfrak{f}$ is bounded by $O(\log(|\Delta_f|))$. □

5. The computation of $R(\mathbb{Z}[\theta])$ a system of fundamental units

In this section, we discuss the computation of $R(\mathbb{Z}[\theta])$ and of a system of fundamental units in compact representation. We start by giving the description of the algorithm, and then we focus on the approximation issues. Indeed, the matrix $M_{\mathbb{R}}$ contains rational approximations of real numbers, and the linear algebra steps leading to $R(\mathbb{Z}[\theta])$ and a system of fundamental units gradually deteriorate the precision. In the last part of this section, we show that the required original precision for the $\log(\alpha)$ during the creation of the relation matrix is low enough to keep the complexity below $L_{\Delta_f}(1/3, O(1))$.

5.1. **Description of the algorithm.** Our approach resembles the one of the computer algebra software Pari [9]. To compute the regulator and a system of fundamental units, we have to find a set of r row vectors that span $\mathcal{L}_\mathbb{R}$. To do that, we first find a set of r independent rows of $A_\mathbb{R}$, and call $A \in \mathbb{R}^{r\times r}$ the matrix corresponding to these rows. All the rows of $A_\mathbb{R}$ are in the $\mathbb{Q}$-vector space generated by the rows of A. Therefore, there exists $B \in \mathbb{Q}^{K_1N\times r}$ such that $BA = A_\mathbb{R}$. This matrix is given by $A_\mathbb{R}A^{-1}$. As we only know rational approximations of A and $A_\mathbb{R}$, we need to perform a rational roundoff via the continued fraction expansion of the coefficients of B to recover their exact values. This method is described and analyzed in [28]. Let Q_{com} be the lowest common multiple of the denominators of the entries of B. The value Q_{com} divides the index of the lattice spanned by the rows of A in $\mathcal{L}_\mathbb{R}$. We compute the Hermite Normal Form H_B of $Q_{\text{com}}B \in \mathbb{Z}^{K_1N\times r}$, along with $U \in \mathrm{GL}_{K_1N\times K_1N}$ such that

$$U \cdot Q_{\text{com}}B = \begin{pmatrix} H_B \\ \cdots\cdots\cdots \\ (0) \end{pmatrix}.$$

Note that this computation is exact since the rational roundoff returns the exact matrix B. The first r rows of U give us the invertible linear combinations of rows of $A_\mathbb{R}$ leading to a $\mathbb{Z}$-basis of $\mathcal{L}_\mathbb{R}$. In the meantime, U contains the information required to compute fundamental units as power-products of the β_i, $i \leq K_1N$.

Algorithm 2 Computation of the regulator and of a system of fundamental units

Input: $A_\mathbb{R}$ and the corresponding units β_i
Output: R and a system of fundamental units $\gamma_1, \ldots, \gamma_r$

1: Use Algorithm 3 to find r linearly independent rows. Let A be the corresponding $r \times r$ matrix.
2: $B \leftarrow A_\mathbb{R}A^{-1}$
3: Perform a rational roundoff on the entries of B with the methods of [28] to recover their exact values.
4: Let Q_{com} be the lowest common multiple of the entries of B
5: $H_B \leftarrow \mathrm{HNF}(Q_{\text{com}}B)$. Let $U \in \mathrm{GL}_{K_1N\times K_1N}$ and $B_\mathbb{R} \in \mathbb{Q}^{r\times r}$ such that

$$U \cdot Q_{\text{com}}B = \begin{pmatrix} H_B \\ \cdots\cdots\cdots \\ (0) \end{pmatrix} \quad \text{and} \quad U \cdot A_\mathbb{R} = \begin{pmatrix} B_\mathbb{R} \\ \cdots\cdots\cdots \\ (0) \end{pmatrix}.$$

6: **for** $1 \leq i \leq r$ **do**
7: $\quad \gamma_i \leftarrow \beta_1^{u_{1,i}} \cdots \beta_{K_1N}^{u_{K_1N,i}}$
8: **end for**
9: $R(\mathbb{Z}[\theta]) \leftarrow \det(B_\mathbb{R})$

Algorithm 2 returns R and a system of fundamental units. Its first step is a call to Algorithm 3 which returns r independent rows of $A_\mathbb{R}$ to ensure that the first determinant computed is not zero. Whenever $\det(A_i^tA_i) \neq 0$, we have i linearly independent rows. The validity of this test depends on the precision of our approximations. We discuss this in § 5.2, where we give a bound on $\det(A_i^tA_i)$ that depends on the precision of our rational approximations of the generators ϕ_j, $j \leq N+K_1N$. We also postpone the computation of the complexity of Algorithms 2

Algorithm 3 Search for r independent rows

Input: $A_{\mathbb{R}}$
Output: A permutation of the rows of $A_{\mathbb{R}}$ such that the first r are independent

$A_1 \leftarrow \mathbf{r}_1^{A_{\mathbb{R}}}$
$i \leftarrow 1$
for $i = 2$ to r **do**
  $m \leftarrow i$
  ret $\leftarrow 0$
  while ret $= 0$ **do**

$$A_i \leftarrow \begin{pmatrix} A_{i-1} \\ \cdots\cdots\cdots \\ \mathbf{r}_m^{A_{\mathbb{R}}} \end{pmatrix}.$$

    if $\det(A_i^t A_i) = 0$ **then**
      $m \leftarrow m + 1$
    else
      Swap $\mathbf{r}_i^{A_{\mathbb{R}}}$ and $\mathbf{r}_m^{A_{\mathbb{R}}}$
      ret $\leftarrow 1$
    end if
  end while
end for

and 3 to § 5.3, after calculating in § 5.2 the precision we have to take for the rational approximations of the logarithms.

