MATHEMATICS OF COMPUTATION
Volume 72, Number 242, Pages 941–951
S 0025-5718(02)01452-7
Article electronically published on June 13, 2002

CONSTRUCTING COMPLETE TABLES OF QUARTIC FIELDS USING KUMMER THEORY

HENRI COHEN, FRANCISCO DIAZ Y DIAZ, AND MICHEL OLIVIER

Abstract. We explain how to construct tables of quartic fields of discriminant less than or equal to a given bound in an efficient manner using Kummer theory, instead of the traditional (and much less efficient) method using the geometry of numbers. As an application, we describe the computation of quartic fields of discriminant up to 10^7, the corresponding table being available by anonymous ftp.

1. Introduction

Traditional methods for computing tables of number fields have mainly relied on the geometry of numbers, more precisely on the use of Hunter's theorem and a relative version due to Martinet (see for example [7], Chapter 9). The main disadvantage of this method is that it is extremely inefficient, since one must often generate a million or more times as many polynomials as necessary, because we have to search for interesting points inside a large ellipsoid.

In degree 2, such a method is of course not necessary and one can very efficiently generate tables of quadratic fields essentially by generating tables of squarefree integers, which can be done very quickly. For degree 3, it has only recently been noticed in the paper of K. Belabas [1], following the pioneering work of Davenport and Heilbronn [14], [15], that one can also very efficiently generate tables of cubic fields.

In degree 4 or higher, the situation is much worse. In the case where the number fields are *imprimitive*, in other words contain a nontrivial subfield, it is possible to use methods coming from class field theory or Kummer theory, for example to construct relative quadratic extensions, but also by more subtle methods, to construct relative cubic extensions (see [7], Chapter 9). This is how tables of imprimitive quartic and sextic fields have been constructed (see [2], [17] for sextic fields), and tables of octic fields containing a quartic subfield [10]. The real difficulty starts with primitive quartic fields, in other words quartic fields of which the Galois group of a Galois closure is isomorphic to the alternating group A_4 or the symmetric group S_4 (by abuse of language we will simply say that the quartic fields have Galois group isomorphic to A_4 or S_4).

In Section 2 of this paper we recall how to construct tables of relative quadratic extensions of number fields, which allow us to construct complete tables of quartic fields with Galois group isomorphic to the cyclic group C_4, the Klein 4-group $V_4 = C_2 \times C_2$ and the dihedral group D_4 of order 8. In Section 3 we explain how to

Received by the editor October 18, 2000 and, in revised form, September 26, 2001.
2000 *Mathematics Subject Classification.* Primary 11Y40, 11R16, 11R29.

©2002 American Mathematical Society

construct tables of quartic A_4- and S_4-extensions of $\mathbb{Q}$. In Section 4 we explain the tools that we have used to *reduce* the equations that we obtain, which is an essential step in the process. Indeed, if this step were omitted, we could construct the tables much faster, but they would be totally unusable because the quartic equations would sometimes have 500-digit coefficients. In the final Section 5, we describe the computation that we have done up to discriminant 10^7 in absolute value, and we give tables describing some statistical data.

The reader should also refer to [9], which gives more theoretical results such as explicit Dirichlet series, concerning the construction of A_4- and S_4-extensions.

2. Construction of tables of imprimitive quartic fields

Since an imprimitive quartic field contains a quadratic subfield, we must explain how to construct relative quadratic extensions of quadratic fields. In fact, the construction can be done independently of the base field, although the fact that the base field is a quadratic field can be used to our advantage to speed up some computations.

2.1. **Relative quadratic extensions.** Let k be a number field, which will be our base field. We want to construct a table of quadratic extensions L of k *up to k-isomorphism*, having a relative discriminant $\mathfrak{d}(L/k)$ such that $\mathcal{N}(\mathfrak{d}(L/k)) \le X$ for a given bound X. Because of the discriminant-conductor relation $|d(L)| = d(k)^2\,\mathcal{N}(\mathfrak{d}(L/k))$ (where $d(K)$ denotes the discriminant of a number field K), this will give a complete table of number fields L which are extensions of k such that $|d(L)| \le d(k)^2 X$, but only up to k-isomorphism. Hence we will have to do a little extra work, since we usually want a table of fields L up to $\mathbb{Q}$-isomorphism. We will see later how this is (easily) done.

We consider two methods for constructing relative quadratic extensions of k. One is by using class field theory, the other by using Kummer theory. The method using class field theory is as follows. Since a quadratic extension L/k is Abelian, it has a conductor $\mathfrak{m}$, and L is isomorphic to the fixed field of the ray class field $k(\mathfrak{m})$ of conductor $\mathfrak{m}$ by a congruence subgroup $\overline{C}$ of index 2 in the ray class group $Cl_{\mathfrak{m}}(k)$. Furthermore, we have in this case the simple relation $\mathfrak{d}(L/k) = \mathfrak{m}_0$, where $\mathfrak{m}_0$ is the finite part of the conductor $\mathfrak{m}$.

