MATHEMATICS OF COMPUTATION
VOLUME 53, NUMBER 187
JULY 1989, PAGES 387–397

On the Computation of Unit Groups and Class Groups of Totally Real Quartic Fields

By J. Buchmann, M. Pohst, and J. v. Schmettow*

Abstract. In this paper we describe the computation of a system of fundamental units and of the class group for each totally real quartic field $\mathscr{F}$ of discriminant less than 10^6. Generating equations, integral bases, and the Galois groups for all those fields were recently given by Buchmann and Ford.

1. Introduction. In this paper we describe the computation of a system of fundamental units and of the class groups for all the 13073 totally real quartic fields of discriminant less than 10^6. Generating equations, integral bases and the Galois groups for all those fields were presented in Buchmann and Ford [3].

The theory for the algorithms used here has been previously presented in Buchmann [1], [2] and in Pohst and Zassenhaus [9], [10]. One motive for doing this work was our interest in the practical performance of those methods. It is our experience that they are, in fact, very efficient. This paper describes the implementation of the algorithms on a computer and the main results of the computations.

The subject of the second section is the computation of subgroups of the unit group of finite index by means of the reduction theory described in [1]. The third section shows how to compute a basis for the full unit group using a new method for computing a lower bound for the regulator (see [10]). In Section 4 the implementation of the class group algorithm [9] is presented together with statistical information about the distribution of the class numbers. The comparison of our results with the predictions of Cohen and Martinet [4] do not show great agreement. We remark, however, that, given the range of discriminants we considered, this could not be expected.

2. Computation of Maximal Systems of Independent Units. In order to compute a maximal system of independent units in the maximal order $\mathscr{O}$ of the totally real quartic field $\mathscr{F}$, we applied the following method which is a modification of the algorithm presented in Buchmann [1].

A number μ from a fractional ideal $\mathbf{a}$ of $\mathscr{O}$ is called a *minimum* of $\mathbf{a}$ if there is no $0 \neq \alpha \in \mathbf{a}$ such that $|\alpha^{(i)}| < |\mu^{(i)}|$ for $1 \leq i \leq 4$. (By $\xi^{(i)}$ we denote the ith conjugate of a number $\xi \in \mathscr{F}$.) The norm of such a minimum is bounded:

$$|N(\mu)| \leq \sqrt{\mathscr{D}} N(\mathbf{a}).$$

Received July 26, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11–04, 11R16, 11R27, 11R29, 11R80.
*Author supported by the Friedrich-Naumann-Stiftung.

Here, $\mathscr{D}$ denotes the discriminant of $\mathscr{F}$ and $N(\mathbf{a})$ is the norm of the ideal $\mathbf{a}$. Each minimum μ of $\mathbf{a}$ has precisely four *principal neighbors* which are defined as follows. The ith principal neighbor of μ is the minimum ν of $\mathbf{a}$ which is uniquely determined by the following conditions:

$$|\nu^{(j)}| < |\mu^{(j)}| \quad \text{for } 1 \le j \le 4,\ j \ne i,$$
$$\{\alpha \in \mathbf{a}\colon |\alpha^{(j)}| < \max\{|\nu^{(j)}|,\ |\mu^{(j)}|\} \text{ for } 1 \le j \le 4\} = \{0\}.$$

The minima of $\mathbf{a}$ together with those neighbor relations form a graph G. The unit group $\mathscr{U}_{\mathscr{F}}$ of $\mathscr{O}$ acts on G and $G/\mathscr{U}_{\mathscr{F}}$ is finite. More precisely, it was shown in Buchmann [2] that

$$|G/\mathscr{U}_{\mathscr{F}}| = O(R),$$

where R is the regulator of $\mathscr{F}$. A fractional ideal $\mathbf{a}$ of $\mathscr{O}$ is called *reduced* if 1 is a minimum of $\mathbf{a}$. If $\mathbf{a}$ is a reduced ideal and if $\gamma_1, \ldots, \gamma_4$ are the principal neighbors of 1 in $\mathbf{a}$, then the ideals

$$\mathbf{a}_i = \frac{1}{\gamma_i}\mathbf{a}$$

are reduced and those reduced ideals are called the *principal neighbors* of $\mathbf{a}$. Hence the reduced ideals together with those neighbor relations form again a graph which is isomorphic to $G/\mathscr{U}_{\mathscr{F}}$. Each reduced principal ideal $\mathbf{a}$ of $\mathscr{O}$ can be written in the form

$$\mathbf{a} = \frac{1}{\mu}\mathscr{O}$$

with a minimum μ of $\mathscr{O}$. Two reduced ideals $\frac{1}{\mu}\mathscr{O}$ and $\frac{1}{\nu}\mathscr{O}$ are equal if and only if μ/ν is a unit in $\mathscr{O}$. It is, however, not advisable to store a reduced ideal $\mathbf{a}$ in terms of the corresponding minimum μ since those numbers become extremely large. We rather use the fact that there is precisely one positive integer d and one integer matrix $(a_{i,j})$ which is in Hermite normal form [10] such that the greatest common divisor of d and all matrix entries $a_{i,j}$ is one and that the numbers