5.2. **Approximation issues.** The matrix $M_{\mathbb{R}}$ contains fixed point rational approximations $\hat{x_{ij}}$ of the logarithms of the units $x_{ij} := \log|\phi_i|_j$. In this section, we discuss the precision loss during the computation of the regulator, which is the major difference between the contexts of number fields and algebraic curves. In the following, we count the precision in bits. We say that $\hat{x}$ is a rational approximation of $x \in \mathbb{R}$ with precision q if $|\hat{x} - x| < 2^{-q}$. We assume that $M_{\mathbb{R}}$ is computed at precision q_0, that is, its entries $\hat{x_{ij}}$ for $i \leq N + K_1 N$ and $j \leq r + 1$ are given by expansions

$$\hat{x_{ij}} = \sum_{k=-q_0}^{\lceil \log|x_{ij}| \rceil} 2^k a_k^{ij},$$

where the a_k^{ij} are the coefficients of the representation of x_{ij} as $\sum_{k=-\infty}^{\infty} 2^k a_k^{ij}$. Before establishing the list of the steps where we might loose precision, we give in Lemma 13 the basic properties that we will use to estimate the loss of precision whenever we add or multiply rational approximations:

Lemma 13. *Let $\hat{x}$ and $\hat{y}$ be rational approximations of precision q_1 of respectively x and y, and $u \in \mathbb{Z}$ such that $\lceil \log_2 u \rceil = q_2 < q_1$, then*

- *$\hat{x} + \hat{y}$ is a rational approximation of $x + y$ of precision $q_1 - 1$.*
- *$u\hat{x}$ is a rational approximation of ux of precision $q_1 - q_2$.*
- *$\hat{x}\hat{y}$ is an approximation of xy of precision $q_1 - \log_2(|x| + |y|) - 1$.*

- *If* $\exists c > 0$ *such that* $|y| \geq c$ *and* $qc \gg 1$*, then* $\frac{\hat{x}}{\hat{y}}$ *is a rational approximation of* $\frac{x}{y}$ *of precision* $q - \log_2\left(|x| + \frac{1}{|y|}\right) - 1$.

Let q_0 be the precision taken for the approximation of the $\log|\phi_i|_j$. Let us enumerate the steps in the algorithm that reduce the precision. The first source of error is the computation of the coefficients of the matrix $A_{\mathbb{R}}$. Indeed, it contains rational approximations of

$$\sum_{i=1}^{N+K_1N} u_j^{(i)} \log|\phi_i|_j,$$

for $j = 1, \ldots, K_1N$. The loss of precision is due to the multiplications by the $u_j^{(i)}$ and to the $N+K_1N$ additions. We deduce from Lemma 11 the following proposition that gives us the loss of precision occurring in the computation of the coefficients of $A_{\mathbb{R}}$ with respect to the original precision taken during the construction of M:

Proposition 14. *The computation of* $\sum_i u_j^{(i)} \log|\phi_i|_j$ *for* $j = 1, \ldots, r$*, with precision* q'*, requires that the precision* q_0 *of the* $\log|\phi_i|_j$ *be*

$$q' + N + K_1N + \max_{i,j}\left\{\log_2|u_j^{(i)}|\right\}.$$

Proof. Multiplying $\log|\phi_i|_j$ by $u_j^{(i)}$ induces a loss of $\log_2|u_j^{(i)}|$ bits of precision. Furthermore every addition induces the loss of one bit of precision. As we perform $N+K_1N$ of them, we thus loose another $N+K_1N$ bits of precision. Consequently, the total loss of precision is bounded from above by

$$N + K_1N + \max_{i,j}\left\{\log_2|u_j^{(i)}|\right\}.$$

□

Once $A_{\mathbb{R}}$ is obtained, we need to compute determinants of matrices of the form $A_i^t A_i$ where A_i is extracted from $A_{\mathbb{R}}$. Every computation of such a determinant induces a loss of precision, and augments the risks of failure of Algorithm 3 due to rounding errors. The following proposition allows us to evaluate the loss of precision for one computation of an $k \times k$ determinant of a matrix $\hat{\Omega} \in \mathbb{R}^{k\times k}$.

Proposition 15. *The computation with precision* q'' *of the determinant of an* $k\times k$ *matrix* $\hat{\Omega}$ *which is a rational approximation of* $\Omega \in \mathbb{R}^{k\times k}$*, requires that*

$$q' = q'' + (k/2+1)\log_2(k)\log_2\left(|\Omega|^{k-1}+1\right),$$

where q' *is the precision of the coefficients of* $\hat{\Omega}$.

Proof. We know that $\Omega = (\omega_1, \ldots, \omega_k)$ and $\hat{\Omega} = (\hat{\omega_1}, \ldots, \hat{\omega_k})$ are $k\times k$ matrices with $|\Omega - \hat{\Omega}| \leq 2^{-q}$. We have by multilinearity of the determinant and by Hadamard's inequality:

$$\begin{aligned}|\det\hat{\Omega} - \det\Omega| &= \left|\sum_{i=1}^{k}\det(\omega_1, \ldots, \omega_{i-1}, \hat{\omega}_i - \omega_i, \hat{\omega}_{i+1}, \ldots, \hat{\omega}_k)\right| \\ &\leq r^{r/2+1}(|\Omega|^{r-1}+1)2^{-q}.\end{aligned}$$

Thus, the loss of precision is

□ $$(k/2+1)\log_2(k)\log_2\left(|\Omega|^{k-1}+1\right).$$

We use this property to calculate the loss of precision encountered during the search for independent rows in Algorithm 3. This loss comes from the computations of $\det(A_i^t A_i)$ for $i \leq r$.

Proposition 16. *The computation with precision q'' of $\det(A_i^t A_i)$ for $i \leq r$ requires that*

$$q' = q'' + \left(\frac{i}{2} + 1\right) \log_2(i) \log_2((r|A_{\mathbb{R}}|^2)^{i-1} + 1) + \log_2(2|A_{\mathbb{R}}|) + (1 + r),$$

where q' is the precision of the coefficients of $A_{\mathbb{R}}$.

