GENERATORS AND RELATIONS FOR $K_2\mathcal{O}_F$

KARIM BELABAS AND HERBERT GANGL

Abstract. Tate's algorithm for computing $K_2\mathcal{O}_F$ for rings of integers in a number field has been adapted for the computer and gives explicit generators for the group and sharp bounds on their order—the latter, together with some structural results on the p-primary part of $K_2\mathcal{O}_F$ due to Tate and Keune, gives a proof of its structure for many number fields of small discriminants, confirming earlier conjectural results. For the first time, tame kernels of non-Galois fields are obtained.

Contents

1991 *Mathematics Subject Classification.* 11Y40 (11R70, 19C20).
Key words and phrases. K_2, number fields, tame kernel.
The second author was supported by the Deutsche Forschungsgemeinschaft.

1. Introduction

The Milnor K-group $K_2\mathcal{O}_F$ of the ring of integers $\mathcal{O}_F$ in a number field F is known to be a finite abelian group. Its actual determination, though, is very difficult.

For totally real abelian F, the "Birch-Tate conjecture" (which follows from the "Main Conjecture" proved by Mazur-Wiles [29] for the odd part and from work of Kolster [38, Appendix A] for the 2-part)

$$|K_2\mathcal{O}_F| = (-1)^{r_1(F)} w_2(F)\zeta_F(-1)$$

enables one to compute the order of $K_2\mathcal{O}_F$, hence often its structure (whenever the order is squarefree). Here ζ_F is the Dedekind zeta function of F, $r_1(F)$ is the number of real places of F and $w_2(F)$ the largest integer n such that the Galois group $\mathrm{Gal}(F(\zeta_n)/F)$ is a 2-elementary abelian group, with ζ_n a primitive n-th root of unity.

For a general number field, Tate [44] has given an algorithm to bound the number of generators which enabled him—after some further clever manipulations—to complete the analysis for the six imaginary quadratic fields of smallest discriminant. Subsequently, other authors (Skałba [42], Qin [34, 36], Browkin [7]) have improved the method and were able to establish several other imaginary quadratic cases, the largest (in absolute value) discriminant treated so far being -35.

We present an algorithm for computing $K_2\mathcal{O}_F$ for a general number field F, that can be divided roughly into three steps:

(a) Find a small set of generators, via a refinement of Tate's and Browkin's elimination procedures.
(b) Create enough relations among those generators. This gives us *upper* bounds on the order of the generators.
(c) Bound the size of the p-primary part of $K_2\mathcal{O}_F$ *from below* with the help of class group computations, via results of Tate and Keune.

The first step was originally based on work of Browkin [7], dealing with the imaginary quadratic case, which in fact gave the impetus for this paper. Eventually it was adapted for arbitrary number fields and implemented in the PARI/GP [33] scripting language. So far, the programs can handle larger discriminants if the field is imaginary quadratic, because some of the refining processes from §3.3.3 were only implemented in this case.

We used the program to compute the structure of $K_2\mathcal{O}_F$ (previously conjectured in [8]) for all imaginary quadratic fields of discriminant Δ such that $|\Delta| \leq 1000$ with only 7 exceptions, and for a few miscellaneous fields of higher degree (cf. §7). In particular, for $F = \mathbb{Q}(\sqrt{-303})$, we obtain $K_2\mathcal{O}_F = \mathbb{Z}/22\,\mathbb{Z}$, and a generator is given by the symbol

$$\{17 + 3\omega_F, 2\}\,.$$

Here and in the sequel, ω_F denotes the standard quadratic generator of $\mathcal{O}_F$: we let $\omega_F = \sqrt{\Delta}/2$ or $(1+\sqrt{\Delta})/2$ depending on the parity of the field discriminant Δ.

Furthermore, in many other cases including the 7 exceptions mentioned above, we still obtain a set of simple generators together with multiplicative bounds on their orders. For instance, if $F = \mathbb{Q}(\sqrt{-755})$, then $K_2\mathcal{O}_F$ is generated by

$$\{2, \omega_F - 1\}^6$$

and its order is either 2 or 2×41. The latter is almost certainly the correct value since it coincides with the conjectured one from [8], which used a different method.

As a last interesting example, we have proven that, for $F = \mathbb{Q}(\sqrt{-4547})$,

$$\{5, 49 + 2\omega_F\}^{56}$$

generates $K_2\mathcal{O}_F$ and has exponent 233, which is prime. We conjecture, as in [8], that $K_2\mathcal{O}_F$ has order 233.

The organization of the paper is as follows. In §2, we give definitions and basic properties of the objects which are computed. We also recall ideas from the computation of class groups via index calculus which we adapt to the $K_2\mathcal{O}_F$ situation. In §§3-4, we discuss Tate's method, further improved by Skałba and Browkin, and systematize it. This covers the first step of the algorithm. In §5, we explain the second step and how one computes a tentative group $\widetilde{K_2}\mathcal{O}_F$ of which $K_2\mathcal{O}_F$ is a quotient. If enough relations have been produced, these two groups should coincide. The third step is dealt with in §6, where we recall Keune's result exhibiting p^n-torsion in $K_2\mathcal{O}_F$ from p^n-torsion in the class group of the cyclotomic extension $F(\zeta_{p^n})$ and discuss its realizability. In a final section §7, we list our results and give a few examples.

Acknowledgements: We would like to thank Henri Cohen, Jean-Louis Colliot-Thélène, Claus Fieker, Rob de Jeu, Thorsten Kleinjung, Manfred Kolster, Chazad Movahhedi, Thong Nguyen Quang Do, and foremost Jerzy Browkin for useful discussions and correspondence. We would also like to thank the Max-Planck-Institut für Mathematik and the Arithmetic Algebraic Geometry Network for financial support.

2. Background

2.1. **The functor K_2.** For the convenience of the reader we recall the setup from Tate's paper [44]. We order the finite primes $v_1, v_2, \dots$ in the number field F by norm, writing Nv for the absolute norm of v, and put

$$S_m = \{v_1, \dots, v_m\}.$$

We let (r_1, r_2) denote the signature of F, and $n = r_1 + 2r_2 = [F : \mathbb{Q}]$. Given a set S of finite places of F, denote by $\mathcal{O}_S$ the ring of S-integers of F, by U_S the group of S-units, by $\mu(F)$ the group of roots of unity in F, and by $k(v)$ the residue field of the place v.

Recall that K_2F can be defined as the quotient of $F^* \otimes F^*$ modulo the subgroup generated by the elements of the form $x \otimes (1-x)$, where $x(1-x) \in F^*$. The symbol $\{a, b\}$ denotes the projection of $a \otimes b \in F^* \otimes F^*$ in K_2F. Let $K_2^S(F)$ be the subgroup of K_2F generated by the symbols with support in S, i.e., those symbols $\{a, b\}$ for which $a, b \in U_S$. We have a natural filtration on $K_2F = \varinjlim_m K_2^{S_m}(F)$.

Let $\partial_v : K_2F \to k(v)^*$ be the tame symbol corresponding to v, given by

$$\partial_v(\{a, b\}) := (-1)^{v(a)v(b)} a^{v(b)}/b^{v(a)} \pmod{v}.$$

(By abuse of notation, we will use the same symbol v for a finite place and the associated normalized valuation.) This is well defined and the group $K_2\mathcal{O}_F$ can be given, via a theorem of Quillen, as the *tame kernel* $\bigcap \operatorname{Ker} \partial_v$, where v runs through all finite places of F.

Garland [18] proved that $K_2\mathcal{O}_F \subset K_2^S(F)$ for a finite set of places S. This immediately implies that $K_2\mathcal{O}_F$ is finitely generated since the S-units are themselves finitely generated, with $|S| + r_1 + r_2$ generators, one of them being torsion, the others of infinite order. Since $K_2\mathcal{O}_F$ is also known to be a torsion group [*loc. cit.*], it is a finite abelian group.

Bass and Tate [2] made Garland's argument effective for any number field, and Tate refined it further for principal imaginary quadratic fields, completing the work for the 6 smallest discriminants (in absolute value): -3, -4, -7, -8, -11, -15. Most of the explicit computations of $K_2\mathcal{O}_F$ referred to in §1 are refinements of Tate's method, and rely on little more than Minkowski's theorem on lattice points.

The best unconditional result is due to Groenewegen [21] (improving considerably on earlier work of Skałba [42] and Browkin [7]).

Theorem 2.1 (Groenewegen)**.** *Let F be a number field of degree n, and Δ its discriminant. Then $K_2\mathcal{O}_F \subset K_2^S(F)$, with $S = \{v : Nv \leq c_F\}$ where*

$$c_F = \max\{2^{2n}\rho d^2, 2^{2n/3}\rho^{1/3}(d\tilde{d})^{2/3}\rho d^3\} \leq 4|\Delta|^{3/2},$$

where

$$d = \frac{2^n\Gamma(n/2+1)}{(\pi n)^{n/2}}|\Delta|^{1/2} \quad \textit{and} \quad \tilde{d} = \left(\frac{2}{\pi}\right)^{r_2}|\Delta|^{1/2}$$

and $\rho = \rho_n$ is the packing density of the n-dimensional sphere ($\rho \leq (n+2)/2^{n/2+1}$, $\rho_2 = \pi/\sqrt{12}$).

2.2. **Computing class groups.** From a theoretical point of view, units and class groups in general number fields are determined from the exact sequence

$$1 \longrightarrow \mathcal{O}_F^* \longrightarrow U_S \xrightarrow{f} \mathbb{Z}^S \xrightarrow{g} \mathrm{Cl}(\mathcal{O}_F) \longrightarrow 1,$$

where S is large enough, $f : x \mapsto (v(x))_{v\in S}$, and $g : (e_v) \mapsto \prod_{v\in S} v^{e_v}$. The S-units are generated by an explicit finite set given by the integral points in a ball of large radius. See Lenstra [28] for precise bounds, which are the basis of Groenewegen's work. The kernel and cokernel of f are determined by simple linear algebra. The problem with this rigorous approach is that it is completely impractical given the huge dimension of the modules involved.

We recall the basic idea of modern *heuristic*[1] algorithms using randomization to alleviate this problem (see [11]). We need the following three ingredients:

- A distinguished set of generators $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ for the class group, namely all prime ideals less than the Minkowski bound, or Bach's bound [1], if one is willing to assume the Generalized Riemann Hypothesis (GRH). They form a nice factor base.
- An easy way to produce relations: one factors elements of small norm on the factor base given above, since a factorization $(x) = \prod \mathfrak{p}_i^{e_i}$ yields a relation among the generators, encoded by the vector $f(x) = (e_i)$. There are other ways, necessary in general (especially when F has many subfields), such as computing random relations using Buchmann's ideal reduction theory, but unfortunately we know of no equivalent in our K_2 situation.
- A rough estimate for the class group size, and more precisely for the product hR of the class number h with the regulator R, provided by Dirichlet's class number formula.

The class group $\mathrm{Cl}(\mathcal{O}_F)$ is completely known once the kernel Λ in

$$1 \longrightarrow \Lambda \longrightarrow \mathbb{Z}^S \xrightarrow{g} \mathrm{Cl}(\mathcal{O}_F) \longrightarrow 1,$$

is determined. Let $\tilde{\Lambda}$ be the submodule of $\mathbb{Z}^S$ generated by a number of relation vectors; and let $M_{\tilde{\Lambda}}$ be the corresponding integral matrix. The Hermite Normal Form (HNF) algorithm, applied to $M_{\tilde{\Lambda}}$, yields the index $\tilde{h} = [\mathbb{Z}^S : \tilde{\Lambda}]$, which is a multiple of the true class number (or equal to ∞). The HNF algorithm also computes the integer kernel of $M_{\tilde{\Lambda}}$, which corresponds to *trivial* relations of the form $\alpha\mathcal{O}_F = \mathcal{O}_F$, in other words, to units. From the logarithmic embeddings of these units, one computes a tentative regulator $\tilde{R}$, which is an integral multiple of the actual one.

Let C be a rough estimate for hR, such that $C/2 < hR < C$. If $\tilde{R}$ is non-zero, which can be checked numerically using Zimmert's universal lower bound for

[1]The algorithm's analysis is only satisfactory for imaginary quadratic fields, see Hafner-McCurley [22].

the regulator $R > 0.056$ [49], we now have a full set of relations and a full set of generating units if and only if $\tilde{h}\tilde{R} < C$, since the latter implies $\tilde{h} = h$ and $\tilde{R} = R$. Once this is achieved, the Smith Normal Form (SNF) algorithm yields the structure of the class group $\mathrm{Cl}(\mathcal{O}_F)$ as a product of cyclic groups, together with explicit generators, and we can extract a system of fundamental units from the information used to compute $\tilde{R}$.

2.3. **Higher class groups.** Ideas analogous to the ones in the previous subsection can be used to compute $K_2^S(F)$. We can easily factor elements of the form $x\otimes(1-x)$ on fixed generators of $U_S \otimes U_S$. Hence, assuming we can find enough relations, we should be able to compute $K_2^S(F)$. Should this be feasible for a sufficiently large S, such as the one given by Groenewegen, the subgroup $K_2\mathcal{O}_F$ would then be given by the intersection of all $\mathrm{Ker}\,\partial_v : K_2^S(F) \to k(v)^*$, $v \in S$, which is obtained by elementary linear algebra (see §5.3). We unfortunately face two serious problems:

(a) Too many generators: Groenewegen's bound c_F is exponential in $\log(|\Delta|)$, and the number of generators for $U_S \otimes U_S$ is $O(|S|^2) = O((c_F/\log c_F)^2)$ by the prime ideal theorem. For $\Delta \approx 100$, this bound is bigger than 200000 and it will be exceedingly hard to HNF-reduce a matrix of that dimension[2].

