

## TABLES OF OCTIC FIELDS WITH A QUARTIC SUBFIELD

H. COHEN, F. DIAZ Y DIAZ, AND M. OLIVIER

ABSTRACT. We describe the computation of extended tables of degree 8 fields with a quartic subfield, using class field theory. In particular we find the minimum discriminants for all signatures and for all the possible Galois groups. We also discuss some phenomena and statistics discovered while making the tables, such as the occurrence of 11 non-isomorphic number fields having the same discriminant, or several pairs of non-isomorphic number fields having the same Dedekind zeta function.

### 1. INTRODUCTION

The construction of tables of number fields has a long history, and is useful in two ways. First, to test the algorithms available for such constructions, and second and probably most importantly, to give to researchers a vast amount of data that they can examine and on which they can make conjectures. Large tables are now available on the internet by anonymous ftp, either from the Kant group ([ftp.math.tu-berlin.de](ftp://ftp.math.tu-berlin.de)) or from our group, the Pari group (<megrez.math.u-bordeaux.fr>).

The tables are built in the following way. In degree 2, we simply need to find squarefree numbers up to a certain bound, and considering the bounds that we must take to be realistic, this is not a problem. In degree 3, it was previously thought that only the general methods were available, but it was observed recently by K. Belabas (see [Be]) that one can adapt methods of Davenport and Heilbronn to the algorithmic construction of cubic fields in time comparable to that of quadratic fields. Thus, computation of tables of cubic fields is now also easy (tables have been built up to discriminant  $10^{11}$ ). In higher degrees, the only methods known to construct general tables of number fields are based on the geometry of numbers. These methods are highly inefficient, since they require looking at orders of magnitudes more polynomials than necessary, but they are the only ones available in general. Large tables exist for degrees 4, 5 and 6, small tables in degree 7, and in degree 8 only the first few minima are known in signatures  $(8, 0)$  and  $(0, 4)$ , and the minima for the other signatures are not even known without assuming the GRH.

If one considers *imprimitive* fields, the situation improves considerably, since, thanks to a relative version of the theorem used in the absolute case due to J. Martinet, we can do all our work using relative data. For example, although it

---

Received by the editor November 20, 1997.

1991 *Mathematics Subject Classification*. Primary 11R37, 11Y40.

*Key words and phrases*. Class field theory, discriminant, number field.

©1999 American Mathematical Society

required a huge amount of work, we now have large tables of degree 9 fields containing a cubic subfield (see [Di-Ol]). One could reasonably do this for degree 8 fields containing a quadratic or quartic subfield, but it has not been done.

Another approach to the computation of imprimitive fields is to use class field theory. Recall that class field theory gives an explicit description of all finite *Abelian* extensions of a number field. Thus, for example, we can use class field theory to compute all quadratic extensions of a given base field, since such extensions are Abelian, and this is what will be described in this paper when the base field has degree 4, thus giving number fields of degree 8. One could of course also apply this to base fields of degree 2 or 3 (but extensive tables have already been done in this case), or to base fields of degree larger than 4.

In the following sections, we describe the methods used for constructing the tables, and then give a number of observations, statistical or otherwise, obtained when constructing the tables (some of these observations are not visible on the tables themselves, but were made during the construction of the tables).

## 2. CONSTRUCTION OF THE TABLES

(A). **Results from class field theory.** We give the definitions and results “à la Hasse”, i.e., without using ideles. This is much better suited to algorithmic practice. See [Ha] and a forthcoming book by the first author.

Let  $K$  be a fixed base number field. For any modulus  $\mathfrak{m}$  (i.e., a pair formed by an integral ideal  $\mathfrak{m}_0$  and a set of real places  $\mathfrak{m}_\infty$  of  $K$ ), let  $I_{\mathfrak{m}}(K)$  be the group of fractional ideals of  $K$  coprime to  $\mathfrak{m}$ , let  $P_{\mathfrak{m}}(K)$  be the group of principal ideals generated by an element  $\alpha \equiv 1 \pmod{* \mathfrak{m}}$ , and let  $Cl_{\mathfrak{m}}(K) = I_{\mathfrak{m}}(K)/P_{\mathfrak{m}}(K)$  be the ray class group.

A *congruence subgroup* is any group of ideals  $C$  such that  $P_{\mathfrak{m}}(K) \subset C \subset I_{\mathfrak{m}}(K)$ . One of the fundamental theorems of class field theory tells us that equivalence classes of pairs  $(\mathfrak{m}, C)$  (for a suitable equivalence relation) are in canonical one-to-one correspondence with  $K$ -isomorphism classes of finite Abelian extensions  $L/K$ , satisfying in particular

$$\text{Gal}(L/K) \simeq I_{\mathfrak{m}}(K)/C \simeq Cl_{\mathfrak{m}}(K)/\overline{C}, \quad \text{where } \overline{C} = C/P_{\mathfrak{m}}(K).$$

In [Co-Di-Ol], we described an efficient method to compute the ray class group  $Cl_{\mathfrak{m}}(K)$ , and to compute the discriminant (relative or absolute), signature and conductor of the corresponding Abelian extension as above. Briefly we proceed as follows. We first note the following (easy) exact sequence:

$$U(K) \rightarrow (\mathbb{Z}_K/\mathfrak{m})^* \rightarrow Cl_{\mathfrak{m}}(K) \rightarrow Cl(K) \rightarrow 1.$$

We first compute the ordinary class group  $Cl(K)$  and unit group  $U(K)$  using the methods that can be found in [Co] or in [Po-Za]. We then compute  $(\mathbb{Z}_K/\mathfrak{m})^*$  using the methods explained in [Co-Di-Ol]. Finally, using the methods explained in that paper for dealing with exact sequences which are not necessarily split, we obtain a complete description of the group  $Cl_{\mathfrak{m}}(K)$  by minimal generators and relations.

Let  $(\mathfrak{m}, C)$  be a congruence subgroup and let  $L/K$  be the Abelian extension which corresponds to  $(\mathfrak{m}, C)$  by class field theory. Assume that  $\mathfrak{m}$  is the conductor, i.e., that  $(\mathfrak{m}, C)$  is minimal in its equivalence class. We know in particular that  $\text{Gal}(L/K) \simeq Cl_{\mathfrak{m}}(K)/\overline{C}$ , and that the prime ideals of  $K$  which ramify in  $L$  are exactly those dividing  $\mathfrak{m}$ . We also know precisely the signature and discriminant of  $L$ , thanks to the following theorem proved in [Co-Di-Ol].

**Theorem 1.** *Let  $L/K$  be the (equivalence class of) an Abelian extension corresponding to the congruence subgroup  $(\mathfrak{m}, C)$  by class field theory, where  $\mathfrak{m}$  is not necessarily assumed to be the conductor.*

*Denote by  $\mathfrak{d}(L/K)$  the relative discriminant ideal of  $L/K$ , and write*

$$\mathfrak{m}_0 = \prod_{\mathfrak{p}|\mathfrak{m}_0} \mathfrak{p}^{v_{\mathfrak{p}}}.$$

*For any divisor  $\mathfrak{n}$  of  $\mathfrak{m}$ , let  $h_{\mathfrak{n},C}$  be the cardinality of  $Cl_{\mathfrak{n}}(K)/s(\overline{C})$ , where  $s$  is the natural surjection from  $Cl_{\mathfrak{m}}(K)$  to  $Cl_{\mathfrak{n}}(K)$  (in particular,  $[L : K] = h_{\mathfrak{m},C}$ ). Then  $\mathfrak{d}(L/K) = \prod_{\mathfrak{p}|\mathfrak{m}_0} \mathfrak{p}^{a_{\mathfrak{p}}}$ , with*

$$a_{\mathfrak{p}} = v_{\mathfrak{p}} h_{\mathfrak{m},C} - \sum_{1 \leq i \leq v_{\mathfrak{p}}} h_{\mathfrak{m}/\mathfrak{p}^i, C}.$$

