The Discrete Logarithm in Logarithmic ℓ-Class Groups and its Applications in K-Theory

Sebastian Pauli and Florence Soriano-Gafiuk

Institut für Mathematik, Technische Universität Berlin and
Département de Mathématiques, Université de Metz

Abstract. We present an algorithm for the computation of the discrete logarithm in logarithmic ℓ-Class Groups. This is applied to the calculation to the ℓ-rank of the wild kernel WK_2 of a number field F and in the determination of generators of the ℓ-part of $WK_2(F)$.

1 Introduction

A new invariant of number fields, called group of logarithmic classes, was introduced by J.-F. Jaulent in 1994 [J3]. The arithmetic of logarithmic classes is interesting because of its applicability to K-Theory. Indeed for a given prime number ℓ, the ℓ-rank of the logarithmic ℓ-class group of a number field F containing the 2ℓ-th roots of unity equals the ℓ-rank of the wild kernel.

In the present paper we give positive answers to the questions:

- If F does not contain the 2ℓ-th roots of unity, can we determine the ℓ-rank of its wild kernel by the arithmetic of the logarithmic divisor class groups ?
- Is it possible to give a complete logarithmic description of the wild kernel ?

First we recall the most important definitions from the theory of logarithmic ℓ-class groups and the algorithm for their computation; we also give an algorithm for the computation of discrete logarithms in these groups (section 2). In section 3 we give a short introduction to the wild kernel and derive the algorithms for the computation of its ℓ-rank in a general setting. Section 4 contains the complete description of the ℓ-part of the wild kernel through the logarithmic ℓ-class group. This is followed by some examples.

In the following, ℓ denotes a fixed prime number and $\mathbb{Z}_\ell$ the completion of $\mathbb{Z}$ with respect to the non-archimedian exponential valuation v_ℓ. F denotes a number field.

2 The Logarithmic ℓ-Class Group

For a detailed presentation of logarithmic theory see [J3]. 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 use the algorithm from [DJ+] as it removes the restriction to Galois extensions of $\mathbb{Q}$. This algorithm uses the ideal theoretic description of the logarithmic ℓ-class groups. Before we discuss it we need some definitions.

Let p be a prime number and 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 $\alpha \in F^*$ we define

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

The logarithmic ramification index $\widetilde{e}_\mathfrak{p}$ can be described as follows. The p-part of the logarithmic ramification index $\widetilde{e}_\mathfrak{p}$ is $[g_\mathfrak{p}(F_\mathfrak{p}^*) : \mathbb{Z}_p]$. 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 $\mathfrak{p}$. The logarithmic inertia degree $\widetilde{f}_\mathfrak{p}$ is defined by the relation $\widetilde{e}_\mathfrak{p} \widetilde{f}_\mathfrak{p} = e_\mathfrak{p} f_\mathfrak{p} = \deg(F/\mathbb{Q})$, where $f_\mathfrak{p}$ is the classic inertia degree. We use it for the definition of the logarithmic degree of a place $\mathfrak{p}$:

$$\deg_\ell \mathfrak{p} := \widetilde{f}_\mathfrak{p} \deg_\ell p \quad \text{where} \quad \deg_\ell p = \begin{cases} \mathrm{Log}_\ell\, p & \text{for } p \neq \ell; \\ \ell & \text{for } p = \ell \neq 2; \\ 4 & \text{for } p = \ell = 2. \end{cases}$$

Furthermore we set

$$\widetilde{v}_\mathfrak{p}(x) := -\frac{\mathrm{Log}_\ell(\mathrm{N}_{F_\mathfrak{p}/\mathbb{Q}_p}(x))}{\deg_\ell(\mathfrak{p})} \text{ for } x \in \mathcal{R}_F = \mathbb{Z}_\ell \otimes_\mathbb{Z} F^*.$$

We define the group of ℓ-ideals

$$\mathcal{I}d_{F,\ell} := \left\{ \mathfrak{a} = \prod_{\mathfrak{p} \nmid \ell} \mathfrak{p}^{\alpha_\mathfrak{p}} \mid \alpha_\mathfrak{p} = 0 \text{ for almost all } \mathfrak{p} \right\},$$

denote by

$$\widetilde{\mathcal{I}d}_{F,\ell} := \{ \mathfrak{a} \in \mathcal{I}d_{F,\ell} | \deg_\ell \mathfrak{d}_F(\mathfrak{a}) = 0 \}$$

the subgroup of ℓ-ideals of degree 0, and denote by

$$\widetilde{\mathcal{P}r}_{F,\ell} := \left\{ \prod_{\mathfrak{p} \nmid \ell} \mathfrak{p}^{v_\mathfrak{p}(a)} \mid \mathfrak{a} \in \mathcal{R}_F \text{ and } \widetilde{v}_\mathfrak{p}(a) = 0 \ \forall \mathfrak{p} \mid \ell \right\}$$

the subgroup of principal ℓ-ideals having logarithmic valuations 0 at all ℓ-adic places. The group of logarithmic ℓ-classes is isomorphic to the quotient of the latter two:

$$\widetilde{\mathcal{C}\ell}_{F,\ell} \cong \widetilde{\mathcal{I}d}_{F,\ell} / \widetilde{\mathcal{P}r}_{F,\ell}.$$

