MATHEMATICS OF COMPUTATION
VOLUME 58, NUMBER 197
JANUARY 1992, PAGES 419–432

THE COMPUTATION OF SEXTIC FIELDS WITH A CUBIC SUBFIELD AND NO QUADRATIC SUBFIELD

M. OLIVIER

ABSTRACT. We describe six tables of sixth-degree fields K containing a cubic subfield k and no quadratic subfield: one for totally real sextic fields, one for sextic fields with four real places, two for sextic fields with two real places, and two for totally imaginary sextic fields (depending on whether the cubic subfield is totally real or not). The tables provide for each possible discriminant d_K of K a quadratic polynomial which defines K/k, the discriminant of the cubic subfield and the Galois group of a Galois closure $N/\mathbb{Q}$ of $K/\mathbb{Q}$.

1. INTRODUCTION

In a previous paper [3] with A.-M. Bergé and J. Martinet, we described relative methods for finding sextic fields with a quadratic subfield up to a given bound on the discriminant. These methods were inspired by general considerations on a geometric approach to this subject explained by J. Martinet in [11] (see also [7]). They provide algorithmic tools for constructing extensive tables of number fields of given degree and signature in the relative case. Here we develop these tools to compute tables of sextic fields with a cubic subfield and no quadratic subfield (those fields with both a cubic and a quadratic subfield are presented in the tables mentioned above [3]).

We first require tables of totally real and complex cubic fields k, their integral bases, and the decomposition of the rational primes in k. In §3 we provide an outline of the computational methods that we employed.

The first step relies on geometric methods. Given a signature, a cubic field k, and a bound M, it consists of building a list of quadratic polynomials over k such that any sextic field $K/\mathbb{Q}$ containing k with absolute value of discriminant less than M is defined by some of these polynomials. The bound M depends on the signature: $7 \cdot 10^7$ for totally real sextic fields, $2 \cdot 10^7$ for sextic fields with four real places, $16 \cdot 10^6$ for sextic fields with two real places and a totally real cubic subfield, $3 \cdot 10^6$ for sextic fields with two real places and a complex cubic subfield, $5 \cdot 10^7$ for totally imaginary sextic fields with a totally real cubic subfield, and $3 \cdot 10^6$ for totally imaginary sextic fields with a complex cubic subfield. This is discussed in §4.

In the second step, we remove the reducible polynomials and those which define a sextic field containing a quadratic subfield (these fields are in the tables

Received July 11, 1990; revised February 25, 1991.
1991 *Mathematics Subject Classification.* Primary 11R21, 11Y40, 11R32.

described in [3]); using approximations of the roots, we then compute by localization the relative discriminant $\mathfrak{d}_{K/k}$ of K/k; a relative integral basis might not exist (§5).

The third step is devoted to testing isomorphisms between sextic fields having the same relative discriminant; in our case, this can be done by two differents methods which are described in §6. We choose from among the quadratic polynomials defining the same sextic field one which gives the smallest index.

In the fourth step (§7) we determine the Galois group of a Galois closure N of K over $\mathbb{Q}$; the classification of such transitive groups of degree six has been done, e.g., by G. Butler and J. McKay ([4]; see also [12]).

Finally, in §8, we provide some comments on the tables. By class field theory we obtain results on imprimitive quartic fields which concern the parity of the class number; we also list the minimal discriminants with given infinite Frobenius for the five isomorphism classes of transitive groups of sixth degree that we consider in this paper.

In order to complete this work, we intend, in a forthcoming paper [13], to use the methods of Pohst [14], to compute extensive tables of primitive sextic fields for all signatures.

2. Notation

We denote by K a quadratic extension of a cubic field k; (r_1, r_2) is the signature of K; $\mathbb{Z}_K$ (resp. $\mathbb{Z}_k$) is the ring of integers of K (resp. k); N is a Galois closure of $K/\mathbb{Q}$; $\mathfrak{d}_{K/k}$ is the ideal discriminant of K/k; d_K is the absolute discriminant of $K/\mathbb{Q}$; and d_P is the discriminant of the polynomial P.

$v_{\mathfrak{p}}$ is the valuation associated with the prime ideal $\mathfrak{p}$ of k (same notation with capital letters $v_{\mathfrak{P}}$, for $\mathfrak{P}$ in K); $\mathrm{Tr}_{k/\mathbb{Q}}$ (resp. $\mathrm{Tr}_{K/k}$) and $N_{k/\mathbb{Q}}$ (resp. $N_{K/k}$) are respectively the trace and the norm of $k/\mathbb{Q}$ (resp. K/k).

The cubic field $k/\mathbb{Q}$ of discriminant d_k is defined by a primitive element α; $\{1, \alpha, \beta\}$ is an integral basis of $\mathbb{Z}_k$, Q (resp. R) the minimal polynomial of α (resp. β) (in most of the cases, we have $\beta = \alpha^2$); $(\alpha, \alpha', \alpha'')$ (resp. (β, β', β'')) are the conjugates of α (resp. β) under the conjugacy of $k/\mathbb{Q}$.

The sextic field K is defined by a primitive element θ over k; its minimal polynomial is $P(x) = x^2 - ax + b \in \mathbb{Z}_k[x]$; θ_1 and θ_2 are the roots of P; we let P' (resp. P'') be the polynomial with coefficients a' and b' (resp. a'' and b''), with roots θ_1' and θ_2' (resp. θ_1'' and θ_2'') in an algebraic closure of $\mathbb{Q}$.

3. Computation in cubic fields

If K is a sextic field containing a cubic subfield k, we have

$$|d_K| = d_k^2 \, N_{k/\mathbb{Q}}(\mathfrak{d}_{K/k});$$

thus, to construct tables of sextic fields having a cubic subfield, and with discriminant up to a given bound M, we need tables of cubic fields with discriminant up to $\sqrt{M}$.

Such tables of cubic fields exist (see, for instance, [2, 5, 8, 10] for totally real cubic fields, and [1, 15] for complex cubic fields).

For our purpose, we use the following method: first search for polynomials $Q(x) = x^3 - c_1x^2 + c_2x - c_3$ in $\mathbb{Z}[x]$ defining $k/\mathbb{Q}$, using the inequality of

Corollary 2.9 in [11]. Given such a polynomial, using Theorem 2 in [9], we compute the discriminant d_k. Then we test isomorphisms between cubic fields having the same discriminant. Finally, the results in Chapter 3 of [16] allow us to find an integral basis of $\mathbb{Z}_k$ of the form $(1, \alpha, \beta)$, with $Q(\alpha) = 0$.

