MATHEMATICS OF COMPUTATION
Volume 66, Number 220, October 1997, Pages 1689–1696
S 0025-5718(97)00868-5

POWER INTEGRAL BASES IN A PARAMETRIC FAMILY OF TOTALLY REAL CYCLIC QUINTICS

ISTVÁN GAÁL AND MICHAEL POHST

ABSTRACT. We consider the totally real cyclic quintic fields $K_n = \mathbb{Q}(\vartheta_n)$, generated by a root ϑ_n of the polynomial

$$f_n(x) = x^5 + n^2x^4 - (2n^3 + 6n^2 + 10n + 10)x^3 + (n^4 + 5n^3 + 11n^2 + 15n + 5)x^2 + (n^3 + 4n^2 + 10n + 10)x + 1.$$

Assuming that $m = n^4 + 5n^3 + 15n^2 + 25n + 25$ is square free, we compute explicitly an integral basis and a set of fundamental units of K_n and prove that K_n has a power integral basis only for $n = -1, -2$. For $n = -1, -2$ (both values presenting the same field) all generators of power integral bases are computed.

INTRODUCTION

Let $n \in \mathbb{Z}$ and denote by ϑ_n a root of the polynomial

$$f_n(x) = x^5 + n^2x^4 - (2n^3 + 6n^2 + 10n + 10)x^3 + (n^4 + 5n^3 + 11n^2 + 15n + 5)x^2 + (n^3 + 4n^2 + 10n + 10)x + 1. \tag{1}$$

These polynomials were discussed by Emma Lehmer (cf. [8]). The corresponding parametric family of cyclic quintic fields $K_n = \mathbb{Q}(\vartheta_n)$, ϑ_n a root of f_n, was also investigated by Schoof and Washington [10] and Darmon [2] for prime conductors $m = n^4 + 5n^3 + 15n^2 + 25n + 25$.

Assuming only that $m = n^4+5n^3+15n^2+25n+25$ is square free, we describe an integral basis and a set of fundamental units of the field $K_n = \mathbb{Q}(\vartheta_n)$. We construct explicitly the index form corresponding to that integral basis. The coefficients in the integral basis of those $\xi \in K_n$ generating a **power integral basis** $\{1, \xi, \xi^2, \xi^3, \xi^4\}$ of K_n can be obtained as solutions of the index form equation. The index form equation reduces to a unit equation in two variables over K_n. By using congruence considerations modulo m we show, that this unit equation is only solvable for $n = -1, -2$.

For $n = -1, -2$ the fields K_n coincide. This field indeed admits power integral bases, generated e.g. by the roots of the polynomial f_n. In fact in this case there

Received by the editor August 13, 1996.
1991 *Mathematics Subject Classification.* Primary 11Y50; Secondary 11Y40, 11D57.
Key words and phrases. Power integral basis, family of quintic fields.
Research supported in part by Grants 16791 and 16975 from the Hungarian National Foundation for Scientific Research and by the Deutsche Forschungsgemeinschaft.

exist several non–equivalent generators of power integral bases which are explicitly determined in the last section of the paper.

It is a classical problem of algebraic number theory to decide if a number field has power integral bases. In connection with this question we considered the problem of the resolution of index form equations in cubic, quartic and special sextic fields in several recent papers (cf. e.g. [6], [4], [3], [5]). For number fields of higher degree k the problem becomes difficult because of the large degree $k(k-1)/2$ of the index form equation and the number of variables $k-1$.

We remark that unit equations are usually solved by combining Baker's method with a numerical reduction algorithm. Sieve methods involving congruence considerations are commonly applied in the last step to obtain the small solutions below the reduced bound. In our case the unit group modulo m is at most of order 10, independently from n which enables us to test the unit equation modulo m in a parametric form.

Most calculations involved in this paper were performed by using MAPLE (cf. [11]). The calculation with elements of K_n and checking if certain elements are integral would hardly be possible without the use of a computer algebra package. Hence, short proofs often involve tedious computations.

A family of cyclic quintics

In the sequel we frequently use two integers related to the number fields under consideration:

$$m := n^4 + 5n^3 + 15n^2 + 25n + 25,$$
$$d := n^3 + 5n^2 + 10n + 7,$$

where m is the conductor of the field and d will turn out to be the index of the equation order of f_n in the maximal order under appropriate premises.

Lemma 1. *The integers m and d are coprime for every $n \in \mathbb{Z}$.*

Proof. Straightforward by Euclid's algorithm.

For simplicity's sake we denote by $\vartheta = \vartheta_n$ a root of f_n of (1) and set $K = K_n = \mathbb{Q}(\vartheta_n)$. This field is totally real, cyclic, and the transformation

$$x \longmapsto x' = \frac{(n+2) + nx - x^2}{1 + (n+2)x} \tag{2}$$

permutes the roots of f_n cyclically ([10]).

