Power Integral Bases in the Family of Simplest Quartic Fields

Péter Olajos

CONTENTS

Several authors have considered the infinite parametric family of simplest quartic fields $K_t = \mathbb{Q}(\xi)$. In this paper, we explicitly give all generators of power integral bases in the ring of integers $\mathbb{Z}_K$ of K_t assuming that t^2+16 is not divisible by an odd square. We use a well known general algorithm for calculating power integral bases in quartic fields.

1. INTRODUCTION

Consider an algebraic number field K of degree n with ring of integers $\mathbb{Z}_K$ and discriminant D_K. An interesting problem in algebraic number theory is to decide if there exist integral bases of type $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$, i.e., *power integral bases*, and to find all elements α with this property.

The index of a primitive element $\alpha \in \mathbb{Z}_K$ is defined as $I(\alpha) = (\mathbb{Z}_K^+ : \mathbb{Z}^+[\alpha])$.

As it is well known, α generates a power integral basis if and only if $I(\alpha) = 1$.

Let $\{1, \omega_2, ..., \omega_n\}$ be an arbitrary integral basis of K. Then, the discriminant of the linear form $l(\underline{x}) = x_1 + x_2\omega_2 + ... + x_n\omega_n$ is equal to

$$D_{K/\mathbb{Q}}(l(\underline{x})) = \prod_{1 \le i < j \le n} (l^{(i)}(\underline{x}) - l^{(j)}(\underline{x}))^2 = I(x_2, ..., x_n)^2 D_K,$$

where $I(x_2, ..., x_n)$ is *the index form* corresponding to the integral basis $\{1, \omega_2, ..., \omega_n\}$.

Obviously $\alpha = x_1 + \omega_2 x_2 + ... + \omega_n x_n \in \mathbb{Z}_K$ has index 1 if and only if

$$I(x_2, ..., x_n) = \pm 1 \ (x_2, \ldots, x_n \in \mathbb{Z}). \qquad (1\text{–}1)$$

K. Győry [Győry 76] gave the first effective upper bounds for the solutions of index form equations using Baker's method. In the last decade, several algorithms were constructed for solving certain types of index form

2000 AMS Subject Classification: Primary 11D57; Secondary 11Y50

Keywords: power integral bases, simplest quartic fields, index form equations

1058-6458/2005$0.50 per page

equations. For details and several connected results see I. Gaál [Gaál 02].

The purpose of the present paper is to give all generators of power integral bases in the family of simplest quartic fields using the result of H. K. Kim and J. S. Kim [Kim and Kim 03] on integral bases of these fields and the procedure of I. Gaál, A. Pethő, and M. Pohst [Gaál et al. 93] for calculating power integral bases in quartic fields.

2. SIMPLEST QUARTIC FIELDS

For $t \in \mathbb{Z} \setminus \{0, \pm 3\}$ let

$$P_t(x) = x^4 - tx^3 - 6x^2 + tx + 1. \tag{2–1}$$

Let $\xi = \xi_t$ be a root of $P_t(x)$, then each field in the infinite parametric family of number fields $K_t = K = \mathbb{Q}(\xi)$ is called a *simplest quartic field*. The simplest quartic field K is a totally real cyclic number field of degree 4. If $t = 0$ or $t = \pm 3$ then $P_t(x)$ is reducible over $\mathbb{Q}$, see M. N. Gras [Gras 77/78].

Power integral bases in the polynomial order $\mathbb{Z}[\xi_t]$ of K_t were described by G. Lettl and A. Pethő [Lettl and Pethő 95]. For finding all generators of power integral bases in the ring of integers of the simplest quartic fields we need the following lemma.

Note that $\mathbb{Q}(\alpha) = \mathbb{Q}(-\alpha)$ (α an algebraic integer), that is we can assume that $t > 0$ and $t \neq 3$. In the following, we also assume that t^2+16 is not divisible by an odd square. Further, denote by $v_2(t)$ the 2-adic valuation of t. Recently, the integral basis of K was explicitly given.

Lemma 2.1. [Kim and Kim 03] An integral basis of $K = K_t$ is given as follows.