In the paper [9] mentioned above, Theorem 1 describes the decomposition of the primes in $\mathbb{Z}_k$. In fact, in §5, we make the effective computations required to choose an explicit representation of the prime ideals $\mathfrak{p}$ in $\mathbb{Z}_k$ above a prime rational p so as to be able, given an integer $x \in \mathbb{Z}_k$ and a prime ideal $\mathfrak{p}$, to compute $v_{\mathfrak{p}}(x)$.

The following lemmas can be used to carry out these tasks.

Lemma 1. *For every prime ideal $\mathfrak{p}$ above p in $\mathbb{Z}_k$, there exists a γ in $\mathbb{Z}_k$ such that $\mathfrak{p} = p\mathbb{Z}_k + \gamma\mathbb{Z}_k$ with the following properties:*

(1) $v_{\mathfrak{p}}(\gamma) = 1$;

(2) *if $\mathfrak{p}'$ is another prime ideal above p, $v_{\mathfrak{p}'}(\gamma) = 0$.*

(When p is inert, we choose $\gamma = p$.)

Proof. If p does not divide the index $[\mathbb{Z}_k : \mathbb{Z}[\alpha]]$, by a classical result, the prime decomposition $\bmod p$ of the minimal polynomial Q of α gives the decomposition of the prime number p in $\mathbb{Z}_k$; if $\overline{Q}(x) = \prod_{1\le i\le g} \overline{\varphi}(x)^{e_i} \bmod p$, we have $p\mathbb{Z}_k = \prod_{1\le i\le g} \mathfrak{p}_i^{e_i}$, with $\mathfrak{p}_i = p\mathbb{Z}_k + \gamma\mathbb{Z}_k$, the degree of $\overline{\varphi}$ is the degree of $\mathfrak{p}_i$, and if $e_i > 1$, then $\gamma = \varphi(\alpha)$, otherwise, $\gamma = \varphi(\alpha)$ or $\varphi(\alpha)+p$ according to the $\mathfrak{p}$-valuation of $\varphi(\alpha)$.

If p divides the index, it is easy to prove that we can choose ε_1 and ε_2 in $\{0, 1\}$ and u in $\mathbb{Z}$ such that $\gamma = \varepsilon_1\alpha + \varepsilon_2\beta + u$, depending on the factorization $\bmod p$ of Q and R.

More precisely, the results are (note that in this situation, p divides d_Q and d_R, and the minimal polynomials of α and β have a multiple root $\bmod p$):

If $p\mathbb{Z}_k = \mathfrak{p}^3$, then Q (resp. R) has a triple root t (resp. t') $\bmod p$; thus, we can take $\gamma = \alpha - t$ if $v_{\mathfrak{p}}(\alpha - t) = 1$, and $\gamma = \beta - t'$ otherwise.

If $p\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$, then if Q has a simple root t_1 and a double root $t_2 \bmod p$, we have $\mathfrak{p}_2 = (p, \alpha - t_1)$ or $(p, \alpha - t_1 + p)$; $\mathfrak{p}_1 = (p, \alpha - t_2)$ if $v_{\mathfrak{p}_1}(\alpha - t_2) = 1$; if $v_{\mathfrak{p}_1}(\alpha - t_2) > 1$, then $\mathfrak{p}_1 = (p, \beta - t')$ if t' is a double root of $R \bmod p$, and $\mathfrak{p}_1 = (p, \alpha + \beta - t_2 - t')$ if t' is of order 3. In the case when Q has a triple root, then R has a single and a double root, so we exchange Q and R in the above discussion.

If $p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_2$ of degree 2, then if Q has a simple root t_1 and a double root $t_2 \bmod p$, then $\mathfrak{p}_1 = (p, \alpha - t_1)$ or $(p, \alpha - t_1 + p)$; if $v_{\mathfrak{p}_2}(\alpha - t_2) = 1$, then $\mathfrak{p}_2 = (p, \alpha - t_2)$; if not, $\mathfrak{p}_2 = (p, \beta - t')$ if t' is a root of order 2 of R, and $\mathfrak{p}_2 = (p, \alpha + \beta - t_2 - t')$ if t' is of order 3. If Q has a triple root, exchange Q and R as above.

Finally, if $p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, the only case is: Q has a simple root t_1 and a double root $t_2 \bmod p$ (idem for R with t_1' and t_2'); let $\mathfrak{p}_1 = (p, \alpha - t_1)$ or $(p, \alpha - t_1 + p)$ and choose $\mathfrak{p}_2 = (p, \beta - t_1')$ or $(p, \beta - t_1' + p)$ and $\mathfrak{p}_3 = (p, \alpha + \beta - t_2 - t_2')$ or $(p, \alpha + \beta - t_2 - t_2' + p)$. □

Lemma 2. *Let $\mathfrak{p} = (p, \gamma)$ be a prime ideal of $\mathbb{Z}_k$ of degree 1, γ as in Lemma 1; let $x = x_1 + x_2\alpha + x_3\beta$ (x_i in $\mathbb{Z}$) be an integer of $\mathbb{Z}_k$, and a (resp. b) in $\mathbb{Z}$ such that $\alpha \equiv a \bmod \mathfrak{p}$ (resp. $\beta \equiv b$); finally, let $y = xN_{k/\mathbb{Q}}(\gamma)/p\gamma$. Then, if $v_p(x_1 + x_2a + x_3b)$ is ≥ 1, y belongs to $\mathfrak{p}$ and $v_{\mathfrak{p}}(x) = 1 + v_{\mathfrak{p}}(y)$.*

Proof. Clearly, $v_p(x_1 + x_2a + x_3b) \geq 1$ is equivalent to $v_{\mathfrak{p}}(x) \geq 1$; moreover, $(x/\gamma) = (py/N_{k/\mathbb{Q}}(\gamma))$ and the hypothesis on γ in Lemma 1 imply the result. □

Now we have an algorithm to compute $v_{\mathfrak{p}}(x)$ for $x \in \mathbb{Z}_k$ and $\mathfrak{p}$ a prime ideal of degree f and ramification index e:

(1) write $x = nx'$ with $n \in \mathbb{Z}$ and $x' = x'_1 + x'_2\alpha + x'_3\beta$ such that $\gcd(x'_1, x'_2, x'_3) = 1$;
(2) compute $v_{\mathfrak{p}}(n) = ev_p(n)$;
(3) if $f = 3$, then $v_{\mathfrak{p}}(x') = 0$;
(4) else if $f = 2$, then $p\mathbb{Z}_k = \mathfrak{p}\mathfrak{p}'$ and $v_{\mathfrak{p}}(x') = \frac{1}{2}(v_p(N_{k/\mathbb{Q}}(x')) - v_{\mathfrak{p}'}(x'))$;
(5) else if $f = 1$ and $e = 3$, then $v_{\mathfrak{p}}(x') = v_p(N_{k/\mathbb{Q}}(x'))$;
(6) else compute a and b such that $\alpha \equiv a$ and $\beta \equiv b \bmod \mathfrak{p}$;

we have $v_{\mathfrak{p}}(x') \geq 1$ if and only if $v_p(x'_1 + x'_2a + x'_3b) \geq 1$; in the case of $v_{\mathfrak{p}}(x') \geq 1$, Lemma 2 gives a recursion formula, $v_{\mathfrak{p}}(x') = 1 + v_{\mathfrak{p}}(x'')$ with $x'' = (x'/p)(N_{k/\mathbb{Q}}(\gamma)/\gamma)$.