Proof. First, we calculate the precision of the $A_i^t A_i$. The coefficients $c_{kl}^{(i)}$ $(k, l \leq i)$ of $A_i^t A_i$ are given by

$$c_{kl}^{(i)} = \sum_{h \leq r} a_{kh}^{(i)} a_{lh}^{(i)},$$

where the $a_{kl}^{(i)}$ $(k \leq i,\ l \leq r)$ are the coefficients of A_i. Therefore, the loss of precision occurring during the computation of $A_i^t A_i$ is bounded by

$$\log_2(2|A_{\mathbb{R}}|) + (1 + r).$$

By using Proposition 15, we prove that the loss of precision we encounter during the determinant computation is of

$$(i/2 + 1) \log_2(i) \log_2\left(|A_i^t A_i|^{i-1} + 1\right) \leq \left(\frac{i}{2} + 1\right) \log_2(i) \log_2((r|A_{\mathbb{R}}|^2)^{i-1} + 1).$$

□

We also lose precision during the computation of B from A^{-1}. As A contains rational approximations of $\log |\beta_i|_j$, its inverse might substantially differ from the inverse of the corresponding matrix in $\mathbb{R}^{r \times r}$. To make sure we can analyze this loss of precision, we invert A by solving r linear systems using Cramer's rule.

Proposition 17. *The computation with precision q'' of $B := A_{\mathbb{R}} A^{-1}$ requires that*

$$q'' = q' + \left(r\left(\frac{r}{2} + 1\right) \log_2(r) + 2r\right) \log_2 |A_{\mathbb{R}}| + r \log_2(r) + 2r + S1 + \log_2(10),$$

where q' is the precision of $A_{\mathbb{R}}$.

Proof. We first assess the precision of A^{-1}. The column j of A^{-1} is obtained by solving

$$AX_j = e_j := (0, \ldots, 0, 1, 0, \ldots, 0)^t.$$

Therefore, by Cramer's rule, the coefficient at index (i, j) of A^{-1} is given by $\det(A_{i,j})/\det(A)$, where $A_{i,j}$ is the matrix obtained by replacing the j-th column of A by e_i. By Proposition 15, $\det(A)$ and $\det(A_{i,j})$ are known with precision

$$q' - (r/2 + 1) \log_2(r) \log_2(|A_{\mathbb{R}}|^{r-1} + 1).$$

As we know that $\det(A)$, which is a multiple of the regulator, is larger than 0.2, we thus have by Lemma 13 the loss of

$$\log_2\left(|\det(A_{i,j})| + \frac{1}{|\det(A)|}\right) \leq \log_2(|\det(A_{i,j})| + 5) \leq r \log_2 |A_{\mathbb{R}}| + \frac{r}{2} \log_2(r) + 1$$

bits of precision during the computation of $\det(A_{i,j})/\det(A)$.
Finally, the computation of the matrix product $A_{\mathbb{R}}A^{-1}$ induces the loss of $r + (\log_2(|A_{\mathbb{R}}| + |A^{-1}|)) + 1$ bits of precision. Each coordinate $a_{i,j}^{-1}$ of A^{-1} satisfies

$$|a_{i,j}^{-1}| \leq \left|\frac{\det(A_{i,j})}{\det A}\right| \leq \frac{|\det(A_{i,j})|}{0.2} \leq 5\left(r^{r/2}|A_{\mathbb{R}}|^r\right).$$

Therefore, the loss of precision induced by the computation of the matrix product $A_{\mathbb{R}}A^{-1}$ is bounded by

$$\begin{aligned} 1 + r + \log_2(2|A^{-1}|) &\leq \log_2(10r^{r/2}|A_{\mathbb{R}}|^r) + r + 1 \\ &= \log_2(10) + \frac{r}{2}\log_2(r) + r\log_2|A_{\mathbb{R}}| + r + 1. \end{aligned}$$

□

The last loss of precision occurs during the computation of the regulator. We first need to compute $B_{\mathbb{R}}$ from $A_{\mathbb{R}}$ and U, and then take its determinant.

Proposition 18. *The computation of $B_{\mathbb{R}}$ with precision q'' requires that*

$$q' = q'' + K_1N + 1 + (2r^2 + r + 1)\log_2|A_{\mathbb{R}}| + r\log_2(25) + \left(r^2 + \frac{3r}{2}\right),$$

where q' is the precision of the coefficients of $A_{\mathbb{R}}$.

Proof. As in the proof of Lemma 11, we have $|U| \leq (\sqrt{r}|Q_{\mathrm{com}}B|)^r$. From the proof of Proposition 17, we know that $|A^{-1}| \leq 5\left(r^{r/2}|A_{\mathbb{R}}|^r\right)$. Therefore, B satisfies

$$|B| \leq 5\left(r^{r/2+1}|A_{\mathbb{R}}|^{r+1}\right).$$

In addition, the common denominator Q_{com} of the coefficient s of B is bounded by the index of the sublattice generated by the rows of A in $\mathcal{L}_{\mathbb{R}}$. It thus satisfies

$$Q_{\mathrm{com}} \leq \frac{\det(A)}{R} \leq \frac{r^{r/2}|A_{\mathbb{R}}|^r}{0.2}.$$

We can thus conclude that $|Q_{\mathrm{com}}B| \leq 25r^{r+1}|A_{\mathbb{R}}|^{2r+1}$ and

$$|U| \leq \left(\sqrt{r}25r^{r+1}|A_{\mathbb{R}}|^{2r+1}\right)^r.$$

The result follow from the fact that the loss of precision during the product of $K_1N \times K_1N$ matrices is bounded by

$$K_1N + 1 + \log_2(|A_{\mathbb{R}}| + |U|) \leq K_1N + 1 + \log_2|A_{\mathbb{R}}| + \log_2|U|.$$

□

Corollary 19. *The computation of the regulator with precision q'' requires that*

$$\begin{aligned} q' = q'' &+ \left(\frac{r}{2} + 1\right)\log_2(r)\log_2\left(|B_{\mathbb{R}}|^{r-1} + 1\right) \\ &+ K_1N + 1 + (2r^2 + r + 1)\log_2|A_{\mathbb{R}}| + r\log_2(25) + \left(r^2 + \frac{3r}{2}\right), \end{aligned}$$

where q' is the precision of the coefficients of $A_{\mathbb{R}}$ and $|B_{\mathbb{R}}| \leq r|A_{\mathbb{R}}||U|$.

