GENERATORS AND RELATIONS FOR $K_2\mathcal{O}_F$, F IMAGINARY QUADRATIC

KARIM BELABAS AND HERBERT GANGL

ABSTRACT. Tate's algorithm [31] 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-th primary part of $K_2\mathcal{O}_F$ due to Tate and Keune, gives a proof of its structure for many imaginary quadratic fields, confirming earlier conjectural results in [7].

CONTENTS

1991 *Mathematics Subject Classification.* 11Y40 (11R11, 11R70, 19C20) .
Key words and phrases. K_2, imaginary quadratic fields, computation.
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 and has been achieved only in a dozen or so cases, where the resulting groups turned out to be either trivial or of order 2, with an obvious generator.

Tate [31] 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 first imaginary quadratic cases (i.e. the ones of smallest discriminant). Subsequently, other authors (Skałba [29], Qin [23, 25], Browkin [6]) have improved the method and were able to establish several other (still imaginary quadratic) cases, the largest (in absolute value) discriminant treated so far being -35.

We present an algorithm for computing $K_2\mathcal{O}_F$, that can be divided roughly into three phases:

(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 phase was originally based on work of Browkin [6], 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 [16] scripting language. So far, parts of the program remain specific to the imaginary quadratic case, for lack of good bounds for the number of generators in the general case.

The program proves the previously conjectured [7] structure of $K_2\mathcal{O}_F$, in terms of explicit generators and their order, for all imaginary quadratic fields of discriminant greater than -1000 with only 7 exceptions (cf. §7). In particular, $K_2\mathcal{O}_{\mathbb{Q}(\sqrt{-303})} = \mathbb{Z}/22\,\mathbb{Z}$, and a generator is given by the symbol

$$\left\{\tfrac{1}{2}(-37-3\sqrt{-303}), \tfrac{1}{2}(-73+\sqrt{-303})\right\}^5 .$$

Furthermore, in many other cases including the 6 exceptions from above, it still gives a set of simple generators together with a bound on their orders. For instance, $K_2\mathcal{O}_{\mathbb{Q}(\sqrt{-755})}$ is generated by

$$\left\{2, \tfrac{1}{2}(577+17\sqrt{-755})\right\}^6$$

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 [7], which used a different method.

As a further interesting example, we are led to conjecture that

$$\left\{\tfrac{1}{2}(1751+\sqrt{-4547}), \tfrac{1}{2}(7+5\sqrt{-4547})\right\}^{12}$$

has order 233 and generates $K_2\mathcal{O}_{\mathbb{Q}(\sqrt{-4547})}$.

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 part 1) of the algorithm. In §5, we explain how relations are generated, 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. In §6, 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 $F(\zeta_p)$ and discuss its realizability, in particular we carefully separate the results into unconditional ones and into ones which hold only under the assumption that a few explicit ideals in $\mathcal{O}_E$ are not principal, a fact which we can only prove assuming the Generalized Riemann Hypothesis (GRH). In a final section §7, we list our results and give a few examples.

Acknowledgements: We would like to thank Claus Fieker, Rob de Jeu, Thorsten Kleinjung, 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 [31]. 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 *tame kernel* $K_2\mathcal{O}_F$ can be given, via a theorem of Quillen, as the subgroup $\bigcap \operatorname{Ker} \partial_v$, where v runs through all finite places of F.

Garland [15] 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 [3] 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 Section 1 are refinements of Tate's method. The best unconditional results are due to Skałba [29] and Browkin [6] and rely on Minkowski's theorem on lattice points:

Theorem 2.1. *Let F be a number field and Δ its discriminant. Then $K_2\mathcal{O}_F \subset K_2^S(F)$, where $S = \{v : Nv \leq B(\Delta)\}$ for some computable*

$$B(\Delta) = O\big(\max(\Delta^3, \Delta^2 f(\Delta))\big)$$

and where f depends on the embeddings of fundamental units of F in $\mathbb{C}$ and is a priori exponential in Δ.

If F is imaginary quadratic, one can take $B(\Delta) = C\Delta^{5/3}$, where

$$C := 2^6/\pi^{10/3} \approx 1.409.$$

Here and in the sequel, all constants implied by the O notation depend at most on the field degree and are computable. The general result is due to Skałba and, although the bound does not appear explicitly in his paper, it follows from his argument. Browkin optimized the special case where F is imaginary quadratic and worked out the constants. We will refer to $B(\Delta)$ as *Browkin's bound.*

When F is a *given* arbitrary number field, one can in general derive tolerable bounds from Skałba's argument, if the fundamental units are not too large. This will be the subject of a later paper but, in the present one, we are lacking a precise bound for the general case, so F will be quadratic imaginary in all our examples. On the other hand, restricting to the imaginary quadratic case does not really make anything simpler, apart from the existence of a better bound $B(\Delta)$, so the algorithms outlined in the sequel are given in full generality.

2.2. **Computing class groups.** We recall the basic idea of modern algorithms to compute class groups and fundamental units in general number fields (see [10]). We need

- A distinguished set of generators $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ for the class group, namely all prime ideals less than the Minkowski bound (or Bach's bound if one is willing to assume GRH). They form a nice factor base.
- An easy way to produce relations: factoring elements of small norms 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 (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 with the regulator, provided by Dirichlet's class number formula. In fact, any B such that $B/\sqrt{2} < hR \leq \sqrt{2}B$ will do.

Let Λ be the submodule of $\mathbb{Z}^n$ generated by a number of relation vectors; and let M_Λ be the corresponding integral matrix. The Hermite Normal Form (HNF) algorithm, applied to M_Λ, makes it easy to compute the index $\tilde{h} = [\mathbb{Z}^n : \Lambda]$, which is a multiple of the true class number (or equal to ∞). The HNF algorithm also computes the integer kernel of M_Λ, which corresponds to *trivial* relations of the form $\alpha\mathcal{O}_F = \mathcal{O}_F$, i.e. 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.

If $\tilde{R}$ is non-zero, which can be checked numerically using Zimmert's universal lower bound for the regulator, we now have a full set of relations and a full set of generating units if and only if $0 < \tilde{h}\tilde{R} \leq \sqrt{2}B$, which 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 Browkin, the subgroup $K_2\mathcal{O}_F$ would then be given by the intersection of all $\operatorname{Ker} \partial_v : K_2^S(F) \to k(v)^*$, $v \in S$, which is obtained by elementary linear algebra (see Section 5.3). We unfortunately face two serious problems:

(a) Too many generators: Browkin's bound is exponential, and the number of generators for $U_S \otimes U_S$ is $O(|S|^2) = O(B(\Delta)^2/\log^2 B(\Delta))$ by the prime ideal theorem. For $\Delta \approx 100$, even in the imaginary quadratic case, this bound is bigger than 200000 and it will be exceedingly hard to HNF-reduce a matrix of that dimension[1].

(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 cannot do it, unless the group is trivial.

We will see in the next section that the first problem is easily overcome: by following explicitly the steps in Browkin's proof, we obtain an algorithm that, starting from Browkin's bound, considerably reduces the number of generators.