4. Computational methods for searching for polynomials

General method.[1] We give here general relative methods for constructing tables of irreducible polynomials $P(x) = x^m - a_1x^{m-1} + \cdots + (-1)^m a_m \in \mathbb{Z}_k[x]$ which define a relative extension K/k of degree m, where k is a number field of degree n' $(n = mn')$. The notation is the following: θ is a primitive element $(K = k(\theta))$, $(\theta_1, \ldots, \theta_m)$ are the roots of P in $\mathbb{C}$; if c is in k, $(c = c^{(1)}, \ldots, c^{(n')})$ are the conjugates of c under the conjugacy of $k/\mathbb{Q}$. By extension, $(P = P^{(1)}, \ldots, P^{(n')})$ denote the polynomials whose coefficients are the $(a_i^{(h)})$'s, and $(\theta_j^{(h)})$ are their roots in $\mathbb{C}$. $(1 = \alpha_1, \ldots, \alpha_{n'})$ is an integral basis of $\mathbb{Z}_k$. Finally, by analogy with the formulation of M. Pohst in [14], we define

$$S_l^{(h)}(\theta) = \sum_{i=1}^{m} (\theta_i^{(h)})^l, \qquad S_l(\theta) = \sum_{h=1}^{n'} S_l^{(h)}(\theta),$$

$$T_l^{(h)}(\theta) = \sum_{i=1}^{m} |\theta_i^{(h)}|^l, \qquad T_l(\theta) = \sum_{h=1}^{n'} T_l^{(h)}(\theta),$$

for $1 \leq l \leq m$. The basic tool of the method is Theorem 2.8 in [11]:

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

$$T_2(\theta) \leq \frac{1}{m} \sum_{h=1}^{n'} |a_1^{(h)}|^2 + \gamma_{n-n'} \left(\frac{|d_K|}{m^{n'}|d_k|} \right)^{1/(n-n')},$$

where γ_q is the Hermite constant in dimension q, and d_k (resp. d_K) is the absolute discriminant of k (resp. K).

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

In the following, we write $c_1 = \frac{1}{m} \sum_{h=1}^{n'} |a_1^{(h)}|^2$ and

$$c(M) = \gamma_{n-n'} \left(\frac{M}{m^{n'}|d_k|} \right)^{1/(n-n')},$$

[1] I am grateful to the referee for a number of suggestions which led to improvements in the first draft of this section.

where M is the bound for the absolute discriminant $|d_K|$ of the fields K we are looking for, and $c_2(M) = c_1 + c(M)$; so, the above inequality becomes $T_2(\theta) \leq c_2(M)$.

We now give inequalities to bound the a_i's.

Changing θ in $\theta+\lambda$, with $\lambda \in \mathbb{Z}_k$, and using the fact that $a_1 = \sum_{1\leq j\leq n'} a_{1,j}\alpha_j = \mathrm{Tr}_{K/k}(\theta)$ ($a_{1,j} \in \mathbb{Z}$), we see that we can choose the $a_{1,j}$'s modulo m.

Now, we fix a_1 (hence c_1) among the $m^{n'}$ possible values and search for the last coefficient $a_m = \sum_{1\leq j\leq n'} a_{m,j}\alpha_j$.

The inequality between arithmetic and geometric means yields the following result:

$$|a_m^{(h)}|^2 = \prod_{i=1}^{m} |\theta_i^{(h)}|^2 \leq \left(\frac{1}{m}\sum_{i=1}^{m} |\theta_i^{(h)}|^2\right)^m = \frac{1}{m^m}(T_2^{(h)}(\theta))^m,$$

and therefore the inequality

$$\sum_{h=1}^{n'} |a_m^{(h)}|^2 \leq \frac{1}{m^m}\sum_{h=1}^{n'}(T_2^{(h)}(\theta))^m \leq \frac{1}{m^m}T_2(\theta)^m.$$

Finally, writing $c_3(M) = c_2(M)^m/m^m$, and applying the above theorem, we obtain

$$\sum_{h=1}^{n'} |a_m^{(h)}|^2 \leq c_3(M).$$

Let $b_{i,j} = \sum_{1\leq h\leq n'} \alpha_i^{(h)}\overline{\alpha_j^{(h)}}$; we have to compute all $(a_{m,j})_{1\leq j\leq n'} \in \mathbb{Z}^{n'}$ subject to

$$\sum_{1\leq i,j\leq n'} b_{i,j}a_{m,i}a_{m,j} \leq c_3(M),$$

where $\sum_{1\leq i,j\leq n'} b_{i,j}x_ix_j$ is a positive definite quadratic form. This can be done using the Fincke-Pohst algorithm (see [6]). Note that this method will be applied for the other a_i's.

We search now for a_2.

For $1 \leq h \leq n'$, we have, $a_2^{(h)} = \frac{1}{2}((S_1^{(h)}(\theta))^2 - S_2^{(h)}(\theta))$, and

$$\sum_{1\leq h\leq n'} |S_2^{(h)}(\theta)|^2 \leq T_2(\theta)^2 \leq c_2(M)^2,$$

and applying the above algorithm, we calculate the integer points into this ellipsoid.

To finish, we need to find the other a_i's for $3 \leq i < m$.

We make use of a method due to M. Pohst which allows us to compute a bound for the $T_i(\theta)$, knowing a_1, a_2, and a_m (cf. Theorem 4 in [14]). Given these bounds, we proceed by recursion on i as follows:

We suppose that we know $a_3, \ldots, a_{i-1}$; then Newton's formula gives

$$a_i^{(h)} = \frac{1}{i}\left(\sum_{j=1}^{i-1}(-1)^{j-1}a_{i-j}^{(h)}S_j^{(h)}(\theta) + (-1)^{i-1}S_i^{(h)}(\theta)\right),$$

and we have

$$\sum_{h=1}^{n'} |S_i^{(h)}(\theta)|^2 \leq T_i(\theta)^2;$$

so, we are able to finish as for the first a_i's.

