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 $F$ 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 $O$ of the totally real quartic field $F$, we applied the following method which is a modification of the algorithm presented in Buchmann [1].

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

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

Received July 26, 1988.


*Author supported by the Friedrich-Naumann-Stiftung.

©1989 American Mathematical Society

0025-5718/89 $1.00 + .25 per page

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Here, $\mathcal{D}$ denotes the discriminant of $\mathcal{O}$ and $N(\alpha)$ is the norm of the ideal $\alpha$. Each minimum $\mu$ of $\mathcal{O}$ has precisely four principal neighbors which are defined as follows. The $i$th principal neighbor of $\mu$ is the minimum $\nu$ of $\mathcal{O}$ which is uniquely determined by the following conditions:

$$|\nu^{(j)}| < |\mu^{(j)}| \quad \text{for} \ 1 \leq j \leq 4, \ j \neq i,$$

$$\{\alpha \in \mathcal{O} : |\alpha^{(j)}| < \max\{|\nu^{(j)}|, |\mu^{(j)}|\} \text{ for } 1 \leq j \leq 4\} = \{0\}.$$

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

$$|G/\mathbb{U}_G| = O(R),$$

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

$$a_i = \frac{1}{\gamma_i} \alpha$$

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

$$\alpha = \frac{1}{\mu} \mathcal{O}$$

with a minimum $\mu$ of $\mathcal{O}$. Two reduced ideals $\frac{1}{\mu_1} \mathcal{O}$ and $\frac{1}{\mu_2} \mathcal{O}$ are equal if and only if $\mu_1/\mu_2$ is a unit in $\mathcal{O}$. It is, however, not advisable to store a reduced ideal $\alpha$ in terms of the corresponding minimum $\mu$ 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

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

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

Before computing a unit $\epsilon$ explicitly, we compute its logarithm vector

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

Only if we know that the unit $\epsilon$ 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 $\mathcal{O}$.
- **Output**: A system $\epsilon_1, \epsilon_2, \epsilon_3$ of independent units of $\mathcal{O}$.

1. **Initialization**

   $p \leftarrow 1$, $k \leftarrow 1$, $\alpha_1 \leftarrow \mathcal{O}$, $\nu_1 \leftarrow 0$, $r \leftarrow 0$. 


2. **(Computation of the principal neighbors)**

Compute the principal neighbors $\eta_1, \ldots, \eta_4$ of 1 in the reduced ideal $a_k$ and the principal neighbors $b_i = \frac{1}{\eta_i}a_k$ ($1 \leq i \leq 4$) of $a_k$.

3. **(Comparison of the new reduced ideals with the old ones)**

For $1 \leq i \leq 4$ execute the following steps:

- Compare $b_i$ with all reduced ideals $a_l$, $1 \leq l \leq p$, which have already been computed.

  If $b_i = a_l$ for some $l$ then compute the logarithm vector $\bar{v}$ of the corresponding unit: $\bar{v} = \bar{v}_k + \log \eta_i - \bar{v}_i$.

  - If $r = 0$, i.e., if we did not find a nontrivial unit so far, and if $\bar{v} \neq \bar{0}$, then put $r \leftarrow 1$, $\bar{e}_1 \leftarrow \bar{v}$, and compute a unit $e_1$ with $\log e_1 = \bar{e}_1$ by means of Algorithm 2.2.

  - If $r > 0$ and if $\bar{e}_1, \ldots, \bar{e}_r$, $\bar{v}$ are linearly independent, then put $r \leftarrow r + 1$, $\bar{e}_r \leftarrow \bar{v}$ and compute a unit $e_r$ with $\log e_r = \bar{e}_r$ by means of Algorithm 2.2. For $r = 3$ terminate.