The generalized Gross conjecture (for the field F and the prime ℓ) asserts that the logarithmic class group $\widetilde{\mathcal{C}\ell}_{F,\ell}$ is finite (cf. [J3]). 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,J4]). Nevertheless, since $\widetilde{\mathcal{C}\ell}_{F,\ell}$ 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. In

[DJ+] we present a method for the computation of an upper bound for m. That algorithm does not terminate in general if Gross' conjecture is false. This upper bound can be used as the ℓ-adic precision in the computation of the logarithmic class group.

2.1 Generators and Relations of $\widetilde{\mathcal{C}\ell}_{F,\ell}$

Let $\mathfrak{a}_1, \dots, \mathfrak{a}_t$ be a basis of the ideal classgroup $\mathcal{C}\ell_F$ 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 $\mathcal{R}_F = \mathbb{Z}_\ell \otimes F^*$ 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 $\widetilde{\mathcal{C}\ell}_{F,\ell}$ is generated by $\overline{\mathfrak{b}}_1, \dots, \overline{\mathfrak{b}}_{t+s}$.

II. Otherwise let $1 \le j \le t+s$ such that $v_\ell(\deg_\ell(\mathfrak{a}_j)) = \min_{1 \le i \le t+s} v_\ell(\deg_\ell(\mathfrak{a}_i))$. If we have $\mathfrak{a} = \overline{\mathfrak{a}} \equiv \overline{\mathfrak{a}}_1^{a_1} \cdot \dots \cdot \overline{\mathfrak{a}}_{t+s}^{a_{t+s}} \bmod \widetilde{\mathcal{P}r}$ 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 $-a_j = \sum_{i \ne j}^{t+s} a_i \deg_\ell(\overline{\mathfrak{a}}_i) / \deg_\ell(\overline{\mathfrak{a}}_j)$. Set $\mathfrak{b}_i := \mathfrak{a}_i / \mathfrak{a}_j^{d_i}$ with $d_i \equiv \frac{\deg_\ell(\mathfrak{a}_i)}{\deg_\ell(\mathfrak{a}_j)} \bmod \ell^m$ where $\ell^m > \exp(\widetilde{\mathcal{C}\ell}_{F,\ell})$. The group $\widetilde{\mathcal{C}\ell}_{F,\ell}$ is generated by $\overline{\mathfrak{b}}_1, \dots, \overline{\mathfrak{b}}_{j-1}, \overline{\mathfrak{b}}_{j+1}, \dots, \overline{\mathfrak{b}}_{t+s}$.

Obviously the ideals $\overline{\mathfrak{a}}_1, \dots, \overline{\mathfrak{a}}_t$ are representatives of generators of the group $\mathcal{C}\ell' := \mathcal{C}\ell_F / \langle \mathfrak{p}_1, \dots, \mathfrak{p}_s \rangle$. Let $\left(a_{i,j}\right)_{i,j}$ be the corresponding relation matrix. The relations between the generators $\overline{\mathfrak{a}}_1, \dots, \overline{\mathfrak{a}}_t$ of $\mathcal{C}\ell'$ 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 $c_1, \dots, c_s$ such that $\overline{(\alpha)} \equiv \prod_{i=1}^s \overline{(\alpha_i)}^{c_i} \bmod \widetilde{\mathcal{P}r}$. This yields the relation $\prod_{i=1}^t \overline{\mathfrak{a}}_i^{a_i} \equiv \prod_{i=1}^s \overline{(\alpha_i)}^{c_i} \bmod \widetilde{\mathcal{P}r}$. 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. Let $\gamma_1, \dots, \gamma_r$ be a basis of the (ℓ)-units of $\mathcal{R}_F$. Set $v_{i,j} := \widetilde{v}_{\mathfrak{p}_j}(\gamma_i)$ $(1 \le i \le r, 2 \le j \le s)$. We obtain the relation matrix

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

For the two cases we obtain:

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

This gives the following algorithm:

Algorithm 1 (Logarithmic Classgroup)
Input: a number field F and a prime number ℓ
Output: generators g and and a relation matrix H for $\widetilde{\mathcal{C}\ell}_{F,\ell}$

- Determine a bound ℓ^m for the exponent of $\widetilde{\mathcal{C}\ell}_{F,\ell}$ and use it as the precision for the rest of the algorithm.
- Compute generators $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ of $\mathcal{C}\ell' = \mathcal{C}\ell_F / \langle \mathfrak{p}_1, \ldots, \mathfrak{p}_s \rangle$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are the ideals of F over ℓ.
- Determine $\mathfrak{a}_{t+1} = (\alpha_1), \ldots, \mathfrak{a}_{t+s} = (\alpha_s)$ with $\widetilde{v}_{\mathfrak{p}_i}(\alpha_j) = \delta_{i,j}$.
- Compute generators $g := (\overline{\mathfrak{b}}_1, \ldots, \overline{\mathfrak{b}}_{t+s})^T$ with $\deg(\mathfrak{b}_i) = 0$ from $\mathfrak{a}_1, \ldots, \mathfrak{a}_{t+s}$ $(i = 1, \ldots, t+s)$.
- Compute a relation matrix M between the generators g.
- 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).