As for the second problem, we will see in Section 6 a number of useful tests, relying in particular on work of Tate [32] and Keune [18], 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 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. A proof of the cohomological version of this conjecture[2] seems to be within reach in the case of abelian fields due to the efforts of Kolster, Nguyen-Quang-Do and Fleckinger [19]. Unfortunately, even after removing erroneous Euler factors in their main formula, the statement is given only up to an unspecified power of 2 (cf. also the recent paper by Huber and Kings [17]). For a *real* abelian field, the exact power of 2 is known (Rognes and Weibel [26]), so Lichtenbaum formula can be used at least in that case.

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 related to $K_3\mathcal{O}_F$ by work of Suslin [30]) under some higher regulator map. 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 $K_3\mathcal{O}_F$ (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 $K_3\mathcal{O}_F$ (in fact rather $B(F)$).

Hence, 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 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 1.

Numerical experiments performed by the second author ([14]) suggest that, if F is imaginary quadratic, Lichtenbaum conjecture should read:

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

[1] The (naive) HNF implementation in PARI can easily treat sparse relation matrices of dimension 1000, but requires too much memory when dimension increases further.

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

where ζ_F is the Dedekind zeta function.

Remark 2.2: It is of course not fortuitous that the class group algorithm generalizes so well. One defines an infinite sequence of K-groups and there is a well-known description for the first two, which makes apparent what is going on:

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

with canonical isomorphisms. 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 Browkin'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 [31].

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 Browkin's initial S, 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. Section 5).

3.1. A notion of smallness.

For $a \in F$, define

$$T_2(a) := \frac{1}{[F:\mathbb{Q}]} \sum_{\sigma} |\sigma(a)|^2 \quad \text{and} \quad \|a\|_2 := \sqrt{T_2(a)},$$

where σ runs through the $[F:\mathbb{Q}]$ embeddings of F into $\mathbb{C}$ and $|x|$ denotes the complex modulus of x. Note that $\|.\|_2$ 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 $\|.\|_2$ 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 is $[F:\mathbb{Q}]^{-1}$ times the usual so-called T_2*-norm*, which is in fact not a norm. The normalization is chosen so that it 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.

3.2. The brute force approach.

We first require[3] 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:

$$\begin{tikzcd} & U \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ K_2^T(F)/K_2^S(F) \arrow[rr, "\partial_v"] & & k^* \end{tikzcd}$$

[3] 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 [2], will be true for S containing the primes of norm less than $12\log^2|\Delta|$.

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 $\{.,.\}$ is skew-symmetric and that $\{\pi,\pi\} = \alpha(-1)$, see [31]. 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 is larger than Browkin's bound, 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 $K_2\mathcal{O}_F \subset K_2^S(F)$. It may happen that the equality holds and the algorithm fails to detect it (return `FAIL` in that case).

(a) [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.
(b) [Compute π]. If v is not principal in A, return `FAIL`. Else compute a generator π of v using Sub-algorithm 3.2.
(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.
(e) [Find an element in U_1]. Compute a small multiplicative combination t of the generators from Step (a). If $u := 1-\pi t$ is an S-unit, go to Step (f). Otherwise, increase `fail`. If the counter gets too big, 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 [10, 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 Section 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 [11, Chapter 7]). When iterating this procedure, one should make sure to arrange the initialization Step (a) so that it can be re-used by simply deleting a generator.

(b) By a famous result of Siegel [28], 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 [34, 13], 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 (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 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, $\operatorname{Im}\beta = k^*$ as soon as S contains all the places dividing the primes less than $2\log^2 Nv$. Note that in order to be rigorous, 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 (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 (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 will be 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 (a) of Algorithm 3.1.

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, 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 to be the subgroup generated by the empty set, i.e. $U_1 = \{1\}$. We would like to apply, for as many primes v as possible, the following criterion of Tate:

Proposition 3.4. [31, Prop. 1, p. 430] *Suppose that W, C and G are subsets of U satisfying the following three conditions*

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

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 $Nv < 4$. 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. 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

$$\|a\|_2 + \|b\|_2 < Nv^{2/n}, \tag{2}$$

then the condition of a) is satisfied.

Proof. a) is exactly [3, Claim 2, p. 63]. As for b), the arithmetic-geometric mean inequality implies that

$$Na \le \|a\|_2^n, \quad \text{for } a \in F.$$

Hence, $N(b-a) \le \|b-a\|_2^n \le (\|a\|_2 + \|b\|_2)^n < Nv^2$. □

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 $m(C)$, $m(G)$, $m(W)$ be the maximum of the $\|x\|_2$ for x in C, G and W, respectively. Condition (T3) is automatically satisfied and one then checks conditions

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

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 is 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. 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 computing $(a/b - 1)\pi^{-1}$ 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 fact, if (T2′) could be omitted, Browkin's bound would be $O(\Delta)$. This is mostly what GRH would do for us (asymptotically) in the case of 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). More precisely, [6, 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 ideal class of $\mathcal{O}_F$ contains an ideal of norm $\leq q_F$ (see Section 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 Browkin's strategy to the case of general number fields. The reduction is split into two phases:
First, we build a list of bad primes, using only bounds and not the actual elements of the sets C, G and W. To ensure we have enough flexibility for the final part of the algorithm (looking for relations), we do not want S to be too small, so we initialize a *black list* with all places v dividing 2 or 3.

(a) For each prime ideal v such that $Nv \leq B(\Delta)$, compute the best possible $m(G)$ using the methods of Section 4.5.
(b) If this succeeds, check whether inequality (4) holds; if so, start over in a with the next v. If not, compute $m(W)$ using the algorithm from Section 4.6.
(c) If a prime fails to satisfy one of the two inequalities (3) and (4), 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 4.7.
(b) [Initialize C]. Compute a good set C as in Section 4.3 except we now take the best possible 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 $m(C)(\|g\|_2 + 1) < Nv$. 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. If the algorithm fails, compute a small element d, possibly larger than c, such that $d \equiv c \pmod{v}$ and $m(W) + \|d\|_2 < Nv$. 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.

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 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 $(cg)' = c$.

In this refinement algorithm, W is a theoretical annoyance that has no impact in practice when the fundamental units are small, since the set is trivial to compute : the bound (4) was nice enough to ensure that W never causes refinement to fail in any of our imaginary quadratic examples. It will become a serious problem if the fundamental units are large, since mW can then be exponential in $\sqrt{\Delta}$, for all S.

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 remarkably short. For instance for $F = \mathbb{Q}(\sqrt{-1016})$, one has $B(\Delta) = 144711$ and only 135 bad primes v. Using the Galois action, they in fact contribute 15 inert rational primes 59 split ones, and 2 ramified ones. Only 24 of them are "serious" problems (corresponding to $|S| \geq 1000$, so that algorithm 3.1 becomes expensive); 7 of them are inert, the largest norm being $157^2 = 24649$. All primes are refined when checking (T2) elementwise, without needing to modify C.

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; most of them are a nuisance, nevertheless. 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 [20]. 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 very slow (exponential time in the bound).

