MATHEMATICS OF COMPUTATION
VOLUME 63, NUMBER 207
JULY 1994, PAGES 361-376

A TABLE OF QUINTIC NUMBER FIELDS

A. SCHWARZ, M. POHST, AND F. DIAZ Y DIAZ

ABSTRACT. All algebraic number fields F of degree 5 and absolute discriminant less than 2×10^7 (totally real fields), respectively 5×10^6 (other signatures) are determined. We describe the methods which we applied and list significant data.

1. INTRODUCTION

In the last few years several extensive lists of number fields were calculated. In particular, we mention the calculation of fourth-degree fields up to a discriminant bound of one million by D. Ford, J. Buchmann, and the second author [2, 3, 5]. The huge amount of computation time showed that similar tables for primitive fields in higher dimensions would require refined techniques. A first attack on the totally real quintic case was done by the third author about 2 years ago [4]. At the same time the determination of the minimum discriminant for totally real octic fields by Pohst, Martinet, and Diaz y Diaz [11] was successful because of much better estimates for several coefficients of a generating polynomial. In this paper we take up those ideas and apply them to fifth-degree polynomials of arbitrary signature.

In §2 we describe the generation of the polynomials and develop new estimates for their coefficients for each of the three possible signatures. In §3 we discuss the processing of those polynomials. Their discriminants are calculated integrally; bounds on the required number of arithmetical operations and on the size of the occurring integers are also given. At the same time polynomials of incorrect signature are removed. Then reducible polynomials are eliminated. All remaining ones are generating polynomials for number fields F. We compute an integral basis for F (hence, also the discriminant d_F of F) with the ROUND-2 algorithm of Zassenhaus [18]. Redundant fields (i.e., those which are isomorphic to a field which was already obtained) are removed with the help of the isomorphy test of [10]. Finally, the Galois group of F is computed with the resolvent method. In the last section we present various numerical data. We found a total of

- 22 740 totally real fields with discriminant less that 2×10^7,
- 79 394 fields with 2 complex conjugates and discriminant larger than -5×10^6,
- 186 906 fields with 4 complex conjugates and discriminant less than 5×10^6.

All data can be obtained from the second author.

Received by the editor June 25, 1992 and, in revised form, December 30, 1992.
1991 *Mathematics Subject Classification*. Primary 11Y40.

2. Generation of polynomials

Let F be an algebraic number field of degree n and discriminant d_F, and let $\mathscr{O}_F$ be the ring of integers of F. Let $F = \mathbb{Q}(\rho)$ for a root ρ of a monic irreducible polynomial $f_\rho(t) \in \mathbb{Z}[t]$ with $\deg(f_\rho) = n$. Then $f_\rho(t)$ is the characteristic polynomial of ρ, and we denote its zeros in $\mathbb{C}$ by $\rho = \rho^{(1)}, \ldots, \rho^{(n)}$. As usual, we choose $\rho^{(1)}, \ldots, \rho^{(r_1)} \in \mathbb{R}$ and $\rho^{(r_1+1)}, \ldots, \rho^{(r_1+r_2)} \in \mathbb{C}\backslash\mathbb{R}$ with $\rho^{(r_1+r_2+j)} = \overline{\rho^{(r_1+j)}}$ for $1 \le j \le r_2$, so that n equals $r_1 + 2r_2$. For any element $x \in F$, say $x = \sum_{i=1}^n q_i \rho^{i-1}$ $(q_i \in \mathbb{Q},\ 1 \le i \le n)$, the conjugates of x are given by $x^{(j)} := \sum_{i=1}^n q_i {\rho^{(j)}}^{i-1}$.

We introduce the function

$$\mathrm{T}_2 \colon F \to \mathbb{R}^{\ge 0} \colon x \mapsto \sum_{i=1}^{n} |x^{(i)}|^2.$$

With $x \in F$ represented by a fixed basis, $\mathrm{T}_2(x)$ becomes a positive definite quadratic form in the coefficients. Also, we need the kth power sum of x,

$$S_k \colon F^\times \to \mathbb{R} \colon x \mapsto \sum_{i=1}^{n} {x^{(i)}}^k \qquad (k \in \mathbb{Z}).$$

We note that for $x \in \mathscr{O}_F$ and $k \ge 0$ the kth power sum of x is a rational integer. Newton's relations

$$S_k + \sum_{i=1}^{k-1} a_i S_{k-i} + k a_k = 0 \qquad (1 \le k \le n)$$

allow us to calculate the power sums from the coefficients of the characteristic polynomial $f_x(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in \mathbb{Z}[t]$ of the algebraic integer $x \in F$, and vice versa. Hence, we can easily estimate the coefficients of $f_x(t)$ if we have bounds for the power sums of $x \in F$. Additionally, we note that

$$S_{-1} = (-1)^n \frac{a_{n-1}}{a_n}.$$

Improving methods in earlier publications, for example [2, 4, 6, 8, 9], we use all our information about the values of S_1, S_2 and a_n to determine good bounds for S_k $(k \in \{3, \ldots, n-1, -1\})$. Thus, the number of generated polynomials is reduced drastically. Without these improved bounds it would not be possible to compute such large sets of algebraic number fields in reasonable CPU-time.

In the sequel, $F = \mathbb{Q}(\rho)$ denotes an algebraic number field of degree five with prescribed signature (r_1, r_2). For an upper bound B on the absolute value of the discriminant of F we choose $B = 2 \times 10^7$ for $r_1 = 5$, and $B = 5 \times 10^6$ otherwise. For each of the three signatures we construct a set M of monic fifth-degree polynomials such that any quintic number field F of correct signature and of absolute discriminant $|d_F| \le B$ contains an integer ρ $(\in F\backslash\mathbb{Q})$ whose characteristic polynomial $f_\rho(t) = t^5 + a_1 t^4 + a_2 t^3 + a_3 t^2 + a_4 t + a_5 \in \mathbb{Z}[t]$ is contained in M. We proceed in analogy to [6, 9].

