ENUMERATION OF QUARTIC FIELDS OF SMALL DISCRIMINANT

JOHANNES BUCHMANN, DAVID FORD, AND MICHAEL POHST

ABSTRACT. With the mixed-type case now completed, all algebraic number fields of degree 4 with absolute discriminant < 10^6 have been enumerated. Methods from the totally real and totally complex cases were used without major modification. Isomorphism of fields was determined by a method similar to one of Lenstra. The T_2 criterion of Pohst was applied to reduce the number of redundant examples.

1. Introduction

We have previously enumerated totally real (signature 4) [1] and totally complex (signature 0) [2] fields. We now treat the remaining case, fields of mixed type (signature 2). The methods of [1] and [2] are used without major modification.

2. Existence of small integers

A consequence of [8, Theorems 1–3] is

Proposition 1. If F is an algebraic number field of degree 4 with discriminant d_F and ring of integers O_F, then there exists \( \rho \in O_F \setminus \mathbb{Z} \) such that

\[
T_2(\rho) \leq 1 + \sqrt[3]{|d_F|/2},
\]

where \( \rho_1, \ldots, \rho_4 \) are the conjugates of \( \rho \), and, for \( k \in \mathbb{Z} \),

\[
T_k(\rho) = \sum_{j=1}^{4} |\rho_j|^k.
\]

We let \( \rho \) be an algebraic number satisfying the conditions of Proposition 1, with characteristic polynomial given by

\[
f(x) = \prod_{j=1}^{4} (x - \rho_j) = x^4 - sx^3 + px^2 - qx + n.
\]

If \( \mathbb{Q}(\rho) \) has signature 2, then \( \rho \) may be assumed to satisfy the following:

\[
\begin{align*}
(1) & \quad 0 \leq s \leq 2, \\
(2) & \quad \frac{s^2 - T_2(\rho)}{2} \leq p \leq \frac{s^2/2 + T_2(\rho)}{2},
\end{align*}
\]

Received by the editor November 5, 1990 and, in revised form, June 15, 1992.

1991 Mathematics Subject Classification. Primary 11-04, 11R16, 11Y40.

The second author's research was supported by the Natural Sciences and Engineering Research Council (Canada) and Fonds pour la Formation de Chercheurs et l'Aide à la Recherche (Québec).

©1993 American Mathematical Society

0025-5718/93 $1.00 + .25 per page

873
Relations (1), (2), and (4) come directly from [8, Theorem 3], while (3) is a consequence of \(|s^3 - 3sp + 3q| = |\sum_{j=1}^{4} p_j^3| \leq T_3(\rho)\). We take

\[T_{21}(d) = \lfloor 1 + \sqrt{|d|/2} \rfloor, \quad T_3(d) = \lfloor (1 + \sqrt{|d|/2})^{3/2} \rfloor,\]
\[T_{22}(d) = \lfloor 2(1 + \sqrt{|d|/2}) \rfloor, \quad T_4(d) = \lfloor 1 + \sqrt{|d|/2} \rfloor,\]

and define \(G_1(d)\) to be the set of all polynomials \(f(x) = x^4 - sx^3 + px^2 - qx + n \in \mathbb{Z}[x]\) with coefficients satisfying

\[0 \leq s \leq 2,\]
\[\frac{s^2 - T_{21}(d)}{2} \leq p \leq \frac{s^2 + T_{22}(d)}{4},\]
\[-\frac{s^3 + 3sp - T_3(d)}{3} \leq q \leq \frac{-s^3 + 3sp + T_3(d)}{3},\]
\[0 \leq n \leq \frac{T_4(d)}{16}.\]

The integer quantities \(T_{21}(d), T_{22}(d), T_3(d), T_4(d)\) are easy to compute, so the question of whether a given polynomial belongs to \(G_1(d)\) can be answered quickly.

Observing that \(|T_2(\rho)| \leq T_{21}(d_F), |2T_2(\rho)| \leq T_{22}(d_F), |T_3(\rho)| \leq |T_2(\rho)^{3/2}| \leq T_3(d_F), |T_2^2(\rho)| \leq T_4(d_F)|\) establishes

**Proposition 2.** If \(F\) is an algebraic number field of degree 4 and signature 2 with discriminant \(d_F\) and ring of integers \(\mathcal{O}_F\), then there exists \(\rho \in \mathcal{O}_F \setminus \mathbb{Z}\) with characteristic polynomial belonging to \(G_1(d_F)\).