$$\alpha_j = \frac{1}{d}\sum_{k=1}^{4} a_{j,k}\omega_k \qquad (1 \le j \le 4)$$

form a $\mathscr{Z}$-basis of $\mathbf{a}$. d is called the *denominator* of $\mathbf{a}$ and $(a_{i,j})$ is called the *HNF-matrix* of $\mathbf{a}$. Reduced ideals are stored and easily compared in terms of their denominators and their HNF-matrices.

Before computing a unit ε explicitly, we compute its logarithm vector

$$\mathbf{Log}\,\varepsilon = (\log|\varepsilon^{(1)}|,\ \log|\varepsilon^{(2)}|,\ \log|\varepsilon^{(3)}|).$$

Only if we know that the unit ε is neither a root of unity nor dependent on the units which we have found previously, do we compute this unit explicitly.

Now we can present the algorithm:

ALGORITHM 2.1

- **Input**: An integral basis of $\mathscr{F}$.
- **Output**: A system $\varepsilon_1, \varepsilon_2, \varepsilon_3$ of independent units of $\mathscr{O}$.

1. (*Initialization*)
   $p \leftarrow 1$, $k \leftarrow 1$, $\mathbf{a}_1 \leftarrow \mathscr{O}$, $\vec{v}_1 \leftarrow \vec{0}$, $r \leftarrow 0$.

2. (*Computation of the principal neighbors*)
   Compute the principal neighbors $\eta_1, \ldots, \eta_4$ of 1 in the reduced ideal $\mathbf{a}_k$ and the principal neighbors $\mathbf{b}_i = \frac{1}{\eta_i}\mathbf{a}_k$ $(1 \leq i \leq 4)$ of $\mathbf{a}_k$.
3. (*Comparison of the new reduced ideals with the old ones*)
   For $1 \leq i \leq 4$ execute the following steps:
   Compare $\mathbf{b}_i$ with all reduced ideals $\mathbf{a}_l$, $1 \leq l \leq p$, which have already been computed.
   If $\mathbf{b}_i = \mathbf{a}_l$ for some l then compute the logarithm vector $\vec{v}$ of the corresponding unit: $\vec{v} = \vec{v}_k + \mathbf{Log}\,\eta_i - \vec{v}_l$.
   - If $r = 0$, i.e., if we did not find a nontrivial unit so far, and if $\vec{v} \neq \vec{0}$, then put $r \leftarrow 1$, $\vec{e}_1 \leftarrow \vec{v}$, and compute a unit ε_1 with $\mathbf{Log}\,\varepsilon_1 = \vec{e}_1$ by means of Algorithm 2.2.
   - If $r > 0$ and if $\vec{e}_1, \ldots, \vec{e}_r$, $\vec{v}$ are linearly independent, then put $r \leftarrow r + 1$, $\vec{e}_r \leftarrow \vec{v}$ and compute a unit ε_r with $\mathbf{Log}\,\varepsilon_r = \vec{e}_r$ by means of Algorithm 2.2. For $r = 3$ terminate.

   But if $\mathbf{b}_i$ is distinct from all the previously computed reduced ideals, then put $p \leftarrow p + 1$, $\mathbf{a}_p \leftarrow B_i$, $\gamma_p \leftarrow \eta_i$, $\vec{v}_p \leftarrow \vec{v}$, $N_p \leftarrow k$. (The numbers N_p will be needed in Algorithm 2.2 for the computation of the units.)
4. Set $k \leftarrow k + 1$ and go to 2.

As we have already pointed out, each reduced ideal $\mathbf{a}_j$ computed in Algorithm 2.1 is of the form

$$A_j = \frac{1}{\mu_j}\mathscr{O}$$

with a minimum μ_j of $\mathscr{O}$. The unit ε_r needed in step 3 of Algorithm 2.1 can be computed via

$$\varepsilon_r = \mu_k \eta_i / \mu_l.$$

In order to calculate this unit we must be able to compute the minima μ_j (and their inverses). This can easily be done by using

ALGORITHM 2.2

- **Input**: The index j and the numbers γ_i, N_i $(1 \leq i \leq j)$ computed in Algorithm 2.1.
- **Output**: The number μ_j.

1. (*Initialization*) Set $\mu_j \leftarrow 1$, $i \leftarrow j$.
2. (*Multiplication*) Set $\mu_j \leftarrow \mu_j \gamma_i$.
3. (*Change i*) Set $i \leftarrow N_i$. For $i = 1$ terminate, else go to 2.