The Smith normal form of H and the respective transformations of the generators yield a basis representation of $\widetilde{\mathcal{C}\ell}_{F,\ell}$.

2.2 The Discrete Logarithm in $\widetilde{\mathcal{C}\ell}_{F,\ell}$

Let $\mathfrak{a} \in \widetilde{\mathcal{I}d}$. Let $g = (\overline{\mathfrak{b}}_1, \ldots, \overline{\mathfrak{b}}_r)^T$ be a vector of generators of $\widetilde{\mathcal{C}\ell}$. The discrete logarithm algorithm returns a vector $c = (c_1, \ldots, c_r)$ such that

$$c^T g = \overline{\mathfrak{b}}_1^{c_1} \ldots \overline{\mathfrak{b}}_r^{c_r} \equiv \mathfrak{a} \bmod \widetilde{\mathcal{P}r}.$$

We use the notation from above and proceed as follows:

Let $\mathfrak{a} \in \widetilde{\mathcal{I}d}$. There exist $\gamma \in \mathcal{R}_F$ and $a_1, \ldots, a_t \in \mathbb{Z}_\ell$ 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 $1 \leq i \leq s$. Now

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

By the definition of $\mathcal{I}d$ we have

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

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

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

For the two cases we obtain:

I. $(a_1, \ldots, a_t, g_1, \ldots, g_s)$ is a representation of $\mathfrak{a}$ in $\widetilde{\mathcal{C}\ell}_{F,\ell}$.
II. Let $(c_1, \ldots, c_{t+s}) = (a_1, \ldots, a_t, g_1, \ldots, g_s)$ then $(c_1, \ldots, c_{j-1}, c_{j+1}, \ldots, c_{t+s})$ is a representation of $\mathfrak{a}$ in $\widetilde{\mathcal{C}\ell}_{F,\ell}$.

3 The Wild Kernel

Let F be a number field. J. Milnor [Mi] introduced the K-groups

$$K_n(F) := (F^* \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} F^*)\big/ I_n$$

where I_n is the subgroup of $F^* \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} F^*$ generated by the element $x_1 \otimes \cdots \otimes x_n$ such that $x_i + x_j = 1$ for some $i \neq j$. It is convenient to set $K_0(F) := \mathbb{Z}$ and $K_1(F) := F^*$. For $n \geq 3$ H. Bass and J. Tate [BT] proved that $K_n(F) \cong (\mathbb{Z}/2\mathbb{Z})^r$, where r is the number of real embeddings of F. Unfortunately the study of

$$K_2(F) \;=\; F^* \otimes_{\mathbb{Z}} F^* \Big/ \big\langle x \otimes_{\mathbb{Z}} (1-x) \mid x \in F \setminus \{0,1\} \big\rangle$$

is much more difficult [T1,T2]. An important tool for working with $K_2(F)$ is the canonical map

$$\{\cdot,\cdot\} : F^* \times F^* \to K_2(F)$$

which is called Steinberg's symbol. We will make use of it in section 4.

In order to understand the structure of $K_2(F)$ one constructs a morphism from $K_2(F)$ to a known abelian group whose kernel is finite. This reduces the problem of studying $K_2(F)$ to studying a finite group. We construct such a morphism. Let $\mathfrak{p}$ be a non-complex place of F. Denote by $\mu_{\mathfrak{p}}$ the torsion subgroup of $F_{\mathfrak{p}}^*$. We define

$$h_{\mathfrak{p}} : F_{\mathfrak{p}}^* \times F_{\mathfrak{p}}^* \to \mu_{\mathfrak{p}},\ (x,y) \mapsto \sqrt[m_{\mathfrak{p}}]{x}^{\,\omega_{\mathfrak{p}}(y)-1}$$

where $m_{\mathfrak{p}} = |\mu_{\mathfrak{p}}|$ and where $\omega_{\mathfrak{p}}$ is the Artin map. It follows from the multiplicativity of the norm residue symbol and Kummer theory [Gr, pp. 195-197] that the map $h_{\mathfrak{p}}$ is a $\mathbb{Z}$-linear map which is trivial for elements of the form $(x, 1-x)$ where $x \in F \setminus \{0,1\}$, *i.e.*, $h_{\mathfrak{p}}$ is a symbol. $h_{\mathfrak{p}}$ gives us a map from $K_2(F)$ to $\mu_{\mathfrak{p}}$, which we also denote by $h_{\mathfrak{p}}$. The wild kernel of K_2 is

$$WK_2(F) = \big\{\mathcal{X} \in K_2(F) \mid h_{\mathfrak{p}}(\mathcal{X}) = 1 \text{ for all non-complex places } \mathfrak{p} \text{ of } F\big\}$$

Garlands theorem [Ga] states that $WK_2(F)$ is finite. There exist idelic [Ko] and cohomologic methods for studying the wild kernel. We chose to use logarithmic methods as it allows for the use of an algorithmic approach.