### 3. Fields with small quartic integers

For each polynomial \(f(x) \in G_1(10^6)\) we perform the following tests (cf. [1]):

1. If \(f(x)\) is reducible in \(\mathbb{Z}[x]\), we exclude \(f\).
2. If \(f(x)\) is irreducible but \(\mathbb{Q}(\rho)\) is not of signature 2, we exclude \(f\).
3. We compute the discriminant \(d_F\) of the field \(F = \mathbb{Q}(\rho)\).
4. If \(|d_F| \geq 10^6\), we exclude \(f\).
5. If \(f \notin G_1(d_F)\), we exclude \(f\).

Among the polynomials surviving these tests is a generating polynomial for every quartic number field of mixed type with absolute discriminant less than \(10^6\), excepting those fields for which no choice of \(\rho\) in Proposition 1 gives a quartic integer. In these fields every such "small" \(\rho\) generates a quadratic subfield; we enumerate these fields separately.
4. Fields with quadratic subfields

We now assume that $F$ is an algebraic number field of degree 4 with signature 2 and discriminant $d_F$, with $|d_F| < 10^6$, and that $F$ contains a quadratic subfield $K$ with discriminant $d_K$. Since $F$ has a real embedding, $d_K > 0$.

Let $\omega, \omega' = \frac{1}{2}(\sigma \pm \sqrt{d_K})$, where $\sigma \in \{0, 1\}$, $\sigma \equiv d_K \pmod{4}$, so that $K = \mathbb{Q}(\omega)$, and $\mathcal{O}_K = \mathbb{Z}[\omega]$ is the ring of integers of $K$.

We take $\rho \in \mathcal{O}_F \setminus \mathcal{O}_K$, and let

$$g(x) = x^2 - \alpha x + \beta \in \mathcal{O}_K[x]$$

be the minimal polynomial of $\rho$ over $K$, with

$$\alpha = a_1 + a_2 \omega, \quad \beta = b_1 + b_2 \omega,$$

$$\alpha' = a_1 + a_2 \omega', \quad \beta' = b_1 + b_2 \omega'.$$

Then the characteristic polynomial of $\rho$ over $\mathbb{Q}$ is

$$f(x) = (x^2 - (a_1 + a_2 \omega)x + (b_1 + b_2 \omega))(x^2 - (a_1 + a_2 \omega')x + (b_1 + b_2 \omega'))$$

$$= (x^2 - \alpha x + \beta)(x^2 - \alpha' x + \beta')$$

$$= x^4 - sx^3 + px^2 - qx + n \in \mathbb{Z}[x].$$

We define the $\mathbb{Z}$-module homomorphism $\lambda : \mathcal{O}_F \to \mathbb{R}_4$ by

$$\lambda(\xi) = (\frac{1}{2}(\xi_1 - \xi_2), \frac{1}{2}(\xi_2 - \xi_1), 0, \xi_3, \xi_3)$$

where $\xi_1, \xi_2, \xi_3$ are the real conjugates of $\xi$, and $\xi_3, \bar{\xi}_3$ the complex conjugates. Then $\lambda(\mathcal{O}_F)$ is a 2-dimensional lattice of determinant $\Delta = \sqrt{|d_F|/8d_K}$, and the kernel of $\lambda$ is $\mathcal{O}_K$. We choose $\rho \in \mathcal{O}_F$ so that $||\lambda(\rho)||^2 \leq 2\Delta/\sqrt{3} = \sqrt{|d_F|/6d_K}$ and $\text{Tr}_{F/K}(\rho) = \alpha \in \{0 + \omega, 1 + \omega, 0 + 2\omega, 1 + 2\omega\}$. (Taking $\alpha \notin \mathbb{Q}$ ensures that $\rho$ has degree 4 over $\mathbb{Q}$.)

Since $\alpha$ and $\beta$ are real, we have

$$\alpha = \rho_1 + \rho_2, \quad \beta = \rho_1 \rho_2,$$

$$\alpha' = \rho_3 + \bar{\rho}_3 = 2\Re \rho_3, \quad \beta' = \rho_3 \bar{\rho}_3, = |\rho_3|^2.$$

Therefore,

$$\beta + \beta' = \frac{1}{4}(\alpha^2 + \alpha'^2) - \frac{1}{4}(\rho_1 - \rho_2)^2 + \Im \rho_3^2,$$

$$\beta - \beta' = \frac{1}{4}(\alpha^2 - \alpha'^2) - \frac{1}{4}(\rho_1 - \rho_2)^2 - \Im \rho_3^2,$$

so that

$$|\beta + \beta'| - \frac{1}{4}(\alpha^2 + \alpha'^2)| \leq \frac{1}{4}(\rho_1 - \rho_2)^2 + \Im \rho_3^2 \leq ||\lambda(\rho)||^2, 0 \leq \frac{1}{4}(\alpha^2 - \alpha'^2) - (\beta - \beta') \leq ||\lambda(\rho)||^2.$$

