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 $2 \times 10^7$ (totally real fields), respectively $5 \times 10^6$ (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 than $2 \times 10^7$,
- 79,394 fields with 2 complex conjugates and discriminant larger than $-5 \times 10^6$,
- 186,906 fields with 4 complex conjugates and discriminant less than $5 \times 10^6$.

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.

©1994 American Mathematical Society

0025-5718/94 $1.00 + .25$ per page
2. Generation of polynomials

Let $F$ be an algebraic number field of degree $n$ and discriminant $d_F$, and let $\mathcal{O}_F$ be the ring of integers of $F$. Let $F = \mathbb{Q}(\rho)$ for a root $\rho$ 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 $\rho$, 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 $\rho^{(r_1+1)}, \ldots, \rho^{(r_1+r_2)} \in \mathbb{C}\setminus\mathbb{R}$ with $\rho^{(r_1+r_2+j)} = \overline{\rho^{(r_1+j)}}$ for $1 \leq j \leq r_2$, so that $n$ equals $r_1 + 2r_2$. For any element $x \in F$, say $x = \sum_{i=1}^{n} q_i \rho^{i-1}$ ($q_i \in \mathbb{Q}$, $1 \leq i \leq n$), the conjugates of $x$ are given by $x^{(j)} := \sum_{i=1}^{n} q_i \rho^{(i-j)}$.

We introduce the function

$$T_2 : F \to \mathbb{R}^{\geq 0} : x \mapsto \sum_{i=1}^{n} |x^{(i)}|^2.$$ 

With $x \in F$ represented by a fixed basis, $T_2(x)$ becomes a positive definite quadratic form in the coefficients. Also, we need the $k$th power sum of $x$,

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

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

$$S_k + \sum_{i=1}^{k-1} a_i S_{k-i} + ka_k = 0 \quad (1 \leq k \leq n)$$

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 $|d_F| \leq B$ contains an integer $\rho \in F \setminus \mathbb{Q}$ 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 $d_F$, $|d_F| \leq B$. Then there exists an algebraic integer $\rho$ in $F$ with
A TABLE OF QUINTIC NUMBER FIELDS

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

\[ a_1 \in \{0, 1, 2 \} \]

and

\[ T_2(\rho) \leq U_2 := \frac{5}{4} + \left( \frac{4}{5} B \right)^{1/4}. \]

As a consequence, we also get bounds for the coefficients \( a_2, a_5 \) of the characteristic polynomial of that element \( \rho \). 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 \( (\rho^{(1)}, \ldots, \rho^{(n)}), (1, \ldots, 1) \), 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 \( T_2(\rho) = S_2(\rho) \geq \frac{3}{2} n \) [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

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

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

\[ T_2(x) := |x_1|^2 + \cdots + |x_5|^2 \leq U_2. \]

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

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

under the restrictions

\[ g_1(x) = x_1 + x_2 + x_3 + x_4 + x_5 - S_1 = 0, \]
\[ g_2(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 - S_2 = 0, \]
\[ g_3(x) = x_1 x_2 x_3 x_4 x_5 + a_5 = 0. \]
Because of \( T_2(x) = S_2(x) \) for all \( x \in \mathbb{R}^5 \), we do not need the side condition \( T_2(x) \leq U_2 \) in this case. The set \( G := \{ x \in \mathbb{R}^5 | g_j(x) = 0, \ j = 1, 2, 3 \} \) 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 \( x = (x_1, \ldots, x_5) \) whose coordinates satisfy

\[
x_1 = x_2 = x_3 \quad \text{or} \quad x_1 = x_2, x_3 = x_4.
\]

