A new Algorithm for the Computation of logarithmic ℓ-Class Groups of Number Fields*

Francisco Diaz y Diaz, Jean-François Jaulent, Sebastian Pauli,
Michael Pohst, Florence Soriano-Gafiuk

Abstract. We present an algorithm for the computation of logarithmic ℓ-class groups of number fields. Our principal motivation is the effective determination of the ℓ-rank of the wild kernel in the K-theory of number fields.

Résumé. Nous développons un nouvel algorithme pour calculer le ℓ-groupe $\widetilde{\mathcal{C}\ell}_F$ des classes logarithmiques d'un corps de nombres F. Il permet en particulier de déterminer effectivement le ℓ-rang du noyau sauvage $WK_2(F)$ du groupe $K_2(F)$.

1 Introduction

A new invariant of number fields, called group of logarithmic classes, was introduced by J.-F. Jaulent in 1994 [J1]. The interest in the arithmetic of logarithmic classes is because of its applicability in K-Theory. Indeed this new group of classes is revealed to be mysteriously related to the wild kernel in the K-Theory for number fields. The new approach to the wild kernel is so attractive since the arithmetic of logarithmic classes is very efficient. Thus it provides an algorithmic and original study of the wild kernel. A first algorithm for the computation of the group of logarithmic classes of a number field F was developed by F. Diaz y Diaz and F. Soriano in 1999 [DS]. We present a new much better performing algorithm, which also eliminates the restriction to Galois extensions.

Let ℓ be a prime number. If a number field F contains the 2ℓ-th roots of unity then the wild kernel of F and its logarithmic ℓ-class group have the same ℓ-rank. If F does not contain the 2ℓ-th roots of unity the arithmetic of the logarithmic classes still yields the ℓ-rank of the the wild kernel. More precisely:

- If ℓ is odd [JS1, So] we consider $F' := F(\zeta_\ell)$, where ζ_ℓ is the ℓ-th root of unity, and use classic techniques from the theory of semi-simple algebras.
- If $\ell = 2$ [JS2] we introduce a new group, which we call the ℓ-group of of the positive divisor classes and which can be constructed from the ℓ-group of logarithmic classes.

In the present article we consider the general situation where F is a number field which does not necessarily contain the 2ℓ-th roots of unity.

*Experimental. Math. **14** (2005), 67–76.

2 The theoretical background

This section is devoted to the introduction of the main notions of logarithmic arithmetic. We also review the facts that are of interest for our purpose. We do not attempt to give a fully detailed account of the logarithmic language. Most proofs may be found in [J1], pp 303-313.

2.1 Review of the main logarithmic objects

For any number field F, let $\mathcal{J}_F$ be the *ℓ-adified group of idèles* of F, i.e. the restricted product

$$\mathcal{J}_F = \prod_{\mathfrak{p}}^{res} \mathcal{R}_{\mathfrak{p}}$$

of the ℓ-adic compactifications $\mathcal{R}_{\mathfrak{p}} = \varprojlim F_{\mathfrak{p}}^{\times}/F_{\mathfrak{p}}^{\times \ell^n}$ of the multiplicative groups of the completions of F at each $\mathfrak{p}$. For each finite place $\mathfrak{p}$ the subgroup $\widetilde{\mathcal{U}}_{\mathfrak{p}}$ of $\mathcal{R}_{\mathfrak{p}}$ of the cyclotomic norms (that is to say the elements of $\mathcal{R}_{\mathfrak{p}}$ which are norms at any finite step of the local cyclotomic $\mathbb{Z}_\ell$-extension $F_{\mathfrak{p}}^c/F_{\mathfrak{p}}$) will be called *the group of logarithmic units* of $F_{\mathfrak{p}}$. The product

$$\widetilde{\mathcal{U}}_F = \prod_{\mathfrak{p}} \widetilde{\mathcal{U}}_{\mathfrak{p}}$$

is denominated the *group of idelic logarithmic units*; it happens to be the kernel of the *logarithmic valuations*

$$\widetilde{v}_{\mathfrak{p}} \mid x \mapsto -\frac{\mathrm{Log}_\ell\,(N_{F_{\mathfrak{p}}/\mathbb{Q}_p}(x))}{\deg_F \mathfrak{p}},$$

defined on the $\mathcal{R}_{\mathfrak{p}}$ and $\mathbb{Z}_\ell$-valued. These are obtained by taking the Iwasawa logarithm of the norm of x in the local extension $F_{\mathfrak{p}}/\mathbb{Q}_p$ with a normalization factor $\deg_F \mathfrak{p}$ whose precise definition is given in the next subsection.

The quotient $\mathcal{D}\ell_F = \mathcal{J}_F/\widetilde{\mathcal{U}}_F$ is the ℓ-group of *logarithmic divisors* of F; via the logarithmic valuations $\widetilde{v}_{\mathfrak{p}}$, it may be identified with the free $\mathbb{Z}_\ell$-module generated by the prime ideals of F

$$\mathcal{D}\ell_F = \mathcal{J}_F/\widetilde{\mathcal{U}}_F = \oplus_{\mathfrak{p}}\, \mathbb{Z}_\ell\, \mathfrak{p}.$$

The *degree* of a logarithmic divisor $\mathfrak{d} = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\, \mathfrak{p}$ is then defined by

$$\deg_F \big(\sum_{\mathfrak{p}} n_{\mathfrak{p}}\, \mathfrak{p}\big) = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \deg_F \mathfrak{p},$$

inducing a $\mathbb{Z}_\ell$-valued $\mathbb{Z}_\ell$-linear map on the class group of logarithmic divisors. The logarithmic divisors of degree zero form a subgroup of $\mathcal{D}\ell_F$ denoted by

$$\widetilde{\mathcal{D}\ell}_F = \{\, \mathfrak{d} \in \mathcal{D}\ell_F \mid \deg_F \mathfrak{d} = 0 \,\}.$$

The image of the map $\widetilde{\mathrm{div}}_F$ defined via the set of logarithmic valuations from the principal idèle subgroup

$$\mathcal{R}_F = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} F^{\times}$$

of $\mathcal{J}_F$ to $\widetilde{\mathcal{D}\ell}_F$ is a subgroup denoted by $\widetilde{\mathcal{P}\ell}_F$, which will be referred to as the subgroup of *principal logarithmic divisors*. The quotient

$$\widetilde{\mathcal{C}\ell}_F = \widetilde{\mathcal{D}\ell}_F / \widetilde{\mathcal{P}\ell}_F$$

is, by definition, the *ℓ-group of logarithmic classes* of F. And the kernel

$$\widetilde{\mathcal{E}}_F = \mathcal{R}_F \cap \widetilde{\mathcal{U}}_F$$

of the morphism $\widetilde{\operatorname{div}}_F$ from $\mathcal{R}_F$ in $\widetilde{\mathcal{D}\ell}_F$ is the group of global *logarithmic units.*

2.2 Logarithmic ramification and ℓ-adic-degrees.

Next we review the basic notions of the logarithmic ramification, which mimic, as a rule, the classical ones.

Let L/F be any finite extension of number fields. Let p be a prime number. Denote by $\widehat{\mathbb{Q}}_p^c$ the cyclotomic $\widehat{\mathbb{Z}}$-extension of $\mathbb{Q}_p$, that is to say the compositum of all cyclotomic $\mathbb{Z}_q$-extension of $\mathbb{Q}_p$ on all prime numbers q. Let $\mathfrak{p}$ be a prime of F above (p) and $\mathfrak{P}$ a prime of L above $\mathfrak{p}$. The logarithmic ramification (resp. inertia) index $\widetilde{e}(L_\mathfrak{P}/F_\mathfrak{p})$ (resp. $\widetilde{f}(L_\mathfrak{P}/F_\mathfrak{p})$) is defined to be the relative degree

$$\widetilde{e}(L_\mathfrak{P}/F_\mathfrak{p}) = [L_\mathfrak{P} : L_\mathfrak{P} \cap \widehat{\mathbb{Q}}_p^c F_\mathfrak{p}] \quad (\text{resp.} \quad \widetilde{f}(L_\mathfrak{P}/F_\mathfrak{p}) = [L_\mathfrak{P} \cap \widehat{\mathbb{Q}}_p^c F_\mathfrak{p} : F_\mathfrak{p}]).$$

As a consequence, L/F is logarithmically unramified at $\mathfrak{P}$, i.e. $\widetilde{e}(L_\mathfrak{P}/F_\mathfrak{p}) = 1$, if and only if $L_\mathfrak{P}$ is contained in the cyclotomic extension of $F_\mathfrak{p}$. Moreover, for any $q \neq p$ the classical and the logarithmic indexes have the same q-part (see theorem 5). Hence they are equal as soon as $p \nmid [F_\mathfrak{p} : \mathbb{Q}_p]$.

