The logarithmic class group package in PARI/GP*

Karim Belabas and Jean-François Jaulent

Abstract. This note presents our implementation in the PARI/GP system of the various arithmetic invariants attached to logarithmic classes and units of number fields. Our algorithms simplify and improve on works of Diaz y Diaz, Pauli, Pohst, Soriano and the second author.

Résumé. (*Le groupe des classes logarithmiques dans PARI/GP*) Cette note présente notre implantation dans le système PARI/GP du calcul des invariants arithmétiques liés aux classes et unités logarithmiques des corps de nombres. Nos algorithmes prolongent et simplifient ceux introduits par Diaz y Diaz, Pauli, Pohst, Soriano et le second auteur.

Contents

1 Introduction **2**

2 Algorithmic preliminaries **4**
- 2.1 The Smith Normal Form 4
- 2.2 Computational algebraic number theory 5
- 2.3 Local norms 6

3 The main algorithm **6**
- 3.1 Computing $\widetilde{e}(\mathfrak{p}/p)$, $\widetilde{f}(\mathfrak{p}/p)$ and $\widetilde{v}_{\mathfrak{p}}(\cdot)$ 7
- 3.2 The group $\mathcal{C}l'$ 9
- 3.3 The group $\widetilde{\mathcal{C}l}(\ell)$ 10
- 3.4 The logarithmic class group 11

4 The bnflog package **12**
- 4.1 The PARI/GP interface 12
- 4.2 Examples 13

*Pub. Math. Besançon 2016, 5–18.

1 Introduction

Classically the class group and unit group of a number field F are defined using the canonical factorization of principal fractional ideals into prime ideals of the ring of integers $\mathbb{Z}_F$:

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}, \quad x \in F^{\times}.$$

The family of valuations $(v_{\mathfrak{p}})_{\mathfrak{p}}$ determines a natural morphism from the multiplicative groupe $F^{\times}$ into the free abelian group generated by the prime ideals $I_F = \oplus_{\mathfrak{p}} \mathbb{Z}\,\mathfrak{p}$ whose kernel and cokernel are respectively the units $E_F = \mathbb{Z}_F^{\times}$ and the ideal class group $\mathcal{C}\ell_F$ attached to F; this yields the standard exact sequence

$$1 \longrightarrow E_F \longrightarrow F^{\times} \xrightarrow{\text{div}} I_F = \oplus_{\mathfrak{p}} \mathbb{Z}\,\mathfrak{p} \longrightarrow \mathcal{C}\ell_F \longrightarrow 1,$$

where $\text{div}(x) = \big(v_{\mathfrak{p}}(x)\big)_{\mathfrak{p}}$. Geometry of numbers then shows on the one hand that the ideal class group is finite and on the other hand that the unit group E_F is the direct product of the cyclic subgroup μ_F of roots of unity contained in F and a free $\mathbb{Z}$-module of rank $r_F + c_F - 1$, where r_F are c_F denote respectively the number of real and complex places of F.

The logarithmic class group and units are defined in an analogous way, by replacing the classical valuations $(v_{\mathfrak{p}})_{\mathfrak{p}}$ by an ad hoc familly $(\widetilde{v}_{\mathfrak{p}})_{\mathfrak{p}}$ taking other arithmetic parameters into account. Before introducing them, let us fix an arbitrary prime number ℓ and tensor the above sequence by $\mathbb{Z}_\ell$, which is flat over $\mathbb{Z}$:

$$1 \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E_F \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} F^{\times} \xrightarrow{\text{div}} \oplus_{\mathfrak{p}} \mathbb{Z}_\ell\,\mathfrak{p} \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{C}\ell_F \longrightarrow 1,$$

where $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{C}\ell_F$ is nothing else than the ℓ-Sylow subgroup of the class group and the kernel $\mathbb{Z}_\ell \otimes E_F$ is the direct product of the ℓ-group $\mu_F^{(\ell)}$ of ℓ-primary roots of unity in F and a free $\mathbb{Z}_\ell$-module of rank $r_F + c_F - 1$.

We now define the ℓ-adic logarithmic valuations by keeping the ordinary definition $\widetilde{v}_{\mathfrak{p}} = v_{\mathfrak{p}}$ at places $\mathfrak{p} \nmid \ell$, but we modify them at places $\mathfrak{p}$ above ℓ [16]:

$$\widetilde{v}_{\mathfrak{p}}(x) = -\frac{\text{Log}_\ell\left(\text{N}_{K_{\mathfrak{p}}/\mathbb{Q}_\ell}(x)\right)}{\deg \mathfrak{p}},$$

where Log_ℓ is the Iwasawa logarithm, $\text{N}_{K_{\mathfrak{p}}/\mathbb{Q}_\ell}$ is the norm operator attached to the local field extension $K_{\mathfrak{p}}/\mathbb{Q}_\ell$ and $\deg \mathfrak{p}$ is a normalization factor chosen so as to yield the local Hilbert symbol [14]:

$$\left(\frac{\zeta, x}{\mathfrak{p}}\right) = \zeta^{\widetilde{v}_{\mathfrak{p}}(x)}$$

for $\zeta \in \mu_F^{(\ell)}$ and $x \in F^{\times}$, for all finite places $\mathfrak{p}$ of F. (We shall give an explicit definition for $\deg \mathfrak{p}$ in the next section together with an algorithm to approximate it.) We finally replace in the last exact sequence the classical valuations $v_{\mathfrak{p}}$ and the div map by a new

$\widetilde{\operatorname{div}} = (\widetilde{v}_{\mathfrak{p}})_{\mathfrak{p}}$, thereby defining the group of logarithmic units $\widetilde{\mathcal{E}}_F$ and the logarithmic class group $\widetilde{\mathcal{C}l}_F$ for the prime ℓ:

$$1 \longrightarrow \widetilde{\mathcal{E}}_F \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} F^\times \xrightarrow{\widetilde{\operatorname{div}}} \oplus_{\mathfrak{p}} \mathbb{Z}_\ell\, \mathfrak{p} \longrightarrow \widetilde{\mathcal{C}l}_F \longrightarrow 1.$$

Just as the image $P_F = \operatorname{div}(F^\times)$ in I_F yields the subgroup of principal ideals, the image $\mathcal{P}_F$ of $\widetilde{\operatorname{div}}$ defines the subgroup of principal logarithmic divisors.

At this point appears an essential difference compared to the classical case, akin to what happens in the function field case: if we define the degree of a logarithmic divisor $\mathfrak{d} = \sum_{\mathfrak{p}} \alpha_{\mathfrak{p}} \mathfrak{p}$ in $\oplus_{\mathfrak{p}} \mathbb{Z}_\ell\, \mathfrak{p}$ additively,

$$\deg\left(\sum_{\mathfrak{p}} \alpha_{\mathfrak{p}}\ \mathfrak{p}\right) = \sum_{\mathfrak{p}} \alpha_{\mathfrak{p}} \deg \mathfrak{p},$$

then the product formula for absolute values shows that principal logarithmic divisors have degree 0; in other words,

$$\mathcal{P}_F \subset \{\mathfrak{d} \in \oplus_{\mathfrak{p}} \mathbb{Z}_\ell\, \mathfrak{p} \colon\ \deg \mathfrak{d} = 0\}\,.$$

It is then natural to consider the quotient group, i.e. the subgroup $\widetilde{\mathcal{C}l}_F^{\,0} \subset \widetilde{\mathcal{C}l}_F$ formed by the classes of degree 0.