(b) The function \( S_4 \) has a global maximum and a global minimum on the set \( G \) at a vector \( x = (x_1, \ldots, x_5) \) whose coordinates satisfy

\[
x_1 = x_2 = x_3 \quad \text{or} \quad x_1 = x_2, x_3 = x_4
\]

or, in case \( S_1 \neq 0 \),

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

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

\[
\begin{align*}
3x_1 + x_4 + x_5 - S_1 &= 0, \\
3x_1^2 + x_4^2 + x_5^2 - S_2 &= 0, \\
x_1^3x_4x_5 + a_5 &= 0,
\end{align*}
\]
we get

\[
x_1^5 - \frac{1}{2}S_1x_1^4 + \frac{1}{12}(S_1^2 - S_2)x_1^3 + \frac{1}{6}a_5 = 0.
\]

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

\[
x_5^2 + (3x_1 - S_1)x_5 + 6x_1^2 - 3S_1x_1 + \frac{1}{2}(S_1^2 - S_2) = 0
\]

and, finally, \( x_4 \) from

\[
x_4 = S_1 - 3x_1 - x_5.
\]

For all solutions \( x \in G \) we compute \( S_k(x) \) 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 \( x \in G \) 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 \( x_4 \pm ix_5 \) with \( x_4, x_5 \in \mathbb{R} \), then we have to search for extrema of the real functions

\[
\begin{align*}
S_3(x) &:= x_1^3 + x_2^3 + x_3^3 + 2(x_4^3 - 3x_4x_5^2), \\
S_4(x) &:= x_1^4 + x_2^4 + x_3^4 + 2(x_4^4 - 6x_4^2x_5^2 + x_5^4), \\
S_{-1}(x) &:= \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + 2\frac{x_4}{x_4^2 + x_5^2}.
\end{align*}
\]
The constraints are
\[ g_1(x) = x_1 + x_2 + x_3 + 2x_4 - S_1 = 0, \]
\[ g_2(x) = x_1^2 + x_2^2 + x_3^2 + 2(x_4^2 - x_5^2) - S_2 = 0, \]
\[ g_3(x) = x_1x_2x_3(x_4^2 + x_5^2) + a_5 = 0, \]
\[ g_4(x) = x_1^2 + x_2^2 + x_3^2 + 2(x_4^2 + x_5^2) - U_2 \leq 0. \]

We define sets
\[ G := \{ x \in \mathbb{R}^5 | g_4(x) \leq 0 \land g_j(x) = 0, \quad j = 1, 2, 3 \}, \]
\[ G_3 := \{ x \in \mathbb{R}^5 | g_j(x) = 0, \quad j = 1, 2, 3 \}, \]
\[ G_4 := \{ x \in \mathbb{R}^5 | g_j(x) = 0, \quad j = 1, 2, 3, 4 \}. \]

Since \( G \) is compact, we have global extrema in \( G \). If \( x \in \mathbb{R}^5 \) is an extremum, then it is either an element of \( G_3 \) which satisfies \( g_4(x) < 0 \), 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 \( x = (x_1, \ldots, x_5) \) which satisfy one of the conditions
1. \( x_1 = x_2 = x_3, \)
2. \( x_1 = x_4 \land x_5 = 0, \)
3. \( x_1 = x_2 \land x_5 = 0. \)

(b) The function \( S_4 \) has its local extrema in the set \( G_4 \) only at points \( x = (x_1, \ldots, x_5) \) which satisfy either one of the conditions (1)-(3) of (a) or, in case \( S_1 \neq 0 \), one of the conditions
4. \( x_1 = x_2 = S_1 \land x_1 \neq x_3 \land x_5 \neq 0, \)
5. \( x_4 = S_1 \land x_5 = 0 \land x_1, x_2, x_3, x_4 \) 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 \( x \in \mathbb{R}^5 \) with \( g_4(x) < 0 \).

To determine the extrema in \( G_4 \) is somewhat more difficult, because we do not have similar conditions for the coordinates of a solution \( x \) as in the totally real case. Thus, it is necessary to calculate Lagrange multipliers explicitly, if the Jacobi matrix
\[ J(x) := \begin{pmatrix} \frac{\partial g_j(x)}{\partial x_i} \\ 1 \leq i \leq 5, 1 \leq j \leq 4 \end{pmatrix} \]
has rank four. Because of \( S_2 \leq U_2 \), we have
\[ 0 \neq x_2^2 = \frac{1}{4}(U_2 - S_2) \]
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 \( J(x) \) is four.