Application to sextic fields. Let us apply the previous method to the totally real sextic fields containing the cubic subfield $k = \mathbb{Q}(\alpha)$, with discriminant 49, the minimal polynomial of α being $x^3 + x^2 - 2x - 1$, whose roots are $\alpha_2^{(1)} = 1.246...$, $\alpha_2^{(2)} = -0.445...$, $\alpha_2^{(3)} = -1.801...$. A $\mathbb{Z}$-basis of $\mathbb{Z}_k$ is $(1, \alpha_2, \alpha_3)$, with $\alpha_3 = \alpha_2^2$, and we have $\alpha_3^{(1)} = 1.554...$, $\alpha_3^{(2)} = 0.198...$, $\alpha_3^{(3)} = 3.246...$.

We are looking for polynomials $P(x) = x^2 - a_1 x + a_2 \in \mathbb{Z}_k[x]$ such that $K = k(\theta)$ and P is the minimal polynomial of θ.

We take $M = 7 \cdot 10^7$; first, we have $c(M) = 70.949...$; we choose a_1 among the eight possible values: $0, 1, \alpha_2, \alpha_2^2, 1 + \alpha_2, 1 + \alpha_2^2, \alpha_2 + \alpha_2^2, 1 + \alpha_2 + \alpha_2^2$.

For $a_1 = 0$, $c_3(M) = 1258.446...$, and we have to solve the inequality

$$3(x_1 - \tfrac{1}{3}x_2 + \tfrac{5}{3}x_3)^2 + \tfrac{14}{3}(x_2 - \tfrac{1}{2}x_3)^2 + \tfrac{7}{2}x_3^2 \leq 1258.446\ldots,$$

with $(x_1, x_2, x_3) \in \mathbb{Z}^3$. We find 27294 vectors; among those vectors, only 1001 give totally real irreducible polynomials satisfying the inequality of the previous theorem.

Irreducibility of quadratic polynomials. Given a polynomial $P(x) = x^2 - ax + b \in \mathbb{Z}_k$, we need to test whether it is irreducible over $k[x]$. To do this, we compute approximations of the roots θ_1, θ_2, θ_1', θ_2', θ_1'', θ_2''; for all reasonable triples (depending on the signature) we test if $\theta_i + \theta_j' + \theta_k''$, $\theta_i\theta_j' + \theta_i\theta_k'' + \theta_j'\theta_k''$, and $\theta_i\theta_j'\theta_k''$ are in $\mathbb{Z}$. If they are, we guess the possible root of P in $\mathbb{Z}_k$ and verify whether or not it is in $\mathbb{Z}_k$.

5. Relative discriminant

Let P be a polynomial in the preceding list with discriminant d_P; for every prime number p dividing $N_{k/\mathbb{Q}}(d_P)$, and for each prime ideal $\mathfrak{p}$ of k above p, we have to compute $v_{\mathfrak{p}}(\mathfrak{d}_{K/k})$.

First of all, since $d_P = \mathfrak{f}^2 \mathfrak{d}_{K/k}$, where $\mathfrak{f}$ is the index of $\mathbb{Z}_k[\theta]$ in $\mathbb{Z}_K$, $v_{\mathfrak{p}}(\mathfrak{d}_{K/k})$ and $v_{\mathfrak{p}}(d_P)$ are simultaneously even or odd and $v_{\mathfrak{p}}(\mathfrak{d}_{K/k})$ is zero as soon as $v_{\mathfrak{p}}(d_P)$ is. So, we have only to deal with those $\mathfrak{p}$ for which $v_{\mathfrak{p}}(d_P)$ is not zero.

We denote by π a uniformizing parameter at $\mathfrak{p}$, and by e_0 the absolute ramification index of (2) in $\mathbb{Z}_k$; then, we use local computations.

We write $d_P = \pi^{2l}x$, with $x \in k$ and $v_{\mathfrak{p}}(x) = 0$ or 1. The effective calculation of $\mathfrak{d}_{K/k}$ is based on the following two results:

Proposition 1. *If $\mathfrak{p}$ does not divide (2), then $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 0$ or 1 according to whether $v_{\mathfrak{p}}(x) = 0$ or 1. If $\mathfrak{p}$ divides (2) and $v_{\mathfrak{p}}(x) = 1$, then $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 1 + 2e_0$.*

The proof is obvious: if $v_{\mathfrak{p}}(x) = 1$, the polynomial $X^2 - x$ is an Eisenstein polynomial with discriminant $4x$; if $v_{\mathfrak{p}}(x) = 0$ and if $\mathfrak{p}$ does not divide (2), the discriminant of the polynomial $X^2 - x$ has valuation zero in $\mathfrak{p}$, and therefore $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 0$. □

The next proposition deals with the remaining case when $\mathfrak{p}$ divides (2) and $v_{\mathfrak{p}}(x) = 0$.

Proposition 2. *Let $m = \max\{n | x = \square \bmod \mathfrak{p}^n\}$; if $m \geq 2e_0$, we have $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 0$, and in the others cases, m is odd and $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 2e_0 - (m-1)$.*

The proof consists of an elementary study of the ramification groups together with some results "à la Hecke" concerning quadratic extensions. □

It is easy to deduce from the above propositions an algorithm to compute $v_{\mathfrak{p}}(\mathfrak{d}_{K/k})$ for all prime ideals $\mathfrak{p}$:

Step 1. If $v_{\mathfrak{p}}(d_P) = 0$, then $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 0$.

Step 2. Else, if $v_{\mathfrak{p}}(d_P)$ is odd, then $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 1$ if $\mathfrak{p} \nmid (2)$ and $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 1 + 2e_0$ if $\mathfrak{p} \mid (2)$.

Step 3. Else ($v_{\mathfrak{p}}(d_P)$ even), if $\mathfrak{p} \nmid (2)$, then $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 0$.

Step 4. Else ($v_{\mathfrak{p}}(d_P)$ even and $\mathfrak{p} \mid (2)$) write $d_P = \pi^{2l}x$. If $x \neq \square \bmod \mathfrak{p}^2$, then $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 2e_0$. Else, if $x = \square \bmod \mathfrak{p}^2$ and $e_0 = 1$, then $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 0$.

Step 5. Else ($x = \square \bmod \mathfrak{p}^2$ and $e_0 \neq 1$), if $x \neq \square \bmod \mathfrak{p}^4$, then $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 2$ if $e_0 = 2$, and $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 4$ if $e_0 = 3$. Else, if $x = \square \bmod \mathfrak{p}^4$ and $e_0 = 2$, then $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 0$.