The following theorem by Jaulent [J2] establishes the relationship between the wild kernel and the logarithmic ℓ-class groups $\widetilde{\mathcal{C}\ell}_{F,\ell}$ for the case where F contains a $2\ell^q$-th roots of unity $\zeta_{2\ell^q}$.

Theorem 2 *Assume that $\zeta_{2\ell^q} \in F^*$. Let $q \in \mathbb{N}$, $q \geq 1$. For every divisor $\mathfrak{a} = \sum_{\mathfrak{p}} a_{\mathfrak{p}} \mathfrak{p}$ of degree 0 there exists $\mathcal{X} \in K_2(F)$ such that $h_{\mathfrak{p}}(\mathcal{X}) = \zeta_{\ell^q}^{a_{\mathfrak{p}}}$. If $\zeta_{2\ell^q} \in F^*$ then the map*

$$\phi : \mu_{\ell^q} \otimes_{\mathbb{Z}} \widetilde{\mathcal{C}\ell}_{F,\ell} \to WK_2(F)/WK_2(F)^{\ell^q}$$

defined by

$$\zeta_{\ell^q} \otimes \mathfrak{a} \mapsto \mathcal{X}^{\ell^q}$$

is an isomorphism.

Moore's exact sequence in [Mo] assures that such an $\mathcal{X}$ exists.

Corollary 3 *If F contains the 2ℓ-th roots of unity, then*

$$\operatorname{rank}_\ell WK_2(F) = \operatorname{rank}_\ell \widetilde{\mathcal{C}\ell}_{F,\ell}.$$

The algorithm in [DJ$^+$] computes the structure of $\widetilde{\mathcal{C}\ell}_F$, and therefore the ℓ-rank of $\widetilde{\mathcal{C}\ell}_F$. Thus by the theorem above, the ℓ-rank of the wild kernel is known if F contains the $2\ell^q$-th roots of unity.

3.1 F does not contain the 2ℓ-th roots of unity

If $\ell = 2$ and $i \notin F$ the group of positive divisor classes can be used for the description of the 2-rank wild kernel [JS2]. We deal with the remaining case and therefore assume in the following that ℓ is odd.

Let ζ_ℓ be a primitive ℓ-th root of unity. Let F' be the Galois extension $F(\zeta_\ell)$. Let $d = |\mathrm{Gal}(F'/F)|$. We have $d \mid (\ell - 1)$ and therefore $\gcd(\ell, d) = 1$. In other words $d \in \mathbb{Z}_\ell^*$.

There is an idempotent $e_\infty \in \mathbb{Z}_\ell[\mathrm{Gal}(F'/F)]$ with $e_\infty = \frac{1}{d}\sum_{\sigma\in\mathrm{Gal}(F'/F)} k_\sigma \sigma$ where $k_\sigma \in \mathbb{Z}_\ell$ such that $\zeta^\sigma = \zeta^{k_\sigma}$ for all $\sigma \in \mathrm{Gal}(F'/F)$. We construct such an element e_∞ in the next section.

Proposition 4 ([JS1]) *If ℓ is odd and F does not contain the 2ℓ-th roots of unity then*

$$\operatorname{rank}_\ell WK_2(F) = \operatorname{rank}_\ell \widetilde{\mathcal{C}\ell}^{e_\infty}_{F(\zeta_\ell),\ell}.$$

For a better understanding we give a more detailed proof than in [JS1].

Proof. Let $F' := F(\zeta_\ell)$. Set $\Delta := \mathrm{Gal}(F'/F)$. Because F' contains the 2ℓ-th roots of unity the isomorphism

$$\mu_\ell \otimes_{\mathbb{Z}} \widetilde{\mathcal{C}\ell}_{F'} \cong WK_2(F')/WK_2(F')^\ell$$

holds (Theorem 2). As Δ acts on $K_2(F')$ such that $\{x, y\}^\sigma = \{x^\sigma, y^\sigma\}$ for all $\sigma \in \Delta$ and all $(x, y) \in \left(F'^*\right)^2$ it follows that

$$\left(\mu_\ell \otimes_{\mathbb{Z}} \widetilde{\mathcal{C}\ell}_{F'}\right)^{e_1} \cong \left(WK_2(F')/WK_2(F')^\ell\right)^{e_1}$$

for $e_1 = \frac{1}{d}\sum_{\sigma\in\Delta} \sigma$. As ℓ does not divide d the idempotent e_1 induces a surjective morphism $\frac{1}{d}\,\mathrm{Tr}$ where Tr is called transfer from the ℓ-part of $K_2(F')$ to the ℓ-part of $K_2(F)$. Therefore $WK_2(F)/WK_2(F)^\ell$ is the image of $WK_2(F')/WK_2(F')^\ell$ under the restriction of the transfer map Tr. Hence

$$\left(\mu_\ell \otimes_{\mathbb{Z}} \widetilde{\mathcal{C}\ell}_{F'}\right)^{e_1} \cong WK_2(F)/WK_2(F)^\ell.$$