Corollary 20. *The total loss of precision during the overall algorithm is dominated by the computation of $B_{\mathbb{R}}$. This loss is bounded by*

$$\begin{aligned}
&N + K_1 N + \max_{i,j}\left\{\log_2 |u_j^{(i)}|\right\} \\
&+ K_1 N + 1 + (2r^2 + r + 1)\log_2 |A_{\mathbb{R}}| + r\log_2(25) + \left(r^2 + \frac{3r}{2}\right) \\
&+ r\left(\frac{r}{2} + 1\right)\log_2(r)\left(\left(r^2 + \frac{3r}{2} + 1\right)\log_2(r) + (2r^2+1)\log_2 |A_{\mathbb{R}}| + r\log_2(25)\right)
\end{aligned}$$

We can derive from this bound on the loss of precision an algorithm for the computation of the regulator with a desired precision q_R . Indeed, all we have to do is to compute an upper bound on $\log_2 |M_{\mathbb{R}}|$ using $\max_{i,j}\{\lfloor \log |\phi_i|_j \rfloor\}$. Then, as coefficients of $A_{\mathbb{R}}$ are scalar products of kernel elements and columns of $(\log |\phi_i|_j)$, we have

$$\begin{aligned}
\log_2 |A_{\mathbb{R}}| &\leq \log_2\left((N + K_1 N)\max_{i,j}\left\{|u_j^{(i)}|\right\}\max_{i,j}\{\log |\phi_i|_j\}\right) \\
&\leq \log_2\left((1+K_1)N\right) + \max_{i,j}\left\{\log_2 |u_j^{(i)}|\right\} + \max_{i,j}\{\log_2 \lfloor \log |\phi_i|_j \rfloor\} =: z. \qquad (9)
\end{aligned}$$

The simplify the mathematical expressions involving the overall loss of precision, we define the function

$$\begin{aligned}
f(r,z) := 1 + r\log_2(25) + \left(r^2 + \frac{3r}{2}\right)\log_2(r) + (2r^2 + r + 1)z \\
+ r\left(\frac{r}{2} + 1\right)\log_2(r)\left(\left(r^2 + \frac{3r}{2} + 1\right) + (2r^2+1)z + r\log_2(25)\right).
\end{aligned}$$

Algorithm 4 summarizes this procedure. As we will see in Proposition 21, we need that the precision be significantly larger than $n\log(n)(1 + o(1))$ during the course of the algorithm. We want the precision of the values we manipulate as small as possible, and as from Corollary 20, and we know that given our loss of precision we have to deal with fixed point approximations of precision at least $L_{\Delta_f}(1/3, \rho + o(1))$. In addition, we need the precision to be at least $L_{\Delta_f}(1/3, 2\rho + o(1))$ throughout the algorithm to ensure the success of the roundoff procedure as we see in §5.3. We thus assume that we seek the regulator at a precision of $q_R = L_{\Delta_f}(1/3, 2\rho + o(1))$.

Algorithm 4 Computation of the ideal class group and the regulator with desired precision q_R

Input: $q_R = L_{\Delta_f}(1/3, 2\rho + o(1))$
Output: $h(\mathcal{O}_\mathbb{K})$, the structure of $\mathrm{Cl}(\mathcal{O}_\mathbb{K})$, $R(\mathbb{Z}[\theta])$ at precision q_R, and a system of fundamental units

1: Find the relation matrix $M_\mathbb{Z}$.
2: Compute the HNF of $M_\mathbb{Z}$
3: Compute the SNF of $M_\mathbb{Z}$ and deduce $h(\mathcal{O}_\mathbb{K})$ and the group structure of $\mathrm{Cl}(\mathcal{O}_\mathbb{K})$
4: Compute a basis $(\vec{u}_j)_{j \leq K_1 N}$ of $\ker M_\mathbb{Z}$ and z with (9)
5: Compute $q_0 := q_R + (2K_1 + 1)N + \max_{i,j} \left\{ \log_2 |u_j^{(i)}| \right\} + f(r, z)$.
6: Compute $M_\mathbb{R}$ with precision q_0
7: Compute $A_\mathbb{R}$
8: Compute $R(\mathbb{Z}[\theta])$ and a system of fundamental units in compact representation with Algorithm 2.
9: Compute h^* and check if $h^* \leq h(\mathcal{O}_\mathbb{K})R(\mathbb{Z}[\theta]) < 2h^*$. If not, go back to step 1

The last approximation issue we need to handle is the validity of Algorithm 3. Indeed, at Step 8 of Algorithm 3, we need to determine whether $\det(A_i^t A_i)$ is the approximation of a null determinant or not. If our approximations are not accurate enough, this test could give the wrong answer and cause Algorithm 3 to fail. We use Minkowski's bound, which states that

$$\sqrt{\det A_i^t A_i} \geq \left(\frac{\|b_1^{(i)}\|_2}{\sqrt{r}} \right)^r, \tag{10}$$

where $b_1^{(i)}$ is the non-zero vector of minimal length in the lattice spanned by the rows of A_i. For every i, the first minima $b_1^{(i)}$ is the vector $(|\epsilon|_i)_{i \leq r}$ of a unit ϵ. In [12], it is shown that for every unit ϵ that is not a root of unity, we have

$$\left(\sum_i \log |\epsilon|_i^2 \right)^{1/2} > \frac{21}{128} \frac{\log n}{n^2}. \tag{11}$$

Therefore, we can prove the following proposition:

Proposition 21. *The precision $q_0 = L_{\Delta_f}(1/3, \rho + o(1))$ is accurate enough to ensure the validity of Algorithm 3.*