Clearly, a slight modification of this algorithm also yields the inverse of μ_j.

Finally, we have to explain how the ith principal neighbor η_i of 1 in a reduced ideal $\mathbf{a}$ of $\mathscr{O}$ and the corresponding principal neighbor $\frac{1}{\eta_i}\mathbf{a}$ is computed. For this purpose we compute a basis $\vec{a}_1, \ldots, \vec{a}_4$ of the Minkowski lattice $L(\mathbf{a})$ which corresponds to the ideal $\mathbf{a}$:

$$\vec{a}_j = (\alpha_j^{(1)}, \ldots, \alpha_j^{(4)}) \qquad (1 \leq j \leq 4),$$

where $\alpha_1, \ldots, \alpha_4$ is a $\mathbb{Z}$-basis of $\mathbf{a}$. Now we apply

ALGORITHM 2.3

- **Input**: A basis $\vec{a}_1, \ldots, \vec{a}_4$ of the lattice $L(\mathbf{a})$ and the index i.
- **Output**: A lattice vector $\vec{b} = \sum_{j=1}^{4} \lambda_j \vec{a}_j$ in $L(\mathbf{a})$ which corresponds to the ith principal neighbor $\eta_i = \sum_{j=1}^{4} \lambda_j \alpha_j$ of 1 in $\mathbf{a}$.

1. (*Initialization*) Set $f \leftarrow 2$, $g \leftarrow 0$, $C_j \leftarrow 1$ for $j \neq i$, $C_i \leftarrow 100$.
2. Search for a lattice point $\vec{0} \neq \vec{b} = (b_1, \ldots, b_4)$ with $|b_j| < C_j$ for $1 \leq j \leq 4$.
3. If the search was successful then set $C_i \leftarrow b_i/f$. Then go to 2. In case of an unsuccessful search and $g = 0$ set $C_i \leftarrow 2C_i$ and go to 2. In case of an unsuccessful search and $g = f = 1$ terminate. Else set $f \leftarrow 1$, $C_i \leftarrow 2C_i$ and go to 2.

Next we explain how to search for the lattice point $\vec{b}$ in step 2 of Algorithm 2.3.

ALGORITHM 2.4

- **Input**: A basis $\vec{a}_1, \ldots, \vec{a}_4$ of the lattice $L(\mathbf{a})$ ($\vec{a}_j = (a_{1,j}, \ldots, a_{4,j})$, $1 \leq j \leq 4$), constants C_i, $1 \leq i \leq 4$.
- **Output**: A lattice vector $\vec{b} = (b_1, \ldots, b_4) \neq L\vec{0} \in L(\mathbf{a})$ with $|b_i| < C_i$ for $1 \leq i \leq 4$ or the information that no such lattice vector exists.

1. (*Rescaling of basis*) Set $a_{i,j} \leftarrow a_{i,j}/C_i$ for $1 \leq i, j \leq 4$.
2. (*Reduction*) Apply LLL-reduction to the basis $\vec{a}_1, \ldots, \vec{a}_4$.
3. (*One basis vector admissible?*) If all the coordinates of one of the basis vectors are in absolute value less than 1, then return the corresponding vector $\vec{b}$ in the original lattice and terminate.
4. (*Enumeration*) Using the search strategy of Fincke and Pohst [6], search for all the lattice vectors whose length is less than 4. For each of those vectors check whether all of its coordinates are in absolute value less than 1. If such a vector is found, then return the corresponding vector $\vec{b}$ in the original lattice and terminate. Otherwise, no admissible lattice vector exists and the algorithm returns this information and terminates.

A basis of $\mathbf{a}' = \frac{1}{\eta_i}\mathbf{a}$ is obtained by dividing all the basis elements of $\mathbf{a}$ by η_i. The denominator d' of $\mathbf{a}'$ can then easily be computed and the Hermite reduction algorithm [5] yields the HNF-matrix of $\mathbf{a}'$.

We conclude this section with some remarks. The algorithm described above can easily be generalized to arbitrary number fields. We will prove in a subsequent paper that the algorithm always succeeds to find a maximal system of independent units of $\mathcal{O}$.

The practical performance of the algorithm is quite impressive. On the one hand, the index I of the subgroup generated by the units found by the algorithm is mostly 1, i.e., most of the time the algorithm actually yields a system of fundamental units. In the rest of the cases, I was either 2 or 3 except for very few cases with small discriminants where indices up to 8 were observed. On the other hand, the number p of reduced ideals needed in Algorithm 2.1 in order to compute the units is quite small (≤ 100).

Table 1 gives an indication of the characteristic behavior of the algorithm.

3. Computation of Fundamental Units. To determine generators for the full unit group $\mathcal{U}_{\mathcal{F}}$ from the units $\varepsilon_1, \varepsilon_2, \varepsilon_3$ computed in Algorithm 2.1, we proceed as follows.