For $\mathfrak{a} \in \mathcal{D}\ell_{F'}$ we have

$$(\zeta \otimes \mathfrak{a})^{d\cdot e_1} = \prod_{\sigma\in\Delta} (\zeta \otimes \mathfrak{a})^\sigma = \prod_{\sigma\in\Delta} \zeta^\sigma \otimes \mathfrak{a}^\sigma = \prod_{\sigma\in\Delta} \zeta^{k_\sigma} \otimes \mathfrak{a}^\sigma = \prod_{\sigma\in\Delta} \zeta \otimes \mathfrak{a}^{k_\sigma \sigma}$$

and

$$(\zeta \otimes a)^{e_1} = \Big(\zeta \otimes \prod_{\sigma \in \Delta} \mathfrak{a}^{k_\sigma \sigma}\Big)^{d^{-1}} = \zeta \otimes a^{e_\infty}.$$

Therefore

$$\big(\mu_\ell \otimes_{\mathbb{Z}} \widetilde{\mathcal{C}\ell}_{F'}\big)^{e_1} = \mu_\ell \otimes \widetilde{\mathcal{C}\ell}_{F'}^{e_\infty}.$$

Example 5 ([JS1]) If $\ell = 3$ and $F = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree then $F' = F(\sqrt{-3})$ with cyclic Galois group $\mathrm{Gal}(F'/F) = \langle \tau \rangle$ and $\zeta_3 = \frac{-1+\sqrt{-3}}{2} \in F'$. Because $\zeta_3^\tau = \zeta_3^{-1}$ we set $e_\infty = 1/2(1-\tau)$. We have

$$\mathrm{rank}_3\, WK_2(F) = \mathrm{rank}_3\, \widetilde{\mathcal{C}\ell}_{F'}^{e_\infty}$$

Because $e_\infty = 1/2(1-\tau) = 1/2(1+\sigma)$ where $\langle \sigma \rangle = \mathrm{Gal}(F'/F_*)$ with $F_* = \mathbb{Q}(\sqrt{-3d})$ we obtain

$$\mathrm{rank}_3\, WK_2(F) = \mathrm{rank}_3\, \widetilde{\mathcal{C}\ell}_{F'}^{1+\sigma} = \mathrm{rank}_3\, \widetilde{\mathcal{C}\ell}_{F_*}$$

and

$$\mathrm{rank}_3\, WK_2(\mathbb{Q}(\sqrt{d})) = \mathrm{rank}_3\, \widetilde{\mathcal{C}\ell}_{\mathbb{Q}(\sqrt{-3d})}.$$

This is particularly interesting as we do not need any computations in the extension $F(\zeta_3)$.

3.2 Computing e_∞

Let $d := |\mathrm{Gal}(F'/F)|$ and let σ be a generator of $\mathrm{Gal}(F'/F)$. We are looking for an element $e \in \mathbb{Z}_\ell[\mathrm{Gal}(F'/F)]$ with $e = e^2$. The element e is of the form $e = \frac{1}{d}\sum_{i=0}^{d-1} k_i \sigma^i$ with $k_i \in \mathbb{Z}_\ell$ $(0 \le i < d)$. Hence the condition $e = e^2$ becomes

$$\left(\sum_{u=0}^{d-1} k_u \sigma^u\right)\left(\sum_{v=0}^{d-1} k_v \sigma^v\right) = d \sum_{i=0}^{d-1} k_i \sigma^i.$$

Let ℓ^m be the exponent of $\widetilde{\mathcal{C}\ell}_{F,\ell}$. It is obvious that it suffices to compute e up to a precision of m ℓ-adic digits. Set

$$S_i := \big\{(u,v) \in \mathbb{Z}^2 \mid u, v \in \{0,\dots,d-1\}, u+v \equiv i \bmod d\big\}.$$

For $0 \le i \le d-1$ we solve the congruences

$$\sum_{(u,v)\in S_i} k_u \cdot k_v \equiv d k_i \bmod \ell^m.$$

We write k_i as $\sum_{j=0}^{m-1} x_{i,j}\ell^j$ with unknown $x_{i,j} \in \{0,\dots,\ell-1\}$ $(0 \le i < d$, $0 \le j < m)$. Thus our congruences become

$$\sum_{(u,v)\in S_i} \left(\sum_{j=0}^{m-1} x_{u,j}\ell^j\right)\left(\sum_{j=0}^{m-1} x_{v,j}\ell^j\right) \equiv d\left(\sum_{j=0}^{m-1} x_{i,j}\ell^j\right) \bmod \ell^m. \tag{1}$$

We start by solving them modulo ℓ:

$$\sum_{(u,v)\in S_i} x_{u,0}x_{v,0} \equiv dx_{i,0}.$$

Let $\alpha \in \mathbb{F}_\ell$ be a generator of the cyclic group $\mathbb{F}_\ell^*$. Set $\delta = \frac{\ell-1}{d}$ then α^δ has order d in $\mathbb{F}_\ell^*$. Let a be a representative of α^δ in $\mathbb{Z}_\ell$. The elements $a_{0,0} = 1$, $a_{1,0} = a$, $a_{2,0} = a^2, \ldots, a_{d-1,0} = a^{d-1}$ are solutions for $x_{0,0}, \ldots, x_{d-1,0}$.