Thus, we generate all possible conductors $\mathfrak{m}$ such that $\mathcal{N}(\mathfrak{m}) \le X$, and for each we compute the ray class group $Cl_{\mathfrak{m}}(k)$, all subgroups $\overline{C}$ of index 2, and finally the corresponding relative quadratic equation. All this can be done completely explicitly and reasonably efficiently (see [7], Chapter 9, and [11]). However, the computations are still quite costly; hence we have preferred to use Kummer theory.

In the case of quadratic extensions, Kummer theory is completely trivial and amounts to saying that such extensions are classified by elements of k^*/k^{*2} minus the unit class. We must simply find an efficient algorithmic way to generate representatives of such elements. If $\overline{\alpha} \in k^*/k^{*2}$, we can write in a unique way $\alpha\mathbb{Z}_k = \mathfrak{a}\mathfrak{q}^2$ with $\mathfrak{a}$ and $\mathfrak{q}$ ideals, and $\mathfrak{a}$ an integral squarefree ideal. It is clear that the ideal $\mathfrak{a}$ is independent of the chosen representative α of the class $\overline{\alpha}$, and that its class in the ordinary class group $Cl(k)$ is the square of the class of $\mathfrak{q}^{-1}$; hence is the square of a class.

Let $\mathfrak{a}$ be such an ideal, and fix some ideal $\mathfrak{q}_0$ and some element α_0 such that $\mathfrak{a}\mathfrak{q}_0^2 = \alpha_0\mathbb{Z}_k$. The set of elements $\overline{\alpha}$ of k^*/k^{*2} corresponding to $\mathfrak{a}$ as above is the set of $\overline{\alpha}$ such that $\alpha\mathbb{Z}_k = \mathfrak{a}\mathfrak{q}^2$ for some ideal $\mathfrak{q}$, or equivalently $\alpha = \alpha_0 u$ with

$u\mathbb{Z}_k = (\mathfrak{q}/\mathfrak{q}_0)^2$. Elements u such that $u\mathbb{Z}_k$ is the square of an ideal will be called *virtual units*, and the group of such elements modulo k^{*2} will be called the *Selmer group* (in fact the 2-Selmer group) $S(k)$ of k. Thus we see that elements of k^*/k^{*2} corresponding to a fixed ideal $\mathfrak{a}$ as above are in natural one-to-one correspondence with the elements of the Selmer group.

Note that it is easy to prove that the Selmer group is finite and that its cardinality is given by

$$|S(k)| = 2^{r(k)+i(k)+r_2(Cl(k))},$$

where $(r(k), i(k))$ denotes the signature of the number field k and $r_2(Cl(k))$ denotes the 2-rank of the class group $Cl(k)$ (see [7], Proposition 5.2.5).

If $(\mathfrak{a}, \overline{u})$ corresponds to an element of k^*/k^{*2}, the corresponding quadratic extension is $L = k(\sqrt{\alpha_0 u})$, where as above α_0 is such that $\mathfrak{a}\mathfrak{q}_0^2 = \alpha_0\mathbb{Z}_k$. We must then compute the relative discriminant of L/k, which can be done by using standard methods, or better, in this case, by using a simple instance of Hecke's theorem which gives the result directly (see [7], Chapter 10). We know that

$$\mathfrak{d}(L/k) = \frac{4\mathfrak{a}}{\mathfrak{c}^2}\ ,$$

where $\mathfrak{c}$ is the largest ideal (for divisibility) dividing 2, coprime to $\mathfrak{a}$ and such that the congruence $x^2 \equiv \alpha_0 u \pmod{{}^*\mathfrak{c}^2}$ is soluble (where $\mathfrak{q}_0$ and the lift u are chosen coprime to 2, and the congruence is taken in the usual multiplicative sense of class field theory). It follows that $\mathcal{N}(\mathfrak{a}) \le \mathcal{N}(\mathfrak{d}(L/k)) \le 4^n\,\mathcal{N}(\mathfrak{a})$, where $n = [k : \mathbb{Q}]$ ($n = 2$ in the case we have in mind). It follows that we will have to make a table of suitable ideals $\mathfrak{a}$ such that $\mathcal{N}(\mathfrak{a}) \le X$, but clearly when $\mathcal{N}(\mathfrak{a}) > X/4^n$, and especially when $\mathcal{N}(\mathfrak{a})$ is close to X, many elements $\overline{u}$ will be rejected; hence there is some waste here. We must make some comments about this.