In a first step we compute an upper bound for the index $(\mathcal{U}_{\mathcal{F}} : \mathcal{U}_\varepsilon)$ for $\mathcal{U}_\varepsilon = \langle -1 \rangle \times \langle \varepsilon_1 \rangle \times \langle \varepsilon_2 \rangle \times \langle \varepsilon_3 \rangle$. Since this index equals the quotient of the regulator of $\mathcal{U}_\varepsilon$, say $R(\mathcal{U}_\varepsilon)$, and the regulator R of $\mathcal{F}$, and since $R(\mathcal{U}_\varepsilon)$ can be numerically calculated, it remains to compute a lower bound for R.

Generalizing an idea of Remak [11], [10], we determine lower bounds $M_1, \ldots, M_j$ for the first j successive minima of the positive definite quadratic form

$$\sum_{j=1}^{4} (\log |\varepsilon^{(j)}|)^2 \qquad (\varepsilon \in \mathcal{U}_{\mathcal{F}})$$

of determinant $4R^2$. Then Minkowski's theorem on successive minima yields

$$R \geq (M_1 \cdots M_{j-1} M_j^{4-j} \tfrac{1}{8})^{1/2} \quad [10].$$

The lower bounds $M_1, \ldots, M_j$ are determined in the following way. In $\mathcal{O}$ we compute a set

$$S = \{\alpha \in \mathcal{O} \setminus \mathcal{Z} : \mathrm{Tr}(\alpha^2) \leq C\}$$

for a suitably chosen constant $C > 6$. The choice of C depends on how much computation time is needed to enumerate the corresponding ellipsoid (see Fincke and Pohst [6]). For example, $C = \max\{\mathrm{Tr}(\varepsilon_i^2) : 1 \leq i \leq 3\}$ would be optimal but is usually too large for exhaustive search. In our computations we chose $C = \mathrm{Tr}(\omega_4^2)$, where the basis $\omega_1, \ldots, \omega_4$ corresponds to an LLL-reduced basis of the lattice $L(\mathcal{O})$.

Let $\tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_k$ be a maximal set of independent units contained in S subject to

$$\sum_{j=1}^{4} |\tilde{\varepsilon}_i^{(j)}|^2 = \min \left\{ \sum_{j=1}^{4} |\varepsilon^{(j)}|^2 : \varepsilon \in \mathcal{U}_{\mathcal{F}} \cap S,\ \tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_{i-1},\ \varepsilon \right.$$
$$\left. \text{independent for } 1 \leq i \leq k \right\}.$$

We set

$$M_i^* = \mathrm{Tr}(\tilde{\varepsilon}_i^2) \quad \text{for } 1 \leq i \leq k,$$
$$M_i^* = C \quad \text{for } k+1 \leq i \leq 3.$$

Then the solution of an extremal value problem with side conditions (see Pohst and Zassenhaus [10]) yields

$$M_i \geq \left(\log \left(\frac{M_i^*}{4} + \left(\frac{(M_i^*)^2}{16} - 1 \right)^{1/2} \right) \right)^2 \quad \text{for } 1 \leq i \leq 3.$$

In this way we obtain very good lower regulator bounds and, correspondingly, very good upper bounds for $(\mathcal{U}_{\mathcal{F}} : \mathcal{U}_\varepsilon)$. Table 1 shows some typical data.

The extension of $\mathcal{U}_\varepsilon$ to $\mathcal{U}_{\mathcal{F}}$ is now routine. Since the upper bounds for $(\mathcal{U}_{\mathcal{F}} : \mathcal{U}_\varepsilon)$ are quite small, and since the rank of the unit group is small, too, we proceed in a straightforward manner by trying to find a unit $\varepsilon \in \mathcal{U}_{\mathcal{F}}$ with

$$\varepsilon = (\pm \varepsilon_1^{m_1} \cdots \varepsilon_{j-1}^{m_{j-1}} \varepsilon^j)^{1/p} \tag{1}$$

for $1 \le j \le 3$, $0 \le m_i < p$ and for each prime number p below $(\mathcal{U}_{\mathcal{F}} : \mathcal{U}_{\varepsilon})$. It suffices to compute the right-hand side of (1) numerically with adequate accuracy to find a solution $\varepsilon \in \mathcal{U}_{\mathcal{F}}$ via the dual basis (if such a solution exists). In the worst case which occurred during our computation, namely for $p = 23$, this requires 553 tests. For larger values of p and larger ranks of the unit group, one should use the more ingenious methods described in Pohst and Zassenhaus [10].

TABLE 1

Lower regulator bounds and period length.

