MATHEMATICS OF COMPUTATION
VOLUME 54, NUMBER 190
APRIL 1990, PAGES 869–884

THE COMPUTATION OF SEXTIC FIELDS WITH A QUADRATIC SUBFIELD

A.-M. BERGÉ, J. MARTINET, AND M. OLIVIER

ABSTRACT. We describe four tables (one for each signature) of sixth-degree fields K containing a quadratic subfield k. The tables contain various information, including, for each possible discriminant d_K of K, a cubic polynomial which defines K/k, the discriminant of the quartic field $\tilde{k}$ such that $\tilde{k}/k$ is the quadratic extension corresponding to K/k, and the Galois group of the Galois closure $N/\mathbb{Q}$ of $K/\mathbb{Q}$.

1. INTRODUCTION

When using geometrical tools to construct tables of fields K of a given degree n, one has to deal with the following problem: when n is not a prime, it may happen that some elements $\theta \in K$, $\theta \notin \mathbb{Q}$ which are given by geometry, generate a proper subfield of K. Two methods have been used in this case. The first (the one used by Pohst in [12] to find the minimal discriminants for the degree 6) relies on the consideration of successive minima. The second, described by one of us in [11], and used by Diaz y Diaz in [4] to find the first 15 discriminants for totally imaginary octic fields, makes use of relative calculations. Here is our method: let K/k be an extension of degree 3 for some quadratic field k; the $\theta \in K$, $\theta \notin k$ given by geometry generates K over k. This enables us to make a list of polynomials such that any field K with discriminant less than a given bound (depending on the signature) can be defined by a polynomial of the mentioned list. (The choosen bounds are $6 \cdot 10^7$, $2 \cdot 10^7$, $8 \cdot 10^6$ and $4 \cdot 10^6$ for the respective signatures $(6, 0)$, $(4, 1)$, $(2, 2)$ and $(0, 3)$.)

We then remove the reducible polynomials by computing an approximation of the roots, and come to the calculation of the relative discriminant $\mathfrak{D}_{K/k}$ of K/k. This is done by a local study (note that we cannot use relative integral bases which may not exist).

We now order the polynomials by increasing absolute values of the discriminants of the corresponding fields, and test the fields with equal discriminants for isomorphism, using the previously computed roots. Among polynomials defining the same field, we choose one with smallest index f, where f is the

Received January 9, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R16, 11Y40; Secondary 11R29, 11Y16.

norm of the ideal $\mathfrak{f}$ defined by $(d_P) = \mathfrak{f}^2 \mathfrak{D}_{K/k}$, d_P being the discriminant of the polynomial P.

Finally, we determine some other data: the Galois group, and the field $\tilde{k}$ such that $\tilde{k}/k$ is the quadratic extension attached to K/k.

As an application, we obtain by class field theory results concerning the imprimitive quartic fields (resp. sextic fields with a quadratic subfield) with relative class number divisible by 3 (resp. 2).

We also get from the tables the minimal discriminants with given infinite Frobeniuses for seven isomorphism classes of transitive groups of degree 6 which have imprimitivity sets with three elements. The analogous problem for quadratic extensions of cubic fields could be solved essentially by hand. However, we intend to construct long tables of fields of this kind, in order that anybody who would like to produce a list of sixth-degree fields should not be bothered by problems caused by imprimitivity.

As a third application, we point out in the table for signature $(0, 3)$ the cubic field on the imaginary quadratic field $\mathbb{Q}(\sqrt{-19})$ defined by the polynomial

$$X^3 - X^2 - \omega X + (\omega - 1), \quad \text{with } \mathfrak{D}_{K/k} = \mathfrak{p}_7^2,$$

where $\omega = (1 + \sqrt{-19})/2$ and $\mathfrak{p}_7$ is a prime ideal of k lying above 7, and $d_K = -336091$. This field is given in the table with index equal to 5. The problem was: does there exist a power basis of $\mathbb{Z}_K$ over $\mathbb{Z}_k$? The answer is related to the following problem: let k be an imaginary quadratic field, $k^{(\mathfrak{F})}$ the ray class field of conductor $\mathfrak{F}$; thus $k^{(1)} = \mathscr{H}ilb(k)$; from work of Ph. Cassou-Noguès, J. Cougnard, V. Fleckinger, R. Schertz and M. Taylor (cf. for instance [13]), it is known that $k^{(\mathfrak{F})}/k^{(1)}$ has a power basis if certain conditions concerning $\mathfrak{F}$ or the ramification at 2 or 3 hold. These conditions are not fulfilled for $d_k = -19$ and $\mathfrak{F} = \mathfrak{p}_7$. An intensive computation seemed to show that there was no power basis; this result has recently been proved by J. Cougnard and V. Fleckinger ([3]).

Note, however, that most of the fields in the tables have an integral power basis.

2. Notation

In what follows, K is a cubic extension of a quadratic field k whose signature is denoted by (r_1, r_2); $\mathbb{Z}_K$ (resp. $\mathbb{Z}_k$) is the ring of integers of K (resp. k).

Let $\tilde{k}/k$ be the quadratic extension attached to K/k by Galois theory ($\tilde{k} = k$ is allowed); let N be the Galois closure of $K/\mathbb{Q}$, and M that of K/k. For a finite extension L'/L of number fields, $\mathfrak{D}_{L'/L}$ is the relative discriminant, whereas $d_{L'}$ stands for the absolute discriminant of L'; we write d for d_k. Similarly, d_P is the discriminant of the polynomial P.

We denote by $v_\mathfrak{p}$ (or simply v) the exponent of the prime ideal $\mathfrak{p}$ of k in a given ideal $\mathfrak{a}$ of k, and use similar notation for K, except that we then choose capital letters ($\mathfrak{P}$ and $\mathfrak{A}$); π is a uniformizing parameter at $\mathfrak{p}$; $e_\mathfrak{p}$ (or

e) is the ramification index of $\mathfrak{p}$ in k ($e = 1$ or 2); $Tr_{K/k}$ and $N_{K/k}$ are the trace and the norm of K/k ($Tr = Tr_{k/\mathbb{Q}}$ and $N = N_{k/\mathbb{Q}}$).

For an element $x \in k$ (resp. a polynomial $P \in k[X]$), x' (resp. P') is the conjugate of x (resp. P) under the conjugacy of $k/\mathbb{Q}$. Moreover, if φ is a root of P in an algebraic closure of $\mathbb{Q}$, the set of roots of P is $\{\varphi_1, \varphi_2, \varphi_3\}$ and the corresponding set for P' is $\{\varphi_1', \varphi_2', \varphi_3'\}$.