As usual, in the special case $L/F = K/\mathbb{Q}$, the absolute logarithmic indexes of a finite place $\mathfrak{p}$ of K over the prime p are just denoted by $\widetilde{e}_\mathfrak{p}$ and $\widetilde{f}_\mathfrak{p}$. With these notations, the ℓ-adic degree of $\mathfrak{p}$ is defined by the formula:

$$\deg_K \mathfrak{p} = \widetilde{f}_\mathfrak{p} \deg_\ell p \quad \text{with} \quad \deg_\ell p = \begin{cases} \operatorname{Log}_\ell p & \text{for } p \neq \ell; \\ \ell & \text{for } p = \ell \neq 2; \\ 4 & \text{for } p = \ell = 2. \end{cases}$$

The extension and norm maps between groups of divisors, denoted by $\iota_{L/F}$ and $N_{L/F}$ respectively, have their logarithmic counterparts, $\widetilde{\iota}_{L/F}$ and $\widetilde{N}_{L/F}$ respectively. To be more explicit, $\widetilde{\iota}_{L/F}$ is defined on every finite place $\mathfrak{p}$ of F by

$$\widetilde{\iota}_{L/F}(\mathfrak{p}) = \textstyle\sum_{\mathfrak{P}|\mathfrak{p}} \widetilde{e}_{L_\mathfrak{P}/F_\mathfrak{p}} \mathfrak{P} \ ,$$

while $\widetilde{N}_{L/F}$ is defined on all $\mathfrak{P}$ lying above $\mathfrak{p}$ by

$$\widetilde{N}_{L/F}(\mathfrak{P}) = \widetilde{f}_{L_\mathfrak{P}/F_\mathfrak{p}} \ \mathfrak{p} \ .$$

These applications are compatible with the usual extension and norm maps defined between $\mathcal{R}_L$ and $\mathcal{R}_F$, in the sense that they sit inside the commutative diagrams:

$$\begin{array}{ccccc} \mathcal{R}_L & \xrightarrow{\widetilde{\operatorname{div}}_L} & \widetilde{\mathcal{D}\ell}_L & \xrightarrow{\deg_L} & \mathbb{Z}_\ell \\ \downarrow{\scriptstyle N_{L/F}} & & \downarrow{\scriptstyle \widetilde{N}_{L/F}} & & \| \\ \mathcal{R}_F & \xrightarrow{\widetilde{\operatorname{div}}_F} & \widetilde{\mathcal{D}\ell}_F & \xrightarrow{\deg_F} & \mathbb{Z}_\ell \end{array} \quad \text{and} \quad \begin{array}{ccccc} \mathcal{R}_L & \xrightarrow{\widetilde{\operatorname{div}}_L} & \widetilde{\mathcal{D}\ell}_L & \xrightarrow{\deg_L} & \mathbb{Z}_\ell \\ \uparrow{\scriptstyle \iota_{L/F}} & & \uparrow{\scriptstyle \widetilde{\iota}_{L/F}} & & \uparrow{\scriptstyle [L:F]} \\ \mathcal{R}_F & \xrightarrow{\widetilde{\operatorname{div}}_F} & \widetilde{\mathcal{D}\ell}_F & \xrightarrow{\deg_F} & \mathbb{Z}_\ell. \end{array}$$

When L/F is a Galois extension with Galois group $\mathrm{Gal}(L/F)$, one deduces from the very definitions the unsurprising and obvious properties:

$$\widetilde{N}_{L/F} \circ \widetilde{\iota}_{L/F} = [L:F] \quad \text{and} \quad \widetilde{\iota}_{L/F} \circ \widetilde{N}_{L/F} = \sum_{\sigma \in \mathrm{Gal}(L/F)} \sigma \ .$$

2.3 Ideal theoretic description of logarithmic classes.

By the weak density theorem every class in $\mathcal{J}_F/\widetilde{\mathcal{U}}_F\mathcal{R}_F$ may be represented by an idele with trivial components at the ℓ-adic places, that is to say that every class in $\mathcal{D}\ell_F/\mathcal{P}\ell_F$ comes from a ℓ-divisor $\mathfrak{d} = \sum_{\mathfrak{p}\nmid\ell} \alpha_\mathfrak{p}\ \mathfrak{p}$.

The canonical map from $\mathcal{R}_F$ to $\mathcal{D}\ell_F$ maps $a \in \mathcal{R}_F$ to $\widetilde{\mathrm{div}}_F(a) = \sum_\mathfrak{p} \widetilde{v}_\mathfrak{p}(a)\mathfrak{p}$. Now for each finite place $\mathfrak{p} \nmid \ell$, the quotient $\widetilde{e}_\mathfrak{p}/e_\mathfrak{p} = f_\mathfrak{p}/\widetilde{f}_\mathfrak{p}$ of the classical and logarithmical indexes associated to $\mathfrak{p}$ is a ℓ-adic unit (theorem 5), say $\lambda_\mathfrak{p}$ (which is 1 for almost all $\mathfrak{p}$), and one has the identity:

$$\widetilde{v}_\mathfrak{p} = \lambda_\mathfrak{p} v_\mathfrak{p}$$

between the logarithmic and the classical valuations. So every ℓ-divisor $\mathfrak{d}$ comes from a ℓ-ideal $\mathfrak{a}$ by the formula:

$$\mathfrak{a} = \prod_{\mathfrak{p}\nmid\ell} \mathfrak{p}^{\alpha_\mathfrak{p}} \mapsto \mathfrak{d}_F(\mathfrak{a}) = \sum_{\mathfrak{p}\nmid\ell} \lambda_\mathfrak{p}\ \alpha_\mathfrak{p}\ \mathfrak{p}\ .$$

This gives the following ideal theoretic description of logarithmic classes:

Definition & Proposition 1. *Let $\mathcal{I}d_F = \{\mathfrak{a} = \prod_{\mathfrak{p}\nmid\ell} \mathfrak{p}^{\alpha_\mathfrak{p}}\}$ be the group of ℓ-ideals, $\widetilde{\mathcal{I}d}_F = \{\mathfrak{a} \in \mathcal{I}d_F | \deg_F \mathfrak{d}_F(\mathfrak{a}) = 0\}$ be the subgroup of ℓ-ideals of degree 0 and $\widetilde{\mathcal{P}r}_F = \{\prod_{\mathfrak{p}\nmid\ell} \mathfrak{p}^{v_\mathfrak{p}(a)} | \widetilde{v}_\mathfrak{p}(a) = 0\ \forall \mathfrak{p} \mid \ell\}$ the subgroup of principal ℓ-ideals generated by principal ideles a having logarithmic valuations 0 at every ℓ-adic places. Then one has:*

$$\widetilde{\mathcal{C}\ell}_F \simeq \widetilde{\mathcal{I}d}_F/\widetilde{\mathcal{P}r}_F$$