(b) No stopping criterion: suppose no matter how many relations we add, the computed value for $|K_2\mathcal{O}_F|$ stabilizes. Unfortunately, we still have to prove that we have a full set of relations, and our construction alone cannot do it, when the wild kernel WK_2F is non-trivial (see §6.1). Unfortunately, this is the most interesting—albeit rather rare—case.

We will see in the next section that the first problem is easily overcome when the discriminant Δ remains relatively small ($|\Delta| \leq 5000$, say): by following explicitly the steps in Tate's proof, we obtain an algorithm that considerably reduces the number of generators, for a given field.

As for the second problem, we will see in §6 a number of useful tests, relying in particular on work of Tate [45] and Keune [25], to determine the p-primary part of $K_2\mathcal{O}_F$, which most of the time yields enough information to conclude. Unfortunately, its implementation requires to assume the GRH unless p is very small (in order to compute class groups of cyclotomic extensions of F), and is not practical, even under GRH, if p is large.

At this point, it is tantalizing to use the Lichtenbaum conjecture, which is a higher analog of Dirichlet's class number formula and specializes to the Birch-Tate formula when F is abelian and real. A proof of the cohomological version of this conjecture[3] seems to be within reach in the case of abelian fields due to the efforts of Kolster, Nguyen-Quang-Do and Fleckinger [26]. Unfortunately, even after removing erroneous Euler factors in their main formula, the statement is given only up to an unspecified power of 2, when the field is complex (cf. also the recent papers of Huber-Kings [23] and Burns-Greither [10]). For non-abelian fields, the conjecture is still completely open.

An exact statement, including the 2-primary part, would allow us to argue as follows: Lichtenbaum's conjecture expresses the product h_2R_2 in terms of accessible invariants, where $h_2 = h_2(F) := |K_2\mathcal{O}_F|$ and $R_2 = R_2(F)$ is the volume of a lattice formed from the images of "higher units" (the Bloch group $B(F)$, which is closely related to K_3F by work of Bloch [3, 4] and Suslin [43]) under a higher regulator map on the Bloch group (given by dilogarithms, and compatible with Borel's regulator

[2]The HNF implementations in PARI can easily treat sparse relation matrices of dimension 2000, but treating dimensions larger than 10000, say, would require a major computational effort.

[3]which in the special case we need to compute $K_2\mathcal{O}_F$, this is known to be equivalent to the K-theoretic formulation.

on K_3F). Reducing the relation lattice in $U_S \otimes U_S$, i.e., computing the span of the exponent vectors provided by the factorizations of the relations $x \otimes (1-x)$, naturally produces elements in $B(F)$ (as relations among the relations). From the relations and higher units found so far, we can derive tentative values for h_2 and R_2, say $\tilde{h}_2$ and $\tilde{R}_2$, which are both *integral multiples* of the correct values. Indeed $\tilde{h}_2/h_2$ is the index of our relation lattice for $K_2\mathcal{O}_F$ in the full one, and $\tilde{R}_2/R_2$ is the index of the span of our higher units in the full lattice of higher units. If $\tilde{h}_2\tilde{R}_2/h_2R_2$ is strictly less than 2, where the denominator is computed via Lichtenbaum's formula, we in fact have $h_2 = \tilde{h}_2$ and $R_2 = \tilde{R}_2$, thereby proving that we have indeed computed $K_2\mathcal{O}_F$ and $B(F)$.

So far, although the algorithm produces useful unconditional information about $K_2\mathcal{O}_F$ in the guise of explicit simple generators and a multiple of their order, it may require the full strength of Lichtenbaum's formula to prove that the presentation is complete. For totally real abelian fields, where the formula is known to hold, it can very easily be applied since there are no higher units: the regulator R_2 is defined to be 1.

Numerical experiments performed by Grayson [20] and, more extensively, by the second author [17] suggest that, if F is imaginary quadratic, Lichtenbaum's conjecture should read:

$$h_2R_2 = \frac{3}{\pi^2}|\Delta|^{3/2}\zeta_F(2),$$

where ζ_F is the Dedekind zeta function and Δ is the field discriminant.

Remark 2.1: It is of course not fortuitous that the class group algorithm generalizes so well. One has canonical isomorphisms

$$K_0\mathcal{O}_F \simeq \mathbb{Z} \oplus \mathrm{Cl}(\mathcal{O}_F) \quad \text{and} \quad K_1\mathcal{O}_F \simeq \mathcal{O}_F^*,$$

and we are replicating the classical algorithm two steps higher, replacing K_0 and K_1 by their analogs K_2 and K_3, respectively.

3. Reducing Groenewegen's bound

In this section, we fix a set S of finite places and $v \notin S$. We write A for $\mathcal{O}_S$, U for U_S and k for $k(v)$. The main ideas are adapted from Tate's seminal paper [44].

Let $T := S \cup \{v\}$ and assume that $K_2\mathcal{O}_F \subset K_2^T(F)$. We want to prove that, in fact, we already have $K_2\mathcal{O}_F \subset K_2^S(F)$. This will be used in the following situation: starting from Groenewegen's initial set S (from Theorem 2.1), we iterate this process, successively truncating S by deleting its last element with respect to the given ordering, hoping to reduce the set of places to a manageable size. As soon as one of the tests described below fails, the reduction process stops and we proceed to the next phase of the algorithm: building the relation matrix (cf. §5).

In fact, Groenewegen's bound c_F is very pessimistic. Our experiments indicate that a small power of $\log|\Delta|$ would be a more sensible order of magnitude: in the ranges we explored ($|\Delta| < 5000$), the final set S happens to contain between 10 and 20 elements. Again, this parallels the class group situation where we can first assume the GRH and use Bach's generators, then prove that all ideals up to Minkowski's bound can be generated from this small subset.

3.1. A notion of smallness.

For $a \in F$, define

$$T_2(a) := \frac{1}{[F:\mathbb{Q}]}\sum_{\sigma}|\sigma(a)|^2 \quad \text{and} \quad \|a\| := \sqrt{T_2(a)},$$

where σ runs through the $[F:\mathbb{Q}]$ embeddings of F into $\mathbb{C}$ and $|x|$ denotes the complex modulus of x. Note that $\|.\|$ is a norm of $\mathbb{Q}$-vector spaces, and T_2 a positive definite quadratic form on the coordinates of a on any $\mathbb{Q}$-basis. The norm

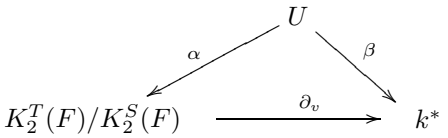
$\|.\|$ gives a precise meaning to the word *small* applied to an element of F. Due to the celebrated LLL algorithm, it is easy to compute vectors in lattices (or grids, i.e., translates of lattices) which are small with respect to T_2, with precise quantitative statements with respect to their relation to the *shortest* vectors. This would not be the case if we had chosen $\|\cdot\|_\infty$ instead, for instance.

The quadratic form T_2 coincides with the ordinary modulus when F is imaginary quadratic. It generalizes to arbitrary number fields the Euclidean techniques used by Tate, Browkin and others to compute the tame kernel of imaginary quadratic fields.

3.2. **The brute force approach.** We first require[4] that v be principal in A, say $v = \pi A$. The tame symbol ∂_v vanishes on $K_2^S(F)$, hence induces a homomorphism

$$\partial_v : K_2^T(F)/K_2^S(F) \to k^* . \tag{1}$$

Recall that we assumed that $K_2\mathcal{O}_F \subset K_2^T(F)$. Obviously, $K_2\mathcal{O}_F \subset K_2^S(F)$ if this induced morphism is injective. We now consider the following commutative triangle:



where $\alpha(u) := \{u, \pi\} \pmod{K_2^S(F)}$ and $\beta(u) := u \pmod{v}$, for $u \in U$. The morphism α is easily seen to be surjective: the only difficulty is to notice that $\{\cdot,\cdot\}$ is skew-symmetric and that $\{\pi, \pi\} = \alpha(-1)$, see [44]. Hence, ∂_v is injective if and only if $\operatorname{Ker}\alpha = \operatorname{Ker}\beta$.

This last property is not usable directly since $\operatorname{Ker}\alpha$ seems to be hard to compute. Fortunately, we know a sizeable chunk of this kernel offhand: define U_1 to be the subgroup of U generated by $(1+\pi U)\cap U$; then $U_1 \subset \operatorname{Ker}\alpha$. Indeed, if $u = 1+\pi t \in U_1$, one has $1 = \{1+\pi t, -\pi t\} = \{u, -t\}\{u, \pi\} \equiv \{u, \pi\} \pmod{K_2^S(F)}$, since both u and t are supported on S.

So $U_1 \subset \operatorname{Ker}\alpha \subset \operatorname{Ker}\beta$. If we are lucky, then $U_1 = \operatorname{Ker}\beta$ and we are done; in fact, this is guaranteed if $Nv > c_F$, and in practice appears to be true for all but a few very small primes. This suggests the following heuristic algorithm.

Algorithm 3.1:
Input: a set S of finite places, and a place $v \notin S$ such that $K_2\mathcal{O}_F \subset K_2^{S\cup\{v\}}(F)$.
Output: check whether $U_1 = \operatorname{Ker}\beta$. If so, $\operatorname{Ker}\alpha = \operatorname{Ker}\beta$ and $K_2\mathcal{O}_F \subset K_2^S(F)$. The algorithm returns `FAIL` if the condition could not be successfully checked (the equality may hold nevertheless).

(a) [Compute π]. If v is not principal in A, return `FAIL`. Else compute a generator π of v using Sub-algorithm 3.2.
(b) [Compute U]. This yields a set W of $d := |S|+r_1+r_2$ independent generators of U_S, as well as technical data needed to solve the discrete logarithm problem in U.
(c) Compute the cardinality B of $\operatorname{Im}\beta$. This is done by reducing the elements of W modulo v and computing their order in the cyclic group k^*; the lcm of the orders is B.
(d) Create an empty relation matrix and set a failure counter `fail` to 0.

[4]In practice, this condition is easy to check and is always satisfied except for very small sets S which we are not interested in reducing anyway. In fact, A itself will be principal as soon as S contains the generators of the class group which, according to Bach's GRH bound [1], will be true for S containing the primes of norm less than $12\log^2|\Delta|$.

(e) [Find an element in U_1]. Compute a small multiplicative combination t of the generators from Step (b). If $u := 1+\pi t$ is an S-unit, go to Step (f). Otherwise, increase `fail`. If the counter gets too large, return `FAIL`.

(f) [Update relation matrix]. Factor $u \in U_1$ on the factor base and append the exponent vector to the relation matrix. If we have found less than d relations, reset `fail` to 0 and go to Step (e).

(g) Let H be the HNF of the relation matrix. If it has maximal rank (namely d) and $\det(H) = B$, return `TRUE`. Otherwise, increase `fail`, delete dependent relations and go to Step (e).

Proof. The only non-trivial step is the last one. Let $\tilde{U}_1 \subset U_1$ be the lattice generated by the S-units $u \in U_1$ constructed so far in Step (e); then $\det(H) = [U : \tilde{U}_1]$. Since $|\operatorname{Im}\beta| = [U : \operatorname{Ker}\beta]$ and $\tilde{U}_1 \subset U_1 \subset \operatorname{Ker}\beta$, we have $\det(H) = |\operatorname{Im}\beta|$ if and only if $\tilde{U}_1 = U_1 = \operatorname{Ker}\beta$. The counter `fail` ensures that the algorithm terminates. □

Sub-algorithm 3.2:
Input: a set S of finite places, and a place $v \notin S$.
Output: a uniformizer in S-integers.

(a) If v is principal in $\mathcal{O}_F$, compute a generator of small T_2-norm using the principal ideal algorithm [11, Chapter 6] and return it.

(b) Factor v on a fixed basis for the class group. Since Step (a) did not succeed, we obtain a non-zero exponent vector $e(v)$. Factor each element v_i of S on the same generators, and stop when $e(v)$ falls into the lattice generated by the exponent vectors $e(v_i)$ corresponding to the v_i (check using successive HNF reductions). In matrix form, $Mu = e(v)$ has an integral solution u_0, where the columns of M are given by the exponent vectors $e(v_i)$.

(c) Using for instance the second reduction algorithm in §4.1, compute a small vector u in the grid $u_0 + \operatorname{Ker} M$.

(d) The corresponding relation in the class group $v \sim \prod v_i^{u_i}$ gives a uniformizer in the S-integers: $(\pi) = v\prod v_i^{-u_i}$, which involves few v_i.

Remark 3.3: (a) All the S-units and principal ideal computations above can be done by a straightforward generalization of the classical situation $S = \emptyset$ (see [12, Chapter 7]). When iterating this procedure, one should make sure to arrange the initialization Step (3.1.b) so that it can be re-used by simply deleting a generator.

(b) By a famous result of Siegel [41], made effective by Baker's theory of linear forms in logarithms, there are only a finite number of solutions to the equation $u+\pi t = 1$ in S-units u and t. There are tractable ways of enumerating them all using Baker's method and LLL-reduction when the S-unit rank is small [14, 48], less than 20, say. In our situation, both the reduced bounds and the actual number of solutions are hopelessly huge, and an exhaustive search is impractical. Fortunately, although it seems hard to fully analyze this behaviour, we only need a very small fraction of these solutions to build U_1. In practice, using at most two generators in the product defining t works very well. This amounts to checking at most $O(|S|^2)$ S-units.