Proof. For every $i \leq r$, we have the value of $\det(A_i^t A_i)$ with a precision q satisfying

$$q = L_{\Delta_f}(1/3, \rho + o(1)).$$

On the other hand, we have a lower bound on the value of $\det(A_i^t A_i)$ from the combination of (10) and (11) in the case where A_i contains approximations of independent rows:

$$\det(A_i^t A_i) \geq \left(\frac{21}{128} \right)^{2r} \frac{1}{r^r} \left(\frac{\log n}{n^2} \right)^{2r}.$$

Furthermore, the bound on $\det(A_i^t A_i)$ satisfies

$$\left| \log \left[\left(\frac{21}{128} \right)^{2r} \frac{1}{r^r} \left(\frac{\log n}{n^2} \right)^{2r} \right] \right| \leq n \log(n)(1 + o(1)) \ll q.$$

We can thus conclude that if $\det(A_i^t A_i) \leq 1/2^q$, then the rows of A_i are necessarily dependent. □

5.3. **Complexity.** Computing $R(\mathbb{Z}[\theta])$ and a system of fundamental units involve manipulating rational approximations of real numbers. In §5.2, we gave bounds on the precision of these approximations, and thus on the size of the integers that occur during the computation of $R(\mathbb{Z}[\theta])$ and a system of fundamental units. In this section, we show that these numbers are small enough to keep the complexity bounded by $L_{\Delta_f}(1/3, O(1))$. The first step of our complexity analysis concerns the creation of $M_{\mathbb{R}}$. We gave in Corollary 6 a bound on the complexity of the relation search which does not allow us directly to quantify the effort required to compute $M_{\mathbb{R}}$. Indeed we need to compute approximation of the ϕ_i, $i \leq N+K_1N$ at precision $q_0 = L_{\Delta_f}(1/3, 2\rho + o(1))$.

Proposition 22. *The computation of $M_{\mathbb{R}}$ at precision $q_0 = L_{\Delta_f}(1/3, \rho + o(1))$ has complexity bounded by*

$$L_{\Delta_f}(1/3, 3\rho + o(1)).$$

Proof. The computation of $\hat{x_{ij}}$ for each $i \leq N + K_1N$ and $j \leq r + 1$ has bit complexity bounded by $\tilde{O}(\mathrm{M}(q_0')) = O\left(L_{\Delta_f}(1/3, \rho + o(1))\right)$ bit operations [4]. As we have to perform this computation

$$r(N + K_1N) = L_{\Delta_f}(1/3, \rho + o(1))$$

times, the time taken for the creation of $M_{\mathbb{R}}$ is bounded by $L_{\Delta_f}(1/3, 3\rho + o(1))$. □

In §4.2, we could not calculate the complexity of the computation of $A_{\mathbb{R}}$ since we did not know the size of the entries of $M_{\mathbb{R}}$.

Proposition 23. *The complexity of the computation of $A_{\mathbb{R}}$ is bounded by*

$$L_{\Delta_f}(1/3, 4\rho + o(1)).$$

Proof. We know from Corollary 4 that $\log |\phi_i|_j = O((\log |\Delta_f|)^{2/3} (\log\log |\Delta_f|)^{1/3})$. In addition, the precision q_0 is bounded by $L_{\Delta_f}(1/3, 2\rho + o(1))$. Therefore, the bit size q_0' required to store the $\hat{x_{ij}}$ is at most $L_{\Delta_f}(1/3, 2\rho + o(1))$. From Lemma 11, we also know that $\log |\vec{u}_j| = L_{\Delta_f}(1/3, \rho + o(1))$, thus the computation of every entry of $A_{\mathbb{R}}$ is an inner product of vectors of fixed point rational approximations of bit size bounded by $L_{\Delta_f}(1/3, 2\rho + o(1))$ and of length $N + K_1N = L_{\Delta_f}(1/3, \rho + o(1))$. As $A_{\mathbb{R}}$ has $r(N + K_1N)$ entries, the total complexity of its computation is bounded by

$$r(N + K_1N)^2 \,\mathrm{M}(q_0') \leq L_{\Delta_f}(1/3, 4\rho + o(1)).$$

□

Let us now estimate the complexity of Algorithm 3. It involves computing products of matrices extracted from $A_{\mathbb{R}}$ and computing their determinant. As we know a bound on the entries of $A_{\mathbb{R}}$ and on their precision, we can deduce the effort required to compute arithmetic operations involving entries of $A_{\mathbb{R}}$.

Proposition 24. *The complexity of Algorithm 3 is bounded by*

$$L_{\Delta_f}(1/3, 2\rho + o(1)).$$

Proof. The entries of $A_{\mathbb{R}}$ are fixed point approximations of linear combinations of the $\log |\phi_i|_j$ with precision $q = L_{\Delta_f}(1/3, 2\rho + o(1))$. We also know from Lemma 11 that

$$\log_2 |A_{\mathbb{R}}| = L_{\Delta_f}(1/3, \rho + o(1)).$$

During Algorithm 3, we need to compute the product $A_i^t A_i$, where A_i is a submatrix of $A_{\mathbb{R}}$ of dimensions at most $r \times r$. As in the proof of Proposition 22, we can prove that the complexity of the computation of $A_i^t A_i$ is bounded by

$$\tilde{O}\left(r^3 \,\mathrm{M}(\log |A_{\mathbb{R}}| + q)\right) = L_{\Delta_f}(1/3, \rho + o(1)).$$

According to Proposition 16, the precision q' of $A_i^t A_i$ satisfies $q' = L_{\Delta_f}(1/3, 2\rho + o(1))$. We also have that $\log_2 |A_i^t A_i| = L_{\Delta_f}(1/3, \rho + o(1))$. By multilinearity, the computation of the determinant of $A_i^t A_i$ boils down to the computation of the determinant of $2^{rq'} A_i^t A_i \in \mathbb{Z}^{r \times r}$ whose entries have bit size bounded by $q' + \log_2 |A_i^t A_i|$. The complexity of the deterministic computation of the determinant of $|A_i^t A_i|$ is bounded by

$$O(r^{1+\omega}(\log_2 |A_i^t A_i| + q')^{1+o(1)}) \leq L_{\Delta_f}(1/3, 2\rho + o(1)),$$

where $2 < \omega \leq 3$ is the exponent such that matrix multiplication can be done in $O(n^\omega)$ (see [26]). As the exponent of r does not impact the overall complexity, we did not consider probabilistic methods for the computation of the determinant since it would require to discuss its probability of success. □

The last part of the regulator and units computation is Algorithm 2, which starts with the computation of $B = A_{\mathbb{R}} A^{-1}$, where $A \in \mathbb{Q}^{r \times r}$ is the output of Algorithm 3.