$\mathcal{D}$	p	R	$R \ge$	$(\mathcal{U}_{\mathcal{F}} : \mathcal{U}_{\varepsilon})$
948609	11	67.4120	21.9628	1
948717	2	39.0451	19.3235	2
948777	13	163.2968	16.4482	1
948800	3	22.2365	13.5956	1
948896	10	169.0664	18.6861	1
949009	18	119.5694	17.5574	1
949085	5	50.5139	23.6635	3
949248	18	81.6801	14.5766	1
949464	5	108.0004	15.6859	1
949464	19	104.5055	15.7258	1
949464	43	313.7682	23.9639	1
949469	6	108.0651	17.9186	1
949504	8	99.5800	26.3687	1
949525	15	51.0950	7.9975	1
949528	10	165.7839	22.9010	1
949644	14	156.3588	19.6653	1

4. Computation of Class Groups. For the computation of the class group $\mathrm{Cl}_{\mathcal{F}}$ we implemented the algorithm of Pohst and Zassenhaus [9], [12].

The main idea is to determine the prime ideal decomposition of all prime numbers below the Minkowski bound

$$M_{\mathcal{F}} = 0.09375\sqrt{\mathcal{D}} < 93.75$$

and to find sufficiently many relations between those prime ideals. (We note that it suffices to choose $M_{\mathcal{F}} = \sqrt{\mathcal{D}/500} = 0.04472\sqrt{\mathcal{D}}$ [8].) The relations are stored in a so-called *class group matrix* $\mathrm{CGM} = (c_{i,j})$. The class group structure is derived from the Hermite normal form of the class group matrix. In this way the number of necessary principal ideal tests is kept to a minimum.

ALGORITHM 4.1

- **Input**: An integral basis $1 = \omega_1, \ldots, \omega_4$ of $\mathcal{F}$ and a system of fundamental units.
- **Output**: The class group structure.

1. Compute the Minkowski bound $M_{\mathcal{F}}$.
2. Decompose all prime numbers $p_1, \ldots, p_w$ below $M_{\mathcal{F}}$ into prime ideals $\mathbf{p}_1, \ldots, \mathbf{p}_v$ viz.
$$p_j\mathcal{O} = \prod \mathbf{p}_i^{c_{i,j}}.$$
The exponent vectors $(c_{1,j}, \ldots, c_{v,j})$ form the first w columns of the class group matrix CGM.

3. Determine (at least $v - w$) additional elements $\beta_j\mathcal{O}$ satisfying $\beta_j\mathcal{O} = \prod \mathbf{p}_i^{c_{i,j}}$ $(j = v+1, \dots)$ and insert the exponent vectors into the corresponding columns of CGM.
4. Replace CGM by its Hermite normal form and set w to the rank of CGM. In case $w < v$ go to 3.
5. Derive the class group structure by the methods explained below and terminate.

In the sequel we explain the steps of Algorithm 4.1 in greater detail.

In step 2 the prime ideal decomposition of the principal ideal $p\mathcal{O}$ generated by the prime number $p \leq M_{\mathcal{F}}$ is obtained as follows. Assume that $\mathcal{F} = \mathcal{Q}(\rho)$ for a zero ρ of a monic irreducible polynomial $f \in \mathcal{Z}[t]$. In case of $p \nmid (\mathcal{O} : \mathcal{Z}[\rho])$ we factorize the generating polynomial f modulo $p\mathcal{Z}[t]$ by Berlekamp's method ([7]):

$$f(t) \equiv \prod_{i=1}^{m} f_i(t)^{e_i} \mod p\mathcal{Z}[t] \tag{2}$$

implying

$$p\mathcal{O} = \prod_{i=1}^{m} \mathbf{p}_i^{e_i} \tag{3}$$

with prime ideals

$$\mathbf{p}_i = p\mathcal{O} + f_i(\rho)\mathcal{O} \quad \text{of norm } N(\mathbf{p}_i) = p^{\deg f_i}. \tag{4}$$

The case $p \mid (\mathcal{O} : \mathcal{Z}[\rho])$ is more difficult to deal with, since the factorization (2) does not necessarily yield prime ideals in (4). Here we applied a more general (but more "expensive") algorithm explained in [10].

We remark that for totally real quartic fields of discriminant less than 10^6, the number of rows of CGM is a priori at most 96. It did not exceed 47 in our computations.