3. Inequalities

Application of [11, Theorem 2.8] yields the following inequality:

Theorem. *There exists $\theta \in \mathbb{Z}_K$ such that $K = k(\theta)$ and*

$$(3.1) \qquad \sum_{i=1}^{3} \left(|\theta_i|^2 + |\theta_i'|^2\right) \leq \frac{1}{3}\left(|Tr_{K/k}(\theta)|^2 + |Tr_{K/k}(\theta')|^2\right) + \left|\frac{4d_K}{9d_k}\right|^{\frac{1}{4}},$$

where $\{\theta_1, \theta_2, \theta_3\}$ are the roots of the minimal polynomial of θ, and $\{\theta_1', \theta_2', \theta_3'\}$ those of its conjugate.

Moreover, θ is arbitrary modulo $\mathbb{Z}_k$.

So, let D be the bound of $|d_K|$ and $B = |\frac{4D}{9d_k}|^{\frac{1}{4}}$.

Let $P(X) = X^3 - aX^2 + bX - c$ be the minimal polynomial of θ, and $(1, \omega)$ be the standard basis of $\mathbb{Z}_k/\mathbb{Z}$ ($\omega = (1+\sqrt{m})/2$ if $d = m$ is odd, and $\omega = \sqrt{m}$ if $d = 4m$).

Replacing θ by $\theta + \alpha$ for some $\alpha \in \mathbb{Z}_k$, we may choose $a = p + q\omega$, with p and $q \in \{-1, 0, 1\}$, and even (by changing θ in $-\theta$), $p = 0$ or 1. Finally, as P' and P define the same field (up to conjugacy), it suffices to consider four values of a, say $\{0, 1, \omega, 1+\omega\}$.

In the particular case $d = -4$ (resp. $d = -3$), multiplication by i (resp. j) allows us to choose a among $\{0, 1, 1+i\}$ (resp. $\{0, 1, 2+j\}$).

Now, such an a being fixed, we determine the possible b's via the element $e = a^2 - 3b$ of $\mathbb{Z}_k$ for which we have a tolerably good bound in terms of $\sum_{1\leq i\leq 3} |\theta_i|^2$:

Lemma. *Let $\theta_1, \ldots, \theta_m$ be m complex numbers ($m \geq 1$). Then, we have*

$$\left|(m-1)\left(\sum_{1\leq i\leq m} \theta_i\right)^2 - 2m \sum_{1\leq i<j\leq m} \theta_i\theta_j\right| + \left|\sum_{1\leq i\leq m} \theta_i\right|^2 \leq m \sum_{1\leq i\leq m} |\theta_i|^2,$$

and equality holds if and only if all the θ_i's are real, in which case we have

$$(m-1)\left(\sum_{1\leq i\leq m} \theta_i\right)^2 - 2m \sum_{1\leq i<j\leq m} \theta_i\theta_j \geq 0.$$

The proof is based on the following equalities:

$$(m-1)\left(\sum_{1\le i\le m}\theta_i\right)^2 - 2m\sum_{1\le i<j\le m}\theta_i\theta_j = \sum_{1\le i<j\le m}(\theta_i-\theta_j)^2$$

and

$$\sum_{1\le i<j\le m}|\theta_i-\theta_j|^2 + \left|\sum_{1\le i\le m}\theta_i\right|^2 = m\sum_{1\le i\le m}|\theta_i|^2.$$

(Note that the inequality between arithmetic and geometric means gives (cf. [11]), for real θ_i's,

$$(m-1)\left(\sum_{1\le i\le m}\theta_i\right)^2 - 2m\sum_{1\le i<j\le m}\theta_i\theta_j \ge \frac{m(m-1)}{2}\, d_P^{\frac{2}{m(m-1)}},$$

where $P(X)=\prod_{1\le i\le m}(X-\theta_i)\in\mathbb{C}[X]$; this bound is optimal for $m=2$, while, for $m=3$, a direct computation of d_P enables us to multiply the right-hand side by $2^{1/3}$.)

In our context, and with the notation of the theorem, the result of the above lemma can be written as

$$\frac{2}{3}|e|+\frac{1}{3}|a|^2 \le \sum_{1\le i\le 3}|\theta_i|^2, \qquad \frac{2}{3}|e'|+\frac{1}{3}|a'|^2 \le \sum_{1\le i\le 3}|\theta_i'|^2, \tag{3.2}$$

and from (3.1) we get

$$|e|+|e'| \le \frac{3}{2}B. \tag{3.3}$$

It follows that $e\in\mathbb{Z}_k$ satisfies the conditions

$$|Tr(e)| \le \frac{3}{2}B \quad\text{and}\quad |N(e)| \le \left(\frac{3}{4}B\right)^2.$$

From the finite set of (e, e') in $\mathbb{Z}_k$ satisfying the above inequalities, we eliminate those for which (3.3) is not valid and those not congruent to a^2 modulo 3.

Actually, we use sharper inequalities for signature $(6, 0)$ and $(4, 1)$, derived from the condition $e>0$ when $d_P>0$.

The coefficients a and b being now chosen, we determine the set of suitable c's by use of (3.1), via the inequality between arithmetic and geometric means.

For instance

$$|c| = \left(\prod_{1\le i\le 3}|\theta_i|^2\right)^{\frac{1}{2}} \le \left(\frac{\sum_{1\le i\le 3}|\theta_i|^2}{3}\right)^{\frac{3}{2}}.$$

Let us denote by A, C, C' the following constants:

$$A=\frac{1}{3}(|a|^2+|a'|^2)+B, \qquad C=A-\frac{1}{3}(|a'|^2+2|e'|), \qquad C'=A-\frac{1}{3}(|a|^2+2|e|).$$

We get

$$|N(c)| \leq \left(\frac{A}{6}\right)^3, \quad \text{and then} \quad \min(|c|, |c'|) \leq \left(\frac{A}{6}\right)^{\frac{3}{2}}.$$

From the lemma we also obtain weaker inequalities

$$|c| \leq \left(\frac{C}{3}\right)^{\frac{3}{2}} \quad \text{and} \quad |c'| \leq \left(\frac{C'}{3}\right)^{\frac{3}{2}}.$$

Finally, we obtain universal (relative to signature) inequalities:

$$|c| + |c'| \leq \left(\frac{A}{6}\right)^{\frac{3}{2}} + \max\left(\left(\frac{C}{3}\right)^{\frac{3}{2}}, \left(\frac{C'}{3}\right)^{\frac{3}{2}}\right), \tag{3.4}$$

and

$$|Tr(c)| \leq \left(\frac{A}{6}\right)^{\frac{3}{2}} + \max\left(\left(\frac{C}{3}\right)^{\frac{3}{2}}, \left(\frac{C'}{3}\right)^{\frac{3}{2}}\right).$$

Actually, we can improve them in the totally imaginary case, replacing (3.4) by $|c| \leq (\frac{A}{6})^{\frac{3}{2}}$. In contrast, for signatures $(6, 0)$ or $(4, 1)$, testing $d_P > 0$ (or $d_{P'} > 0$) gives us sharper (and independent of D) bounds for c, c' and $Tr(c)$, using the equality

$$27d_P = 4e^3 - (2a^3 - 9ab + 27c)^2.$$

Now, for each pair of conjugate integers of k corresponding to given $Tr(c)$ and $N(c)$, we test back the conditions (3.4). Of course, we take into account, when possible, all symmetries.