Proposition 25. *The computation of B has bit complexity bounded by*

$$L_{\Delta_f}(1/3, 2\rho + o(1)).$$

Proof. To compute A^{-1}, we proceed as in the proof of Proposition 17. The entries of A^{-1} are quotients of $r \times r$ determinants of the matrices A and $A_{i,j}$ whose entries bounded by $|A_{\mathbb{R}}|$ and given at precision

$$q = L_{\Delta_f}(1/3, 2\rho + o(1)).$$

Therefore, we can compute $\det(A)$ and $\det(A_{i,j})$ in expected time bounded by $O(r^{1+\omega}(\log_2 |A_{\mathbb{R}}| + q)^{1+o(1)}) \leq L_{\Delta_f}(1/3, \rho + o(1))$. From Hadamard's inequality, $\det(A)$ and $\det(A_{i,j})$ are bounded by

$$(\sqrt{r}|A_{\mathbb{R}}|)^r.$$

Therefore, the division $\det(A)/\det(A_{i,j})$ can be done in bit complexity bounded by

$$\tilde{O}\left(\mathrm{M}\left(r\left(\log_2\left(\sqrt{r}|A_{\mathbb{R}}|\right) + q\right)\right)\right) \leq L_{\Delta_f}(1/3, 2\rho + o(1)).$$

To compute A^{-1}, we need to repeat this operation r^2 times, which has complexity bounded by

$$L_{\Delta_f}(1/3, 2\rho + o(1)).$$

We know from the proof of Proposition 17 that

$$\log_2 |A^{-1}| \leq L_{\Delta_f}(1/3, \rho + o(1)).$$

The precision of $A_{\mathbb{R}}$ and A^{-1} is bounded by $L_{\Delta_f}(1/3, 2\rho + o(1))$. We proceed as in the proof of Proposition 23 to deduce that the computation of $B = A_{\mathbb{R}}A^{-1}$ has complexity bounded by

$$L_{\Delta_f}(1/3, 2\rho + o(1)).$$

□

Now, let us calculate the complexity of the rational roundoff. In [28], it is proved that given a rational number $\alpha = n/m$, and a natural number k, we can find, if it exists, a rational number p_α/q_α such that $1 \leq q \leq k$ and $|\alpha - p_\alpha/q_\alpha| < 1/(2k^2)$ in expected time bounded by

$$O\left(\log(m)(\log\log(m))^2 \log\log\log m\right).$$

If this solution exists, it is necessarily unique.

Proposition 26. *The computation of the rational roundoff of B is done in expected time bounded by*

$$L_{\Delta_f}(1/3, \rho + o(1)).$$

Proof. In our context, the P/Q that we need to recover are the coefficients of B for which we know a rational approximation with precision q larger than $L_{\Delta_f}(1/3, 2\rho + o(1))$. The common denominator Q_{com} of the coefficients of B is bounded by the index of the sublattice generated by the rows of A in $\mathcal{L}_{\mathbb{R}}$. It thus satisfies

$$Q_{\text{com}} \leq \frac{\det(A)}{R} \leq \frac{r^{r/2}|A_{\mathbb{R}}|^r}{0.2}.$$

By setting $k := 2^{\lceil (q-1/2)\rceil} \geq Q_{\text{com}}$, we have the desired result. □

We can now deduce the complexity of Algorithm 2.

Proposition 27. *The complexity of Algorithm 2 is bounded by*

$$L_{\Delta_f}(1/3, 4\rho + o(1)).$$

Proof. There are four remaining steps of Algorithm 2 to be analyzed, namely the computation of H_B, the computation of U, the product $UA_{\mathbb{R}}$, and the computation of $\det(B_{\mathbb{R}})$. As $Q_{\text{com}} \leq \frac{\det(A)}{R} \leq \frac{r^{r/2}|A_{\mathbb{R}}|^r}{0.2}$, and as $\log_2|B| \leq L_{\Delta_f}(1/3, \rho + o(1))$, the integer matrix $Q_{\text{com}}B$ has entries of size bounded by $L_{\Delta_f}(1/3, \rho + o(1))$. By using the HNF algorithm of [27], we can compute H_B in complexity bounded by

$$\tilde{O}\left(r^4 K_1 N(\log|Q_{\text{com}}B|)^2 + K_1 N r^3\, \mathrm{M}(\log(R))\right).$$

As $\log R \leq O(\log|\Delta_f|)$, we can conclude that the computation of H_B has complexity

$$L_{\Delta_f}(1/3, 3\rho + o(1)).$$

As we saw in § 4.2, we can recover U in complexity r^3, and $B_{\mathbb{R}}$ result from the product $UA_{\mathbb{R}}$ which can be done in complexity

$$\tilde{O}\left((K_1 N)^3 \max\{\log|U|, \log|A_{\mathbb{R}}|\}\right) \leq L_{\Delta_f}(1/3, 4\rho + o(1)).$$

Finally, $R = \det(B_{\mathbb{R}})$ takes $O(r^{1+\omega}(\log_2|B_{\mathbb{R}}| + q')^{1+o(1)}) \leq L_{\Delta_f}(1/3, 2\rho + o(1))$, where q' is the precision of $B_{\mathbb{R}}$. □

6. Subexponentiality

In this section, we show that we achieve a subexponential complexity for the overall running time of the algorithm and prove the main theorem of this paper, which we stated at the end of §2.