*If, in addition,  $\mathfrak{m}$  is the conductor, we have the following:*

- (1) *If  $h_{\mathfrak{m},C} = [L : K] = \ell$  is prime, then  $\mathfrak{d}(L/K) = \mathfrak{m}_0^{\ell-1}$ .*
- (2) *Denote by  $m_{\infty}$  the number of real places in the modulus  $\mathfrak{m}$ , and by  $(r_1, r_2)$  (resp.  $(R_1, R_2)$ ) the signature of  $K$  (resp.  $L$ ). Then  $R_2 = h_{\mathfrak{m},C}(m_{\infty}/2 + r_2)$ .*
- (3) *The absolute discriminant  $d(L)$  is given by*

$$d(L) = (-1)^{m_{\infty} h_{\mathfrak{m},C}/2} d(K)^{h_{\mathfrak{m},C}} \mathcal{N}(\mathfrak{d}(L/K)).$$

(B). **Finding all suitable pairs  $(\mathfrak{m}, C)$ .** Let  $K$  be a fixed quartic field and let  $L$  be an octic field obtained by class field theory as a quadratic extension of  $K$  corresponding to the pair  $(\mathfrak{m}, C)$ . Since we will restrict to the case where  $\mathfrak{m}$  is the conductor, Theorem 1 tells us that  $\mathfrak{m}_0 = \mathfrak{d}(L/K)$ , hence that  $|d(L)| = d(K)^2 \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{m}_0)$ . Thus, if we want to compute octic fields such that  $|d(L)| \leq B$  for a certain bound  $B$ , it is enough to consider all quartic fields  $K$  such that  $|d(K)| \leq B^{1/2}$ , and for each such quartic field all moduli such that  $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{m}_0) \leq B/d(K)^2$ . Furthermore, to obtain the correct signature, we have to include in  $\mathfrak{m}$  exactly the correct number of ramified real places (more precisely, if we want  $R_1$  real places in  $L$ , we must take  $K$  with  $r_1 \geq R_1/2$  real places and exactly  $r_1 - R_1/2$  of those real places dividing  $\mathfrak{m}$ ).

For a given quartic field  $K$ , we construct all integral ideals of norm up to a given bound by a recursive procedure similar to the sieve of Erathosthenes. We initialize the procedure by saying that there is a single ideal of norm 1, i.e.,  $\mathbb{Z}_K$ . Then, we split each prime number up to the bound into a product of prime ideals in  $K$ , and multiply each of the already obtained ideals by successive powers of the prime ideals, as long as the norm of the results are less than the given bound. This gives a very efficient procedure, although the amount of storage can become large (for some of our computations, we have had to use a bound close to  $10^6$ , and this can give storage of several hundred megabytes).

For each of the moduli, we then compute the class group  $Cl_{\mathfrak{m}}(K)$  using the method explained in [Co-Di-Ol]. We can also do this in a similar recursive procedure to speed up the computation. Furthermore, since we do this recursively, it is easy to eliminate from the list of moduli those for which  $(\mathfrak{m}, P_{\mathfrak{m}})$  is not a conductor. Indeed, a very easy lemma tells us that if  $\mathfrak{m}$  is the conductor for *some* congruence group  $C$ , then it is the conductor for  $P_{\mathfrak{m}}$ .

For each remaining modulus  $\mathfrak{m}$ , we compute all the subgroups  $\overline{C}$  of  $Cl_{\mathfrak{m}}(K)$  of index 2, using the method explained in [Co-Di-Ol]. If  $E$  is the diagonal matrix in Smith normal form giving the structure of  $Cl_{\mathfrak{m}}(K)$ , this amounts to finding all

integer matrices  $H$  in Hermite normal form such that  $H^{-1}E$  is an integer matrix, and  $\det(H) = 2$ . If the diagonal entries of  $E$  are  $(e_i)$  with  $e_{i+1}|e_i$ , let  $r$  be the largest index such that  $e_i$  is even (0 if none exist), so that  $r$  is equal to the 2-rank of  $Cl_{\mathfrak{m}}(K)$ . It is easy to show that the possible matrices  $H = (h_{i,j})$  are exactly those matrices such that there exists an integer  $i_0$  satisfying the following conditions:

- (1)  $i_0 \leq r$ .
- (2)  $h_{i,i} = 1$  if  $i \neq i_0$  and  $h_{i_0,i_0} = 2$ .
- (3)  $h_{i_0,j} = 0$  or  $1$  if  $i_0 < j \leq r$ .
- (4)  $h_{i,j} = 0$  for all other pairs  $(i, j)$ .

There are  $2^r - 1$  such matrices, corresponding to the  $2^r - 1$  subgroups of index 2 of a group of 2-rank equal to  $r$ . We keep only the subgroups  $\overline{C}$  for which  $\mathfrak{m}$  is equal to the conductor of  $(\mathfrak{m}, C)$ .

By class field theory, the pairs  $(\mathfrak{m}, C)$  thus found are in one-to-one correspondence with  $K$ -isomorphism classes of quadratic extensions of  $K$ . Note that, even though two different pairs will correspond to two fields  $L$  which are not  $K$ -isomorphic, they may of course be  $\mathbb{Q}$ -isomorphic. Furthermore, different quartic fields may give isomorphic octic fields. However, at this state we do not worry about this problem, since, unlike the methods using the geometry of numbers, the number of polynomials that we will have to remove because of isomorphisms will not be very large.

(C). **Finding the polynomial equations.** For a given base quartic field  $K$ , we now have a large number of pairs  $(\mathfrak{m}, C)$ , and we know that  $\mathfrak{m}$  is the conductor of the equivalence class of  $(\mathfrak{m}, C)$ . We must find the relative and absolute equations of the quadratic extension  $L/K$  corresponding to  $(\mathfrak{m}, C)$ . We do this by using Kummer theory, which is the standard method for this kind of computation (although if  $K$  is totally real, we can also use Stark's conjecture, see [Ro]). Here we are in a very favorable case, since the square roots of unity are already in our field  $K$ , so we do not need to adjoin them.

We need some notation.

If  $\mathfrak{p}$  is a prime ideal of  $K$ , let  $z(\mathfrak{p}) = 2e(\mathfrak{p}/2) + 1$ , where  $e(\mathfrak{p}/2) = 0$  when  $\mathfrak{p}$  is not a prime above 2.

We define seven sets of prime ideals associated to  $\mathfrak{m}$  as follows:

- (1)  $S_{\mathfrak{m},1}$  (resp.  $S_{\mathfrak{m},2}$ , resp.  $S_{\mathfrak{m},3}$ ) is the set of prime ideals  $\mathfrak{p}$  of  $K$  which divide both 2 and  $\mathfrak{m}$ , and such that  $v_{\mathfrak{p}}(\mathfrak{m}) = z(\mathfrak{p})$  (resp.  $v_{\mathfrak{p}}(\mathfrak{m}) < z(\mathfrak{p})$ , resp.  $v_{\mathfrak{p}}(\mathfrak{m}) > z(\mathfrak{p})$ ).
- (2)  $S_2$  (resp.  $S_{\mathfrak{m}}$ ) is the set of all prime ideals dividing 2 and not  $\mathfrak{m}$  (resp. dividing  $\mathfrak{m}$  and not 2).
- (3)  $S_{\emptyset}$  is the set of all prime ideals dividing neither  $\mathfrak{m}$  nor 2.
- (4)  $S = S_{\mathfrak{m}} \cup S_{\mathfrak{m},1}$ .

