MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 204
OCTOBER 1993, PAGES 873–879

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 $\mathcal{O}_F$, then there exists $\rho \in \mathcal{O}_F \setminus \mathbb{Z}$ such that*

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

where $\rho_1, \ldots, \rho_4$ are the conjugates of ρ, and, for $k \in \mathbb{Z}$,

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

We let ρ 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 ρ may be assumed to satisfy the following:

$$0 \le s \le 2, \tag{1}$$

$$\frac{s^2 - T_2(\rho)}{2} \le p \le \frac{s^2/2 + T_2(\rho)}{2}, \tag{2}$$

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).

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

$$\frac{-s^3+3sp-T_3(\rho)}{3} \le q \le \frac{-s^3+3sp+T_3(\rho)}{3}, \tag{3}$$

$$0 \le n \le \frac{T_2^2(\rho)}{16}. \tag{4}$$

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

$$\widehat{T}_{21}(d) = \lfloor 1+\sqrt[3]{|d|/2}\rfloor, \qquad \widehat{T}_3(d) = \lfloor (1+\sqrt[3]{|d|/2})^{3/2}\rfloor,$$
$$\widehat{T}_{22}(d) = \lfloor 2(1+\sqrt[3]{|d|/2})\rfloor, \qquad \widehat{T}_4(d) = \lfloor (1+\sqrt[3]{|d|/2})^2\rfloor,$$

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

$$0 \le s \le 2, \tag{5}$$

$$\frac{s^2-\widehat{T}_{21}(d)}{2} \le p \le \frac{s^2+\widehat{T}_{22}(d)}{4}, \tag{6}$$

$$\frac{-s^3+3sp-\widehat{T}_3(d)}{3} \le q \le \frac{-s^3+3sp+\widehat{T}_3(d)}{3}, \tag{7}$$

$$0 \le n \le \frac{\widehat{T}_4(d)}{16}. \tag{8}$$

The integer quantities $\widehat{T}_{21}(d)$, $\widehat{T}_{22}(d)$, $\widehat{T}_3(d)$, $\widehat{T}_4(d)$ are easy to compute, so the question of whether a given polynomial belongs to $G_1(d)$ can be answered quickly.

Observing that $\lfloor T_2(\rho)\rfloor \le \widehat{T}_{21}(d_F)$, $\lfloor 2T_2(\rho)\rfloor \le \widehat{T}_{22}(d_F)$, $\lfloor T_3(\rho)\rfloor \le \lfloor T_2(\rho)^{3/2}\rfloor \le \widehat{T}_3(d_F)$, $\lfloor T_2^2(\rho)\rfloor \le \widehat{T}_4(d_F)$ 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 $\rho \in \mathcal{O}_F\backslash\mathbb{Z}$ 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 $|d_F| \ge 10^6$, 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 ρ in Proposition 1 gives a quartic integer. In these fields every such "small" ρ 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 $\mathscr{O}_K = \mathbb{Z}[\omega]$ is the ring of integers of K.

We take $\rho \in \mathscr{O}_F \backslash \mathscr{O}_K$, and let

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

be the minimal polynomial of ρ over K, with

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

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

$$\begin{aligned} (9)\quad f(x) &= (x^2 - (a_1 + a_2\omega)x + (b_1 + b_2\omega))(x^2 - (a_1 + a_2\omega')x + (b_1 + b_2\omega')) \\ &= (x^2 - \alpha x + \beta)(x^2 - \alpha' x + \beta') \\ &= x^4 - sx^3 + px^2 - qx + n \in \mathbb{Z}[x]. \end{aligned}$$

We define the $\mathbb{Z}$-module homomorphism $\lambda : \mathscr{O}_F \longrightarrow \mathbb{R}^4$ by

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

where ξ_1, ξ_2, are the real conjugates of ξ, and ξ_3, $\overline{\xi}_3$ the complex conjugates. Then $\lambda(\mathscr{O}_F)$ is a 2-dimensional lattice of determinant $\Delta = \sqrt{|d_F|/8d_K}$, and the kernel of λ is $\mathscr{O}_K$. We choose $\rho \in \mathscr{O}_F$ so that $\|\lambda(\rho)\|^2 \le 2\Delta/\sqrt{3} = \sqrt{|d_F|/6d_K}$ and $\mathrm{Tr}_{F/K}(\rho) = \alpha \in \{0+\omega, 1+\omega, 0+2\omega, 1+2\omega\}$. (Taking $\alpha \notin \mathbb{Q}$ ensures that ρ has degree 4 over $\mathbb{Q}$.)