Assume that we have found $a_{i,j} \in \{1\ldots, \ell-1\}$ $(0 \le i < d,\ 0 \le j < w < m)$ such that

$$A_{i,w} := -\sum_{(u,v)\in S_i}\left(\sum_{j=0}^{w-1} a_{u,j}\ell^j\right)\left(\sum_{j=0}^{w-1} a_{v,j}\ell^j\right) + d\left(\sum_{j=0}^{w-1} a_{i,j}\ell^j\right) \equiv 0 \bmod \ell^w.$$

With (1) we obtain

$$\sum_{(u,v)\in S_i} x_{u,w}\ell^w a_{v,0} + x_{v,w}\ell^w a_{u,0} \equiv dx_{i,w}\ell^w + A_{i,w} \bmod \ell^{w+1}.$$

and as $A_{i,w} \equiv 0 \bmod \ell^w$ this becomes

$$\sum_{(u,v)\in S_i} x_{u,w}a_{v,0} + x_{v,w}\ a_{u,0} - dx_{i,w} \equiv \frac{A_{i,w}}{\ell^w} \bmod \ell \tag{2}$$

for $i = 1, \ldots, d-1$ which is a system of d linear equations in d variables over $\mathbb{F}_\ell$.

Therefore we obtain a solution to (1) by first computing $a_{0,0}, \ldots, a_{d-1,0}$ as described above and then solving systems of linear equations (2) inductively for $w = 1, \ldots, m-1$ to obtain values $a_{0,w}, \ldots, a_{d-1,w}$ for $x_{0,w}, \ldots, x_{d-1,w}$.

3.3 Computing the ℓ-Rank of the Wild Kernel

By proposition 4 the ℓ-rank of the wild kernel of F equals the ℓ-rank of $\widetilde{C\ell}^{e_\infty}_{F(\zeta_\ell),\ell}$. Let $\overline{\mathfrak{b}}_1, \ldots, \overline{\mathfrak{b}}_r$ be a basis of $\widetilde{C\ell}_{F(\zeta_\ell),\ell}$ and let ℓ^{b_i} be the order of $\overline{\mathfrak{b}}_i$ in $\widetilde{C\ell}_{F(\zeta_\ell),\ell}$ $(1 \le i \le r)$, *i.e.*,

$$\widetilde{C\ell}_{F(\zeta_\ell),\ell} = \bigoplus_{i=1}^{r} \mathbb{Z}/\ell^{b_i}\mathbb{Z}[\overline{\mathfrak{b}}_i].$$

The elements $\overline{\mathfrak{b}}_1^{e_\infty}, \ldots, \overline{\mathfrak{b}}_r^{e_\infty}$ are generators of $\widetilde{C\ell}^{e_\infty}_{F(\zeta_\ell),\ell}$. For $1 \le i \le r$ the discrete logarithm in $\widetilde{C\ell}_{F(\zeta_\ell),\ell}$ gives representations $(n_{i,1}, \ldots, n_{i,r})$ of the $\overline{\mathfrak{b}}_i^{e_\infty}$ with

$$\overline{\mathfrak{b}}_i^{e_\infty} \equiv \overline{\mathfrak{b}}_1^{n_{i,1}} \cdots \overline{\mathfrak{b}}_r^{n_{i,r}} \bmod \widetilde{\mathcal{P}r}.$$

Let $A \in \mathbb{Z}_\ell^{r\times 2r}$ such that

$$\begin{pmatrix} \ell^{b_1} & & 0 & n_{1,1} & \ldots & n_{r,1} \\ & \ddots & & \vdots & \ddots & \vdots \\ 0 & & \ell^{b_r} & n_{1,r} & \ldots & n_{r,r} \end{pmatrix} A = 0.$$

We write $A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$ where $A_1, A_2 \in \mathbb{Z}_\ell^{r\times r}$. A_2 is a relation matrix of the subgroup $\widetilde{\mathcal{C}\ell}^{e\infty}_{F(\zeta_\ell),\ell}$ generated by $\overline{\mathfrak{b}}_1, \dots, \overline{\mathfrak{b}}_r$ which are represented by $(n_{i,1}, \dots, n_{i,r})$ $(1 \le i \le r)$. Denote by $\left(h_{i,j}\right)_{i,j}$ the ℓ-adic Hermite normal form of A_2. Then

$$\operatorname{rank}_\ell WK_2(F) = \operatorname{rank}_\ell \widetilde{\mathcal{C}\ell}^{e\infty}_{F(\zeta_\ell),\ell} = \#\{h_{i,i} \mid 1 \le i \le r,\, h_{i,i} \ne 1\}.$$