Let

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

be the ordinary class group of  $K$ , where the  $d_i$  are ordered so that  $d_{i+1}|d_i$ , and assume that the representatives of the ideal classes  $\overline{\mathfrak{a}}_i$  are chosen to be integral ideals coprime to the ideal  $2\mathfrak{m}$  (this can always be done). Let  $\alpha_i$  be elements such that  $\mathfrak{a}_i^{d_i} = \alpha_i\mathbb{Z}_K$ . These  $\alpha_i$  can easily be found using the solution to the *principal*

ideal problem (see [Co]), and by our assumption will be coprime to  $\mathfrak{m}$ . Let  $h$  be the largest index (0 if none exist) such that  $d_i$  is even.

For each  $\mathfrak{p} \in S$ , we can write

$$\mathfrak{p} = \beta_{\mathfrak{p}} \prod_{1 \leq i \leq g} \alpha_i^{p_{i,\mathfrak{p}}},$$

again by using the solution to the principal ideal problem.

By Theorem 1, since  $\mathfrak{m}$  is the conductor and the relative degree is equal to 2, the relative discriminant  $\mathfrak{d}(L/K)$  is equal to  $\mathfrak{m}$ . Using Hecke's theorem on ramification in Kummer extensions of prime degree, it is not difficult to prove the following theorem (see for example [Co-Di-Ol]).

**Theorem 2.** *With the above notation, let  $L/K$  be a quadratic extension of conductor equal to  $\mathfrak{m}$ . We have  $L = K(\sqrt{\alpha})$ , where  $\alpha$  is of the following form:*

$$\alpha = \epsilon \prod_{1 \leq i \leq h} \alpha_i^{n_i} \prod_{\mathfrak{p} \in S} \beta_{\mathfrak{p}},$$

and  $\epsilon$  is a unit.

In addition, the following conditions must be satisfied:

- (1)  $S_{\mathfrak{m},3} = \emptyset$ .
- (2) If  $\mathfrak{p} \in S_{\mathfrak{m},2}$ , then  $v_{\mathfrak{p}}(\mathfrak{m}) \geq 2$ .
- (3) If  $\mathfrak{p} \in S_{\mathfrak{m}}$ , then  $v_{\mathfrak{p}}(\mathfrak{m}) = 1$ .
- (4) For all  $i \leq h$ , we must have  $\sum_{\mathfrak{p} \in S} p_{i,\mathfrak{p}} \equiv 0 \pmod{2}$ .
- (5) For all  $i \leq h$ , we have  $n_i = 0$  or 1.
- (6) For  $\mathfrak{p} \in S_{\mathfrak{m},2}$ , the largest  $k$  such that the congruence

$$x^2 \equiv \alpha \pmod{\mathfrak{p}^k}$$

has a solution must be equal to  $z(\mathfrak{p}) - v_{\mathfrak{p}}(\mathfrak{m})$ .

- (7) For each  $\mathfrak{p} \in S_2$ , the congruence

$$x^2 \equiv \alpha \pmod{\mathfrak{p}^{z(\mathfrak{p})-1}}$$

has a solution.

- (8) For each  $\sigma \in \mathfrak{m}_{\infty}$ , we have  $\sigma(\alpha) < 0$ , while for each embedding  $\sigma$  such that  $\sigma \notin \mathfrak{m}_{\infty}$ , we have  $\sigma(\alpha) > 0$ .
- (9)  $\alpha \notin (K^*)^2$  (this condition is necessary only if  $\mathfrak{m} = \mathbb{Z}_K$ ).

Conversely, if  $\alpha$  is chosen as above and the conditions are satisfied, then  $L/K$  is a quadratic extension of conductor equal to  $\mathfrak{m}$ .

The solubility of the congruences needed in the above theorem can easily be established by computing the structure of the groups  $(\mathbb{Z}_K/\mathfrak{p}^k)^*$  as explained in [Co-Di-Ol].

If all the conditions are satisfied, then  $K(\sqrt{\alpha})$  will be a quadratic extension of  $K$  which has the correct signature and relative discriminant  $\mathfrak{d}(L/K)$ . However, it may not be the field that we are looking for, since we must also ask that its norm group be equal to  $C$ .

To terminate, for each  $\alpha$  that we find we compute the norm group of  $K(\sqrt{\alpha})$  and we check that we obtain once and only once all the subgroups of  $I_{\mathfrak{m}}(K)$  of index 2 (otherwise there is an error), and this tells us precisely which group corresponds to which  $\alpha$ . If we do not care about the norm group, we do not need to do this, since we know by class field theory that up to squares there will be exactly the same

number of  $\alpha$  as subgroups of index 2 and conductor  $\mathfrak{m}$  of  $I_{\mathfrak{m}}(K)$ . Thus, to check the correctness of our computations, it is sufficient to check that the *number* is the same, not the exact correspondence. Note also that it is quite easy to compute the norm group explicitly by using its characterization in terms of the decomposition of unramified prime ideals.

Once we know that  $L = K(\sqrt{\alpha})$ , it is a trivial matter to find the absolute equation of  $L/\mathbb{Q}$ . This equation usually has quite large coefficients, and we then use a strong polynomial reduction algorithm (analogous to the Polred algorithm described in [Co-Di], but searching for minima using the Fincke-Pohst algorithm, instead of simply small vectors using LLL), and we finally obtain an absolute equation with quite small coefficients.

(D). **Removing isomorphisms.** We now have a large list of degree 8 polynomials (in our tables, we chose the bounds so as to have between 13000 and 18000 polynomials at this stage). We must remove the polynomials defining isomorphic number fields over  $\mathbb{Q}$ . The use of the strong polynomial reduction algorithm mentioned above is already a very big step in this direction, since it is not frequent that two different strongly reduced polynomials define isomorphic number fields, although it may of course happen.

We sort the table according to increasing absolute value of discriminant, and for two entries having the same discriminant, we do the following. If the reduced polynomials are the same, evidently the fields are isomorphic, so we remove one of the two. Otherwise, we factor the two polynomials modulo small primes not dividing the indices of one or the other (so that the factorization modulo the prime reflects the factorization into prime ideals). If the factorizations differ, the fields are not isomorphic. If they are equal, then we use an absolutely certain but slow method, i.e., we factor one polynomial in the number field defined by the other. Once this is done, we also compute the Galois group of the Galois closure of the corresponding number field, since we will be interested in this later.

It must be noticed that our method using class field theory is much less wasteful than the methods based on the geometry of numbers also with respect to isomorphisms: in our methods, we rarely found more than two distinct polynomials defining isomorphic number fields, while in methods based on the geometry of numbers, there are usually many more isomorphic fields.

In fact, using our methods, we can find distinct polynomials defining isomorphic number fields only when the octic field contains at least two non-isomorphic quartic fields, and this rarely happens.

In performing this routine and apparently uninteresting task, we stumbled onto two quite interesting phenomena.

First, fields which cannot be distinguished by prime factorizations alone are rare, but do occur. In fact, we have looked closely at these examples, and they are all *arithmetically equivalent* fields, i.e., number fields having the same Dedekind  $\zeta$  function. We refer to the literature on the subject (see [Ga], [Pe]), but we note the following.

Even though equality of the  $\zeta$  function implies the equality of many arithmetic quantities, it does *not* imply the identity of the ramification exponents, only the residual indices. We have several examples of arithmetically equivalent fields which can be distinguished by factoring a ramified prime.

In addition, it is well known that arithmetic equivalence is a purely group-theoretical property. In the case of degree 8 fields, one can show that there are exactly two Galois groups among all the possible 50 transitive groups of degree 8 having this property (see below). These are the groups  $\mathcal{H}ol(C_8)$  (denoted  $T_{15}$  in [Bu-Mc]) of order 32, equal to the semidirect product of the cyclic group  $C_8$  by its group of automorphisms acting in the natural way, and the group  $GL_2(\mathbb{F}_3)$  (denoted  $T_{23}$  in [Bu-Mc]) of order 48.