Step 6. Else ($x = \square \bmod \mathfrak{p}^4$ and $e_0 = 3$), if $x \neq \square \bmod \mathfrak{p}^6$, then $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 2$, else $v_{\mathfrak{p}}(\mathfrak{d}_{K/k}) = 0$.

Note that this algorithm needs to know if x is or is not congruent to a square mod $\mathfrak{p}^2$, or $\mathfrak{p}^4$, or $\mathfrak{p}^6$. This is done by use of $\mathfrak{p}$-adic computation depending on the degree of $\mathfrak{p}$.

6. Quadratic subfields and isomorphisms

Now, we have tables of sextic fields containing a cubic field, with their relative discriminants. Those fields with a quadratic subfield are in the tables mentioned earlier (see [3]). So, we have to detect whether K contains a quadratic subfield $\tilde{k}$; if the answer is positive, we eliminate those sextic fields from the tables. Next, for sextic fields having the same discriminant, we have to test for $\mathbb{Q}$-isomorphism.

Quadratic subfields. If there exists a quadratic subfield $\tilde{k} = \mathbb{Q}(\sqrt{m})$, then K is the compositum $k \cdot \tilde{k}$ and the polynomials $P(x)$ and $x^2 - m$ define K/k; therefore, the algebraic integer $N_{k/\mathbb{Q}}(d_P)d_P$ is a square in $\mathbb{Z}_k$ and the converse is true. This assertion gives an algorithm to test whether $\tilde{k}$ exists or not.

Otherwise, if we know approximations to the roots of $P(x)$, there exists a $\tilde{k}$ if and only if there is a partition $\{\theta_1, \theta_i', \theta_j''\}$ and $\{\theta_2, \theta_{3-i}', \theta_{3-j}''\}$ (for i and j among 1 and 2) of the six conjugates of θ such that $\tilde{k} = \mathbb{Q}(s_1, s_2, s_3)$ or $\tilde{k} = \mathbb{Q}(\sqrt{d_k})$, (s_1, s_2, s_3) being the elementary symmetric functions of $(\theta_1, \theta_i', \theta_j'')$.

Consequently, this provides another method for testing if there is a quadratic subfield: for all possible permutations of $\{1, 2\}$, we calculate approximations of the s_i's and we test if the s_i's are quadratic integers.

Isomorphisms. We give here two methods for testing the existence of a $\mathbb{Q}$-isomorphism between sextic fields with the same discriminant.

First we refer to [3, §5] for a general method; in our case, let $K = k(\theta)$ and $L = k(\varphi)$ be two sextic fields containing k and defined by polynomials P and Q in $\mathbb{Z}_k[x]$. Note that since neither K nor L contains a quadratic field, the

cubic subfield k is unique. Thus, K and L are isomorphic if and only if there exists a permutation σ of $\{1, 2\}$ such that for $h = 0, 1$ the sums

$$\alpha_h = \sum_{1\le i\le 2} \theta_i^h \varphi_{\sigma(i)}, \quad \alpha'_h = \sum_{1\le i\le 2} \theta_i'^h \varphi'_{\sigma(i)}, \quad \alpha''_h = \sum_{1\le i\le 2} \theta_i''^h \varphi''_{\sigma(i)}$$

belong respectively to k and its conjugates. A numerical computation with sufficient accuracy allows us to decide this effectively.

The second method is based on the following observation: if K and L are $\mathbb{Q}$-isomorphic, they are k-isomorphic unless K is cyclic; in this last situation, we need to take into account the possible conjugacies. Therefore, $K = k(\sqrt{\lambda})$ and $L = k(\sqrt{\mu})$ are isomorphic if and only if λ/μ is in k^2, i.e., $N_{k/\mathbb{Q}}(\lambda)/N_{k/\mathbb{Q}}(\mu)$ is a square in $\mathbb{Q}$.

7. Galois groups

One can find in [4] the sixteen possible transitive permutation groups of degree six which may be associated with each sextic field. Among these sixteen groups, only five correspond to a sextic field with a cubic subfield and no quadratic subfield (two of them are even).

We give in the table below all such groups for $K = k(\sqrt{\lambda})$, according to the permutation group defined by the cubic subfield k (C_n is the cyclic group of order n, S_n is the symmetric group on n letters, and A_n is the subgroup of even permutations in S_n), and the degree of $k_1 = \mathbb{Q}(\sqrt{N_{k/\mathbb{Q}}(\lambda)})$ and $k_2 = \mathbb{Q}(\sqrt{d_k})$ over $\mathbb{Q}$.

type of K	type of k	k_1, k_2	possible r_1's
A_4	C_3	$k_1 = k_2 = \mathbb{Q}$	6, 2
$A_4 \times C_2$	C_3	$[k_1 : \mathbb{Q}] = 2$, $k_2 = \mathbb{Q}$	6, 4, 2, 0
S_4^+	S_3	$k_1 = \mathbb{Q}$, $[k_2 : \mathbb{Q}] = 2$	6, 2 (*)
S_4^-	S_3	$k_1 = k_2$, $[k_1 : \mathbb{Q}] = 2$	6, 2, 0
$S_4 \times C_2$	S_3	$[k_1 : \mathbb{Q}] = [k_2 : \mathbb{Q}] = 2$	6, 4, 2, 0 (**)

(*) two possible Frobenius substitutions when $r_1 = 2$

(**) idem when $r_1 = 2$ or 0.

S_4^+ (*resp.* S_4^-) *denotes the even (resp. odd) permutation of* S_4 *on six letters.*

By examining the above table we can easily deduce an algorithm to compute the type of $K/\mathbb{Q}$:

If k is of type C_3, then the type of K is A_4 if $N_{k/\mathbb{Q}}(\lambda)$ is a square, and $A_4 \times C_2$ if not.

If k is of type S_3, then the type of K is S_4^+ if $N_{k/\mathbb{Q}}(\lambda)$ is a square, S_4^- if $N_{k/\mathbb{Q}}(\lambda)/d_k$ is a square, and $S_4 \times C_2$ otherwise.

Actually, the effective computation is simply done using the following computational trick: We write $d_k = d \cdot f^2$ in such a way that $d = 1$ means that the type of k is C_3 (if $d_k = mg^2$ with m squarefree, then $d = m$ and $f = g$ if $m \equiv 1 \bmod 4$, and $d = 4m$, $f = g/2$ in the other cases). To conclude, it suffices to know $N_{k/\mathbb{Q}}(d_P)$; if $d = 1$, then the type of K is A_4 when $N_{k/\mathbb{Q}}(d_P)$ is a square, otherwise $A_4 \times C_2$; if $d \neq 1$, then the type is S_4^+ if $N_{k/\mathbb{Q}}(d_P)$ is a square, else S_4^- if $N_{k/\mathbb{Q}}(d_P)/d$ is a square, and $S_4 \times C_2$ otherwise.