(1) We have used above a one-to-one correspondence between quadratic extensions of k up to k-isomorphism and suitable pairs $(\mathfrak{a}, \overline{u})$. It is possible to refine this correspondence into one between quadratic extensions and suitable triplets $(\mathfrak{c}, \mathfrak{a}, \overline{u})$, where $\mathfrak{c}$ is as above, so that the relative discriminant is known in advance.

(2) This new correspondence leads to a more complicated although slightly faster implementation, but since our goal is to make complete tables of imprimitive *and* primitive extensions, the computations of S_4-extensions being by far the longest, we have not found it useful to spend too much implementation time here. If one is interested in relative extensions per se, the refined correspondence should probably be used.

(3) In the specific case where k is a quadratic field, which is the one we are most interested in, if we want to *count* suitable relative extensions instead of constructing them explicitly, the refined correspondence leads to very efficient counting methods which have enabled us to count imprimitive quartic fields up to discriminant 10^{17}, see [12].

For a detailed description of the algorithm, we refer to [7], Algorithm 9.2.3.

2.2. **Imprimitive quartic fields.** Although by laziness, because of remark (2) above we have not proceeded exactly as follows, let us explain how one should proceed to obtain complete tables of imprimitive quartic fields using tables of relative quadratic extensions.

First, we need to determine the Galois group of the Galois closure of the absolute extensions $L/\mathbb{Q}$ that we obtain. Thanks to our one-to-one correspondence, this is very easy. Let L correspond to a pair $(\mathfrak{a}, \overline{u})$, with $\mathfrak{a}\mathfrak{q}_0^2 = \alpha_0\mathbb{Z}_k$. If $\mathcal{N}(\alpha_0)$ is a square or, equivalently, if $\mathcal{N}(\mathfrak{a})$ is a square and $\mathcal{N}(\alpha_0)$ is positive, then $d(L)$ is a square, and hence the Galois group is necessarily isomorphic to V_4. If $\mathcal{N}(\alpha_0)$ is equal to $d(k)$ times a square (which can of course occur only if k is a real quadratic field) or, equivalently, if $\mathcal{N}(\mathfrak{a})$ is equal to $d(k)$ times a square and $\mathcal{N}(\alpha_0)$ is positive, the Galois group is isomorphic to C_4. In all other cases it is isomorphic to D_4.

We must now remove $\mathbb{Q}$-isomorphic fields. The C_4-extensions will be obtained exactly once, and for a single quadratic field k; hence there is nothing to check. The V_4-extensions will be obtained only once per quadratic field, but for exactly three different quadratic fields. However, if a V_4-extension is obtained for a pair $(\mathfrak{a}, \overline{u})$, since $\mathcal{N}(\mathfrak{a})$ is a square and $\mathfrak{a}$ is squarefree, we will have $\mathfrak{a} = \alpha_0\mathbb{Z}_k$ for $\alpha_0 \in \mathbb{Z}$. It follows that the two other quadratic fields giving isomorphic V_4-extensions will be $\mathbb{Q}(\sqrt{\alpha_0})$ and $\mathbb{Q}(\sqrt{\alpha_0 d(k)})$, so the isomorphisms between V_4-extensions are easily removed. Finally, the D_4-extensions will be obtained for a single quadratic field k, but exactly twice, corresponding to an element $\alpha_0 u$ and its conjugate under the unique nontrivial Galois automorphism τ of k. Note that for V_4-extensions $\alpha_0 u\tau(\alpha_0 u)$ is a square; hence $\tau(\alpha_0 u)$ defines the same extension as $\alpha_0 u$, and for C_4-extensions $\alpha_0 u\tau(\alpha_0 u) = \sqrt{d(k)}^2 x^2$ for some rational number x, and since $\sqrt{d(k)} \in k$, $\tau(\alpha_0 u)$ again defines the same extension as $\alpha_0 u$. Thus, when constructing the table of squarefree ideals $\mathfrak{a}$, which is done using a standard sieving method (see [7], Algorithm 2.3.24), we choose only one ideal in the pairs $(\mathfrak{a}, \tau(\mathfrak{a}))$. For such ideals $\mathfrak{a}$ with $\tau(\mathfrak{a}) \neq \mathfrak{a}$, we range through all elements $\overline{u}$ of $S(k)$. On the other hand, for ideals $\mathfrak{a}$ with $\tau(\mathfrak{a}) = \mathfrak{a}$, the element $v_0 = \tau(\alpha_0)/\alpha_0$ is a virtual unit, and when ranging over elements $\overline{u} \in S(k)$, we choose only one element in the pairs $(\overline{u}, \overline{v_0\tau(u)})$.