A list of these fields will be given in the next section (see Tables 8–14).

The second phenomenon we have observed (and which we call the “mirror effect”) is that in many cases, certain simple changes on the polynomial coefficients modify the signature without modifying the Galois group. This will be described in detail below (see Section 3 (B)(3)).

### 3. DESCRIPTION OF THE TABLES

(A). **Length of the tables.** We have chosen the discriminant bounds so that the tables are roughly of the same length, and contain at least 10000 non-isomorphic octic fields. As indicated above, there are very few isomorphic number fields corresponding to distinct polynomials, hence we could easily judge at an early stage whether our bounds were sufficient.

Table 1 gives the chosen bounds, as well as the number of non-isomorphic octic fields up to that bound, corresponding to the five possible signatures.

TABLE 1

Signature	Bound for discriminants	Number of non-isomorphic fields
(0,4)	5000 00000	11639
(2,3)	-16000 00000	12301
(4,2)	35000 00000	13077
(6,1)	-5 00000 00000	11680
(8,0)	25 00000 00000	13796

(B). **Galois groups.** We have computed the Galois group of every octic field that we have found, using the methods described in [Ei] and [Ei-Ol]. The Galois groups which we obtain are necessarily among those corresponding to octic fields containing a quartic subfield, and this corresponds to 36 of the 50 possible Galois groups in degree 8 (see the table in signature (0, 4) or (8, 0) for the complete list).

Even though we found many octic fields, there was no reason to expect that we would find all the possible combinations of signatures and Galois groups, and indeed we found only 97 of the 114 possible combinations.

For the 17 missing ones, we used several methods.

We first looked for an example of a field having the desired signature and Galois group. The discriminant of this field gave us a (possibly quite large) upper bound for the minimal discriminant. We then used a systematic search up to this bound as was done for the main tables, using the specific properties of the group that we

were looking for. For example, the search was greatly simplified when the group was even since we needed to use only quartic fields with square discriminant.

The methods we used to find at least one example were the following.

- (1) Specializations of the parametrized solutions given in the literature, for example in [Sm]. Of course, these solutions do not necessarily have the correct signature.
- (2) Particular polynomials found in the literature. More precisely, we checked that the minimal discriminant for the Galois group  $T_5^+$  and signature  $(0, 4)$  is indeed as given by S.-H. Kwon in [Kw]. On the other hand, the discriminant for the Galois group  $T_{23}$  and signature  $(0, 4)$  given by A. Jehanne in [Je] gives us an upper bound but is not minimal.
- (3) The “mirror effect” already mentioned above: an octic field  $L$  having a quartic subfield  $K$  can be defined by an even polynomial  $P(X^2) \in \mathbb{Z}[X]$ . Let  $D$  be a rational integer such that  $\sqrt{D}$  is not in the Galois closure  $N$  of  $L$  over  $\mathbb{Q}$ , and denote by  $G$  the Galois group of the extension  $N/\mathbb{Q}$ . The field obtained by adjoining to the rationals the roots  $\{\pm\theta_1, \pm\theta_2, \pm\theta_3, \pm\theta_4\}$  of  $P(X^2)$  as well as  $\sqrt{D}$  is Galois over  $\mathbb{Q}$ , and its Galois group is isomorphic to  $G \times C_2$ . In this group, the intersection of the stabilizers of the elements  $\sqrt{D}\theta_j$  is trivial if there does not exist  $\sigma \in G$  such that  $\sigma(\theta_j) = -\theta_j$  for  $j = 1, 2, 3, 4$ , and it is equal to  $H = \{(1, 1), (\sigma, 1)\} \simeq C_2$ , otherwise. In this case, since  $\sigma$  is a central element in  $G$ , we have  $(G \times C_2)/H \simeq G$  as an abstract group.

Thus, replacing  $P(X^2)$  with  $P((X\sqrt{D})^2) = P(DX^2)$  gives a polynomial whose Galois group is (as an abstract group) isomorphic to  $G \times C_2$  in the first case above, and to  $G$  in the second case.

Using this, one can prove (Y. Eichenlaub, personal communication) that the Galois group of the Galois closure of  $L/\mathbb{Q}$  is not changed except when  $G$  is the group  $T_4^+$  (resp.  $T_{14}^+$ ) in which case the new group becomes  $T_4^+$  or  $T_9^+$  (resp.  $T_{24}^+$ ).

The most useful case of the above transformation corresponds to  $D = -1$ . In that case, starting with an octic field of signature  $(r_1, r_2)$ , we obtain an octic field of signature  $(r'_1, r'_2)$  with the following possibilities. If  $r_1 = 8$ , we obtain  $r'_1 = 0$ . If  $r_1 = 6$ , we obtain  $r'_1 = 2$ . If  $r_1 = 4$ , we can have  $r'_1 = 4$  or  $r'_1 = 0$ . If  $r_1 = 2$ , we can have  $r'_1 = 2$  or  $r'_1 = 6$ . Finally, if  $r_1 = 0$ , we can have  $r'_1 = 0$ ,  $r'_1 = 4$  or  $r'_1 = 8$ .

- (4) The direct study of the group structure. For example, the group  $T_{14}^+$  is the group  $S_4$  considered as a transitive group of degree 8. It is not difficult to prove that an octic field having such a Galois group is obtained by taking a quartic field of Galois group  $S_4$ , and adjoining the square root of the discriminant of the quartic field (which of course belongs to the Galois closure).
- (5) Pushing this idea further, we adjoined to quartic fields square roots of *divisors* of the discriminant, and we obtained in this way practically all the missing groups and signatures.

For all signatures and for all possible Galois groups of the Galois closure corresponding to this signature Tables 2–6 give the following.

- (1) The name of the Galois group in the notation of [Bu-Mc]. We chose not to use the more recent (but more complex) notation of [Co-Hu-Mc].



TABLE 2. Signature (0, 4)

$G$	#	$d_{\min}$	$G$	#	$d_{\min}$	$G$	#	$d_{\min}$
$T_1$	0	2147483648*	$T_{13}^+$	9	17850625	$T_{26}$	26	18753525
$T_2^+$	14	1265625	$T_{14}^+$	13	60886809	$T_{27}$	592	1578125
$T_3^+$	10	5308416	$T_{15}$	8	31443200	$T_{28}$	20	37879808
$T_4^+$	31	1750329	$T_{16}$	5	9453125	$T_{29}^+$	201	3504384
$T_5^+$	0	12230590464*	$T_{17}$	55	1257728	$T_{30}$	1	215378125
$T_6$	14	4102893	$T_{18}^+$	194	6036849	$T_{31}$	1017	1513728
$T_7$	0	5120000000*	$T_{19}^+$	3	67108864	$T_{32}^+$	0	1142440000*
$T_8$	0	104963309568*	$T_{20}^+$	7	26265625	$T_{35}$	4194	1327833
$T_9^+$	209	3211264	$T_{21}$	7	33554432	$T_{38}$	4	167186432
$T_{10}^+$	27	1890625	$T_{22}^+$	31	25401600	$T_{39}^+$	262	4227136
$T_{11}^+$	38	3240000	$T_{23}$	0	33971001237*	$T_{40}$	10	12008989
$T_{12}^+$	0	705911761*	$T_{24}^+$	510	1763584	$T_{44}$	4127	1361513

TABLE 3. Signature (2, 3)

$G$	#	$d_{\min}$	$G$	#	$d_{\min}$	$G$	#	$d_{\min}$
$T_6$	18	-4286875	$T_{26}$	51	-7486875	$T_{35}$	2798	-4461875
$T_8$	5	-107171875	$T_{27}$	40	-74671875	$T_{38}$	0	-4941382327*
$T_{15}$	20	-40960000	$T_{30}$	18	-21434375	$T_{40}$	25	-22665187
$T_{23}$	46	-22665187	$T_{31}$	21	-79360000	$T_{44}$	9259	-4711123