For the second, 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 last 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 is much better, both theoretically (polynomial time) 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 $\lceil e\rfloor$ 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 gives a crude but fast estimate, 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 S is the set of prime divisors of a list P of rational primes.

Sub-algorithm 4.1:
Input: $x \in F$, 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 it succeeds, 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 of 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 is enough to check 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 should be precomputed). One then has to check that 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.
Output: `TRUE` if $x \in U_1$, `FAIL` otherwise (could not conclude).

(a) If $(x-1)/\pi \in U$, return `TRUE`.
(b) Otherwise, pick a few small elements in U_1, 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). Multiply x by each of them 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 $1 \pmod v$ by the methods of Section 5.3. We keep only those which are included in U_1, according to the above test; when S contains all primes less than a huge 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 Section 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) above. 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 [29, GTT] asserts that, provided $Nv > (\frac{4}{\pi^2})^{r_2}|\Delta|$ *and we allow denominators*, 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 Section 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 section 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 least efficient of the grid reduction algorithms in terms of the size of the element produced, but it is very fast since most of the data (in particular P^{-1}) do not depend on ε and can be precomputed.

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 $p\,\mathrm{Id}$ and the procedure above simply picks the unique representative whose coordinates are all bounded by $(p-1)/2$. This produces the same set C 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 4.6 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

$$x_\varepsilon \in U \quad \text{such that} \quad \beta(x_\varepsilon) = \gamma \quad \text{and} \quad \|x_\varepsilon\|_2 < \texttt{MAX} \tag{5}$$

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 Section 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 $\|\xi x\|_2 = \|x\|_2$. 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. It is tempting to use the structure of $\mathbb{F}_p$-vector space on $k(v) \simeq (\mathbb{F}_p)^f$ to find good representatives $\varepsilon_1, \dots, \varepsilon_f$ for the elements in a basis, which satisfy (5). We could then try to use sphere packings, e.g. $\|x_\varepsilon + \alpha\|_2 \le \|x_\varepsilon\|_2 + \|\alpha\|_2$ for α a small combination of the ε_i, hence a few evenly distributed x_ε might be enough to yield all the representatives we need. Unfortunately, the bounds we obtain for $\|x_\varepsilon + \alpha\|_2$, although lower than `MAX`, are rarely sufficient to ensure that $x_\varepsilon + \alpha$ belongs to U (if $x \in \mathcal{O}_F$, $\|x\|_2 < Nv^{1/n}$ obviously implies that $x \in U$ for instance, but this is far too stringent), hence all those elements have to be checked individually, which is the most time-consuming part in Algorithm 4.5: roughly half the time is spent there.

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

$$m_i(C) = \max_{\frac{c_1}{c_2}\in C} \|c_i\|_2, \quad i = 1, 2.$$

Note that this depends on the particular representative 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 $\|x\|_2$ and $\|y\|_2$ 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 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), we only need $m(G)$, but if it fails and we want to check (T2) elementwise, we need an explicit subset which is 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 4.6:
Input: S and v. A precomputed 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 $\|a\|_2$.
(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 4.7:
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 $L' = \operatorname{lcm}(n, L)$. 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 $\operatorname{lcm}(L', L) \neq Nv - 1$, then set $L' = \operatorname{lcm}(L', n)$ 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 [6, 3.2]. We have a general algorithm to compute a minimal set of small generating S-units but it cannot be applied to a huge set S, since it implies HNF-reducing a square matrix of size $|S|$.

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 [10, 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 ([6, 3.2])

$$(i) \quad (a) = \mathfrak{p}\mathfrak{q},$$
$$(ii) \quad (a) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3,$$

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 [10]) 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 4.8: Although, as we have seen, W is particularly easy to compute, it is even nicer in the imaginary quadratic setting where $\|a\|_2 = \sqrt{Na}$. 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, $\|a\|_2 = \sqrt{N\mathfrak{p}N(\mathfrak{p}')}$ 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 $K_2\mathcal{O}_F \subset K_2^S(F)$ and assume that we have already computed a basis $(\omega_i)_{1\leq i\leq r}$ for the S-units, where $r := r_S := |S| + r_1 + r_2$, and w_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 $(\alpha_i\beta_j)_{1\leq i,j\leq r}$.

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 $(\alpha_i\beta_i \pmod 2)_{1\leq i\leq r} \oplus (\alpha_i\beta_j - \alpha_j\beta_i)_{1\leq i<j\leq r}$, thus cutting the dimension in half. Note that $x \otimes x$ has exponent 2, hence the reduction mod 2 in the first factor.

5.2. **Producing relations.** Our goal is to minimize the index of the lattice spanned by relation vectors for K_2F in $U_S \otimes U_S$. For that, we generate many relations of the form $u \otimes (1 - u)$, $u \in U_S$. Although there is no guarantee 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, we obtain new relations, of the form $(u'/u) \otimes (1 - (u'/u))$.

Unfortunately, we are lacking a good stopping criterion that would tell us that the lattice of relations Λ is complete, so we decide 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 $[U_S \otimes U_S : \Lambda] \neq \infty$, 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 that 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 $U_S \otimes U_S$, and its determinant appears to be minimal. By definition, $K_2\mathcal{O}_F$ 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 $\mathcal{B} = \{b_J\}$ 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, J), compute $n_{v,J} \in \mathbb{Z}/(Nv-1)\mathbb{Z}$ such that $\partial_v(b_J) = g_v^{n_{v,J}}$.

(c) Compute the kernel $\operatorname{Ker} d$ of the linear map

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

This is done by computing the integer kernel of the matrix

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

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 $(M_{\operatorname{Ker} d} | M_\Lambda)$. Let $\binom{U}{V}$ be the kernel, then $M_{\operatorname{Ker} d} U$, or equivalently $M_\Lambda V$, generates the intersection. Hence U is a matrix of relations among the generators of $K_2\mathcal{O}_F$, and the SNF of U 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 will be much smaller than the full set $(\omega_i \otimes \omega_j)_{i \leq j}$.

(b) Since we realize an explicit isomorphism $\widetilde{K_2\mathcal{O}_F} \simeq \mathbb{Z}[B]/U$, 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 $\mathbb{Z}[B]$, via factorization in U_S; hence a product in $\widetilde{K_2\mathcal{O}_F}$ reduces to an addition in $\mathbb{Z}[B]$ and a reduction modulo U. 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 the equality is known, it is enough to check that the quotient, mapped to $\mathbb{Z}[B]$, lies in the image of U.

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 Section 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 [10, 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 may also think that these generators are most probably 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. **Known results.** Let us first recall a few explicit lower bounds or formulas for the p^n-ranks for $K_2\mathcal{O}_F$, for an imaginary quadratic field $F = \mathbb{Q}(\sqrt{-\Delta})$:

(a) The group $K_2\mathcal{O}_F$ for fields of discriminant $|\Delta| \leq 35$ is known precisely (Tate [31], Skałba [29], Qin [23, 25], Browkin [6]), and in fact is either trivial or equal to $\mathbb{Z}/2\mathbb{Z}$, generated by $\{-1,-1\}$.