Since α and β are real, we have

$$\alpha = \rho_1 + \rho_2, \qquad \beta = \rho_1\rho_2,$$
$$\alpha' = \rho_3 + \overline{\rho}_3 = 2\Re\rho_3, \qquad \beta' = \rho_3\overline{\rho}_3, = |\rho_3|^2.$$

Therefore,

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

so that

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

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

$$\alpha^2 + \alpha'^2 = \tfrac{1}{2}A_1, \qquad \beta + \beta' = 2b_1 + b_2\sigma,$$
$$\alpha^2 - \alpha'^2 = A_2\sqrt{d_K}, \qquad \beta - \beta' = b_2\sqrt{d_K}.$$

It follows that

$$(10)\qquad \frac{A_2 - M}{4} \le b_2 \le \frac{A_2}{4},$$

$$(11)\qquad \frac{A_1 - 8b_2\sigma - N}{16} \le b_1 \le \frac{A_1 - 8b_2\sigma + N}{16},$$

where

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

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 $\rho \in \mathcal{O}_F \backslash \mathcal{O}_K$ 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 $\rho \in \mathcal{O}_F \backslash \mathbb{Z}$ 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 $f \notin G_2(d_F, d_K)$, 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 $\rho \in \mathcal{O}_F \backslash \mathbb{Z}$ 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 $\mathbb{Z}[x]$, α and β 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 α and β to lie in $\mathbb{Z}_p$. Suppose

$$\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\alpha^3 + \lambda_4\beta = 0, \qquad \lambda_j \in \mathbb{Z}_p,\ 0 \leq j \leq 4. \tag{12}$$

The rational solutions of (12) form a $\mathbb{Z}$-lattice of rank at most 1 (otherwise 1, α, α^2, α^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

$$\begin{array}{cccc} -\alpha & -\alpha^2 & -\alpha^3 & -\beta \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}$$

Consider now the relation

$$\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\alpha^3 + \lambda_4\beta \equiv 0 \pmod{p^m}. \tag{13}$$

The rational solutions of (13) form a $\mathbb{Z}$-lattice L_m of rank 5, with $\mathbb{Z}$-basis given by the columns

$$\begin{array}{ccccc} p^m & -\overline{\alpha} & -\overline{\alpha}^2 & -\overline{\alpha}^3 & -\overline{\beta} \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}$$

where $\overline{\alpha}$, $\overline{\beta}$ are rational approximations to α, β, correct modulo p^m. ($\overline{\alpha}$ and $\overline{\beta}$ 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

	D_8	S_4
0:	193	822
20000:	190	1144
40000:	204	1236
60000:	186	1359
80000:	195	1355
100000:	187	1419
120000:	195	1402
140000:	212	1457
160000:	224	1544
180000:	181	1513
200000:	179	1534
220000:	179	1459
240000:	222	1531
260000:	195	1663
280000:	186	1582
300000:	209	1620
320000:	219	1505
340000:	190	1635
360000:	180	1636
380000:	190	1647
400000:	176	1634
420000:	197	1658
440000:	195	1649
460000:	188	1637
480000:	193	1628
500000:	214	1646
520000:	187	1708
540000:	196	1675
560000:	193	1733
580000:	196	1696
600000:	188	1764
620000:	184	1753
640000:	206	1726
660000:	200	1648
680000:	197	1745
700000:	201	1737
720000:	211	1762
740000:	185	1827
760000:	185	1799
780000:	195	1762
800000:	215	1726
820000:	226	1750
840000:	180	1740
860000:	213	1758
880000:	184	1810
900000:	188	1786
920000:	193	1719
940000:	198	1806
960000:	194	1749
980000:	178	1805
Total:	9772	80899
Percent:	10.78	89.22

BIBLIOGRAPHY

1. J. Buchmann and D. Ford, *On the computation of totally real quartic fields of small discriminant*, Math. Comp. **52** (1989), 161–174.
2. D. Ford, *Enumeration of totally complex quartic fields of small discriminant*, Computational Number Theory, Proceedings of the Colloquium on Computational Number Theory, Debrecen (Hungary), 1989 (A. Pethö, M. Pohst, H. C. Williams, and H. G. Zimmer, eds.), de Gruyter, Berlin and New York, 1991, pp. 129–138.
3. I. Gerst and J. Brillhart, *On the prime divisors of a polynomial*, Amer. Math. Monthly **78** (1971), 250–266.

4. H. J. Godwin, *On quartic fields of signature one with small discriminant*, Quart. J. Math. Oxford Ser. (2) **8** (1957), 214–222.
5. ———, *On quartic fields of signature one with small discriminant.* II, Math. Comp. **42** (1984), 707–711.
6. A. K. Lenstra, *Lattices and factorization of polynomials over algebraic number fields,* Proceedings Eurocam 82, Lecture Notes in Comput. Sci., vol. 144, Springer, Berlin, 1982, pp. 32–39.
7. A. K. Lenstra, H. W. Lenstra Jr., and L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.
8. M. Pohst, *On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields*, J. Number Theory **14** (1982), 99–117.
9. ———, *On computing isomorphisms of equation orders*, Math. Comp. **48** (1987), 309–314.
10. I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, S.-B. Berlin Math. Ges. **11** (1912), 40–50.

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: kbkfe24@vax2.concordia.ca

MATHEMATISCHES INSTITUT, HEINRICH-HEINE-UNIVERSITÄT, DÜSSELDORF, GERMANY
E-mail address: pohst@ze8.rz.uni-duesseldorf.de