Once this is done, we have relative equations for our number fields, for which it is easy to compute an absolute equation, which we then reduce using one of the now standard polynomial reduction algorithms.

3. Construction of tables of primitive quartic fields

We now want to construct tables of *primitive* quartic fields $L/\mathbb{Q}$, in other words such that the Galois group of the Galois closure is isomorphic either to the alternating group A_4 or to the symmetric group S_4. We will do this by using the cubic resolvent and the corresponding Hasse diagram.

Let $L/\mathbb{Q}$ be a quartic field, let N be a Galois closure of $L/\mathbb{Q}$, and assume that the Galois group of $N/\mathbb{Q}$ is isomorphic either to A_4 or to S_4. Then N has a unique cubic subfield K, which is cyclic over $\mathbb{Q}$ for A_4-extensions, and noncyclic otherwise.

With this notation, we recall the following well-known theorem whose proof is a simple computation of conductors of induced characters.

Theorem 3.1. (1) *There exists a natural one-to-one correspondence between the set of isomorphism classes of primitive quartic extensions $L/\mathbb{Q}$ and the set of isomorphism classes of pairs (K, k), where K is a cubic extension of $\mathbb{Q}$ and k is a quadratic extension of K of square norm, in other words of the form $k = K(\sqrt{\alpha})$ with $\mathcal{N}_{K/\mathbb{Q}}(\alpha)$ a square in $\mathbb{Q}$.*

(2) *Under this correspondence, the A_4-extensions correspond to the cases where K is a cyclic cubic field, and in this case, if σ denotes a generator of* $\mathrm{Gal}(K/\mathbb{Q})$*, we must in particular identify (K,k) with $(K,\sigma^i(k))$ for $i=1$ and $i=2$.*

(3) *We have $d(L)=d(K)\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{d}(k/K))$.*

(4) *Let $k=K(\sqrt{\alpha})$ with α of square norm as above, and let $C_\alpha(X)=X^3-a_1X^2+a_2X-a_3$ be the characteristic polynomial of α in K, so that $a_3=\mathcal{N}_{K/\mathbb{Q}}(\alpha)$ is a square. An absolute equation for $L/\mathbb{Q}$ is given by the polynomial*

$$P(X)=X^4-2a_1\,X^2-8\sqrt{a_3}\,X+a_1^2-4a_2\,.$$

Furthermore, we have $\mathrm{disc}(P)=2^{12}\,\mathrm{disc}(C_\alpha)$.

To construct tables of primitive quartic fields of absolute discriminant up to some bound X, we therefore proceed as follows. Using the methods of K. Belabas [1] for noncyclic cubic fields, or simple direct constructions for cyclic cubic fields, we generate a table of suitable cubic fields of discriminant up to X. Note that, since we are going to treat each cubic field independently, it is not necessary to store the table of cubic fields (which may be huge). For each cubic field K, we then proceed as follows.

We first compute the group of virtual units coprime to 2 and of square norm. To do this, let

$$Cl(K)=\bigoplus_{1\le i\le g}(\mathbb{Z}/d_i\mathbb{Z})\overline{\mathfrak{a}_i}$$

for some integral ideals $\mathfrak{a}_i$, and let d_i be even if and only if $1\le i\le r$. Multiplying by suitable elements (see [7], Algorithm 1.3.14), we may assume that the $\mathfrak{a}_i$ are coprime to 2. Using the principal ideal algorithm, we can compute v_i for $1\le i\le r$ such that $\mathfrak{a}_i^{d_i}=v_i\mathbb{Z}_K$, and we change v_i into $-v_i$ if the norm of v_i is minus a square (here and afterwards, we of course use the fact that $[K:\mathbb{Q}]=3$ is odd). If $(\varepsilon_1,\dots,\varepsilon_{r_u})$ is a system of fundamental units of K (with $r_u=1$ or 2), where as before we may assume that the ε_i are of norm 1, then the v_i for $1\le i\le r$ together with the ε_i for $1\le i\le r_u$ form a basis of the group of virtual units of square norm modulo squares.

However, at this stage it is essential to be careful about computational issues: we cannot do much about the size of the fundamental units ε_i. On the other hand, if the virtual units v_i are chosen carelessly, we will have huge coefficients.