TABLE 4. Signature (4, 2)

$G$	#	$d_{\min}$	$G$	#	$d_{\min}$	$G$	#	$d_{\min}$
$T_7$	2	56953125	$T_{20}^+$	12	268435456	$T_{31}$	50	104960000
$T_9^+$	60	40960000	$T_{21}$	0	8830503125*	$T_{32}^+$	0	45178352704*
$T_{10}^+$	25	64000000	$T_{22}^+$	15	368640000	$T_{35}$	2899	17318125
$T_{11}^+$	16	23040000	$T_{24}^+$	344	39375625	$T_{38}$	0	5647294088*
$T_{15}$	0	11662589952*	$T_{26}$	7	321978368	$T_{39}^+$	576	20502784
$T_{16}$	3	320000000	$T_{27}$	105	71303168	$T_{40}$	0	7495014493*
$T_{17}$	6	15243125	$T_{28}$	67	31878125	$T_{44}$	8515	15297613
$T_{18}^+$	183	19360000	$T_{29}^+$	188	25755625			
$T_{19}^+$	0	27710263296*	$T_{30}$	4	1076890625			

TABLE 5. Signature (6, 1)

$G$	#	$d_{\min}$	$G$	#	$d_{\min}$	$G$	#	$d_{\min}$
$T_{27}$	1205	-746 71875	$T_{35}$	5657	-688 56875	$T_{44}$	4045	-1034 05923
$T_{31}$	764	-2494 95552	$T_{38}$	9	-49413 82327			

TABLE 6. Signature (8, 0)

$G$	#	$d_{\min}$	$G$	#	$d_{\min}$	$G$	#	$d_{\min}$
$T_1$	3	4103 38673	$T_{13}^+$	3	6 05238 72256	$T_{26}$	12	25760 88125
$T_2^+$	28	3240 00000	$T_{14}^+$	0	82 13869 40416*	$T_{27}$	1407	12922 03125
$T_3^+$	9	33177 60000	$T_{15}$	6	11 94356 44125	$T_{28}$	57	81608 00000
$T_4^+$	20	4420 50625	$T_{16}$	3	4 78975 78125	$T_{29}^+$	100	50694 40000
$T_5^+$	1	1 22305 90464	$T_{17}$	49	2823 00416	$T_{30}$	4	12 39119 40625
$T_6$	8	59101 06112	$T_{18}^+$	163	41634 75625	$T_{31}$	795	19481 60000
$T_7$	8	51200 00000	$T_{19}^+$	1	8 75781 16096	$T_{32}^+$	0	315 03303 56889*
$T_8$	3	1 60984 53125	$T_{20}^+$	13	1 48840 00000	$T_{35}$	6139	3095 93125
$T_9^+$	142	15341 32224	$T_{21}$	1	17 51562 32192	$T_{38}$	6	6 28261 46729
$T_{10}^+$	79	10643 90625	$T_{22}^+$	8	1 80633 60000	$T_{39}^+$	125	52400 22544
$T_{11}^+$	43	4326 40000	$T_{23}$	8	2 14154 71433	$T_{40}$	0	46 31434 05393*
$T_{12}^+$	6	58873 39441	$T_{24}^+$	295	23936 55625	$T_{44}$	4251	11527 84549

- (2) The number of non-isomorphic number fields having this Galois group and signature in the limits of our main tables. In particular, when the minimal discriminant was obtained by specific methods (indicated by \*), the corresponding number is 0.
- (3) The minimal discriminant (in absolute value) corresponding to this Galois group.

TABLE 7

Signature	2	3	4	5	6	7	8	9	10	11
(0,4)	2009	134	210	22	15	6	12	1	4	1
(2,3)	2775	92	307	9	18	2	12	0	2	0
(4,2)	1799	141	108	7	14	3	3	1	0	0
(6,1)	1868	169	288	6	12	7	10	0	0	0
(8,0)	1160	28	35	1	0	0	0	0	0	0

(C). **Non-isomorphic fields having the same discriminant.** We have observed that non-isomorphic fields having the same discriminant occur very frequently. In the limits of our tables, the maximum number observed is a set of 11 such fields in signature (0, 4). This corresponds to discriminant  $4840 00000 = 2^8 \cdot 5^6 \cdot 11^2$ .

Below we give the eleven polynomials defining these fields, together with their Galois group:

$$\begin{aligned}
 P_1(X) &= X^8 - X^6 + X^4 + 24X^2 + 16 : T_9^+ \\
 P_2(X) &= X^8 - 7X^6 + 34X^4 - 88X^2 + 121 : T_{10}^+ \\
 P_3(X) &= X^8 + X^6 + 16X^4 + 66X^2 + 121 : T_{10}^+ \\
 P_4(X) &= X^8 - X^6 + 16X^4 - 66X^2 + 121 : T_{10}^+ \\
 P_5(X) &= X^8 + 5X^6 + 20X^4 + 50X^2 + 25 : T_{18}^+ \\
 P_6(X) &= X^8 + 4X^6 + X^4 + 4X^2 + 1 : T_{18}^+ \\
 P_7(X) &= X^8 + 7X^6 + 19X^4 + 28X^2 + 16 : T_{18}^+ \\
 P_8(X) &= X^8 - 12X^6 + 64X^4 - 143X^2 + 121 : T_{20}^+ \\
 P_9(X) &= X^8 + 12X^6 + 64X^4 + 143X^2 + 121 : T_{20}^+ \\
 P_{10}(X) &= X^8 - 11X^6 + 51X^4 - 121X^2 + 121 : T_{20}^+ \\
 P_{11}(X) &= X^8 + 11X^6 + 51X^4 + 121X^2 + 121 : T_{20}^+
 \end{aligned}$$

Observe once again in this table the “mirror effect”. For the polynomials  $P_3, P_4, P_8, P_9, P_{10}$  and  $P_{11}$ , changing  $X$  into  $X\sqrt{-1}$  changes the number field into a non-isomorphic one having the same discriminant, Galois group and signature. For the polynomials  $P_5, P_6$  and  $P_7$  (having Galois group  $T_{18}^+$ ), it changes the number field into a number field having the same discriminant and Galois group, but in signature  $(4, 2)$ . For the polynomial  $P_1$ , we obtain a reducible polynomial, but this is clearly irrelevant to the problem. Finally, for the polynomial  $P_2$ , it changes the number field into a number field having the same Galois group and the same signature, but a discriminant which is 256 times smaller. Different choices for  $D$  would lead to similar results.

Since we have obtained 3 fields having the same discriminant and Galois group in signature  $(4, 2)$  by using the mirror effect, we observed in our tables that in signature  $(4, 2)$  there are two more number fields having the same discriminant:

$$\begin{aligned}
 X^8 - 5X^6 + 5X^4 - 25X^2 + 25 : T_{10}^+ \\
 X^8 - 3X^6 + 4X^4 - 7X^2 + 1 : T_{10}^+.
 \end{aligned}$$

Note that in certain cases (but not in the examples that we have just given), we could obtain isomorphic number fields by this method.

Table 7 gives, for each signature, the number of doublets, triplets, etc. of non-isomorphic number fields having the same discriminant.

(D). **Arithmetically equivalent fields.** In this section we give all the examples of non-isomorphic octic fields having the same Dedekind  $\zeta$ -function found in the tables (such fields are called arithmetically equivalent).

The following theorem gives a necessary and sufficient condition for the existence of arithmetically equivalent fields (see [Ga]).