For each polynomial P of the remaining set with suitable sign of d_P and $d_{P'}$, we compute an approximation of the roots θ_i of P and θ'_i of P' by Cardano formulae and test whether (3.1) is fulfilled.

It remains to verify that P is irreducible over $k[X]$, in other words (P being cubic), whether one of the roots of P belongs to k. We then test, for all reasonable pairings (θ_i, θ'_j) (9, 3, 1, 3 tests for $r_1 = 6, 4, 2, 0$ respectively), if $\theta_i + \theta'_j$ and $\theta_i\theta'_j$ are, or are not, in $\mathbb{Z}$. In practice, we guess from a weak accuracy of θ_i and θ'_j the possible integers, and substitute in P by a formal computation.

4. Relative discriminant

We write now $\mathfrak{D}$ and $\mathfrak{d}$ for the respective discriminants $\mathfrak{D}_{K/k}$ and $\mathfrak{D}_{\tilde{k}/k}$. (Recall that $\mathfrak{d} = \mathbb{Z}_k$ if $\tilde{k} = k$, i.e., if K/k is cyclic.)

Let $\mathfrak{g}$ be the conductor of the cyclic extension $M/\tilde{k}$. It can be proved that $\mathfrak{g}$ comes from an ideal of k, still denoted by $\mathfrak{g}$; this is a consequence of [14, Ch. IV, §2, Cor.1 to Prop. 9]. Note that $\mathfrak{g}$ is divisible exactly by the ideals of k which are totally ramified in K/k.

Proposition 4.1. *We have* $\mathfrak{D} = \mathfrak{d}\mathfrak{g}^2$.

This is obvious when K/k is cyclic. When K/k is dihedral, $\mathfrak{D}$ is the Artin conductor of the irreducible degree-2 character of $\mathcal{G}al(M/k)$, and the induction formula gives the proposition, since $\mathfrak{g}$ is the conductor of a degree-one character of $M/\tilde{k}$.

Proposition 4.2. *The g.c.d. of* $\mathfrak{d}$ *and* $\mathfrak{g}$ *divides* (3).

For the first ramification group in M/k, if nontrivial, is a 3-group.

We want now to calculate $\mathfrak{d}$ and $\mathfrak{g}$ from the knowledge of the polynomial P which defines K/k.

Of course, $v(\mathfrak{d})$ and $v(\mathfrak{g})$ are zero when $v(d_P) = 0$.

For $v(d_P)$ nonzero, we make a local study of K/k at $\mathfrak{p}$. In the sequel, $k_\mathfrak{p}$ (resp. $K_\mathfrak{p}$) denotes the completion of k (resp. K) at $\mathfrak{p}$; note that $K_\mathfrak{p}$ need not be a field. We have the obvious congruences

$$v(d_P) \equiv v(\mathfrak{D}) \equiv v(\mathfrak{d}) \pmod 2.$$

Using elementary properties of ramification in quadratic extensions, we prove the following two results:

Assertion 1. *If* $v(d_P)$ *is odd, then*

$$v(\mathfrak{d}) = \begin{cases} 1 & \text{if } p \geq 3, \\ 3 & \text{if } p = 2 \text{ and } e = 1, \\ 5 & \text{if } p = 2 \text{ and } e = 2. \end{cases}$$

Moreover, $v(\mathfrak{g}) = 0$ *if* $p \neq 3$ *or if* $p = 3$ *and* $v(d_P) = 1$.

Assertion 2. *If* $v(d_P)$ *is even and if* $p \neq 2$, *then* $v(\mathfrak{d}) = 0$.

We are left with the following two problems:

(i) To compute $v(\mathfrak{g})$ for $v(d_P)$ even and nonzero, and for $p = 3$, $v(d_P) \geq 3$ and odd.

(ii) To compute $v(\mathfrak{d})$ for $p = 2$, when $v(d_P)$ is even and nonzero (then, P splits in $k_\mathfrak{p}$).

When there are at least two prime ideals in K lying above $\mathfrak{p}$, by classical results of Kummer extensions (cf. e.g. [7, §39]), we have:

Assertion 3. *If* P *splits in* $k_\mathfrak{p}$,

1) $K_\mathfrak{p}$ *is isomorphic to* $k_\mathfrak{p} \times \tilde{k}_\mathfrak{p}$, *so that* $v(\mathfrak{g}) = 0$.

2) *If* $p = 2$ *and* $v(d_P)$ *is even and nonzero, write* $d_P = \pi^{2x}\, a$, *with* $a \in k$, a $\mathfrak{p}$*-unit, and*

$$t = \min\{u \in \mathbb{N} \mid \ a \text{ is a square modulo } \mathfrak{p}^{2(e-u)}\} \qquad (0 \leq t \leq e).$$

We then have $v(\mathfrak{d}) = 2t$.

Finally, when there is a unique ideal lying above $\mathfrak{p}$, we use the obvious assertion:

Assertion 4.

1) *If* $\mathfrak{p}$ *is inert in* K/k, *then* $v(\mathfrak{D}) = 0$.
2) *If* $\mathfrak{p}$ *is totally ramified in* K/k,
   a) *if* $p \neq 3$, *then* $v(\mathfrak{g}) = 1$, $v(\mathfrak{d}) = 0$,
   b) *if* $p = 3$, *then* $v(\mathfrak{g}) = (v(\mathfrak{D}) - v(\mathfrak{d}))/2$, $v(\mathfrak{d}) = 0$ *or* 1 *according to the parity of* $v(d_P)$; *in this last case,* $v(\mathfrak{D})$ *is given by the discriminant of an Eisenstein polynomial which defines the extension* K/k.

We now describe the **Disc** algorithm which either proves that P splits in $k_{\mathfrak{p}}$, or proves that it is inert in K/k, or produces an Eisenstein polynomial which defines the same extension.

Disc 1. If $v(d_P) = 0$, the algorithm terminates with $v(\mathfrak{D}) = 0$.

Disc 2. If $v(d_P)$ is odd and $p \neq 3$, or $p = 3$ and $v(d_P) = 1$, use Assertion 1 and the algorithm terminates.