Proposition 2.1. *Let F be an algebraic number field of degree $n = 5$ with discriminant d_F, $|d_F| \le B$. Then there exists an algebraic integer ρ in F with*

$F = \mathbb{Q}(\rho)$ and characteristic polynomial $f_\rho(t)$ satisfying

$$a_1 \in \{0, 1, 2\}$$

and

$$\mathrm{T}_2(\rho) \leq U_2 := \frac{5}{4} + \left(\frac{4}{5}B\right)^{1/4}.$$

As a consequence, we also get bounds for the coefficients a_2, a_5 of the characteristic polynomial of that element ρ. Newton's relation $a_2 = (a_1^2 - S_2)/2$ immediately yields

$$a_2 \geq (a_1^2 - U_2)/2.$$

Applying the Cauchy-Schwarz inequality to the vectors $(\rho^{(1)}, \dots, \rho^{(n)})$, $(1, \dots, 1)$, we obtain $a_1^2 \leq 5(U_2 + S_2)/2$; hence,

$$a_2 \leq \left(U_2 + \frac{3}{5}a_1^2\right)/2.$$

The inequality between arithmetic and geometric means implies

$$1 \leq |a_5| = \left|\prod_{j=1}^{5} \rho^{(j)}\right| \leq \left(\frac{U_2}{5}\right)^{5/2}.$$

Remark 2.2. For totally real fields F, i.e., $r_1 = 5$, we have $\mathrm{T}_2(\rho) = S_2(\rho) \geq \frac{3}{2}n$ [15] and therefore much better upper bounds

$$a_2 \leq \frac{1}{2}a_1^2 - \frac{15}{4} \quad \text{and} \quad |a_5| \leq \left(\frac{S_2}{5}\right)^{5/2}.$$

Estimates for a_3, a_4 are derived from bounds for S_3, S_4, S_{-1}, and the latter are obtained by calculating global maxima and minima of the functions

$$S_k : \mathbb{C}^5 \to \mathbb{R} : \mathbf{x} \mapsto \sum_{i=1}^{n} x_i^k$$

for $k \in \{3, 4, -1\}$ and fixed values of S_1, S_2 and a_5 and under the additional constraint

$$\mathrm{T}_2(\mathbf{x}) := |x_1|^2 + \cdots + |x_5|^2 \leq U_2.$$

These extrema are determined by the Lagrange multiplier method.

In the sequel we assume that $S_1, S_2, a_5 \in \mathbb{Z}$ and $U_2 \in \mathbb{R}^{>0}$ are fixed.

2.1. **Polynomials with signature $r_1 = 5$ and $r_2 = 0$.** We determine extrema of the functions

$$S_k : \mathbb{R}^5 \to \mathbb{R} : \mathbf{x} \mapsto \sum_{i=1}^{n} x_i^k, \qquad k \in \{3, 4, -1\},$$

under the restrictions

$$\begin{aligned} g_1(\mathbf{x}) &= x_1 + x_2 + x_3 + x_4 + x_5 - S_1 = 0, \\ g_2(\mathbf{x}) &= x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 - S_2 = 0, \\ g_3(\mathbf{x}) &= x_1 x_2 x_3 x_4 x_5 + a_5 = 0. \end{aligned}$$

Because of $T_2(\mathbf{x}) = S_2(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{R}^5$, we do not need the side condition $T_2(\mathbf{x}) \le U_2$ in this case. The set $G := \{\mathbf{x} \in \mathbb{R}^5 | g_j(\mathbf{x}) = 0\,,\ j = 1\,,2\,,3\}$ is compact. Hence, S_k attains a maximum and a minimum in G for $k \in \{3\,,4\,,-1\}$. The following proposition is a consequence of Lagrange's multiplier method (see [13]).

Proposition 2.3. (a) *Each of the functions S_3 and S_{-1} has a global maximum and a global minimum on the set G at a vector $\mathbf{x} = (x_1\,, \dots\,, x_5)$ whose coordinates satisfy*

$$x_1 = x_2 = x_3 \quad or \quad x_1 = x_2 \wedge x_3 = x_4.$$

(b) *The function S_4 has a global maximum and a global minimum on the set G at a vector $\mathbf{x} = (x_1\,, \dots\,, x_5)$ whose coordinates satisfy*

$$x_1 = x_2 = x_3 \quad or \quad x_1 = x_2 \wedge x_3 = x_4$$

or, in case $S_1 \neq 0$,

$$x_1 = x_2 = S_1 \quad and \quad x_1\,, x_3\,, x_4\,, x_5 \text{ are pairwise distinct.}$$

We thus must consider three cases for which we calculate all $\mathbf{x} \in G$ subject to one of the conditions of the last proposition. We give a short example how to determine all vectors $\mathbf{x} \in G$ with $x_1 = x_2 = x_3$. Eliminating x_4 and x_5 from the system of equations

$$\begin{aligned} 3x_1 + x_4 + x_5 - S_1 &= 0\,, \\ 3x_1^2 + x_4^2 + x_5^2 - S_2 &= 0\,, \\ x_1^3 x_4 x_5 + a_5 &= 0\,, \end{aligned}$$

we get

$$x_1^5 - \frac{1}{2}S_1 x_1^4 + \frac{1}{12}(S_1^2 - S_2)x_1^3 + \frac{1}{6}a_5 = 0.$$

For every real solution x_1 of that equation we compute x_5 from

$$x_5^2 + (3x_1 - S_1)x_5 + 6x_1^2 - 3S_1 x_1 + \frac{1}{2}(S_1^2 - S_2) = 0$$

and, finally, x_4 from

$$x_4 = S_1 - 3x_1 - x_5.$$

For all solutions $\mathbf{x} \in G$ we compute $S_k(\mathbf{x})$ for $k \in \{3\,,4\,,-1\}$. In the other two cases we proceed analogously.

The required extrema are among the S_k-values for the finitely many $\mathbf{x} \in G$ obtained. All polynomials for x_1 are of degree at most five. Using the bounds for S_3 we can estimate a_3 by Newton's relations. The bounds for S_4 and S_{-1} yield estimates for a_4. Additional bounds from [6, 8] are used to possibly further reduce the ranges for a_3 and a_4.