(c) In Step (3.1.c), we expect that $\operatorname{Im}\beta = k^*$ as soon as S includes enough small primes. For instance, assuming GRH, Bach's version of Ankeny's theorem (see [1]) says that the integers up to $2\log^2(p)$ in absolute value generate the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. Taking for G this set of rational integers, it implies that, for a place v of inertia degree 1, one has $\operatorname{Im}\beta = k^*$ as soon as S contains all the places dividing the primes less than $2\log^2 Nv$. Note that we should also check that this set G is included in U, and we can only ensure this in general by requiring that $2\log^2 Nv < \sqrt{Nv}$, i.e.,

$Nv \geq 57829$, which is far beyond the limits of our HNF implementation. In short, this line of reasoning, although interesting asymptotically, has mostly heuristic value. It tells us that the first few elements should generate $\operatorname{Im}\beta$ in Step (3.1.c), and not $O(|S|)$ many as the size of W would indicate. Hence one checks the elements of W one by one and computes an lcm after each order computation: we abort this step as soon as the lcm reaches $Nv-1$, thereby proving that $\operatorname{Im}\beta = k^*$.

(d) We are only interested in factoring S-units in Step (3.1.f), and this is easily done by trial dividing by the primes in S. More precisely, given $x \in F$, we trial divide the absolute norm of x by the rational primes covered by the elements of S, and compute only those valuations lying above the primes which divide the norm of x. All the other valuations are 0.

(e) The class group of F is computed via a finite presentation, and its generators (g_i) are initially given in terms of a fixed factor base $\mathcal{B}$ of prime ideals. Conversely, the elements of $\mathcal{B}$ are easily obtained in terms of the g_i. If S is not too large, it will be contained in $\mathcal{B}$, and the factorization of the v_i in Sub-algorithm 3.2 will be already known. Note that these factorizations were also needed to compute U_S in Step (3.1.b).

The whole point of Algorithm 3.1 is that, assuming we can truncate S all the way down to bounded size, we handle $O(|S|)$ relation matrices of dimension $O(|S|)$, instead of a single one of size $O(|S|^2)$. Since no linear time HNF algorithm is known (in fact, none can exist), this is a definite improvement. The storage requirements are likewise lowered.

On the other hand, this method is still unable to handle really large sets S. We will see in the next subsection a clever construction, due to Tate, which implements the same test ($U_1 = \operatorname{Ker}\beta$) in a simpler way. It is less efficient as far as lowering the bound goes since, in general, it succeeds only when Algorithm 3.1 would, but is much faster to execute.

3.3. **Tate's method.**

3.3.1. *The general case.* The setup is the same as in the previous section, except that we do not assume that v is principal. If v happens to be non-principal we define $U_1 := \{1\}$. We would like to apply, for as many primes v as possible, the following criterion of Tate:

Proposition 3.4. [44, Prop. 1, p. 430] *Suppose that W, C and G are subsets of U satisfying the following three conditions*

$$\begin{array}{lll} \text{(T1)} & W \subset CU_1, \quad \textit{and} & W \textit{ generates } U, \\ \text{(T2)} & CG \subset CU_1, \quad \textit{and} & \beta(G) \textit{ generates } k^*, \\ \text{(T3)} & 1 \in (C \cap \operatorname{Ker}\beta) \subset U_1. & \end{array}$$

Then $U_1 = \operatorname{Ker}\beta$ and ∂_v (see (1)) is bijective.

These conditions arise quite naturally when trying to construct an explicit inverse to ∂_v by brute force. (T2) together with (T3) is a devious way to ensure that CU_1 is a subgroup of U, which will be the whole of U by (T1); multiplying on both sides by U_1, (T3) now implies that $\operatorname{Ker}\beta \subset U_1$. In particular, these conditions imply that C contains a complete system of representatives of k^*. In practice, we will choose it to be minimal, that is $|C| = |k^*| = Nv - 1$.

Remark 3.5: If this method succeeds with a finite C, then v is principal unless F is imaginary quadratic, S is empty and $Nv \leq 3$. If v is not principal, $U_1 = \{1\}$; since $CU_1 = U$, we have $C = U$. Hence, U contains only roots of unity, which forces F to be imaginary quadratic, or $\mathbb{Q}$ whose ring of integers is principal. In

fact $U = \{-1, 1\}$ since $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ are the only ones to contain higher roots of unity and they are both principal fields. The condition on Nv follows from $\langle\, \beta(G)\,\rangle = k^* \subset \{-1, 1\}$, since $G \subset U$, where $\langle\ \rangle$ denotes the span as a $\mathbb{Z}$-module.

We need one more easy lemma:

Lemma 3.6. *Assume that S is the set of all places smaller than v. Let $a, b \in U \cap \mathcal{O}_F$ satisfying $\beta(a) = \beta(b)$.*

a) If $N(b-a) < Nv^2$, then $a/b \in U_1$.

b) Let $n = [F : \mathbb{Q}]$. If

$$\|a\| + \|b\| < Nv^{2/n}, \tag{2}$$

then the condition of a) is satisfied.

Proof. a) is exactly [2, Claim 2, p. 63]. As for b), the arithmetic-geometric mean inequality implies that

$$Na \le \|a\|^n, \quad \text{for } a \in F.$$

Hence, $N(b-a) \le \|b-a\|^n \le (\|a\| + \|b\|)^n < Nv^2$. □

This is used in the following way: one constructs minimal sets C, G, W in $U \cap \mathcal{O}_F$ such that $\langle\, \beta(G)\,\rangle = k^*$, $\langle\, W\,\rangle = U$, and C is a complete set of representatives of k^*, containing 1. Let $m(C)$, $m(G)$, and $m(W)$ be the maximum of the $\|x\|$ for x in C, G and W, respectively. Condition (T3) is automatically satisfied and one then replaces the conditions (T1) and (T2) by the following ones:

$$\begin{array}{lrcl} (\mathrm{T1}') & m(W) + m(C) & < & Nv^{2/n}, \\ (\mathrm{T2}') & m(C)(m(G)+1) & < & Nv^{2/n}, \end{array}$$

since each of them easily implies the related one from Proposition 3.4. For example assume that (T2′) holds. Then, given $c \in C$, $g \in G$, one picks $c' \in C$ such that $\beta(cg) = \beta(c')$ and the lemma asserts that the quotient cg/c' belongs to U_1, hence (T2) is also satisfied.

3.3.2. *Browkin's optimization.* In the imaginary quadratic case, Browkin's bound (now superseded by c_F from Theorem 2.1) was directly derived from the proposition and the lemma in the previous section, with slight modifications to allow denominators, by taking cleverly chosen balls for the various sets. Groenewegen's construction is more roundabout, but deals also with complete balls, not with specific elements.

It should be apparent that there is ample room for improvement when working with explicit sets, if only by checking the conditions elementwise, or by checking directly that $(a/b-1)\pi^{-1}$ is in U instead of applying Lemma 3.6. The key condition is of course (T2′), since improvements to $m(C)$ or $m(G)$ will make their product significantly smaller.

In the rest of this paragraph, let us assume that F is imaginary quadratic. In this case, Browkin's bound would be $O(\Delta)$ if (T2′) could be omitted[5]. More precisely, [7, Lemma 8] says that if

$$Nv > \frac{16}{\pi^2} m(G) |\Delta|, \tag{3}$$

then it is possible to construct C such that (T2) holds. There is an inequality for (T1), analogous to (3), possibly making the computation of $m(C)$ entirely superfluous if the right conditions are met: let q_F be the least integer such that every

[5]This is mostly what GRH would do for us (asymptotically) for places of degree 1, since it asserts that one could take $m(G)$ logarithmic in Nv in this case (see Remark 3.3, part c).

ideal class of $\mathcal{O}_F$ contains an ideal of norm $\leq q_F$ (see §4.6 for how to bound this quantity). If

$$Nv > \max\left(\frac{16}{\pi^2}|\Delta|, \left(\sqrt{2q_F}\frac{2}{\pi}\sqrt{|\Delta|} + \frac{1}{\sqrt{2}}\right)^2\right), \tag{4}$$

is satisfied (the rightmost term is always dominant unless the field is principal), then (T1) holds with the same set C that resulted from (3).

3.3.3. *Reducing the set S.* We adapt Tate's strategy to the case of general number fields. The reduction is split into two phases (described in detail in the next section): First, we build a *black list* of bad primes, using only bounds and not the actual elements of the sets C, G and W. This list is initially empty.

(a) For each prime ideal v such that $Nv \leq c_F$, compute the best possible $m(G)$ using the methods of §4.5.
(b) If this succeeds, compute $m(W)$ using the algorithm from §4.6.
(c) Evaluate $m(C)$ and check conditions (T1′) and (T2′) using Algorithm 4.5. This is not so fast (a few seconds per prime) and is in fact the only practical bottleneck of the reduction phase.
(d) If it also fails, stigmatize the prime as *bad* and add it to the black list.

This ends the first phase. Now we check the black list and try to refine the reluctant primes into submission, starting from primes of highest norm. For $x \in U$, we denote by x' the unique element of C congruent to $x \pmod{v}$. This time, we explicitly compute the sets:

(a) [Initialize G]. Pick up the largest v in the list and compute a good set G as in Algorithm 4.8.
(b) [Initialize C]. Compute a good set C as in §4.3 except we now take the smallest representative for each class of $k^*/\mu(F)$, even those which violate (T2′). Compute $m(C)$.
(c) [Check W]. Check that (T1′) is satisfied (it always is in practice). If not, we abort the whole refinement procedure.
(d) [Update G]. Truncate G from below: remove all elements $g \in G$ such that $m(C)(\|g\| + 1) < Nv$. The resulting G should be non-empty.

If any of the two steps below succeed, delete v from the list and start over in Step (a).

(e) [Check (T2) elementwise]. For all pairs $(c, g) \in C \times G$, try to prove that $cg \in (cg)'U_1$ using Algorithm 4.3 below. If the algorithm fails, compute a small element d, possibly larger than c, such that $d \equiv c \pmod{v}$ and $m(W) + \|d\| < Nv$. If $dg \in (dg)'U_1$ and $d/g \in (d/g)'U_1$ for all $g \in G$, replace c by d in the set C and proceed. If not, the test fails.
(f) [Compute U_1]. If all else fails, try to prove directly that $U_1 = \operatorname{Ker}\beta$ using Algorithm 3.1.

As soon as we meet an ideal v_0 in the list that we are unable to discard, we take S equal to all the places v such that $Nv \leq Nv_0$ and apply the final class group-type construction in Algorithm 3.1.

To ensure we have enough flexibility for the final part of the algorithm (which looks for relations among Steinberg tensors supported on S-units), we do not want S to be too small, so we make sure S contains all places v dividing 2 or 3 for instance.

Remark 3.7: The replacement criterion applied in Step (e) is straightforward. We first check whether (d, g) passes the test for all g, just as (c, g) was supposed to. If so, we further check whether anytime we have $(\gamma g)' = c$ for some $\gamma \in C$ and $g \in G$ (which implies $\gamma = (c/g)' = (d/g)'$), the expected inclusion $\gamma g \in dU_1$ holds; then

we can replace c by d in C. Note that since G is minimal, it does not contain any element $\equiv 1 \pmod{v}$, so there is no ambiguity in the procedure: we can never have $(cg)' = c$.

Remark 3.8: For imaginary quadratic fields, Browkin's inequalities (4) and (3) can be used to speed up the first phase. Intermediate bounds in Groenewegen's construction could certainly be used for the same purpose, but we have not yet worked out the details.

Remark 3.9: We make one final remark which is very important for practical computations. When $F/\mathbb{Q}$ is Galois, the Galois group acts on prime ideals of given norm (in fact, transitively on the prime ideals dividing a given rational prime). We can then try to delete not only v, but all primes of norm Nv in one sweep. For that, one takes S to be the set of all primes of strictly smaller norm, and picks an arbitrary v of the chosen norm. If we can build the sets C, G and W for v, then σC, σG, and σW get rid of σv. More generally, when F is Galois over a proper subfield (the smaller, the better), that is if it has non-trivial automorphisms, only one prime ideal out of each Galois orbit needs to be considered.

In practice, the black list is relatively short. For instance for $F = \mathbb{Q}(\sqrt{-4547})$, one has $c_F = 71744$ and 741 bad primes v out of 10631, the largest norm being 67819. Using the Galois action, they in fact contribute 28 inert rational primes, 356 split ones, and 1 ramified one.

Inert primes are a disproportionate threat. Recall that the bound is on the norm, not the underlying rational prime, so very few inert primes actually play a role: in the example above, there are only 28 inert primes less than c_F, but all of them are a nuisance. This is not surprising since, if v is inert, we have little freedom to change the representatives of k^* without increasing considerably their T_2-norm.

4. Filling in some details

4.1. **Small vectors in grids.** For future reference, we review quickly in this section three basic algorithms dealing with short vectors in grids (translates of lattices), all of them applications of the LLL algorithm [27]. Given a Euclidean space E with a positive definite quadratic form Q, a free $\mathbb{Z}$-submodule Λ, and $e \in E$, the problem is to find a vector x in $e + \Lambda$ such that $Q(x)$ is small. We assume that Λ is given by a basis (λ_i), which is LLL-reduced with respect to Q.

The first algorithm, due to Fincke and Pohst, diagonalizes the form and finds recursively all points in the grid whose norm is less than a given bound. All small vectors are found, but the search is slow.

For the second one, fix an isomorphism $E \simeq \mathbb{R}^n$ and embed E in $\mathbb{R}^{n+1} \simeq E \times \mathbb{R}$ via $e \to (e, 0)$. Then consider the lattice in $\mathbb{R}^{n+1}$ generated by the $(\lambda_i, 0)$ and (x, C), where C is a huge real number (bigger than $C_0 \max_i Q(\lambda_i)$, where C_0 depends only on the dimension and a certain "quality ratio" chosen for the reduction). Then reduce this new lattice with respect to the quadratic form $Q + X_{n+1}^2$. The largest vector in the basis, projected back to E, will be a small vector belonging to $\pm e + \Lambda$ (the other vectors will have 0 as $(n+1)$-th coordinate), maybe not the smallest one, but often so in practice. The complexity of this algorithm is much better, both theoretically and in practice.