We define $A_1 = 4a_1^2 + 4a_1a_2\sigma + a_2^2(d_K + \sigma)$, $A_2 = a_2(2a_1 + a_2\sigma)$, so that

$$\alpha^2 + \alpha'^2 = \frac{1}{2}A_1, \quad \beta + \beta' = 2b_1 + b_2\sigma,$$

$$\alpha^2 - \alpha'^2 = A_2\sqrt{d_K}, \quad \beta - \beta' = b_2\sqrt{d_K}.$$

It follows that

$$\frac{A_2 - M}{4} \leq b_2 \leq \frac{A_2}{4},$$

$$\frac{A_1 - 8b_2\sigma - N}{16} \leq b_1 \leq \frac{A_1 - 8b_2\sigma + N}{16},$$
where

\[ M = \lfloor 4\sqrt{|d_F|/6|d_K|^2} \rfloor, \quad N = \lfloor 8\sqrt{|d_F|/6|d_K|} \rfloor. \]

We define \( G_2(d_F, d_K) \) to be the set of all polynomials \( f(x) \in \mathbb{Z}[x] \) defined by (9), with \( a_1 \in \{0, 1\} \), \( a_2 \in \{1, 2\} \), and \( b_1, b_2 \) satisfying (10), (11).

**Proposition 3.** If \( F \) is an algebraic number field of degree 4 and signature 2 with discriminant \( d_F \) and ring of integers \( \mathcal{O}_F \), and if \( F \) contains a quadratic subfield \( K \) with discriminant \( d_K \) and ring of integers \( \mathcal{O}_K \), then there exists \( \rho \in \mathcal{O}_F \setminus \mathcal{O}_K \) with characteristic polynomial belonging to \( G_2(d_F, d_K) \), such that \( F = \mathbb{Q}(\rho) \).

### 5. Fields with small quadratic integers

Let \( F \) be a quartic number field of signature 2 with discriminant \( d_F > -10^6 \). Suppose there exists \( \rho \in \mathcal{O}_F \setminus \mathbb{Z} \) with characteristic polynomial in \( G_1(d_F) \) such that \( K = \mathbb{Q}(\rho) \) is a quadratic subfield of \( F \). It follows from Proposition 2, using (5)–(8) with \( d = -10^6 \), that \( 0 < d_K < 80 \).

For each quadratic field discriminant \( d_K \) with \( 0 < d_K < 80 \) we generate the polynomials in \( G_2(-10^6, d_K) \) according to (9), taking \( a_1 \in \{0, 1\} \), \( a_2 \in \{1, 2\} \), and \( b_1, b_2 \) running through the values specified by (10) and (11). For each such polynomial \( f(x) \) we perform the following tests:

1. If \( f(x) \) is reducible in \( \mathbb{Z}[x] \), we exclude \( f \).
2. If \( f(x) \) is irreducible but \( \mathbb{Q}(\rho) \) is not of signature 2, we exclude \( f \).
3. We compute the discriminant \( d_F \) of the field \( F = \mathbb{Q}(\rho) \).
4. If \( |d_F| \geq 10^6 \), we exclude \( f \).
5. If \( f \not\in G_2(d_F, d_K) \), we exclude \( f \).

Among the polynomials surviving these tests is a generating polynomial for every quartic number field of signature 2 with absolute discriminant less than \( 10^6 \), such that no \( \rho \in \mathcal{O}_F \setminus \mathbb{Z} \) with characteristic polynomial in \( G_1(d_F) \) is a quartic integer.

### 6. Determining field isomorphism

Let \( f \) and \( g \) be irreducible monic quartic polynomials in \( \mathbb{Z}[x] \), \( \alpha \) and \( \beta \) roots of \( f \) and \( g \), respectively, \( p \) a rational prime not dividing \( D_f \) or \( D_g \), and \( n_f \) and \( n_g \) the number of solutions in \( \mathbb{Z}/p\mathbb{Z} \) to the congruences \( f(x) \equiv 0 \pmod{p} \) and \( g(x) \equiv 0 \pmod{p} \). From Hensel's Lemma we know that \( n_f \) and \( n_g \) give the number of roots of \( f \) and \( g \) in \( \mathbb{Z}_p \).