(b) The 2-rank is known in terms of 2-class groups by work of Tate [32] (see also Browkin-Schinzel [8]) and an explicit basis was given by Browkin [4].

(c) The most comprehensive and rather explicit results on the 4-rank are given by Qin [24] who covers the case where Δ is divisible by ≤ 3 different odd prime numbers.

(d) The 3-rank is (for simple reasons) bounded from below by 1 if $d \equiv 6 \pmod 9$ (Browkin [5]). Furthermore, there is a relationship between the 3-rank of $K_2\mathcal{O}_F$ and the class group for the real quadratic field $\mathbb{Q}(\sqrt{-3\Delta})$. A similar result for the prime 5, namely that the 5-rank $K_2\mathcal{O}_F$ is $\leq$ the 5-rank of the class group of $\mathbb{Q}(\sqrt{5\Delta})$, was conjectured in [14] on the basis of experimental data, and proved in [5].

6.2. **Formulas and lower bounds for $r_p(K_2\mathcal{O}_F)$.** One trivial but important 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: one defines the *wild kernel* $W(F)$ analogously to $K_2\mathcal{O}_F$, replacing the tame symbols $\delta_v : K_2F \to k(v)^*$ by Hilbert's norm residue symbols $(\cdot,\cdot)_v : K_2F \to \mu(F_v)$, where v runs through $\mathbb{P}_F$, the set of finite and real places of F, F_v is the completion of F at v and $(a,b)_v$ is $\left(\frac{a,b}{v}\right)_{m_v}$, the norm residue symbol of order $m_v = |\mu(F_v)|$.

By definition, $W(F) := \bigcap \mathrm{Ker}(\cdot,\cdot)_v$ where v runs through $\mathbb{P}_F$. It turns out to be a subgroup of $K_2\mathcal{O}_F$, and the quotient $K_2\mathcal{O}_F/W(F)$ can in principle be determined via Moore's exact sequence [22] :

$$1 \to W(F) \to K_2\mathcal{O}_F \to \bigoplus_{v\in\mathbb{P}_F} \mu(F_v) \to \mu(F) \to 1.$$

One restricts the sequence to p-primary parts, and determines $\mu(F_v)\otimes\mathbb{Z}_p$ via the observation that $\zeta_{p^n}\in F_v$ iff v splits completely in $F(\zeta_{p^n})/F$. When F is quadratic, the recipe turns out to be trivial:

Theorem 6.1 (Browkin [4])**.** *Let F be the quadratic field of discriminant Δ. The index $i_F := [K_2\mathcal{O}_F : W(F)]$ divides 6, and we have*

$$\begin{array}{lll} 2|i_F & \textit{iff} & \Delta/\gcd(4,\Delta)\equiv \pm 1 \pmod 8, \\ 3|i_F & \textit{iff} & \Delta\equiv 6 \pmod 9, \quad \Delta\neq -3. \end{array}$$

So 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 $W(F)=0$, but this is a less severe restriction than $K_2\mathcal{O}_F = 0$.

6.3. **Local norm symbols and Brauer groups.** If we believe that $W(F)\neq 0$, 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, and determine their properties there, in particular trying to assert that they are non-zero. 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 ζ_n of unity, 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 [32]) 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. [21]. This element is trivial (i.e. is isomorphic to the matrix algebra $M_{n^2}(E)$) 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 the question whether a is 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 $\wp|p$, otherwise the image will be trivial). The latter is a cyclic group of order p 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 [12]) and stands no better chance of success, except that it provides a neat way to compute the said symbol.

Unfortunately, the following proposition shows that these localization maps will not detect anything new if F is quadratic: they are trivial on the wild kernel.

Proposition 6.1. *Let F be the quadratic field of discriminant Δ, p a prime number, $E = F(\zeta_p)$, and $\wp$ some place in $\mathbb{P}_E$. By abuse of notation, let $(\cdot,\cdot)_\wp$ be the norm residue symbol of order p in $E_\wp$. If $\{a,b\} \in W(F)$, then $(a,b)_\wp = 1$.*

Proof. By contradiction, assume that $(a,b)_\wp \neq 1$. The case $p=2$ is trivial since $F(\zeta_2) = F$, so we assume that p is odd. We can also restrict to the case $\wp | p$; namely, since $p \neq 2$, the norm residue symbols at infinity are trivial, and if $\wp \nmid p$ then $(a,b)_\wp = \partial_\wp(a,b)$, but the latter is 1 since $\{a,b\} \in K_2\mathcal{O}_F$.

Since E contains the p-th roots of unity, the product formula asserts that

$$\prod_{\wp \in \mathbb{P}_E} (a,b)_\wp = 1\,.$$

On the other hand, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is totally ramified at p, hence there are at most two places above p in $E = F(\zeta_p)$. Due to the product formula, there cannot be a single non-trivial symbol, hence there are exactly two places above p in E. Let $\wp$ be one of them.

We first show that $E_\wp = \mathbb{Q}_p(\zeta_p)$. Since $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \simeq p^{\mathbb{Z}/2\mathbb{Z}} \times \mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ (recall that $p \neq 2$), there are three quadratic extensions of $\mathbb{Q}_p$, only one of which is included in $\mathbb{Q}_p(\zeta_p)$ (namely $\mathbb{Q}_p(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2}p$). If $E_\wp \supsetneq \mathbb{Q}_p(\zeta_p)$, then it contains all three quadratic extensions, including the unramified one. This would imply that there is a single place above p in E, of inertia degree 2, which is a contradiction.

Let F_v be the completion of F at a place v above p. Either p splits in F and $F_v = \mathbb{Q}_p$ or it is ramified and $F_v = \mathbb{Q}(\sqrt{p^*})$ by the preceding argument. Hence the assertion we are trying to prove translates to: if a and b belong to $F_v \subset E_\wp = \mathbb{Q}_p(\zeta_p)$, then $(a,b)_\wp = 1$. Let $\pi_F := p$ (if p is unramified in F) or $\sqrt{p^*}$ (if p is ramified) be a uniformizer in F_v and $\pi := \pi_E := 1 - \zeta_p$.

Using the multiplicative structure of the local field $\mathbb{Q}_p(\sqrt{p^*})$ together with the standard properties of the norm residue symbol (see e.g. [9, Exercise 2.13]), one reduces to the case where $a = \pi_F$, and b is a unit of the form $1 + \sum_{i>0} b_i \pi_F^i$. (Note that $(a,a)_\wp = (-1,b)_\wp = 1$ for $p \neq 2$.) We can even assume that $a = p^*$ since $(\sqrt{p^*}, b)_\wp^2 = (p^*, b)_\wp$ and $p \neq 2$. For $b \in \mathbb{Q}_p(\zeta_p)$ as above, Artin and Hasse [1] have proven the following *explicit formula*:

$$(p,b)_\wp = \zeta_p^{\mathrm{Tr}\left(\frac{\log b}{\pi^p}\right)},$$

where log denotes the p-adic logarithm and Tr is the absolute trace in $\mathbb{Q}_p(\zeta_p)$. We develop $\log(b)$ as a power series in π_F and $(p,b)_\wp = 1$ follows by the following Lemma 6.1 unless $p = 3$ and $F_v = E_\wp = \mathbb{Q}_3(\zeta_3)$. But in that case we still have $(a,b)_\wp = 1$ since $\{a,b\} \in W(F)$. Note that $F_v = E_\wp = \mathbb{Q}_3(\zeta_3)$ occurs iff $\Delta \equiv 6 \pmod 9$, which recovers in a very complicated way part of Theorem 6.1. □

Lemma 6.1. *For all $n > 0$ and p odd, we have*

$$\mathrm{Tr}(\pi_F^n/\pi^p) \equiv 0 \pmod p$$

unless $n = 1$, $p = 3$, and $F_v = \mathbb{Q}_3(\zeta_3)$ (i.e. 3 ramifies in F).