The last algorithm is the most naïve one: take the orthogonal (with respect to Q) projection of e onto the subspace spanned by Λ, and call it ε, say. If L denotes the matrix whose columns give the LLL-reduced basis of Λ, then $f := L\lceil L^{-1}\varepsilon \rfloor$ is a point of Λ close to ε, where $\lceil . \rfloor$ denotes rounding to the closest integer coordinatewise, and $L^{-1}\varepsilon$ is the inverse image of ε, corresponding to the usual matrix inverse if Λ spans E. The point $e - f$ belongs to L and has relatively small

norm. This is crude but fast, assuming the data associated to the subspace spanned by Λ have been precomputed.

4.2. **Does x belong to U_1?** We describe a simple heuristic check to decide whether a given x is in U_1, without trying to compute the whole subgroup as in Algorithm 3.1.

For the sake of completeness, we first make the trivial check for $x \in U$ explicit. We first assume the field is Galois and we are making use of the Galois action, checking all places dividing a given rational prime simultaneously. Hence we take S to be the set of prime divisors of a list P of rational primes.

Sub-algorithm 4.1:
Input: $x \in F$, F Galois over $\mathbb{Q}$.
Output: `TRUE` if $x \in U$, `FALSE` otherwise.

(a) Compute the denominator of x in the integral basis, that is write $x = a/b$ with $a \in \mathcal{O}_F$, $b \in \mathbb{Z}_{>0}$ for the smallest possible b (note that this is likely to be the original representation for x).
(b) Trial divide b by all primes in P. If the result is not 1, the factorization involves a prime not in the list, and we return `FALSE`.
(c) Compute $|Na|$ and trial divide as in Step (b). If the result is 1, return `TRUE`. Return `FALSE` otherwise.

Proof. Due to the special form of S, we have $a \in U$ if and only if $Na \in U$, and a rational integer belongs to U iff it is not divisible by any element outside P. Hence, if the algorithm returns `TRUE`, then $x \in U$.

Conversely, if $x \in U$, its minimal polynomial m_x is $\prod_{\sigma\in H}(X - \sigma(x))$ for some $H \subset \mathrm{Gal}(F/\mathbb{Q})$. The denominator d of m_x has the same prime divisors as b. Since if $v \in S$, so are all its conjugates, all the $\sigma(x)$ belong to U, hence the valuation of any of the coefficients of m_x at $v \in S$ is non-negative. In particular, the denominator d, hence b, belongs to U. Since U is a subgroup, so does a. □

Remark 4.2: Step (b) is needed since simply checking the norm would let numbers whose factorization contains a factor $v/\sigma(v)$ for some $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ slip through. Note also that if we are not in the Galois case, the procedure above verifies that $x \in U_{S'}$ where S' is the subset of S obtained by removing all v from S such that there exist $w \notin S$ above the same rational prime (of course the list of such v is precomputed). At this point, $x \in U_S$ iff the valuation of x at all $v \in S - S'$ is 0.

We now cater for the subgroup U_1:

Sub-algorithm 4.3:
Input: $x \equiv 1 \pmod{v}$, a small uniformizer π such that $\pi\mathcal{O}_S = v$, as in Sub-algorithm 3.2. A finite subset $U_0 \subset U_1$ of small elements, for instance the $1 + u\pi$ and their inverses where u runs through generators of the units or small rational integers in U (less than 5, say).
Output: `TRUE` if x is detected to be in U_1, `FAIL` otherwise (could not conclude).

(a) If $(x-1)/\pi \in U$, return `TRUE`.
(b) Otherwise, multiply x by each element of U_0 in turn, testing the product as in Step (a) above.
(c) If none of the modified elements satisfies the condition in Step (a), return `FAIL`.

Remark 4.4: It looks difficult to mix strategies by computing part of U_1 as in Algorithm 3.1 when Algorithm 4.3 fails: computing U explicitly is out of the question when S is huge. On the other hand, one can fix a much smaller set S' and find multiplicative generators (u_i) for the S'-units which are congruent to 1 (mod v) by the methods of §5.3. We keep only those which are included in U_1, according to

the above test; when S contains all primes less than some large bound, the u_i will all pass the test, since their T_2-norm will be small enough. After taking logarithmic embeddings of F into $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$, we can use one of the grid reduction algorithms in §4.1 to find exponents (n_i) such that $y := x \prod u_i^{n_i}$ has small T_2-norm. Now Step (a) can be applied to y. This procedure is a more sophisticated version of Step (b). In practice, Step (b) is sufficient as it stands.

4.3. **Constructing the set C.** We want to find a complete system of representatives C of k^* in $U \cap \mathcal{O}_F$, whose elements have minimal T_2-norm.

A theorem of Skałba [42, GTT] asserts that, provided $Nv > (\frac{4}{\pi^2})^{r_2}|\Delta|$ *and we allow denominators in* C, it is possible to find such representatives with numerators and denominators both $O((|\Delta|Nv)^{1/2n})$, where the O constant depends at most on the degree $n := [F : \mathbb{Q}]$. This situation will be considered in §4.4. In the current section, we insist on $C \subset \mathcal{O}_F$.

For all $e \in k^*$, we want to find a small $x \in U \cap \mathcal{O}_F$ such that $\beta(x) = e$, i.e., such that x belongs to the grid $\varepsilon + v$, where $\varepsilon \in U \cap \mathcal{O}_F$ is any representative of e, and the ideal v is regarded as a lattice. We use the last algorithm of §4.1 and take $x = \varepsilon - P\lceil P^{-1}\varepsilon \rfloor$, where the columns of P give a reduced basis (p_i) of the lattice v, in terms of a fixed integral basis. This is the fastest, but also the least efficient of the grid reduction algorithms in terms of the size of the element produced.

Note that, starting from a fixed reduced basis, the result does not depend on the chosen representative ε. Note also that if v is an inert rational odd prime and the chosen integral basis is LLL-reduced, then P is the diagonal matrix $p \cdot \mathrm{Id}$ and the procedure above simply picks the unique representative whose coordinates are all bounded by $(p-1)/2$. This produces the same set C for inert primes as in Browkin's procedure for the imaginary quadratic case, and possibly slightly worse ones in the non-inert cases, where he uses a much slower exhaustive enumeration.

If the resulting bound is not satisfactory, we can check whether the other two grid reduction algorithms produce better representatives. We obtain the following algorithm:

Algorithm 4.5:
Input: a finite place v. The values $m(G)$ and $m(W)$ from Algorithm 4.7 and §4.6 respectively. The set $\mu(F)$ of roots of unity belonging to F.
Output: a suitable bound for $m(C)$ such that (T1′) and (T2′) are both satisfied. Or return `FAIL` (v is a bad prime).

(a) Compute the maximum allowed norm for elements in C if (T1′) and (T2′) are to be satisfied: $\texttt{MAX} := \min(Nv/(m(G)+1),\ Nv - m(W))$.
(b) Compute a reduced basis for v (with respect to T_2), given by a matrix L on a fixed integral basis. Compute L^{-1}.
(c) For each element γ of $k^*/\beta(\mu(F))$, pick a representative $\varepsilon \in \mathcal{O}_F$. We try to find

$$x_\varepsilon \in U \quad \text{such that} \quad \beta(x_\varepsilon) = \gamma \quad \text{and} \quad \|x_\varepsilon\| < \texttt{MAX} \tag{5}$$

using the increasingly complicated possibilities below. As soon as one of the elements produced satisfies (5), we start over from (c) with the next γ.
- Compute $x_\varepsilon := \varepsilon - L\lceil L^{-1}\varepsilon \rfloor$.
- Check the neighbouring points: try all other possible rounding combinations (2 in each coordinate, 2^n possibilities in total).
- Try again to find a suitable x_ε using the second algorithm in §4.1.
- Using the Fincke-Pohst algorithm, compute the smallest elements which are congruent to $\varepsilon \pmod v$ and of norm less than `MAX` until one of them lies in U. If such an element does not exist, return `FAIL`.

Of course, once a representative x for ε is known, ξx is an equally good representative for $\xi\varepsilon$, for any root of unity ξ, since $\|\xi x\| = \|x\|$. This justifies our choice to check orbits modulo $\mu(F)$ in Step (c).

The last possibility in the algorithm, using exhaustive enumeration as a last chance, should probably be avoided as soon as v gets large, since it is less costly to check (T2) elementwise first. Given our experiments, it is not yet clear where the cutoff point should lie. For imaginary quadratic fields, the exhaustive search is rarely needed and relatively cheap; it pays off to always include it. In any case, constructing C in this way is by far the longest part of the algorithm, and becomes the main bottleneck as $|\Delta|$ increases.

Remark 4.6: We tried the following sphere packing approach in order to cover $k(v)^*$ while checking a minimal number of elements:

- find a few "evenly spaced" elements in $k(v)^*$, lifting to small elements of U.
- define balls in $\mathcal{O}_F$ centered at those lifts such that
  (a) their radius is small enough to guarantee that their interior points belong to U,
  (b) their radius is large enough for the projections of the balls to $k(v)^*$ to cover it entirely.

Unfortunately, we could not fulfill condition (a), so that we still needed to check that $x \in U$ for most individual interior points x in any given ball, which is the most time-consuming part in Algorithm 4.5. More precisely, if c is the center of a ball containing x, even though $\|x\|$ is close to $\|c\|$ by the triangle inequality, such size bounds are in general insufficient to ensure that x belongs to U. For instance, if $x \in \mathcal{O}_F$ and $\|x\| < Nv^{1/n}$, then $x \in U$, but this condition is far too restrictive.

4.4. **A set C with denominators.** If we allow denominators in C, we can expect to improve the bounds, but the conditions (T1) and (T2) need to be modified. Assume that C can be written as $\left\{\frac{c_1}{c_2}, c_i \in U \cap \mathcal{O}_F\right\}$; this will be case for the sets we construct, and is automatic for any subset of U when S contains a set of generators for the class group. Now define

$$m_i(C) = \max_{\frac{c_1}{c_2} \in C} \|c_i\|, \quad i = 1, 2.$$

Note that this depends on the particular representatives chosen; we want them to be as small as possible, of course.

The more general conditions we need to check are:

$$\begin{array}{lrcl} (\mathrm{T1}'') & m(W)m_2(C) + m_1(C) & < & Nv, \\ (\mathrm{T2}'') & m_1(C)m_2(C)(m(G)+1) & < & Nv. \end{array}$$

A similar idea as in the previous section can be applied, in a homogeneous setting this time. Given $a \in U$ we want to find x, y in $U \cap \mathcal{O}_F$ such that $c := x/y \equiv a \pmod{v}$, i.e., $x - ay \in v$. The points (x, y) satisfying this last property obviously form a sublattice of $\mathcal{O}_F \oplus \mathcal{O}_F$ which, in matrix form, can be written as

$$(x, y) \in \mathrm{Im} \begin{pmatrix} P & A \\ 0 & \mathrm{Id} \end{pmatrix}$$

on a fixed integral basis for the two copies of $\mathcal{O}_F$. In this expression, P denotes a set of generators of v and A is the matrix of the multiplication by a. Compute an LLL-reduced basis for this lattice with respect to the quadratic form $T_2 \oplus T_2$, and pick the smallest vector (x, y) in which $y \neq 0$ (there will be at least $[F : \mathbb{Q}]$ of them). One can expect both $\|x\|$ and $\|y\|$ to be small.

The bounds $m_1(C)$ and $m_2(C)$ play a symmetrical role in (T2″), not so in (T1″). So we should allow $m_1(C)$ to be a bit larger than $m_2(C)$ (by a factor of $m(W)$),

assuming their product more or less remains constant. To achieve this effect one can reduce with respect to $T_2 \oplus NT_2$, for a suitable integer N.

At present, the practical usefulness of this algorithm is not clear: bad primes are so easily refined that we are yet to find an example where adding denominators would make a difference.

4.5. **The set G.** The goal is to find a set G of small representatives in $U \cap \mathcal{O}_F$ of multiplicative generators of k^*. To verify (3) or (T2′), we only need to determine $m(G)$. But if the inequality is violated, and we want to check (T2) elementwise, we need an explicit subset, preferably minimal with respect to the required property.

Given a subset of k^*, the order of the subgroup it generates is the lcm of the orders of the individual elements. Assuming the factorization of $Nv-1$ is known, the classical algorithm (computing local orders for all primes dividing $Nv-1$) computes the individual orders quite efficiently.

Computing $m(G)$ is straightforward, and is very quick assuming that k^* can be generated by small elements:

Algorithm 4.7:
Input: S and v. A set $\mathcal{A}$ containing representatives in $\mathcal{O}_F$ of all elements in $(\mathcal{O}_F - \{0\})/\mu(F)$ of small T_2-norm (about 100 or 200 of them, say), ordered by increasing norm.
Output: the bound $m(G)$.

(a) Set $L = 1$. Factor $|k^*| = Nv - 1$.
(b) For each element a of $\mathcal{A}$
- Compute the order n of $\beta(a)$ (set $n = 0$ if $\beta(a) = 0$).
- Compute $L' = \mathrm{lcm}(n, L)$. If $L' > L$ and $a \in U$, set $L = L'$.
- If $L = Nv - 1$, return $\|a\|$.

(c) We have exhausted $\mathcal{A}$ and $\beta(\mathcal{A})$ does not generate k^*. Double the size of $\mathcal{A}$ and restart the previous step with the appended elements.

Proof. Obvious, since in a cyclic group the order of the subgroup generated by two elements is the lcm of their orders. We check that $a \in U$ before letting L increase, since we need $G \subset U$. □

To compute a minimal G, we need the following variant:

Algorithm 4.8:
Input: as above.
Output: the set G.