Hence, if \( J(x) \) 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 \( J(x) \) has rank four.
Determining the extrema of \( S_3 \) by the Lagrange multiplier method yields \( \lambda_1, \ldots, \lambda_4 \in \mathbb{R} \) subject to

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

Eliminating \( x_1, x_2, x_3 \), we obtain

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

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

\[
g_j(x_1, x_2, x_3, x_4, x_5), \quad 1 \leq j \leq 3,
\]

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

\[
\begin{align*}
S_3(x) &:= x_1^3 + 2(x_3^3 - 3x_2x_3^2) + 2(x_4^3 - 3x_4x_3^2), \\
S_4(x) &:= x_1^4 + 2(x_2^4 - 6x_2^2x_3^2 + x_3^4) + 2(x_4^4 - 6x_4^2x_3^2 + x_3^4), \\
S_{-1}(x) &:= \frac{1}{x_1} + 2x_2 + 2x_4 = \frac{1}{x_1} + \frac{x_2}{x_2^2 + x_3^2} + \frac{2}{x_4}.
\end{align*}
\]

subject to the restrictions

\[
\begin{align*}
g_1(x) &:= x_1 + 2x_2 + 2x_4 - S_1 = 0, \\
g_2(x) &:= x_1^2 + 2(x_2^2 - x_3^2) + 2(x_4^2 - x_5^2) - S_2 = 0, \\
g_3(x) &:= x_1(x_2^2 + x_3^2)(x_4^2 + x_5^2) + a_5 = 0, \\
g_4(x) &:= x_1^2 + 2(x_2^2 + x_3^2) + 2(x_4^2 + x_5^2) - U_2 \leq 0.
\end{align*}
\]

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 $x = (x_1, \ldots, x_5)$ which satisfy one of the conditions

1. $x_3 = x_5 = 0$,
2. $x_1 = x_2 \land x_3 = 0$,
3. $x_2 = x_4 \land x_3 = x_5$.

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

4. $x_1 \neq x_2 = S_1 \land x_3 = 0 \land x_5 \neq 0$.

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

The cases $x_2 = x_4$ or $x_2^2 + x_3^2 = x_4^2 + x_3^2$ 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 $n$th-degree polynomial $f(t) \in \mathbb{Z}[t]$ we define the quadratic form

$$q_f(x_1, \ldots, x_n) := \sum_{1 \leq i, j \leq n} S_{i+j-2} x_i x_j = x^T Q_f x$$

with coefficient matrix

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

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 $M_i := (m_{jk})_{1 \leq j, \k \leq i} (1 \leq i \leq n)$. Then the number of negative eigenvalues of $M$ is equal to the number of sign changes in the sequence $1, \det(M_1), \ldots, \det(M_n)$. 


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 $M = (m_{ij})_{1 \leq i, j \leq n}$ be a real symmetric $n \times n$-matrix with $\det(M) \neq 0$, and let $q(x) := \sum_{i,j=1}^{n} m_{ij}^{(0)} x_i x_j$ be the corresponding quadratic form. Then for each $k \in \{0, \ldots, n-1\}$ the form $q(x)$ 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

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

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

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

We remark that the principal minors of $M$ satisfy

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

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 $0 \leq k \leq 2n - 2$ via Newton's relations and initialize the Hankel matrix $Q_f = (m_{ij})_{1 \leq i, j \leq n} \leftarrow (S_{i+j-2})_{1 \leq i, j \leq n}$.
   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 $k < l \leq n$ and $m_{ll} \neq 0$, then
       interchange $m_{ki}$ and $m_{li}$ for $k \leq i \leq n$ and then
       interchange $m_{ik}$ and $m_{il}$ for $k \leq i \leq n$.
     Else if $m_{ii} = 0$ for all $i$ ($k \leq i \leq n$) and there is an index $l$ with $k < l \leq n$ and $m_{kl} \neq 0$ then
       set $m_{ki} \leftarrow m_{ki} + m_{li}$ for $k \leq i \leq n$ and then
       set $m_{ik} \leftarrow m_{ik} + m_{il}$ for $k \leq i \leq n$.
     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 $i \leq j \leq n$. 