Proof. As explained above, the surjectivity follows from the weak approximation theorem. So let us consider the kernel of the canonical map $\phi_F : \widetilde{\mathcal{I}d}_F \mapsto \widetilde{\mathcal{C}\ell}_F$. Clearly we have: $\ker\phi_F = \{\mathfrak{a} \in \widetilde{\mathcal{I}d}_F \mid \exists a \in \mathcal{R}_F \quad \mathfrak{d}_F(\mathfrak{a}) = \widetilde{\mathrm{div}}_F(a)\}$. The condition $\mathfrak{d}_F(\mathfrak{a}) = \widetilde{\mathrm{div}}_F(a)$ with $\mathfrak{a} \in \widetilde{\mathcal{I}d}_F$ implies $\widetilde{v}_\mathfrak{p}(a) = 0\ \forall \mathfrak{p} \mid \ell$; and then gives $(a) \in \widetilde{\mathcal{P}r}_F$ as expected. $\square$

The generalized Gross conjectures (for the field F and the prime ℓ) asserts that the logarithmic class group $\widetilde{\mathcal{C}\ell}_F$ is finite (cf. [J1]). This conjecture, which is a consequence of the p-adic Schanuel conjecture was only proved in the abelian case and a few others (cf. [FG, J5]). Nevertheless, since $\widetilde{\mathcal{C}\ell}_F$ is a $\mathbb{Z}_\ell$-module of finite type (by the ℓ-adic class field theory), the Gross conjecture just claims the existence of an integer m such that ℓ^m kills the logarithmic class group. As in numerical situations it is rather easy to compute such an exponent m (when the classical invariants of the number field are known), this give rise to a more suitable description of $\widetilde{\mathcal{C}\ell}_F$ in order to carry on numerical computations:

Proposition 2. *Assume the integer m to be large enough such that the logarithmic class group $\widetilde{\mathcal{C}\ell}_F$ is annihilated by ℓ^m. Thus introduce the group:*

$$\widetilde{\mathcal{I}d}_F^{(\ell^m)} = \{\mathfrak{a} \in \mathcal{I}d_F | \deg_F \mathfrak{d}_F(\mathfrak{a}) \in \ell^m \deg_F \mathcal{D}\ell_F\} = \widetilde{\mathcal{I}d}_F\ \mathcal{I}d_F^{\ell^m}$$

Thus, denoting $\widetilde{\mathcal{P}r}_F^{(\ell^m)} = \widetilde{\mathcal{P}r}_F\ \widetilde{\mathcal{I}d}_F^{\ell^m}$, one has: $\widetilde{\mathcal{C}\ell}_F \simeq \widetilde{\mathcal{I}d}_F^{(\ell^m)}/\widetilde{\mathcal{P}r}_F^{(\ell^m)}$.

Proof. The hypothesis gives $\widetilde{\mathcal{I}d}_F^{\ell^m} \subset \widetilde{\mathcal{P}r}_F$ and by a straightforward calculation:

$$\begin{aligned}\widetilde{\mathcal{I}d}_F^{(\ell^m)}/\widetilde{\mathcal{P}r}_F^{(\ell^m)} &= \widetilde{\mathcal{I}d}_F\mathcal{I}d^{\ell^m}/\widetilde{\mathcal{P}r}_F\mathcal{I}d^{\ell^m} \simeq \widetilde{\mathcal{I}d}_F/(\widetilde{\mathcal{I}d}_F \cap \widetilde{\mathcal{P}r}_F\mathcal{I}d^{\ell^m}) \\ &\simeq \widetilde{\mathcal{I}d}_F/\widetilde{\mathcal{P}r}_F\widetilde{\mathcal{I}d}_F^{\ell^m} = \widetilde{\mathcal{I}d}_F/\widetilde{\mathcal{P}r}_F \simeq \widetilde{\mathcal{C}\ell}_F.\end{aligned}$$

□

Remark 3. A lower bound for m which will be required for a sufficient precision of the p-adic calculations will be given after lemma 12.

3 The algorithms

Throughout this section a finite abelian group G is presented by a column vector $g \in G^m$, whose entries form a system of generators for G, and by a matrix of relations $M \in \mathbb{Z}^{n\times m}$ of rank m, such that $v^T g = 0$ for $v \in \mathbb{Z}^m$ if and only if v^T is an integral linear combination of the rows of M. We note that for every $a \in G$ there is a $v \in \mathbb{Z}^m$ satisfying $a = v^T g$. If $g_1, \ldots, g_m$ is a basis of G, M is usually a diagonal matrix. Algorithms for calculations with finite abelian groups can be found in [C2]. If G is a multiplicative abelian group, then $v^T g$ is an abbreviation for $g_1^{v_1} \cdots g_m^{v_m}$.

One of the steps in the computation of the logarithmic class group is the computation of the ideal class group of a number field. Algorithms for this can be found in [C1, He, PZ]. One tool used in these algorithms are the $\mathfrak{s}$-units, which we will also use directly in our algorithm.

Definition 4 ($\mathfrak{s}$-units). Let $\mathfrak{s}$ be an ideal of a number field F. We call the group

$$\left\{\alpha \in F^\times \mid v_{\mathfrak{p}}(\alpha) = 0 \text{ for all } \mathfrak{p} \nmid \mathfrak{s}\right\}$$

the $\mathfrak{s}$-units of F.

For this section let F be a fixed number field. We denote the ideal class group of F by $\mathcal{C}\ell = \mathcal{C}\ell_F$. We also write $\widetilde{\mathcal{C}\ell}$ for $\widetilde{\mathcal{C}\ell}_F$, $\widetilde{\mathcal{D}\ell}$ for $\widetilde{\mathcal{D}\ell}_F$, and so on.

3.1 Computing $\deg_F(\mathfrak{p})$ and $\widetilde{v}_{\mathfrak{p}}(\cdot)$

We describe how invariants of the logarithmic objects can be computed. Some of the tools presented here also applied directly in the computation of the logarithmic class group.

Definition & Proposition 5. *Let p be a prime number. Let F be a number field. Let $\mathfrak{p}$ be a prime ideal of F over p. For $a \in \mathbb{Q}_p^\times \cong p^{\mathbb{Z}} \times \mathbb{F}_p^\times \times (1 + 2p\mathbb{Z}_p)$ denote by $\langle a\rangle$ the projection of a to $(1 + 2p\mathbb{Z}_p)$. Let $F_{\mathfrak{p}}$ be the completion of F with respect to $\mathfrak{p}$. For $\alpha \in F$ define*

$$h_{\mathfrak{p}}(\alpha) := \frac{\operatorname{Log}_p\langle \mathrm{N}_{F_{\mathfrak{p}}/\mathbb{Q}_p}(\alpha)\rangle}{[F_{\mathfrak{p}} : \mathbb{Q}_p]\cdot \deg_p p}.$$

The p-part of the logarithmic ramification index $\widetilde{e}_{\mathfrak{p}}$ is $[h_{\mathfrak{p}}(F_{\mathfrak{p}}^\times) : \mathbb{Z}_p]$. For all primes q with $q \neq p$ the q-part of $\widetilde{e}_{\mathfrak{p}}$ is the q-part of the ramification index $e_{\mathfrak{p}}$ of $\mathfrak{p}$.

For a proof see [J1].

In section 2.2 we have seen that the degree $\deg_F(\mathfrak{p})$ of a place $\mathfrak{p}$ can be computed as $\deg_F(\mathfrak{p}) = \widetilde{f}_{\mathfrak{p}} \deg_\ell p$. From section 2.3 we know that $\widetilde{e}_{\mathfrak{p}} \widetilde{f}_{\mathfrak{p}} = e_{\mathfrak{p}} f_{\mathfrak{p}}$. We have

$$\widetilde{v}_{\mathfrak{p}}(x) = -\frac{\mathrm{Log}_\ell(\mathrm{N}_{F_{\mathfrak{p}}/\mathbb{Q}_p}(x))}{\deg_F(\mathfrak{p})}.$$

Thus we can concentrate on the computation of $\widetilde{e}_{\mathfrak{p}}$ for which we need the completion $F_{\mathfrak{p}}$ of F at $\mathfrak{p}$ and generators of the unit group $F_{\mathfrak{p}}^\times$.

The Round Four Algorithm was originally conceived as an algorithm for computing integral bases of number fields. It can be applied in three different ways in the computation of logarithmic classgroups. Firstly, it is used for factoring ideals over number fields; secondly, it returns generating polynomials of completions of number fields; and thirdly, it can be used for determining integral bases of maximal orders.