Proof. The lemma is trivial if $n > 2$ (recall that $v_\wp(p) = p-1$ and $v_\wp(\pi) = 1$). Let $u_n := (\sqrt{p^*})^n$ (note that $\pi_F = \pm u_1$ or u_2); the action of $\sigma_i : \zeta_p \mapsto \zeta_p^i \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ on u_n is given by $\chi_n := \left(\frac{\cdot}{p}\right)^n$, hence the trace is equal to

$$\sum_{i=1}^{p-1} \frac{\chi_n(i) u_n}{(1-\zeta_p^i)^p} = \frac{u_n}{\pi^p} \sum_{i=1}^{p-1} \frac{\chi_n(i)}{(\sum_{j=0}^{i-1} \zeta_p^j)^p}\,.$$

Using $v_\wp(u_n/\pi^p) \geq -(p+1)/2 \geq -(p-1)$ (one of these inequalities is strict unless $n=1$ and $p=3$), it remains to study the sum

$$\sum_{i=1}^{p-1} \frac{\chi_n(i)}{(\sum_{j=0}^{i-1} \zeta_p^j)^p} \equiv \sum_{i=1}^{p-1} \frac{\chi_n(i)}{i} \equiv \frac{\chi_n(g)}{g} \sum_{i=1}^{p-1} \frac{\chi_n(i)}{i} \pmod p$$

for any $g \in \mathbb{F}_p^*$, so the sum is 0 modulo p when χ_n is not the identity, i.e. unless $p=3$ and $n=1$. This proves the lemma. ☐

It looks plausible that this lemma holds in greater generality, i.e. that $F \subset F(\zeta_p)$ induces a natural map from $W(F)$ to $W(F(\zeta_p))$ for a much larger class of number fields F, but we did not investigate this question.

6.4. **Keune's exact sequences.** The correct generalization of these ideas is due to Tate [32] and Keune [18], and affords a complete solution to our problem *assuming* we can compute certain class groups. We quote Keune's formulation :

Theorem 6.2. [18, (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 $E = F$,*

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

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

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

- *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 $\wp|p$.*

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

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 [18, 6.2] to go back from $K_2\mathcal{O}_{F(i)}$ to $K_2\mathcal{O}_F$.

(b) If F is quadratic, then the p-part of $\mu(F_\wp)$ is equal to μ_4 if $p = 2$ and μ_p otherwise. Indeed, μ_{p^r} is included in $F_\wp$ if and only if $\wp$ is totally split in $F(\zeta_{p^r})$. Hence the ramification index of a place above p in $F(\zeta_{p^r})$ is $e(\wp/p) \leq 2$. Since it is already equal to $p^{r-1}(p-1)$ in $\mathbb{Q}(\zeta_{p^r})$, the result follows.

(c) 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 [11, Chapter 7]).

(d) 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 [3, p. 382] and [27]). If the set S we choose when computing $\widetilde{K_2\mathcal{O}_F}$ is large enough, these symbols factor on our S-unit factor base 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, we obtain simple generators for the p-primary part of $K_2\mathcal{O}_F$.

(e) Remarkably, as 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 $q = p^r$ be the exponent of the p-primary part of our conjectural $\widetilde{K_2\mathcal{O}_F}$. If we can compute the class group of $F(\zeta_q)$, we obtain the p-primary part of $K_2\mathcal{O}_F$ (since $K_2\mathcal{O}_F$ is a quotient of $\widetilde{K_2\mathcal{O}_F}$, q also kills the p-primary part of $K_2\mathcal{O}_F$). If the p-primary parts coincide for all $p|\widetilde{K_2\mathcal{O}_F}$, we know that $\widetilde{K_2\mathcal{O}_F} = K_2\mathcal{O}_F$. In particular, we have proven the non-triviality of our generating elements, although in a roundabout way. Otherwise, we now know the structure of $K_2\mathcal{O}_F$, in particular its exact order and we look for more relations until the required index is obtained.

In the unfortunate case that $q = p^r$ is so large that $\mathrm{Cl}(F(\zeta_q))$ cannot be computed, we still obtain lower bounds on the order of our generating elements if $\mathrm{Cl}(F(\zeta_p))$ can be computed. It may even occur that the p-primary part of $K_2\mathcal{O}_F$ is p-torsion (with a high p-rank) and that we can compute exact orders after all. Hence, it makes sense in any case to compute $\mathrm{Cl}(F(\zeta_p))$ first in order to take advantage of that possibility. If p itself is large, nothing can be salvaged.

Finally it should be noted[4] that if $F(\zeta_{p^r})$ is a CM-field, the natural map from the maximal real subfield $\mathrm{Cl}(F(\zeta_{p^r})^+) \to \mathrm{Cl}(F(\zeta_{p^r}))$ is injective on the p-th primary part for odd p (see e.g. Washington [33, 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 $\mathrm{Cl}(F(\zeta_{11}))$, but the computations needs 2 days instead of 15 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 cyclotomic extension itself.

Note that the first part of the algorithm proved that

$$K_2\mathcal{O}_F = \left\langle \left\{ -\tfrac{1}{2}(37 + 3\sqrt{-303}), \tfrac{1}{2}(-73 + \sqrt{-303}) \right\} \right\rangle$$

and has exponent 22. 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

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

is consistent with the heuristic result obtained in [7] assuming the truth of Lichtenbaum's conjecture.

7. Tables

We have proven the correct structure of $K_2\mathcal{O}_F$ for all imaginary quadratic fields F of discriminant $|\Delta| < 1000$, 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 [7] by experimental methods (even for the 7 discriminants above). Computing times range from 5s to 1h per discriminant, not including the final certification.