Set \( m_{ki} \leftarrow 0 \) for \( k + 1 \leq i \leq n \).
Set \( m_{ij} \leftarrow m_{ij} \) for \( k \leq i \leq n - 1 \) and \( i + 1 \leq j \leq n \).
Set \( s \leftarrow s + \text{sign}(m_{kk}) \cdot \text{sign}(d) \) and \( d \leftarrow m_{kk} \).

(3) Set \( D(f) \leftarrow m_{nn} \), \( s \leftarrow s + \text{sign}(m_{nn}) \cdot \text{sign}(d) \) 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 \( n \geq 2 \) and define \( a := \max(\{|a_i| \mid 1 \leq i \leq n\} \cup \{1\}) \). Then

(a) Algorithm 3.3 requires at most
\[
4(n-1)^2 + 2n(n-1) + \frac{2}{3}n(n-1)(n+1) + 2 = O(n^3)
\]
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.

\[
\begin{align*}
S_5 & \quad 1 \times (1,1,1,1,1), 10 \times (2,1,1,1,1), 15 \times (2,2,1), 20 \times (3,1,1), 20 \times (3,2), 30 \times (4,1), 24 \times (5) \\
\text{Hol}(C_5) & \quad 1 \times (1,1,1,1,1), 5 \times (2,2,1), 10 \times (4,1), 4 \times (5) \\
A_5 & \quad 1 \times (1,1,1,1,1), 15 \times (2,2,1), 20 \times (3,1,1), 24 \times (5) \\
D_5 & \quad 1 \times (1,1,1,1,1), 5 \times (2,2,1), 4 \times (5) \\
C_5 & \quad 1 \times (1,1,1,1,1), 4 \times (5)
\end{align*}
\]
The groups include each other in the following way:

\[
\begin{array}{c}
S_5 \\
\downarrow \\
A_5 \\
\downarrow \\
\text{Hol}(C_5) \\
\downarrow \\
D_5 \\
\downarrow \\
C_5
\end{array}
\]

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 \( f \equiv f_1 \cdots f_r \mod p \) be a congruence factorization into monic irreducible polynomials. Then \( \Gamma_f \) contains an element \( \pi = \pi_1 \cdots \pi_r \), where the \( \pi_j \) are disjoint cycles of length \( \deg(f_j) \) (\( 1 \leq j \leq r \)).

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

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

**Lemma 3.8.** Let \( f(t) \) be as in Lemma 3.5. Then its Galois group \( \Gamma_f \) 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 \( \Gamma_f \) 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 \( \Gamma_f \) is contained in \( \text{Hol}(C_5) \), \( C_5 \), respectively. Let

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

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

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

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

Similarly, we define

\[
g_2(x_1, \ldots, x_5) := x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_5^2 + x_5x_1^2
\]
and

