A TABLE OF TOTALLY REAL QUINTIC NUMBER FIELDS

F. DIAZ Y DIAZ

Abstract. We give a table of the 1077 totally real number fields of degree five having a discriminant less than 2,000,000. There are two nonisomorphic fields of discriminant 1,810,969 and two nonisomorphic fields of discriminant 1,891,377. All the other number fields in the table are characterized by their discriminant. Among these fields, three are cyclic and four have a Galois closure whose Galois group is the dihedral group $D_5$. The Galois closure for all the other fields in the table has a Galois group isomorphic to $S_5$.

1. Introduction

A systematic study of 5th-degree number fields was done by H. Cohn in [4]; in that paper he gave a list of small discriminants for each of the three possible signatures, and he made the conjecture that these tables are complete in the ranges covered by the given values. In [3] P. Cartier and Y. Roy proved that the different polynomials of [4] having the same discriminant generate isomorphic number fields.

Some years later, J. Hunter [5], using methods of the geometry of numbers, determined the minimal discriminants for the three signatures of the number fields of degree five. They are: 1,649 for the signature $(1, 2)$, $-4,511$ for the signature $(3, 1)$, and 14,641 for the totally real quintics. He also enlarged the conjectural tables constructed by H. Cohn.

More recently, D. G. Rish [10] gave complete tables for quintics having one or three real places. Unfortunately, the author does not give proofs of the inequalities used, and these inequalities seem to have been obtained in a manner analogous to that used by J. Liang and H. Zassenhaus in [7] that are known to be incorrect (cf. [9]).

For the totally real quintics K. Takeuchi [11] found all the number fields of discriminants smaller than 150,000, and his list confirms the conjectural results in [4, 5] for that signature. It should be pointed out, however, that K. Takeuchi's table of totally real number fields of degree five contains two errors to which J. Martinet has drawn my attention: the polynomials $X^5 + 2X^4 - 6X^3 - 4X^2 + 5X - 1$ of discriminant 107,653 and $X^5 - 8X^3 - 2X^2 + 3X + 1$ of discriminant 146,205.

Received May 19, 1989.

Key words and phrases. Totally real number fields, discriminant, Galois group.

©1991 American Mathematical Society
0025-5718/91 $1.00 + .25 per page

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
do not generate quintic number fields because they are reducible: the first one is divisible by \( X^2 + 3X - 1 \) and the second by \( X^2 + 3X + 1 \). Our computations show that the table of \( K \). Takeuchi is correct if we eliminate these two discriminants.

The table given in the Supplement section contains the complete list of the 1077 totally real number fields of degree five of discriminant smaller than 2,000,000. For the computation of the table we used the techniques of the geometry of numbers, and we will give a brief description of them in the next section. These methods have already been used by different authors in the construction of extensive tables of number fields [1, 2].

In §3 we describe the simplifications used to reduce as much as possible the number of polynomials to be considered. We also explain what tests are used for the determination of the signature of the fields, the irreducibility of the polynomials, and the exact value of the discriminant of the fields.

In §4 we show how we found the possible existence of isomorphisms among the number fields generated by the roots of the different polynomials having the same discriminant. Thus, we prove the existence of two nonisomorphic fields of discriminant 1,810,969 and two nonisomorphic fields of discriminant 1,891,377. All the other fields in the table are characterized by their discriminant.

Finally, in §5, we study the Galois group of the Galois closure of each number field in the table. We then prove that in the range of the table there exist exactly three abelian number fields and four number fields for which the Galois group of the Galois closure is the dihedral group \( D_5 \). All the other number fields in the table have a Galois closure having a Galois group isomorphic to the symmetric group \( S_5 \).

All the computations were done on the UNIVAC 1110 at the University of Paris XI.

We wish to thank J. Martinet for his suggestions and help in verifying that the table was complete.

2. **The method**

Let \( K \) be a totally real number field of degree 5 having a discriminant \( d_K \) < 2,000,000, and let \( \mathbb{Z}_K \) denote its ring of integers. We know that \( K \) is always a primitive extension of \( \mathbb{Q} \) generated by a root \( \theta \) of an irreducible polynomial \( P(X) = X^5 + a_1 X^4 + a_2 X^3 + a_3 X^2 + a_4 X + a_5 \in \mathbb{Z}[X] \) having only real roots.