In order to determine principal ideals $\beta\mathcal{O}$ which can be completely factorized over the factor base $P := \{\mathbf{p}_1, \dots, \mathbf{p}_v\}$ in step 3 of Algorithm 4.1, we compute vectors of Euclidean length below C (C appropriately chosen, in our case $C = 30$) in the Minkowski lattice $L(\mathcal{O})$. By the inequality between geometric and arithmetic means, the norms of the corresponding algebraic integers $\beta = b_1\omega_1 + \cdots + b_4\omega_4$ satisfy

$$|N(\beta)| \leq \frac{C^2}{16}.$$

If $N(\beta)$ is a product of prime numbers $p \leq M_{\mathcal{F}}$, then $\beta\mathcal{O}$ can be completely factorized over P. In order to find the maximum exponent k such that $\mathbf{p}^k \mid \beta\mathcal{O}$ for some prime ideal $\mathbf{p} = p\mathcal{O} + \alpha\mathcal{O} \in P$, we must check whether $\mathbf{p}^k \mid \beta\mathcal{O}$, i.e., $\beta \in \mathbf{p}^k = p^k\mathcal{O} + \alpha^k\mathcal{O}$. We first compute the HNF-matrix of $\mathbf{p}^k$. For this purpose, we note that $p^k\omega_1, \dots, p^k\omega_4, \alpha^k\omega_1, \dots, \alpha^k\omega_4$ is a system of generators for $\mathbf{p}^k$ over $\mathcal{Z}$. The HNF-matrix H of $\mathbf{p}^k$ is therefore obtained by applying Hermite reduction

modulo p^k [5] to the matrix

$$\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & p^k & 0 & 0 & 0 \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & 0 & p^k & 0 & 0 \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & 0 & 0 & p^k & 0 \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & 0 & 0 & 0 & p^k \end{pmatrix},$$

where the $a_{i,j}$ are defined by

$$\alpha^k \omega_j = \sum_{i=1}^{4} a_{i,j} \omega_i.$$

Then $\beta \in \mathbf{p}^k$ if and only if the system

$$H\vec{x} = \begin{pmatrix} b_1 \\ \vdots \\ b_4 \end{pmatrix}$$

has a solution $\vec{x} \in \mathcal{Z}^4$. But that can be easily checked.

In step 5 of Algorithm 4.1, CGM is a nonsingular $v \times v$ matrix in Hermite normal form. The columns represent exponent vectors with respect to the prime ideals $\mathbf{p}_i$ whose power products are principal ideals. The determinant of CGM is a multiple of $h_{\mathcal{F}}$. For det(CGM) = 1 the class number is 1 and we are done. This occurred in 11934 cases. Now let det(CGM) > 1. For $c_{i,i} = 1$ we remove column i and row i of CGM without loss of information about the class group. The general treatment of the remaining matrix is contained in [9] and [12]; we only discuss those types of matrices which actually occurred in the 13073 cases we dealt with. In this last stage we applied the principal ideal test of [10].

1. CGM = (q), $q \in \{2, 3, 5\}$ (1014, 65, 4 cases), $h_{\mathcal{F}} \in \{1, q\}$. We only need to check whether $\mathbf{p}$ itself is principal. In that case the class number is 1, otherwise we obtain $h_{\mathcal{F}} = q$ and $\mathrm{Cl}_{\mathcal{F}} \cong C_q$.
2. CGM = (4) (51 cases), $h_{\mathcal{F}} \in \{1, 2, 4\}$. The class number is

$$\left\{ \begin{matrix} 1 \\ 2 \\ 4 \end{matrix} \right\} \quad \text{for} \quad \left\{ \begin{matrix} \mathbf{p} \text{ principal} \\ \mathbf{p}^2 \text{ principal, } \mathbf{p} \text{ not principal} \\ \mathbf{p}^2 \text{ not principal} \end{matrix} \right\}.$$

3. CGM = (6) (1 case; $\mathcal{D} = 861025$), $h_{\mathcal{F}} \in \{1, 2, 3, 6\}$. Since neither $\mathbf{p}^3$ nor $\mathbf{p}^2$ are principal, the result is $h_{\mathcal{F}} = 6$, $\mathrm{Cl}_{\mathcal{F}} \cong C_6$.
4. CGM = $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ (4 cases; $\mathcal{D} \in \{665856, 738000, 882000, 946125\}$). We know that $\mathbf{p}_1^2 \in H_F$, $\mathbf{p}_2^2 \in H_F$. First we check $\mathbf{p}_2 \in H_F$. In all four cases the result is negative. Hence we check whether $\mathbf{p}_1\mathbf{p}_2$ or $\mathbf{p}_1$ are principal. In all cases both are not principal. Thus we have proved $\mathrm{Cl}_{\mathcal{F}} \cong C_2 \times C_2$, $h_{\mathcal{F}} = 4$.

The multiplication of the prime ideals in the last case was done by using the ideal arithmetic developed in [9].