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}[1, \xi, \xi^2, \frac{1+\xi^3}{2}] & \text{if } v_2(t) = 0, \\ \mathbb{Z}[1, \xi, \frac{1+\xi^2}{2}, \frac{\xi+\xi^3}{2}] & \text{if } v_2(t) = 1, \\ \mathbb{Z}[1, \xi, \frac{1+\xi^2}{2}, \frac{1+\xi+\xi^2+\xi^3}{4}] & \text{if } v_2(t) = 2, \\ \mathbb{Z}[1, \xi, \frac{1+2\xi-\xi^2}{4}, \frac{1+\xi+\xi^2+\xi^3}{4}] & \text{if } v_2(t) \geq 3. \end{cases}$$

The main result of our paper is the following theorem.

Theorem 2.2. *The ring of integers $\mathbb{Z}_K$ of the simplest quartic field $K = K_t$ (where $t^2 + 16$ is not divisible by an odd square) admits power integral bases only for $t = 2$ and $t = 4$. In these cases, all generators of power integral bases are the following:*

- $t = 2$, $\alpha = x \cdot \xi + y \cdot \frac{1+\xi^2}{2} + z \cdot \frac{\xi+\xi^3}{2}$, *where* $(x, y, z) = (4, 2, -1)$, $(-13, -9, 4)$, $(-2, 1, 0)$, $(1, 1, 0)$, $(-8, -3, 2)$, $(-12, -4, 3)$, $(0, -4, 1)$, $(6, 5, -2)$, $(-1, 1, 0)$, $(0, 1, 0)$; *and*
- $t = 4$, $\alpha = x \cdot \xi + y \cdot \frac{1+\xi^2}{2} + z \cdot \frac{1+\xi+\xi^2+\xi^3}{4}$, *where* $(x, y, z) = (3, 2, -1)$, $(-2, -2, 1)$, $(4, 8, -3)$, $(-6, -7, 3)$, $(0, 3, -1)$, $(1, 3, -1)$.

3. PROOF OF THEOREM 2.2

Let $t \in \mathbb{Z}^+ \setminus \{3\}$, $\xi = \xi_t$ be a root of $P_t(x)$ in (2–1), $K = K_t = \mathbb{Q}(\xi)$ be a simplest quartic field, and let $\{1, \omega_2, \omega_3, \omega_4\}$ be an integral basis of K as in Lemma 2.1. For simplicity, we omit t, but all the formulas implicitly depend on t. Let $I(x, y, z)$ be the index form corresponding to the integral basis $\{1, \omega_2, \omega_3, \omega_4\}$. Assume that $\alpha = x_0\omega_2 + y_0\omega_3 + z_0\omega_4$ has index 1, i.e., $I(x_0, y_0, z_0) = \pm 1$. We can represent α in the form

$$\alpha = \frac{a + x_1\xi + y_1\xi^2 + z_1\xi^3}{g}.$$

Note that this implies a one-to-one correspondence between (x_0, y_0, z_0) and (x_1, y_1, z_1). Set

$$\begin{aligned} F(u, v) &= u^3 + 6u^2v + (-t^2 - 4)uv^2 \\ &\quad + (-24 - 2t^2)v^3 \\ &= (u + 2v)(u^2 + 4uv - v^2t^2 - 12v^2), \\ Q_1(x_1, y_1, z_1) &= x_1^2 + tx_1y_1 - 6y_1^2 + (t^2 + 12)x_1z_1 \\ &\quad - 5ty_1z_1 + (t^2 + 37)z_1^2, \\ Q_2(x_1, y_1, z_1) &= y_1^2 - x_1z_1 + ty_1z_1 - 6z_1^2. \end{aligned}$$

By I. Gaál, A. Pethő and M. Pohst [Gaál et al. 93, Gaál et al. 96] (see also [Gaál 02]) there is a $(u, v) \in \mathbb{Z}^2$ with

$$F(u, v) = \pm\frac{g^6}{I(\xi)} = i,$$

such that $Q_1(x_1, y_1, z_1) = u$ and $Q_2(x_1, y_1, z_1) = v$.