4 A Complete Description of the ℓ-part of the Wild Kernel

Assume that $\widetilde{\mathcal{C}\ell}_{F,\ell}$ is not trivial, then

$$\widetilde{\mathcal{C}\ell}_{F,\ell} = \bigoplus_{i=1}^{r} \mathbb{Z}/\ell^{n_i}\mathbb{Z}[\mathfrak{a}_i].$$

Therefore there exist a family $(\alpha_i) \subset \mathcal{R}_F = \mathbb{Z}_\ell \otimes_\mathbb{Z} F^*$ such that $\ell^{n_i}\mathfrak{a}_i = \widetilde{\operatorname{div}}(\alpha_i)$ for $1 \le i \le r$. Assume that $\zeta_{\ell^{m+1}} \in F$ where $\ell^m = \exp \widetilde{\mathcal{C}\ell}_{F,\ell}$. Then the ℓ-part of the wild kernel is [So]

$$\bigoplus_{i=1}^{r} \mathbb{Z}/\ell^{n_i}\mathbb{Z}\{\zeta_{\ell^{n_i}}, \alpha_i\}.$$

Let $\alpha \in \mathcal{R}_F$. We denote by $\overline{\alpha}$ the approximation of α to a precision of m ℓ-adic digits. As Steinberg's symbol is $\mathbb{Z}_\ell$-bilinear we have $\{\zeta_{\ell^{n_i}}, \alpha\} = \{\zeta_{\ell^{n_i}}, \overline{\alpha}\}$ for all $\alpha \in \mathcal{R}_F$. Therefore the ℓ-part of the wild kernel is

$$\bigoplus_{i=1}^{r} \mathbb{Z}/\ell^{n_i}\mathbb{Z}\{\zeta_{\ell^{n_i}}, \overline{\alpha}_i\}.$$

5 Examples

All algorithms presented here have been implemented in the computer algebra system Magma [C$^+$]. The groups are given as lists of the orders of their cyclic factors. By i we denote a root of x^2+1, by ζ_m we denote a primitive m-th root of unity.

Belabas and Gangl [BG] have developed an algorithm for the computation of the tame kernel $K_2\mathcal{O}_F$ [BG]. The following table contains the structure of $K_2\mathcal{O}_F$ as computed by Belabas and Gangl and the ℓ-rank of the wild kernel $WK_2(F)$ calculated with our methods. The starred entry is a conjectural result.

F	$K_2\mathcal{O}_F$	ℓ	$\widetilde{\mathcal{C}\ell}_{F(\zeta_\ell),\ell}$	$\widetilde{\mathcal{C}\ell}^{e_\infty}_{F(\zeta_\ell),\ell}$	$\mathrm{rank}_\ell(WK_2)$
$\mathbb{Q}(\sqrt{-331})$	[3]	3	[3,3]	[3]	1
$\mathbb{Q}(\sqrt{-367})$	[3]	3	[3,9]	[3]	1
$\mathbb{Q}(\sqrt{-472})$	[5]	5	[5,5]	[5]	1
$\mathbb{Q}(\sqrt{-571})$	[5]	5	[5,5]	[5]	1
$\mathbb{Q}(\sqrt{-696})$	[42]	3	[3]	[1]	0
		7	[7,7]	[7]	1
$\mathbb{Q}(\sqrt{-759})$	$[2,18]^*$	3	[3,3]	[3]	1

The next table contains more fields together with the main data needed for the computation of the ℓ-rank of WK_2. χ_α denotes the minimal polynomial of α over $\mathbb{Q}$.

F	ℓ	$\widetilde{\mathcal{C}\ell}_{F(\zeta_\ell),\ell}$	$\widetilde{\mathcal{C}\ell}^{e_\infty}_{F(\zeta_\ell),\ell}$	$\mathrm{rank}_\ell(WK_2)$
$\mathbb{Q}(\sqrt{-7307})$	5	[5,25]	[1]	0
$\mathbb{Q}(\sqrt{-356467})$	3	[3,3,27]	[3]	1
$\mathbb{Q}(\alpha)$, $\chi_\alpha = x^3 + x^2 - 9x - 365$	3	[9]	[9]	1
$\mathbb{Q}(\alpha)$, $\chi_\alpha = x^3 + x^2 - 133x - 1937$	3	[3,3]	[3]	1
$\mathbb{Q}(\alpha)$, $\chi_\alpha = x^3 + x^2 - 65x + 1875$	3	[3,3,3]	[3,3]	2
$\mathbb{Q}(\alpha)$, $\chi_\alpha = x^3 + x^2 - 65x + 1875$	3	[3,3,3]	[3,3]	2
$\mathbb{Q}(\alpha)$, $\chi_\alpha = x^4 + 9x^2 + 125$	3	[3,3]	[3]	1

Our last table gives examples of the ℓ-part of the wild kernel together with the generators of the cyclic factors. We made extensive use of the discrete logarithm in $\widetilde{\mathcal{C}\ell}_{F,\ell}$ in order to find small generators for it.