Let $\Phi(x)$ be a monic, squarefree polynomial over $\mathbb{Z}_p$. The algorithm for factoring polynomials over local fields as described in [Pa] returns

- a factorization $\Phi(x) = \Phi_1(x) \cdot \cdots \cdot \Phi_s(x)$ of $\Phi(x)$ into irreducible factors $\Phi_i(x)$ $(1 \le i \le s)$ over $\mathbb{Z}_p$,
- the inertia degrees e_i and ramification indexes f_i of the extensions of $\mathbb{Q}_p$ given by the $\Phi_i(x)$ $(1 \le i \le s)$, and
- two element certificates $(\Gamma_i(x), \Pi_i(x))$ with $\Gamma_i(x), \Pi_i(x) \in F[x]$ such that $v_i\big(\Pi_i(\alpha_i)\big) = 1/e_i$ and $[\mathbb{F}_p(\overline{\Gamma_i(\alpha_i)}) : \mathbb{F}_p] = f_i$ where α_i is a root of $\Phi_i(x)$ in $F[x]/(\Phi_i(x))$, v_i is an extension of the exponential valuation v_p of $\mathbb{Q}_p$ to $\mathbb{Q}_p[x]/(\Phi_i(x))$ with $v_i|_{\mathbb{Q}_p} = v_p$.

The factorization algorithm in [FPR] returns the certificates combined in one polynomial for each irreducible factor. The data returned by these algorithms can be applied in several ways.

- An integral basis of the extension of $\mathbb{Q}_p$ generated by a root α_i of $\Phi_i(x)$ is given by the elements $\Gamma_i(\alpha_i)^h \Pi_i(\alpha_i)^j$ with $0 \le h \le f_i$ and $0 \le j \le e_i$. The local integral bases can be combined to a global integral basis for the extension of $\mathbb{Q}$ generated by $\Phi(x)$.
- For the computation of $\widetilde{v}_{\mathfrak{p}}$ we need to compute the norm of an element in the completions of F. The completions of F are given by the irreducible factors of the generating polynomial of F over $\mathbb{Q}$.

Lemma 6 (Ideal Factorization). *Let $\Phi(x) \in \mathbb{Z}_p[x]$ be irreducible over $\mathbb{Q}$. Let $\Phi_1(x), \ldots, \Phi_s(x) \in \mathbb{Z}_p[x]$ be the irreducible factors of $\Phi(x)$ with two element certificates $(\Gamma_i(x), \Pi_i(x))$. Denote by e_i the ramification indexes of the extensions of $\mathbb{Q}_p$ given by the $\Phi_i(x)$ $(1 \le i \le s)$. The Chinese Remainder Theorem gives polynomials $\Theta_1(x), \ldots, \Theta_s(x) \in \mathbb{Q}_p[x]$ with*

$$\begin{aligned} \Theta_i(x) &\equiv \Pi_i(x) \bmod \Phi_i(x) \\ \Theta_i(x) &\equiv 1 \bmod \textstyle\prod_{j \ne i} \Phi_j(x). \end{aligned}$$

Let $L := \mathbb{Q}(\alpha)$ where α is a root of $\Phi(x)$ in $\mathbb{C}$. Then

$$(p) = \big(p, \Theta_1(\alpha)\big)^{e_1} \cdot \cdots \cdot \big(p, \Theta_s(\alpha)\big)^{e_s}$$

is a factorization of (p) into prime ideals.

In order to compute $[h_{\mathfrak{p}}(F_{\mathfrak{p}}^{\times}) : \mathbb{Z}_p]$ it is sufficient to compute the image of a set of generators of $F_{\mathfrak{p}}^{\times}$. Algorithms for this task were recently developed with respect to the computation of ray class groups of number fields and function fields [C2, HPP], also see [Ha, chapter 15].

Proposition 7.

$$F_{\mathfrak{p}}^{\times} \cong \pi^{\mathbb{Z}} \times (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})^{\times} \times (1+\mathfrak{p})$$

Let $\mathfrak{p}$ be the prime ideal over the prime number p in $\mathcal{O}_{\mathfrak{p}}$. Let $e_{\mathfrak{p}}$ be the ramification index and $f_{\mathfrak{p}}$ the inertia degree of $\mathfrak{p}$. We define the set of fundamental levels

$$\mathcal{F}_e := \left\{ \nu \mid 0 < \nu < \tfrac{pe_{\mathfrak{p}}}{p-1}, p \nmid \nu \right\}$$

and let $\varepsilon \in \mathcal{O}_{\mathfrak{p}}^{\times}$ such that $p = -\pi^e \varepsilon$. Furthermore we define the map

$$h_2 : a + \mathfrak{p} \longmapsto a^p - \varepsilon a + \mathfrak{p}.$$

Theorem 8 (Basis of $(1+\mathfrak{p})$). *Let $\omega_1, \ldots, \omega_f \in \mathcal{O}_{\mathfrak{p}}$ be a fixed set of representatives of a $\mathbb{F}_p$-basis of $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$. If $(p-1)$ does not divide e or h_2 is an isomorphism, then the elements*

$$1 + \omega_i \pi^{\nu} \text{ where } \nu \in \mathcal{F}_e, 1 \leq i \leq f$$

are a basis of the group of principal units $1+\mathfrak{p}$.

Theorem 9 (Generators of $(1+\mathfrak{p})$). *Assume that $(p-1) \mid e$ and h_2 is not an isomorphism. Choose e_0 and μ_0 such that p does not divide e_0 and such that $e = p^{\mu_0 - 1}(p-1)e_0$. Let $\omega_1, \ldots, \omega_f \in \mathcal{O}_{\mathfrak{p}}$ be a fixed set of representatives of a $\mathbb{F}_p$-basis of $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$ subject to $\omega_1^{p^{\mu_0}} - \varepsilon \omega_1^{p^{\mu_0 - 1}} \equiv 0 \bmod \mathfrak{p}$. Choose $\omega_* \in \mathcal{O}_{\mathfrak{p}}$ such that $x^p - \varepsilon x \equiv \omega_* \bmod \mathfrak{p}$ has no solution. Then the group of principal units $1+\mathfrak{p}$ is generated by*

$$1 + \omega_* \pi^{p^{\mu_0} e_0} \text{ and } 1 + \omega_i \pi^{\nu} \text{ where } \nu \in \mathcal{F}_e,\ 1 \leq i \leq f.$$

3.2 Computing a bound for the exponent of $\widetilde{\mathcal{C}\ell}$

Let F be a number field and ℓ a prime number. Let $\widetilde{\mathcal{C}\ell} = \widetilde{\mathcal{C}\ell}_F \cong \widetilde{\mathcal{I}d}/\widetilde{\mathcal{P}r}$ be the ℓ-group of logarithmic divisor classes. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the ℓ-adic places of F.

We describe an algorithm which returns an upper bound ℓ^m of the exponent of $\widetilde{\mathcal{C}\ell}$ (see proposition 2). We denote by

- $\widetilde{\mathcal{C}\ell}(\ell)$ the ℓ group of logarithmic divisor classes of degree zero:

$$\widetilde{\mathcal{C}\ell}(\ell) := \left\{ [\mathfrak{a}] \in \widetilde{\mathcal{C}\ell} \mid \mathfrak{a} = \textstyle\sum_{i=1}^{s} a_i \mathfrak{p}_i \text{ with } \deg_F(\mathfrak{a}) = 0 \right\}$$

- $\mathcal{C}\ell'$ the ℓ-group of the ℓ-ideal classes, *i.e.*, the ℓ-part of $\mathcal{C}\ell/\langle [\mathfrak{p}_1], \ldots, [\mathfrak{p}_s] \rangle$.

Remark 10. If $(\ell) = \mathfrak{p}^e$ where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ then the group $\widetilde{\mathcal{C}\ell}(\ell)$ is trivial.