2.2. **Polynomials with signature $r_1 = 3$ and $r_2 = 1$.** If we denote the real roots by $x_1\,, x_2\,, x_3$ and the complex roots by $x_4 \pm i x_5$ with $x_4\,, x_5 \in \mathbb{R}$, then we have to search for extrema of the real functions

$$\begin{aligned} S_3(\mathbf{x}) &:= x_1^3 + x_2^3 + x_3^3 + 2(x_4^3 - 3x_4 x_5^2)\,, \\ S_4(\mathbf{x}) &:= x_1^4 + x_2^4 + x_3^4 + 2(x_4^4 - 6x_4^2 x_5^2 + x_5^4)\,, \\ S_{-1}(\mathbf{x}) &:= \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + 2\frac{x_4}{x_4^2 + x_5^2}. \end{aligned}$$

The constraints are

$$g_1(\mathbf{x}) = x_1 + x_2 + x_3 + 2x_4 - S_1 = 0,$$
$$g_2(\mathbf{x}) = x_1^2 + x_2^2 + x_3^2 + 2(x_4^2 - x_5^2) - S_2 = 0,$$
$$g_3(\mathbf{x}) = x_1x_2x_3(x_4^2 + x_5^2) + a_5 = 0,$$
$$g_4(\mathbf{x}) = x_1^2 + x_2^2 + x_3^2 + 2(x_4^2 + x_5^2) - U_2 \leq 0.$$

We define sets

$$G := \{\mathbf{x} \in \mathbb{R}^5 | g_4(\mathbf{x}) \leq 0 \wedge g_j(\mathbf{x}) = 0,\ j = 1, 2, 3\},$$
$$G_3 := \{\mathbf{x} \in \mathbb{R}^5 | g_j(\mathbf{x}) = 0,\ j = 1, 2, 3\},$$
$$G_4 := \{\mathbf{x} \in \mathbb{R}^5 | g_j(\mathbf{x}) = 0,\ j = 1, 2, 3, 4\}.$$

Since G is compact, we have global extrema in G. If $\mathbf{x} \in \mathbb{R}^5$ is an extremum, then it is either an element of G_3 which satisfies $g_4(\mathbf{x}) < 0$, or it is an element of G_4. So we must determine all local extrema in G_3 and G_4. Again, we apply the method of Lagrange multipliers and obtain the following proposition ([13]).

Proposition 2.4. (a) *Each of the functions S_3 and S_{-1} has its local extrema in the set G_3 only at points $\mathbf{x} = (x_1, \dots, x_5)$ which satisfy one of the conditions*
(1) $x_1 = x_2 = x_3$,
(2) $x_1 = x_4 \wedge x_5 = 0$,
(3) $x_1 = x_2 \wedge x_5 = 0$.

(b) *The function S_4 has its local extrema in the set G_3 only at points $\mathbf{x} = (x_1, \dots, x_5)$ which satisfy either one of the conditions* (1)–(3) *of* (a) *or, in case $S_1 \neq 0$, one of the conditions*
(4) $x_1 = x_2 = S_1 \wedge x_1 \neq x_3 \wedge x_5 \neq 0$,
(5) $x_4 = S_1 \wedge x_5 = 0 \wedge x_1, x_2, x_3, x_4$ *pairwise distinct.*

There are only finitely many local extrema. The degree of the polynomials whose roots we must compute is at most five. We only consider solutions $\mathbf{x} \in \mathbb{R}^5$ with $g_4(\mathbf{x}) < 0$.

To determine the extrema in G_4 is somewhat more difficult, because we do not have similar conditions for the coordinates of a solution $\mathbf{x}$ as in the totally real case. Thus, it is necessary to calculate Lagrange multipliers explicitly, if the Jacobi matrix

$$J(\mathbf{x}) := \left(\frac{\partial g_j(\mathbf{x})}{\partial x_i}\right)_{1 \leq i \leq 5, 1 \leq j \leq 4}$$

has rank four. Because of $S_2 < U_2$, we have

$$0 \neq x_5^2 = \frac{1}{4}(U_2 - S_2)$$

in G_4.

Remark 2.5. If $x_5 \neq 0$ and x_1, x_2, x_3 are pairwise distinct, then the rank of $J(\mathbf{x})$ is four.

Hence, if $J(\mathbf{x})$ is not of maximal rank, then two of the coordinates x_1, x_2, x_3 must be equal, and without loss of generality we can assume $x_1 = x_2$. Computing resultants of the polynomials $g_j(x_1, x_1, x_3, x_4, \frac{1}{4}(U_2 - S_2))$ $(1 \leq j \leq 3)$, we obtain an equation of degree ten for x_4.

In the sequel we assume that $J(\mathbf{x})$ has rank four.

Determining the extrema of S_3 by the Lagrange multiplier method yields $\lambda_1, \dots, \lambda_4 \in \mathbb{R}$ subject to

$$\begin{aligned}
3x_1^2 + \lambda_1 + 2\lambda_2 x_1 - \lambda_3 \frac{a_5}{x_1} + 2\lambda_4 x_1 &= 0, \\
3x_2^2 + \lambda_1 + 2\lambda_2 x_2 - \lambda_3 \frac{a_5}{x_2} + 2\lambda_4 x_2 &= 0, \\
3x_3^2 + \lambda_1 + 2\lambda_2 x_3 - \lambda_3 \frac{a_5}{x_3} + 2\lambda_4 x_3 &= 0, \\
3(x_4^2 - x_5^2) + \lambda_1 + 2\lambda_2 x_4 - \lambda_3 x_4 \frac{a_5}{x_4^2 + x_5^2} + 2\lambda_4 x_4 &= 0, \\
-6x_4 - 2\lambda_2 - \lambda_3 \frac{a_5}{x_4^2 + x_5^2} + 2\lambda_4 &= 0.
\end{aligned}$$

Eliminating x_1, x_2, x_3, we obtain

$$\begin{aligned}
\lambda_3 &= -\frac{3}{x_4^2 + x_5^2}, \\
\lambda_4 &= 3x_4 - \frac{3}{4}\left(\frac{a_5}{(x_4^2 + x_5^2)^2} + S_1\right), \\
\lambda_2 &= -\lambda_4 - \frac{3}{2}(S_1 - 2x_4), \\
\lambda_1 &= \frac{3}{2}((S_1 - 2x_4)^2 - (S_2 - 2(x_4^2 - x_5^2))).
\end{aligned}$$

These results are inserted into the fourth equation above to obtain an equation of degree six in x_4. For the functions S_4 and S_{-1} we proceed similarly and get equations of degree seven in x_4 in each case.

Having calculated x_4, we form resultants of the polynomials

$$g_j(x_1, x_2, x_3, x_4, x_5), \qquad 1 \le j \le 3,$$

in the variables x_1 and x_2. This yields an equation of degree three for x_3.