  But if $b_i$ is distinct from all the previously computed reduced ideals, then put $p \leftarrow p + 1$, $a_p \leftarrow B_i$, $\gamma_p \leftarrow \eta_i$, $\bar{v}_p \leftarrow \bar{v}$, $N_p \leftarrow k$. (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 $a_j$ computed in Algorithm 2.1 is of the form

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

with a minimum $\mu_j$ of $\mathcal{O}$. The unit $e_r$ needed in step 3 of Algorithm 2.1 can be computed via

$$e_r = \mu_k \eta_i / \mu_i.$$

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

**ALGORITHM 2.2**

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

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 $\mu_j$.

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

$$\tilde{a}_j = (\alpha_j^{(1)}, \ldots, \alpha_j^{(4)}) \quad (1 \leq j \leq 4).$$
where \( \alpha_1, \ldots, \alpha_4 \) is a \( \mathcal{O} \)-basis of \( \alpha \). Now we apply

**Algorithm 2.3**

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

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 \( \bar{b} \neq \bar{0} = (b_1, \ldots, b_4) \) 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 \( \bar{b} \) in step 2 of Algorithm 2.3.

**Algorithm 2.4**

- **Input:** A basis \( \bar{a}_1, \ldots, \bar{a}_4 \) of the lattice \( L(\alpha) \) \( (\bar{a}_j = (a_{1,j}, \ldots, a_{4,j}) \), \( 1 \leq j \leq 4 \) \), constants \( C_i \), \( 1 \leq i \leq 4 \).
- **Output:** A lattice vector \( \bar{b} = (b_1, \ldots, b_4) \neq \bar{0} \in L(\alpha) \) 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 \( \bar{a}_{i,j} \leftarrow a_{i,j}/C_i \) for \( 1 \leq i, j \leq 4 \).
2. (Reduction) Apply LLL-reduction to the basis \( \bar{a}_1, \ldots, \bar{a}_4 \).
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 \( \bar{b} \) 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 \( \bar{b} \) in the original lattice and terminate. Otherwise, no admissible lattice vector exists and the algorithm returns this information and terminates.

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

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 (\( \leq 100 \)).

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 \( \mathcal{U}_\mathcal{J} \) 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 \( (\mathcal{U}_\mathcal{J} : \mathcal{U}_\varepsilon) \) 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 \( \mathcal{U}_\mathcal{J} \), 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

\[
\sum_{j=1}^{4} (\log |\varepsilon^{(j)}|)^2 \quad (\varepsilon \in \mathcal{U}_\mathcal{J})
\]

of determinant \( 4R^2 \). Then Minkowski’s theorem on successive minima yields

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

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

\[
S = \{ \alpha \in \mathcal{O} \setminus \mathcal{J} : \text{Tr}(\alpha^2) \leq C \}
\]

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, \( C = \max \{ \text{Tr}(\varepsilon_i^2) : 1 \leq i \leq 3 \} \) would be optimal but is usually too large for exhaustive search. In our computations we chose \( C = \text{Tr}(\omega_i^2) \), 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

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

We set

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

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 \( (\mathcal{U}_\mathcal{J} : \mathcal{U}_\varepsilon) \). Table 1 shows some typical data.

The extension of \( \mathcal{U}_\varepsilon \) to \( \mathcal{U}_\mathcal{J} \) is now routine. Since the upper bounds for \( (\mathcal{U}_\mathcal{J} : \mathcal{U}_\varepsilon) \) 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 \( \varepsilon \in \mathcal{U}_\mathcal{J} \) with

(1)

\[
\varepsilon = (\pm \varepsilon_1^{m_1} \cdots \varepsilon_{j-1}^{m_{j-1}} \varepsilon_j^{m_j})^{1/p}
\]
for $1 \leq j \leq 3$, $0 \leq m_i < p$ and for each prime number $p$ below $(\mathcal{O}_\mathcal{F} : \mathcal{O}_\mathcal{F})$. It suffices to compute the right-hand side of (1) numerically with adequate accuracy to find a solution $\varepsilon \in \mathcal{O}_\mathcal{F}$ 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.