Disc 3. Factorize P mod $\mathfrak{p}$ (there is at least a double root mod $\mathfrak{p}$).

Disc 4. If P possesses a simple root mod $\mathfrak{p}$ (then P splits in $k_{\mathfrak{p}}$), use Assertion 3 and the algorithm terminates.

Disc 5. Make a translation on X in $P(X)$, in order that $P(X) = X^3 - aX^2 + bX - c$, with $v(a)$, $v(b)$ and $v(c) \geq 1$. If $v(c) = 1$, then P is Eisenstein; use Assertion 4 and the algorithm terminates.

Disc 6. If $v(b) = 1$, then $\mathfrak{p}$ splits in K (use the Newton polygon). Use Assertion 3 and the algorithm terminates.

Disc 7. If $v(c) \geq 3$, then replace P by the polynomial $Q(X) = X^3 - \frac{a}{\pi}X^2 + \frac{b}{\pi^2}X - \frac{c}{\pi^3}$, with $v(d_Q) = v(d_P) - 6$. Go to **Disc 1.**

Disc 8. The minimal polynomial of $\frac{\theta^2}{\pi}$,

$$R(X) = X^3 - \frac{(a^2 - 2b)}{\pi}X^2 + \frac{(b^2 - 2ac)}{\pi^2}X - \frac{c^2}{\pi^3},$$

with $v(d_R) = v(d_P) - 2$, is Eisenstein. Use Assertion 4 and the algorithm terminates.

5. Isomorphisms

In this section and the next ones, all number fields are in a given algebraic closure $\mathbb{Q}$ of $\mathbb{Q}$. Let k be a number field and let K and L be two extensions of k with the same degree m. We write $K = k(\theta)$ and $L = k(\varphi)$, where θ

and φ are algebraic integers defined by their minimal polynomials P and Q in $\mathbb{Z}_k[X]$. For every embedding $\tau\colon k \to \mathbb{C}$, let $\theta_{i,\tau}$ and $\varphi_{j,\tau}$ be the conjugates of θ and φ above τ.

If K and L are isomorphic, there exists a permutation $\sigma \in S_m$ such that for all $h \in \mathbb{N}$, the sums

$$\alpha_{\tau,h} = \sum_{1 \le i \le m} \theta_{i,\tau}^h \varphi_{\sigma(i),\tau}$$

belong to $\tau(k)$ (and even to $\mathbb{Z}_{\tau(k)}$).

Conversely, if the $\alpha_{\tau,h}$'s belong to $\tau(k)$ (for one τ), the solution $(x_0, x_1, \ldots, x_{m-1})$ in $\mathbb{Q}^m$ of the linear system

$$\sum_{0 \le j \le m-1} x_j \theta_{i,\tau}^j = \varphi_{\sigma(i),\tau}, \qquad i = 1, \ldots, m,$$

belongs to $\tau(k)^m$, since it is also the solution of the linear system

$$\sum_{0 \le j \le m-1} x_j \sum_{1 \le i \le m} \theta_{i,\tau}^{j+h} = \alpha_{\tau,h}, \qquad h = 0, \ldots, m-1,$$

with coefficients in $\tau(k)$ and nonzero determinant, namely $\tau(d_P)$.

So, for every h, we test whether $\alpha_{\tau,h}$ belongs to $\tau(k)$, by computing an approximation of its conjugates: since θ and φ are integral, the $\alpha_{\tau,h}$'s must be the roots of monic polynomials in $\mathbb{Z}[X]$. We guess these polynomials, and then verify that the α_j's are integers of k.

In practice, we test the existence of an isomorphism only when K and L have the same signature and the same relative (ideal) discriminant.

Let us go back to the case $[K\colon k] = 3$ and $[k\colon \mathbb{Q}] = 2$. For $r_1 = 6$ (resp. 4, 2, 0), the numbers of permutations of the $\varphi_{i,\tau}$ to consider are 36 (resp. 12, 4, 6), and these numbers are to be doubled if $\mathfrak{D}_{K/k}$ is an invariant ideal of k, for K and L can be isomorphic without being k-isomorphic. (Note that for arbitrary sextic fields, the numbers of permutations to be considered are respectively 720, 48, 16, 48.)

6. Galois groups

Using a Galois action on a primitive element of K, one can attach to each sextic field a transitive permutation group of degree six. The list of such groups is given in [2]; seven of those groups correspond to a sextic field with quadratic subfield, and only one of them (denoted by G_{36}^+) is even.

In the table below, we give all possible groups for K, $\tilde{k}$ and K_0, where K_0 —if it exists— is a cubic subfield of K (C_n is the cyclic group of order n, and D_n is the dihedral group of order $2n$).

type of K	type of $\tilde{k}$	type of K_0	possible r_1's
C_6	C_2	C_3	6, 0
$D_3 \simeq S_3$	C_2	D_3	6, 0
$D_6 \simeq S_3 \times C_2$	C_2^2	D_3	6, 2, 0 (*)
$G_{18} = C_3^2 \rtimes C_2 \simeq C_3 \times D_3$	C_2		6, 0
$G_{36}^+ = C_3^2 \rtimes C_4$	C_4		6, 2
$G_{36}^- = C_3^2 \rtimes C_2^2 \simeq D_3 \times D_3$	C_2^2		6, 2, 0
$G_{72} = C_3^2 \rtimes D_4$	D_4		6, 4, 2, 0

(*) two possible Frobenius substitutions when $r_1 = 0$.

We now just have to test the nature of $\tilde{k}$ and K_0 (when it exists). First, the type of $\tilde{k}/\mathbb{Q}$ is: C_2 if d_P is a square in $\mathbb{Z}_k$, C_2^2 if $N(d_P)$ is a square but d_P is not, C_4 if $N(d_P)/d_k$ is a square, and D_4 otherwise.

Finally, it is easy to see that if K has a cubic subfield K_0, then the conjugate θ' of θ over K_0 is defined by P', and if $\theta + \theta'$ is not in $\mathbb{Z}$, $K_0 = \mathbb{Q}(\theta + \theta')$, otherwise, $K_0 = \mathbb{Q}(\theta\theta')$. This provides a simple method for finding the type of K_0, based on a straightforward computation of $(\theta_i + \theta'_{\sigma(i)})$ and $(\theta_i\theta'_{\sigma(i)})$ for σ in S_3. Moreover, the type of K_0 is C_3 if d_{K_0} is a square, and D_3 if not; note that K_0 is cyclic if and only if the discriminant of $\theta + \theta'$ (or $\theta\theta'$) is a square.

These obvious assertions allow us to compute the type of K, using the following **Gal** algorithm:

Gal 1. If $N(d_P)$ is a square, go to **Gal 4**.

