Journal de Théorie des Nombres
de Bordeaux **13** (2001), 137–142

Computing all monogeneous mixed dihedral quartic extensions of a quadratic field

par István GAÁL* et Gábor NYUL

Résumé. Soit M un corps quadratique réel. Nous donnons un algorithme rapide pour déterminer tous les corps quartiques diédraux K avec signature mixte, monogènes (*i.e.* ayant des bases d'entiers $\{1, \alpha, \alpha^2, \alpha^3\}$) et contenant M comme sous-corps. Nous déterminons également tous les générateurs α des bases dans K ayant cette forme. Notre algorithme combine un résultat récent de Kable [9] avec l'algorithme de Gaál, de Pethő et de Pohst [6], [7]. On applique la méthode à $M = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$.

Abstract. Let M be a given real quadratic field. We give a fast algorithm for determining all dihedral quartic fields K with mixed signature having *power integral bases* and containing M as a subfield. We also determine all generators of power integral bases in K. Our algorithm combines a recent result of Kable [9] with the algorithm of Gaál, Pethő and Pohst [6], [7]. To illustrate the method we performed computations for $M = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5})$.

1. Introduction

It is a classical problem of algebraic number theory to decide if a number field N of degree n admits *power integral bases*, that is integral bases of the form $\{1, \alpha, \dots, \alpha^{n-1}\}$ and, if yes, to determine all possible generators of these bases. In case there exist power integral bases in N, the field is called *monogeneous*.

In a recent paper Kable [9] studied quartic fields K with dihedral Galois group, having power integral basis. These fields have a unique quadratic subfield M. In the following the discriminants of K and M will be denoted by D_K and D_M, respectively.

The main theorem of [9] gives necessary and sufficient conditions for K containing the subfield M to have a power integral basis. The condition is general but does not allow us to settle the problem of existence of power

Manuscrit reçu le 28 septembre 1999.
*Research supported in part by Grants 16975 and 25157 from the Hungarian National Foundation for Scientific Research by FKFP 0343/2000.

integral bases in K without further analysis. The result has two important consequences.

Lemma 1 ([9, Corollary 1]). *Let K be a dihedral quartic field containing the quadratic subfield M. If K has a power integral basis, then, with a suitable choice of sign, $D_K \pm 4D_M^3$ is a square.*

In the special case of dihedral quartic fields with mixed signature the discriminant is negative and the quadratic subfield is real. Hence

Lemma 2 ([9, Corollary 2]). *Let K be a mixed dihedral quartic field containing the quadratic subfield M. If K has a power integral basis, then $|D_K| \leq 4D_M^3$. In particular there are only finitely many mixed dihedral quartic fields having a power integral basis and containing a given real quadratic subfield.*

Hence, for a given totally real quadratic field M we can enumerate all mixed dihedral quartic fields K satisfying the inequality

$$|D_K| \leq 4D_M^3 \tag{1}$$

and then we can select those fields K containing M as subfield and having power integral bases. This way we can determine all mixed dihedral quartic fields K having power integral bases and containing the given real quadratic field M as a subfield. This is the purpose of the present paper.

2. Power integral bases in quartic fields

For a given quartic field K there are efficient methods for determining all power integral bases, cf. Gaál, Pethő and Pohst [3], [4], [5], [8]. A general fast method is described in [6], [7].

Assume that K is generated by an algebraic integer ξ over $\mathbb{Q}$. Let $f(t) = t^4 + a_1t^3 + a_2t^2 + a_3t + a_4 \in \mathbb{Z}[t]$ be the minimal polynomial of ξ. Let $n = I(\xi) = (\mathbb{Z}_K^+ : \mathbb{Z}[\xi]^+)$ be the index of ξ. We can represent any integer α in K in the form

$$\alpha = \frac{a + x\xi + y\xi^2 + z\xi^3}{d} \tag{2}$$

with $a, x, y, z \in \mathbb{Z}$ where $d \in \mathbb{Z}$ is a fixed common denominator. Note that $n | d^3$.

Lemma 3 ([6, Theorem 2.1]). *The element α of (2) generates a power integral basis in K if and only if there is a solution $(u, v) \in \mathbb{Z}^2$ of the cubic equation*

$$F(u,v) = \tag{3}$$

$$u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3 = \pm\frac{d^6}{n}$$

such that (x, y, z) of (2) satisfies

$$
\begin{aligned}
Q_1(x,y,z) &= x^2 - a_1xy + a_2y^2 + (a_1^2 - 2a_2)xz + (a_3 - a_1a_2)yz \\
&\quad +(-a_1a_3 + a_2^2 + a_4)z^2 = u \ , \\
Q_2(x,y,z) &= y^2 - xz - a_1yz + a_2z^2 = v \ . \qquad (4)
\end{aligned}
$$

According to the above remark the right hand side of (3) is an integer. If the form $F(u, v)$ is reducible, then (3) is trivial to solve, otherwise it is a cubic Thue equation.