By ℓ-adic class field theory (cf. [15, 8]), the group $\widetilde{\mathcal{C}l}_F^{\,0}$ appears as a canonical quotient of a standard Iwasawa module and the group of logarithmic units $\widetilde{\mathcal{E}}_F$ as the subgroup of norms in the cyclotomic $\mathbb{Z}_\ell$-extension of F. It would follow from a conjecture of Kuz'min (also known as "generalized Gross conjecture") that the group $\widetilde{\mathcal{C}l}_F^{\,0}$ is finite, or equivalently that the group $\widetilde{\mathcal{E}}_F$ of logarithmic units is the direct product of the cyclic ℓ-groupe $\mu_F^{(\ell)}$ and a free $\mathbb{Z}_\ell$-module of rank $r_F + c_F$; and the Gross-Kuz'min conjecture is equivalent to these statements. The Baker-Brumer independence theorem shows that those assertions are true when the number field F is abelian over $\mathbb{Q}$. More generally, they hold when there exist a subfield K of F, abelian over $\mathbb{Q}$, such that there is a single place $\mathfrak{p}_F$ of F above each ℓ-adic place $\mathfrak{p}_K$ of K, see [10].

Moreover, as suggested by the explicit expression of the Hilbert symbol above, the group $\widetilde{\mathcal{C}l}_F^{\,0}$ is closely related to the wild kernels of K-theory. Precisely, if $s \geqslant 1$ is such that the field F contains the $2\ell^s$-th roots of unity, then the finite group $WK_2(F)$ and the quotient $\widetilde{\mathcal{C}l}_F^{\,0} \otimes_{\mathbb{Z}} \mathbb{Z}/\ell^s\mathbb{Z}$ have the same ℓ^s-rank (cf. [19]). A similar result holds for the higher étale kernels $WK_{2i}(K)$, $i \geqslant 1$ (cf. [17]).

Last, as for ideals, transition morphisms (norm and extension) attached to a number field extension K/F lead to the definition of logarithmic inertia degrees $\widetilde{f}(\mathfrak{p}_K/\mathfrak{p}_F)$ and ramification indices $\widetilde{e}(\mathfrak{p}_K/\mathfrak{p}_F)$ for $\mathfrak{p}_K \subset \mathbb{Z}_K$ dividing $\mathfrak{p}_F \subset \mathbb{Z}_F$, with formal properties analogous to the classical indices $e(\mathfrak{p}_K/\mathfrak{p}_F)$ and $f(\mathfrak{p}_K/\mathfrak{p}_F)$, without coinciding with them. These local indices are multiplicative and satisfy the product formula

$$\widetilde{e}(\mathfrak{p}_K/\mathfrak{p}_F)\widetilde{f}(\mathfrak{p}_K/\mathfrak{p}_F) = e(\mathfrak{p}_K/\mathfrak{p}_F) f(\mathfrak{p}_K/\mathfrak{p}_F) = [K_{\mathfrak{p}} : F_{\mathfrak{p}}].$$

They are introduced as follows: by multiplicativity, it suffices to define $\widetilde{f}(\mathfrak{p}_F/p)$ since $\widetilde{f}(\mathfrak{p}_K/\mathfrak{p}_F) = \widetilde{f}(\mathfrak{p}_K/p) / \widetilde{f}(\mathfrak{p}_F/p)$. Now let $F_{\mathfrak{p}}^{ab}$ be the maximal subextension of the local field $F_{\mathfrak{p}}$ which is abelian over $\mathbb{Q}_p$. The classical inertia degree $f(\mathfrak{p}/p)$ is the degree $[F_{\mathfrak{p}}^{ab} \cap \mathbb{Q}_p^{unr} : \mathbb{Q}_p]$, where $\mathbb{Q}_p^{unr}$ denotes the *unramified* $\hat{\mathbb{Z}}$-extension of $\mathbb{Q}_p$. The logarithmic inertia degree is the degree $[F_{\mathfrak{p}}^{ab} \cap \mathbb{Q}_p^{c} : \mathbb{Q}_p]$, where $\mathbb{Q}_p^{c}$ is the *cyclotomic* $\hat{\mathbb{Z}}$-extension of $\mathbb{Q}_p$. In particular the logarithmic indices do not depend on the choice of the prime ℓ.

One says that the extension K/F ramifies logarithmically at a finite prime $\mathfrak{p}_F$ whenever $\widetilde{e}(\mathfrak{p}_K/\mathfrak{p}_F) > 1$ for some $\mathfrak{p}_K \mid \mathfrak{p}_F$. As in the classical case, an extension of number fields is unramified (in the logarithmic sense) except at a finite number of primes. However a logarithmically unramified extension may ramify in the ordinary sense. Such extensions play a crucial role in the capitulation for the Bertrandias-Payan module studied in the present volume (cf. [9, 11, 20]).

This note presents our implementation in the PARI/GP system of the various arithmetic invariants attached to logarithmic classes and units. The algorithms do not depend on any conjecture: if the program stops, its output is correct, and it in fact proves that the Gross-Kuz'min conjecture holds for that particular prime ℓ and number field F.

Acknowledgements: we thank Sebastian Pauli for sharing his Magma implementation, José Villanueva-Gutiérrez for feedback and examples, and Bill Allombert for many useful discussions.

2 Algorithmic preliminaries

We recall in this section well known facts from computational number theory, to fix notations. The next section will deal with the main algorithms, germane to the computation of logarithmic objects.

2.1 The Smith Normal Form

We say that a $\mathbb{Z}$-module of finite type G is known if

- we have a Smith Normal Form description (SNF)

$$G = \bigoplus_{1 \leqslant i \leqslant s} \mathbb{Z}/(d_i) \cdot g_i,$$

  for some generators g_i, where $d_s \mid \cdots \mid d_1$ are the elementary divisors of G; if G has a free part of rank r, then $d_1 = \cdots = d_r = 0$. If $r = 0$, then G is finite and its exponent $\mathrm{e}(G)$ is d_1.

- we can solve discrete logarithm problems in G, i.e. decompose elements $x \in G$ as $x = \sum_{i \leqslant s} x_i \cdot g_i$, where $x_i \in \mathbb{Z}/(d_i)$.