Theorem. *Let $\kappa > 0$ be a constant, and number fields of the form $\mathbb{K} = \mathbb{Q}(\theta)$ in $\mathcal{C}_\kappa$, then under the Generalized Riemann Hypothesis (GRH) and other heuristics specified in the next sections, the expected time for computing $\mathrm{Cl}(\mathbb{Z}[\theta])$, the regulator, and a system of fundamental units of $\mathbb{Z}[\theta]$ lies in*

$$L_{\Delta_f}(1/3, O(1)),$$

where f is the conductor of $\mathbb{Z}[\theta]$, and Δ_f is its discriminant.

From Corollary 6, we know that the expected number of principal ideals (ϕ) to be tested for smoothness is

$$L_{\Delta_f}\left(1/3, \frac{\kappa(\nu+\delta)}{3\rho} + o(1)\right).$$

On the other hand, the number of ϕ in the search space is bounded by $L_{\Delta_f}\left(1/3, \nu\delta\kappa + o(1)\right)$. We thus have the following constraint on the parameters

$$\nu\delta\kappa = \frac{\kappa(\nu+\delta)}{3\rho} + \rho. \tag{12}$$

As in [11], we can prove that the strategy minimizing the overall time (minus the time to factor f which does not depend on the parameters) is the one where the relation collection and the linear algebra take the same time.

Proposition 28. *If the expected running time of the linear algebra phase and the computation of the regulator and of a system of fundamental units is in*

$$L_{\Delta_f}(1/3, \Omega\rho + o(1)),$$

where $\Omega \geq 2$, then the optimal strategy is the one where the relation collection and the rest of the algorithm take the same time.

Proof. The overall expected running time for all the steps except the factorization of f is bounded by

$$L_{\Delta_f}\left(1/3, \frac{\kappa(\nu+\delta)}{3\rho} + \rho + o(1)\right) + L_{\Delta_f}(1/3, \Omega\rho + o(1))$$
$$= L_{\Delta_f}\left(1/3, \max\left\{\frac{\kappa(\nu+\delta)}{3\rho} + \rho, \Omega\rho\right\} + o(1)\right).$$

Let $f(\rho) := \frac{\kappa(\nu+\delta)}{3\rho} + \rho$. The optimal ρ that minimizes the relation collection time is the minimum of f, that is $\rho_0 := \sqrt{\frac{\kappa(\nu+\delta)}{3}}$. We have $f(\rho_0) = 2\rho_0$. If $\Omega \geq 2$, then the minimum of $\max\left\{\frac{\kappa(\nu+\delta)}{3\rho} + \rho, \Omega\rho\right\}$ is reached at the intersection of $y = \Omega\rho$ and $y = f(\rho)$, that is when ρ satisfies

$$\Omega\rho = \frac{\kappa(\nu+\delta)}{3\rho} + \rho.$$

□

As the the rest of the algorithm has its complexity dominated by the HNF computation which lies is $O(L(1/3, 5\rho + o(1)))$, we thus have the additional constraint

$$\kappa\nu\delta = 5\rho. \tag{13}$$

From (12) and (13), we obtain

$$\nu\delta = \frac{5\rho}{\kappa}$$
$$\nu + \delta = \frac{12\rho^2}{\kappa}.$$

Thus, δ and ν are roots of the polynomial

$$X^2 - \frac{24\rho^2}{\kappa}X + \frac{5\rho}{\kappa}.$$

These roots exist providing we have

$$\rho \geq \sqrt[3]{\frac{5\kappa}{144}}.$$

The optimal choice is to minimize ρ, thus fixing the parameters δ and ν

$$\delta = \nu = \sqrt{\frac{5\rho}{\kappa}} = \sqrt[6]{\frac{625}{144\kappa^2}}.$$

The total running time becomes $L\left(1/3, \max\left\{5\rho, \sqrt[3]{64/9})\right\} + o(1)\right)$, with

$$\rho = \sqrt[3]{\frac{5\kappa}{144}}.$$

7. Conclusion

We proved that under GRH and other assumptions, we can compute the structure of $\mathrm{Cl}(\mathbb{Z}[\theta])$ along with the regulator and a system of fundamental units of $\mathbb{Z}[\theta]$ in expected time bounded by

$$L\left(1/3, \max\left\{4\rho, \sqrt[3]{64/9})\right\} + o(1)\right),$$

with $\rho = \sqrt[3]{\frac{4\kappa}{81}}$, in certain infinite classes of number fields. This method was inspired by the one of Enge, Gaudry and Thomé [11] who described an $L(1/3)$ algorithm for computing discrete logarithms in the Jacobian of certain classes of algebraic curves. As in [11], we needed to work on restricted classes of number fields and rely on assumptions concerning the smoothness probability of principal ideals. Indeed, even under GRH, the only proven results concern fixed degree number fields. The heuristic concerning the number of relations to be found is also a potential direction for new investigations in the domain. In [5], the relations are randomized which allows to estimate the expected time for finding the whole lattice of the relations without relying on Heuristic 2. On the other hand, this randomization process involves the reduction of ideals which is exponential in the degree of the field. As our classes do not have fixed degree, it remains an open question to decide whether we can prove a probability of success without relying on Heuristic 2. Note that the validity of Heuristic 1 when the degree of the number field is not fixed is also an open problem, even under GRH.