<table>
<thead>
<tr>
<th>$\mathcal{O}$</th>
<th>$p$</th>
<th>$R$</th>
<th>$R_\geq$</th>
<th>$(\mathcal{O}<em>\mathcal{F} : \mathcal{O}</em>\mathcal{F})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>948609</td>
<td>11</td>
<td>67.4120</td>
<td>21.9628</td>
<td>1</td>
</tr>
<tr>
<td>948717</td>
<td>2</td>
<td>39.0451</td>
<td>19.3235</td>
<td>2</td>
</tr>
<tr>
<td>948777</td>
<td>13</td>
<td>163.2968</td>
<td>16.4482</td>
<td>1</td>
</tr>
<tr>
<td>948800</td>
<td>3</td>
<td>22.2365</td>
<td>13.5956</td>
<td>1</td>
</tr>
<tr>
<td>948896</td>
<td>10</td>
<td>169.0664</td>
<td>18.6861</td>
<td>1</td>
</tr>
<tr>
<td>949009</td>
<td>18</td>
<td>119.5694</td>
<td>17.5574</td>
<td>1</td>
</tr>
<tr>
<td>949085</td>
<td>5</td>
<td>50.5139</td>
<td>23.6635</td>
<td>3</td>
</tr>
<tr>
<td>949248</td>
<td>18</td>
<td>81.6801</td>
<td>14.5766</td>
<td>1</td>
</tr>
<tr>
<td>949464</td>
<td>10</td>
<td>108.0004</td>
<td>15.6859</td>
<td>1</td>
</tr>
<tr>
<td>949464</td>
<td>19</td>
<td>104.5055</td>
<td>15.7258</td>
<td>1</td>
</tr>
<tr>
<td>949464</td>
<td>43</td>
<td>313.7682</td>
<td>23.9639</td>
<td>1</td>
</tr>
<tr>
<td>949469</td>
<td>6</td>
<td>108.0651</td>
<td>17.9186</td>
<td>1</td>
</tr>
<tr>
<td>949504</td>
<td>8</td>
<td>99.5800</td>
<td>26.3687</td>
<td>1</td>
</tr>
<tr>
<td>949525</td>
<td>15</td>
<td>51.0950</td>
<td>7.9975</td>
<td>1</td>
</tr>
<tr>
<td>949528</td>
<td>10</td>
<td>165.7839</td>
<td>22.9010</td>
<td>1</td>
</tr>
<tr>
<td>949644</td>
<td>14</td>
<td>156.3588</td>
<td>19.6653</td>
<td>1</td>
</tr>
</tbody>
</table>

4. Computation of Class Groups. For the computation of the class group $\text{Cl}_\mathcal{F}$ 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

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

and to find sufficiently many relations between those prime ideals. (We note that it suffices to choose $M_\mathcal{F} = \sqrt{D}/500 = 0.04472\sqrt{D}$ [8].) The relations are stored in a so-called class group matrix $\text{CGM} = (c_{i,j})$. 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 $p_1, \ldots, p_v$ viz.

$$p_j \mathcal{O} = \prod p_i^{c_{i,j}}.$$  

The exponent vectors $(c_{1,1}, \ldots, c_{v,j})$ form the first $w$ columns of the class group matrix $\text{CGM}$.  

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
3. Determine (at least v − w) additional elements β_{jΩ} satisfying β_{jΩ} = \prod p_i^{e_{i,j}} (j = v + 1, \ldots) 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\Ω generated by the prime number p ≤ M_Ω is obtained as follows. Assume that \Ω = \Ω(ζ) for a zero ζ of a monic irreducible polynomial f ∈ ℤ[t]. In case of p ⊗ (\Ω : ℤ[ζ]) we factorize the generating polynomial f modulo p^2t by Berlekamp’s method ([7]):

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

implying

\[ p\Ω = \prod_{i=1}^{m} p_i^{e_i} \]

with prime ideals

\[ p_i = p\Ω + f_i(ζ)\Ω \text{ of norm } N(p_i) = p^{\deg f_i}. \]

The case p | (\Ω : ℤ[ζ]) 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 β\Ω which can be completely factorized over the factor base P := \{p_1, \ldots, 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(Ω). By the inequality between geometric and arithmetic means, the norms of the corresponding algebraic integers β = b_1ω_1 + \cdots + b_4ω_4 satisfy

\[ |N(β)| \leq \frac{C^2}{16}. \]