We will also use Newton’s relations

\[
S_k + k \cdot a_k + \sum_{i=1}^{k-1} a_i \cdot S_{k-i} = 0,
\]

valid for all \( k \in \mathbb{N} \) if we define \( a_k = 0 \) for \( k > 5 \) and where the \( S_k \) denote the \( k \)th power sums,

\[
S_k = S_k(\theta) = \text{Tr}_{K/Q}(\theta^k).
\]
If we fix an order for the roots of the polynomial \( P(X) = \prod_{i=1}^{5}(X - \theta_i) \), we can obtain an embedding of \( K \) in \( \mathbb{R}^5 \) by using the map

\[
\tau \begin{cases}
K \to \mathbb{R}^5, \\
\theta \mapsto (\theta_1, \ldots, \theta_5),
\end{cases}
\]

and under this map \( Z_K \) becomes a lattice \( M \) of \( \mathbb{R}^5 \) of discriminant \( d_K \).

The map

\[
q \begin{cases}
Z_K \to \mathbb{R}, \\
\theta \mapsto \sum_{i=1}^{5} \theta_i^2
\end{cases}
\]

is a positive definite quadratic form. The restriction of \( q \) to the sublattice \( M' \), the image by \( \tau \) of the ring \( \mathbb{Z}[\theta] \), is still a positive definite quadratic form whose matrix relative to the basis \( \{1, \theta, \ldots, \theta^4\} \) is

\[
\begin{pmatrix}
S_5 & S_1 & S_2 & S_3 & S_4 \\
S_1 & S_2 & S_3 & S_4 & S_5 \\
S_2 & S_3 & S_4 & S_5 & S_6 \\
S_3 & S_4 & S_5 & S_6 & S_7 \\
S_4 & S_5 & S_6 & S_7 & S_8
\end{pmatrix}
\]

and has determinant \( d(\theta) = f^2 \cdot d_K \), where \( f \) is the index of the ring \( \mathbb{Z}[\theta] \) in \( \mathbb{Z}_K \).

Our computations are based upon the following fundamental result:

**Theorem 1** (Hunter [5], Pohst [9], Martinet [8]). There exists an algebraic integer \( \theta \in K, \theta \not\in \mathbb{Q} \), such that

\[
\begin{align*}
(2) & \quad 0 \leq \text{Tr}_{K/\mathbb{Q}}(\theta) \leq 2, \\
(3) & \quad 6 \leq \text{Tr}_{K/\mathbb{Q}}(\theta^2) \leq \left(\frac{\text{Tr}_{K/\mathbb{Q}}(\theta)}{5}\right)^2 + 35.566.
\end{align*}
\]

For each value of \( S_2 \) in the range defined by inequalities (3) we have:

**Lemma 1.** The polynomial \( P(X) \) for which \( \theta \) is a root satisfies

\[
\begin{align*}
(4) & \quad |a_5| = |P(\theta)| \leq (S_2/5)^{2.5}, \\
(5) & \quad |P(1)| \leq \left(\frac{S_2 - 2S_1 + 5}{5}\right)^{2.5}, \\
(6) & \quad |P(-1)| \leq \left(\frac{S_2 + 2S_1 + 5}{5}\right)^{2.5}.
\end{align*}
\]

This follows from the inequalities between arithmetic and geometric means.

Conditions (2)–(6) suffice to construct all the polynomials where a root generates each one of the fields \( K \) under consideration; however, in order to minimize the number of polynomials to be considered, we will try to find, in a
different way, more inequalities for the coefficients of \( P(X) \) and for the symmetric functions \( S_k \) for \( k = 3, 4 \). Let us fix the value of \( a_5 \); if we write \( N = |a_5| \) \((\neq 0)\) and \( T = S_2 \) we have:

**Theorem 2** (Pohst [9]). Let \( y_t \) denote the smallest positive root of the equation

\[
2^t \cdot \left( N \frac{x^{5-t}}{x^5} \right)^{2/t} + (5-t) \cdot x^2 = T, \quad t = 1, 2, 3, 4,
\]

and

\[
T_m = \max_{1 \leq t < 4} \left\{ t \cdot \left( N \frac{x^{5-t}}{y_t^m} \right)^{m/t} + (5-t)y_t^m \right\} \text{ for } m = -1, 3, 4.
\]

Then we have the inequalities

\[
-a_5 |T_{-1} \leq a_4 \leq |a_5|T_{-1},
\]

\[
-T_3 \leq S_3 \leq T_3,
\]

\[
0 < S_4 \leq T_4.
\]

Moreover, the coefficients of \( P(X) \) satisfy Newton's inequalities because the roots of this polynomial are real:

\[
2a_1a_3 \leq a_2^2,
\]

\[
2a_2a_4 \leq a_3^2,
\]

\[
5a_3a_5 \leq 2a_4^2.
\]