2.3. **Polynomials with signature** $r_1 = 1$ **and** $r_2 = 2$. We apply the same method as before. We denote the zeros of a generating polynomial by $x_1, x_2 \pm ix_3, x_4 \pm ix_5$. Hence, we need to determine maxima and minima of the functions

$$\begin{aligned}
S_3(\mathbf{x}) &:= x_1^3 + 2(x_2^3 - 3x_2x_3^2) + 2(x_4^3 - 3x_4x_5^2), \\
S_4(\mathbf{x}) &:= x_1^4 + 2(x_2^4 - 6x_2^2x_3^2 + x_3^4) + 2(x_4^4 - 6x_4^2x_5^2 + x_5^4), \\
S_{-1}(\mathbf{x}) &:= \frac{1}{x_1} + 2\frac{x_2}{x_2^2 + x_3^2} + 2\frac{x_4}{x_4^2 + x_5^2}
\end{aligned}$$

subject to the restrictions

$$\begin{aligned}
g_1(\mathbf{x}) &:= x_1 + 2x_2 + 2x_4 - S_1 = 0, \\
g_2(\mathbf{x}) &:= x_1^2 + 2(x_2^2 - x_3^2) + 2(x_4^2 - x_5^2) - S_2 = 0, \\
g_3(\mathbf{x}) &:= x_1(x_2^2 + x_3^2)(x_4^2 + x_5^2) + a_5 = 0, \\
g_4(\mathbf{x}) &:= x_1^2 + 2(x_2^2 + x_3^2) + 2(x_4^2 + x_5^2) - U_2 \le 0.
\end{aligned}$$

Let the sets G, G_3, and G_4 be defined as in the preceding case. For the extrema in G_3 we get the following result (see [13]).

Proposition 2.6. (a) *Each of the functions* S_3 *and* S_{-1} *has its local extrema in the set* G_3 *only at points* $\mathbf{x} = (x_1, \dots, x_5)$ *which satisfy one of the conditions*

(1) $x_3 = x_5 = 0$,

(2) $x_1 = x_2 \wedge x_3 = 0$,

(3) $x_2 = x_4 \wedge x_3 = x_5$.

(b) *The function* S_4 *has its local extrema in the set* G_3 *only at points* $\mathbf{x} = (x_1, \dots, x_5)$ *which satisfy either one of the conditions* (1)–(3) *of* (a) *or, in case* $S_1 \neq 0$, *the condition*

(4) $x_1 \neq x_2 = S_1 \wedge x_3 = 0 \wedge x_5 \neq 0$.

Again we obtain only finitely many local extrema. Solving the corresponding system of equations we must calculate the zeros of polynomials of degree at most five.

For finding the global extrema in G_4 we have to check if the Jacobi matrix has rank four. For this, the following remark is helpful.

Remark 2.7. For $x_2 \neq x_4$, $x_2^2 + x_3^2 \neq x_4^2 + x_5^2$ and $x_3 \neq 0 \neq x_5$, the rank of the Jacobi matrix is four.

The cases $x_2 = x_4$ or $x_2^2 + x_3^2 = x_4^2 + x_5^2$ or $x_3 = 0$ are not difficult to handle. We notice that x_3 and x_5 cannot both be zero. If the rank of the Jacobi matrix is four, then we compute the Lagrange multipliers as functions of x_1 and obtain a polynomial equation for x_1. We note that in this case the degree can become as large as 17.

3. Processing of generated polynomials

Since the set M of polynomials generated by the ideas of the preceding section turns out to be quite large for each signature (see §4), the methods of this section should be really fast. In a first step we compute the discriminant and the signature of each polynomial simultaneously. For a monic nth-degree polynomial $f(t) \in \mathbb{Z}[t]$ we define the quadratic form

$$q_f(x_1, \dots, x_n) := \sum_{1 \le i, j \le n} S_{i+j-2} x_i x_j = \mathbf{x}^{\mathrm{tr}} Q_f \mathbf{x}$$

with coefficient matrix

$$Q_f = \begin{pmatrix} S_0 & S_1 & S_2 & \cdots & S_{n-1} \\ S_1 & S_2 & & & \vdots \\ S_2 & & & & \vdots \\ \vdots & & & & \vdots \\ S_{n-1} & \dots & \dots & \dots & S_{2n-2} \end{pmatrix},$$

i.e., the coefficients are the power sums of the zeros of $f(t)$. We note that $\det(Q_f)$ is the discriminant of $f(t)$ and that the number of real roots of $f(t)$ equals the difference of the numbers of positive and negative eigenvalues of Q_f [7]. The latter are easily computable by an application of the following lemma from [13].

Lemma 3.1. *Let* M *be a real symmetric* $n \times n$*-matrix, and* $\det(M_i) \neq 0$ *for* $M_i := (m_{jk})_{1 \le j, k \le i}$ $(1 \le i \le n)$. *Then the number of negative eigenvalues of* M *is equal to the number of sign changes in the sequence* $1, \det(M_1), \dots, \det(M_n)$.

We remark that in our case $\det(Q_f) \neq 0$, because otherwise we can discard $f(t)$ immediately, and therefore we can always achieve that the principal minors of Q_f are not zero. Hence, using a Cholesky-type method [9] for evaluating the determinant of Q_f, we obtain the signature of $f(t)$ at the same time for free. The following proposition from [13] allows us to do all calculations with rational integers. The advantage of operating exclusively with integers was already discussed in [1].

Proposition 3.2. *Let $M = (m_{ij}^{(0)})_{1\le i,j\le n}$ be a real symmetric $n \times n$-matrix with $\det(M) \neq 0$, and let $q(\mathbf{x}) := \sum_{i,j=1}^{n} m_{ij}^{(0)} x_i x_j$ be the corresponding quadratic form. Then for each $k \in \{0, \dots, n-1\}$ the form $q(\mathbf{x})$ is equivalent to the quadratic form*

$$\sum_{i=1}^{k} \frac{m_{ii}^{(k)}}{m_{i-1,i-1}^{(k)}} x_i^2 + \frac{1}{m_{kk}^{(k)}} \sum_{i,j=k+1}^{n} m_{ij}^{(k)} x_i x_j ,$$

defining $m_{00}^{(0)} := 1$ and

$$m_{ij}^{(k)} := \frac{m_{ij}^{(k-1)} m_{kk}^{(k-1)} - m_{ki}^{(k-1)} m_{kj}^{(k-1)}}{m_{k-1,k-1}^{(k-1)}}$$

for $k > 0$ and $k < i, j \le n$. If we have $M \in \mathbb{Z}^{n\times n}$, then also

$$m_{ij}^{(k)} \in \mathbb{Z} \quad \text{for } 0 \le k \le n-1, \ k < i, j \le n.$$

We remark that the principal minors of M satisfy

$$\det(M_k) = m_{kk}^{(k-1)} = m_{kk}^{(k)} \qquad (1 \le k \le n).$$

The following algorithm is immediate.