The fields \( \mathbb{Q}[\alpha] \) and \( \mathbb{Q}[\beta] \) are isomorphic if and only if there is a polynomial \( h \in \mathbb{Q}[x] \) such that \( h(\alpha) \) has characteristic polynomial \( g \). If \( \mathbb{Q}[\alpha] \) and \( \mathbb{Q}[\beta] \) are isomorphic, then any root of \( f \) lying in \( \mathbb{Z}_p \) is taken by \( h \) to a root in \( \mathbb{Z}_p \) of \( g \). It follows that \( f \) and \( g \) have the same number of roots in \( \mathbb{Z}_p \), and that \( h \) gives a one-to-one correspondence between them.

It is well known [3, Theorem 1], [10] that \( n_f > 0 \) for infinitely many choices of \( p \). We assume therefore that \( p \) has been chosen so that \( n_f = n_g > 0 \), and take \( \alpha \) and \( \beta \) to lie in \( \mathbb{Z}_p \). Suppose

\[ \lambda_0 + \lambda_1 \alpha + \lambda_2 \alpha^2 + \lambda_3 \alpha^3 + \lambda_4 \beta = 0, \quad \lambda_j \in \mathbb{Z}_p, \ 0 \leq j \leq 4. \]

The rational solutions of (12) form a \( \mathbb{Z} \)-lattice of rank at most 1 (otherwise \( 1, \alpha, \alpha^2, \alpha^3 \) would be dependent over \( \mathbb{Q} \)). The \( p \)-adic solutions of (12) form a \( \mathbb{Z}_p \)-lattice of rank 4, with \( \mathbb{Z}_p \)-basis given by the columns

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Consider now the relation
\[ \lambda_0 + \lambda_1 \alpha + \lambda_2 \alpha^2 + \lambda_3 \alpha^3 + \lambda_4 \beta \equiv 0 \pmod{p^m}. \]
The rational solutions of (13) form a \( \mathbb{Z} \)-lattice \( L_m \) of rank 5, with \( \mathbb{Z} \)-basis given by the columns
\[
\begin{pmatrix}
\alpha & -\alpha^2 & -\alpha^3 & -\beta \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
\end{pmatrix}
\]
where \( \alpha, \beta \) are rational approximations to \( \alpha, \beta \), correct modulo \( p^m \). (\( \alpha \) and \( \beta \) are easily computed by Hensel-Newton lifting from roots modulo \( p \) of \( f \) and \( g \).)

If a nontrivial rational solution of (12) exists, it can be shown (see [6]) that for sufficiently large \( m \) it appears as a short vector in the lattice \( L_m \), and is therefore accessible via lattice basis reduction techniques (see [1, 7]).

It is known that the effectiveness of basis reduction depends upon, and is predictable from, the size of the entries. For these computations we found a choice of \( m \) such that \( p^m \approx 10^{25} \) to be effective.

7. Results

It should be noted to begin with, that our results are in complete agreement with the work of Godwin [4, 5]. The distribution of Galois groups by field discriminant appears in the appendix (cf. [1, 2]).

The main computations were done on a Digital Equipment VAX 8550 computer at the Computer Centre of Concordia University. Statistics for the totally real and totally complex cases (using the most recent versions of the software) are included for comparison. Execution times are expressed in CPU-hours.

Signature 0: 104:12 CPU-hours, 81322 fields.
Signature 2: 222:15 CPU-hours, 90671 fields.
Signature 4: 5:30 CPU-hours, 13073 fields.

The following data has been prepared for each of the fields (all signatures):
- generating polynomial
- field discriminant
- Galois group
- integral basis
- quadratic subfield discriminants (imprimitive fields only)
- fundamental units
- class group

The computation of fundamental units and class groups was done with KANT on Hewlett-Packard Apollo workstations at Düsseldorf. The data is available on magnetic media from the authors.
Appendix