(a) Factor $Nv - 1$.
(b) Set $L = 1$ and $\mathcal{B} = \emptyset$.
(c) For each element a of $\mathcal{A}$
- Compute the order n of $\beta(a)$ (set $n = 0$ if $\beta(a) = 0$).
- Compute $L' = \mathrm{lcm}(n, L)$. If $L' > L$ and $a \in U$, append to $\mathcal{B}$ the triple $[a, n, L]$, then set $L = L'$.
- If $L = Nv - 1$, go to Step (e).

(d) $\beta(\mathcal{A})$ does not generate k^*. Double the size of $\mathcal{A}$ and restart the previous step with the appended elements.
(e) Set $L' = 1$ and $G = \emptyset$.
(f) For each element $[a, n, L]$ of $\mathcal{B}$, starting from the last one, if $\mathrm{lcm}(L', L) \neq Nv - 1$, then set $L' = \mathrm{lcm}(L', n)$ and append a to G. If $L' = Nv - 1$, return G.

Proof. In Step (f), L is the order of the subgroup of all the elements occurring before a (excluded) in $\mathcal{B}$, and L' is the order of the subgroup generated by the

elements lying in G at this point. If the lcm of L and L' is equal to the group order, then $\langle\, \beta(\mathcal{B}-\{a\})\,\rangle = \langle\, \beta(\mathcal{B})\,\rangle = k^*$. Otherwise, $\mathcal{B}-\{a\}$ generates a proper subgroup, hence a needs to be included. □

Note that, although $m(G)$ is well defined and best possible, G depends on the representatives chosen in $\mathcal{A}$. When checking (T2) elementwise, some sets G may succeed where others fail. We do not know how to cater for that phenomenon, which remains theoretical, except by retrying the procedure with a few different G (there are finitely many possible G, if one keeps the optimal sequence of T_2-norms).

4.6. **The set W.** This is computed as in Browkin [7, 3.2]. We assume that $|S|$ is big enough, so that $\mathcal{O}_S$ is principal. Let Q be a set of representatives of small norm, supported on S, representing all the ideal classes of $\mathcal{O}_F$. This is easily produced from arbitrary representatives by applying Buchmann's ideal reduction [11, Chapter 6], which coincides with Gauss's reduction theory of binary forms in the quadratic setting. By definition, q_F is bounded by $\max_{\mathfrak{q}\in Q} N\mathfrak{q}$.

Since $\mathcal{O}_S$ is principal, one can take W to be given by the union of a set of generators of the units and a set of generators of the principal ideals of $\mathcal{O}_F$ of one of the following forms [7, 3.2]

$$\begin{array}{ll}(i) & (a)=\mathfrak{p}\mathfrak{q},\\ (ii) & (a)=\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3,\end{array}$$

where $\mathfrak{p}\in S$ and $\mathfrak{q}$, $\mathfrak{q}_1$, $\mathfrak{q}_2$, $\mathfrak{q}_3\in Q$. Given a suitable ideal, the principal ideal algorithm (see [11]) will yield a generator of small T_2-norm (this is important when there are fundamental units).

Note that only generators of type (i) depend on S. Obviously, if one needs to compute W for a given S, the values of the T_2-norm of the generators of this type can be stored in an array, indexed by the corresponding $\mathfrak{p}$. Then $m(W)$ can be trivially computed for any subset of S simply by deleting some norms before taking the maximum. Since this construction is applied to sets S of the form $\{v, Nv<B\}$ for a given bound B, the set W in fact needs to be computed only once.

Remark 4.9: Although, as we have seen, W is particularly easy to compute, it is even nicer in the imaginary quadratic setting where $\|a\|=\sqrt{Na}$. For any ideal I, denote by I' the reduced ideal (in the sense of Gauss) which is equivalent to I. In that case, for generators of type (i), we can take $\mathfrak{q}=(\mathfrak{p}^{-1})'$, and $N\mathfrak{q}=N((\mathfrak{p}^{-1})')=N(\mathfrak{p}')$. Hence, $\|a\|=\sqrt{N\mathfrak{p}N(\mathfrak{p}')}$ is obtained without computing the actual element. The same technique applies to the other type of generators.

5. Creating the relation matrix

5.1. **Representing symbols.** We fix a set S of finite places in F such that $K_2\mathcal{O}_F$ is contained in $K_2^S(F)$, and assume that we have already computed a basis $(\omega_i)_{1\le i\le r}$ for the S-units, where $r:=r_S:=|S|+r_1+r_2$, and ω_1 generates $\mu(F)$. In order to encode a representative $a\otimes b\in U_S\otimes U_S$ for the symbol $\{a,b\}\in K_2F$, we decompose

$$a=\prod\omega_i^{\alpha_i},\quad\text{and}\quad b=\prod\omega_i^{\beta_i}$$

on the above basis, and associate to $a\otimes b$ the vector $(\alpha_i\beta_j)_{1\le i,j\le r}$.

Due to the antisymmetry of symbols in K_2F, we will in fact work in the quotient of $U_S\otimes U_S$ by the symmetric tensors $\{x\otimes y+y\otimes x : x,y\in U_S\}$, and the corresponding representation becomes $(\alpha_i\beta_i \pmod 2)_{1\le i\le r}\oplus(\alpha_i\beta_j-\alpha_j\beta_i)_{1\le i<j\le r}$, thus cutting the dimension roughly in half. Note that $\{x,x\}$ is 2-torsion, hence the reduction mod 2 in the first factor.

5.2. **Producing relations.** Our goal is to minimize the index of the lattice in $U_S \otimes U_S$, spanned by vectors arising from relations among symbols. For that, we generate many relations of the form $u \otimes (1-u)$, $u \in U_S$. Although it is not guaranteed that this should be enough to generate all relations (in principle, we should consider all $u \in F - \{0,1\}$), it turns out to be sufficient in practice. All such relations can be factored on our basis $(\omega_i \otimes \omega_j)_{i,j}$ and encoded as above.

The relations $x \otimes (1-x)$ for $x \in F - \{0,1\}$ induce the following *trivial relations*: $\omega_i \otimes (-\omega_i)$, $(\omega_i \otimes \omega_i)^2$, and $(\omega_1 \otimes \omega_i)^w$, where w is the order of $\mu(F)$.

Furthermore we increase the lattice of relations by producing a list L of S-units and considering all pairs $(u,u') \in L^2$, whose difference $u-u'$ is again an S-unit, producing the new relation $(u'/u) \otimes (1-(u'/u))$.

Unfortunately, we are lacking a good stopping criterion that would tell us that the lattice of relations Λ is complete, so we decide to terminate the algorithm when its index stabilizes. Although we believe that $\widetilde{K}_2^S(F) := (U_S \otimes U_S)/\Lambda$ is equal to $K_2^S(F)$, we have no way of proving it at this point. We will see in the next section how to combine the information obtained so far with theoretical results, in order to prove this claim.

Algorithm 5.1:
Input: a set S of primes in F, a basis (ω_i) for the S-units.
Output: a lattice of full rank in $U_S \otimes U_S$ formed from some $x \otimes (1-x)$, with index believed to be minimal.

(a) Set Λ to be the lattice generated by the trivial relations as above.
(b) Collect a set L of integral S-units with bounded coefficients on a fixed LLL-reduced integer basis, then add to L all $\prod w_i^{e_i}$ for bounded e_i.
(c) Check pairs $(u,u') \in L^2$ until $u-u' \in U_S$; then go to Step (d). If there are no pairs left, go to Step (e).
(d) Replace Λ by the lattice generated by Λ and the relation corresponding to $(u'/u) \otimes (1-(u'/u))$. If the index of Λ is not ∞ and stayed the same for, say, 100 consecutive pairs, return Λ and terminate the algorithm. Otherwise go to Step (c) for the next pair.
(e) If $[U_S \otimes U_S \colon \Lambda] \neq \infty$, issue a warning message stating that Λ may not be complete, then return Λ. Otherwise collect more elements in L and go to Step (c). If no more elements could be collected, increase S and start over in Step (a).

5.3. **The final step.** In this subsection, we are given an explicit presentation of a finite group $\widetilde{K}_2^S(F)$ such that $K_2^S(F)$ is a quotient of $\widetilde{K}_2^S(F)$ (and where we believe that in fact $K_2^S(F) = \widetilde{K}_2^S(F)$). In other words, by factoring enough Steinberg tensors $x \otimes (1-x)$ in U_S, we have been able to build a relation lattice Λ of maximal rank in $U_S \otimes U_S$. We know furthermore that $K_2\mathcal{O}_F$ is the intersection of the kernels of the ∂_v, $v \in S$.

This is easily computed once the problem is linearized (see Step (c) below). We pick $\mathcal{B} = \{b_t\}$ a set of elements in $U_S \otimes U_S$ that generate $K_2^S(F)$, for instance the $(\omega_i \otimes \omega_j)_{i \leq j}$ from the previous section; we have a natural projection from the free abelian group $\mathbb{Z}[\mathcal{B}]$ to $K_2^S(F)$. Given a lattice $C \subset \mathbb{Z}[\mathcal{B}]$, we choose generators and a matrix M_C expressing them in terms of the basis $\mathcal{B}$.

Algorithm 5.2:
Input: a lattice Λ as above.
Output: a presentation for a finite abelian group $\widetilde{K_2\mathcal{O}_F}$, of which $K_2\mathcal{O}_F$ is a quotient.

(a) For all $v \in S$, choose a generator g_v of the cyclic group $k(v)^*$. Since Nv is very small, this and the discrete logarithm problem in the next step are best done by trial and error.

(b) For all (v,t), compute $n_{v,t} \in \mathbb{Z}/(Nv-1)\mathbb{Z}$ such that $\partial_v(b_t) = g_v^{n_{v,t}}$.
(c) Compute the kernel $\operatorname{Ker} d$ of the linear map

$$\begin{aligned} d : \mathbb{Z}[\mathcal{B}] &\longrightarrow \bigoplus_{v\in S} \mathbb{Z}/(Nv-1)\mathbb{Z} \\ [b_t] &\mapsto (n_{v,t}). \end{aligned}$$

This is done by computing the integer kernel of the matrix

$$\Big((n_{v,t})_{v,t} \mid \mathsf{Diag}(Nv-1)_v\Big).$$

By definition, the elements of $\operatorname{Ker} d$ span $K_2\mathcal{O}_F$.
(d) Compute $\widetilde{K_2}\mathcal{O}_F := \operatorname{Ker} d/(\operatorname{Ker} d \cap \Lambda)$ by taking the integer kernel of the block matrix $(M_{\operatorname{Ker} d} \mid M_\Lambda)$. Let $\binom{Y}{Z}$ be the kernel, then $M_{\operatorname{Ker} d}Y$, or equivalently $M_\Lambda Z$, generates the intersection. Hence Y is a matrix of relations among the generators of $K_2\mathcal{O}_F$, and the SNF of Y computes the elementary divisors of $\widetilde{K_2}\mathcal{O}_F$. It is straightforward to extract explicit tensors that generate the cyclic components from the SNF algorithm.

Remark 5.3: (a) In general, most entries on the diagonal of the HNF of the relation matrix M_Λ for $K_2^S(F)$ will be equal to 1. In other words, the corresponding generator can be expressed in terms of the other ones. Obviously, one should not include these redundant tensors in $\mathcal{B}$ above, which we can make much smaller than the full set $(\omega_i \otimes \omega_j)_{i\le j}$.

(b) Since we realize an explicit isomorphism $\widetilde{K_2}\mathcal{O}_F \simeq \mathbb{Z}[\mathcal{B}]/Y$, it is now possible to compute in $\widetilde{K_2}\mathcal{O}_F$. A tame element in $U_S \otimes U_S$ is mapped to $\mathbb{Z}[\mathcal{B}]$, via factorization in U_S; hence a product in $\widetilde{K_2}\mathcal{O}_F$ reduces to an addition in $\mathbb{Z}[\mathcal{B}]$ and a reduction modulo Y. Until we ascertain that $\widetilde{K_2}\mathcal{O}_F = K_2\mathcal{O}_F$, we still cannot really compute in $K_2\mathcal{O}_F$ since we do not even have a test for equality between two symbols there. Of course, once we know $\widetilde{K_2}\mathcal{O}_F = K_2\mathcal{O}_F$, it is enough to check that their quotient, mapped to $\mathbb{Z}[\mathcal{B}]$, lies in the image of Y.

Algorithm 5.2 further provides enough data to partly solve the discrete logarithm problem in $K_2\mathcal{O}_F$. We can express any tame element in $U_S \otimes U_S$ as a product P of generators for $\widetilde{K_2}\mathcal{O}_F$ computed above, by first factoring it on the $\omega_i \otimes \omega_j$, then expressing it in terms of generators of $\operatorname{Ker} d$. By keeping track of all base change matrices involved, the original element is given as a product of explicit trivial Steinberg tensors $x \otimes (1-x)$ multiplied by P. If we start from an arbitrary element in $F^* \otimes F^*$, Tate's method from §3 can in principle reduce it to $U_S \otimes U_S$, up to explicit trivial tensors. But it is not really practical if the support of the tensor is much larger than S.

(c) In the class group case, an arbitrary ideal I can be factored on the factor base by multiplying I by random products of elements in the factor base, until the reduction of I along some direction is smooth (see [11, Chapter 6]). The ideal I can then be factored on the factor base up to an explicit principal ideal, of which a generator is known. Unfortunately, we could not devise an analog to Buchmann's reduction in the K_2 setting.

6. The p-rank of $K_2\mathcal{O}_F$

From the previous sections, we can exhibit an explicit presentation of some finite abelian group, denoted $\widetilde{K_2}\mathcal{O}_F$, of which $K_2\mathcal{O}_F$ is a quotient. In other words, we know how to produce a list of explicit generators for $K_2\mathcal{O}_F$ as well as, for each of them, a multiple of its order. We also believe that these generators are independent

and that the bound is in fact equal to their true order. We will now investigate various ways that can be used to actually prove that $\widetilde{K_2}\mathcal{O}_F = K_2\mathcal{O}_F$.