Gal 2. If $N(d_P)/d_k$ is a square, K is of type G_{36}^+ and the algorithm terminates.

Gal 3. K is of type G_{72} and the algorithm terminates.

Gal 4. If K_0 exists, go to **Gal 7**.

Gal 5. If d_P is a square in $\mathbb{Z}_k$, K is of type G_{18} and the algorithm terminates.

Gal 6. K is of type G_{36}^- and the algorithm terminates.

Gal 7. If d_{K_0} is a square, K is of type C_6 and the algorithm terminates.

Gal 8. If d_{K_0}/d_k is a square, K is of type D_3 and the algorithm terminates.

Gal 9. K is of type D_6 and the algorithm terminates.

7. Remarks on class numbers

For a number field L, let $\mathscr{C}l_L$ be the ideal class group of L; for a finite extension L'/L, let $\mathscr{C}l_{L'/L}$ be the relative class group of L'/L, i.e., the kernel of the norm $N_{L'/L}: \mathscr{C}l_{L'} \to \mathscr{C}l_L$; we denote by $h_{L'/L}$ the order of $\mathscr{C}l_{L'/L}$.

In this section, we discuss the divisibility of $h_{\tilde{k}/k}$ by 3 (resp. of $h_{K/k}$ by 2) in connection with the existence of some cubic (resp. quadratic) unramified extension of $\tilde{k}$ (resp. K).

Let F be a number field; by class field theory (see, e.g., [1]), there is a unique one-to-one correspondence between unramified abelian extensions and subgroups of $\mathscr{C}l_F$, which maps F'/F on the norm group $H = N_{F'/F}(\mathscr{C}l_{F'})$; the Artin map $\omega_{F'/F}: \mathscr{C}l_F \to \mathscr{G}al(F'/F)$ is onto, and its kernel is the norm group.

The same considerations apply to abelian extensions which are solely assumed to be unramified at finite primes, with $\mathscr{C}l_F$ replaced by $\mathscr{C}l_F^+$, the narrow class group.

7.1. *Assume first that F is quadratic over some subfield E.*

Since F is Galois over E, then F'/E is Galois if and only if H is invariant under $\mathscr{G}al(F/E)$, and, when this condition is fulfilled, $\omega_{F'/F}$ is a homomorphism of $\mathscr{G}al(F/E)$-modules (cf., for instance, [14, Ch. 11, §3]).

The number of cubic unramified extensions of F which are cyclic (resp. dihedral) over E is equal to the number of order-3 subgroups of $\mathscr{C}l_E$ (resp. $\mathscr{C}l_{F/E}$): for, denoting by $\{1, \tau\}$ the Galois group of F/E, the cubic unramified extension F' of F which corresponds to a given subgroup H of index 3 of $\mathscr{C}l_F$ invariant under τ is cyclic (resp. dihedral) over E if and only if τ acts on $\mathscr{C}l_F/H$ by $\tau(\bar{x}) = \bar{x}$ (resp. $\tau(\bar{x}) = \bar{x}^{-1}$). In the canonical isomorphism $\mathscr{C}l_{F,3} \simeq \mathscr{C}l_{E,3} \times \mathscr{C}l_{F/E,3}$ between 3-components, τ acts trivially on $\mathscr{C}l_{E,3}$, and by $\bar{x} \mapsto \bar{x}^{-1}$ on $\mathscr{C}l_{F/E,3}$. Hence, the subgroups H of index 3 invariant by τ that we consider are in one-to-one correspondence with the subgroups of index 3 of $\mathscr{C}l_{E,3}$ (resp. $\mathscr{C}l_{F/E,3}$) in the cyclic (resp. dihedral) case. Our claim is then established by a duality argument, these subgroups being in one-to-one (noncanonical) correspondence with the subgroups of order 3.

Accordingly, we see that the number of cubic extensions E'/E with corresponding quadratic extension F/E and with discriminant $\mathfrak{D}_{E'/E} = \mathfrak{D}_{F/E}$ is $(3^r - 1)/2$, where r is the 3-rank of the group $\mathscr{C}l_{F/E}$.

We now apply the above results to the groups $\mathscr{C}l_{\tilde{k}/k}$, counting cubic extensions K/k with $\mathfrak{D}_{K/k} = \mathfrak{D}_{\tilde{k}/k}$. One has $d_K = d_k d_{\tilde{k}}$, hence $|d_K| \leq |d_{\tilde{k}}|^{\frac{3}{2}}$. Thus, a table of fields K with $|d_K| \leq D$ for some D allows us to find all imprimitive fields $\tilde{k}$ of degree 4 with relative class number divisible by 3 whose discriminants satisfy the inequality $|d_{\tilde{k}}| \leq D^{\frac{2}{3}}$, and even $|d_{\tilde{k}}| \leq (\sqrt{3}D)^{\frac{2}{3}}$ (resp. $(2D)^{\frac{2}{3}}$) when $\tilde{k}$ is (resp. is not) of mixed signature, if we except bicyclic fields $\tilde{k}/\mathbb{Q}$ (and then, $\mathscr{C}l_{\tilde{k}}$ is the direct product of the class groups of the 3 quadratic subfields). When $\tilde{k}/\mathbb{Q}$ is cyclic, the cubic unramified extensions K/k we must consider are of type G_{36}^+, and there is no occurrence within the size of our tables. (It is known, cf. [5] and [6], that $\mathscr{C}l_{\tilde{k}/k}$ is of order divisible by 3 only for very large discriminants.) We are thus left with dihedral quartic fields $\tilde{k}$ (K is of type G_{72}). Then the four possibilities

$\tilde{r}_1 = 4,\ 2,\ 0$ and k real , $\tilde{r}_1 = 0$ and k imaginary correspond to cubic extensions K/k with $r_1 = 6,\ 4,\ 2,\ 0$.

In our tables, we find the first five discriminants of such fields $\tilde{k}$ (of type D_4) in signature $(4, 0)$, the first thirty-one in signature $(2, 1)$, the first fifty-four in signature $(0, 2)$ with k real, and the first forty-eight in signature $(0, 2)$ with k imaginary. We give below the list of the first five for each signature.

$(4, 0)$	$(2, 1)$	$(0, 2)$, k real	$(0, 2)$, k imag.
97025	−20975	6025	3897
135232	−23488	6208	5517
193225	−24048	7025	5648
196025	−28975	10225	7677
230009	−29975	10525	8001

Looking at systems of four nonisomorphic fields K with equal discriminants, we found 26 examples of fields $\tilde{k}$ of type D_4 with $\mathscr{C}l_{\tilde{k}/k}$ of 3-rank 2: fourteen over $\mathbb{Q}(\sqrt{-3})$, one over $\mathbb{Q}(i)$, ten imaginary over $\mathbb{Q}(\sqrt{5})$, and one of mixed signature over $\mathbb{Q}(\sqrt{5})$. We give below the value of $N(\mathfrak{D}_{\tilde{k}/k})$ for these fields:

$d_k = -3$: 41617, 73849, 83269, 88432, 103557, 109969, 111261, 116521, 120397, 122437, 126901, 142141, 144741, 146341.