More generally, let R be a matrix in $M_{s\times t}(\mathbb{Z})$. A $\mathbb{Z}$-module of finite type G is given by generators $(g_1,\dots,g_s)$ and relations R when $(g_1,\dots,g_s)\cdot X = 0_G$ holds for some $X\in\mathbb{Z}^s$ if and only if $X = MY$ for some $Y\in\mathbb{Z}^t$. In that case, there exist matrices $U\in\mathrm{GL}_s(\mathbb{Z})$ and $V\in\mathrm{GL}_t(\mathbb{Z})$ such that UMV is in Smith Normal Form (SNF), i.e.

$$UMV = (D \mid 0) \ \text{ when } t\geqslant s \quad\text{or}\quad \begin{pmatrix} D\\ 0\end{pmatrix} \ \text{ when } t\leqslant s,$$

where D is the diagonal matrix $\mathrm{diag}(d_1,\dots,d_s)$. In both cases, $(g_1,\dots,g_s)\cdot U^{-1}$ are SNF generators of order $d_s \mid \cdots \mid d_1$. The SNF algorithm applied to R produces U and V in polynomial time (in s, t and $\log\|R\|_2$).

The same technique allows to handle $\mathbb{Z}_\ell$-modules: when $R\in M_{s\times t}(\mathbb{Z}_\ell)$, there exist $U\in\mathrm{GL}_s(\mathbb{Z}_\ell)$ and $V\in\mathrm{GL}_t(\mathbb{Z}_\ell)$ such that UMV is in SNF. Given $M_N = M \bmod \ell^N$, the above algorithm applied to $(M_N \mid \ell^N\,\mathrm{Id}_s)$ produces U and V modulo ℓ^N and the matrix U^{-1} modulo ℓ^N describing SNF generators for $G\otimes_{\mathbb{Z}}\mathbb{Z}/(\ell^N)$, the running time is now polynomial in s, t and $N\log\ell$.

2.2 Computational algebraic number theory

The number field F of degree n is given by the minimal polynomial $T\in\mathbb{Z}[X]$ of an integral generating element, in other words $F=\mathbb{Q}[X]/(T)$. We write $\overline{X}$ for the class of $X \bmod T$; an element $\alpha\in F$ is given by a rational polynomial $A\in\mathbb{Q}[X]$ such that $\alpha = A(\overline{X})$. For any $\alpha\in F$ we let $\|\alpha\| = \prod_v \max(1,|\alpha|_v)$ where v runs through all places of F and $|\alpha|_v$ is the attached normalized absolute value. We assume given a $\mathbb{Z}$-basis of its maximal order $\mathbb{Z}_F$. This is in general an expensive invariant, not necessary for all our algorithms, for instance Algorithm 1 and Corollary 3.5; on the other hand current algorithms to compute the class group of F and the unit group $\mathbb{Z}_F^\times$ require it.

We further assume that the class group $\mathcal{C}l_F$ and unit group E_F are known in the sense of 2.1. In the context of the class group $\mathcal{C}l_F$, the discrete logarithm problem is solved in I_F in the following extended sense. The generators classes are represented by integral ideals g_i; given a fractional ideal $\mathfrak{a}$ in I_F, we can find $\alpha\in F^\times$ so that our ideal decomposes as a product of the generators g_i multiplied by the principal ideal (α). We refer to [3] for how to handle these standard tasks. Practical algorithms to compute $\mathcal{C}l_F$ and E_F require assuming the truth of the Generalized Riemann Hypothesis for the unramified Hecke L-functions $L_F(\chi,s)$, $\chi\in\widehat{\mathcal{C}l_F}$, and for the Riemann ζ function. But this assumption can be lifted provided the discriminant $\operatorname{disc} F$ is not too large. (The certification process requires time proportional to $\sqrt{|\operatorname{disc} F|}$.)

To each maximal ideal $\mathfrak{p}\subset\mathbb{Z}_F$ above a rational prime p we attach the completed local field $F_\mathfrak{p}$. There exist an irreducible monic divisor $T_\mathfrak{p}\in\mathbb{Z}_p[X]$ of T, of degree $n_\mathfrak{p} = [K_\mathfrak{p}:\mathbb{Q}_p] = e(\mathfrak{p}/p)f(\mathfrak{p}/p)$, such that $K_\mathfrak{p} = \mathbb{Q}_p[X]/(T_\mathfrak{p})$. Given T and a prime p, and for any given p-adic accuracy k, we can produce in polynomial time $O(k\log p\cdot n\log\|T\|_\infty)^C$

- the prime ideals $\mathfrak{p}_i = p\mathbb{Z}_F + \pi_i\mathbb{Z}_F$ dividing p, together with their ramification indices and residue degrees, where $v_{\mathfrak{p}_i}(\pi_i) = 1$ (this is automatic if $e(\mathfrak{p}_i/p) > 1$ and one of π_i or $\pi_i + p$ satisfy this condition in any case);

- for each $\mathfrak{p}_i$, a p-adic approximation $T_{\mathfrak{p}_i,k} \in \mathbb{Z}[X]$ such that $T_{\mathfrak{p}_i,k} \equiv T_{\mathfrak{p}_i} \pmod{p^k}$;

see for instance the Round 4 algorithm as finalized in [7]. The older (and much simpler) Round 2 algorithm and Buchmann-Lenstra factorization would also achieve this result, see [2].

2.3 Local norms

We shall need to compute local norms and their Iwasawa logarithms. We can write any $\alpha \in F^\times$ as $A(\overline{X})/a$ for $a \in \mathbb{Z}_{>0}$ and $A \in \mathbb{Z}[X]$ and the representation is unique if a and the content of A are coprime. Since $N_{F_\mathfrak{p}/\mathbb{Q}_p}(a) = a^{n_\mathfrak{p}}$, we may focus on $\alpha \in \mathbb{Z}[\overline{X}]$.

Lemma 2.1. *Let $\alpha = A(\overline{X})$, $\alpha \neq 0$, where $A \in \mathbb{Z}[X]$. For each integer $k > v_p\left(\mathrm{N}_{F_\mathfrak{p}/\mathbb{Q}_p}(\alpha)\right)$, let $N_k = \mathrm{Res}(A, T_{\mathfrak{p},k}) \bmod p^k \in \mathbb{Z}$ then*

$$\mathrm{N}_{F_\mathfrak{p}/\mathbb{Q}_p}(\alpha) \equiv N_k \pmod{p^k}.$$

In particular, $v_p(N_k) = v_p\left(\mathrm{N}_{F_\mathfrak{p}/\mathbb{Q}_p}(\alpha)\right)$ does not depend on k and

$$\mathrm{Log}_p \mathrm{N}_{F_\mathfrak{p}/\mathbb{Q}_p}(\alpha) \equiv \mathrm{Log}_p N_k \pmod{p^{k-v_p(N_k)}}.$$

Note that if the size $\|\alpha\|$ of α is controlled, so is $\left|\mathrm{N}_{F/\mathbb{Q}}(\alpha)\right| \leqslant \|\alpha\|^n$. Thus $v_p(N_k) \leqslant v_p\left(\mathrm{N}_{F/\mathbb{Q}}(\alpha)\right)$ is controlled and finally, any $k > v_p\left(\mathrm{N}_{F/\mathbb{Q}}(\alpha)\right)$ satisfies the condition in the lemma. This allows to approximate $\widetilde{v}_\mathfrak{p}(\alpha)$ to any given accuracy from a sufficiently precise approximation $T_{\mathfrak{p},k}$ of $T_\mathfrak{p}$.