In all the tables, we list $d = |\Delta|$ where $\Delta \leq 0$ is the discriminant of the imaginary quadratic field $F = \mathbb{Q}(\sqrt{\Delta})$ and x stands for $\sqrt{\Delta}$. When appropriate, we list $|K_2\mathcal{O}_F|$, the elementary divisors of $K_2\mathcal{O}_F$, and the corresponding generators. No effort has been made to have "best possible" generators (for instance all 2-torsion symbols could easily be written as $\{-1, a\}$, for some simple $a \in F^*$ by the methods of [4]). 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	$\{3, \frac{1}{2}x - \frac{9}{2}\}^{16}$
187	$\{-1, \frac{1}{2}x - \frac{3}{2}\}$	267	$\{3, \frac{1}{2}x - \frac{15}{2}\}^{8}$
328	$\{\frac{1}{2}x - 4, \frac{1}{2}x + 3\}^{12}$	339	$\{-1, -4x - 101\}$
340	$\{2, \frac{1}{2}x - 5\}^{20}$	411	$\{-1, \frac{11}{2}x + \frac{113}{2}\}$
451	$\{-1, 4x + 153\}$	456	$\{\frac{1}{2}x - 6, \frac{1}{2}x - 1\}^{44}$
520	$\{2, \frac{1}{2}x - 10\}^{44}$	584	$\{\frac{13}{2}x - 149, \frac{41}{2}x + 732\}^{2}$
680	$\{x - 7, 3\}$	699	$\{5, \frac{1}{2}x - \frac{1}{2}\}^{12}$
712	$\{-1, -\frac{1}{2}x + 68\}$	779	$\{-1, -\frac{7}{2}x + \frac{445}{2}\}$
803	$\{2, \frac{23}{2}x + \frac{561}{2}\}^{30}$	843	$\{\frac{1}{2}x - \frac{23}{2}, \frac{1}{2}x + \frac{33}{2}\}^{66}$

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

39	6	6	$\{-\frac{1}{2}x-\frac{5}{2},\frac{1}{2}x-\frac{7}{2}\}^5$
68	8	8	$\{\frac{1}{2}x+1,\frac{1}{2}x-2\}^6$
84	6	6	$\{2,\frac{1}{2}x-5\}^{11}$
107	3	3	$\{2,\frac{1}{2}x-\frac{7}{2}\}^{12}$
111	6	6	$\{-1,-1\}\{-\frac{3}{2}x-\frac{5}{2},\frac{1}{2}x+\frac{23}{2}\}^4$
119	4	2, 2	$\{-1,\frac{1}{2}x-\frac{3}{2}\}$, $\{-1,-1\}$
120	6	6	$\{2,\frac{1}{2}x+12\}^{28}$
132	4	4	$\{2,\frac{1}{2}x+1\}\{3,\frac{1}{2}x+1\}^2$
136	4	4	$\{\frac{1}{2}x+4,\frac{1}{2}x-21\}^{18}$
164	4	4	$\{-\frac{1}{2}x+11,3\}^2$
183	6	6	$\{-1,-1\}\{2,\frac{1}{2}x-\frac{3}{2}\}^2$
195	4	2, 2	$\{3,x\}^{12}$, $\{-1,-1\}$
219	12	12	$\{-1,\frac{1}{2}x+\frac{9}{2}\}\{\frac{1}{2}x+\frac{9}{2},2\}^{-3}\{\frac{1}{2}x+\frac{9}{2},\frac{1}{2}x-\frac{1}{2}\}^{-10}$
228	12	12	$\{2,\frac{1}{2}x-9\}^{22}\{2,\frac{1}{2}x-1\}^{-28}$
231	4	2, 2	$\{-1,\frac{1}{2}x+\frac{5}{2}\}$, $\{-1,3\}$
255	12	6, 2	$\{3,\frac{1}{2}x+\frac{15}{2}\}^4$, $\{-1,3\}$
260	4	4	$\{2,x-19\}^{22}$
264	6	6	$\{\frac{1}{2}x-3,5\}^4$
287	4	2, 2	$\{-1,\frac{1}{2}x-\frac{1}{2}\}$, $\{-1,-1\}$
291	12	12	$\{\frac{1}{2}x+\frac{3}{2},5\}^4$
292	4	4	$\{\frac{1}{2}x-5,7\}^3$
303	22	22	$\{-\frac{3}{2}x-\frac{37}{2},\frac{1}{2}x-\frac{73}{2}\}^5$
327	6	6	$\{-1,-1\}\{2,\frac{5}{2}x-\frac{23}{2}\}^8$
331	3	3	$\{2,\frac{1}{2}x+\frac{3}{2}\}^{24}$
356	4	4	$\{-\frac{1}{2}x-37,\frac{7}{2}x+16\}^{18}$
367	6	6	$\{-1,-1\}\{2,-\frac{3}{2}x-\frac{5}{2}\}^{12}$
388	8	8	$\{-1,-1\}\{\frac{1}{2}x-1,3x-55\}^{18}$
391	4	2, 2	$\{-1,-1\}$, $\{-1,\frac{1}{2}x-\frac{11}{2}\}$
399	24	12, 2	$\{-1,-1\}\{-1,\frac{1}{2}x-\frac{25}{2}\}\{3,\frac{1}{2}x-\frac{9}{2}\}^4$, $\{-1,-1\}$
408	6	6	$\{2,\frac{1}{2}x-6\}^{22}$
419	3	3	$\{2,\frac{1}{2}x-\frac{7}{2}\}^{12}$
420	8	4, 2	$\{-1,-1\}\{-1,3\}\{2,\frac{1}{2}x+3\}^{-8}\{3,\frac{1}{2}x+3\}^2$, $\{-1,-1\}$
435	12	6, 2	$\{5,\frac{1}{2}x+\frac{15}{2}\}^{20}$, $\{5,\frac{1}{2}x+\frac{15}{2}\}^{10}\{5,\frac{1}{2}x-\frac{5}{2}\}^{-22}$
452	8	8	$\{\frac{1}{2}x+7,3\}^2$
455	4	2, 2	$\{-1,-1\}$, $\{-1,\frac{1}{2}x-\frac{43}{2}\}$
471	6	6	$\{2,-\frac{7}{2}x-\frac{155}{2}\}^{11}$