We summarize the distribution of the class numbers in dependence on the structure of the Galois groups $\Gamma := \mathrm{Gal}(\mathscr{F}/\mathscr{Q})$:

Γ	$h_{\mathscr{F}}=1$	$h_{\mathscr{F}}=2$	$h_{\mathscr{F}}=3$	$h_{\mathscr{F}}=4$	$h_{\mathscr{F}}=5$	$h_{\mathscr{F}}=6$	$\sum$
D8	3822	582	45	34	2	1	4486
C4	35	22	–	2	–	–	59
V4	130	53	5	8	–	–	196
S4	7936	343	15	5	2	–	8301
A4	22	9	–	–	–	–	31
$\sum$	11945	1009	65	49	4	1	13073

Γ	$h_{\mathscr{F}}=1$	$h_{\mathscr{F}}=2$	$h_{\mathscr{F}}=3$	$h_{\mathscr{F}}=4$	$h_{\mathscr{F}}=5$	$h_{\mathscr{F}}=6$	$\sum$
D8	85.20%	12.97%	1.00%	0.76%	0.04%	0.02%	34.32%
C4	59.32%	37.29%	–	3.39%	–	–	0.45%
V4	66.33%	27.04%	2.55%	4.08%	–	–	1.50%
S4	95.60%	4.13%	0.18%	0.06%	0.02%	–	63.50%
A4	70.97%	29.03%	–	–	–	–	0.24%
$\sum$	91.37%	7.72%	0.50%	0.37%	0.03%	0.01%	100%

The last tables present number fields of smallest discriminant for a given class group depending on the Galois group ($h_{\mathscr{F}}=4$ denotes the cyclic group of order 4, $h_{\mathscr{F}}=2\cdot 2$ indicates the Klein four group).

Γ	$h_{\mathscr{F}}=1$	$h_{\mathscr{F}}=2$	$h_{\mathscr{F}}=3$	$h_{\mathscr{F}}=4$	$h_{\mathscr{F}}=2\cdot 2$	$h_{\mathscr{F}}=5$	$h_{\mathscr{F}}=6$
D8	725	32625	97025	416000	738000	804005	861025
C4	1125	51200	–	–	882000	–	–
V4	1600	21025	485809	270400	665856	–	–
S4	1957	56025	191769	556357	–	761428	–
A4	26569	76729	–	–	–	–	–

We now present the above fields in greater detail: the first column contains the coefficients a_1, a_2, a_3, a_4 of the minimal polynomial $f(t) = t^4 + a_1 t^3 + a_2 t^2 + a_3 t + a_4$, the second column the field discriminant. In the third column we list an integral basis in terms of powers of a root ρ of f. The last two columns contain the coefficients of a full set of fundamental units in terms of the integral basis and the regulator.

f	$\mathscr{D}$	integral basis	$\mathscr{U}_{\mathscr{F}}$	R
$-1,-3,1,1$	725	$1,\rho,\rho^2,\rho^3$	$-1,2,1,-1$ $0,-1,0,0$ $-1,1,0,0$	0.8251
$-1,-4,4,1$	1125	$1,\rho,\rho^2,\rho^3$	$-1,3,0,-1$ $1,-1,0,0$ $1,3,-1,-1$	1.1655
$0,-6,0,4$	1600	$1,\rho,\rho^2/2,\rho^3/2$	$1,0,-1,0$ $1,-2,-1,1$ $1,2,0,-1$	1.5425
$0,-4,-1,1$	1957	$1,\rho,\rho^2,\rho^3$	$0,-1,0,0$ $2,-3,-1,1$ $0,-2,-1,1$	1.9184
$-2,-23,24,-1$	21025	$1,\rho,(1+\rho+\rho^2)/2,$ $(2+\rho+3\rho^2+\rho^3)/18$	$1,-2,-1,2$ $0,-1,0,1$ $-6,5,2,-4$	5.0410
$-2,-7,3,8$	26569	$1,\rho,\rho^2,\rho^3$	$-1,-1,0,0$ $9,-3,-7,2$ $-11,-15,-2,2$	15.7092
$-1,-24,29,31$	32625	$1,\rho,(1+\rho+\rho^2)/3,$ $(-1+\rho^3)/18$	$-1,1,0,-1$ $0,-1,1,-1$ $-1,-1,1,1$	5.9428
$0,-24,-40,14$	51200	$1,\rho,\rho^2,$ $(-2\rho+\rho^2+\rho^3)/7$	$-1,4,1,-2$ $-3,9,3,-5$ $-3,-1,0,0$	9.8280
$0,-9,-5,9$	56025	$1,\rho,\rho^2,\rho^3$	$5,-5,-2,1$ $7,1,-1,0$ $10,-12,-3,2$	15.2956
$-1,-16,3,1$	76729	$1,\rho,\rho^2,$ $(1+2\rho+2\rho^2+\rho^3)/4$	$0,-1,0,0$ $-6,22,4,-5$ $2,-5,-1,1$	12.7132
$-1,-37,-2,164$	97025	$1,\rho,\rho^2,$ $(26+13\rho+35\rho^2+\rho^3)/110$	$-1,-1,-1,3$ $5,2,2,-7$ $1,-1,-2,5$	8.2606
$-1,-11,18,-1$	191769	$1,\rho,\rho^2,\rho^3$	$2,-1,0,0$ $0,-1,0,0$ $-2,-6,2,1$	16.2576
$0,-18,0,16$	270400	$1,\rho,\rho^2/2,$ $(2\rho+\rho^3)/4$	$-1,5,0,-1$ $-3,-4,0,1$ $-17,-19,2,4$	23.3504
$0,-20,-40,-15$	416000	$1,\rho,\rho^2,\rho^3$	$8,16,2,-1$ $7,15,2,-1$ $-17,-39,-8,3$	24.6795
$0,-29,0,36$	485809	$1,\rho,(\rho+\rho^2)/2,$ $(6+\rho+\rho^3)/12$	$-3,4,0,-2$ $17,10,-14,-16$ $1,0,-2,2$	97.1575
$-1,-18,44,-25$	556357	$1,\rho,\rho^2,\rho^3$	$1,-1,0,0$ $2,-1,0,0$ $-11,16,-1,-1$	13.0653