Algorithm 3.3. (Computation of polynomial discriminant and signature)
Input. Degree n of the polynomial f and the polynomial coefficients.
Output. Polynomial discriminant $D(f)$ and the number of real roots of f in case $D(f) \neq 0$.

(1) (Initialization)
Compute the power sums S_k for $0 \le k \le 2n-2$ via Newton's relations and initialize the Hankel matrix $Q_f = (m_{ij})_{1\le i,j\le n} \leftarrow (S_{i+j-2})_{1\le i,j\le n}$.
Set $s \leftarrow 0$ and $d \leftarrow 1$.

(2) For $k = 1$ to $n-1$ do
If $m_{kk} = 0$ then
If there is an index l with $k < l \le n$ and $m_{ll} \neq 0$, then
interchange m_{ki} and m_{li} for $k \le i \le n$ and then
interchange m_{ik} and m_{il} for $k \le i \le n$.
Else if $m_{ii} = 0$ for all i $(k \le i \le n)$ and there is an index l with $k < l \le n$ and $m_{kl} \neq 0$ then
set $m_{ki} \leftarrow m_{ki} + m_{li}$ for $k \le i \le n$ and then
set $m_{ik} \leftarrow m_{ik} + m_{il}$ for $k \le i \le n$.
Else
set $D(f) \leftarrow 0$ and terminate.
For $i = k+1$ to n do
Set $m_{ij} \leftarrow (m_{kk} m_{ij} - m_{ik} m_{kj})/d$ for $i \le j \le n$.

Set $m_{ki} \leftarrow 0$ for $k+1 \le i \le n$.
Set $m_{ji} \leftarrow m_{ij}$ for $k \le i \le n-1$ and $i+1 \le j \le n$.
Set $s \leftarrow s + \operatorname{sign}(m_{kk}) \cdot \operatorname{sign}(d)$ and $d \leftarrow m_{kk}$.
(3) Set $D(f) \leftarrow m_{nn}$, $s \leftarrow s + \operatorname{sign}(m_{nn}) \cdot \operatorname{sign}(d)$ and terminate.

Regarding the complexity of the algorithm we get (see [13]):

Proposition 3.4. *Let* $f(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in \mathbb{Z}[t]$ *be a polynomial of degree* $n \ge 2$ *and define* $a := \max(\{|a_i| \mid 1 \le i \le n\} \cup \{1\})$. *Then*
(a) *Algorithm* 3.3 *requires at most*

$$4(n-1)^2 + 2n(n-1) + \tfrac{2}{3}n(n-1)(n+1) + 2 = O(n^3)$$

arithmetical operations.
(b) *The absolute values of the intervening integers are bounded by*

$$2^{3(n-1)}(a+1)^{4(n-1)^2}.$$

This method of computing the polynomial discriminant and the signature simultaneously is very fast in practice. Comparisons with the PARI system showed that for our polynomials, Algorithm 3.3 is about ten times faster.

After the calculation of all polynomials of the signature under consideration we must check them for irreducibility. Factoring them modulo small prime numbers and comparing the degrees of potential factors often proves irreducibility in a fast way. If proper factors can still exist, we easily obtain estimates for their coefficients and test all remaining candidates.

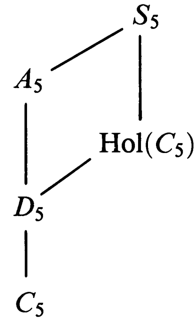
The irreducible polynomials then generate fields of correct signature. Next we must check whether the field discriminant lies within the given bounds. We use the Dedekind criterion (see [12], for example) to detect index divisors. If there are none, then we know that the equation order is maximal and the discriminant of the polynomial coincides with the field discriminant. In the remaining cases we compute an integral basis of the corresponding maximal order by a specialized version of the ROUND-2 algorithm of Zassenhaus [18].

Our methods sometimes yield several generating polynomials for one field. Hence, a final task is to reject all redundant ones. An easy test to check whether several polynomials generate isomorphic fields is given in [10].

3.1. **Computation of Galois groups.** As a prerequisite we list all transitive subgroups of the symmetric group S_5, and for each of them the frequency of cycle distributions. For example, " $15 \times (2, 2, 1)$ " means that the group contains 15 elements which decompose into two cycles of length two and one cycle of length one.

S_5	$1 \times (1,1,1,1,1)$, $10 \times (2,1,1,1)$, $15 \times (2,2,1)$, $20 \times (3,1,1)$, $20 \times (3,2)$, $30 \times (4,1)$, $24 \times (5)$
$\mathrm{Hol}(C_5)$	$1 \times (1,1,1,1,1)$, $5 \times (2,2,1)$, $10 \times (4,1)$, $4 \times (5)$
A_5	$1 \times (1,1,1,1,1)$, $15 \times (2,2,1)$, $20 \times (3,1,1)$, $24 \times (5)$
D_5	$1 \times (1,1,1,1,1)$, $5 \times (2,2,1)$, $4 \times (5)$
C_5	$1 \times (1,1,1,1,1)$, $4 \times (5)$

The groups include each other in the following way:



To decide which subgroup of S_5 is the Galois group of a given monic irreducible polynomial $f(t) \in \mathbb{Z}[t]$, we use the following criteria which are contained in (or easily deducible from) [17, pp. 202–204].

Lemma 3.5. *Let $f(t) \in \mathbb{Z}[t]$ be a monic irreducible polynomial of degree n, and let $\Gamma_f \subseteq S_n$ be the Galois group of f. Let p be a prime number not dividing the discriminant of f, and let $f \equiv f_1 \cdots f_r \bmod p$ be a congruence factorization into monic irreducible polynomials. Then Γ_f contains an element $\pi = \pi_1 \cdots \pi_r$, where the π_j are disjoint cycles of length $\deg(f_j)$ $(1 \le j \le r)$.*

Lemma 3.6. *Let $f(t)$ be as in the preceding lemma. If Γ_f contains cycles of length 2 and $\deg(f)$, respectively, then Γ_f is the symmetric group S_n.*

Lemma 3.7. *Let $f(t)$ be as in Lemma 3.5 but of prime degree $p \ge 3$. If f has exactly two nonreal roots, then its Galois group Γ_f is the symmetric group S_p.*

Lemma 3.8. *Let $f(t)$ be as in Lemma 3.5. Then its Galois group Γ_f is contained in the alternating group A_n if and only if the discriminant of f is a square in $\mathbb{Z}$.*