472	5	5	$\{5,-\frac{3}{2}x-4\}^{120}$
479	14	14	$\{-1,-1\}\{2,-\frac{41}{2}x-\frac{711}{2}\}^{4}$
483	4	2, 2	$\{-1,-1\}\ ,\ \{7,\frac{1}{2}x-\frac{21}{2}\}^{30}$
*491	13	13	$\{2,\frac{1}{2}x-\frac{7}{2}\}^{12}$
503	6	6	$\{-1,-1\}\{\frac{1}{2}x-\frac{3}{2},\frac{1}{2}x+\frac{5}{2}\}^{10}$
511	4	2, 2	$\{-1,-1\}\ ,\ \{\frac{1}{2}x-\frac{17}{2},5\}^{4}$
516	12	12	$\{3,\frac{1}{2}x-6\}^{50}\{-1,\frac{1}{2}x-11\}^{-1}$
527	4	2, 2	$\{-1,-\frac{1}{2}x-\frac{39}{2}\}\ ,\ \{-1,-1\}$
543	6	6	$\{-1,-1\}\{\frac{5}{2}x-\frac{53}{2},5\}^{-1}$
548	4	4	$\{-\frac{5}{2}x-56,-\frac{1}{2}x-22\}^{22}$
552	6	6	$\{-1,-1\}\{-1,\frac{1}{2}x+3\}\{\frac{1}{2}x+3,\frac{1}{2}x-4\}^{10}\{2,\frac{1}{2}x+3\}^{-1}$
555	28	14, 2	$\{5,\frac{1}{2}x+\frac{5}{2}\}^{14}\ ,\ \{-1,-1\}$
571	5	5	$\{2,\frac{1}{2}x-\frac{27}{2}\}^{12}$
579	12	12	$\{\frac{19}{2}x-\frac{59}{2},\frac{1}{2}x+\frac{89}{2}\}^{8}$
580	4	4	$\{2x-9,\frac{3}{2}x-19\}^{16}\{2,2x-9\}^{-1}$
*583	34	34	$\{-1,-1\}\{2,\frac{1}{2}x+\frac{5}{2}\}^{18}$
595	4	2, 2	$\{-1,5\}\ ,\ \{-1,-1\}$
615	12	6, 2	$\{3,\frac{1}{2}x-\frac{11}{2}\}^{11}\{\frac{1}{2}x-\frac{59}{2},\frac{1}{2}x+\frac{9}{2}\}^{-14}\ ,\{-1,-1\}$
623	4	2, 2	$\{-1,\frac{1}{2}x+\frac{23}{2}\}\ ,\ \{-1,-\frac{1}{2}x-\frac{87}{2}\}$
627	4	2, 2	$\{3,\frac{1}{2}x+\frac{33}{2}\}^{6}\{11,\frac{1}{2}x-\frac{33}{2}\}^{12}\ ,\{3,\frac{1}{2}x+\frac{33}{2}\}^{6}\{3,\frac{1}{2}x+\frac{11}{2}\}^{-16}$
643	3	3	$\{\frac{1}{2}x+\frac{27}{2},\frac{1}{2}x-\frac{71}{2}\}^{7}\{\frac{1}{2}x+\frac{27}{2},\frac{1}{2}x+\frac{13}{2}\}^{-1}\{2,\frac{1}{2}x+\frac{13}{2}\}^{12}$
*644	32	16, 2	$\{\frac{1}{2}x-8,-x-59\}^{2}\ ,\ \{-1,\frac{1}{2}x-8\}$
651	12	6, 2	$\{2,\frac{7}{2}x+\frac{51}{2}\}^{132}\{3,\frac{1}{2}x-\frac{207}{2}\}^{28}\ ,\{2,\frac{7}{2}x+\frac{51}{2}\}^{132}$
660	12	6, 2	$\{2,\frac{1}{2}x-3\}^{28}\ ,\ \{2,\frac{1}{2}x-5\}^{36}$
663	4	2, 2	$\{-1,3\}\ ,\ \{-1,-1\}$
679	20	10, 2	$\{2,\frac{1}{2}x+\frac{29}{2}\}^{36}\ ,\ \{-1,-\frac{1}{2}x-\frac{37}{2}\}$
687	6	6	$\{2,\frac{1}{2}x+\frac{119}{2}\}^{28}\{-1,-\frac{3}{2}x-\frac{101}{2}\}$
696	42	42	$\{-1,-1\}\{2,\frac{1}{2}x+4\}^{-72}\{2,2x-29\}^{-28}$
*703	74	74	$\{-1,-1\}\{2,\frac{1}{2}x+\frac{31}{2}\}^{12}$
708	4	4	$\{2,\frac{1}{2}x+3\}^{10}$
715	4	2, 2	$\{-1,-1\}\ ,\ \{-1,11\}$
723	12	12	$\{-\frac{9}{2}x+\frac{1}{2},x-148\}^{80}$
731	4	4	$\{2,\frac{1}{2}x+\frac{5}{2}\}^{6}$
740	4	4	$\{2,-x+31\}^{6}$
*755	82	82	$\{2,-\frac{17}{2}x-\frac{577}{2}\}^{6}$
*759	36	18, 2	$\{-1,-\frac{1}{2}x-\frac{125}{2}\}\{2,\frac{1}{2}x-\frac{3}{2}\}^{2}\ ,\{-\frac{1}{2}x-\frac{125}{2},-\frac{1}{2}x+\frac{131}{2}\}^{12}$
771	6	6	$\{-\frac{9}{2}x-\frac{7}{2},x-2\}^{30}$

772	8	8	$\{\frac{1}{2}x-7,\frac{1}{2}x+26\}^{65}$
776	4	4	$\{2,\frac{1}{2}x+4\}^{12}$
791	4	2, 2	$\{-1,\frac{1}{2}x-\frac{19}{2}\}$, $\{-1,-1\}$
795	12	6, 2	$\{11,\frac{1}{2}x-\frac{5}{2}\}^{40}$, $\{11,\frac{1}{2}x+\frac{15}{2}\}^{240}$
799	8	4, 2	$\{\frac{1}{2}x-\frac{1}{2},2\}^{2}$, $\{-1,-1\}$
∗804	36	36	$\{\frac{1}{2}x+7,5\}^{6}\{3,-16x-99\}^{22}$
820	4	4	$\{2,\frac{1}{2}x-13\}^{40}$
831	6	6	$\{-1,-1\}\{-1,-\frac{1}{2}x+\frac{97}{2}\}\{2,-\frac{1}{2}x+\frac{97}{2}\}^{-2}$
835	6	6	$\{\frac{1}{2}x-\frac{67}{2},x+10\}^{4}\{5,\frac{1}{2}x-\frac{45}{2}\}^{-4}$
836	4	4	$\{-\frac{5}{2}x+232,\frac{11}{2}x-73\}\{-1,\frac{11}{2}x-73\}$
840	12	6, 2	$\{5,\frac{1}{2}x-15\}^{28}$, $\{5,\frac{1}{2}x-15\}^{28}\{2,\frac{1}{2}x+15\}^{-28}$
863	6	6	$\{-1,-1\}\{\frac{1}{2}x+\frac{47}{2},-\frac{87}{2}x+\frac{1543}{2}\}^{16}$
868	8	4, 2	$\{\frac{1}{2}x+5,\frac{1}{2}x-6\}^{110}$, $\{-1,-1\}$
879	10	10	$\{-\frac{239}{2}x-\frac{3257}{2},\frac{1}{2}x+\frac{7}{2}\}^{7}$
884	4	4	$\{-1,-1\}\{-2x-55,\frac{1}{2}x+7\}^{4}$
887	10	10	$\{-\frac{281}{2}x+\frac{45579}{2},-\frac{1}{2}x+\frac{195}{2}\}^{9}$
903	12	6, 2	$\{5,\frac{1}{2}x-\frac{75}{2}\}^{16}$, $\{-1,-1\}$
904	4	4	$\{-\frac{1}{2}x-32,5\}^{4}$
915	4	2, 2	$\{-1,-1\}$, $\{3,\frac{1}{2}x-\frac{45}{2}\}^{12}$
932	20	20	$\{5,\frac{1}{2}x-8\}^{120}\{-\frac{1}{2}x+35,3\}^{-2}$
935	4	2, 2	$\{-1,-1\}$, $\{-1,\frac{1}{2}x-\frac{91}{2}\}$
939	12	12	$\{\frac{1}{2}x-\frac{81}{2},-6x-139\}^{16}$
943	4	2, 2	$\{-1,-1\}$, $\{-1,\frac{1}{2}x-\frac{73}{2}\}$
948	6	6	$\{-6x-289,\frac{1}{2}x-29\}\{5,\frac{19}{2}x-943\}^{14}\{-x+9,5\}^{-4}$
952	4	2, 2	$\{-1,-1\}$, $\{-1,7\}$
959	8	4, 2	$\{2,-\frac{1}{2}x-\frac{95}{2}\}^{12}$, $\{-1,-1\}$
964	8	8	$\{\frac{1}{2}x+2,-x+131\}^{14}\{\frac{1}{2}x-3,7\}^{-2}$
971	5	5	$\{\frac{1}{2}x+\frac{23}{2},-733x+14516\}^{2}$
979	4	4	$\{2,\frac{1}{2}x-\frac{211}{2}\}^{12}$
984	6	6	$\{x-121,\frac{1}{2}x-3\}^{4}$
987	4	2, 2	$\{-1,3\}$, $\{2,-\frac{17}{2}x-\frac{135}{2}\}^{18}\{3,\frac{1}{2}x+\frac{39}{2}\}^{-18}$
996	4	4	$\{\frac{1}{2}x-1,-2x+129\}^{2}$