**Theorem 3.** *Let  $K_1$  and  $K_2$  be two number fields (assumed to be in a fixed algebraic closure of  $\mathbb{Q}$ ). The fields  $K_1$  and  $K_2$  are arithmetically equivalent if and only if the following two conditions are satisfied.*

- (1) *The fields have a common Galois closure  $N$ .*  
 (2) *Let  $G = \text{Gal}(N/\mathbb{Q})$ ,  $G_1 = \text{Gal}(N/K_1)$  and  $G_2 = \text{Gal}(N/K_2)$ . Then for each conjugacy class  $C$  in  $G$ , we must have  $|G_1 \cap C| = |G_2 \cap C|$  (where  $|\cdot|$  denotes cardinality).*

From this theorem, it is not difficult to deduce the following (Y. Eichenlaub, personal communication).

**Corollary.** *If  $K_1$  and  $K_2$  are non-isomorphic arithmetically equivalent octic fields, their Galois group is isomorphic to  $T_{15}$  or to  $T_{23}$ . Conversely, if an octic field  $K_1$  has a Galois group isomorphic to  $T_{15}$  or to  $T_{23}$ , then there exists a non-isomorphic field  $K_2$  arithmetically equivalent to  $K_1$ .*

Since  $T_{15}$  cannot occur in signature  $(6, 1)$ , we cannot have arithmetically equivalent fields with such a Galois group in that signature. Within the limits of our tables, we found no example in signature  $(4, 2)$ , but the desired (minimal) example was found during the search for the minimal discriminant with Galois group  $T_{15}$ .

Similarly,  $T_{23}$  cannot occur in signatures  $(4, 2)$  and  $(6, 1)$ ; hence we cannot have arithmetically equivalent fields with such a Galois group in these signatures. Within the limits of our tables, we found no example in signature  $(0, 4)$ , but the desired (minimal) example was found during the search for the minimal discriminant with Galois group  $T_{23}$  using the upper bound from [Je].

In Tables 8–14, we give for each signature all the examples found within the limits of our tables (plus the example of  $T_{15}$  in signature  $(4, 2)$  and  $T_{23}$  in signature  $(0, 4)$ ). For each pair of fields having the same  $\zeta$ -function, we give octic polynomials generating the corresponding fields. In some cases, ramified ideals do not have the same decomposition as a product of prime ideals in both fields. When this occurs, we denote by  $\mathfrak{p}, \mathfrak{p}', \dots$  prime ideals of residual degree equal to 1 and by  $\mathfrak{q}, \mathfrak{q}', \dots$  prime ideals of residual degree equal to 2.

Within the limits of our tables, we have found two examples of quadruplets of number fields having the same discriminant, signature and Galois group, forming two pairs of arithmetically equivalent fields (all having  $T_{23}$  as Galois group). These examples occur for discriminants  $-150730227$  and  $-1327373299$ .

Two arithmetically equivalent fields have the same product  $h(K)R(K)$  of the class number by the regulator. Since the class number is very often equal to 1, it is usually the case that the class numbers and the regulators are equal. It has however been noticed by several authors (see, for example, [Sm-Pe]) that the class numbers (hence the regulators) of arithmetically equivalent fields may be different.

Two of the 18 pairs of arithmetically equivalent fields with  $T_{15}$  as Galois group that we have found give such examples. Both are in signature  $(2, 3)$ . The pairs are for discriminant  $-518711875$  and  $-1097440000$ , for which the second field given below has class number 2 while the first has class number 1. In both of these cases, the narrow class numbers of the fields coincide and are equal to 2.

TABLE 8. Signature (0, 4) Group  $T_{15}$

$d_K$	Polynomial	Different factorisation
31443200	$X^8 - X^6 - 4X^5 - 2X^4 + 4X^3 + 12X^2 + 6X + 1$	$5\mathbb{Z}_K = p^2 p'^2 q q'$ $17\mathbb{Z}_K = p^2 p' p'' q^2$
31443200	$X^8 - 2X^7 + 3X^6 - 6X^5 + 13X^4 - 20X^3 + 21X^2 - 14X + 5$	$5\mathbb{Z}_K = p^2 p' p'' q^2$ $17\mathbb{Z}_K = p^2 p'^2 p''^2 q$
70304000	$X^8 - 4X^7 + 7X^6 - 2X^5 - 8X^4 + 8X^3 + 2X^2 - 4X + 1$	$5\mathbb{Z}_K = p^2 p'^2 p''^2 q$ $13\mathbb{Z}_K = p^2 p' p'' q^2$
70304000	$X^8 + X^6 - 2X^5 + 5X^4 - 2X^3 + X^2 + 1$	$5\mathbb{Z}_K = p^2 p' p'' q^2$ $13\mathbb{Z}_K = p^2 p'^2 p''^2 q$
143327232	$X^8 + 6X^6 + 15X^4 + 12X^2 + 3$	
143327232	$X^8 + 3X^4 + 3$	
212556032	$X^8 - 4X^7 + X^6 + 8X^5 + 5X^4 - 14X^3 - 13X^2 + 4X + 17$	
212556032	$X^8 - 2X^7 + 5X^6 - 10X^5 + 23X^4 - 36X^3 + 51X^2 - 48X + 17$	

TABLE 9. Signature (0, 4) Group  $T_{23}$

$d_K$	Polynomial	Different factorisation
33971001237	$X^8 - 4X^7 + 8X^6 - 9X^5 + 27X^4 - 39X^3 + 35X^2 - 17X + 7$	$3\mathbb{Z}_K = p^3 p'^3 q$
33971001237	$X^8 - X^7 - X^5 + 25X^4 - 54X^3 + 50X^2 - 8X + 9$	$3\mathbb{Z}_K = pp' q^3$

TABLE 10. Signature (2, 3) Group  $T_{15}$

$d_K$	Polynomial	Different factorisation
-40960000	$X^8 + 4X^6 + 5X^4 + 2X^2 - 1$	
-40960000	$X^8 - X^4 - 1$	
-131274675	$X^8 - X^7 + X^6 - 4X^5 + X^4 - 4X^3 + X^2 - X + 1$	$5\mathbb{Z}_K = p^2 p'^2 q q'$
-131274675	$X^8 - 2X^7 + 4X^6 - 5X^5 + X^4 - 5X^3 + 4X^2 - 2X + 1$	$5\mathbb{Z}_K = p^2 p' p'' q^2$
-342102016	$X^8 + 8X^4 - 1$	
-342102016	$X^8 + 4X^6 + 5X^4 + 2X^2 - 4$	
-359661568	$X^8 - 4X^6 - 4X^5 + 2X^4 - 2$	$7\mathbb{Z}_K = p^2 p'^2 p''^2 q$
-359661568	$X^8 - 4X^5 + 8X^3 + 4X^2 + 4X + 1$	$7\mathbb{Z}_K = p^2 p' p'' q^2$
-518711875	$X^8 - 6X^6 - X^5 + 4X^4 + 13X^3 + 9X^2 + 10X - 5$	$19\mathbb{Z}_K = p^2 p'^2 p''^2 q$
-518711875	$X^8 - X^7 - 6X^6 + 8X^5 + 11X^4 - 15X^3 - 29X^2 + 55X - 25$	$19\mathbb{Z}_K = p^2 p' p'' q^2$
-1024000000	$X^8 - 15X^4 - 50X^2 - 25$	
-1024000000	$X^8 + 5X^4 - 25$	
-1097440000	$X^8 - 5X^6 + 3X^4 + 15X^2 - 19$	$19\mathbb{Z}_K = p^2 p' p'' q^2$
-1097440000	$X^8 + 5X^6 + 3X^4 - 15X^2 - 19$	$19\mathbb{Z}_K = p^2 p'^2 p''^2 q$
-1119744000	$X^8 - 2X^7 + X^6 - 8X^5 + X^4 - 8X^3 + X^2 - 2X + 1$	$5\mathbb{Z}_K = p^2 p' p'' q^2$
-1119744000	$X^8 - 2X^7 + X^6 + 4X^5 - 5X^4 + 4X^3 + X^2 - 2X + 1$	$5\mathbb{Z}_K = p^2 p'^2 p''^2 q$
-1344252672	$X^8 - 3X^6 + 6X^2 - 3$	
-1344252672	$X^8 + 3X^6 - 6X^2 - 3$	
-1517535243	$X^8 - X^7 - 5X^6 + 8X^5 + 4X^4 - 25X^3 - 5X^2 + 11X - 5$	$17\mathbb{Z}_K = p^2 p' p'' q^2$
-1517535243	$X^8 - X^7 + 4X^6 - X^5 + 7X^4 - 10X^3 - 8X^2 + 14X - 5$	$17\mathbb{Z}_K = p^2 p'^2 p''^2 q$