We should also bear in mind the fact that the second derivative of \( P(X) \) has three real roots and, consequently, a positive discriminant. Following [5], we obtain the inequality

\[
|25a_3 - 15a_1a_2 + 4a_1^3| \leq \sqrt{2(2a_1^2 - 5a_2)^3}.
\]

The lower bound in inequality (9) can be improved if we consider the lattice \( M' \) and the restriction of the quadratic form \( q \) to the submodules containing points of \( M' \), where at least one of their coordinates in the basis \( \{1, \theta, \theta^2, \theta^3, \theta^4\} \) is zero. These restrictions are also positive definite quadratic forms and therefore have a positive determinant. A first rough estimate is obtained by the inequality

\[
\begin{vmatrix}
S_2 & S_3 \\
S_3 & S_4
\end{vmatrix} > 0,
\]

and a stronger lower bound is obtained by

\[
\begin{vmatrix}
5 & S_1 & S_2 \\
S_1 & S_2 & S_3 \\
S_2 & S_3 & S_4
\end{vmatrix} > 0.
\]
3. THE COMPUTATIONS

We begin by fixing the (integer) value of \( S_2 \) in the range (3), and we consider the values of \( S_1 \) in the interval (2) having the same parity as that of \( S_2 \) because, according to the relations (1), the residue class \((\mathbb{Z}/k)\) of \( S_k \) is entirely determined by the residue class \((\mathbb{Z}/k)\) of \( S_1, \ldots, S_{k-1} \), for \( k = 2, 3, 4, 5 \).

We first determine the coefficients \( a_1 \) and \( a_2 \) of \( P(X) \), and then we compute 
\[
D' = 1.25(S_2 - a_1^2/5)^4.
\]
According to Theorem 1 we know that all the number fields \( K \) of discriminant \( d_K < D' \) have already been found for values of \( S_2 \) smaller than those we are now considering. The computation of \( D' \) allows us to restrict our research to the values of the discriminant \( d_K \) in the range \( D' < d_K < 2 000 000 \), which becomes narrower when the value of \( S_2 \) is crossed. The search for the inessential factors of the discriminant of the polynomial is then made easier.

Next we consider the intervals obtained for \( a_5 \), \( P(1) \) and \( P(-1) \), using inequalities (4)-(6). In the special case where \( a_1 = 0 \) we can take \( a_5 > 0 \); the value of \( a_5 \) being fixed, we use Theorem 2 to determine \( T_{-1} \), \( T_3 \), and \( T_4 \).

We then choose the values for \( s_3 \) in \( |s_3| \leq T_3' \) with \( T_3' = \min(T_3, \sqrt{S_2 T_4}) \) because, according to inequality (14), we must have \( S_3^2 < S_2 S_4 \). We can now compute the value of \( a_3 \), which must satisfy inequalities (10) and (13).

Inequality (15) gives us a lower bound \( T_4' \) for \( s_4 \), and we take \( s_4 \) in the interval \([T_4', T_4]\) which is sometimes empty. This allows us to compute the last coefficient \( a_4 \) which is still unknown. We then use inequalities (7), (11), (12), (5), and (6) in that order. For the polynomials whose coefficients and power sums satisfy inequalities (1)-(15), we determine the number of real roots, using Sturm’s Theorem, and when all the roots are real, we compute them with an accuracy of less than \( 10^{-11} \).

To test whether or not \( P(X) \) is reducible, we first consider the polynomial obtained from \( P(X) \) by reduction (mod 2) of their coefficients, and we compare it with the complete list of irreducible polynomials of degree five in \( \mathbb{F}_2[X] \). When the reduced polynomial appears in this list, we know that \( P(X) \) is irreducible in \( \mathbb{Z}[X] \) and the test is finished. Otherwise, we use the roots to verify if there exist divisors of degree 1 or 2 of \( P(X) \). Let us suppose that \( P(X) \) is irreducible; then we compute an approximate value of its discriminant, using the formula 
\[
d_p = \prod_{i=1}^{5} P'(\theta_i),
\]
and its exact value in the finite fields \( \mathbb{F}_{100003} \) and \( \mathbb{F}_{100019} \). The Chinese Remainder Theorem suffices to determine the exact value of \( d_K \).