For each i such that $1\le i\le r$, to compute a suitable v_i we proceed as follows. We first compute the ideal $\mathfrak{b}_i'=\mathfrak{a}_i^{d_i/2}$, and we then set $\mathfrak{b}_i=\gamma_i\mathfrak{b}_i'$ for a suitable element γ_i so that $\mathfrak{b}_i$ is integral and coprime to 2, using [7], Algorithm 1.3.14 (note that $\mathfrak{a}_i$ and 2 may not be coprime). We then use an *ideal reduction algorithm*, such as [7], Algorithm 4.3.4, to find an integral ideal $\mathfrak{c}_i$ in the same ray ideal class modulo 2 as $\mathfrak{b}_i$, but much "smaller" in a suitable sense. An alternate procedure would be to compute directly an ideal $\mathfrak{c}_i'$ in the same ordinary ideal class as $\mathfrak{b}_i'$ (using the same algorithm), and only then computing an ideal $\mathfrak{c}_i$ of the form $\gamma_i'\mathfrak{c}_i'$ coprime to 2 using [7], Algorithm 1.3.14. This would almost certainly give a worse ideal $\mathfrak{c}_i$, so we do not advise using it.

Finally, we apply the principal ideal algorithm to the ideal $\mathfrak{c}_i^2$, thus finding (we hope) a small v_i such that $\mathfrak{c}_i^2 = v_i\mathbb{Z}_K$. This procedure clearly gives much smaller virtual units than the direct application of the definitions.

Once the virtual units are constructed, we must generate the ideals. By a sieving procedure analogous to [7], Algorithm 2.3.24, we generate all squarefree ideals $\mathfrak{a}$ of K whose norm is a square less than or equal to $X/|d(K)|$. Such ideals are coprime products of ideals which are either of the form $\mathfrak{p}_i\mathfrak{p}_j$ with $i \neq j$, where p is a prime number totally split in K as $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, or of the form $\mathfrak{p}_1\mathfrak{p}_2$, where p is partially ramified in K as $p\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2$, or of the form $\mathfrak{p}_2$, where p is partially split in K as $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_i$ of degree i. Of course, if K is cyclic cubic, only the first type of ideals occur.

Once these ideals $\mathfrak{a}$ are generated, we weed out those whose class does not belong to $Cl(K)^2$ by applying the principal ideal algorithm (see for example [6], Chapter 6) already used for computing the virtual units v_i. For each ideal $\mathfrak{a}$ whose class is in $Cl(K)^2$, we compute an ideal $\mathfrak{q}_0$ coprime to 2 (which we do not keep) and an element α_0 such that $\mathfrak{a}\mathfrak{q}_0^2 = \alpha_0\mathbb{Z}_K$, and by changing if necessary α_0 into $-\alpha_0$, we may assume that $\mathcal{N}(\alpha_0)$ is a square.

Then for each u belonging to the finite group (of cardinality 2^{r+r_u}) generated by the v_i and ε_i modulo squares, we have a quadratic extension $k = K(\sqrt{\alpha})$ with trivial norm and with $\alpha = \alpha_0 u$, and the corresponding quartic extension has discriminant equal to

$$d(L) = d(K)\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{d}(k/K)).$$

We have $\mathfrak{d}(k/K) = 4\mathfrak{a}/\mathfrak{c}^2$, where, as in the preceding section, $\mathfrak{c}$ is the largest ideal dividing 2 and coprime to $\mathfrak{a}$ such that $x^2 \equiv \alpha \pmod{{}^*\mathfrak{c}^2}$ has a solution. Thus, especially when the norm of $\mathfrak{a}$ is close to the upper bound $X/|d(K)|$, we may have some virtual units u giving extensions of discriminant larger than X, which we must of course discard. If the discriminant is suitable, we then compute the quartic equation for the field L by using Theorem 3.1.

As in the imprimitive case, we could use a refined one-to-one correspondence where, instead of using pairs $(\mathfrak{a}, \overline{u})$ of squarefree ideals of square norm whose class belong to $Cl(K)^2$ and classes of virtual units of square norm, we use triplets $(\mathfrak{c}, \mathfrak{a}, \overline{u})$, where $\mathfrak{c}$ is an ideal dividing 2. This correspondence would avoid computing $\mathfrak{d}(k/K)$ by Hecke's theorem or, equivalently, each individual ideal $\mathfrak{c}$. However, almost all of the time is spent in computing the virtual units and the list of squarefree ideals, in other words in the computation of the class and unit group of K and in the principal ideal algorithm; hence we have not done so.

4. Reducing the equation

By using the procedure above, we have obtained completely explicit absolute equations for the desired number fields. One notices immediately that in practice the coefficients of these equations can be rather large, with several hundred decimal digits. In particular, the discriminant of the polynomial can be even larger; hence it is completely out of the question to try to factor it, hence to use a polynomial reduction algorithm as we can do in milder cases, such as in the imprimitive quartic case. Thus, we must look for a better method.