6.1. **The wild kernel.** One trivial case occurs when $\widetilde{K_2}\mathcal{O}_F = 0$, which implies that the tame kernel is also trivial. Unfortunately, this occurs quite rarely. However, it is possible to do better by introducing the *wild kernel*, which is the non-trivial part of $K_2\mathcal{O}_F$, and which we will now define.

For a field E, let $\mu(E)$ be the group of roots of unity in the field. Let $\mathbb{P}_F$ the set of finite and real places of F, F_v the completion of F at $v \in \mathbb{P}_F$. We let $m := |\mu(F)|$, and $m_v := |\mu(F_v)|$ for $v \in \mathbb{P}_F$; for v dividing the rational prime p, we let $m_v^1 := |\mu^1(F_v)|$ where $\mu^1(F_v)$ is the Sylow p-subgroup of $\mu(F_v)$.

One defines the *wild kernel* WK_2F analogously to $K_2\mathcal{O}_F$, replacing the tame symbols

$$\partial_v : K_2F \longrightarrow k(v)^* \simeq \mu(F_v)/\mu^1(F_v)$$

by Hilbert's norm residue symbols

$$(\cdot,\cdot)_v : K_2F \longrightarrow \mu(F_v),$$

where $(a,b)_v$ is $\left(\frac{a,b}{v}\right)_{m_v}$, the norm residue symbol of order m_v. By definition, $WK_2F := \bigcap \mathrm{Ker}(\cdot,\cdot)_v$ where v runs through $\mathbb{P}_F$.

We have $\partial_v = (\cdot,\cdot)_v^{m_v^1}$ (cf. [16, 5.3]), hence WK_2F is a subgroup of $K_2\mathcal{O}_F$. The quotient $K_2\mathcal{O}_F/\,WK_2F$ can in principle be determined by coupling Moore's exact sequence [31] and the localization sequence (see e.g., Browkin [5], Gras [19, Section 1]). In particular one obtains

$$i_F := [K_2\mathcal{O}_F : WK_2F] = \frac{2^{r_1}}{m}\prod_v m_v^1 \tag{6}$$

where v runs through the finite places of F, and r_1 is the number of real places of F. Note that if $\mu_{p^r} \subset F_v$ then

$$p^{r-1}(p-1) \le e(v/p) \le [F_v : \mathbb{Q}] \le [F : \mathbb{Q}]; \tag{7}$$

indeed, $\mathbb{Q}_p(\zeta_{p^r})$ is totally ramified of degree $p^{r-1}(p-1)$. Hence only small primary factors may divide i_F. To compute $\mu^1(F_v)$, note that $\mu_{p^r} \subset F_v$ if and only if the cyclotomic polynomial Φ_{p^r} has a root in F_v, which is easy to decide by lifting roots modulo v^k, increasing k until Hensel's criterion can be applied. For F quadratic, or a cyclotomic field of prime order, (6) is made completely explicit in [5].

So i_F is easily computable, and whenever $|\widetilde{K_2}\mathcal{O}_F| = i_F$ we obtain a proof that $\widetilde{K_2}\mathcal{O}_F = K_2\mathcal{O}_F$. Of course, this can only happen when $WK_2F = 0$, but this is a less severe restriction than $K_2\mathcal{O}_F = 0$. In fact, it occurs quite frequently.

6.2. **Local norm symbols and Brauer groups.** If we believe that $WK_2F \neq 0$, it is a natural idea to try and exploit the explicit symbols that our algorithm provides by mapping them to a more manageable group G, via some morphism $\varphi : K_2\mathcal{O}_F \to G$ which we would like to be as close to an isomorphism as possible. Namely, suppose $\{a,b\} \in K_2\mathcal{O}_F$ is n-torsion in $\widetilde{K_2}\mathcal{O}_F$; if $\varphi(\{a,b\})$ has order n, which is easily checked if we can test for 0 in G and factor n, then so has the symbol $\{a,b\}$ in $K_2\mathcal{O}_F$.

If E contains a primitive n-th root of unity ζ_n, one classically defines a map to the Brauer group of E:

$$K_2(E)/nK_2(E) \to \mathrm{Br}(E)$$

(which is in fact an isomorphism onto the n-torsion of $\mathrm{Br}(E)$ by a deep theorem of Tate [45]) by associating to $\{a,b\}$ the algebra $[a,b]_{\zeta_n}$ generated by two elements x

and y over E subject to the relations

$$x^n = a, \quad y^n = b, \quad yx = \zeta_n xy,$$

see e.g., [30]. This element is trivial (i.e., is isomorphic to the matrix algebra $M_n(E)$) if and only if a is a norm from the extension $E(b^{1/n})/E$. By letting $E := F(\zeta_n)$, one can consider the composite map

$$K_2\mathcal{O}_F/nK_2\mathcal{O}_F \to K_2(E)/nK_2(E) \to \mathrm{Br}(E)$$

which is unfortunately not an isomorphism anymore. We then try to prove that a is *not* a norm in $E(b^{1/n})/E$, which would show that $\{a, b\} \neq 0$ in $K_2\mathcal{O}_F$. The extension is cyclic, so the Hasse principle applies and to show a is not a global norm in this extension reduces to showing that there exists a place $\wp$ in $\mathbb{P}_E$ such that a is not a local norm at $\wp$.

A slight variation on the above formulation would be to use an embedding $\mathcal{O}_F \subset F \subset E \subset E_\wp$ in order to map $K_2\mathcal{O}_F$ to $K_2(E_\wp)/pK_2(E_\wp)$ (where $\wp \mid p$, otherwise the image will be trivial). The latter is a cyclic group of order p (cf. [16, IX.4]) where explicit computations can be easily done, and we can check whether the image of $\{a, b\}$ is non-trivial there. This is essentially equivalent to the computation of the norm residue symbol $(a, b)_\wp$ (see Daberkow [13]) and stands no better chance of success, except that it provides a neat way to compute the said symbol.

Unfortunately, these localization maps will not detect anything new: they are trivial on the wild kernel. To see this, we invoke the following well-known proposition, whose proof (explained to us by J.-L. Colliot-Thélène) we include here, since we could not find it explicitly in the literature:

Proposition 6.1. *If E/F is an extension of number fields, then the natural map $K_2F \to K_2E$ maps WK_2F to WK_2E.*

Proof. For any local field k, Moore proved that the kernel of the Hilbert symbol $K_2k \to \mu(k)$ is an infinitely divisible group (see Milnor [30, Appendix A]).

Let E_w/F_v be the extension of local fields corresponding to a non-complex place w of E, above v in F. If $\{a, b\} \in K_2F_v$ is in the kernel of the Hilbert symbol associated to v, it is an n-th power for any $n > 0$, in particular a $|\mu(E_w)|$-th power. Hence it lands in the kernel of $(\cdot, \cdot)_w : K_2E_w \to \mu(E_w)$. If w is complex, the Hilbert symbol is trivial by definition. The result follows. □

It was also pointed out to us independently by C. Movahhedi and K. Hutchinson that this result can be seen quite explicitly from Moore's sequence:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & WK_2E & \longrightarrow & K_2E & \longrightarrow & \bigoplus_{w\in\mathbb{P}_E} \mu(E_w) & \longrightarrow & \mu(E) \longrightarrow 1 \\
 & & \uparrow f & & \uparrow & & \uparrow g & & \\
1 & \longrightarrow & WK_2F & \longrightarrow & K_2F & \longrightarrow & \bigoplus_{v\in\mathbb{P}_F} \mu(F_v) & \longrightarrow & \mu(F) \longrightarrow 1
\end{array}$$

where the existence of the map $f : WK_2F \to WK_2E$ follows from the existence of g which is constructed in Ryan [40, §1.3].

6.3. **Miscellaneous explicit results.** We recall here a few explicit results appearing in the literature, about the Sylow p-subgroup of $K_2\mathcal{O}_F$, which can help prove (or disprove) that $\widetilde{K_2}\mathcal{O}_F = K_2\mathcal{O}_F$.

For any number field F, the 2-rank of $K_2\mathcal{O}_F$ is known in terms of 2-class groups by work of Tate [45] (see also Browkin-Schinzel [9]) and an explicit basis for $K_2\mathcal{O}_F \otimes \mu_2$ is given by Browkin [5].

Let now F be a quadratic field of discriminant Δ.

(a) For $\Delta > 0$, the order of $K_2\mathcal{O}_F$ is known from the Birch-Tate conjecture.
(b) When $-35 \leq \Delta < 0$, the group $K_2\mathcal{O}_F$ is known precisely (Tate [44], Skałba [42], Qin [34, 36], Browkin [7]), and in fact is either trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$, generated by $\{-1,-1\}$.
(c) The most comprehensive and rather explicit results on the 4-rank (resp. 8-rank) are given by Qin [35, 37] who covers the case where Δ is divisible by ≤ 3 different (resp. one) odd prime numbers (for other results on the 8-rank, cf. Vazzana [46]).
(d) Browkin [6] uses reflection theorems (and Keune's result from the next section) to work out inequalities between the p-rank of $K_2\mathcal{O}_F$ and the p-rank of class groups of related fields (explicit examples are given for $p = 3, 5$), proving some of the conjectures in [17].

6.4. **Keune's exact sequences.** The correct generalization of these ideas is due to Tate [45] and Keune [25], and affords a complete solution to our problem *assuming* we can compute certain class groups. We quote Keune's formulation:

Theorem 6.1. [25, (5.3), (5.4), (6.6)] *Let F be a number field, p^r an odd prime power, $E := F(\zeta_{p^r})$ and $\Gamma = \mathrm{Gal}(E/F)$. Let $\mathcal{O}_{E,p}$ be the ring of S-integers in E, where S is the set of places of E dividing p. We have the following short exact sequences of Γ-modules:*

• *if $E = F$,*

$$1 \longrightarrow \mu_p \otimes \mathrm{Cl}(\mathcal{O}_{E,p}) \xrightarrow{\iota} K_2\mathcal{O}_F/p \longrightarrow \bigoplus_{\substack{v\mid p\\ v\subset\mathcal{O}_F}} \mu_p \longrightarrow \mu_p \to 1$$

• *if $E = F(\zeta_p)$ and $E \neq F$,*

$$1 \longrightarrow (\mu_p \otimes \mathrm{Cl}(\mathcal{O}_{E,p}))^{\Gamma} \xrightarrow{\iota} K_2\mathcal{O}_F/p \longrightarrow \bigoplus_{\substack{v\mid p\\ v\subset\mathcal{O}_F}} \mu_p(F_v) \longrightarrow 1$$

• *if p^r kills the p-primary part of $K_2\mathcal{O}_F$ and μ_{p^r} contains the p-primary part of $\mu(F_\wp)$ for all $\wp \mid p$,*

$$1 \longrightarrow (\mu_{p^r} \otimes \mathrm{Cl}(\mathcal{O}_{E,p}))_{\Gamma} \xrightarrow{\iota} WK_2F \otimes \mathbb{Z}_p \longrightarrow 1$$

In these statements, μ_{p^i} is the Galois module $\mu_{p^i}(E)$, and the Galois action on $\mu \otimes \mathrm{Cl}$ is diagonal, given by $(\zeta \otimes I)^\sigma := \zeta^\sigma \otimes I^\sigma$. Here, Γ is cyclic generated by σ, A^Γ denotes the invariants $\{a \in A, a^\sigma = a\}$, and A_Γ the coinvariants $A/A^{1-\sigma}$. The map ι sends $\zeta_p \otimes I$ to $\mathrm{Tr}_{E/F}\, x^p$, where $x \in K_2(E)$ satisfies $\partial_v(x) \equiv \zeta^{v_\wp(I)} \pmod{\wp}$ for all $\wp$ not dividing p, and $\mathrm{Tr}_{E/F} : K_2(E) \to K_2(F)$ denotes the transfer map.

Remark 6.2: (a) The statements in the theorem have to be slightly modified when $p = 2$. Most importantly, F has to be replaced by $F(i)$ ($F(\sqrt{2})$ would also do). One then applies [25, 6.2] to go back from $K_2\mathcal{O}_{F(i)}$ to $K_2\mathcal{O}_F$.
(b) The Galois action is trivial to compute by the very construction of E as $F(\zeta_p)$: σ acts trivially on F and sends ζ_p to ζ_p^g for a given primitive element $g \in \mathbb{F}_p^*$, which we fix from now on. Computing the required invariants and coinvariants translates to simple linear algebra over $\mathbb{F}_p$ once generators and relations for $\mathrm{Cl}(\mathcal{O}_{E,p})$ are known. The latter is isomorphic to the quotient of the class group of E by the subgroup generated by the places of E dividing p. If the class group of E is known algorithmically, including the solution to the discrete logarithm problem, $\mathrm{Cl}(\mathcal{O}_{E,p})$ is easily computed (see [12, Chapter 7]).
(c) In order to evaluate $\iota(\zeta_p \otimes I) := \mathrm{Tr}_{E/F}(x^p)$, we can choose an x via the approximation theorem and the transfer $\mathrm{Tr}_{E/F}$ is easily computed uniquely in terms of symbols (see [2, p. 382] and [39]). If the set S we choose when

computing $\widetilde{K_2}\mathcal{O}_F$ is large enough, these symbols factor on $(\omega_i \otimes \omega_j)$, cf. §5.2, and we can map the resulting product of symbols to $\widetilde{K_2}\mathcal{O}_F$. Reducing modulo the HNF basis for the relation module Λ (cf. §5.2), we obtain simple generators for the Sylow p-subgroup of $K_2\mathcal{O}_F$.