If N(β) is a product of prime numbers p ≤ M_Ω, then β\Ω can be completely factorized over P. In order to find the maximum exponent k such that p^k | β\Ω for some prime ideal p = p\Ω + \α\Ω ∈ P, we must check whether p^k | β\Ω, i.e., β \in p^k = p^k\Ω + \α^k\Ω. We first compute the HNF-matrix of p^k. For this purpose, we note that p^kω_1, p^kω_4, α^kω_1, \ldots, α^kω_4 is a system of generators for p^k over ℤ. The HNF-matrix H of 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 $\beta \in p^k$ if and only if the system

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

has a solution $\vec{x} \in \mathcal{O}^4$. 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 $p_i$ whose power products are principal ideals. The determinant of CGM is a multiple of $h_{\mathcal{O}}$. 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), $h_{\mathcal{O}} \in \{1, q\}$. We only need to check whether $p$ itself is principal. In that case the class number is 1, otherwise we obtain $h_{\mathcal{O}} = q$ and $\text{Cl}_{\mathcal{O}} \cong C_q$.

2. CGM = $(4)$ (51 cases), $h_{\mathcal{O}} \in \{1, 2, 4\}$. The class number is

$$\begin{cases}
1 & \text{for } p \text{ principal} \\
2 & \text{p}^2 \text{ principal, } p \text{ not principal} \\
4 & \text{p}^2 \text{ not principal}
\end{cases}.$$

3. CGM = $(6)$ (1 case; $\mathcal{D} = 861025$), $h_{\mathcal{O}} \in \{1, 2, 3, 6\}$. Since neither $p^3$ nor $p^2$ are principal, the result is $h_{\mathcal{O}} = 6$, $\text{Cl}_{\mathcal{O}} \cong C_6$.

4. CGM = $(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix})$ (4 cases; $\mathcal{D} \in \{665856, 738000, 882000, 946125\}$). We know that $p_1^2 \in H_F$, $p_2^2 \in H_F$. First we check $p_2 \in H_F$. In all four cases the result is negative. Hence we check whether $p_1 p_2$ or $p_1$ are principal. In all cases both are not principal. Thus we have proved $\text{Cl}_{\mathcal{O}} \cong C_2 \times C_2$, $h_{\mathcal{O}} = 4$.

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 $\Gamma := \text{Gal}(\mathcal{F}/\mathbb{F})$:

<table>
<thead>
<tr>
<th>$\Gamma$</th>
<th>$h_{\mathcal{F}} = 1$</th>
<th>$h_{\mathcal{F}} = 2$</th>
<th>$h_{\mathcal{F}} = 3$</th>
<th>$h_{\mathcal{F}} = 4$</th>
<th>$h_{\mathcal{F}} = 5$</th>
<th>$h_{\mathcal{F}} = 6$</th>
<th>$\sum$</th>
</tr>
</thead>
<tbody>
<tr>
<td>D8</td>
<td>3822</td>
<td>582</td>
<td>45</td>
<td>34</td>
<td>2</td>
<td>1</td>
<td>4486</td>
</tr>
<tr>
<td>C4</td>
<td>35</td>
<td>22</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>59</td>
</tr>
<tr>
<td>V4</td>
<td>130</td>
<td>53</td>
<td>5</td>
<td>8</td>
<td>-</td>
<td>-</td>
<td>196</td>
</tr>
<tr>
<td>S4</td>
<td>7936</td>
<td>343</td>
<td>15</td>
<td>5</td>
<td>2</td>
<td>-</td>
<td>8301</td>
</tr>
<tr>
<td>A4</td>
<td>22</td>
<td>9</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>31</td>
</tr>
<tr>
<td>$\sum$</td>
<td>11945</td>
<td>1009</td>
<td>65</td>
<td>49</td>
<td>4</td>
<td>1</td>
<td>13073</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>$\Gamma$</th>
<th>$h_{\mathcal{F}} = 1$</th>
<th>$h_{\mathcal{F}} = 2$</th>
<th>$h_{\mathcal{F}} = 3$</th>
<th>$h_{\mathcal{F}} = 4$</th>
<th>$h_{\mathcal{F}} = 5$</th>
<th>$h_{\mathcal{F}} = 6$</th>
<th>$\sum$</th>
</tr>
</thead>
<tbody>
<tr>
<td>D8</td>
<td>85.20%</td>
<td>12.97%</td>
<td>1.00%</td>
<td>0.76%</td>
<td>0.04%</td>
<td>0.02%</td>
<td>34.32%</td>
</tr>
<tr>
<td>C4</td>
<td>59.32%</td>
<td>37.29%</td>
<td>-</td>
<td>3.39%</td>
<td>-</td>
<td>-</td>
<td>0.45%</td>
</tr>
<tr>
<td>V4</td>
<td>66.33%</td>
<td>27.04%</td>
<td>2.56%</td>
<td>4.08%</td>
<td>-</td>
<td>-</td>
<td>1.50%</td>
</tr>
<tr>
<td>S4</td>
<td>95.60%</td>
<td>4.13%</td>
<td>0.18%</td>
<td>0.06%</td>
<td>0.02%</td>
<td>-</td>
<td>63.50%</td>
</tr>
<tr>
<td>A4</td>
<td>70.97%</td>
<td>29.03%</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0.24%</td>
</tr>
<tr>
<td>$\sum$</td>
<td>91.37%</td>
<td>7.72%</td>
<td>0.50%</td>
<td>0.37%</td>
<td>0.03%</td>
<td>0.01%</td>
<td>100%</td>
</tr>
</tbody>
</table>