Next we try to decompose \( d_p \) in the form \( d_p = f^2 \cdot d_K \) with \( D' < d_K < 2 000 000 \), and when this is possible, we consider the different prime divisors of \( f \) to decide whether or not they are inessential divisors of the discriminant. This can be done using Dedekind’s Criterion (cf. [9]). If \( p \) is a prime which divides \( f \) and appears in the decomposition in primes of \( d_p \) at a high power, we construct a basis of integers of \( K \) to determine the exact power of \( p \) dividing \( d_K \).
4. ISOMORPHIC FIELDS

In spite of the fact that the use of the lower bound \( D' \) reduces the number of polynomials generating number fields of the same discriminant, we usually obtain several polynomials for each discriminant. To decide whether or not two such polynomials correspond to isomorphic fields, we proceed in the following way: we fix a polynomial, among those having the same discriminant, for which the index \( f' \) is as small as possible (this is the polynomial which appears in the table), and we fix an order for its roots \( \theta_1, \ldots, \theta_5 \). For each one of the other polynomials having the same value of \( d_K \) (designated in the sequel by \( P'(X) \) with roots \( \theta'_1, \ldots, \theta'_5 \)), we successively consider the products

\[
S_1(\sigma) = \sum_{i=1}^{5} \theta_i \theta'_{\sigma(i)},
\]

where \( \sigma \) describes all the permutations in five elements.

Considering the permutation \( \sigma \), when we find a value of \( S_1(\sigma) \) near an integer, we compute the products

\[
s_k = S_k(\sigma) = \sum_{i=1}^{5} \theta_i^k \theta'_{\sigma(i)} \quad \text{for } k = 2, 3, 4,
\]

and if \( s_2, s_3, \) and \( s_4 \) are also near integers, we try to solve the system

\[
\begin{bmatrix}
5 & S_1 & S_2 & S_3 & S_4 \\
S_1 & S_2 & S_3 & S_4 & S_5 \\
S_2 & S_3 & S_4 & S_5 & S_6 \\
S_3 & S_4 & S_5 & S_6 & S_7 \\
S_4 & S_5 & S_6 & S_7 & S_8
\end{bmatrix}
\begin{bmatrix}
x_0 \\
x_1 \\
x_2 \\
x_3 \\
x_4
\end{bmatrix}
= \begin{bmatrix}
s_0 \\
s_1 \\
s_2 \\
s_3 \\
s_4
\end{bmatrix},
\]

where \( s_0 = S_1(\theta') \).

If \( f \cdot x_i \) is near an integer for \( 0 \leq i \leq 4 \), we verify that the polynomial with roots equal to

\[
\theta'_i = x_0 + x_1 \theta_i + x_2 \theta_i^2 + x_3 \theta_i^3 + x_4 \theta_i^4 \quad \text{for } i = 1, \ldots, 5
\]

is exactly \( P'(X) \).

Thus, we obtain the following theorem.

**Theorem 3.** Within the range covered by the table there exist two nonisomorphic fields of discriminant 1810969 and two nonisomorphic fields of discriminant 1891377. All the other fields in the table are characterized by their discriminant.

**Proof.** In only two cases did the system (16) lack a solution \( (x_0, x_1, x_2, x_3, x_4) \) with \( f \cdot x_i \) integer for \( i = 0, \ldots, 4 \): this was the case for the polynomials

\[
P_1(X) = X^5 - 4X^4 - 7X^3 + 7X^2 + 6X - 5 \quad \text{with } P_1(\theta) = 0 \quad \text{and} \quad P'_1(X) = X^5 - 2X^4 - 8X^3 + 9X^2 + 16X - 7 \quad \text{with } P'_1(\theta') = 0
\]

of discriminant 1810969 as well as for the polynomials

\[
P_2(X) = X^5 - X^4 - 7X^3 + 6X^2 + 9X - 6 \quad \text{with}
\]

\[
P_2(\theta) = 0 \quad \text{and} \quad P'_2(X) = X^5 - 2X^4 - 8X^3 + 9X^2 + 16X - 7 \quad \text{with } P'_2(\theta') = 0.
\]
To prove that the fields $K = \mathbb{Q} (\theta)$ and $K' = \mathbb{Q} (\theta')$ are nonisomorphic, we consider the decomposition of the ideal (3) in these two fields; we have:

(3) remains prime in $K$,

(3) = $\varphi_1 \cdot \varphi'_1 \cdot \varphi_3$ in $K$, where $\varphi_1 = (3, \theta' + 1)$, $\varphi'_1 = (3, \theta - 1)$, and $\varphi_3 = (3, \theta^3 + \theta^2 + 2\theta + 1)$.

The fields $K_1 = \mathbb{Q} (\mu)$ and $K'_1 = \mathbb{Q} (\mu')$ are not isomorphic either because we have

(3) = $\varphi_3 \cdot \varphi_2$ in $K_1$, where $\varphi_1 = (3, \mu)$ and $\varphi_2 = (3, \mu^2 + 2\mu + 2)$, and

(3) = $\varphi'_3 \cdot \varphi''_1$ in $K'_1$, where $\varphi_1 = (3, \mu')$, $\varphi'_1 = (3, \mu' + 1)$, and $\varphi''_1 = (3, \mu' - 1)$.