According to Lemma 2.1 we have to consider the following cases.

Case I. Set $\{1, \omega_2, \omega_3, \omega_4\} = \{1, \xi, \xi^2, \frac{1+\xi^3}{2}\}$ and $v_2(t) = 0$.

In this case, $g = 2$ and $I(\xi) = 2$, i.e., $i = \pm 2^5 = 32$. Using the factorization of $F(u, v)$ we have the following solutions (t, u, v) to equation $F(u, v) = i$: $(t, u, v) = (1, \mp 12, \pm 2), (1, \pm 4, \pm 2), (5, \pm 22, \pm 5), (5, \pm 42, \mp 5)$.

Case II. Set $\{1, \omega_2, \omega_3, \omega_4\} = \{1, \xi, \frac{1+\xi^2}{2}, \frac{\xi+\xi^3}{2}\}$ and $v_2(t) = 1$.

u	v	p	q	k	x_1	y_1	z_1	x_0	y_0	z_0
2	1	±1	0	±1	±59	±31	∓7	±4	±2	∓1
2	1	±6	∓1	±4	±22	±9	∓4	±13	±9	∓4
2	1	±4	∓1	±4	±4	∓1	0	±2	∓1	0
2	1	±2	±1	±4	±2	±1	0	±1	±1	0
2	1	0	±1	±4	±14	±3	∓2	±8	±3	∓2
2	1	±4	0	±16	±59	±31	∓7	±4	±2	∓1
2	1	±12	∓2	±16	±22	±9	∓4	±13	±9	∓4
2	1	±8	∓2	±16	±4	∓1	0	±2	∓1	0
2	1	±4	±2	±16	±2	±1	0	±1	±1	0
2	1	0	±2	±16	±14	±3	∓2	±8	±3	∓2

TABLE 1. Solutions in Case II.

In this case, $g = 2$ and $I(\xi) = 4$, i.e., $i = \pm 2^4 = 16$. Using similar calculations as above, we have solutions (t, u, v) to equation $F(u, v) = i$: $(t, u, v) = (2, \pm2, \pm1), (2, \pm6, \mp1)$.

Case III. $\{1, \omega_2, \omega_3, \omega_4\} = \{1, \xi, \frac{1+\xi^2}{2}, \frac{1+\xi+\xi^2+\xi^3}{4}\}$ and $v_2(t) = 2$.

In this case, $g = 4$ and $I(\xi) = 8$, i.e., $i = \pm 2^9 = 512$. Using similar calculations as above, we have for solutions (t, u, v) to equation $F(u, v) = i$: $(t, u, v) = (4, \pm4, \pm2)$, $(4, \pm12, \mp2)$, $(4, \pm10, \pm3)$, $(4, \pm22, \mp3)$, $(t, \pm8, 0)$.

Case IV. $\{1, \omega_2, \omega_3, \omega_4\} = \{1, \xi, \frac{1+2\xi-\xi^2}{4}, \frac{1+\xi+\xi^2+\xi^3}{4}\}$ and $v_2(t) \geq 3$.

In this case, $g = 4$ and $I(\xi) = 16$, i.e., $i = \pm 2^8 = 256$. Using similar calculations as above, we have solutions (t, u, v) to equation $F(u, v) = i$: $(t, u, v) = (8, \pm2, \pm1)$, $(8, \pm6, \mp1)$, $(16, \pm14, \pm1)$, $(16, \pm18, \mp1)$.

For all solutions $(u, v) \in \mathbb{Z}^2$ to $F(u, v) = i$, we solve the system of equations $Q_1(x_1, y_1, z_1) = u$, $Q_2(x_1, y_1, z_1) = v$ is solved in (x_1, y_1, z_1) by using similar calculations and applying the ideas in [Gaál et al. 96]. We obtain that, in each case the equation $Q_2(p, q) = k^2 \cdot v$ is equal to a constant multiple of the equation $Q_1(p, q) = k^2 \cdot u$, where $k \in \mathbb{Z}^+$ is divisor of certain coefficients.

To give a sense of these calculations we detail two characteristic examples from the previous cases.