Lemma 11 ([DS]). *Let*

$$\theta : \widetilde{\mathcal{C}\ell} \longrightarrow \mathcal{C}\ell',\ \textstyle\sum_{\mathfrak{p}} m_{\mathfrak{p}} \mathfrak{p} \longmapsto \prod_{\mathfrak{p} \nmid \ell} \mathfrak{p}^{(1/\lambda_{\mathfrak{p}}) m_{\mathfrak{p}}}.$$

The sequence

$$0 \longrightarrow \widetilde{\mathcal{C}\ell}(\ell) \longrightarrow \widetilde{\mathcal{C}\ell} \xrightarrow{\theta} \mathcal{C}\ell' \longrightarrow \operatorname{Coker} \theta \longrightarrow 0$$

is exact.

Proof. Recall that, if $\mathfrak{p} \nmid \ell$, $\widetilde{v}_\mathfrak{p} = \lambda_\mathfrak{p} v_\mathfrak{p}$. Denote by $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ the ℓ-adic places of F. Let

$$\widetilde{\mathfrak{a}} = \sum_\mathfrak{q} a_\mathfrak{q} \mathfrak{q} = \widetilde{\operatorname{div}}(\alpha) = \sum_\mathfrak{p} \widetilde{v}_\mathfrak{p}(\alpha)\mathfrak{p} = \sum_{\mathfrak{p}\nmid\ell} \lambda_\mathfrak{p} v_\mathfrak{p}(\alpha)\mathfrak{p} + \sum_{i=1}^{s} \widetilde{v}_{\mathfrak{p}_i}(\alpha)\mathfrak{p}_i$$

be a principal logarithmic divisor. A representative of the image of $\widetilde{\mathfrak{a}}$ under θ in terms of ideals is of the form

$$\mathfrak{a} = \prod_{q\nmid(\ell)} \mathfrak{q}^{v_\mathfrak{q}(\alpha)} = (\alpha\mathcal{O}_K) \times \prod_{i=1}^{s} \mathfrak{p}_i^{-v_{p_i}(\alpha)}.$$

This shows that the homomorphism θ is well defined. It follows immediately that $\operatorname{Ker}\theta = \widetilde{\mathcal{C}\ell}(\ell)$. $\square$

Lemma 12. *Set $\ell^{m'} = \exp \mathcal{C}\ell'$ and $\ell^{\widetilde{m}} = \exp \widetilde{\mathcal{C}\ell}(\ell)$. Then*

$$\ell^{m'+\widetilde{m}}\mathfrak{a} \equiv 0 \bmod \widetilde{\mathcal{P}\ell} \textit{ for all } \mathfrak{a} \in \widetilde{\mathcal{D}\ell}.$$

Proof. It follows from the exact sequence in lemma 11 that for all $\mathfrak{a} \in \widetilde{\mathcal{D}\ell}$ the congruence $\ell^{m'}\theta(\mathfrak{a}) \equiv 1$ holds in $\mathcal{C}\ell'$. Thus $\ell^{m'}\mathfrak{a} \in \operatorname{Ker}\theta = \widetilde{\mathcal{C}\ell}(\ell)$ and $\ell^{m'+\widetilde{m}}\mathfrak{a} \equiv 0 \bmod \widetilde{\mathcal{P}\ell}$. $\square$

Lemma 12 suggests setting the precision for the computation of $\widetilde{\mathcal{C}\ell}$ to $m := m' + \widetilde{m}$ ℓ-adic digits. If the ideal class group $\mathcal{C}\ell$ is known we can easily compute m'. In order to find $\widetilde{m}$ we compute a matrix of relations for $\widetilde{\mathcal{C}\ell}(\ell)$.

Lemma 13 (Generators and Relations of $\widetilde{\mathcal{C}\ell}(\ell)$). *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the ℓ-adic places of F. Assume that $s > 1$. Reorder the $\mathfrak{p}_i$ such that $v_\ell(\deg(\mathfrak{p}_1)) = \min_{1\le i\le s} v_\ell(\deg(\mathfrak{p}_i))$. Let $\gamma_1, \ldots, \gamma_r$ be a basis of the ℓ-units of F. Then the group $\widetilde{\mathcal{C}\ell}(\ell)$ is given by the generators $[\mathfrak{g}_i] := \left[\mathfrak{p}_i - \frac{\deg(\mathfrak{p}_i)}{\deg(\mathfrak{p}_1)}\mathfrak{p}_1\right]$ $(i = 2, \ldots, s)$ with relations $\sum_{i=2}^{s} \widetilde{v}_{\mathfrak{p}_i}(\gamma_j)[\mathfrak{g}_i] = [0]$.*

Proof. We consider a logarithmic divisor $\mathfrak{a} = \sum_{i=1}^{s} a_i\mathfrak{p}_i$ of degree zero over F that is constructed from the ℓ-adic places. By the choice of $\mathfrak{p}_1$ and as $\deg(\mathfrak{a}) = \deg(\sum_{i=1}^{s} a_i\mathfrak{p}_i) = \sum_{i=1}^{s} a_i \deg(\mathfrak{p}_i) = 0$ the coefficient a_1 is given by the other $s-1$ coefficients. Thus the $[\mathfrak{g}_i]$ generate $\widetilde{\mathcal{C}\ell}(\ell)$.

The relations between the classes of $\widetilde{\mathcal{C}\ell}(\ell)$ are of the form $\sum_{i=2}^{s} b_i[\mathfrak{g}_i] = [0]$. That is there exists $\beta \in \mathcal{R}_F$ such that

$$\sum_{i=2}^{s} b_i\mathfrak{g}_i = \sum_{j=1}^{s} a_j\mathfrak{p}_j = \widetilde{\operatorname{div}}(\beta),$$

with $v_\mathfrak{q}(\beta) = 0$ for all $\mathfrak{q} \nmid (\ell)$. Thus β is an element of the group of ℓ-units $\{\alpha \in \mathcal{R}_F \mid v_\mathfrak{q}(\alpha) = 0\}$ of $\mathcal{R}_F$. Hence we obtain the relations given above. $\square$

A version of this lemma for the case that F is Galois can be found in [DS].

Algorithm 14 (Precision).

Input: a number field F and a prime number ℓ, the ℓ-adic places $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of F, and a basis $\gamma_1, \ldots, \gamma_r$ of the ℓ-units of F

Output: an upper bound for the exponent of $\widetilde{\mathcal{C}\ell}$

- Set $\ell^{m'} \leftarrow \exp \mathcal{C}\ell'$, set $m \leftarrow \max\{m', 4\}$.
- If $s = 1$ then return $\ell^{m'}$. [Remark 10]
- Repeat
  - Set $m \leftarrow m + 2$
  - Set [Lemma 13]

$$A \leftarrow \begin{pmatrix} \widetilde{v}_{\mathfrak{p}_2}(\gamma_1) & \dots & \widetilde{v}_{\mathfrak{p}_s}(\gamma_1) \\ \vdots & \ddots & \vdots \\ \widetilde{v}_{\mathfrak{p}_2}(\gamma_r) & \dots & \widetilde{v}_{\mathfrak{p}_s}(\gamma_r) \end{pmatrix} \bmod \ell^m.$$

  - Let H be the Hermite normal form of A modulo ℓ^m.
- Until $\operatorname{rank}(H) = s - 1$.
- Let $S = (S_{i,j})_{i,j}$ be the Smith normal form of A modulo ℓ^m.
- Set $\widetilde{m} \leftarrow \max_{1 \le i \le s-1}\big(v_\ell(S_{i,i})\big)$, return $\ell^{m'+\widetilde{m}}$.

Remark 15. Algorithm 14 does not terminate in general if Gross' conjecture is false.

3.3 Computing $\widetilde{\mathcal{C}\ell}$

We use the ideal theoretic description from section 2.3 for the computation of $\widetilde{\mathcal{C}\ell} \cong \widetilde{\mathcal{I}d}/\widetilde{\mathcal{P}r}$. In the previous section we have seen how we can compute a bound for the exponent of $\widetilde{\mathcal{C}\ell}$. It is clear that this bound also gives a lower bound for the precision in our calculations.