$d_k = -4$: 54713.

$d_k = 5$ and $\tilde{k}$ imaginary: 8921, 11909, 15445, 18749, 20329, 26669, 39344, 43321, 44669, 48809.

$d_k = 5$ and $\tilde{k}$ of mixed signature: 127271.

7.2. *Assume now that F is cubic over some subfield E.*

We discuss here the parity of $h_{F/E}$ or $h^+_{F/E}$ in connection with the existence of some special primitive quartic extension E'/E.

The quadratic extensions F'/F, including F itself, can be given a group structure denoted by $\mathscr{Q}(F)$, for which $F'_1 F'_2 = F(\sqrt{a_1 a_2})$ if $F'_1 = F(\sqrt{a_1})$ and $F'_2 = F(\sqrt{a_2})$, and the norm $N_{F/E}$ induces a homomorphism $\mathscr{N}$ from $\mathscr{Q}(F)$ to $\mathscr{Q}(E)$ (the analogous group for E).

Since $[F: E]$ is odd, $\mathscr{N}$ is onto, and $i^*: F'/E \mapsto FF'/F$ is an injective section of $\mathscr{N}$ ($\mathscr{N} \circ i^* = \mathrm{id}$). We thus have a direct decomposition $\mathscr{Q}(F) \simeq \mathrm{Ker}\,\mathscr{N} \times \mathscr{Q}(E)$. The same results hold for the subgroup $\mathscr{Q}(F)^{n.r.}$ of those elements of $\mathscr{Q}(F)$ which are unramified over F.

If F/E is non-Galois, primitive quartic extensions E'/E associated with F by Galois theory are in one-to-one correspondence with quadratic extensions $F'/F \in \mathrm{Ker}\,\mathscr{N}$ (one must accept F itself as a quartic field when $F' = F$).

Furthermore, an easy calculation with Artin conductors shows the relation

$$\mathfrak{D}_{E'/E} = \mathfrak{D}_{F/E}\,\mathfrak{A}^2, \quad \text{where } \mathfrak{A}^2 = N_{F/E}(\mathfrak{D}_{F'/F}).$$

Hence, quartic extensions E'/E with $\mathfrak{D}_{E'/E} = \mathfrak{D}_{F/E}$ are in bijection with extensions F'/F in $\mathrm{Ker}\,\mathscr{N}$ unramified at finite primeš.

Now, by class field theory, the group $\mathscr{Q}(F)^{n.r.}$ (resp. $\mathscr{Q}(E)^{n.r.}$) is in one-to-one correspondence with the group of order-2 characters of $\mathscr{C}l_F$ (resp. $\mathscr{C}l_E$), and analogous results hold for class groups in the narrow sense. By the canonical isomorphism

$$\mathscr{C}l^+_{F,2} \simeq \mathscr{C}l^+_{E,2} \times \mathscr{C}l^+_{F/E,2},$$

the number of primitive quartic extensions E'/E (up to conjugacy) corresponding to F/E with $\mathfrak{D}_{E'/E} = \mathfrak{D}_{F/E}$ is equal to the number of order-2 characters of $\mathscr{C}l^+_{F/E}$, and then, by duality, is equal to the number of order-2 elements in $\mathscr{C}l^+_{F/E}$. Note that if F/E is Galois, one must divide by 3 the number of characters.

We now apply these considerations to the groups $\mathscr{C}l_{K/k}$ and $\mathscr{C}l^+_{K/k}$. The following table gives the number of real places to consider in E', k, K and F' above each infinite place of k, and the nature of the classes of K involved above each infinite place of k : "o" for ordinary, "n" for narrow.

E'	k	K	F'	$\mathscr{C}l_K$ or $\mathscr{C}l^+_K$
(4,4)	2	(3,3)	(6,6)	(o,o)
(4,2)	2	(3,1)	(6,2)	(o,o)
(4,0)	2	(3,3)	(6,2)	(o,n)
(2,2)	2	(1,1)	(2,2)	(o,o)
(2,0)	2	(3,1)	(2,2)	(n,o)
(0,0)	2	(3,3)	(2,2)	(n,n)
(0,0)	0	(0,0)	(0,0)	(o,o)

Using tables of octic fields taken from [8], [9], and [10], we find six examples of extensions K/k with groups $\mathscr{C}l_{K/k}$ of even order: five with $k = \mathbb{Q}(\sqrt{-3})$, one with $k = \mathbb{Q}(\sqrt{-1})$, and one with even group $\mathscr{C}l^+_{K/k}$ over $\mathbb{Q}(\sqrt{5})$ and signature $(4, 1)$ for K.

d_k	d_K	cubic polynomial on k
-4	-440896	$X^3 - X^2 - 3X + 4$
-3	-447471	$X^3 - X^2 + (2 - 4\omega)X + (1 - \omega)$
-3	-599103	$X^3 - X^2 + (4 - 3\omega)X - 4$
-3	-706023	$X^3 - X^2 - 3\omega X + (1 + 2\omega)$
-3	-739071	$X^3 - (1 + \omega)X^2 - (6 - 2\omega)X - 3(1 - \omega)$
-3	-771471	$X^3 + (3 - \omega)X - 3\omega$
5	-1151375	$X^3 - \omega X^2 - 4\omega X + (3 + 5\omega)$

Let us look more closely at the case $d_k < 0$ (resp. K totally real). Diaz y Diaz's unconditional lower bounds for discriminants in degree 12 give, for K with even class number, the lower bound $|d_K| \geq 165923$ (resp. $d_K \geq 11956734$). Using lower bounds in degree 8 together with the relation $d_{E'} = d_k d_K$, one obtains $|d_K| \geq 1052356/|d_k|$ (resp. $d_K \geq 159055768/d_k$). Then,

the trivial inequality $|d_k|^3 \leq d_K$ only gives $|d_K| \geq |d_{E'}|^{\frac{3}{4}}$, and finally $|d_K| \geq 32857$ (resp. $d_K \geq 1416323$). However, we get better results when k has a small discriminant, e.g. $|d_K| \geq 350786$ for $d_k = -3$, and $d_K \geq 31811154$ for $d_k = 5$. For $d_k < 0$, we can do a little more: since Diaz y Diaz found in [4] the first 15 totally imaginary octic fields, we can prove the inequality $|d_K| \geq 1656111/|d_k|$ whenever K is totally imaginary with exactly one exception, namely the field K with discriminant $d_K = -3^3 \cdot 16573 = -447471$. (It is now known (Diaz y Diaz) that all primitive quartic extensions E'/k have discriminant greater than 330,000,000; thus, for K totally real of even class number, one has the inequality $d_K \geq 330{,}000{,}000/d_k$.)