8. A LOOK AT THE TABLES

The algorithms were implemented on a "sparc-station 1."

The bounds for the discriminants depend only on the signature and on the running time of the algorithms; intensive use of the multiprecision package "PARI" allowed us to avoid being concerned about the size of the integers (these may be about 17 decimal digits in the case of polynomial discriminants).

We chose M = 70,000,000 (resp. 20,000,000, 16,000,000, 3,000,000, 50,000,000 and 3,000,000) for $r1 = 6$ (resp. 4, 2 and totally real cubic subfield, 2 and complex cubic subfield, 0 and totally real cubic subfield, and 0 and complex cubic subfield); we found respectively 947, 994, 850, 1448, 724, and 1548 sextic fields for 27771, 20434, 16908, 15100, 18296, and 17080 irreducible polynomials with suitable signature. On the workstation mentioned above, the cpu-running times were respectively 101, 27, 23, 11, 68, and 12 minutes.

Distribution of the sextic fields according to Galois type. We give below the distribution of these fields according to signature and Galois type.

sign.	$\lvert d_K \rvert$ max.	A_4	$A_4 \times C_2$	S_4^+	S_4^-	$S_4 \times C_2$
6	69948333	6	507	45	3	386
4	19983523	×	470	×	×	524
2 (*r.*)	15981056	16	359	131	8	336
2 (*i.*)	2999824	×	×	113	×	1335
0 (*r.*)	49843600	×	370	×	×	354
0 (*i.*)	2999959	×	×	×	29	1519

(" × " means "impossible"; *r.* (resp. *i.*) points out that the cubic subfield is totally real (resp. complex).)

Note that the norm of the $\mathbb{Z}_k$-index of $\mathbb{Z}_k[\theta]$ in $\mathbb{Z}_K$ which we found is equal to 1 most of the time; the number of exceptions is 30 (resp. 21, 45, 30, 16, and 31) for $r_1 = 6$ (resp. 4, 2 and totally real cubic subfield, 2 and complex cubic subfield, 0 and totally real cubic subfield, 0 and complex cubic subfield).

Minimal discriminants. In the next table, we give the minimal discriminant of sextic fields containing a cubic subfield but no quadratic subfield for each signature and each possible type.

sign.	(6,0)	(4,1)	(2,2)	(0,3)
type				
A_4	25969216	×	153664	×
$A_4 \times C_2$	434581	−103243	31213	−400967
S_4^+	3356224	×	$\begin{cases} r. & 52441 \\ i. & 33856 \end{cases}$	×
S_4^-	33076161	×	810448	−85184
$S_4 \times C_2$	1387029	−309123	$\begin{cases} r. & 109520 \\ i. & 28037 \end{cases}$	$\begin{cases} r. & -503792 \\ i. & -10051 \end{cases}$

(" × " means "impossible".)

Coincidences of discriminants. Finally, we show the coincidences of discriminants that are in each of the six tables of sextic fields (i.e., the number of systems of two (resp. three, four, five, and six) nonisomorphic sextic fields with the same discriminants).

r_1	6	4	2(*r.*)	2(*i.*)	0(*r.*)	0(*i.*)
2 fields	9	144	116	147	8	155
3 fields	3	44	27	48	2	57
4 fields	0	3	3	2	0	0
5 fields	0	2	0	0	0	2
6 fields	0	0	0	2	0	0

Remarks on class numbers. Let k_3 be a cubic field; the discriminant of an A_4 or S_4 extension (say k_4) attached to k_3 is $d_{k_4} = d_{k_3} N_{k_3/\mathbb{Q}}(\mathfrak{d}_{k_6/k_3})$, where k_6 is an A_4 or S_4^+ sextic field (A_4 when $k_3/\mathbb{Q}$ is cyclic, S_4^+ otherwise). The signature of k_4 is given by the following rules: either k_6/k_3 is unramified at infinity, and then k_4 is totally real if k_3 is totally real, and of mixed signature if k_3 is complex, or k_3 is totally real, two infinite primes of k_3 ramify in k_6/k_3, and k_4 is totally imaginary. The equality $d_{k_4} = d_{k_3}$ holds if and only if k_6/k_3 is unramified for finite primes. Thus, we recover from the three tables for the signature (6, 0) and (2, 2), the well-known lists of coincidences between quartic

and cubic discriminants: $1957, 2777, \ldots, -283, -331, \ldots, 229, 257, \ldots$; our results are in accordance with Godwin's.

We can describe the corresponding extensions k_6/k_3 by class field theory. When the involved S_4 field is not totally imaginary, the extensions k_6/k_3 are in one-to-one correspondence with the subgroups of index 2 in $\mathscr{C}l_{k_3}$ when k_3 is not cyclic, and of index 4 and quotient $C_2 \times C_2$ when k_3 is cyclic. Examples of S_4^+ extensions appear in the tables, but the smallest A_4 example has a discriminant $(163^4 = 705{,}911{,}761)$ which lies beyond the limit of our tables. When the S_4 field is totally imaginary, we must consider subgroups of $\mathscr{C}l_{k_3}^+$ which are not pull-backs of a subgroup of $\mathscr{C}l_{k_3}$. This is possible if and only if the 2-rank of $\mathscr{C}l_{k_3}^+$ is larger than the 2-rank of $\mathscr{C}l_{k_3}$. This never happens when k_3 is cyclic, and we therefore cannot find A_4 examples, but S_4^+ examples can be found in our tables.

Excerpts of the tables. We conclude with some short excerpts from the tables. Complete tables can be obtained from the author. They are available on floppy disk (source TEX) or on paper (353 pages) (contact the author by e-mail).

For each of the six tables, we give the first ten sextic fields. The seven columns provide the following data: d_K, d_k, $N_{k/\mathbb{Q}}(\mathfrak{d}_{K/k})$, the Galois group of a Galois closure of $K/\mathbb{Q}$, $f = N_{k/\mathbb{Q}}(\mathfrak{f})$ such that $d_P = \mathfrak{f}^2 \mathfrak{d}_{K/k}$, a polynomial P which defines K/k, and finally d_P.

The coefficients of the polynomial P are in $\mathbb{Z}_k$; so for all the cubic fields which appear in the second column of the tables, we give below a polynomial which defines $k/\mathbb{Q}$ and an integral basis for $\mathbb{Z}_k$ of the form $(1, \alpha, \beta)$, β being a quadratic polynomial in α.