Theorem 16 (Generators of $\widetilde{\mathcal{C}\ell}$). *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_t$ be a basis of the ideal class-group of F with $\gcd(\mathfrak{a}_i, \ell) = 1$ for all $1 \le i \le t$. Denote by $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ the ℓ-adic places of F. Let $\alpha_1, \dots, \alpha_s$ be elements of $\mathcal{R}_F$ with $\widetilde{v}_{\mathfrak{p}_i}(\alpha_j) = \delta_{i,j}$ $(i, j = 1, \dots, s)$ and $\gcd((\alpha_i), \ell) = 1$ for all $1 \le i \le s$. Set $\mathfrak{a}_{t+i} := (\alpha_i)$ for $1 \le i \le s$. For an ideal $\mathfrak{a}$ of F denote by $\overline{\mathfrak{a}}$ the projection of $\mathfrak{a}$ from $\bigoplus_{\mathfrak{p}} \mathfrak{p}^{\mathbb{Z}_\ell}$ to $\bigoplus_{\mathfrak{p} \nmid (\ell)} \mathfrak{p}^{\mathbb{Z}_\ell}$. We distinguish two cases:*

- **I.** *If $\deg_\ell(\mathfrak{a}_i) = 0$ for all $1 \le i \le t + s$ then set $\mathfrak{b}_i := \mathfrak{a}_i$. The group $\widetilde{\mathcal{C}\ell}_F$ is generated by $\overline{\mathfrak{b}}_1, \dots, \overline{\mathfrak{b}}_{t+s}$.*
- **II.** *Otherwise let $1 \le j \le t+s$ such that $v_\ell(\deg_\ell(\mathfrak{a}_j)) = \min_{1 \le i \le t+s} v_\ell(\deg_\ell(\mathfrak{a}_i))$. Set $\mathfrak{b}_i := \mathfrak{a}_i/\mathfrak{a}_j^d$ with $d \equiv \frac{\deg_\ell(\mathfrak{a}_i)}{\deg_\ell(\mathfrak{a}_j)} \bmod \ell^m$ where $\ell^m > \exp(\widetilde{\mathcal{C}\ell})$. The group $\widetilde{\mathcal{C}\ell}_F$ is generated by $\overline{\mathfrak{b}}_1, \dots, \overline{\mathfrak{b}}_{j-1}, \overline{\mathfrak{b}}_{j+1}, \dots, \overline{\mathfrak{b}}_{t+s}$.*

Proof. Let $\mathfrak{a} \in \widetilde{\mathcal{I}d}$. There exist $\gamma \in \mathcal{R}_F$ and $a_1, \dots, a_t \in \mathbb{Z}_\ell$ such that $\mathfrak{a} = \prod_{i=1}^t \mathfrak{a}_i^{a_i} \cdot (\gamma)$. Set $g_i := \widetilde{v}_{\mathfrak{p}_i}(\gamma)$ for $1 \le i \le s$. Now

$$\mathfrak{a} = \textstyle\prod_{i=1}^s \mathfrak{a}_i^{a_i} \cdot \big((\gamma) \cdot \prod_{j=1}^s (\alpha_i)^{-g_i}\big) \cdot \big(\prod_{j=1}^s (\alpha_i)^{g_i}\big).$$

By the definition of $\mathcal{I}d$ (Definition and Proposition 1) we have

$$\mathfrak{a} = \overline{\mathfrak{a}} = \textstyle\prod_{i=1}^t \overline{\mathfrak{a}}_i^{a_i} \cdot \overline{\big((\gamma) \cdot \prod_{j=1}^s (\alpha_j)^{-g_j}\big)} \cdot \big(\prod_{j=1}^s \overline{(\alpha_j)^{g_j}}\big)$$

As $\widetilde{v}_{\mathfrak{p}_i}\big((\gamma)\prod_{j=1}^s(\alpha_j)^{-g_j}\big) = 0$ for $i = 1, \ldots, s$ we obtain

$$\mathfrak{a} \equiv \prod_{i=1}^t \mathfrak{a}_i^{a_i} \cdot \big(\prod_{j=1}^s \overline{(\alpha_j)}^{g_j}\big) \bmod \widetilde{\mathcal{P}r}.$$

Thus all elements of $\widetilde{\mathcal{C}\ell}$ can be represented by $\overline{\mathfrak{a}}_1, \ldots, \overline{\mathfrak{a}}_t, \overline{\mathfrak{a}}_{t+1} = \overline{(\alpha_1)}, \ldots, \overline{\mathfrak{a}}_{t+s} = \overline{(\alpha_s)}$. For the two cases we obtain:

I. It follows immediately that $\overline{\mathfrak{b}}_1, \ldots, \overline{\mathfrak{b}}_{t+s}$ are generators of $\widetilde{\mathcal{C}\ell}$.

II. If we have $\overline{\mathfrak{a}} \equiv \overline{\mathfrak{a}}_1^{a_1} \cdot \cdots \cdot \overline{\mathfrak{a}}_{t+s}^{a_{t+s}} \bmod \widetilde{\mathcal{P}r}$ for an ideal $\mathfrak{a} \in \widetilde{\mathcal{I}d}$ then $0 = \deg(\overline{\mathfrak{a}}) = \sum_{i=1}^{t+s} a_i \deg_\ell(\overline{\mathfrak{a}}_i)$, thus $-a_j = \sum_{i\neq j}^s a_i \deg_\ell(\overline{\mathfrak{a}}_i)/\deg_\ell(\overline{\mathfrak{a}}_j)$. Hence $\overline{\mathfrak{b}}_1, \ldots, \overline{\mathfrak{b}}_{j-1}, \overline{\mathfrak{b}}_{j+1}, \ldots, \overline{\mathfrak{b}}_{t+s}$ are generators of $\widetilde{\mathcal{C}\ell}$.

□

We continue to use the notation from theorem 16. Set $\mathcal{C}\ell' := \mathcal{C}\ell/\langle \mathfrak{p}_1, \ldots, \mathfrak{p}_s\rangle$.

Remark 17. The definition of $\mathcal{C}\ell'$ in this section and the previous section, where we considered the ℓ-part of $\mathcal{C}\ell/\langle \mathfrak{p}_1, \ldots, \mathfrak{p}_s\rangle$, differ. The definition we chose here makes the description of the algorithm easier. In the algorithm we make sure that only the ℓ-part of the group appears in the result by computing the ℓ-adic Hermite normal form of the relation matrix.

The relations between the generators $\overline{\mathfrak{a}}_1, \ldots, \overline{\mathfrak{a}}_t$ of the group $\mathcal{C}\ell'$ are of the form $\prod_{i=1}^t \overline{\mathfrak{a}}_i^{a_i} = \overline{(\alpha)}$ with $\alpha \in \mathcal{R}_F$. There exist integers $c_1, \ldots, c_n$ such that $\overline{(\alpha)} \equiv \prod_{i=1}^s \overline{(\alpha_i)}^{c_i} \bmod \widetilde{\mathcal{P}r}$. This yields the relation $\prod_{i=1}^t \overline{\mathfrak{a}}_i^{a_i} \equiv \prod_{i=1}^s \overline{(\alpha_i)}^{c_i} \bmod \widetilde{\mathcal{P}r}$ in $\widetilde{\mathcal{C}\ell}$. We can derive all relations involving the generators $\overline{\mathfrak{a}}_i + \widetilde{\mathcal{P}r}$ from their relations as generators of the group $\mathcal{C}\ell'$ in this way.