Distribution of Galois groups by field discriminant

<table>
<thead>
<tr>
<th>Discriminant</th>
<th>$D_8$</th>
<th>$S_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-</td>
<td>193</td>
<td>822</td>
</tr>
<tr>
<td>20000-</td>
<td>190</td>
<td>1144</td>
</tr>
<tr>
<td>40000-</td>
<td>204</td>
<td>1236</td>
</tr>
<tr>
<td>60000-</td>
<td>186</td>
<td>1359</td>
</tr>
<tr>
<td>80000-</td>
<td>195</td>
<td>1355</td>
</tr>
<tr>
<td>100000-</td>
<td>187</td>
<td>1419</td>
</tr>
<tr>
<td>120000-</td>
<td>195</td>
<td>1402</td>
</tr>
<tr>
<td>140000-</td>
<td>212</td>
<td>1457</td>
</tr>
<tr>
<td>160000-</td>
<td>224</td>
<td>1544</td>
</tr>
<tr>
<td>180000-</td>
<td>181</td>
<td>1513</td>
</tr>
<tr>
<td>200000-</td>
<td>179</td>
<td>1534</td>
</tr>
<tr>
<td>220000-</td>
<td>179</td>
<td>1459</td>
</tr>
<tr>
<td>240000-</td>
<td>222</td>
<td>1531</td>
</tr>
<tr>
<td>260000-</td>
<td>196</td>
<td>1663</td>
</tr>
<tr>
<td>280000-</td>
<td>186</td>
<td>1582</td>
</tr>
<tr>
<td>300000-</td>
<td>209</td>
<td>1620</td>
</tr>
<tr>
<td>320000-</td>
<td>219</td>
<td>1505</td>
</tr>
<tr>
<td>340000-</td>
<td>190</td>
<td>1635</td>
</tr>
<tr>
<td>360000-</td>
<td>180</td>
<td>1636</td>
</tr>
<tr>
<td>380000-</td>
<td>190</td>
<td>1647</td>
</tr>
<tr>
<td>400000-</td>
<td>176</td>
<td>1634</td>
</tr>
<tr>
<td>420000-</td>
<td>197</td>
<td>1658</td>
</tr>
<tr>
<td>440000-</td>
<td>196</td>
<td>1649</td>
</tr>
<tr>
<td>460000-</td>
<td>188</td>
<td>1637</td>
</tr>
<tr>
<td>480000-</td>
<td>193</td>
<td>1628</td>
</tr>
<tr>
<td>500000-</td>
<td>214</td>
<td>1646</td>
</tr>
<tr>
<td>520000-</td>
<td>187</td>
<td>1708</td>
</tr>
<tr>
<td>540000-</td>
<td>196</td>
<td>1675</td>
</tr>
<tr>
<td>560000-</td>
<td>193</td>
<td>1733</td>
</tr>
<tr>
<td>580000-</td>
<td>196</td>
<td>1696</td>
</tr>
<tr>
<td>600000-</td>
<td>188</td>
<td>1764</td>
</tr>
<tr>
<td>620000-</td>
<td>194</td>
<td>1753</td>
</tr>
<tr>
<td>640000-</td>
<td>206</td>
<td>1726</td>
</tr>
<tr>
<td>660000-</td>
<td>200</td>
<td>1648</td>
</tr>
<tr>
<td>680000-</td>
<td>197</td>
<td>1745</td>
</tr>
<tr>
<td>700000-</td>
<td>201</td>
<td>1737</td>
</tr>
<tr>
<td>720000-</td>
<td>211</td>
<td>1762</td>
</tr>
<tr>
<td>740000-</td>
<td>185</td>
<td>1827</td>
</tr>
<tr>
<td>760000-</td>
<td>185</td>
<td>1799</td>
</tr>
<tr>
<td>780000-</td>
<td>195</td>
<td>1762</td>
</tr>
<tr>
<td>800000-</td>
<td>215</td>
<td>1726</td>
</tr>
<tr>
<td>820000-</td>
<td>226</td>
<td>1750</td>
</tr>
<tr>
<td>840000-</td>
<td>180</td>
<td>1740</td>
</tr>
<tr>
<td>860000-</td>
<td>213</td>
<td>1758</td>
</tr>
<tr>
<td>880000-</td>
<td>184</td>
<td>1810</td>
</tr>
<tr>
<td>900000-</td>
<td>188</td>
<td>1786</td>
</tr>
<tr>
<td>920000-</td>
<td>193</td>
<td>1719</td>
</tr>
<tr>
<td>940000-</td>
<td>198</td>
<td>1806</td>
</tr>
<tr>
<td>960000-</td>
<td>194</td>
<td>1749</td>
</tr>
<tr>
<td>980000-</td>
<td>178</td>
<td>1805</td>
</tr>
</tbody>
</table>

Total: 9772 80899
Percent: 10.78 89.22

Bibliography


**Fachbereich 10, Informatik, Universität des Saarlandes, Saarbrücken, Germany**

*E-mail address*: buchmann@cs.uni-sb.de

**Department of Computer Science, Concordia University, Montréal, Canada**

*E-mail address*: kbbfe24@vax2.concordia.ca

**Mathematisches Institut, Heinrich-Heine-Universität, Düsseldorf, Germany**

*E-mail address*: pohst@ze8.rz.uni-duesseldorf.de