3 The main algorithm

We follow the general strategy of [6], while introducing numerous improvements and simplifications along the way. Let ℓ be a fixed prime number and denote $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_l\}$ the set of places of F above ℓ. We rely on the obvious exact sequence of pro-ℓ groups

$$0 \longrightarrow \widetilde{\mathcal{C}\ell}(\ell) \longrightarrow \widetilde{\mathcal{C}\ell} \xrightarrow{\psi} \mathcal{C}\ell' \longrightarrow 0$$

where $\widetilde{\mathcal{C}\ell}(\ell)$ is the subgroup generated by the logarithmic classes of the $\mathfrak{p}_i$, the group $\mathcal{C}\ell'$ is the ℓ-Sylow subgroup of the quotient of the ideal class group by the subgroup generated by the ideal classes of the $\mathfrak{p}_i$, and where

$$\psi : \sum_{\mathfrak{p}} m_\mathfrak{p} \mathfrak{p} \longmapsto \prod_{\mathfrak{p} \nmid \ell} \mathfrak{p}^{m_\mathfrak{p}}.$$

We shall compute the groups $\widetilde{\mathcal{C}\ell}(\ell)$ and $\mathcal{C}\ell'$ independently, by generators and relations, then build up $\widetilde{\mathcal{C}\ell}$ using the exact sequence.

Remark 3.1. We depart here from [5, 6] which use $\theta : \sum_{\mathfrak{p}} m_{\mathfrak{p}}\mathfrak{p} \mapsto \prod_{\mathfrak{p}\nmid\ell} \mathfrak{p}^{(\widetilde{f}_{\mathfrak{p}}/f_{\mathfrak{p}})m_{\mathfrak{p}}}$. The latter has good properties in extensions, which we will not need. When the field is fixed, it makes no difference: for $\mathfrak{p} \nmid \ell$, the factor $\widetilde{f}_{\mathfrak{p}}/f_{\mathfrak{p}}$ belongs to $\mathbb{Z}_\ell^\times$ so the kernel and cokernel of θ and ψ are the same. More substantially, we do not restrict to degree 0 divisors $\widetilde{Cl}(\ell)^0$ and $\widetilde{Cl}^0$ at this stage, which would introduce a nontrivial cokernel (as some ideal classes might not be representable by degree 0 divisors). This avoids the technical difficulty of having to modify natural generators so that their degree become zero as in [6, Corollary 18]. This is not obvious and Corollary 18 is incorrect as stated.

3.1 Computing $\widetilde{e}(\mathfrak{p}/p)$, $\widetilde{f}(\mathfrak{p}/p)$ and $\widetilde{v}_{\mathfrak{p}}(\cdot)$

We first explain how to compute the logarithmic inertia and residue degrees. The algorithm is a straightforward consequence of the following two lemmas:

Lemma 3.2. *Let $\mathfrak{p}$ be a maximal ideal above a rational prime p. We write e, f, $\widetilde{e}$, $\widetilde{f}$ respectively for $e(\mathfrak{p}/p)$ $f(\mathfrak{p}/p)$, $\widetilde{e}(\mathfrak{p}/p)$ and $\widetilde{f}(\mathfrak{p}/p)$.*

(1) *We have $\widetilde{e}\widetilde{f} = n_{\mathfrak{p}} = ef$.*

(2) *The prime to p part of $\widetilde{e}$ and e coincide, i.e. $v_q(e) = v_q(\widetilde{e})$ for all primes $q \neq p$.*

(3) *The logarithmic ramification index $\widetilde{e}$ and $[h_{\mathfrak{p}}(F_{\mathfrak{p}}^\times) : \mathbb{Z}_p]$ have the same valuation at p, where*

$$h_{\mathfrak{p}}(\alpha) = \frac{\operatorname{Log}_p \mathrm{N}_{F_{\mathfrak{p}}/\mathbb{Q}_p}(\alpha)}{n_{\mathfrak{p}} \cdot (2p)}.$$

Note that $h_{\mathfrak{p}}(\mathbb{Q}_p^\times) = \mathbb{Z}_p$.

(4) *We have $v_p(\widetilde{f}) \leqslant v_p(e)$. In particular if $p \nmid e$, then $v_p(\widetilde{e}) = v_p(f)$ and $v_p(\widetilde{f}) = 0$.*

Proof. The first three points are proved in [13]. The final one follows from a direct calculation using $h_{\mathfrak{p}}$ or using the abstract definition $\widetilde{f}(\mathfrak{p}/p) = [F_{\mathfrak{p}}^{ab} \cap \widehat{\mathbb{Q}}_p^c \colon \mathbb{Q}_p]$, where $\widehat{\mathbb{Q}}_p^c$ is the compositum of all cyclotomic $\mathbb{Z}_q$ extensions of $\mathbb{Q}_p$ on all prime numbers q. Thus the p-primary part of $\widetilde{f}$ is the degree over $\mathbb{Q}_p$ of the intersection L of $F_{\mathfrak{p}}^{ab}$ with the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$. The claim follows by multiplicativity of ramification indices in $F_{\mathfrak{p}}/L/\mathbb{Q}_p$. □

Lemma 3.3. *Let $\mathfrak{p}$ be a maximal ideal above the prime p with ramification index $e = e(\mathfrak{p}/p)$. Let $\mathcal{D} = \mathcal{D}_{F_{\mathfrak{p}}/\mathbb{Q}_p}$ denote the local different and let $k > e/(p-1)$. Then $\operatorname{Log}_p \mathrm{N}_{F_{\mathfrak{p}}/\mathbb{Q}_p}(1+\mathfrak{p}^k) = p^{\lfloor v/e \rfloor}\mathbb{Z}_p$, where $v = k + v_{\mathfrak{p}}(\mathcal{D})$.*

Proof. For $k > e/(p-1)$, we have $1 + \mathfrak{p}^k = \exp(\mathfrak{p}^k)$ and $\operatorname{Log}_p \mathrm{N}_{F_{\mathfrak{p}}/\mathbb{Q}_p}(1+\mathfrak{p}^k) = \operatorname{Tr}_{F_{\mathfrak{p}}/\mathbb{Q}_p}(\mathfrak{p}^k)$. We then use the equivalence $\operatorname{Tr}_{F_{\mathfrak{p}}/\mathbb{Q}_p} \mathfrak{p}^k \subset \mathfrak{a} \Leftrightarrow \mathfrak{p}^k\mathcal{D} \subset \mathfrak{a}$ for any fractional ideal $\mathfrak{a} \subset \mathbb{Q}_p$. □

Algorithm 1 Compute $\widetilde{e}(\mathfrak{p}/p)$, $\widetilde{f}(\mathfrak{p}/\mathfrak{p})$

Input: A maximal ideal $\mathfrak{p} = p\mathbb{Z}_F + \pi\mathbb{Z}_F$, $v_\mathfrak{p}(\pi) = 1$ above some prime p of ramification index $e = e(\mathfrak{p}/p)$ and residue degree $f = f(\mathfrak{p}/p)$.