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 $\rho$ 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.
<table>
<thead>
<tr>
<th>( f )</th>
<th>( D )</th>
<th>integral basis</th>
<th>( \mathcal{H}_f )</th>
<th>( R )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(-1, -3, 1, 1)</td>
<td>725</td>
<td>(1, \rho, \rho^2, \rho^3)</td>
<td>(-1, 2, 1, -1)</td>
<td>0.8251</td>
</tr>
<tr>
<td>(-1, -4, 1, 1)</td>
<td>1125</td>
<td>(1, \rho, \rho^2, \rho^3)</td>
<td>(-1, 3, 0, -1)</td>
<td>1.1655</td>
</tr>
<tr>
<td>(0, -6, 0, 4)</td>
<td>1600</td>
<td>(1, \rho, \rho^2/2, \rho^3/2)</td>
<td>(1, 0, -1, 0)</td>
<td>1.5425</td>
</tr>
<tr>
<td>(0, -4, -1, 1)</td>
<td>1957</td>
<td>(1, \rho, \rho^2, \rho^3)</td>
<td>(0, -1, 0, 0)</td>
<td>1.9184</td>
</tr>
<tr>
<td>(-2, -23, 24, -1)</td>
<td>21025</td>
<td>(1, \rho, (1 + \rho + \rho^2)/2, (2 + \rho + 3\rho^2 + \rho^3)/18)</td>
<td>(1, -2, -1, 2)</td>
<td>5.0410</td>
</tr>
<tr>
<td>(-2, -7, 3, 8)</td>
<td>26569</td>
<td>(1, \rho, \rho^2, \rho^3)</td>
<td>(-1, -1, 0, 0)</td>
<td>15.7092</td>
</tr>
<tr>
<td>(-1, -24, 29, 31)</td>
<td>32625</td>
<td>(1, \rho, (1 + \rho + \rho^2)/3, (-1 + \rho^3)/18)</td>
<td>(-1, 1, 0, -1)</td>
<td>5.9428</td>
</tr>
<tr>
<td>(0, -24, -40, 14)</td>
<td>51200</td>
<td>(1, \rho, \rho^2, (-2\rho + \rho^2 + \rho^3)/7)</td>
<td>(-1, 4, 1, -2)</td>
<td>9.8280</td>
</tr>
<tr>
<td>(0, -9, -5, 9)</td>
<td>56025</td>
<td>(1, \rho, \rho^2, \rho^3)</td>
<td>(5, -5, -2, 1)</td>
<td>15.2956</td>
</tr>
<tr>
<td>(-1, -16, 3, 1)</td>
<td>76729</td>
<td>(1, \rho, \rho^2, (1 + 2\rho + 2\rho^2 + \rho^3)/4)</td>
<td>(0, -1, 0, 0)</td>
<td>12.7132</td>
</tr>
<tr>
<td>(-1, -37, -2, 164)</td>
<td>97025</td>
<td>(1, \rho, \rho^2, (26 + 13\rho + 35\rho^2 + \rho^3)/110)</td>
<td>(-1, -1, -1, 3)</td>
<td>8.2606</td>
</tr>
<tr>
<td>(-1, -11, 18, -1)</td>
<td>191769</td>
<td>(1, \rho, \rho^2, \rho^3)</td>
<td>(2, -1, 0, 0)</td>
<td>16.2576</td>
</tr>
<tr>
<td>(0, -18, 0, 16)</td>
<td>270400</td>
<td>(1, \rho, \rho^2/2, (2\rho + \rho^3)/4)</td>
<td>(-1, 5, 0, -1)</td>
<td>23.3504</td>
</tr>
<tr>
<td>(0, -20, -40, -15)</td>
<td>416000</td>
<td>(1, \rho, \rho^2, \rho^3)</td>
<td>(8, 16, 2, -1)</td>
<td>24.6795</td>
</tr>
<tr>
<td>(0, -29, 0, 36)</td>
<td>485809</td>
<td>(1, \rho, (p + \rho^2)/2, (6 + p + \rho^3)/12)</td>
<td>(-3, 4, 0, -2)</td>
<td>97.1575</td>
</tr>
<tr>
<td>(-1, -18, 44, -25)</td>
<td>556357</td>
<td>(1, \rho, \rho^2, \rho^3)</td>
<td>(1, -1, 0, 0)</td>
<td>13.0653</td>
</tr>
<tr>
<td>( f )</td>
<td>( \mathcal{D} )</td>
<td>integral basis</td>
<td>( \mathbb{Z}_f )</td>
<td>( R )</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>0, -52, 0, 625</td>
<td>665856</td>
<td>( 1, \rho, \rho^2, \frac{-2\rho + p^3}{25} )</td>
<td>-1, 1, 0, -1</td>
<td>21.5450</td>
</tr>
<tr>
<td>-2, -91, 152, 1681</td>
<td>738000</td>
<td>( 1, \rho, \rho^2, \frac{-13 + 8\rho - 11\rho^2 + p^3}{31} )</td>
<td>-13, -4, 1, 2</td>
<td>12.5293</td>
</tr>
<tr>
<td>-2, -24, -30, -8</td>
<td>761428</td>
<td>( 1, \rho, \rho^2, \rho^3 / 2 )</td>
<td>9, 21, -3, -2</td>
<td>33.9772</td>
</tr>
<tr>
<td>-2, -20, 21, 10</td>
<td>804005</td>
<td>( 1, \rho, \rho^2, \frac{1 + 2\rho + 2\rho^2 + \rho^3}{7} )</td>
<td>6, 10, 1, -3</td>
<td>47.1464</td>
</tr>
<tr>
<td>-2, -93, 94, 2129</td>
<td>861025</td>
<td>( 1, \rho, \frac{-3 - \rho + \rho^2}{8}, \frac{-3\rho - \rho^2 + \rho^3}{8} )</td>
<td>50, 1, -8, 1</td>
<td>15.1622</td>
</tr>
<tr>
<td>-2, -106, 212, 1996</td>
<td>882000</td>
<td>( 1, \rho, \rho^2 / 2, \frac{-42 + 52\rho + 9\rho^2 + \rho^3}{118} )</td>
<td>3, 1, 0, -1</td>
<td>15.7995</td>
</tr>
</tbody>
</table>

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