Lemma 3.9. *Let $f(t)$ be as in Lemma 3.5 but of degree $n = 5$. If its Galois group Γ_f is the cyclic group C_5, then f has five real roots.*

Hence, we decompose a given monic irreducible polynomial $f(t)$ modulo $p\mathbb{Z}[t]$ into its prime factors for a few (usually not more than 10) small prime numbers p. From these results we can already guess the corresponding Galois group in most cases. For the remaining ones we use indicator functions (see [12, 16]) which tell us whether Γ_f is contained in $\mathrm{Hol}(C_5)$, C_5, respectively. Let

$$g_1(x_1, \dots, x_5) := (x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1)^2$$

and V_1 be a full set of representatives of $S_5/\mathrm{Hol}(C_5)$, for example,

$$V_1 = \{(1), (12435), (15243), (12453), (12543), (12)(34)\}.$$

Assume that the values $g_1(x_{\tau(1)}, \dots, x_{\tau(5)})$ are distinct for $\tau \in V_1$. Then the Galois group Γ_f is contained in $\mathrm{Hol}(C_5)$ if and only if $y = g_1(x_{\pi(1)}, \dots, x_{\pi(5)})$ is a rational integer for some $\pi \in V_1$.

Similarly, we define

$$g_2(x_1, \dots, x_5) := x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_5^2 + x_5x_1^2$$

and

$$V_2 := \{(1), (12)(35)\}.$$

Assume that the values $g_2(x_{\tau(1)}, \dots, x_{\tau(5)})$ are distinct for $\tau \in V_2$. Then the Galois group Γ_f is contained in (hence equal to) C_5 if and only if $y = g_2(x_{\pi(1)}, \dots, x_{\pi(5)})$ is a rational integer for some $\pi \in V_2$.

4. Numerical results

All computations were carried out on Apollo workstations (CPU Motorola 68020, 68030, 68040). The use of the software package KANT [14] was absolutely essential.

4.1. **Totally real fields with** $d_F \leq 20\,000\,000$. According to Proposition 2.1, we have to compute all characteristic polynomials of algebraic integers ρ with $T_2(\rho) \leq 64.50$. Our method generates 110 476 592 polynomials, 35 758 669 of which are totally real. There remain 22 740 nonisomorphic fields. In Table 1 we list the first 50 field discriminants and the coefficients of a corresponding generating polynomial in each case. An integral basis is always a power basis for these generators.

Next, in Table 2 (next page), we consider the distribution of the fields with respect to their Galois group. Among all 22 740 fields, 22 676 have symmetric Galois group S_5 (99.72%). We list the remaining 64 fields.

TABLE 1

No	d_F	f					No	d_F	f				
1	14641	1	−4	−3	3	1	26	170701	1	−6	0	4	−1
2	24217	0	−5	1	3	−1	27	173513	2	−5	−3	3	1
3	36497	0	−6	1	4	1	28	176281	1	−5	−3	4	1
4	38569	0	−5	0	4	1	29	176684	0	−6	1	5	1
5	65657	1	−7	−1	4	−1	30	179024	0	−8	0	6	2
6	70601	1	−5	−2	3	1	31	180769	0	−7	4	2	−1
7	81509	0	−6	1	5	−2	32	181057	1	−7	−2	3	1
8	81589	0	−8	4	2	−1	33	186037	1	−6	−2	5	2
9	89417	2	−7	−4	2	1	34	195829	2	−5	−6	7	−1
10	101833	1	−5	−5	2	1	35	202817	2	−5	−4	2	1
11	106069	2	−7	−2	3	1	36	205225	1	−6	−3	7	3
12	117688	1	−5	−4	4	1	37	207184	1	−6	−2	7	1
13	122821	2	−4	−4	3	1	38	210557	1	−6	−4	8	1
14	124817	0	−7	6	2	−1	39	216637	0	−7	2	3	−1
15	126032	0	−6	0	6	2	40	218524	2	−4	−5	3	1
16	135076	2	−7	−1	4	−1	41	220036	2	−11	5	2	−1
17	138136	1	−6	−3	4	2	42	220669	1	−7	−5	3	2
18	138917	0	−6	2	3	−1	43	223824	1	−8	2	3	−1
19	144209	0	−6	1	6	1	44	223952	0	−6	2	6	−2
20	147109	2	−4	−5	3	2	45	224773	1	−6	−2	7	−2
21	149169	0	−6	3	4	−1	46	230224	2	−4	−6	3	2
22	153424	1	−6	−2	3	1	47	233489	1	−6	−1	5	1
23	157457	2	−4	−5	4	1	48	236549	1	−6	−7	2	1
24	160801	1	−5	−4	3	1	49	240133	2	−6	−4	2	1
25	161121	1	−6	−3	5	−1	50	240881	1	−7	−6	7	−1

TABLE 2

Galois group $\mathrm{Hol}(C_5)$

No	d_F	f					No	d_F	f				
1	2382032	0	−9	4	17	−12	9	11122069	2	−12	−24	8	23
2	2450000	0	−10	0	20	10	10	11250000	0	−20	0	80	16
3	3698000	1	−8	−6	13	9	11	15051125	1	−13	−1	23	9
4	6725897	1	−8	−3	13	−3	12	16200000	0	−15	0	45	30
5	6889792	1	−11	−9	1	1	13	19120976	1	−14	−6	3	1
6	6903125	0	−10	0	20	9	14	19503125	0	−10	0	20	7
7	7129088	1	−12	−4	18	2	15	19827925	1	−24	−56	29	104
8	8804429	2	−18	22	−2	−3							

Galois group A_5

No	d_F	f					No	d_F	f				
1	3104644	1	−11	−1	12	4	10	11812969	0	−25	11	7	−1
2	5184729	2	−7	−11	11	11	11	12271009	2	−10	−9	9	−1
3	6160324	1	−15	15	6	−4	12	13060996	1	−21	−48	−2	38
4	6180196	2	−15	−12	2	2	13	14584761	2	−13	−2	34	−19
5	7017201	0	−17	30	−4	−7	14	15784729	2	−9	−13	13	7
6	7409284	2	−19	17	22	−25	15	16386304	2	−22	−40	57	−2
7	8305924	1	−9	−8	8	4	16	16662724	1	−17	−13	52	52
8	10791225	1	−14	1	49	−41	17	18088009	2	−10	−23	−6	4
9	11744329	2	−15	−31	6	5	18	19096900	2	−21	−35	6	9