Output: $\widetilde{e} = \widetilde{e}(\mathfrak{p}/p)$ and $\widetilde{f} = \widetilde{f}(\mathfrak{p}/p)$.

1: If $v_p(e) = 0$, set $\widetilde{e} \leftarrow e \cdot p^{v_p(f)}$, $\widetilde{f} \leftarrow f \cdot p^{-v_p(f)}$ and stop.

2: Let $n_\mathfrak{p} \leftarrow ef$ and let $k \leftarrow 1 + \lfloor e/(p-1) \rfloor > 1$.

3: Let $g_0 \leftarrow \pi$ and let $(g_1, \ldots, g_s)$ be independent generators for the finite abelian group $(1+\mathfrak{p})/(1+\mathfrak{p}^k)$; see [4, §4.2.3].

4: Let $v \leftarrow \min_{0\leqslant i\leqslant s} v_p\left(\mathrm{Log}_p \mathrm{N}_{F_\mathfrak{p}/\mathbb{Q}_p}(g_i)\right)$, computed using Lemma 2.1.

5: Let $v_\infty = \left\lfloor \left(k + v_\mathfrak{p}(\mathcal{D}_{F_\mathfrak{p}/\mathbb{Q}_p})\right)/e \right\rfloor$. If $v_\infty < v$, let $v \leftarrow v_\infty$.

6: Let $v \leftarrow v - v_p(f \cdot 2p)$. Set $\widetilde{e} \leftarrow e \cdot p^{-v}$ and $\widetilde{f} \leftarrow f \cdot p^v$.

Proof. The problem boils down to computing the valuation at p of $\widetilde{e}(\mathfrak{p}/p)$. Using statement (3) in the lemma, this is the non-negative integer w such that $h_\mathfrak{p}(F_\mathfrak{p}^\times) = p^{-w}\mathbb{Z}_p$. We decompose $F_\mathfrak{p}^\times = \pi^\mathbb{Z} \times \mu_{F_\mathfrak{p}} \times (1+\mathfrak{p}\mathbb{Z}_{F_\mathfrak{p}})$; since $h_\mathfrak{p}$ is additive and $h_\mathfrak{p}(\mu_{F_\mathfrak{p}}) = 0$, it is enough to determine the valuation of $h_\mathfrak{p}$ evaluated at π and on multiplicative generators of $1 + \mathfrak{p}\mathbb{Z}_{F_\mathfrak{p}}$, i.e. on generators of $(1+\mathfrak{p})/(1+\mathfrak{p}^k)$ and $1+\mathfrak{p}^k$; the latter are handled by Lemma 3.3 yielding the v_∞ contribution. □

Remark 3.4. By Lemma 3.3, if generator $g = g_i$ of the p-group $(1+\mathfrak{p})/(1+\mathfrak{p}^k)$ has order $d = d_i$, then $\mathrm{Log}_p \mathrm{N}(g^d)$ has valuation $\geqslant v_\infty$. So, when we compute the minimum of the valuations incrementally for $g_1, g_2, \ldots$, by decreasing order, we can stop as soon the lower bound $v_\infty - v_p(d_i)$ for the valuation of $\mathrm{Log}_p \mathrm{N}(g_i)$ becomes larger than the current minimum. We can also restrict to the generators of $(1+\mathfrak{p})/(1+\mathfrak{p}^k)$ modulo the p-primary roots of unity in $F_\mathfrak{p}$. Finally, we compute $v_p\left(\mathrm{Log}_p \mathrm{N}_{F_\mathfrak{p}/\mathbb{Q}_p}(g_i)\right)$ as $v_p\left(\mathrm{N}_{F_\mathfrak{p}/\mathbb{Q}_p}(g_i) - 1\right)$ for $i > 0$.

In comparison, the algorithms of [6, §3.1] need the full set of multiplicative generators of $1 + \mathfrak{p}\mathbb{Z}_{F_\mathfrak{p}}$, whose description is complicated and uses the principal unit filtration up to $k = pe/(p-1)$. Introducing v_∞ thus reduces the size of the generator system by a rough factor p; and we in fact expect to consider only g_0 and g_1 due to the a priori lower bound $v_\infty - v_p(d_i)$. The early abort when $v_p(e) = 0$ also skips the non-trivial part of the algorithm unless p belongs to the tiny set of (wildly ramified) prime divisors of $[F : \mathbb{Q}]$.

Corollary 3.5. *Let ℓ be our fixed prime and $\mathfrak{p}$ be a maximal ideal above some prime p. Lemma 2.1 and Algorithm 1 allow to compute the following quantities to any desired ℓ-adic accuracy in time polynomial in $\log \ell$, $\log p$, n, $\log \|T\|_\infty$ and $\log \|x\|$*

(1) $\deg \mathfrak{p} = \widetilde{f}(\mathfrak{p}/p) \deg_\ell p$, *where* $\deg_\ell p = \begin{cases} \mathrm{Log}_\ell\, p & \text{if } p \neq \ell, \\ \ell & \text{if } p = \ell \neq 2, \\ 4 & \text{if } p = \ell = 2. \end{cases}$

(2) *For* $x \in F^\times$, $\widetilde{v}_{\mathfrak{p}}(x) = \begin{cases} v_{\mathfrak{p}}(x) & \text{if } p \neq \ell, \\ -\dfrac{\mathrm{Log}_p\left(\mathrm{N}_{F_{\mathfrak{p}}/\mathbb{Q}_p}(x)\right)}{\deg \mathfrak{p}} & \text{if } p = \ell. \end{cases}$

Remark 3.6. The logarithmic degree $\deg_\ell \ell$ may be multiplied by an ℓ-adic unit without changing the structure of $\widetilde{\mathcal{C}l}$. In other contexts, defining respectively

$$\deg_\ell \ell = \mathrm{Log}_\ell(1+\ell) \quad \text{and} \quad \mathrm{Log}_2(1+4)$$

will be more convenient. Indeed, with the latter definition, the exponential of $\deg \mathfrak{p}$ would always be a natural number.