Recall that our quartic extension $L/\mathbb{Q}$ comes from a quadratic extension $K(\sqrt{\alpha})$, where K is a cubic number field and $\mathcal{N}(\alpha)$ is a square in $\mathbb{Q}$. Thus, to reduce our equation, it is enough to find a simpler α, and since the discriminant of our quartic equation is equal to 2^{12} times the discriminant of the characteristic polynomial of α, this is the quantity that we have to reduce.

The only freedom that we have with α is to multiply it by a square γ^2, and since we want to preserve integrality of our equations, the element $\alpha\gamma^2$ must still be an algebraic integer. After many trials, we have obtained the following reduction method, which works very well and, at least up to discriminant 10^7, has enabled us to find completely reduced quartic equations using a polynomial reduction algorithm on the simplified equation. We emphasize that this method is completely heuristic, but based on reasonable principles.

Considering what has been said above, we first measure the *size* of an algebraic integer α as the absolute value of the discriminant of its characteristic polynomial. The aim is to reduce this size by multiplying α by suitable squares.

First, we note that, as soon as the size of α is less than 10^{40}, say, it will be easy to find a reduced equation using a polynomial reduction algorithm, since factoring a 40-digit number is nowadays very fast (1 or 2 seconds). We will thus use this as a stopping criterion.

Second, we compute the ideal factorization of α as

$$\alpha\mathbb{Z}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}} ,$$

and we set

$$\mathfrak{q}_0 = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor a_{\mathfrak{p}}/2 \rfloor} .$$

This is the largest ideal such that $\mathfrak{q}_0^2 \mid \alpha\mathbb{Z}_K$. Note that, considering the way in which α has been computed, when the class group of K is large the exponents $a_{\mathfrak{p}}$ may be large, hence $\mathfrak{q}_0$ also.

We now use an ideal reduction algorithm such as [6], Algorithm 6.5.5, to compute an element β such that $\mathfrak{q}_1 = \mathfrak{q}_0/\beta$ is an integral ideal which is in some sense reduced, meaning at least that it should be rather "small". If we set $\alpha_1 = \alpha/\beta^2$, we have

$$\alpha_1\mathbb{Z}_K = (\mathfrak{q}_0/\beta)^2(\alpha\mathbb{Z}_K/\mathfrak{q}_0^2) = \mathfrak{q}_1^2(\alpha\mathbb{Z}_K/\mathfrak{q}_0^2);$$

hence α_1 is still an algebraic integer, which we hope has a smaller size than α, in which case we replace α by α_1.

Whether or not this is the case, we proceed to a third step. Although we could multiply α by randomly chosen squares of algebraic integers, we proceed as follows. We make a list of elements of three different types. The first is a basis of the ordinary unit group. These elements can of course be raised to positive or negative exponents and remain algebraic integers, while the other elements that we will add will have to be raised to nonnegative exponents. Second, we complement this to a basis of the Selmer group, by adding suitable virtual units. These two types of elements are natural, but far from sufficient. We finally add elements of a third type, which are S-units for small finite sets S. More precisely, for every prime ideal $\mathfrak{p}$ of degree 1 and of reasonably small norm (less than or equal to 1000, say), we check if $\mathfrak{p}$ is a principal ideal. If it is, we add a generator of $\mathfrak{p}$ (found by a principal ideal algorithm) to our list of elements. We continue this process until we find $\min(10, \lfloor 50/h(K) \rfloor)$ elements, where $h(K) = |Cl(K)|$ is the class number of K, or

until the bound 1000 is exhausted. The rationale for this number is as follows: if the class number is small, it will be very easy to find suitable elements, and we do not want too large a loop afterwards, so we stop at 10. On the other hand, if the class number is large, it will be difficult to find principal prime ideals of degree 1, and the probability of finding one is roughly proportional to $1/h(K)$, whence the $50/h(K)$, which is reasonable.

Once we have this list of elements, we multiply α by the square of a product of these elements raised to the power -1, 0 or 1 for units, or to the power 0 or 1 for the other elements. This is done by a standard backtracking process, but it should be emphasized that one should first search with as many 0-exponents as possible among the elements of the third type. We of course keep the product which gives the smallest size.

Once all the elements have been tried, we check whether the size of α has decreased since the first step. If this is the case, we go back to the first step, and start again with the smaller value of α. If not, we cannot reduce α anymore, and hope that it has become small enough so that its characteristic polynomial can be treated using a polynomial reduction algorithm. In the tables that we have made up to 10^7, it occurred only four times that the discriminant of this characteristic polynomial had more than 70 decimal digits, and in these four cases it was possible to factor the discriminant, hence to reduce the polynomial.