Galois group D_5

No	d_F	f					No	d_F	f				
1	160801	1	−5	−4	3	1	14	9790641	1	−11	0	21	−9
2	667489	1	−6	−5	3	1	15	10118761	2	−11	−15	22	17
3	1194649	0	−8	3	10	−4	16	10582009	1	−15	13	13	−11
4	1940449	1	−7	−6	3	1	17	12852225	1	−28	17	21	−9
5	2042041	2	−12	−3	12	4	18	12967201	2	−17	7	13	1
6	2692881	1	−10	−1	21	−9	19	15429184	1	−28	32	27	−1
7	3083536	2	−10	−14	21	16	20	15976009	1	−15	9	21	−7
8	3598609	1	−13	−8	27	−1	21	16785409	1	−17	−41	−18	9
9	3984016	0	−9	4	10	−4	22	18671041	1	−10	−9	3	1
10	4330561	2	−11	−28	−6	9	23	18948609	1	−23	−15	120	−9
11	4635409	1	−8	−7	3	1	24	18983449	0	−19	32	9	−28
12	8456464	2	−15	−4	36	−16	25	19722481	1	−23	19	14	1
13	9740641	1	−9	−8	3	1	26	19749136	1	−25	29	24	2

Galois group C_5

No	d_F	f				
1	14641	1	−4	−3	3	1
2	390625	0	−10	5	10	1
3	923521	1	−12	−21	1	5
4	2825761	1	−16	5	21	−9
5	13845841	1	−24	−17	41	−13

There are 61 discriminants below 20 000 000 belonging to two nonisomorphic fields, namely,

1810969	7333232	11790544	13520196	14600416	17946025	18908613
1891377	7834576	12055149	13898797	14731145	17946064	19303645
3060944	8760289	12096169	14009328	15873344	18038480	19444016
3350673	9262117	12174592	14118473	15910101	18371721	19595088
4569808	9344997	12329168	14186448	16209381	18536121	19630237
4602229	10782801	12500560	14282192	16509232	18623952	19720013
4641232	10796517	12965184	14313136	16959193	18640592	19984208
6470593	11022656	13072837	14321232	17362512	18652329	
6499197	11160412	13075749	14433201	17515184	18871504	

All other fields are uniquely determined by their discriminant.

4.2. **Fields with signature $r_1 = 3$ and $r_2 = 1$ and $|d_F| \leq 5\,000\,000$.** Applying Proposition 2.1, we compute all characteristic polynomials of algebraic integers ρ with $T_2(\rho) \leq 45.98$. We get 502 250 482 polynomials, 248 231 495 of which are of correct signature. There remain 79 394 nonisomorphic fields with a discriminant of absolute value below 5 000 000. All of them have Galois group S_5 according to Lemma 3.7.

In Table 3 we list the first 50 fields, each of which has a power integral basis.

TABLE 3

No	d_F	f					No	d_F	f				
1	−4511	0	−2	1	0	−1	26	−15919	0	−3	2	0	−1
2	−4903	1	−2	1	1	−1	27	−16816	1	4	0	−3	−1
3	−5519	0	−3	1	1	−1	28	−17151	0	−1	0	−2	1
4	−5783	1	−3	1	2	−1	29	−17348	1	−2	1	2	−2
5	−7031	0	−1	1	−1	−1	30	−18063	1	−2	−1	−1	−1
6	−7367	0	−4	1	2	−1	31	−18463	0	−3	2	2	−3
7	−7463	2	0	−1	−2	−1	32	−18583	1	−2	−1	−1	1
8	−8519	1	−1	0	−1	−1	33	−18839	1	−3	0	1	−1
9	−8647	2	−1	0	−2	1	34	−19015	0	−2	1	−2	1
10	−9439	1	−1	−1	−2	−1	35	−19951	1	1	3	−4	1
11	−9759	2	−1	0	2	−1	36	−21191	1	0	1	−3	1
12	−10407	1	−3	0	3	1	37	−21227	1	0	4	3	−2
13	−11119	2	1	−1	−3	−1	38	−22331	1	−4	0	2	−1
14	−11243	1	0	0	−2	−1	39	−22424	0	−2	1	−1	−1
15	−11551	1	−3	2	1	−1	40	−22448	1	−2	2	1	−1
16	−12447	0	1	1	−3	1	41	−22583	0	0	1	−2	−1
17	−13219	0	0	2	−1	−1	42	−22687	1	1	1	−2	−1
18	−13523	2	−3	0	3	1	43	−22935	0	−1	5	3	−3
19	−13799	1	−1	−2	−3	−1	44	−23103	1	0	−1	−3	−1
20	−13883	1	−2	0	1	−2	45	−23119	0	−3	0	0	1
21	−14103	2	−1	−2	−2	−1	46	−23339	1	0	−2	−2	1
22	−14631	1	−1	1	0	−3	47	−23679	2	0	−1	−2	−3
23	−14891	2	−1	0	3	−1	48	−23831	0	−3	2	4	1
24	−14911	1	−2	1	3	−1	49	−23891	1	−3	1	3	−2
25	−15536	2	0	0	0	−2	50	−24299	1	−1	−3	−1	2

There are various discriminants for which nonisomorphic fields exist. Table 4 gives a short account on this phenomenon. If there are more than 10 different discriminants for which μ nonisomorphic fields of that discriminant occur (which happens to be the case for $\mu = 2, 3$), we only list the 10 largest discriminants.

TABLE 4

number of nonisomorphic fields	2	3	4	6
discriminants	−28976	−428976	−2025648	−1673136
	−100656	−447232	−2170800	
	−107467	−490288	−2711232	
	−112919	−643127	−3223600	
	−125391	−646704	−3539376	
	−159196	−818096	−3830976	
	−171184	−853456	−3912624	
	−174608	−956623		
	−195203	−1051056		
	−210352	−1068336		
total	2139	106	7	1