For every solution (u, v) of (3) we have to determine the corresponding solutions (x, y, z) of (4). We follow the algorithm of [7]. Denote by (x_Q, y_Q, z_Q) a non-trivial solution of

$$Q_0(X, Y, Z) = uQ_2(X, Y, Z) - vQ_1(X, Y, Z) = 0.$$

If $z_Q \neq 0$ (the other cases are treated similarly), then there are rational parameters p, q, r such that

$$x = rx_Q + p, \quad y = ry_Q + q, \quad z = rz_Q. \qquad (5)$$

Since any solution (x, y, z) of (4) satisfies $Q_0(x, y, z) = 0$ we get $r(c_1p + c_2q) = c_3p^2 + c_4pq + c_5q^2$ with integers $c_1, \ldots, c_5$ which are easily calculated. Multiply (5) by $(c_1p + c_2q)$ and use the above relation to eliminate r. In addition, multiply these equations with the square of the common denominator of p, q to get integer relations, and then divide the equations by $\gcd(p, q)^2$. This way we obtain

$$
\begin{aligned}
k \cdot x = \ & f_x(p,q) = \ c_{11}p^2 + c_{12}pq + c_{13}q^2, \\
k \cdot y = \ & f_y(p,q) = \ c_{21}p^2 + c_{22}pq + c_{23}q^2, \qquad (6) \\
k \cdot z = \ & f_z(p,q) = \ c_{31}p^2 + c_{32}pq + c_{33}q^2,
\end{aligned}
$$

where $k > 0, c_{ij}$ are integers and the parameters $p, q \in \mathbb{Z}$ are coprime. By [7] k must divide $\det(c_{ij})/\gcd\{c_{ij}\}^3$ which is usually a small integer, allowing just a few possibilities for k. For each k we substitute the representations (6) into (4) to get

$$F_1(p,q) = Q_1(f_x(p,q), f_y(p,q), f_z(p,q)) = k^2u \ , \qquad (7)$$

$$F_2(p,q) = Q_2(f_x(p,q), f_y(p,q), f_z(p,q)) = k^2v \ . \qquad (8)$$

By [7] at least one of these equations is a Thue equation over the original field K. Solving this equation we can determine p, q and by (6) the corresponding values of x, y, z.

Thus in general to determine all generators of power integral bases in K we have to solve a cubic and some corresponding quartic Thue equations. This can easily be done using the method of Bilu and Hanrot [1] which is already implemented in KASH [2]. Note that in our case for dihedral quartic fields K the form $F(u, v)$ is always a product of a linear and a quadratic form (cf. Kappe and Warren [10, Theorem 1]) and the resolution of (3) is trivial.

3. The algorithm

input: a real quadratic field M
output: all those mixed dihedral quartic fields K, that have power integral bases and contain M as a subfield. Moreover all possible generators of power integral bases in K are computed.

1. Determine all those mixed quartic fields, the discriminant of which satisfies (1).

   (This can be done by using the tables computed by KASH [2]. Note that by $M \subset K$ and (1) we have

   $$D_M^2 | D_K, \qquad D_M^2 \le |D_K| \le 4D_M^3 ,$$

   hence there are relatively few candidates for K.)
2. Calculate the Galois groups and subfields of the candidate fields K. We keep only those quartic fields K which have dihedral Galois group and contain M as a subfield.

   (This is done again by using KASH.)
3. Determine all possible generators of power integral bases of K. We drop the candidates K having no power integral bases.

   (Use the methods of Gaál, Pethő and Pohst [6], [7], along the lines of Section 2. As we noticed already at the end of Section 2, equation (3) is trivially solved for dihedral fields. For the resolution of (7), (8) we used KASH.)

4. Numerical examples

To illustrate our algorithm we performed computations for $M = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$. The following table contains the results of our computation. For each of these quadratic fields M we list the discriminants D_K of the mixed dihedral quartic fields K containing M as a subfield and having power integral bases. For each discriminant we display the minimal polynomial $f(t)$ of the generating element ξ of K, the common denominator d of (2) and the coordinates (x, y, z) of the α in (2) generating power integral bases.

At some fields *no solutions* means that the field is a mixed dihedral quartic field containing M as a subfield, but having no power integral bases.

The method was implemented in Maple, the quartic Thue equations (7), (8) were solved by KASH. The CPU time was a few minutes for every quartic field.

$M = \mathbb{Q}(\sqrt{2})$

$D_K = -448, f(t) = t^4 - 2t^3 + t^2 + 2t - 1, d = 1$
$(x, y, z) = (0, 1, -1), (1, -6, 4), (4, -3, 1), (1, 0, 0), (1, -2, 1)$

$D_K = -1024, f(t) = t^4 - 2t^2 - 1, d = 1$
$(x, y, z) = (1, 0, 0), (2, 0, -1)$

$D_K = -1472, f(t) = t^4 - 2t^3 - 3t^2 - 2t - 1, d = 1$
$(x, y, z) = (1, 0, 0), (0, 3, -1), (3, 2, -1)$

$D_K = -1792, f(t) = t^4 - 2t^2 - 4t - 2, d = 1$
$(x, y, z) = (1, 0, 0), (1, 1, -1)$