8. Algorithm

Field 1. Using the inequalities of §3, we establish a list of polynomials such that any field with discriminant below the given bound D can be defined by at least one polynomial of the table.

For each polynomial, we compute the roots by Cardano's formulae, and get rid of the reducible ones, and of those which do not satisfy the inequality (3.1).

Field 2. We compute the relative discriminant $\mathfrak{D}_{K/k}$ of K/k by the **Disc** algorithm of §4, and suppress P if d_K is bigger than the bound D.

Then, we order fields by increasing discriminants and determine $\mathfrak{D}_{\hat{k}/k}$ and $d_{\hat{k}}$.

Field 3. We test the fields with equal discriminants for isomorphism, as detailed in §5.

Field 4. We use the **Gal** algorithm to compute the Galois group as explained in §6.

9. Tables

The algorithm **Field** is implemented on a station "Matra/Sun 3/260" with MC 68020 cpu at 25 Mhz, 16 Mbytes of main memory, under UNIX system environment.

With the bound $6 \cdot 10^7$ (resp. $2 \cdot 10^7$, $8 \cdot 10^6$ and $4 \cdot 10^6$) for $r_1 = 6$ (resp. 4, 2, 0), there are 1057 (resp. 2646, 2055, 4041) sextic fields.

Let us give a few statistics on the first thousand fields for each signature.

For $r_1 = 6$ to 0, the number of polynomials we had to handle was 205529 (resp. 55299, 69027, 30994). Hence, it is no wonder that the computation time is much greater in the totally real case, as summarized below, together with the distribution of the fields in dependence on the possible types.

r_1	$\lvert d_K\rvert$ max.	time	C_6	D_3	D_6	G_{18}	G_{36}^+	G_{36}^-	G_{72}
6	57405413	15 h 30'	25	12	48	31	1	2	881
4	8581375	2 h 50'	×	×	×	×	×	×	1000
2	3982000	4 h 40'	×	×	91	×	6	32	871
0	1102400	3 h 30'	6	17	77	38	×	5	857

(" × " means "impossible"; "time" is the running time of the algorithm.)

Note that among the 77 totally imaginary fields of type D_6, only 5 correspond to a real cubic subfield (this is indicated in the tables by the appendix "r" or "i").

We give now a few comments about the index f alluded to in the introduction (f is the absolute norm of the $\mathbb{Z}_k$-index of $\mathbb{Z}_k[\theta]$ in $\mathbb{Z}_K$, where $K = k(\theta)$). The smallest index f we found is equal to 1 except for very few cases (22, 4, 24 and 30 exceptions for $r_1 = 6$, 4, 2, and 0) among the first thousand fields, i.e., most of the time, the algorithm actually yields an integral power basis $(1, \theta, \theta^2)$ for K/k. Let us look more closely at the first three exceptions in the totally imaginary case, namely the fields with discriminants $d_K = (-8)^3 \cdot 625$, $(-19)^3 \cdot 49$ (the ones referred to in the introduction), and $(-20)^3 \cdot 49$, for which we found $f = 2$, 5 and 3, respectively (actually the smallest possible values for f). That f must be greater than 1 comes from local reasons in the first case (f must be even), from [3] in the second case, and from the fact that $\mathbb{Z}_K$ is not a free $\mathbb{Z}_k$-module in the last case.

We give below the minimal discriminants of sextic fields with quadratic subfield for each signature and each possible type

sign.	(6, 0)	(4, 1)	(2, 2)	(0, 3)
type				
C_6	300125	×	×	-16807
D_3	810448	×	×	-12167
D_6	2738000	×	66125	imag. -14283 real -309123
G_{18}	722000	×	×	-9747
G_{36}^+	55130625	×	525625	×
G_{36}^-	27848000	×	242000	-309123
G_{72}	485125	-104875	30125	-11691

(" × " means "impossible")

Finally, the following table shows the coincidences of discriminants among the first thousand fields of each signature.

r_1	6	4	2	0
2 fields	6	23	38	40
3 fields	0	2	9	6
4 fields	0	0	7	0

sig.(6,0)

300125	5	2401	5	C6r	1	$X^3-(7+7\omega)X+(7+14\omega)$	$(245+392\omega)$
371293	13	169	13	C6r	1	$X^3-\omega X^2+(-10+5\omega)X+(2-\omega)$	$(10777-4680\omega)$
453789	21	49	21	C6r	1	$X^3-\omega X^2+(-1+\omega)X+(-3+\omega)$	$(21-7\omega)$
485125	5	3881	97025	G72	1	$X^3+(-6-7\omega)X+(7+10\omega)$	$(1741+2816\omega)$
722000	5	5776	5	G18	1	$X^3-X^2+(-5-4\omega)X+(-1-6\omega)$	$(232+364\omega)$
810448	37	16	37	D3r	1	$X^3-X^2+(-5-2\omega)X+(-5-2\omega)$	$(244+96\omega)$
820125	5	6561	5	C6r	1	$X^3+(-6-6\omega)X+(6+11\omega)$	$(81+81\omega)$
966125	5	7729	193225	G72	1	$X^3-X^2+(-4-5\omega)X+(-1-3\omega)$	$(1381+2232\omega)$
980125	5	7841	196025	G72	1	$X^3-(1+\omega)X^2+(-3+\omega)X+(-1+\omega)$	$(85+8\omega)$
1075648	28	49	28	C6r	1	$X^3-\omega X^2+\omega$	(7)

sig.(4,1)

-104875	5	-839	-20975	G72	1	$X^3-(2+2\omega)X-(1+\omega)$	$(106+175\omega)$
-144875	5	-1159	-28975	G72	1	$X^3-\omega X^2-(2+3\omega)X+(8+13\omega)$	$(-4163-6736\omega)$
-149875	5	-1199	-29975	G72	1	$X^3-\omega X^2+(-4+3\omega)X+(-2+\omega)$	$(581-360\omega)$
-158875	5	-1271	-31775	G72	1	$X^3-(1+\omega)X^2+(3-\omega)X+(-5+3\omega)$	$(-931+576\omega)$
-174875	5	-1399	-34975	G72	1	$X^3-\omega X^2+(4-3\omega)X+(8-5\omega)$	$(-2459+1520\omega)$
-187904	8	-367	-23488	G72	1	$X^3+(-5-2\omega)X+(-3-3\omega)$	$(251+178\omega)$
-188875	5	-1511	-37775	G72	1	$X^3-(1+\omega)X^2+(-3+3\omega)X+(11-7\omega)$	$(-3883+2400\omega)$
-202375	5	-1619	-40475	G72	1	$X^3-(1+\omega)X^2-2\omega X+(1+5\omega)$	$(-74+55\omega)$
-214875	5	-1719	-42975	G72	1	$X^3-(1+\omega)X^2+(-8+6\omega)X+(-13+8\omega)$	$(-2679+1656\omega)$
-221875	5	-1775	-1775	G72	1	$X^3-X^2-\omega X+(-1+\omega)$	$(-35+40\omega)$

sig.(2,2)