The other relations between the generators of $\widetilde{\mathcal{C}\ell}$ are obtained as follows. A relation between the generators $\overline{\alpha}_i$ is of the form $\prod_{i=1}^s \overline{(\alpha_i)}^{v_i} \equiv (1) \bmod \mathcal{P}r$ or equivalently $\prod_{i=1}^s (\alpha_i)^{v_i} \cdot \prod_{i=1}^s \mathfrak{p}_i^{w_i} = (\alpha)$ for some $\alpha \in \mathcal{R}_F$. The last equality is fulfilled if and only if $\prod_{i=1}^s \mathfrak{p}_i^{w_i}$ is principal, *i.e.*, if $\prod_{i=1}^s \mathfrak{p}_i^{w_i}$ is an (ℓ)-unit. Assume that $\prod_{i=1}^s \mathfrak{p}_i^{w_i} = (\gamma)$ for some $\gamma \in \mathcal{R}_F$. As $\widetilde{v}_{\mathfrak{p}_j}(\alpha) = 0$ for all $\overline{(\alpha)} \in \widetilde{\mathcal{P}r}$ and $\mathfrak{p}_j \mid (\ell)$ the equation $\widetilde{v}_{\mathfrak{p}_j}\big(\prod_{i=1}^s \alpha_i^{v_i} \cdot \gamma\big) = 0$ must hold. By the definition of the β_i we obtain $v_i = -\widetilde{v}_{\mathfrak{p}_i}(\gamma)$ for $1 \le i \le s$.

Corollary 18 (Relations of $\widetilde{\mathcal{C}\ell}$). *Let $\big((\overline{\mathfrak{a}}_1, \ldots, \overline{\mathfrak{a}}_t), (a_{i,j})_{i,j\in\{1,\ldots,t\}}\big)$ be a basis and a relation matrix of $\mathcal{C}\ell' := \mathcal{C}\ell\langle \mathfrak{p}_1, \ldots, \mathfrak{p}_s\rangle$. Let $\mathfrak{a}_{t+1} = (\alpha_1), \ldots, \mathfrak{a}_{t+s} = (\alpha_s)$ be as above. For each $1 \le k \le t$ we find $c_{k,2}, \ldots, c_{k,s}$ such that $\prod_{i=1}^t \overline{\mathfrak{b}}_i^{a_{k,i}} = \prod_{i=2}^s \overline{(\alpha_i)}^{c_{k,i}}$. Let $\gamma_1, \ldots, \gamma_r$ be a basis of the (ℓ)-units of $\mathcal{R}_F$. Set $v_{i,j} := \widetilde{v}_{\mathfrak{p}_j}(\gamma_i)$ $(1 \le i \le r, 2 \le j \le s)$. Set*

$$M := \begin{pmatrix} b_{1,1} & \ldots & b_{1,t} & -c_{1,2} & \ldots & -c_{1,s} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ b_{t,1} & \ldots & b_{t,t} & -c_{t,2} & \ldots & -c_{t,s} \\ 0 & \ldots & 0 & v_{1,2} & \ldots & v_{1,s} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & v_{r,2} & \ldots & v_{r,s} \end{pmatrix}.$$

For the two cases we obtain:

I. $((\overline{\mathfrak{b}}_1, \overline{\mathfrak{b}}_{t+s}), M)$ *are generators and relations of* $\widetilde{\mathcal{C}\ell}$.

II. *Let j be chosen as in Theorem 16. Denote by N the matrix obtained by removing the j-th column from M. Then* $((\overline{\mathfrak{b}}_1, \dots, \overline{\mathfrak{b}}_{j-1}, \overline{\mathfrak{b}}_{j+1}, \dots, \overline{\mathfrak{b}}_{t+s}), N)$ *are generators and relations of* $\widetilde{\mathcal{C}\ell}$.

Now we only need to find the elements $\alpha_1, \dots, \alpha_s$ with $\widetilde{v}_{\mathfrak{p}_i}(\alpha_j) = \delta_{i,j}$. Let $\eta_{i,1}, \dots, \eta_{i,r_i}$ be a system of generators of $\mathcal{O}_{\mathfrak{p}}^{\times}$ for $1 \le i \le s$. Let

$$M := \begin{pmatrix} \widetilde{v}_{\mathfrak{p}_1}(\eta_{1,1}) & \dots & v_{\mathfrak{p}_s}(\eta_{1,1}) \\ \vdots & \ddots & \vdots \\ \widetilde{v}_{\mathfrak{p}_1}(\eta_{1,r_1}) & \dots & v_{\mathfrak{p}_s}(\eta_{1,r_1}) \\ \vdots & \vdots & \vdots \\ \widetilde{v}_{\mathfrak{p}_1}(\eta_{s,1}) & \dots & v_{\mathfrak{p}_s}(\eta_{s,1}) \\ \vdots & \ddots & \vdots \\ \widetilde{v}_{\mathfrak{p}_1}(\eta_{s,r_s}) & \dots & v_{\mathfrak{p}_s}(\eta_{s,r_s}) \end{pmatrix}.$$

Let $S = LMR$ be the ℓ-adic Smith normal form of M with transformation matrices L and R. Application of the left transformation matrix L to the generators $\eta_{1,1}, \dots, \eta_{s,r_s}$ yields elements $\alpha_1, \dots, \alpha_s$ with the desired properties.

Algorithm 19 (Logarithmic Classgroup).
Input: a number field F and a prime number ℓ
Output: generators g and and a relation matrix H for $\widetilde{Cl}_F$

- Determine a bound ℓ^m for the exponent of $\widetilde{Cl}_F$ and use it as the precision for the rest of the algorithm. [Algorithm 14]
- Compute generators $\mathfrak{a}_1, \dots, \mathfrak{a}_t$ of $\mathcal{C}\ell' = \mathcal{C}\ell / \langle \mathfrak{p}_1, \dots, \mathfrak{p}_s \rangle$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ are the ideals of F over ℓ.
- Determine $\mathfrak{a}_{t+1} = (\alpha_1), \dots, \mathfrak{a}_{t+s} = (\alpha_s)$ with $\widetilde{v}_{\mathfrak{p}_i}(\alpha_j) = \delta_{i,j}$.
- Compute generators $g := (\overline{\mathfrak{b}}_1, \dots, \overline{\mathfrak{b}}_{t+s})^T$ with $\deg(\mathfrak{b}_i) = 0$ [Theorem 16] from $\mathfrak{a}_1, \dots, \mathfrak{a}_{t+s}$.
- Compute a relation matrix M between the generators g. [Corollary 18]
- In case **II.** remove the j-th column from M and the j-th generator from g.
- Compute the ℓ-adic Hermite normal form H of M.
- Return (g, H).

4 Examples

All methods presented here have been implemented in the computer algebra system Magma [C+].

We recomputed the logarithmic class groups from [DS, section 6] with our new algorithm. Our results differ in one example. For the field $F = \mathbb{Q}(i, \sqrt{1173})$ and $\ell = 2$ we obtain $\widetilde{\mathcal{C}\ell}_F \cong C_2 \times C_2 \times C_2$ instead of $\widetilde{\mathcal{C}\ell}_F \cong C_2 \times C_2 \times C_2 \times C_2$. As F contains the 4th roots of unity, the 2-rank of the wild kernel of F is 3.

The table contains examples of logarithmic ℓ-class groups $\widetilde{\mathcal{C}\ell}$ of selected number fields F together with their class groups $\mathcal{C}\ell$, Galois groups Gal, and the factorization of the ideals (ℓ). $\chi_\alpha(x)$ denotes the minimal polynomial of α and i denotes a root of x^2+1. The class groups are presented as a list of the orders of their cyclic factors, $\mathcal{C}\ell' = \mathcal{C}\ell/\langle \mathfrak{p}_1, \ldots, \mathfrak{p}_s\rangle$, and ℓ^m is the bound for the exponent of $\widetilde{\mathcal{C}\ell}$ as returned by algorithm 14.