Case II. $(t, u, v) = (2, \pm2, \pm1)$. Solving equation

$$\begin{aligned} Q_1(p, q) &= 2(p^4 + 8p^3q + 4p^2q^2 - 48pq^3 + 16q^4) \\ &= k^2 \cdot u \end{aligned}$$

as a Thue equation, using Kash [Daberkow et al. 97] for all k with $k|16$, we find the solutions $(p, q) \in Z^2$ listed in Table 1. The table also contains the corresponding $(x_1, y_1, z_1) \in \mathbb{Z}^3$ and $(x_0, y_0, z_0) \in \mathbb{Z}^3$. Note that in the present case, there are always suitable solutions (x_0, y_0, z_0) to $I(x_0, y_0, z_0) = \pm1$ that correspond to (x_1, y_1, z_1).

Among the possible solutions (t, u, v) to $F(u, v) = i$, listed in Cases I–IV, there is a special one, namely, in Case III, $(u, v) = (\pm8, 0)$ is a solution for any $t \in \mathbb{Z}$.

Case III. $(t, u, v) = (t, \pm8, 0)$. In this case the equation

$$\begin{aligned} Q_1(p, q) &= 64(p^4 - tp^3q - 6p^2q^2 + tpq^3 + q^4) \\ &= k^2 \cdot u, \end{aligned} \tag{3–1}$$

(where $k \in \mathbb{Z}$ with $k|8$) is a parametric Thue equation in $(p, q) \in \mathbb{Z}^2$. If $k^2 = 1$ or $k^2 = 4$, then there are no solutions (p, q) to Equation (3–1).

If $k^2 = 16$, then we have to solve the equation

$$p^4 - tp^3q - 6p^2q^2 + tpq^3 + q^4 = \pm2, \tag{3–2}$$

and if $k^2 = 64$, then we have to solve the equation

$$p^4 - tp^3q - 6p^2q^2 + tpq^3 + q^4 = \pm8. \tag{3–3}$$

If we consider Equations (3–2) and (3–3) modulo 2 (and repeat the process a few times), then it is easily seen that these equations have no solutions in (p, q).

ACKNOWLEDGMENTS

The author was supported in part by Grant T-037367 from the Hungarian National Foundation for Scientific Research and by the Netherlands Organization for Scientific Research.

REFERENCES

[Daberkow et al. 97] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, and K. Wildanger. "KANT V4." *J. Symbolic Comp.* 24 (1997), 267–283.

[Gaál 02] I. Gaál. *Diophantine Equations and Power Integral Bases.* Boston: Birkhäuser, 2002.

[Gaál et al. 93] I. Gaál, A. Pethő, and M. Pohst. "On the Resolution of Index Form Equations in Quartic Number Fields." *J. Symbolic Comput.* 16 (1993), 563–584.

[Gaál et al. 96] I. Gaál, A. Pethő, and M. Pohst. "Simultaneous Representation of Integers by a Pair of Ternary Quadratic Forms—With an Application to Index Form Eqautions in Quadratic Number Fields." *J. Number Theory* 57 (1996), 90–104.

[Gras 77/78] M. N. Gras. "Table numerique du nombre de classes et des unites des extensions cycliques reelles de degré 4 in $\mathbb{Q}$." *Publ. Math. Fac. Sci. Besançon* (1977-1978) fasc. 2.

[Győry 76] K. Győry. "Sur les polynômes à coefficients entiers et de discriminant donné, III." *Publ. Math. (Debrecen)* 23 (1976), 141–165.

[Kim and Kim 03] H. K. Kim and J. S. Kim. "Computation of the Different of the Simplest Quartic Fields." Manuscript, 2003.

[Lettl and Pethő 95] G. Lettl and A. Pethő. "Complete Solution of a Family of Quartic Thue Equations." *Abh. Math. Sem. Univ. Hamburg* 65 (1995), 365–383.

Péter Olajos, Eszterházy Károly College, Institute of Mathematics and Informatics, H–3300 Eger, Eszterházy tér 1, Hungary (olaj@ektf.hu)

Received March 2, 2004; accepted in revised form January 18, 2005.