TABLE 5

No	d_F	f					No	d_F	f				
1	1609	0	−1	1	1	−1	26	4897	0	1	1	−1	−1
2	1649	1	−1	0	1	−1	27	5025	1	−1	0	−1	1
3	1777	0	−2	1	2	−1	28	5164	1	−1	0	2	−1
4	2209	0	−1	2	−2	1	29	5437	2	0	−1	−1	−2
5	2297	0	1	1	1	1	30	5501	0	0	2	3	1
6	2617	0	1	2	0	1	31	5584	1	0	0	1	−1
7	2665	0	1	0	−2	1	32	5653	1	0	0	2	1
8	2869	0	0	0	−1	1	33	5753	1	−1	−2	−1	−1
9	3017	0	−1	0	0	1	34	5864	1	1	−2	−2	−1
10	3089	0	−1	0	2	1	35	5913	1	−1	2	−1	1
11	3233	0	0	1	0	1	36	6241	1	1	2	3	1
12	3369	0	1	1	−1	1	37	6449	0	3	1	1	1
13	3857	0	−1	1	−1	1	38	6581	0	0	2	0	1
14	3889	1	0	1	1	1	39	6757	1	0	−3	−2	−1
15	4169	0	2	1	2	1	40	6793	1	0	1	−1	1
16	4261	0	0	2	−2	1	41	7096	0	0	1	1	−1
17	4409	1	−1	0	1	1	42	7177	1	0	3	1	−3
18	4417	0	1	2	2	1	43	7265	1	1	−2	−1	−1
19	4429	0	−1	2	−1	1	44	7333	2	0	−4	−3	−1
20	4432	1	0	−2	−1	−1	45	7373	1	−2	0	2	1
21	4477	0	1	0	1	1	46	7376	1	−2	0	3	−1
22	4549	0	2	2	1	1	47	7672	1	1	0	−2	1
23	4597	0	1	2	−1	1	48	7684	0	−1	1	0	1
24	4757	1	2	1	2	1	49	7717	2	0	0	2	−1
25	4817	2	1	2	2	1	50	7909	1	−2	2	−2	1

4.3. **Fields with signature $r_1 = 1$ and $r_2 = 2$ and $d_F \leq 5\,000\,000$.** We compute all characteristic polynomials of algebraic integers ρ with $T_2(\rho) \leq 45.98$. This yields $670\,725\,968$ polynomials, $534\,326\,207$ of which have exactly one real zero. There remain $186\,906$ nonisomorphic fields of a discriminant below $5\,000\,000$. We list in Table 5 the smallest 50 fields, all of them with a power basis as integral basis.

There are 81 fields with Galois group $\mathrm{Hol}(C_5)$, 258 fields with A_5, and 129 fields with D_5. The group C_5 cannot occur as Galois group. For every possible Galois group we present the field of smallest discriminant. In each case an integral basis is a power basis.

Group	d_F	f				
S_5	1609	0	−1	1	1	−1
Hol(C_5)	35152	1	2	4	1	1
A_5	18496	1	0	−2	−2	−2
D_5	2209	0	−1	2	−2	1

Table 6 gives some information on discriminant values for which nonisomorphic fields occur. If there are more than 10 different discriminants for a fixed number of nonisomorphic fields, only the 10 smallest discriminants are listed.

TABLE 6

number of nonisomorphic fields	2	3	4	5	6	7	9
discriminants	16757	17744	225872	721872	1672272	2432592	4050000
	20432	48592	258768	1153872	2016576	4081104	
	34129	206928	514512	1333584	2059344		
	37584	213840	587088	1350864	2245968		
	37892	214272	640629	1664976	2546640		
	40912	216432	752976	1710288	3089664		
	45009	223737	880848	1862352	3707856		
	47797	251984	939600	2348496	4482000		
	48629	254148	1048896	2415312			
	49744	255312	1057104	2592000			
total	9333	756	103	29	8	2	1

BIBLIOGRAPHY

1. E. H. Bareiss, *Sylvester's identity and multistep integer preserving Gaussian elimination*, Math. Comp. **22** (1968), 565–578.
2. J. Buchmann and D. J. Ford, *On the computation of totally real quartic fields of small discriminant*, Math. Comp. **52** (1989), 161–174.
3. J. Buchmann, D. Ford, and M. Pohst, *Enumeration of quartic fields of small discriminant*, Math. Comp. **61** (1993), 873–879.
4. F. Diaz y Diaz, *A table of totally real quintic number fields*, Math. Comp. **56** (1991), 801–808.
5. D. Ford, *Enumeration of totally complex quartic fields of small discriminant*, Computational Number Theory, Proc. Colloq. on Comp. Number Theory (Debrecen, Hungary, 1989) (A. Pethö, M. E. Pohst, H. C. Williams, and H. G. Zimmer, eds.), de Gruyter, Berlin and New York, 1991, pp. 129–138.
6. J. Hunter, *The minimum discriminant of quintic fields*, Proc. Glasgow Math. Assoc. **3** (1957), 57–67.
7. N. Obreschkoff, *Verteilung und Berechnung der Nullstellen reeller Polynome*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1963.
8. M. Pohst, *Berechnung kleiner Diskriminanten total reeller algebraischer Zahlkörper*, J. Reine Angew. Math. **278/279** (1975), 278–300.
9. ——, *On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields*, J. Number Theory **14** (1982), 99–117.
10. ——, *On computing isomorphisms of equation orders*, Math. Comp. **48** (1987), 309–314.
11. M. Pohst, J. Martinet, and F. Diaz y Diaz, *The minimum discriminant of totally real octic fields*, J. Number Theory **36** (1991), 145–159.

12. M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge Univ. Press, Cambridge, 1989.

13. A. Schwarz, *Berechnung von Zahlkörpen fünften Grades mit kleiner Diskriminante*, Diplomarbeit, Heinrich-Heine-Universität Düsseldorf, 1991.

14. J. Graf von Schmettow, *KANT–a tool for computations in algebraic number fields*, Computational Number Theory (A. Pethö, M. E. Pohst, H. C. Williams, and H. G. Zimmer, eds.), de Gruyter, Berlin and New York, 1991, pp. 321–330.

15. C. L. Siegel, *The trace of totally positive and real algebraic integers*, Ann. of Math. (2) **46** (1945), 302–312.

16. R. P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996.

17. B. L. van der Waerden, *Algebra*. I, 8th ed., Heidelberger Taschenbücher 12, Springer-Verlag, Berlin, Heidelberg, New York, 1971.

18. H. Zassenhaus, *On the second round of the maximal order program*, Applications of Number Theory to Numerical Analysis, Academic Press, New York, 1972, pp. 398–431.

ITTERSTR. 107, 40589 DÜSSELDORF, GERMANY

FACHBEREICH 3 MATHEMATIK, TU BERLIN, STRASSE DES 17. JUNI 136, 10623 BERLIN, GERMANY

MATHÉMATIQUES ET INFORMATIQUE, UNIVERSITÉ DE BORDEAUX I, 351, COURS DE LA LIBÉRATION, F-33405 TALENCE CEDEX, FRANCE