Despite the obstructions due to these open theoretical problems, several improvements could be made to our approach. First of all, further investigations on the constraints on n and d could be made to achieve a complexity below $L(1/3)$.In particular, we would need to assume $f = 1$ since the factorization of f is in $L(1/3)$. As a consequence, the range of applicability of our algorithm would be reduced. Note that any improvement toward a complexity lower than $L(1/3)$ is likely to apply to algebraic curves. However, it seems unlikely that a complexity as low as $L(1/4)$ could be achieved on infinite classes of number fields with our approach. Indeed, a direct substitution of the exponents required to achieve $L(1/4)$ in (3) and (4) show that we would necessarily have

$$\frac{nd}{\log |\Delta_f|} \to 0.$$

We could not find any example of an infinite class of number fields having this property since we expect the condition $nd \geq O\left((\log |\Delta_f|)\,(1 + o(1))\right)$ to hold. Following the approach of this paper, it should also be possible to adapt the $\mathfrak{q}$-descent strategy described in [11] to decompose a given ideal of $\mathcal{O}_{\mathbb{K}}$ as a product of a principal ideal and ideals of the factor base. Such a procedure would allow us to solve the discrete logarithm problem in $\mathrm{Cl}(\mathbb{Z}[\theta])$ as it is shown in [11], but also decide whether an ideal is principal and compute its generator, or find extra relations involving the prime ideals dividing the conductor f in order to compute $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$, and the regulator and fundamental units of $\mathcal{O}_{\mathbb{K}}$ even when $f \neq 1$.

Acknowledgments

The author thanks Andreas Enge for his support, the fruitful discussions we had, and his careful reading of this article. He also thanks Steven Galbraith for the original suggestion of adapting the $L(1/3)$ algorithm of [11] to the context of number fields, Michael Pohst for pointing out [12], Karim Belabas for giving extensive details on the regulator algorithm of Pari, Claus Fieker for giving a simple proof of Proposition 12, and the anonymous referee for his many helpfull suggestions to improve this paper.

References

[1] L. M. Adleman, J. DeMarrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In Leonard M. Adleman and Ming-Deh Huang, editors, *Algorithmic Number Theory*, volume 877 of *Lecture Notes in Computer Science*, pages 28–40, Berlin, 1994. Springer-Verlag.

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

[3] E. Bach. Improved approximations for Euler products. *Journal of the American mathematical society*, 15:13–28, 1995.

[4] R.P. Brent. Fast multiple-precision evaluation of elementary functions. *Journal of the ACM*, 23:242–251, 1976.

[5] J. Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In Catherine Goldstein, editor, *Séminaire de Théorie des Nombres, Paris 1988–1989*, Progress in Mathematics, pages 27–41, Boston, 1990. Birkhäuser.

[6] E.R. Canfield, P. Erdős, and C. Pomerance. On a problem of Oppenheim concerning 'factorisatio numerorum'. *J. Number Theory*, 17:1–28, 1983.

[7] A.L. Chistov. The complexity of constructing the ring of integers of a global field. *Dokl. Akad. Nauk SSSR* 306 (1989), 1063-1067. English translation. *Soviet Math. Dokl.*, (1989), 597-600.

[8] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, 1991.
[9] H. Cohen. Pari. http://pari.math.u-bordeaux.fr/
[10] A. Enge. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. *Mathematics of Computation*, 71:729–742, 2001.
[11] A. Enge, P. Gaudry and E. Thomé. An L (1/3) Discrete Logarithm Algorithm for Low Degree Curves. *Journal of Cryptology* 24(1):24–41, 2011.
[12] C. Fieker and M. Pohst. Dependency of units in number fields. *Mathematics of Computation*, 75:1507–1518, 2006.
[13] M. Giesbrecht, M. Jacobson, and A. Storjohann. Algorithms for large integer matrix problems. In S. Boztas and I. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-14*, volume 2227 of *Lecture Notes in Computer Science*, pages 297–307, Heidelberg, 2001. Springer Verlag.
[14] J.L. Hafner and K.S. McCurley. A rigorous subexponential algorithm for computation of class groups. *Journal of American Society*, 2:839–850, 1989.
[15] M. Jacobson and H.C. Williams. *Solving the Pell equation*. CMS Books in Mathematics. Springer-Verlag, 2009.
[16] E. Kaltofen. and G. Villard On the complexity of computing determinants. *Computational Complexity*, 13:91–130, 2005.
[17] H.W. Lenstra, Jr. On the calculation of regulators and class numbers of quadratic fields. In *Journées arithmétiques*, pages 123–150. Cambridge Univ. Press, 1982.
[18] M. Mignotte. An inequality about factors of polynomials. *Mathematics of Computation*, 28:1153–1157, 1974.
[19] S. Neukirch. *Algebraic number theory*. Comprehensive Studies in Mathematics. Springer-Verlag, 1999. ISBN 3-540-65399-6.
[20] S. Pauli and J. Klüners. Computing residue class rings and Picard groups of orders. *Journal of Algebra*, 292:47–64, 2005.
[21] J.B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, 6:64–94, 1962.
[22] M. Seysen. A probabilistic factorization algorithm with quadratic forms of negative discriminant. *Mathematics of computation*, 48:757–780, 1987.
[23] D. Shanks. Class number, a theory of factorization, and genera. In W. J. LeVeque and E. G. Straus, editors, *Proceedings of Symposia in Pure Mathematics*, volume 20, pages 415–440. American Mathematical Society, 1969.
[24] D. Shanks. The infrastructure of a real quadratic field and its applications. In *Proceedings of the 1972 Number Theory Conference*, pages 217–224. Boulder: University of Colorado, 1972.
[25] C. L. Siegel. Über die Classenzahl quadratischer Zahlkörper. *Acta Arithmetica*, 1:83–86, 1935.
[26] A. Storjohann. *Algorithms for Matrix Canonical Forms*. PhD thesis, Department of Computer Science, Swiss Federal Institute of Technology – ETH, 2000.
[27] U. Vollmer. A note on the Hermite basis computation of large integer matrices. In J. Rafael Sendra, editor, *International Symposium on Symbolic and Algebraic Computation, ISSAC '03*, pages 255–257. ACM Press, 2003.
[28] X. Wang and V. Pan. Acceleration of euclidean algorithm and rational number reconstruction. *SIAM J. Comput.*, 32(2):548–556, 2003.

LIX , École Polytechnique , 91128 PALAISEAU , France
E-mail address: biasse@lix.polytechnique.fr