5. Galois groups

Theorem 4. The fields of discriminant 14641 = $11^4$, 390625 = $5^8$, and 923521 = $31^4$ are cyclic.

These fields are well known.

Remarks. 1. The field of discriminant 14641 is generated by a root $\theta$ of the polynomial $X^5 - X^4 - 4X^3 + 3X^2 + 3X - 1$. It can easily be verified that the other roots are $-\theta^2 + 2$, $\theta^3 - 3\theta$, $-\theta^4 + 4\theta^2 - 2$, and $\theta^4 - \theta^3 - 3\theta^2 + 2\theta + 1$.

2. The field of discriminant 390625 is generated by a root $\theta$ of the polynomial $X^5 - 10X^3 + 5X^2 + 10X + 1$ and the other roots are

$$(-2\theta^4 + \theta^3 + 23\theta^2 - 18\theta - 25) / 7, \quad (4\theta^4 - 2\theta^3 - 39\theta^2 + 36\theta + 22) / 7,$$

$$(-3\theta^4 - 2\theta^3 + 36\theta^2 - 6\theta - 6) / 7.$$

3. The field of discriminant 923521 is generated by a root $\theta$ of the polynomial $X^5 - X^4 - 12X^3 + 21X^2 + X - 5$ and the other roots are

$$(-3\theta^4 - \theta^3 - 22\theta^2 + 31\theta) / 5, \quad (2\theta^4 + 4\theta^3 - 17\theta^2 - 14\theta + 10) / 5,$$

$$(-3\theta^4 - \theta^3 + 33\theta^2 - 24\theta - 15) / 5, \quad (-\theta^4 - 2\theta^3 + 6\theta^2 + 2\theta + 10) / 5.$$

Theorem 5. The Galois group of the Galois closure of the fields of discriminant 160801 = $401^2$, 667489 = $19^2 \cdot 43^2$, 1194649 = $1093^2$, and 1940449 = $72 \cdot 199^2$ is the dihedral group $D_5$.

It can easily be verified that the quadratic fields $\mathbb{Q} (\sqrt{401})$, $\mathbb{Q} (\sqrt{817})$, $\mathbb{Q} (\sqrt{1093})$, and $\mathbb{Q} (\sqrt{1393})$ have class number equal to 5.

Theorem 6. The Galois group of the Galois closure of the totally real quintic number fields of discriminant less than 2000000 not indicated in Theorems 4 and 5 above is the symmetric group $S_5$. 

Proof. We know from [8] that the minimal discriminant for the totally real quintics whose Galois closure has a Galois group isomorphic to the affine group $\text{Aff}_5$ is 2 382 032 and out of the range of the table. The discriminant of the number fields having a Galois closure with Galois group isomorphic to $A_5$ is a square, but there are only seven perfect squares among the discriminants in the table and their group has been established in Theorems 4 and 5. This proves our theorem. □

Remark. The minimal discriminant for the totally real quintics whose Galois group of its Galois closure is the group $A_5$ seems to be the field of discriminant $3 104 644 = 2^2 \cdot 881^2$ generated by a root of the polynomial $x^5 - x^4 - 11x^3 + x^2 + 12x - 4$.

BIBLIOGRAPHY


UNIVERSITÉ DE BORDEAUX I, MATHEMATIQUES PURES, 351, COURS DE LA LIBÉRATION, 33405 TALENCE CÉDEX, FRANCE
Supplement to
A TABLE OF TOTALLY REAL
QUINTIC NUMBER FIELDS

F. DIAZ Y DIAZ

DESCRIPTION OF THE TABLE

The first five columns of the table give, in this order, the coefficients $a_1, a_2, a_3, a_4, a_5$ of the polynomial $P(X) = X^5 + a_1X^4 + a_2X^3 + a_3X^2 + a_4X + a_5$. The next column gives the discriminant $d_K$ of the field $K$, and is followed by the index $f$ of the ring $\mathbb{Z}[\theta]$ in $\mathbb{Z}_K$: one thus has $d_P = f^2 d_K$, where $d_P$ is the discriminant of $P(X)$. Finally, the decomposition in prime factors of the discriminant of the field is given, where the exponents are placed between parentheses if they are greater than 1.
<table>
<thead>
<tr>
<th>F</th>
<th>A1</th>
<th>A2</th>
<th>A3</th>
<th>A4</th>
<th>A5</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>A2</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>A3</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>A4</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
</tr>
<tr>
<td>A5</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
</tr>
</tbody>
</table>