30125	5	241	6025	G72	1	$X^3-(1+\omega)X^2-(1+\omega)X+(3+5\omega)$	$(-287-464\omega)$
35125	5	281	7025	G72	1	$X^3-\omega X^2+(-4+3\omega)X+(8-5\omega)$	$(-2343+1448\omega)$
49664	8	97	6208	G72	1	$X^3-(1+\omega)X^2+2X+(1-\omega)$	$(-77+54\omega)$
51125	5	409	10225	G72	1	$X^3-\omega X^2+(-1+\omega)X+(-2+\omega)$	$(-86+51\omega)$
52625	5	421	10525	G72	1	$X^3-(1+\omega)X^2+(-1+2\omega)X+(-4+2\omega)$	$(-562+347\omega)$
56125	5	449	11225	G72	1	$X^3-\omega X^2-X+(-3+3\omega)$	$(-415+256\omega)$
66125	5	529	13225	D6i	1	$X^3-(1+\omega)X^2+(5+8\omega)$	$(-2047-3312\omega)$
71125	5	569	14225	G72	1	$X^3-\omega X^2+(6-3\omega)X+(-2+\omega)$	$(-1683+1040\omega)$
82000	5	656	1025	G72	1	$X^3-(1+\omega)X^2+\omega X-1$	$(-28+4\omega)$
82625	5	661	16525	G72	1	$X^3-\omega X^2-\omega X+(-1-2\omega)$	$(-203-327\omega)$

sig.(0,3)

-9747	-3	361	-3	G18	1	$X^3-(1+\omega)X^2+\omega X+(1-\omega)$	$(-5+21\omega)$
-10816	-4	169	-4	G18	1	$X^3-(1+\omega)X^2+5\omega X+(-1-4\omega)$	$(-5-12\omega)$
-11691	-3	433	3897	G72	1	$X^3-(1+\omega)X^2+(-2+2\omega)X+1$	$(13-24\omega)$
-12167	-23	1	-23	D3i	1	$X^3-(1+\omega)X^2+(-2+\omega)X+1$	(1)
-14283	-3	529	4761	D6i	1	$X^3+(1-\omega)X-1$	(-23)
-16551	-3	613	5517	G72	1	$X^3-(1+\omega)X^2+2X+(-1+\omega)$	$(28-9\omega)$
-16807	-7	49	-7	C6r	1	$X^3-\omega X^2+(-1+\omega)X+1$	(-7)
-19683	-3	729	-3	C6r	1	$X^3+(-1+\omega)$	(27ω)
-21168	-3	784	-3	G18	1	$X^3-X^2+(1-2\omega)X+1$	$(-32+12\omega)$
-21296	-11	16	-11	D3i	1	$X^3-\omega X^2+(-1+\omega)X+1$	(4)

Looking at the extended tables, we found for $r_1 = 6$ (resp. 4, 2, 0) zero (resp. one, eleven, eighteen) systems of four nonisomorphic fields with the same discriminants.

We conclude with a short excerpt from the tables; we simply give in each case the first ten fields; more extensive tables can be requested from the authors. The eight columns correspond to the following data: d_K, d_k, $N(\mathfrak{D}_{K/k})$, $d_{\tilde{k}}$, f, the Galois group of a Galois closure of $K/\mathbb{Q}$, a polynomial P which defines K/k and finally d_P.

ACKNOWLEDGMENTS

We should like to thank H. Cohen for several useful discussions; moreover, he is the originator of the PARI-package (due to C. Batut, D. Bernardi, M. Olivier and H. Cohen himself) which we intensively used for the computations. We also thank L. Fallot for his help in the utilization of the UNIX system.

BIBLIOGRAPHY

1. E. Artin and J. Tate, *Class field theory*, Harvard, 1954.
2. G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), 863–911.
3. J. Cougnard and V. Fleckinger, *Sur la monogénéité de l'anneau des entiers de certains corps de rayon*, Manuscripta Math. **63** (1989), 363–376.
4. F. Diaz y Diaz, *Petits discriminants des corps de nombres totalement imaginaires de degré* 8, J. Number Theory **25** (1987), 34–52.
5. M.-N. Gras, *Classes et unités des extensions cycliques réelles de degré* 4 *de* $\mathbb{Q}$, Ann. Inst. Fourier **29** (1979), 107–124, et Publ. Math. Besançon, Th. Nombres, **fasc. 2** (1977/1978).
6. K. Hardy, R. H. Hudson, D. Richman, K. S. Williams and N. M. Holtz, *Calculation of the class numbers of imaginary cyclic quartic fields*, Math. Comp. **49** (1987), 615–620.
7. E. Hecke, *Lectures on the theory of algebraic numbers*, Springer-Verlag, Berlin, 1981.
8. H. W. Lenstra, Jr., *Euclidean number fields of large degree*, Invent. Math. **38** (1977), 237–254.
9. A. Leutbecher, *Euclidean fields having a large Lenstra constant*, Ann. Inst. Fourier **35** (1985), 83–106.
10. A. Leutbecher and J. Martinet, *Lenstra's constant and Euclidean number fields*, Astérisque **94** (1982), 87–131.
11. J. Martinet, *Méthodes géométriques dans la recherche des petits discriminants*, Progress in Mathematics, vol. 59, Birkhäuser, 1985, pp. 147–179.
12. M. Pohst, *On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields*, J. Number Theory **14** (1982), 99–117.
13. R. Schertz, *Konstruktion von Potenzganzheitsbasen in Strahlklassenkörpern über imaginär quadratischen Zahlkörpern*, J. Reine Angew. Math. **398** (1989), 105–129.
14. J.-P. Serre, *Corps locaux* (3-ième édition), Hermann, Paris, 1968.

CEREMAB, 351, COURS DE LA LIBÉRATION, 33405 TALENCE CEDEX, FRANCE. *E-mail*: berge@alkaid.greco-prog.fr; martinet@alcor.greco-prog.fr; olivier@mizar.greco-prog.fr