References

[1] E. Artin & H. Hasse, Über den zweiten Ergänzungssatz zum Reziprozitätsgesetz der l-ten Potenzreste im Körper k_ζ der l-ten Einheitswurzeln und in Oberkörpern von k_ζ, *J. reine angew. Math.* **154** (1925), pp. 143–148.

[2] E. Bach, Explicit bounds for primality testing and related problems, *Math. Comp.* **55** (1990), no. 191, pp. 355–380.

[3] H. Bass & J. Tate, The Milnor ring of a global field, 349–446. Lecture Notes in Math., Vol. 342, Springer, 1973, pp. 349–446. Lecture Notes in Math., Vol. 342.

[4] J. Browkin, The functor K_2 for the ring of integers of a number field, in *Universal algebra and applications (Warsaw, 1978)* (Warsaw), PWN, Warsaw, 1982, pp. 187–195.

[5] J. Browkin, On the p-rank of the tame kernel of algebraic number fields, *J. Reine Angew. Math.* **432** (1992), pp. 135–149.

[6] J. Browkin, Computing the tame kernel of quadratic imaginary fields, *Math. Comp.* **69** (2000), no. 232, pp. 1667–1683, With an appendix by K. Belabas and H. Gangl.

[7] J. Browkin & H. Gangl, Tame and wild kernels of quadratic imaginary number fields, *Math. Comp.* **68** (1999), no. 225, pp. 291–305.

[8] J. Browkin & A. Schinzel, On Sylow 2-subgroups of K_2O_F for quadratic number fields F, *J. Reine Angew. Math.* **331** (1982), pp. 104–113.

[9] J. W. S. Cassels & A. Fröhlich (eds.), Algebraic number theory, Academic Press Inc., 1986, Reprint of the 1967 original.

[10] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, 1993.

[11] H. Cohen, *Advanced topics in computational number theory*, Springer-Verlag, 2000.

[12] M. Daberkow, On computations in Kummer extensions, 1999, preprint.

[13] B. M. M. de Weger, *Algorithms for Diophantine equations*, Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[14] H. Gangl, Werte von Dedekindschen Zetafunktionen, Dilogarithmuswerte und Pflasterungen des hyperbolischen Raumes, 1989, Diplomarbeit, Bonn.

[15] H. Garland, A finiteness theorem for K_2 of a number field, *Ann. of Math. (2)* **94** (1971), pp. 534–548.

[16] The PARI Group, PARI/GP, version `2.1`, Bordeaux, 2000, available from the address `http://www.parigp-home.de`.

[17] A. Huber & G. Kings, Bloch-Kato Conjecture and Main Conjecture of Iwasawa theory for Dirichlet characters, 2001, preprint, `http://arXiv.org/abs/math/0101071`.

[18] F. Keune, On the structure of the K_2 of the ring of integers in a number field, *K-Theory* **2** (1989), no. 5, pp. 625–645.

[19] M. Kolster, T. Nguyen Quang Do, & V. Fleckinger, Twisted S-units, p-adic class number formulas, and the Lichtenbaum conjectures, *Duke Math. J.* **84** (1996), no. 3, pp. 679–717, errata: *Duke Math. J.* **90** (1997), no. 3, pp. 641–643.

[20] A. K. Lenstra, H. W. Lenstra, Jr., & L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), no. 4, pp. 515–534.

[21] J. Milnor, *Introduction to algebraic K-theory*, Princeton University Press, Princeton, N.J., 1971, Annals of Mathematics Studies, No. 72.

[22] C. C. Moore, Group extensions of p-adic and adelic linear groups, *Inst. Hautes Études Sci. Publ. Math. No.* **35** (1968), pp. 157–222.

[23] H. Qin, Computation of $K_2\mathbb{Z}[\sqrt{-6}]$, *J. Pure Appl. Algebra* **96** (1994), no. 2, pp. 133–146.

[24] H. Qin, The 2-Sylow subgroups of the tame kernel of imaginary quadratic fields, *Acta Arith.* **69** (1995), no. 2, pp. 153–169.

[25] H. Qin, Computation of $K_2\mathbb{Z}[(1+\sqrt{-35})/2]$, *Chinese Ann. Math. Ser. B* **17** (1996), no. 1, pp. 63–72, A Chinese summary appears in Chinese Ann. Math. Ser. A **17** (1996), no. 1, 121.

[26] J. Rognes & C. Weibel, Two-primary algebraic K-theory of rings of integers in number fields, *J. Amer. Math. Soc.* **13** (2000), no. 1, pp. 1–54, Appendix A by Manfred Kolster.

[27] S. Rosset & J. Tate, A reciprocity law for K_2-traces, *Comment. Math. Helv.* **58** (1983), no. 1, pp. 38–47.

[28] C.-L. Siegel, Über einige Anwendungen diophantischer Approximationen, *Abh. preuß. Akad. Wiss. Phys.-math. Klass.* (1929), no. 1, pp. 209–266.

[29] M. Skałba, Generalization of Thue's theorem and computation of the group K_2O_F, *J. Number Theory* **46** (1994), no. 3, pp. 303–322.

[30] A. A. Suslin, K_3 of a field, and the Bloch group, *Trudy Mat. Inst. Steklov.* **183** (1990), pp. 180–199, 229, Galois theory, rings, algebraic groups and their applications (Russian).

[31] J. Tate, Appendix, in *Algebraic K-theory II*, Lecture Notes in Math., vol. 342, Springer-Verlag, 1973, pp. 429–446.

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

[33] L. C. Washington, *Introduction to cyclotomic fields*, second ed., Springer-Verlag, 1997.

[34] K. Wildanger, Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern, *J. Number Theory* **82** (2000), no. 2, pp. 188–224.

Karim Belabas, Mathématique–Bâtiment 425, Université de 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