TABLE 11. Signature (2, 3) Group  $T_{23}$

$d_K$	Polynomial	Different factorisation
-22665187	$X^8 - X^7 + X^6 - 2X^5 + X^4 - 9X^3 + 7X^2 - 6X + 1$	
-22665187	$X^8 - 3X^7 + 4X^6 - 8X^5 + 8X^4 - X^3 + 2X^2 - 3X - 1$	
-32019867	$X^8 - 4X^7 + 7X^6 - 7X^5 + 7X^4 - 7X^3 + 2X^2 + X - 1$	$3\mathbb{Z}_K = p^2q^3$ $11\mathbb{Z}_K = p^3p'q$
-32019867	$X^8 - X^7 + X^6 - 2X^5 - X^4 - 2X^3 + X^2 - X + 1$	$3\mathbb{Z}_K = p^6q$ $11\mathbb{Z}_K = pp'q^3$
-36264691	$X^8 - 4X^7 + 5X^6 - X^5 - 3X^4 + 3X^3 - X - 1$	
-36264691	$X^8 - 2X^7 + 3X^6 - 7X^4 + 17X^3 - 17X^2 + 11X - 1$	
-81415168	$X^8 - 4X^7 + 8X^6 - 8X^5 + 6X^3 - 2X^2 - 2$	
-81415168	$X^8 - 4X^7 + 10X^6 - 14X^5 + 10X^4 + 2X^3 - 10X^2 + 8X - 2$	
-110716875	$X^8 - 4X^7 + 5X^6 - X^5 - 2X^4 + X^3 + 4X^2 - 4X - 1$	$3\mathbb{Z}_K = p^6q$ $5\mathbb{Z}_K = pp'q^3$
-110716875	$X^8 - 4X^7 + 7X^6 - 7X^5 + 4X^4 - X^3 - 4X^2 + 4X - 1$	$3\mathbb{Z}_K = p^2q^3$ $5\mathbb{Z}_K = p^3p'q$
-118370771	$X^8 - 2X^7 - X^5 + 7X^3 + X - 9$	
-118370771	$X^8 - 3X^7 + 7X^6 - 10X^5 + 11X^4 - 5X^3 + 3X^2 - 2X - 3$	
-150730227	$X^8 - X^7 + X^6 + 5X^5 - 11X^4 + 8X^3 - 7X^2 + 4X - 1$	$3\mathbb{Z}_K = p^2q^3$
-150730227	$X^8 - 2X^7 + 2X^6 - X^5 + 2X^4 + X^3 - 5X^2 + 4X - 1$	$3\mathbb{Z}_K = p^6q$
-150730227	$X^8 - 4X^7 + 7X^6 - 6X^5 - 3X^4 + 9X^3 - X^2 - 5X - 1$	$3\mathbb{Z}_K = p^3p'p''^2$
-150730227	$X^8 + 2X^6 - 2X^5 - 3X^4 - 7X^3 - 11X^2 - 6X - 1$	$3\mathbb{Z}_K = p^6p'p''$
-178453547	$X^8 - 2X^7 + 3X^6 + X^5 - 4X^4 + 12X^3 - 7X^2 + 2X - 9$	
-178453547	$X^8 - X^7 - 2X^6 + 6X^5 - 11X^3 + 5X^2 + 8X - 3$	
-181398528	$X^8 - 2X^6 - 2X^5 - 2X^3 - 2X^2 + 1$	$3\mathbb{Z}_K = p^6q$
-181398528	$X^8 - 6X^4 + 4X^2 - 3$	$3\mathbb{Z}_K = p^2q^3$
-182660427	$X^8 - 4X^7 + 7X^6 - 7X^5 + 4X^4 - X^3 + 4X^2 - 4X + 1$	$17\mathbb{Z}_K = p^3p'q$
-182660427	$X^8 - X^7 + 4X^6 - 4X^5 - 2X^4 - 4X^3 - 5X^2 - X + 1$	$17\mathbb{Z}_K = pp'q^3$
-265847707	$X^8 - 2X^7 + 3X^6 + X^5 - 7X^4 + 18X^3 - 12X^2 + 4X - 1$	
-265847707	$X^8 - X^7 - X^6 + 5X^5 - 3X^4 + 2X^3 - 6X^2 + 9X - 1$	
-286557184	$X^8 - 5X^6 + 6X^4 + 3X^2 - 1$	$23\mathbb{Z}_K = p^3p'q$
-286557184	$X^8 + 5X^6 + 6X^4 - 3X^2 - 1$	$23\mathbb{Z}_K = pp'q^3$
-325660672	$X^8 - 2X^7 + 6X^6 - 12X^5 + 16X^4 - 10X^3 - 4X^2 + 4X - 1$	
-325660672	$X^8 - 2X^7 + 4X^6 - 12X^5 + 16X^4 - 18X^3 + 10X^2 - 1$	
-423564751	$X^8 - 2X^7 + 2X^6 - 4X^5 - 4X^4 + 20X^3 - 14X^2 + 13X - 4$	
-423564751	$X^8 - X^7 - 2X^6 + 4X^5 - 9X^4 + 17X^3 - 21X^2 + 7X - 4$	
-425329947	$X^8 - X^7 - 3X^6 + 2X^5 + 4X^4 + 3X^3 - 5X^2 - 7X - 3$	$3\mathbb{Z}_K = p^6p'p''$
-425329947	$X^8 - 6X^4 - X^2 - 3$	$3\mathbb{Z}_K = p^3p'p''^2$
-725594112	$X^8 - 6X^4 - 4X^2 - 3$	$3\mathbb{Z}_K = p^3p'p''^2$
-725594112	$X^8 - 4X^6 + 12X^2 - 12$	$3\mathbb{Z}_K = p^6p'p''$
-941391011	$X^8 - 2X^7 - 2X^6 + 17X^5 - 32X^4 + 31X^3 - 15X^2 + 4X - 1$	$29\mathbb{Z}_K = p^3p'q$
-941391011	$X^8 + 2X^6 - 9X^4 + 6X^2 - 11$	$29\mathbb{Z}_K = pp'q^3$
-999406512	$X^8 - 4X^7 + X^6 + 11X^5 - 11X^4 - X^3 + 4X^2 - X - 2$	$2\mathbb{Z}_K = pp'q^3$
-999406512	$X^8 - 4X^7 + 7X^6 - 7X^5 - 2X^4 + 11X^3 - 2X^2 - 4X - 2$	$2\mathbb{Z}_K = p^3p'q$
-1280239375	$X^8 - 2X^7 + 5X^5 - 6X^4 - 10X^3 + 21X^2 + 5X - 13$	$5\mathbb{Z}_K = p^3p'q$
-1280239375	$X^8 - 4X^7 + 10X^6 - 16X^5 + 18X^4 - 14X^3 + 4X^2 + X - 1$	$5\mathbb{Z}_K = pp'q^3$

TABLE 11. (Continued)