F	$\widetilde{\mathcal{C}\ell}_{F,2}$	2-part of $WK_2(F)$
$\mathbb{Q}(i,\sqrt{85})$	[2,2]	$\mathbb{Z}/2\mathbb{Z}\,\{-1, i-2\} \oplus \mathbb{Z}/2\mathbb{Z}\left\{-1, \frac{\sqrt{85}+11}{2}\right\}$
$\mathbb{Q}(i,\sqrt{357})$	[2,2,2]	$\mathbb{Z}/2\mathbb{Z}\,\{-1, 3\} \oplus \mathbb{Z}/2\mathbb{Z}\left\{-1, \frac{i\sqrt{357}+21i+2}{2}\right\} \oplus$ $\mathbb{Z}/2\mathbb{Z}\left\{-1, \frac{(i+4)\sqrt{357}+19i+76}{2}\right\}$
$\mathbb{Q}(i,\sqrt{1173}$	[2,2,2]	$\mathbb{Z}/2\mathbb{Z}\,\{-1, 3\} \oplus \mathbb{Z}/2\mathbb{Z}\left\{-1, \frac{(4i+16)\sqrt{1173}+137i+548}{2}\right\} \oplus$ $\mathbb{Z}/2\mathbb{Z}\left\{-1, \frac{(-927i-3300)\sqrt{1173}-31749i-13022}{2}\right\}$
$\mathbb{Q}(\zeta_8,\sqrt{561})$	[4,4,4]	$\mathbb{Z}/4\mathbb{Z}\left\{i, (2\zeta_8^3+3\zeta_8^2+2\zeta_8)\sqrt{561} - 80\zeta_8^3 + 80\zeta_8 + 114\right\} \oplus$ $\mathbb{Z}/4\mathbb{Z}\left\{i, \frac{(15\zeta_8^3+12\zeta_8^2+38\zeta_8+12)\sqrt{561}-93\zeta_8^3+12\zeta_8^2-330\zeta_8-372}{2}\right\} \oplus$ $\mathbb{Z}/4\mathbb{Z}\left\{i, (-\zeta_8^3+\zeta_8^2-\zeta_8)\sqrt{561} + 13\zeta_8^3 - 28\zeta_8^2 + 15\zeta_8 + 2\right\}$

References

[BT] H. Bass and J. Tate, *The Milnor ring of a global field*, in H. Bass (ed.), Algebraic K-theory, Lecture Notes in Math. **342**, Springer Verlag Berlin (1973), 349–446.

[BG] K. Belabas and H. Gangl, *Generators and Relations for* $K_2\mathcal{O}_F$, preprint.

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

[DJ$^+$] F. Diaz y Diaz, J.-F. Jaulent, S. Pauli, M.E. Pohst, and F. Soriano, *A new Algorithm for the Computation of logarithmic* ℓ*-class groups of number fields*, will be submitted soon.

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

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

[Ga] H. Garland, *A finiteness theorem for* K_2 *of a number field*, Ann. of Math. **94** (1971), 534–548.

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

[J1] J.-F. Jaulent, *Introduction au* K_2 *des corps de nombres*, Publ. Math. Fac. Sci. Besançon (Théorie des nombres), Anèes 1984/85–1985/86.

[J2] J.-F. Jaulent, *Sur le noyau sauvage des corps de nombres*, Acta Arithmetica **67** (1994), 335–348.

[J3] J.-F. Jaulent, *Classes logarithmiques des corps de nombres*, J. Théor. Nombres Bordeaux **6** (1994), 301–325.

[J4] J.-F. Jaulent, *Classes logarithmiques des corps ide nombres totalement réels*, Acta Arithmetica **103** (2002), 1–7.

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

[JS2] J.-F. Jaulent and F. Soriano-Gafiuk, *2-Groupe des classes positives et noyau sauvage de la* K_2*-Théorie*, to appear in J. Number Theory.

[Ko] M. Kolster, *An idelic Approach to the Wild Kernel*, Invent. Math. 103 (1991), 9-24.

[Mi] J. Milnor, *Introduction to Algbraic* K*-Theory*, Ann. of Math. Studies **72**, Princeton Univ. Press, Princeton (1971).

[Mo] C. Moore *Group extensions of p-adic and adelic linear groups*, Publ. Math. I.H.E.S. **35** (1969), 5–74.

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

[T1] J. Tate, *Symbols in arithmetic*, Actes Congrès Int. de Math. 1970, Tome 1, 201–211.

[T2] J. Tate, *Relations between* K_2 *and Galois cohomology*, Invent. Math. **36** (1976), 257–274.