5. A table of quartic fields of discriminants up to 10^7

Using the methods above, in about 1 month of CPU time on a Pentium III 600 Mhz workstation we have constructed complete tables of quadratic number fields L such that $|d(L)| \leq 10^7$, which is 10 times larger than the published tables [16], [4], [5] obtained about 10 years ago using the geometry of numbers. It is quite plausible that one could construct tables up to 10^7 using the geometry of numbers, although this may be a difficult task, not so much because of the amount of time, but more because of the sheer number of polynomials which would have to be considered. Evidently, our method is much more elegant, and could be used for even larger discriminants if desired. It is limited to quartic number fields, although it can also be used for larger degree number fields if we add certain limitations on the Galois group.

The complete tables, which include a reduced polynomial equation, the signature, Galois group, discriminant, and the class and unit groups, can be obtained by anonymous ftp from the URL

`ftp://megrez.math.u-bordeaux.fr/pub/numberfields/degree4long`

In the following tables, we summarize the statistical data obtained for each signature and Galois group. The tables up to 10^6 were of course already known.

Table 1. Summary of data for 10^3

Sign : Gal	C_4	V_4	D_4	A_4	S_4	Total
$(4,0)$	0	0	1	0	0	1
$(2,1)$	—	—	6	—	10	16
$(0,2)$	1	8	17	0	8	34
Total	1	8	24	0	18	51

TABLE 2. Summary of data for 10^4

Sign : Gal	C_4	V_4	D_4	A_4	S_4	Total
$(4,0)$	6	6	25	0	13	50
$(2,1)$	—	—	93	—	351	444
$(0,2)$	4	41	295	4	206	550
Total	10	47	413	4	570	1044

TABLE 3. Summary of data for 10^5

Sign : Gal	C_4	V_4	D_4	A_4	S_4	Total
$(4,0)$	15	42	379	4	449	889
$(2,1)$	—	—	968	—	5916	6884
$(0,2)$	17	201	3417	23	3374	7032
Total	32	243	4764	27	9739	14805

TABLE 4. Summary of data for 10^6

Sign : Gal	C_4	V_4	D_4	A_4	S_4	Total
$(4,0)$	59	196	4486	31	8301	13073
$(2,1)$	—	—	9772	—	80899	90671
$(0,2)$	54	818	36238	90	44122	81322
Total	113	1014	50496	121	133322	185066

TABLE 5. Summary of data for 10^7

Sign : Gal	C_4	V_4	D_4	A_4	S_4	Total
$(4,0)$	182	876	47562	129	120622	169371
$(2,1)$	—	—	98413	—	989587	1088000
$(0,2)$	181	3331	370424	385	525099	899420
Total	363	4207	516399	514	1635308	2156791

Remark. Denote by $N_{R,I}(G,X)$ the number of quartic extensions of $\mathbb{Q}$ of signature (R,I), of Galois group of a Galois closure isomorphic to G, and absolute value of the discriminant less than or equal to X, and omit the subscript (R,I) if all signatures are considered together. Thanks to work of several people including the authors, precise asymptotic estimates for many of these numbers are now known, and other are conjectured (see [3], [8], [12], [13], [18]). For the convenience of the reader, we recall these estimates in a weaker and shorter form. Refer to the cited papers for

more precise estimates.

$$\begin{aligned}
N(C_4,X) &\sim c(C_4)\,X^{1/2} \quad \text{with} \quad c(C_4) = 0.12205267325139676...,\\
N_{4,0}(C_4,X) &\sim N_{0,2}(C_4,X) \sim N(C_4,X)/2,\\
N(V_4,X) &\sim c(V_4)\,X^{1/2}\log^2 X \quad \text{with} \quad c(V_4) = 0.002752430222755481...,\\
N_{4,0}(V_4,X) &\sim N(V_4,X)/4, \quad N_{0,2}(V_4,X) \sim 3N(V_4,X)/4,\\
N(D_4,X) &\sim c(D_4)\,X \quad \text{with} \quad c(D_4) = 0.052326011...,\\
N_{4,0}(D_4,X) &\sim (c^+(D_4)/4)\,X \quad \text{with} \quad c^+(D_4) = 0.019711375...,\\
N_{2,1}(D_4,X) &\sim 2N_{4,0}(D_4,X),\\
N_{0,2}(D_4,X) &\sim (c(D_4) - 3c^+(D_4)/4)\,X,\\
N(A_4,X) &\sim c(A_4)\,X^{1/2}\log X \quad \text{with} \quad c(A_4) = 0.0179...,\\
N_{4,0}(A_4,X) &\sim c_0(A_4)\,X^{1/2}\log X \quad \text{with} \quad c_0(A_4) = 0.0048...,\\
N_{0,2}(A_4,X) &\sim c_2(A_4)\,X^{1/2}\log X \quad \text{with} \quad c_2(A_4) = 0.0131...,\\
N(S_4,X) &\sim c(S_4)\,X \quad \text{with} \quad c(S_4) = 0.23446635737257419...,\\
N_{4,0}(S_4,X) &\sim N(S_4,X)/10, \quad N_{2,1}(S_4,X) \sim 3N(S_4,X)/5,\\
N_{0,2}(S_4,X) &\sim 3N(S_4,X)/10.
\end{aligned}$$

In the above, the estimates for A_4 are conjectures due to the authors, and the proven results for S_4 are due to M. Bhargava [3] (see also the work of A. Yukie [18]).