3.2 The group $\mathcal{C}l'$

Let S be the set of places above ℓ. We compute the S-class group

$$\mathcal{C}l_F / \langle S \rangle = \bigoplus_{1 \leqslant i \leqslant s} (\mathbb{Z}/d_i\mathbb{Z}) \cdot g_i,$$

where each g_i has order d_i and $d_s \mid \cdots \mid d_1$, using the obvious definition by generators (the g_i generating the class group) and relations (the subgroup generated by the classes of elements of S) and computing the attached SNF, see [4, §7.4.2]. We obtain its ℓ-Sylow subgroup $\mathcal{C}l'$ by raising each SNF generator g_i to the power $d_i \ell^{-v_\ell(d_i)}$. Alternatively, we can first read off the exponent $e = \ell^{v_\ell(d_1)}$ of $\mathcal{C}l'$ from the SNF description of $\mathcal{C}l_F/\langle S \rangle$, then compute its ℓ-adic SNF by adding $g_i^e = 1$, $i \leqslant s$, to the relations. The latter method is likely to yield smaller base change matrices, hence smaller generators. In any case, the generators of $\mathcal{C}l'$ are represented by integral ideals in $\mathbb{Z}_F$, which we may assume to be coprime to ℓ. Indeed, if $g \subset \mathbb{Z}_F$ is an arbitrary generator and $(g_{\mathbb{Z}}) = g \cap \mathbb{Z}$, we can replace g by

$$g + \left(g_{\mathbb{Z}} \cdot \ell^{-v_\ell(g_{\mathbb{Z}})}\right) \mathbb{Z}_F = g \cdot \prod_{\mathfrak{p} \mid \ell} \mathfrak{p}^{-v_{\mathfrak{p}}(g)}.$$

Solving the discrete logarithm problem is a standard extension, see [4, §4.1.3]. The only thing to note is that as described the algorithm will produce huge generators, as the initial class group generators are raised to huge powers through the necessary linear algebra. We use the "group ring representation" from [1, §7] keeping principal ideals in factored form, i.e. as elements in $\mathbb{Z}[\mathbb{Z}_F]$, and LLL-reducing general ideals along the way; in this manner the principal parts, in class groups or S-class groups discrete logarithm decompositions, are obtained in the form $\alpha = \prod_{i \leqslant r} \alpha_i^{e_i}$, where the α_i are small elements in F ($\|\alpha_i\|$ is controlled) and the e_i are possibly large integers.

Definition 3.7. For any $\alpha \in \mathbb{Z}[\mathbb{Z}_F]$ given in factored representation we write $x \in \operatorname{Supp} \alpha$ when x belongs to the support of α, i.e. is one of the $\alpha_i \in \mathbb{Z}_F$ occuring in the factored representation.

This factored representation of elements is quite suitable to compute multiplicative or additive functions such as local norms and their ℓ-adic logarithms, or standard and logarithmic valuations $v_{\mathfrak{p}}$ and $\widetilde{v}_{\mathfrak{p}}$.

3.3 The group $\widetilde{\mathcal{C}l}(\ell)$

We describe $\widetilde{\mathcal{C}l}(\ell)$ by generators (the classes of the ℓ-adic places $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_l\}$) and relations (derived from $\widetilde{\operatorname{div}}(u) = 0$, u an S-unit). Thus the group is given by the ℓ-adic SNF of the matrix $M = \big(\widetilde{v}_{\mathfrak{p}_i}(u_j)\big)$, where the (u_j), $1 \leqslant j \leqslant J = r_F + c_F + l - 1$, generate the free part of the S-unit group.

The (u_j) are computed as in [4, §7.4.2], again taking care to use factored representations. Let

$$\delta(u_1, \dots, u_J) = \max_i \left(v_\ell(\deg \mathfrak{p}_i) + \max_{j,\, \alpha \in \operatorname{Supp} u_j} v_\ell(\mathrm{N}_{F_{\mathfrak{p}_i}/\mathbb{Q}_\ell}(\alpha)) \right),$$

where $\operatorname{Supp} u_j$ was defined in the previous paragraph. This quantity accounts for the maximal loss of accuracy when approximating the $\widetilde{v}_{\mathfrak{p}_i}(u_j)$ by Lemma 2.1 and Corollary 3.5. For increasing $N > \log_2 \delta$, we approximate the $\widetilde{v}_{\mathfrak{p}_i}$ modulo $\ell^{2^N} > \delta$ and compute the SNF of M modulo $L_N = \ell^{2^N - \delta}$. We may stop as soon as the computed SNF has a single elementary divisor of largest valuation:

Lemma 3.8. *If the computed SNF of the finite ℓ-group*

$$\widetilde{\mathcal{C}l}(\ell) \,/\, \widetilde{\mathcal{C}l}(\ell)^{L_N} = \bigoplus_{i \leqslant s} \mathbb{Z}/(\ell^{v_i}) \cdot g_i$$

has a single elementary divisor of largest valuation $v_1 > v_2$, then the Gross-Kuz'min conjecture for the field F and the prime ℓ holds. Indeed, in this case, we have $\widetilde{\mathcal{C}l}(\ell) = \mathbb{Z}_\ell \cdot g_1 \oplus \widetilde{\mathcal{C}l}(\ell)^0$, where $\widetilde{\mathcal{C}l}(\ell)^0 = \oplus_{i>1}(\mathbb{Z}/\ell^{v_i}) \cdot g_i$ has exponent ℓ^{v_2}.

Proof. $\widetilde{\mathcal{C}l}(\ell)$ has $\mathbb{Z}_\ell$-rank bigger than 1 due to the product formula:

$$\sum_{i \leqslant l} \deg \mathfrak{p}_i \cdot \widetilde{v}_{\mathfrak{p}_i}(x) = 0,$$

for any S-unit x. The Gross-Kuz'min conjecture states that this rank is exactly 1. □

Concretely, we apply the SNF algorithm to obtain matrices $U \in \mathrm{GL}_l(\mathbb{Z})$ and $V \in \mathrm{GL}_{r_F + c_F + 2l - 1}(\mathbb{Z})$ such that

$$U\big(M \bmod \ell^{L_N} \mid \ell^{L_N} \cdot \mathrm{Id}_l\big)V = \big(\operatorname{diag}(d_i) \mid 0\big)$$

is in rectangular Smith Normal Form, and stop when $L_N = v_\ell(d_1) > v_\ell(d_2)$. The g_i are given in terms of the logarithmic classes of the $\mathfrak{p}_i$ by

$$(g_1, \dots, g_l) = (\mathfrak{p}_1, \dots, \mathfrak{p}_l) \cdot U^{-1}.$$

We then delete the trivial g_i, $s < i \leqslant l$, such that $d_i = 1$. Of course, the algorithm will not stop if the conjecture is false and $\operatorname{rk}_{\mathbb{Z}_\ell} \widetilde{\mathcal{C}l}(\ell) > 1$.

Remark 3.9. This is the equivalent of Algorithm 14 and Theorem 16 in [6], simplified by the fact that we do not need the generators to have degree 0. The system of ℓ-adic $\alpha_j \in F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ such that $\widetilde{v}_{\mathfrak{p}_i}(\alpha_j) = \delta_{i,j}$ are no longer needed. (Note that the construction given before [6, Algorithm 19] must be modified so that it guarantees that $(\alpha_j, \ell) = 1$.)