f	$\mathscr{D}$	integral basis	$\mathscr{U}_{\mathscr{F}}$	R
$0, -52, 0, 625$	665856	$1, \rho, \rho^2, (-2\rho + \rho^3)/25$	$-1, 1, 0, -1$ $0, 2, 0, -3$ $26, 5, -1, -5$	21.5450
$-2, -91, 152, 1681$	738000	$1, \rho, \rho^2, (-13 + 8\rho - 11\rho^2 + \rho^3)/31$	$-13, -4, 1, 2$ $-12, 1, 0, -1$ $64, 19, -5, -10$	12.5293
$-2, -24, -30, -8$	761428	$1, \rho, \rho^2, \rho^3/2$	$9, 21, 3, -2$ $-7, -20, -3, 2$ $3, 1, 0, 0$	33.9772
$-2, -20, 21, 10$	804005	$1, \rho, \rho^2, (1 + 2\rho + 2\rho^2 + \rho^3)/7$	$6, 10, 1, -3$ $0, 0, 1, -1$ $2, 6, 1, -1$	47.1464
$-2, -93, 94, 2129$	861025	$1, \rho, (-3 - \rho + \rho^2)/8, (-3\rho - \rho^2 + \rho^3)/8$	$5, 0, -1, 0$ $50, 7, -8, -1$ $-63, -9, 14, 2$	15.1622
$-2, -106, 212, 1996$	882000	$1, \rho, \rho^2/2, (-42 + 52\rho + 9\rho^2 + \rho^3)/118$	$3, 1, 0, -1$ $-12, -1, 1, -1$ $-61, -31, -2, 30$	15.7995

Acknowledgment. We thank the referee for useful hints.

Heinrich-Heine-Mathematisches Institut
Universität Düsseldorf
Universitätsstrasse 1
D-4000 Düsseldorf, West Germany
E-mail: pohst@dd0rud81.bitnet

1. J. BUCHMANN, "On the computation of units and class numbers by a generalization of Lagrange's algorithm," *J. Number Theory*, v. 26, 1987, pp. 8–30.

2. J. BUCHMANN, "On the period length of the generalized Lagrange algorithm," *J. Number Theory*, v. 26, 1987, pp. 31–37.

3. J. BUCHMANN & D. FORD, "On the computation of totally real quartic fields of small discriminant," *Math Comp.*, v. 52, 1989, pp. 161–174.

4. H. COHEN & J. MARTINET, "Class groups of number fields: Numerical heuristics," *Math. Comp.*, v. 48, 1987, pp. 123–137.

5. P. D. DOMICH, R. KANNAN & L. E. TROTTER, JR., "Hermite normal form computation using modulo determinant arithmetic," *Math. Oper. Res.*, v. 12, 1987, pp. 50–59.

6. U. FINCKE & M. POHST, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Math. Comp.*, v. 44, 1985, pp. 463–471.

7. D. E. KNUTH, *The Art of Computer Programming, Vol. 2 : Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1981.

8. P. NOORDZIJ, "Über das Produkt von vier reellen, homogenen, linearen Formen," *Monatsh. Math.*, v. 71, 1967, pp. 436–445.

9. M. POHST & H. ZASSENHAUS, "Über die Berechnung von Klassenzahlen und Klassengruppen algebraischer Zahlkörper," *J. Reine Angew. Math.*, v. 361, 1985, pp. 50–72.

10. M. POHST & H. ZASSENHAUS, *Algorithmic Algebraic Number Theory*, Cambridge Univ. Press, New York, 1989.

11. R. REMAK, "Über die Grössenbeziehung zwischen Diskriminante und Regulator eines algebraischen Zahlkörpers," *Compositio Math.*, v. 10, 1952, pp. 245–285.

12. J. GRAF V. SCHMETTOW, *Über die Berechnung von Klassengruppen algebraischer Zahlkörper*, Diplomarbeit, Düsseldorf, 1987.