In addition, in [13], we have computed extensive tables of the quantities $N_{R,I}(G, 10^k)$ for $G = C_2$ and $k \le 25$, $G = C_3$ and $k \le 37$, $G = C_4$ and $k \le 32$, $G = V_4$ and $k \le 36$, $G = D_4$ and $k \le 17$, $G = A_4$ and $k \le 13$, as well as $G = S_4$ and $k \le 7$ as above (tables for $G = S_3$ are given in [1]).

References

1. K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), 1213–1237. MR **97m:**11159
2. A.-M. Bergé, J. Martinet, and M. Olivier, *The computation of sextic fields with a quadratic subfield*, Math. Comp. **54** (1990), 869–884. MR **90k:**11169
3. M. Bhargava, *Gauss Composition and Generalizations*, Proceedings ANTS V, Sydney (2002), Lecture Notes in Comp. Sci., Springer-Verlag (2002), to appear.
4. J. Buchmann and D. Ford, *On the computation of totally real quartic fields of small discriminant*, Math. Comp. **52** (1989), 161–174. MR **89f:**11147
5. J. Buchmann, D. Ford, and M. Pohst, *Enumeration of quartic fields of small discriminant*, Math. Comp. **61** (1993), 873–879. MR **94a:**11164
6. H. Cohen, *A Course in Computational Algebraic Number Theory (third printing)*, Graduate Texts in Math. **138**, Springer-Verlag, 1996. MR **94i:**11105 (1st printing)
7. ———, *Advanced Topics in Computational Number Theory*, Graduate Texts in Math. **193**, Springer-Verlag, 2000. MR **2000k:**11144
8. H. Cohen, F. Diaz y Diaz and M. Olivier, *Density of number field discriminants*, in preparation.
9. ———, *Construction of tables of quartic fields*, Proceedings ANTS IV, Leiden (2000), Lecture Notes in Comp. Sci. **1838**, Springer-Verlag (2000), 257–268.
10. ———, *Tables of octic fields with a quartic subfield*, Math. Comp. **68** (1999), 1701–1716. MR **99m:**11132
11. ———, *Computing ray class groups, conductors and discriminants*, Math. Comp. **67** (1998), 773–795. MR **98g:**11128
12. ———, *Enumerating quartic dihedral extensions of* $\mathbb{Q}$, Compositio Math., to appear.

13. ———, *Counting discriminants of number fields*, in preparation.
14. H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields (I)*, Bull. London Math. Soc. **1** (1969), 345–348. MR **40:**7223
15. ———, *On the density of discriminants of cubic fields (II)*, Proc. Roy. Soc. London **322** (1971), 405–420. MR **58:**10816
16. D. Ford, *Enumeration of totally complex quartic fields of small discriminant*, Computational Number Theory (1989) (A. Pethö, M. Pohst, H. C. Williams, and H. Zimmer, eds.), de Gruyter, Berlin and New York (1991), 129–138. MR **93b:**11140
17. M. Olivier, *The computation of sextic fields with a cubic subfield and no quadratic subfield*, Math. Comp. **58** (1992), 419–432. MR **92e:**11119
18. A. Yukie, *Density theorems related to prehomogenous vector spaces*, preprint in English; also in Swikaisekikenkiyosho Kokyuroku, No. 1173 (2000), 171–183 (Japanese).

Laboratoire A2X, U.M.R. 5465 du C.N.R.S., Université Bordeaux I, 351 Cours de la Libération, 33405 Talence Cedex, France
E-mail address: cohen@math.u-bordeaux.fr

Laboratoire A2X, U.M.R. 5465 du C.N.R.S., Université Bordeaux I, 351 Cours de la Libération, 33405 Talence Cedex, France
E-mail address: diaz@math.u-bordeaux.fr

Laboratoire A2X, U.M.R. 5465 du C.N.R.S., Université Bordeaux I, 351 Cours de la Libération, 33405 Talence Cedex, France
E-mail address: olivier@math.u-bordeaux.fr