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

Assume that the values \( g_2(x_{\tau(1)}, \ldots, x_{\tau(5)}) \) are distinct for \( \tau \in V_2 \). Then the Galois group \( \Gamma_F \) is contained in (hence equal to) \( C_5 \) if and only if \( y = g_2(x_{\pi(1)}, \ldots, x_{\pi(5)}) \) 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 \( \rho \) 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>
<thead>
<tr>
<th>No</th>
<th>( d_F )</th>
<th>( f )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14641</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>24217</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>36497</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>38569</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>65657</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>70601</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>81509</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>81589</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>89417</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>101833</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>106069</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>117688</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>122821</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>124817</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>126032</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>135076</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>138136</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>138917</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>144209</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>147109</td>
<td>2</td>
</tr>
<tr>
<td>21</td>
<td>149169</td>
<td>0</td>
</tr>
<tr>
<td>22</td>
<td>153424</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>157457</td>
<td>2</td>
</tr>
<tr>
<td>24</td>
<td>160801</td>
<td>1</td>
</tr>
<tr>
<td>25</td>
<td>161121</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No</th>
<th>( d_F )</th>
<th>( f )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14641</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>24217</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>36497</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>38569</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>65657</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>70601</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>81509</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>81589</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>89417</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>101833</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>106069</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>117688</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>122821</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>124817</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>126032</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>135076</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>138136</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>138917</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>144209</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>147109</td>
<td>2</td>
</tr>
<tr>
<td>21</td>
<td>149169</td>
<td>0</td>
</tr>
<tr>
<td>22</td>
<td>153424</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>157457</td>
<td>2</td>
</tr>
<tr>
<td>24</td>
<td>160801</td>
<td>1</td>
</tr>
<tr>
<td>25</td>
<td>161121</td>
<td>1</td>
</tr>
</tbody>
</table>
There are 61 discriminants below 20 000 000 belonging to two nonisomorphic fields, namely,
A TABLE OF QUINTIC NUMBER FIELDS

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

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 $\mu$ nonisomorphic fields of that discriminant occur (which happens to be the case for $\mu = 2, 3$), we only list the 10 largest discriminants.
4.3. Fields with signature $r_1 = 1$ and $r_2 = 2$ and $d_F \leq 500000$. We compute all characteristic polynomials of algebraic integers $p$ with $T_2(p) \leq 45.98$. 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 Hol($C_5$), 258 fields with $A_5$, and 129 fields with $D$. 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.
A TABLE OF QUINTIC NUMBER FIELDS

<table>
<thead>
<tr>
<th>Group</th>
<th>$d_F$</th>
<th>$f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_5$</td>
<td>1609</td>
<td>0 -1 1 1 -1</td>
</tr>
<tr>
<td>$\text{Hol}(C_5)$</td>
<td>35152</td>
<td>1 2 4 1 1</td>
</tr>
<tr>
<td>$A_5$</td>
<td>18496</td>
<td>1 0 -2 -2 -2</td>
</tr>
<tr>
<td>$D_5$</td>
<td>2209</td>
<td>0 -1 2 -2 1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>number of nonisomorphic fields</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>discriminants</td>
<td>16757</td>
<td>17744</td>
<td>225872</td>
<td>721872</td>
<td>1672272</td>
<td>2432592</td>
<td>4050000</td>
</tr>
<tr>
<td></td>
<td>20432</td>
<td>48592</td>
<td>258768</td>
<td>1153872</td>
<td>2016576</td>
<td>4081104</td>
<td></td>
</tr>
<tr>
<td></td>
<td>34129</td>
<td>206928</td>
<td>514512</td>
<td>1333584</td>
<td>2059344</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>37584</td>
<td>213840</td>
<td>587088</td>
<td>1350864</td>
<td>2254968</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>37892</td>
<td>214272</td>
<td>640629</td>
<td>1664976</td>
<td>2546640</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>40912</td>
<td>216432</td>
<td>752976</td>
<td>1710288</td>
<td>3089664</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>45009</td>
<td>223737</td>
<td>880848</td>
<td>1862352</td>
<td>3707856</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>47797</td>
<td>251984</td>
<td>939600</td>
<td>2348496</td>
<td>4482000</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>48629</td>
<td>254148</td>
<td>1048896</td>
<td>2415312</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>49744</td>
<td>255312</td>
<td>1057104</td>
<td>2592000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>total</td>
<td>9333</td>
<td>756</td>
<td>103</td>
<td>29</td>
<td>8</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

BIBLIOGRAPHY