(d) Remarkably, while our previous method based on relation finding was computing $K_2\mathcal{O}_F$ "from above", the map ι provides a way to compute it "from below" by computing its p-primary parts for a few small p. Since the required class groups can only be computed when p^r is very small, this method also fails to give a complete algorithmic answer. In the next section, we shall see that the practical situation is still rather satisfactory.

Keune's theorem is used as follows: let $q = p^r = \max(\tilde{e}, \max e_\wp)$, where $\tilde{e}$ is the exponent of the Sylow p-subgroup of our conjectural $\widetilde{K_2}\mathcal{O}_F$, and $e_\wp$ is the exponent of the Sylow p-subgroup of $\mu(F_\wp)$, where $\wp \mid p$. Since $K_2\mathcal{O}_F$ is a quotient of $\widetilde{K_2}\mathcal{O}_F$, q also kills the p-primary part of $K_2\mathcal{O}_F$.

Provided we can compute the class groups of $F(\zeta_q)$, for all q as above, we obtain $|WK_2F|$ from Keune's isomorphism, from which we deduce $|K_2\mathcal{O}_F|$ using (6). Note that, from (7), $e_\wp \leq [F:\mathbb{Q}]/(1-1/p) \leq 2[F:\mathbb{Q}]$ is small, and $\tilde{e}$ divides a fixed integer (the exponent of $\widetilde{K_2}\mathcal{O}_F$). Hence few different q need to be considered.

If $|\widetilde{K_2}\mathcal{O}_F| = |K_2\mathcal{O}_F|$, then these two groups are equal. In particular, we have proven the non-triviality of our generating elements, although in a roundabout way. Otherwise, we now know the exact order of $K_2\mathcal{O}_F$ and we look for more relations until the required index is obtained.

In the unfortunate case that $q = p^r$ is so large that $\mathrm{Cl}(\mathcal{O}_{F(\zeta_q)})$ cannot be computed, we still obtain lower bounds on the order of our generating elements if $\mathrm{Cl}(\mathcal{O}_{F(\zeta_p)})$ can be computed. If p itself is large, nothing can be salvaged.

Finally it should be noted[6] that if $F(\zeta_{p^r})$ is a CM-field, the natural map from the maximal real subfield $\mathrm{Cl}(\mathcal{O}_{F(\zeta_{p^r})^+}) \to \mathrm{Cl}(\mathcal{O}_{F(\zeta_{p^r})})$ is injective on the p-th primary part for odd p (see Washington [47, Theorem 10.3]). Hence, the required invariant classes may be found in the maximal real subfield, in which case all computations can be done there. This is by no means a necessary condition, but it should be checked first, since class group computations will be much easier in this subfield of index 2 than in the full cyclotomic extension.

For instance when $F = \mathbb{Q}(\sqrt{-303})$ and $E = F(\zeta_{11})$, *assuming GRH*, PARI/GP succeeds in proving that $\mathrm{Cl}(\mathcal{O}_{E^+,11})$ contains a class of order 11, which can be represented by an ideal of norm 109×571. The latter is transformed in a suitable way under the Galois action, thereby proving that $r_{11}(K_2\mathcal{O}_F) \geq 1$. PARI could prove the same result working in $\mathrm{Cl}(\mathcal{O}_E)$, but the computations need 2 days (still assuming GRH), instead of 10 minutes. Certifying the result in order to remove the GRH assumption in the maximal real subfield takes another 3 days, and is not practical in the full cyclotomic extension.

Note that the first part of the algorithm proved that

$$K_2\mathcal{O}_F = \left\langle \{-17-3\omega, -37+\omega\}^5 \right\rangle$$

and has exponent 22, with $\omega = (1+\sqrt{-303})/2$. Since $r_2(K_2\mathcal{O}_F)$ is easily proven to be 1 in that case, we obtain an unconditional proof that the generator above indeed has order 22. This is consistent with the heuristic result obtained in [8] assuming the truth of Lichtenbaum's conjecture.

Using our partial solution to the discrete logarithm problem (cf. Remark 5.3.b), we can now compute in $K_2\mathcal{O}_F$: we can express any symbol with support in S in

[6]We are grateful to Jerzy Browkin and Thorsten Kleinjung for this remark.

terms of this initial generator. In this way, we produce nicer looking generators, for instance

$$\{3\omega + 17, 2\} = (\{-17 - 3\omega, -37 + \omega\}^5)^{17}.$$

(Deriving this identity without using a factor base is probably a tough exercise!)

Remark 6.3: Diaz y Diaz and Soriano [15] use the logarithmic class group $\widetilde{\mathrm{Cl}(F)}$ defined by Jaulent [24] to compute $WK_2F \otimes \mu_p \simeq \widetilde{\mathrm{Cl}(F)} \otimes \mu_p$, provided $\mu_{2p} \subset F$. As a prerequisite, their algorithm requires that $\mathrm{Cl}(F)$ be computed. Also, they assume that F is Galois, and $\widetilde{\mathrm{Cl}(F)}$ is finite (which is not known a priori; it follows from Gross's conjecture, hence is true if F is abelian).

We feel that, in order to compute $WK_2F \otimes \mu_p$, it is simpler to deduce it from $K_2\mathcal{O}_F \otimes \mu_p$, computed with the second exact sequence in Keune's theorem. The computational costs are about the same: in both cases, by far the most time-consuming part is the (unconditional) computation of $\mathrm{Cl}(F)$. But we can use standard class group calculators, and apply the algorithm to arbitrary number fields F, without assuming it is Galois or contains enough roots of unity (which is also possible with the Diaz y Diaz – Soriano approach, but requires further descent arguments).

Also, as we have seen, once the exponent of WK_2F is bounded (from the computation of $\widetilde{K_2}\mathcal{O}_F$ and, ultimately, Groenewegen's bound), Keune's theorem describes the full Sylow p-subgroup of WK_2F, not only its p-rank.

7. Tables

7.1. **Imaginary quadratic fields.** We have proven the correct structure of $K_2\mathcal{O}_F$ for all imaginary quadratic fields F of discriminant Δ, $|\Delta| < 1000$, with the exception of the 7 starred ones in the table below, for which the certification has not been attempted. The results coincide with the ones predicted in [8] by experimental methods (even for the 7 discriminants above). Computing times range from 1s to 1h per discriminant, *not* including the final certification when Keune's result is needed. More than 95% of that computing time is spent reducing Groenewegen's bound.

In all the tables, we list $d = |\Delta|$ where $\Delta < 0$ is the discriminant of the imaginary quadratic field $F = \mathbb{Q}(\sqrt{\Delta})$ and ω stands for $\sqrt{\Delta}/2$ (resp. $(1+\sqrt{\Delta})/2$) if Δ is even (resp. odd). When appropriate, we list $|K_2\mathcal{O}_F|$, the elementary divisors of $K_2\mathcal{O}_F$, and the corresponding generators. As output by the algorithm, the generators are simple products of symbols involving fundamental S-units for the small S obtained after reducing Groenewegen's bound. We have used our partial solution to the discrete logarithm problem to obtain "better looking" generators (for instance all 2-torsion symbols were written as $\{-1, a\}$, for some $a \in F^*$, with $a = -1$ whenever possible). Starred entries denote conjectural results, meaning that the true orders of the generators may divide the given ones.

Table of d with trivial $K_2\mathcal{O}_F$:

3	4	8	11	19	20	24	40	43	52	59	67	83	88
104	116	131	139	148	152	163	179	211	212	227	232	244	251
283	296	307	344	347	379	404	424	436	443	467	488	499	523
536	547	563	587	596	619	628	659	664	683	691	692	724	739
787	788	808	811	827	856	859	872	883	907	916	947		

Table of d with $K_2\mathcal{O}_F$ of order 2 generated by $\{-1, -1\}$:

7	15	23	31	35	47	55	56	71	79	87	91	95	103
115	127	143	151	155	159	167	168	184	191	199	203	215	223
235	239	247	248	259	263	271	276	280	295	299	308	311	312
319	335	355	359	371	376	383	395	403	407	415	427	431	439
440	447	463	487	515	519	532	535	551	559	564	568	591	599
607	611	616	631	632	635	647	655	667	671	695	707	719	727
728	743	744	751	760	763	767	807	815	823	824	839	851	852
871	888	895	899	911	919	920	923	951	955	967	983	991	995

Table of d with $K_2\mathcal{O}_F$ of order 2, where $\{-1,-1\}$ is trivial:

51	$\{-1,3\}$	123	$\{-1,3\}$
187	$\{-1,\omega-2\}$	267	$\{-1,3\}$
328	$\{-1,\omega-4\}$	339	$\{-1,8\omega+97\}$
340	$\{-1,5\}$	411	$\{-1,11\omega+51\}$
451	$\{-1,3\omega+13\}$	456	$\{-1,2\omega+13\}$
520	$\{-1,5\}$	584	$\{-1,41\omega+732\}$
680	$\{-1,2\omega-7\}$	699	$\{-1,133\omega+2517\}$
712	$\{-1,\omega-68\}$	779	$\{-1,7\omega-226\}$
803	$\{-1,1173\omega-3088\}$	843	$\{-1,3\}$

Table of d with $K_2\mathcal{O}_F$ of order >2:

39	6	6	$\{2,\omega+2\}$
68	8	8	$\{3,w+1\}^2$
84	6	6	$\{2,\omega-3\}^4$
107	3	3	$\{2,\omega-1\}^6$
111	6	6	$\{\omega-5,-6\omega-2\}$
119	4	2, 2	$\{-1,\omega-2\}$, $\{-1,-1\}$
120	6	6	$\{3,\omega-6\}^{10}$
132	4	4	$\{2,\omega+3\}^6$
136	4	4	$\{5,\omega+4\}^5$
164	4	4	$\{-\omega+11,3\}^2$
183	6	6	$\{2,\omega+14\}$
195	4	2, 2	$\{-1,-1\}$, $\{-1,5\}$
219	12	12	$\{5,\omega-1\}^{10}$
228	12	12	$\{3,\omega+9\}^{22}$
231	4	2, 2	$\{-1,-1\}$, $\{-1,\omega+2\}$
255	12	6, 2	$\{3,\omega-1\}$, $\{-1,-1\}$
260	4	4	$\{2,\omega+4\}$
264	6	6	$\{2,\omega-3\}^2$
287	4	2, 2	$\{-1,-1\}$, $\{-1,\omega-1\}$
291	12	12	$\{\omega+1,5\}^4$
292	4	4	$\{\omega-5,7\}^3$

303	22	22	$\{3\omega+17,2\}$
323	4	4	$\{2,\omega+26\}^{84}$
327	6	6	$\{2,7\omega+6\}$
331	3	3	$\{2,\omega+6\}^{12}$
356	4	4	$\{3,\omega+37\}^{2}$
367	6	6	$\{2,w-1\}^{11}$
388	8	8	$\{5,-\omega-48\}^{3}$
391	4	2, 2	$\{-1,-1\}$, $\{-1,\omega-6\}$
399	24	12, 2	$\{3,\omega-5\}^{4}$, $\{-1,-1\}$
408	6	6	$\{2,\omega+6\}^{22}$
419	3	3	$\{2,13\omega+38\}^{6}$
420	8	4, 2	$\{3,\omega+3\}^{18}$, $\{-1,-1\}$
435	12	6, 2	$\{\omega+1,\omega+7\}^{20}$, $\{-1,5\}$
452	8	8	$\{\omega+7,3\}^{2}$
455	4	2, 2	$\{-1,-1\}$, $\{-1,\omega-22\}$
471	6	6	$\{2,17\omega-186\}$
472	5	5	$\{2,\omega-15\}$
479	14	14	$\{2,5\omega-109\}^{3}$
483	4	2, 2	$\{-1,-1\}$, $\{-1,7\}$
$*491$	13	13	$\{2,11\omega+64\}^{6}$
503	6	6	$\{2,\omega-2\}$
511	4	2, 2	$\{-1,-1\}$, $\{-1,\omega-1\}$
516	12	12	$\{2\omega+3,\omega-36\}^{2}$
527	4	2, 2	$\{-1,-1\}$, $\{-1,-\omega-19\}$
543	6	6	$\{2,5\omega-29\}$
548	4	4	$\{3,\omega-5\}^{2}$
552	6	6	$\{2,5\omega+64\}^{10}$
555	28	14, 2	$\{5,\omega-8\}^{4}$, $\{-1,5\}$
571	5	5	$\{2,4\omega-31\}^{4}$
579	12	12	$\{5,19\omega-39\}^{16}$
580	4	4	$\{2,4\omega-9\}^{3}$
$*583$	34	34	$\{2,\omega+10\}$
595	4	2, 2	$\{-1,5\}$, $\{-1,-1\}$
615	12	6, 2	$\{3,\omega+10\}^{10}$, $\{-1,-1\}$
623	4	2, 2	$\{-1,-1\}$, $\{-1,\omega+43\}$
627	4	2, 2	$\{-1,3\}$, $\{-1,11\}$
643	3	3	$\{2,\omega+13\}^{3}$
$*644$	32	16, 2	$\{3,\omega-33\}^{2}$, $\{-1,\omega-8\}$
651	12	6, 2	$\{5,\omega+1\}^{20}$, $\{-1,-1\}$
660	12	6, 2	$\{2,\omega-3\}^{28}$, $\{-1,3\}$
663	4	2, 2	$\{-1,3\}$, $\{-1,-1\}$