3.4 The logarithmic class group

We use [4, §4.1.4] to describe $\widetilde{\mathcal{C}l}$ by generators and relations. The logarithmic classes of the ℓ-adic places $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_l\}$ generate $\widetilde{\mathcal{C}l}(\ell)$, with relations computed above. Let $\oplus_{i\leqslant s}(\mathbb{Z}/d_i)\cdot\mathfrak{a}_i$ be the SNF of $\mathcal{C}l'$ where we chose integral ideal representatives $\mathfrak{a}_i$ coprime to ℓ for the generating ideal classes. Those generators lift naturally to divisors, still denoted $\mathfrak{a}_i$, in $\widetilde{\mathcal{C}l}$ via $\prod \mathfrak{p}^{e_\mathfrak{p}} \to \sum e_\mathfrak{p}\mathfrak{p}$. Then $d_i \cdot \mathfrak{a}_i$ belongs to $\operatorname{Ker}\psi$, hence to $\widetilde{\mathcal{C}l}(\ell)$ and we can write

$$(d_1 \cdot \mathfrak{a}_1, \ldots, d_s \cdot \mathfrak{a}_s) = (\mathfrak{p}_1, \ldots, \mathfrak{p}_l) \cdot (-P)$$

in $\widetilde{\mathcal{C}l}$ for some matrix $P \in M_{l\times s}(\mathbb{Z}_\ell)$, from which we derive the ℓ-adic matrix of relations between the generators $(\mathfrak{p}_1, \ldots, \mathfrak{p}_l, \mathfrak{a}_1, \ldots, \mathfrak{a}_s)$:

$$\begin{pmatrix} M & P \\ 0 & \operatorname{diag}(d_1, \ldots, d_s) \end{pmatrix}$$

We now need to determine the matrix P.

Lemma 3.10. *For each $1 \leqslant i \leqslant s$, write*

$$\mathfrak{a}_i^{d_i} = (\alpha_i) \prod_{j\leqslant l} \mathfrak{p}_j^{*_{i,j}}$$

for some principal ideal (α_i) and integral exponents $*_{i,j}$. Let $P \in M_{s\times l}(\mathbb{Z}_\ell)$ be the matrix $(\widetilde{v}_{\mathfrak{p}_j}(\alpha_i))$. In the group $\widetilde{\mathcal{C}l}$, it holds

$$(d_1 \cdot \mathfrak{a}_1, \ldots, d_s \cdot \mathfrak{a}_s) = (\mathfrak{p}_1, \ldots, \mathfrak{p}_l) \cdot (-P).$$

Proof. Since the ideal $\mathfrak{a}_i$ is coprime to ℓ, it follows that $\prod_{\mathfrak{p}\nmid\ell} \mathfrak{p}^{v_\mathfrak{p}(\alpha_i)} = \mathfrak{a}_i^{d_i}$ and that, in $\widetilde{\mathcal{C}l}$, we have

$$0 = \widetilde{\operatorname{div}}(\alpha_i) = \sum_{\mathfrak{p}\nmid\ell} v_\mathfrak{p}(\alpha_i)\cdot\mathfrak{p} + \sum_{j\leqslant l} \widetilde{v}_{\mathfrak{p}_j}(\alpha_i)\cdot\mathfrak{p}_j = d_i\cdot\mathfrak{a}_i + \sum_{j\leqslant l} \widetilde{v}_{\mathfrak{p}_j}(\alpha_i)\cdot\mathfrak{p}_j.$$

□

Concretely, the decomposition

$$\mathfrak{a}_i^{d_i} = (\alpha_i) \prod_{j} \mathfrak{p}_j^{*_{i,j}}$$

is computed by solving a discrete logarithm problem in $\mathcal{C}l_F$ where, as usual, the $(\alpha_i)_{i\leqslant s}$ are given in factored representation. As in §3.3, we bound the loss of accuracy when estimating the $\widetilde{v}_{\mathfrak{p}_j}(\alpha_i)$ and set

$$L := \max\left(\delta(\alpha_1, \ldots, \alpha_l), v_\ell(\mathrm{e}(\mathcal{C}l')) + v_\ell(\mathrm{e}(\widetilde{\mathcal{C}l}(\ell))) + 1\right).$$

Then we compute the SNF of

$$\begin{pmatrix} M \bmod \ell^L & \ell^L \cdot \mathrm{Id}_l & P \bmod \ell^L \\ 0 & 0 & \mathrm{diag}(d_1, \dots, d_s) \end{pmatrix}.$$

Including the kernel and image exponents in the maximum guarantees that the SNF has a unique maximal elementary divisor, allowing to split off the rank 1 $\mathbb{Z}_\ell$-free part and the finite $\widetilde{\mathcal{C}l}_F^0$.

4 The bnflog package

4.1 The PARI/GP interface

In PARI/GP [21] version 2.8.1, the above algorithms are implemented as functions `bnflogef` and `bnflog`. All examples below are written in the GP scripting language.

- The function `bnflogef` takes as input a number field F and a prime ideal $\mathfrak{p}$ and returns the logarithmic indices $\widetilde{e}(\mathfrak{p}/p)$ and $\widetilde{f}(\mathfrak{p}/p)$. This is an elementary function requiring only basic arithmetic invariants of F, hence the use of the simple `nfinit` to define the number field structure:

```
? T = x^6 - 3*x^5 + 5*x^3 - 3*x + 1;
? F = nfinit(T);  \\ the number field Q[x]/(T)
? P2 = idealprimedec(F,2)[1]; \\ a prime above 2
? [P2.e, P2.f]    \\ ramification index and residue degree
%3 = [3, 2]       \\ e(P/p) = 3, f(P,p) = 2
? bnflogef(F, P2)
%4 = [6, 1]       \\ etilde(P/p) = 6, ftilde(P/p) = 1
```

- The function `bnflog` takes as input a prime ℓ and a number field F. It returns a vector of three group structures, given by their elementary divisors: $(\widetilde{\mathcal{C}l}_F^0, \widetilde{\mathcal{C}l}_F^0(\ell), \mathcal{C}l')$. This function requires the class group and units of F, hence the more involved initialization using `bnfinit`:

```
? T = x^4 + 13*x^2 - 12*x + 52;
? F = bnfinit(T); \\ F = Q[x]/(T), together with class group
? F.cyc
%3 = [14]            \\ Cl_F ~ Z/(14)]
? bnflog(F, 2)
%4 = [[], [], []]    \\ all 3 groups are trivial
? bnflog(F, 3)
%5 = [[3], [3], []]  \\ Cl^0 = Cl^0(3) ~ Z/(3)
? bnflog(F, 7)
%6 = [[7], [], [7]]  \\ Cl^0 ~ Cl' ~ Z/(7)
```

4.2 Examples

• The following two examples exhibit pathologies expected from the exact sequence relating $\widetilde{Cl}^0_F$, $\widetilde{Cl}^0_F(\ell)$ and Cl':

```
? T = x^4 - 511*x^2 + 65536;
? bnflog(bnfinit(T),2)
%2 = [[128, 4], [64], [8]] \\ the sequence doesn't split

? T = x^4 - 26*x^2 + 225;
? bnflog(bnfinit(T),2)
%4 = [[], [], [2]]          \\ coker(psi) = Z/2
```