$D_K = -1984, f(t) = t^4 - 2t^3 + t^2 - 2, d = 1$
$(x, y, z) = (1, 0, 0)$

$D_K = -2048, f(t) = t^4 - 2, d = 1$
$(x, y, z) = (1, 0, 0), (1, 1, 1), (1, -1, 1)$

$M = \mathbb{Q}(\sqrt{3})$

$D_K = -1728, f(t) = t^4 - 2t^3 - 2t + 1, d = 1$
$(x, y, z) = (1, 0, 0), (0, 2, -1)$

$D_K = -3312, f(t) = t^4 - 2t^3 - t^2 + 2t - 2, d = 1$
$(x, y, z) = (1, 0, 0)$

$D_K = -3312, f(t) = t^4 + t^2 - 6t + 1, d = 3$
no solutions

$D_K = -4608, f(t) = t^4 + 2t^2 - 2, d = 1$
$(x, y, z) = (1, 0, 0), (3, 1, 1), (3, -1, 1)$

$D_K = -4608, f(t) = t^4 - 2t^2 - 2, d = 1$
$(x, y, z) = (1, 0, 0)$

$D_K = -5616, f(t) = t^4 - 3t^2 - 6t - 3, d = 1$
$(x, y, z) = (2, 1, -1), (1, 0, 0)$

$D_K = -5616, f(t) = t^4 - 2t^3 + 3t^2 - 2t - 2, d = 1$
$(x, y, z) = (1, 0, 0), (17, -10, 4), (9, -2, 4)$

$D_K = -6336, f(t) = t^4 - 2t^3 - 4t^2 - 4t - 2, d = 1$
$(x, y, z) = (1, 0, 0), (1, 3, -1)$

$D_K = -6336, f(t) = t^4 - 2t^3 - 8t^2 - 6t - 3, d = 3$
no solutions

$D_K = -6768, f(t) = t^4 - 2t^3 + t^2 - 3, d = 1$
$(x, y, z) = (1, 0, 0), (1, 0, 1), (4, -3, 1)$

$D_K = -6768, f(t) = t^4 - t^2 - 6t - 2, d = 2$
$(x, y, z) = (2, 1, -2), (2, -1, 0), (2, 1, 0), (1, 1, -1)$

$D_K = -6912, f(t) = t^4 - 3, d = 1$
$(x, y, z) = (1, 0, 0)$

$M = \mathbb{Q}(\sqrt{5})$

$D_K = -275, f(t) = t^4 - t^3 + 2t - 1, d = 1$

$(x, y, z) = (0, 0, 1), (1, 0, 0), (2, -2, 1), (1, 2, -4), (0, 1, -1)$

$D_K = -400, f(t) = t^4 - t^2 - 1, d = 1$

$(x, y, z) = (1, 0, 0), (0, 1, 1), (1, 0, -1), (0, 1, -1)$

$D_K = -475, f(t) = t^4 - t^3 - 2t^2 - 2t - 1, d = 1$

$(x, y, z) = (1, 0, 0), (0, 2, -1), (2, 1, -1)$

References

[1] Y. BILU, G. HANROT, *Solving Thue equations of high degree.* J. Number Theory **60** (1996), 373–392.

[2] M. DABERKOW, C. FIEKER, J. KLÜNERS, M. POHST, K. ROEGNER, K. WILDANGER, *KANT V4.* J. Symbolic Comp. **24** (1997), 267–283.

[3] I. GAÁL, A. PETHŐ, M. POHST, *On the resolution of index form equations in biquadratic number fields, I.* J. Number Theory **38** (1991), 18–34.

[4] I. GAÁL, A. PETHŐ, M. POHST, *On the resolution of index form equations in biquadratic number fields, II.* J. Number Theory **38** (1991), 35–51.

[5] I. GAÁL, A. PETHŐ, M. POHST, *On the resolution of index form equations in biquadratic number fields, III. The bicyclic biquadratic case.* J. Number Theory **53** (1995), 100–114.

[6] I. GAÁL, A. PETHŐ, M. POHST, *On the resolution of index form equations in quartic number fields.* J. Symbolic Computation **16** (1993), 563–584.

[7] I. GAÁL, A. PETHŐ, M. POHST, *Simultaneous representation of integers by a pair of ternary quadratic forms – with an application to index form equations in quartic number fields.* J. Number Theory **57** (1996), 90–104.

[8] I. GAÁL, A. PETHŐ, M. POHST, *On the resolution of index form equations in dihedral number fields.* J. Experimental Math. **3** (1994), 245–254.

[9] A.C. KABLE, *Power integral bases in dihedral quartic fields.* J. Number Theory **76** (1999), 120–129.

[10] L.C. KAPPE, B. WARREN, *An elementary test for the Galois group of a quartic polynomial.* Amer. Math. Monthly **96** (1989), 133–137.

István GAÁL, Gábor NYUL
University of Debrecen
Mathematical Institute
H–4010 Debrecen Pf.12.
Hungary
E-mail : igaal@math.klte.hu
gnyul@dragon.klte.hu