679	20	10, 2	$\{2,-\omega-18\}\ ,\ \{-1,-\omega-18\}$
687	6	6	$\{2,5\omega-89\}^{11}$
696	42	42	$\{2,\omega+24\}^{4}$
$*703$	74	74	$\{2,5\omega+107\}$
708	4	4	$\{2,\omega+3\}^{10}$
715	4	2, 2	$\{-1,-1\}\ ,\ \{-1,11\}$
723	12	12	$\{2,2\omega-149\}^{40}$
731	4	4	$\{2,\omega+2\}^{6}$
740	4	4	$\{2,5\omega+44\}$
$*755$	82	82	$\{2,\omega-1\}^{6}$
$*759$	36	18, 2	$\{2,\omega+14\}^{2}\ ,\ \{-1,-1\}$
771	6	6	$\{2,9\omega-1\}^{6}$
772	8	8	$\{11,\omega-7\}^{10}$
776	4	4	$\{2,\omega+34\}^{2}$
791	4	2, 2	$\{-1,\omega-10\}\ ,\ \{-1,-1\}$
795	12	6, 2	$\{5,\omega-3\}^{20}\ ,\ \{-1,-1\}$
799	8	4, 2	$\{\omega-1,2\}^{2}\ ,\ \{-1,-1\}$
$*804$	36	36	$\{7\omega-76,\omega-18\}^{2}$
820	4	4	$\{2,\omega-13\}^{40}$
831	6	6	$\{2,1027\omega+6509\}$
835	6	6	$\{5,2\omega+9\}^{80}$
836	4	4	$\{2,\omega+13\}^{6}$
840	12	6, 2	$\{2,\omega-15\}^{28}\ ,\ \{-1,3\}$
863	6	6	$\{-7\omega-1441,9\omega-49\}^{9}$
868	8	4, 2	$\{7,\omega+5\}^{15}\ ,\ \{-1,-1\}$
879	10	10	$\{2,21\omega-313\}^{11}$
884	4	4	$\{2,\omega+7\}^{4}$
887	10	10	$\{281\omega-22930,2\}$
903	12	6, 2	$\{2,\omega-6\}\ ,\ \{-1,-1\}$
904	4	4	$\{\omega+32,5\}^{4}$
915	4	2, 2	$\{-1,-1\}\ ,\ \{-1,3\}$
932	20	20	$\{5,-35\omega+496\}$
935	4	2, 2	$\{-1,-1\}\ ,\ \{-1,\omega-46\}$
939	12	12	$\{5,29\omega+61\}^{4}$
943	4	2, 2	$\{-1,-1\}\ ,\ \{-1,\omega-37\}$
948	6	6	$\{2\omega-9,13\omega+113\}^{2}$
952	4	2, 2	$\{-1,-1\}\ ,\ \{-1,7\}$
959	8	4, 2	$\{2,-\omega+17\}\ ,\ \{-1,-1\}$
964	8	8	$\{7,18\omega+71\}^{3}$
971	5	5	$\{2,781\omega-174659\}^{12}$
979	4	4	$\{2,\omega-106\}^{12}$

984	6	6	$\{3, 23\omega + 171\}^{16}$
987	4	2, 2	$\{-1,-1\}$, $\{-1,-3\}$
996	4	4	$\{\omega - 1, 4\omega - 129\}^2$

7.2. **Miscellaneous fields.** Using the same programs, we computed $K_2\mathcal{O}_F$ for fields of small discriminants with various signatures, taken from the Bordeaux database [32].

In all cases, the wild kernel WK_2F happens to be trivial, and the orders coincide with the values predicted by heuristic computations using variants of Lichtenbaum's conjecture. Computing times range between a few seconds and 30 minutes, except for the last field (90 hours).

We list a defining polynomial P for the field $F = \mathbb{Q}[x]/(P)$, the discriminant Δ, the signature (r_1, r_2) and the structure of $K_2\mathcal{O}_F$. The first two cubic fields and the last two quartic fields are Galois (the first two lines are easily derived from the Birch-Tate formula, but were included as a check for our general programs).

P	Δ	(r_1, r_2)	$K_2\mathcal{O}_F$	
$x^3 + x^2 - 2x - 1$	49	$(3,0)$	$2,2,2$	$\{-1,-1\},\{-1,x\},\{-1,1+x\}$
$x^3 - 3x - 1$	81	$(3,0)$	$2,2,2$	$\{-1,-1\},\{-1,x\},\{-1,1+x\}$
$x^3 + x^2 - 3x - 1$	148	$(3,0)$	$2,2,2$	$\{-1,-1\},\{-1,x\},\{-1,1+x\}$
$x^3 + x^2 + 2x + 1$	-23	$(1,1)$	2	$\{-1,-1\}$
$x^3 + x + 1$	-31	$(1,1)$	2	$\{-1,-1\}$
$x^3 + 2x^2 + 2x + 1$	-44	$(1,1)$	2	$\{-1,-1\}$
$x^3 + 2x + 1$	-59	$(1,1)$	$2,2$	$\{-1,-1\},\{-1,x\}$
$x^3 + x^2 + 3$	-255	$(1,1)$	6	$\{-2,x\}$
$x^4 - x^3 + 2x - 1$	-275	$(2,1)$	$2,2$	$\{-1,-1\},\{-1,x\}$
$x^4 - x - 1$	-283	$(2,1)$	$2,2$	$\{-1,-1\},\{-1,x\}$
$x^4 - x^3 + x^2 + x - 1$	-331	$(2,1)$	$2,2$	$\{-1,-1\},\{-1,x\}$
$x^4 - x^3 - x^2 + x + 1$	117	$(0,2)$	1	
$x^4 - x^3 + x^2 - x + 1$	125	$(0,2)$	1	
$x^4 - x^2 + 1$	144	$(0,2)$	1	
$x^5 - x^3 - x^2 + x + 1$	1609	$(1,2)$	2	$\{-1,-1\}$

References

1. E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380. MR **91m:**11096
2. H. Bass and J. Tate, *The Milnor ring of a global field*, pp. 349–446. Lecture Notes in Math., Vol. 342, Springer, 1973. MR 56 #449
3. S. Bloch, *Applications of the dilogarithm function in algebraic K-theory and algebraic geometry*, Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977) (Tokyo), Kinokuniya Book Store, 1978, pp. 103–114. MR **82f:**14009
4. ———, *Higher regulators, algebraic K-theory, and zeta functions of elliptic curves*, American Mathematical Society, Providence, RI, 2000. MR **2001i:**11082
5. J. Browkin, *The functor K_2 for the ring of integers of a number field*, Universal algebra and applications (Warsaw, 1978), PWN, Warsaw, 1982, pp. 187–195. MR **85f:**11084
6. ———, *On the p-rank of the tame kernel of algebraic number fields*, J. Reine Angew. Math. **432** (1992), 135–149. MR **93j:**11077
7. ———, *Computing the tame kernel of quadratic imaginary fields*, Math. Comp. **69** (2000), no. 232, 1667–1683, With an appendix by K. Belabas and H. Gangl. MR **2001a:**11189

8. J. Browkin and H. Gangl, *Tame and wild kernels of quadratic imaginary number fields*, Math. Comp. **68** (1999), no. 225, 291–305. MR **99c:**11144
9. J. Browkin and A. Schinzel, *On Sylow 2-subgroups of K_2O_F for quadratic number fields F*, J. Reine Angew. Math. **331** (1982), 104–113. MR **83g:**12011
10. D. Burns and C. Greither, *On the equivariant Tamagawa conjecture for Tate motives*, Inventiones Mathematicae **153** (2003), no. 2, 303–359.
11. H. Cohen, *A course in computational algebraic number theory*, third ed., Springer-Verlag, 1996. MR **94i:**11105
12. ———, *Advanced topics in computational number theory*, Springer-Verlag, 2000. MR 1 728 313
13. M. Daberkow, *On computations in Kummer extensions*, J. Symbolic Comput. **31** (2001), no. 1-2, 113–131, Computational algebra and number theory (Milwaukee, WI, 1996). MR **2001m:**11221
14. B. M. M. de Weger, *Algorithms for Diophantine equations*, Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 1989. MR **90m:**11205
15. F. Diaz y Diaz and F. Soriano, *Approche algorithmique du groupe des classes logarithmiques*, J. Number Theory **76** (1999), no. 1, 1–15. MR **2000k:**11122
16. I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions*, second ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, Providence, RI, 2002. MR **2003c:**11150
17. H. Gangl, *Werte von Dedekindschen Zetafunktionen, Dilogarithmuswerte und Pflasterungen des hyperbolischen Raumes*, 1989, Diplomarbeit, Bonn.
18. H. Garland, *A finiteness theorem for K_2 of a number field*, Ann. of Math. (2) **94** (1971), 534–548. MR 45 #6785
19. G. Gras, *Remarks on K_2 of number fields*, J. Number Theory **23** (1986), no. 3, 322–335. MR **87j:**11124
20. D. Grayson, *Dilogarithm computations for K_3*, Algebraic K-theory, Evanston 1980 (Proc. Conf., Northwestern Univ., Evanston, Ill., 1980), Springer, Berlin, 1981, pp. 168–178. MR **82i:**12012
21. R. Groenewegen, *Bounds for computing the tame kernel*, Math. Comp., posted on July 29, 2003, PII S 0025-5718(03)01592-8 (to appear in print), `http://www.math.leidenuniv.nl/reports/2002-13.shtml`.
22. J. L. Hafner and K. S. McCurley, *A rigorous subexponential algorithm for computation of class groups*, J. Amer. Math. Soc. **2** (1989), no. 4, 837–850. MR **91f:**11090
23. A. Huber and G. Kings, *Bloch-Kato Conjecture and Main Conjecture of Iwasawa theory for Dirichlet characters*, Duke Math. J. **119** (2003), no. 3, 393–464.
24. J.-F. Jaulent, *Classes logarithmiques des corps de nombres*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 301–325. MR **96m:**11097
25. F. Keune, *On the structure of the K_2 of the ring of integers in a number field*, K-Theory **2** (1989), no. 5, 625–645. MR **90g:**11162
26. M. Kolster, T. Nguyen-Quang-Do, and V. Fleckinger, *Twisted S-units, p-adic class number formulas, and the Lichtenbaum conjectures*, Duke Math. J. **84** (1996), no. 3, 679–717, errata: *Duke Math. J.* **90** (1997), no. 3, pp. 641–643. MR **97g:**11136
27. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534. MR **84a:**12002
28. H. W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. (N.S.) **26** (1992), no. 2, 211–244. MR **93g:**11131
29. B. Mazur and A. Wiles, *Class fields of abelian extensions of $\mathbb{Q}$*, Invent. Math. **76** (1984), no. 2, 179–330. MR **85m:**11069
30. J. Milnor, *Introduction to algebraic K-theory*, Princeton University Press, Princeton, N.J., 1971, Annals of Mathematics Studies, No. 72. MR 50 #2304
31. C. C. Moore, *Group extensions of p-adic and adelic linear groups*, Inst. Hautes Études Sci. Publ. Math. No. **35** (1968), 157–222. MR 39 #5575
32. *Number fields database*, available from the address `ftp://megrez.math.u-bordeaux.fr/pub/numberfields`.
33. *PARI/GP, version* `2.1.5`, Bordeaux, 2003, `http://pari.math.u-bordeaux.fr/`.
34. H. Qin, *Computation of $K_2\mathbb{Z}[\sqrt{-6}]$*, J. Pure Appl. Algebra **96** (1994), no. 2, 133–146. MR **95i:**11135
35. ———, *The 2-Sylow subgroups of the tame kernel of imaginary quadratic fields*, Acta Arith. **69** (1995), no. 2, 153–169. MR **96a:**11132
36. ———, *Computation of $K_2\mathbb{Z}[(1+\sqrt{-35})/2]$*, Chinese Ann. Math. Ser. B **17** (1996), no. 1, 63–72. MR **97a:**19004

37. ———, *Tame kernels and Tate kernels of quadratic number fields*, J. Reine Angew. Math. **530** (2001), 105–144. MR **2002g:**11167
38. J. Rognes and C. Weibel, *Two-primary algebraic K-theory of rings of integers in number fields*, J. Amer. Math. Soc. **13** (2000), no. 1, 1–54, Appendix A by Manfred Kolster. MR **2000g:**19001
39. S. Rosset and J. Tate, *A reciprocity law for K_2-traces*, Comment. Math. Helv. **58** (1983), no. 1, 38–47. MR **85b:**11105
40. D. Ryan, *Galois Co-Descent for Wild Kernels*, Ph.D. thesis, National University of Ireland, Dublin, 2002.
41. C.-L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. preuß. Akad. Wiss. Phys.-math. Klass. (1929), no. 1, 209–266.
42. M. Skałba, *Generalization of Thue's theorem and computation of the group K_2O_F*, J. Number Theory **46** (1994), no. 3, 303–322. MR **95d:**19001
43. A. A. Suslin, *K_3 of a field, and the Bloch group*, Trudy Mat. Inst. Steklov. **183** (1990), 180–199, 229, Galois theory, rings, algebraic groups and their applications (Russian). MR **91k:**19003
44. J. Tate, *Appendix*, Algebraic K-theory II, Lecture Notes in Math., vol. 342, Springer-Verlag, 1973, pp. 429–446.
45. J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274. MR 55 #2847
46. A. Vazzana, 8-*ranks of K_2 of rings of integers in quadratic number fields*, J. Number Theory **76** (1999), no. 2, 248–264. MR **2000c:**11191
47. L. C. Washington, *Introduction to cyclotomic fields*, second ed., Springer-Verlag, 1997. MR **97h:**11130
48. K. Wildanger, *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern*, J. Number Theory **82** (2000), no. 2, 188–224. MR 1 761 620
49. R. Zimmert, *Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung*, Invent. Math. **62** (1981), no. 3, 367–380. MR **83g:**12008

Karim Belabas, Mathématiques–Bâtiment 425, Université Paris–Sud, F–91405 Orsay Cedex, email: Karim.Belabas@math.u-psud.fr

Herbert Gangl, Max-Planck-Institut für Mathematik, Vivatsgasse 7, D–53111 Bonn, email: herbert@mpim-bonn.mpg.de