The logarithmic 2-class group of $\mathbb{Q}(i, \sqrt{78})$ is an example for the fact that the cokernel of θ in the exact sequence in lemma 11 is not trivial in general. Indeed one can show [DuS] that for $F = \mathbb{Q}(i, \sqrt{d})$ with $d \neq 2$ and d squarefree

$$\mathrm{Coker}(\theta) \cong \begin{cases} C_2 & \text{if } d \equiv \pm 2 \bmod 16, \\ C_1 & \text{otherwise.} \end{cases}$$

F	$\mathcal{C}\ell$	Gal	ℓ	(ℓ)	$\mathcal{C}\ell'$	ℓ^m	$\widetilde{\mathcal{C}\ell}$
$\mathbb{Q}(\sqrt{-521951})$	[1024]	$S(2)$	2	$\mathfrak{p}_1\mathfrak{p}_2$	[4]	8	[2,4]
$\mathbb{Q}(i,\sqrt{11})$	[1]	$E(4)$	5	$\mathfrak{p}_1\cdots\mathfrak{p}_4$	[1]	5	[5]
$\mathbb{Q}(i,\sqrt{78})$	[2,2]	$E(4)$	2	$\mathfrak{p}_1^4$	[2]	2	[1]
$\mathbb{Q}(i,\sqrt{455})$	[2,2,10]	$E(4)$	2	$\mathfrak{p}_1^2\mathfrak{p}_2^2$	[2,2]	512	[2,512]
$\mathbb{Q}(i,\sqrt{1173})$	[2,2,6]	$E(4)$	2	$\mathfrak{p}_1^2$	[2,2,2]	2	[2,2,2]
$\mathbb{Q}(i,\sqrt{1227})$	[4,4]	$E(4)$	613	$\mathfrak{p}_1\cdots\mathfrak{p}_4$	[4,4]	613	[613]
$\mathbb{Q}(\alpha)$	[14]	$D(4)$	2	$\mathfrak{p}_1^2\mathfrak{p}_2^2$	[1]	1	[1]
$\chi_\alpha(x) = x^4+13x^2-12x+52$			3	$\mathfrak{p}_1^2\mathfrak{p}_2^2$	[1]	3	[3]
			7	$\mathfrak{p}_1$	[14]	7	[7]
$\mathbb{Q}(\sqrt{1234577},\sqrt{-3})$	[273]	$E(4)$	2	$\mathfrak{p}_1\mathfrak{p}_2$	[273]	4	[4,4]
			3	$\mathfrak{p}_1^2$	[273]	3	[3]
			13	$\mathfrak{p}_1\mathfrak{p}_2$	[273]	169	[13,13]
$\mathbb{Q}(\zeta_3,\sqrt{303})$	[14]	$E(4)$	2	$\mathfrak{p}_1^2$	[14]	2	[2]
			3	$\mathfrak{p}_1^2\mathfrak{p}_2^2$	[1]	9	[9]
			7	$\mathfrak{p}_1\cdots\mathfrak{p}_4$	[1]	1	[1]
$\mathbb{Q}(\beta)$	[2,6,6]	$S(5)$	2	$\mathfrak{p}_1\mathfrak{p}_2$	[2,2,6]	2	[2,2,2]
$\chi_\beta(x)=x^5+2x^4+18x^3+34x^2+17x+3^{10}$			3	$\mathfrak{p}_1\cdots\mathfrak{p}_4$	[6]	3	[3]
$\mathbb{Q}(\zeta_5,\sqrt{5029})$	[15,150]	[2,4]	2	$\mathfrak{p}_1\mathfrak{p}_2$	[3,150]	4	[2,2]
			3	$\mathfrak{p}_1\mathfrak{p}_2$	[15,150]	3	[3,3]
			5	$\mathfrak{p}_1\mathfrak{p}_2$	[3,150]	25	[5,25]
$\mathbb{Q}(i,\sqrt{11},\sqrt{-499})$	[3,105]	$E(8)$	5	$\mathfrak{p}_1\cdots\mathfrak{p}_8$	[3]	25	[5,5,25]
$\mathbb{Q}(i,\sqrt{11},\gamma)$	[2,2,2,6]	$S(3)\times$	2	$\mathfrak{p}_1^2$	[2,2,2,6]	2	[2,2,2,2]
$\chi_\gamma(x) = x^3+3x^2+2x+125$		$E(4)$	3	$\mathfrak{p}_1\mathfrak{p}_2$	[2,2,2,6]	9	[3,3]
			5	$\mathfrak{p}_1\cdots\mathfrak{p}_{12}$	[2]	5	[5,5]

References

[C$^+$] J.J. Canon et al., The computer algebra system Magma, University of Sydney (2003), `http://magma.maths.usyd.edu.au/magma/`.

[C1] H. Cohen, *A course in computational algebraic number theory*, Springer Verlag, New York, 1993.

[C2] H. Cohen, *Advanced topics in computational number theory*, Springer Verlag, New York, 2000.

[DS] F. Diaz y Diaz & F. Soriano, *Approche algorithmique du groupe des classes logarithmiques,* J. Number Theory **76** (1999), 1–15.

[DuS] I. Dubois & F. Soriano, *Un nouveau reǵulateur de type Gross,* submitted Abh. Hamburg.

[FG] L.J. Federer & B.H. Gross, (with an appendix by W. Sinnot) *Regulators and Iwasawa modules,* Invent. Math. **62** (1981), 443–457.

[FPR] D. Ford, S. Pauli & X.-F. Roblot, *A fast algorithm for polynomial factorization over $\mathbb{Q}_p$*, J. Théor. Nombres Bordeaux **14** (2002), 151–170.

[Gr] G. Gras, *Class Field Theory*, Springer Monographs in Mathematics (2003).

[Ha] H. Hasse, *Number theory*, Springer Verlag, Berlin, 1980.

[He] F. Hess, *Zur Klassengruppenberechnung in algebraischen Zahlkörpern*, Diplomarbeit, TU - Berlin, 1996,
`http://www.math.TU-Berlin.DE/~kant/publications/diplom/hess.ps.gz`.

[HPP] F. Hess, S. Pauli & M.E. Pohst, *Computing the Multiplicative Group of Residue Class Rings*, Mathematics of Computation **72** (2003).

[J1] J.-F. Jaulent, *Classes logarithmiques des corps de nombres*, J. Théor. Nombres Bordeaux **6** (1994), 301–325.

[J2] J.-F. Jaulent, *Théorie ℓ-adique du corps de classes*, J. Théor. Nombres Bordeaux **10** (1998), 355–397.

[J3] J.-F. Jaulent, *Classes logarithmiques signées des corps de nombres*, J. Théor. Nombres Bordeaux **12** (2000), 455–474.

[J4] J.-F. Jaulent, *Corrigendum à Classes logarithmiques signées des corps de nombres*, J. Théor. Nombres Bordeaux **14** (2002), 1–5.

[J5] J.-F. Jaulent, *Classes logarithmiques des corps totalement réels*, Acta Arithmetica **103** (2002), 1–7.

[JS1] J.-F. Jaulent & F. Soriano, *Sur le noyau sauvage des corps de nombres et le groupe des classes logarithmiques*, Math. Z. **238** (2001), 335–354.

[JS2] Jean-François Jaulent & Florence Soriano-Gafiuk, *2-groupe des classes positives d'un corps de nombres et noyau sauvage de la K-thorie*, submitted to J. Number Theory.

[Pa] S. Pauli, *Factoring polynomials over local fields*, J. Symb. Comp. **32** (2001), 533–547.

[PZ] M.E. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, 1989.

[So] F. Soriano, *Sur le noyau hilbertien d'un corps de nombres*, C. R. Acad. Sci. Paris, t. 330, Série I (2000), 863-866.

Francisco Diaz y Diaz
Université Bordeaux I
Laboratoire A2X
351 Cours de la Libération
33405 Talence Cedex, France
diaz@math.u-bordeaux.fr

Jean-François Jaulent
Université Bordeaux I
Institut des Mathématiques de Bordeaux
351 Cours de la Libération
33405 Talence Cedex, France
jaulent@math.u-bordeaux.fr

Florence Soriano-Gafiuk
Université de Metz
Département de Mathématiques
Ile du Saulcy
57000 Metz, France
soriano@poncelet.univ-metz.fr

Sebastian Pauli
Technische Universität Berlin
Institut für Mathematik - MA 8-1
Straße des 17. Juni 136
10623 Berlin, Germany
pauli@math.tu-berlin.de

Michael E. Pohst
Technische Universität Berlin
Institut für Mathematik - MA 8-1
Straße des 17. Juni 136
10623 Berlin, Germany
pohst@math.tu-berlin.de