Signature $(6, 0)$

434581	49	181	$A_4 \times C_2$	1	$x^2 - \alpha x + (1 + \alpha - 3\beta)$	$-4 - 4\alpha + 13\beta$
703493	49	293	$A_4 \times C_2$	1	$x^2 - (1 + \alpha)x + (-1 + \alpha)$	$5 - 2\alpha + \beta$
905177	49	377	$A_4 \times C_2$	1	$x^2 - \beta x + (-1 - 2\alpha - \beta)$	$3 + 7\alpha + 7\beta$
1279733	49	533	$A_4 \times C_2$	1	$x^2 - \beta x + (-4 - 11\alpha - 5\beta)$	$15 + 43\alpha + 23\beta$
1292517	81	197	$A_4 \times C_2$	1	$x^2 - \alpha x + (3 + 7\alpha - 5\beta)$	$-12 - 28\alpha + 21\beta$
1387029	257	21	$S_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + (1 + 2\alpha + \beta)$	$3 + 7\alpha + 4\beta$
1397493	81	213	$A_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + (2 + 10\alpha - 3\beta)$	$-5 - 31\alpha + 18\beta$
1528713	81	233	$A_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + (4 + 10\alpha - 4\beta)$	$-13 - 31\alpha + 22\beta$
1683101	49	701	$A_4 \times C_2$	1	$x^2 - (\alpha + \beta)x + (-13 + 4\alpha + 6\beta)$	$53 - 13\alpha - 22\beta$
1997632	49	832	$A_4 \times C_2$	1	$x^2 + (3 + 6\alpha - 7\beta)$	$-12 - 24\alpha + 28\beta$

Signature $(4, 1)$

-103243	49	-43	$A_4 \times C_2$	1	$x^2 - (1 + \alpha)x + (-19 + 5\alpha + 9\beta)$	$77 - 18\alpha - 35\beta$
-124659	81	-19	$A_4 \times C_2$	1	$x^2 - \alpha x + (-1 - 4\alpha - 2\beta)$	$4 + 16\alpha + 9\beta$
-153664	49	-64	$A_4 \times C_2$	1	$x^2 + (1 - 3\alpha - 2\beta)$	$-4 + 12\alpha + 8\beta$
-170471	49	-71	$A_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + (-3 + 3\alpha + 3\beta)$	$14 - 7\alpha - 8\beta$
-199283	49	-83	$A_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + 3\alpha$	$2 - 7\alpha + 4\beta$
-218491	49	-91	$A_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + (-2 - 2\alpha + 5\beta)$	$10 + 13\alpha - 16\beta$
-304927	49	-127	$A_4 \times C_2$	1	$x^2 - \beta x + (2 + 4\alpha - 4\beta)$	$-9 - 17\alpha + 19\beta$
-309123	321	-3	$S_4 \times C_2$	1	$x^2 - (1 + \alpha)x + (-3 + \alpha + \beta)$	$13 - 2\alpha - 3\beta$
-333739	49	-139	$A_4 \times C_2$	1	$x^2 - (\alpha + \beta)x + (19 - 4\alpha - 8\beta)$	$-75 + 19\alpha + 34\beta$
-334611	81	-51	$A_4 \times C_2$	1	$x^2 - \alpha x + (-1 - 3\alpha - \beta)$	$4 + 12\alpha + 5\beta$

Signature $(2, 2)$ on a totally real cubic field

31213	49	13	$A_4 \times C_2$	1	$x^2 - x + (-4 + \alpha + 2\beta)$	$17 - 4\alpha - 8\beta$
52441	229	1	S_4^+	1	$x^2 - x - \alpha$	$1 + 4\alpha$
66049	257	1	S_4^+	1	$x^2 - (1 + \alpha + \beta)x + (2 + 4\alpha + 2\beta)$	$-1 - \alpha$
69629	49	29	$A_4 \times C_2$	1	$x^2 - (1 + \alpha)x + (-1 - 3\alpha - \beta)$	$5 + 14\alpha + 5\beta$
87616	148	4	S_4^+	1	$x^2 - (1 + \alpha)x + (2\alpha + \beta)$	$1 - 6\alpha - 3\beta$
98441	49	41	$A_4 \times C_2$	1	$x^2 - (1 + \beta)x + (1 + \alpha)$	$-4 - 5\alpha + 5\beta$
109520	148	5	$S_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + (4 + \alpha)$	$-14 + 2\alpha + 5\beta$
111537	81	17	$A_4 \times C_2$	1	$x^2 - (1 + \beta)x + (-5 - 4\alpha + 5\beta)$	$21 + 17\alpha - 15\beta$
142805	169	5	$A_4 \times C_2$	1	$x^2 - x + (3 + 2\alpha)$	$-11 - 8\alpha$
153664	49	64	A_4	1	$x^2 + (-2\alpha - \beta)$	$8\alpha + 4\beta$

Signature $(2, 2)$ on a complex cubic field

28037	−23	53	$S_4 \times C_2$	1	$x^2 - \alpha x + (-1 - 2\alpha - \beta)$	$4 + 8\alpha + 5\beta$
32269	−23	61	$S_4 \times C_2$	1	$x^2 - (1 + \beta)x + (1 - \beta)$	$-4 + \alpha + 7\beta$
33856	−23	64	S_4^+	1	$x^2 + (-2 - 2\alpha - \beta)$	$8 + 8\alpha + 4\beta$
35557	−31	37	$S_4 \times C_2$	1	$x^2 - (1 + \alpha)x + 1$	$-3 + 2\alpha + \beta$
40733	−23	77	$S_4 \times C_2$	1	$x^2 - (\alpha + \beta)x + (-5 - 7\alpha - 4\beta)$	$21 + 29\alpha + 16\beta$
44965	−23	85	$S_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + (-1 - \alpha)$	$6 + 7\alpha + 2\beta$
47081	−23	89	$S_4 \times C_2$	1	$x^2 - (1 + \alpha)x + (-2 + 2\alpha + 2\beta)$	$9 - 6\alpha - 7\beta$
50933	−31	53	$S_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + (1 + \beta)$	$3\alpha + 2\beta$
53429	−23	101	$S_4 \times C_2$	1	$x^2 - \alpha x + (1 - \alpha - \beta)$	$-4 + 4\alpha + 5\beta$
56144	−44	29	$S_4 \times C_2$	1	$x^2 - \beta x + \alpha$	$1 - 2\alpha + 2\beta$