• This program fixes a misprint in [6, p. 12], which reports $\widetilde{Cl}^0$ for $F = \mathbb{Q}(\sqrt{1234577}, \sqrt{-3})$ to be $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (it is cyclic of order 4):

```
? T = polcompositum(x^2+3, x^2-1234577, 2);
? bnflog(bnfinit(T,1),2)
%2 = [[4], [4], []]
```

• The following program proves [12, Proposition 3.4]; the locally cyclotomic 2-tower of $F = \mathbb{Q}(\sqrt{-p})$ is infinite:

```
? {
    forprime(p = 2, 5000,
      if (p%64 != 63, next);
      F = bnfinit(x^2+p);
      G = bnflog(F,2); Cl = G[1]; if(!Cl || Cl[1] % 16,next);
      print([p,G]))
  }
[3967, [[16], [16], []]]
[4159, [[32], [32], []]]
```

• The following program proves [12, Proposition 3.5]; the locally cyclotomic 2-tower of $F = \mathbb{Q}(\sqrt{pq})$ is infinite:

```
? {
    forprime(p = 2, 2000,
      if (p % 64 != 1 && p % 64 != 63, next);
      forprime(q = p+1, 2000, if ((p*q)%64 != 1, next);
      F = bnfinit(x^2-p*q, 1);
      G = bnflog(F,2); C = G[1]; if (!C || C[1] % 16, next);
      print([p,q,G])))
  }
[127,  1151, [[32], [32], []]]
```

```
[193,  257,  [[32], [8], [4]]]
[193,  1217, [[16], [4], [4]]]
[449,  577,  [[256], [128], [2]]]
[577,  1601, [[64, 2], [16], [8]]]
[641,  769,  [[16, 2], [16], [2]]]
[1151, 1663, [[16], [16], []]]
```

• We now give two examples with large 3-rank (and *large* class group); factored representations must be used throughout to avoid catastrophic cancellation:

```
? F = bnfinit(x^2 + 5393946914743);
? bnflog(F, 3)
%2 = [[3, 3, 3, 3, 3], [], [3, 3, 3, 3, 3]]

\\ This assumes the truth of the GRH:
? F = bnfinit(x^2 + 14138863693162613823739799380212181908);
? F.cyc
%4 = [693468857222922, 6, 6, 6, 3]
? bnflog(F, 3)
%5 = [[3, 3, 3, 3, 3], [9], [3, 3, 3, 3]]
```

The final computation is conditional on the truth of the GRH, since it is not practical to certify the class group of a field F with such a large discriminant. The total running time for all the above computations is about 4 minutes, 99% of which are spent in the final example.

• This program prints the smallest real quadratic field whose $\widetilde{\mathcal{C}l}^{\,0}$ has 2-rank equal to 5 (and its locally cyclotomic 2-tower is infinite). This fixes a misprint in [18] which erroneously reports $F = \mathbb{Q}(\sqrt{3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17})$ as the real quadratic field with smallest discriminant with this property (but its 2-rank is 4). This computation requires about 5 hours.

```
? D = 3*5*7*11*13*17*19;
? {
    for(d=2, D,
      if (!issquarefree(d),next);
      F = bnfinit(x^2-d, 1);
      G = bnflog(F,2); if (#G[1] >= 5, print([d,G])))
  }
[4849845, [[4, 2, 2, 2, 2], [], [4, 2, 2, 2, 2]]]

? bnflog(bnfinit(x^2-3*5*7*11*13*17), 2);
%3 = [[2, 2, 2, 2], [], [2, 2, 2, 2]]
```

References

[1] K. Belabas, Topics in computational algebraic number theory, *J. Théor. Nombres Bordeaux* **16** (2004), no. 1, pp. 19–63.

[2] J. Buchmann & H. W. Lenstra, Jr., Approximating rings of integers in number fields, *J. Théor. Nombres Bordeaux* **6** (1994), no. 2, pp. 221–260.

[3] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[4] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000.

[5] F. Diaz y Diaz & F. Soriano, Approche algorithmique du groupe des classes logarithmiques, *J. Number Theory* **76** (1999), no. 1, pp. 1–15.

[6] F. Diaz y Diaz, J.-F. Jaulent, S. Pauli, M. Pohst, & F. Soriano-Gafiuk, A new algorithm for the computation of logarithmic l-class groups of number fields, *Experiment. Math.* **14** (2005), no. 1, pp. 65–74.

[7] D. Ford, S. Pauli, & X.-F. Roblot, A fast algorithm for polynomial factorization over $\mathbb{Q}_p$, *J. Théor. Nombres Bordeaux* **14** (2002), no. 1, pp. 151–169.

[8] G. Gras, *Class field theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003, From theory to practice, Translated from the French manuscript by Henri Cohen.

[9] T. Gras, Sur le module de Bertrandias-Payan – Noyau de capitulation, *Pub. Math. Besançon*, à paraître.

[10] J.-F. Jaulent, Normes cyclotomiques naïves et unités logarithmiques, *preprint*, `https://arxiv.org/abs/1609.01901`.

[11] J.-F. Jaulent, Sur la capitulation pour le module de Bertrandias-Payan, *Pub. Math. Besançon*, à paraître.

[12] J.-F. Jaulent & C. Maire, À propos de la tour localement cyclotomique d'un corps de numbres, *Abh. Math. Sem. Univ. Hamburg* **70** (2000), pp. 239–250.

[13] J.-F. Jaulent, Classes logarithmiques des corps de nombres, *J. Théor. Nombres Bordeaux* **6** (1994), no. 2, pp. 301–325.

[14] J.-F. Jaulent, Sur le noyau sauvage des corps de nombres, *Acta Arith.* **67** (1994), no. 4, pp. 335–348.

[15] J.-F. Jaulent, Théorie ℓ-adique globale du corps de classes, *J. Théor. Nombres Bordeaux* **10** (1998), no. 2, pp. 355–397.

[16] J.-F. Jaulent, Classes logarithmiques signées des corps de nombres, *J. Théor. Nombres Bordeaux* **12** (2000), no. 2, pp. 455–474, Colloque International de Théorie des Nombres (Talence, 1999).

[17] J.-F. Jaulent & A. Michel, Approche logarithmique des noyaux étales sauvages des corps de nombres, *J. Number Theory* **120** (2006), no. 1, pp. 72–91.

[18] J.-F. Jaulent & F. Soriano, Sur les tours localement cyclotomiques, *Arch. Math. (Basel)* **73** (1999), no. 2, pp. 132–140.

[19] J.-F. Jaulent & F. Soriano, Sur le noyau sauvage des corps de nombres et le groupe des classes logarithmiques, *Math. Z.* **238** (2001), no. 2, pp. 335–354.

[20] T. Nguyen-Quang-Do, Descente galoisienne et capitulation pour le module de Bertrandias-Payan, *Pub. Math. Besançon*, à paraître.

[21] The PARI Group, Bordeaux, PARI/GP, version `2.8.1`, 2016, `http://pari.math.u-bordeaux.fr/`.