$d_K$	Polynomial	Different factorisation
-1327373299	$X^8 - X^7 - 2X^6 - 6X^5 + 10X^4 + 15X^3 - 6X^2 - 5X - 7$	
-1327373299	$X^8 - 3X^7 + 2X^6 - 3X^4 + 11X^3 - 13X^2 + 15X - 11$	
-1327373299	$X^8 - 6X^6 - 5X^5 + 19X^4 + 21X^3 - 18X^2 - 36X - 5$	
-1327373299	$X^8 - X^7 - 4X^6 + 4X^5 + 4X^4 - 9X^3 + 2X^2 - 3X - 5$	
-1399680000	$X^8 - 6X^6 + 12X^4 - 6X^3 - 6X^2 + 18X - 3$	$5\mathbb{Z}_K = \mathfrak{p}\mathfrak{p}'\mathfrak{q}^3$
-1399680000	$X^8 - 6X^4 - 12X^2 - 3$	$5\mathbb{Z}_K = \mathfrak{p}^3\mathfrak{p}'^3\mathfrak{q}$

TABLE 12. Signature (4, 2) Group  $T_{15}$

$d_K$	Polynomial	Different factorisation
11662589952	$X^8 - 4X^7 + 2X^6 - 4X^5 + 12X^4 + 12X^3 - 4X - 2$	
11662589952	$X^8 - 4X^7 + 6X^6 + 8X^5 - 36X^4 + 32X^3 + 14X^2 - 24X + 1$	

TABLE 13. Signature (8, 0) Group  $T_{15}$

$d_K$	Polynomial	Different factorisation
119435644125	$X^8 - 4X^7 - 3X^6 + 23X^5 - 3X^4 - 37X^3 + 8X^2 + 15X - 5$	$5\mathbb{Z}_K = \mathfrak{p}^2\mathfrak{p}'^2\mathfrak{p}''^2\mathfrak{q}$ $17\mathbb{Z}_K = \mathfrak{p}^2\mathfrak{p}'^2\mathfrak{p}''^2\mathfrak{q}$
119435644125	$X^8 - X^7 - 11X^6 + 4X^5 + 21X^4 - 4X^3 - 11X^2 + X + 1$	$5\mathbb{Z}_K = \mathfrak{p}^2\mathfrak{p}'\mathfrak{p}''\mathfrak{q}^2$ $17\mathbb{Z}_K = \mathfrak{p}^2\mathfrak{p}'\mathfrak{p}''\mathfrak{q}^2$
131153375232	$X^8 - 12X^6 + 45X^4 - 54X^2 + 12$	
131153375232	$X^8 - 9X^6 + 24X^4 - 21X^2 + 3$	
186601439232	$X^8 - 14X^6 + 44X^4 - 46X^2 + 13$	$13\mathbb{Z}_K = \mathfrak{p}^2\mathfrak{p}'^2\mathfrak{p}''^2\mathfrak{q}$
186601439232	$X^8 - 10X^6 + 32X^4 - 38X^2 + 13$	$13\mathbb{Z}_K = \mathfrak{p}^2\mathfrak{p}'\mathfrak{p}''\mathfrak{q}^2$

TABLE 14. Signature (8, 0) Group  $T_{23}$

$d_K$	Polynomial	Different factorisation
21415471433	$X^8 - 15X^6 - 8X^5 + 66X^4 + 61X^3 - 57X^2 - 53X + 1$	
21415471433	$X^8 - 4X^7 - 4X^6 + 26X^5 + 2X^4 - 52X^3 + 31X + 1$	
60276601856	$X^8 - 2X^7 - 8X^6 + 8X^5 + 16X^4 - 8X^3 - 8X^2 + 2X + 1$	
60276601856	$X^8 - 4X^7 - 4X^6 + 24X^5 + 4X^4 - 42X^3 + 4X^2 + 22X - 7$	
95281280000	$X^8 - 2X^7 - 10X^6 + 14X^5 + 16X^4 - 22X^3 - 2X^2 + 8X - 2$	$5\mathbb{Z}_K = \mathfrak{p}^3\mathfrak{p}'^3\mathfrak{q}$
95281280000	$X^8 - 14X^6 - 14X^5 + 38X^4 + 54X^3 - 10X^2 - 28X - 2$	$5\mathbb{Z}_K = \mathfrak{p}\mathfrak{p}'\mathfrak{q}^3$
108105297381	$X^8 - 4X^7 - 5X^6 + 29X^5 - 14X^4 - 25X^3 + 10X^2 + 8X + 1$	
108105297381	$X^8 - 3X^7 - 9X^6 + 21X^5 + 33X^4 - 33X^3 - 54X^2 - 12X + 3$	

## REFERENCES

- [Be] K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), 1213–1237. MR **97m**:11159
- [Bu-Mc] G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), 863–911. MR **84f**:20005
- [Co] H. Cohen, *A course in computational algebraic number theory*, GTM 138, Springer-Verlag, Berlin, Heidelberg, New York, 1993. MR **94i**:11105
- [Co-Di] H. Cohen and F. Diaz y Diaz, *A polynomial reduction algorithm*, Sémin. Th. des Nombres Bordeaux (série 2) **3** (1991), 351–360. MR **93a**:11107
- [Co-Di-Ol] H. Cohen, F. Diaz y Diaz and M. Olivier, *Computing ray class groups, conductors and discriminants*, Math. Comp. **67** (1998), 773–795. MR **98g**:11128
- [Co-Hu-Mc] J. Conway, A. Hulpke and J. McKay, *On transitive permutation groups*, LMS J. Comput. Math., **1** (1998), 1–8.
- [Di-Ol] F. Diaz y Diaz and M. Olivier, *Imprimitive ninth-degree number fields with small discriminants*, Math. Comp. **64** (1995), 305–321. MR **95e**:11153
- [Ei] Y. Eichenlaub, *Problèmes effectifs de théorie de Galois en degrés 8 à 11*, Thèse, Université Bordeaux I, 1996.
- [Ei-Ol] Y. Eichenlaub and M. Olivier, *Computation of Galois groups for polynomials with degree up to eleven* (1996), Preprint.
- [Ga] F. Gassmann, *Bemerkungen zur Vorstehenden Arbeit von Hurwitz*, Math. Z. **25** (1926), 665–675.
- [Ha] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Physica-Verlag, Wien-Würtzburg, 1970. MR **42**:1795
- [Je] A. Jehanne, *Sur les extensions de  $\mathbb{Q}$  à groupe de Galois  $S_4$  et  $\tilde{S}_4$* , Acta Arith. **69** (1995), 259–276. MR **95m**:11126
- [Kw] S.-H. Kwon, *Sur les discriminants minimaux des corps quaternioniens*, Arch. Math. **67** (1996), 119–125. MR **97d**:11165
- [Pe] R. Perlis, *On the equation  $\zeta_K(s) = \zeta_{K'}(s)$* , J. Number Th. **9** (1977), 342–360. MR **56**:5503
- [Po-Za] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of Math. and its Applications, Cambridge University Press, Cambridge, 1989. MR **92b**:11074
- [Ro] X.-F. Roblot, *Unités de Stark et corps de classes de Hilbert*, C. R. Acad. Sci. Paris **323** (1996), 1165–1168. MR **97k**:11162
- [Sm-Pe] B. de Smit and R. Perlis, *Zeta functions do not determine class numbers*, Bull. Am. Math. Soc. **31** (1994), 213–215. MR **95a**:11100
- [Sm] G. W. Smith, *Some polynomials over  $\mathbb{Q}(t)$  and their Galois groups* (1993), Preprint.

LABORATOIRE A2X, UNIVERSITÉ BORDEAUX I, 351 COURS DE LA LIBÉRATION, 33405 TALENCE CEDEX, FRANCE

*E-mail address:* cohen@math.u-bordeaux.fr

*E-mail address:* diaz@math.u-bordeaux.fr

*E-mail address:* olivier@math.u-bordeaux.fr