Signature $(0, 3)$ on a totally real cubic field

−400967	49	−167	$A_4 \times C_2$	1	$x^2 - \beta x + 3$	$-13 - \alpha + 3\beta$
−465831	81	−71	$A_4 \times C_2$	1	$x^2 - x + (2 + \alpha)$	$-7 - 4\alpha$
−503792	148	−23	$S_4 \times C_2$	1	$x^2 - x + (4 - \alpha - \beta)$	$-15 + 4\alpha + 4\beta$
−573839	49	−239	$A_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + 4$	$-14 + 5\alpha + 4\beta$
−602651	49	−251	$A_4 \times C_2$	1	$x^2 - \alpha x + (2 - 5\alpha + 3\beta)$	$-8 + 20\alpha - 11\beta$
−679024	148	−31	$S_4 \times C_2$	1	$x^2 - x + (-\alpha + \beta)$	$1 + 4\alpha - 4\beta$
−839056	229	−16	$S_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + (1 + 4\alpha + 3\beta)$	$-1 - 5\alpha - 5\beta$
−909979	49	−379	$A_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + (1 + 4\alpha + 5\beta)$	$-2 - 11\alpha - 16\beta$
−1142512	404	−7	$S_4 \times C_2$	1	$x^2 - \alpha x + (4 + 2\alpha)$	$-16 - 8\alpha + \beta$
−1178891	49	−491	$A_4 \times C_2$	1	$x^2 - \alpha x + (1 - \alpha + \beta)$	$-4 + 4\alpha - 3\beta$

Signature $(0, 3)$ on a complex cubic field

−10051	−23	−19	$S_4 \times C_2$	1	$x^2 - (1 + \alpha)x + 1$	$-3 + 2\alpha + \beta$
−10571	−31	−11	$S_4 \times C_2$	1	$x^2 - (1 + \beta)x + (1 + \beta)$	$-2 + \alpha - \beta$
−18515	−23	−35	$S_4 \times C_2$	1	$x^2 - (\alpha + \beta)x + (-2 + 4\alpha - \beta)$	$9 - 15\alpha + 4\beta$
−22747	−23	−43	$S_4 \times C_2$	1	$x^2 - (1 + \alpha)x + (3 + 4\alpha + 2\beta)$	$-11 - 14\alpha - 7\beta$
−27556	−83	−4	$S_4 \times C_2$	1	$x^2 - \beta x + 1$	$-2 + \alpha$
−27848	−59	−8	$S_4 \times C_2$	1	$x^2 - (1 + \alpha)x + (2 + \alpha + \beta)$	$-7 - 2\alpha - 3\beta$
−29095	−23	−55	$S_4 \times C_2$	1	$x^2 - (\alpha + \beta)x + (1 + 2\alpha + \beta)$	$-3 - 7\alpha - 4\beta$
−31211	−23	−59	$S_4 \times C_2$	1	$x^2 - x + \alpha$	$1 - 4\alpha$
−33856	−23	−64	$S_4 \times C_2$	1	$x^2 + \alpha$	-4α
−37479	−31	−39	$S_4 \times C_2$	1	$x^2 - (1 + \alpha + \beta)x + (-1 - 3\alpha + 5\beta)$	$8 + 15\alpha - 14\beta$

Totally real cubic fields

d_k	ind.	polyn. of α	integ. basis
49	1	x^3+x^2-2x-1	$(1, \alpha, \alpha^2)$
81	1	x^3-3x-1	$(1, \alpha, \alpha^2)$
148	1	x^3+x^2-3x-1	$(1, \alpha, \alpha^2)$
169	1	x^3-x^2-4x-1	$(1, \alpha, \alpha^2)$
229	1	x^3-4x-1	$(1, \alpha, \alpha^2)$
257	1	x^3-5x-3	$(1, \alpha, \alpha^2)$
321	1	x^3+x^2-4x-1	$(1, \alpha, \alpha^2)$
404	1	x^3-x^2-5x-1	$(1, \alpha, \alpha^2)$

Complex cubic fields

-23	1	x^3+x^2-1	$(1, \alpha, \alpha^2)$
-31	1	x^3-x^2-1	$(1, \alpha, \alpha^2)$
-44	1	x^3-x^2-x-1	$(1, \alpha, \alpha^2)$
-59	1	x^3+2x^2-1	$(1, \alpha, \alpha^2)$
-83	1	x^3-x^2+x-2	$(1, \alpha, \alpha^2)$

Acknowledgments

This work could not have been conducted without the sound advice of J. Martinet. In order to perform the many calculations needed here, we made intensive use of the PARI-package, created under the supervision of H. Cohen; this package is implemented on SUN workstations which are partially supported by the "P.R.C. mathématiques et informatique."

Bibliography

1. I. O. Angell, *A table of complex cubic fields*, Bull. London Math. Soc. **5** (1973), 37–38.
2. ———, *A table of totally real cubic fields*, Math. Comp. **30** (1976), 184–187.
3. A.-M. Bergé, J. Martinet, and M. Olivier, *The computation of sextic fields with a quadratic subfield*, Math. Comp. **54** (1990), 869–884.
4. G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), 863–911.
5. V. Ennola and R. Turunen, *On totally real cubic fields*, Math. Comp. **44** (1985), 495–518.
6. U. Fincke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), 463–471.
7. H. J. Godwin, *The determination of fields of small discriminant with a given subfield*, Math. Scand. **6** (1958), 40–46.
8. H. J. Godwin and P. Samet, *A table of real cubic fields*, J. London Math. Soc. **34** (1959), 108–110.
9. P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc. **87** (1983), 579–585.
10. P. Llorente and J. Quer, *On totally real cubic fields with discriminant* $D < 10^7$, Math. Comp. **50** (1988), 581–594.
11. J. Martinet, *Méthodes géométriques dans la recherche des petits discriminants*, Progr. Math., vol. 59, Birkhäuser, Boston, 1985, pp. 147–179.
12. ———, *Discriminants and permutation groups*, Number Theory (Richard A. Mollin, ed.), Walter de Gruyter, Berlin and New York, 1990, pp. 359–385.

13. M. Olivier, *Corps sextiques primitifs*, Ann. Inst. Fourier (Grenoble) **40** (1990), 757–767.
14. 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.
15. D. Shanks, *Review of I. O. Angell, "Table of complex cubic fields"*, Math. Comp. **29** (1975), Review **33**, 661–665.
16. P. Smadja, *Calculs effectifs sur les idéaux des corps de nombres algébriques*, Univ. d'Aix-Marseille, U.E.R. de Luminy, 1976.

CENTRE DE RECHERCHE EN MATHÉMATIQUES DE BORDEAUX, 351 COURS DE LA LIBÉRATION, 33405 TALENCE CEDEX, FRANCE
E-mail address: olivier@mizar.greco-prog.fr