Lemma 2. *Assume that $p^2 \nmid m$ for any prime $p \neq 5$. An integral basis of K is given by $\{1, \vartheta, \vartheta^2, \vartheta^3, \omega_5\}$ with*

$$\omega_5 = \frac{1}{d}\left((n+2) + (2n^2+9n+9)\vartheta + (2n^2+4n-1)\vartheta^2 + (-3n-4)\vartheta^3 + \vartheta^4\right).$$

The discriminant of K is

$$D_K = m^4. \tag{3}$$

Proof. Using (2) we have

$$\vartheta' = \alpha + (n+2)^2\omega_5$$

with

$$\alpha = (n+2) + (n^3+4n^2+5n)\vartheta + (-2n^2-6n-5)\vartheta^2 + (n+2)\vartheta^3.$$

It is easily seen that $\gcd(n+2,d)=1$, whence ω_5 is an algebraic integer in K.

The discriminant of the generating polynomial of ϑ is

$$d^2m^4 = D(\vartheta) = (I(\vartheta))^2 D_K.$$

We shall show, that the index $I(\vartheta) = (\mathbb{Z}_K : \mathbb{Z}[\vartheta])$ is equal to d, which in view of $D(1,\vartheta,\vartheta^2,\vartheta^3,\omega_5) = m^4$ implies, that $\{1,\vartheta,\vartheta^2,\vartheta^3,\omega_5\}$ is indeed an integral basis. The inclusion $\mathbb{Z}_K \supseteq \mathbb{Z}[\vartheta,\omega_5] \supseteq \mathbb{Z}[\vartheta]$ and $(\mathbb{Z}[\vartheta,\omega_5] : \mathbb{Z}[\vartheta]) = d$ show, that d divides $I(\vartheta)$.

In view of Lemma 1 we must still show, that no prime number p dividing m occurs in that index. We discuss the cases $p \neq 5$ and $p = 5$ separately.

Let us assume that $p \neq 5$ at first. Then $-n^2/5$ is a five–fold zero of $f_n(x)$ modulo $p\mathbb{Z}[x]$. We get

$$f_n(x) - \left(x + \frac{n^2}{5}\right)^5 = \sum_{i=1}^{4} b_i x^{4-i}$$

with

$$\begin{aligned}
b_1 &= -\frac{2}{5}n^4 - 2n^3 - 6n^2 - 10n - 10,\\
b_2 &= -\frac{2}{25}n^6 + n^4 + 5n^3 + 11n^2 + 15n + 5,\\
b_3 &= -\frac{1}{125}n^8 + n^3 + 4n^2 + 10n + 10,\\
b_4 &= -\frac{1}{3125}n^{10} + 1.
\end{aligned}$$

Setting

$$\tilde{m} = \begin{cases} m & \text{for} \quad 5 \nmid m, \\ \dfrac{m}{25} & \text{for} \quad 5 | m, \end{cases}$$

we see that

$$5^i b_i \equiv 0 \bmod \tilde{m}.$$

From this we conclude

$$3125\left[f_n(x_0) - \left(x_0 + \frac{n^2}{5}\right)^5\right]_{x_0 = -\frac{n^2}{5}} = mk$$

with $k = 4n^6 + 3n^5 + 65n^4 - 200n^2 - 125n + 125$. Another gcd computation shows that $\gcd(\tilde{m},k) = 1$. Hence, the Dedekind test (Ch. 4.5 (5.55) in [9]) tells us that $R := \mathbb{Z}[1,\vartheta,\vartheta^2,\vartheta^3,\omega_5]$ is p–maximal precisely for $p^2 \nmid m$.

Finally, we consider the case $p = 5$. Clearly, 5 must divide n. Setting $n = 5\tilde{n}$ we obtain $m = 5^2\tilde{m}$ with $\tilde{m} = 5(5\tilde{n}^4 + 5\tilde{n}^3 + 3\tilde{n}^2 + \tilde{n}) + 1$. An easy calculation shows that

$$f_n(x) \equiv x^5 - 10x^3 + 5x^2 + 10x + 1 \bmod 25\mathbb{Z}[x]$$

and therefore

$$f_n(x) \equiv (x+1)^5 \bmod 5\mathbb{Z}[x].$$

For the Dedekind test we must check whether -1 is a zero of

$$h_n(x) = 5^{-1}(f_n(x) - (x+1)^5)$$

in $\mathbb{Z}/5\mathbb{Z}$. Because of

$$h_n(-1) = 5^{-1}(n^4 + 6n^3 + 14n^2 + 15n + 15) \equiv 3 \bmod 5$$

we see that R is 5–maximal.

The discriminant is obtained by direct calculations.

Corollary. *Except for $n = -1, -2$ the order $R := \mathbb{Z}[\vartheta, \omega_5]$ is strictly larger than $\mathbb{Z}[\vartheta]$. R is the maximal order of K if and only if there is no prime number $p \neq 5$ whose square divides m.*

Lemma 3. *Any four distinct roots of f_n form a set of fundamental units in K.*

Proof. The proof is along the lines of the one given for Theorem 3.5 in [10] for the case that m is a prime number. We briefly consider the major steps. By i we denote the index of the subgroup generated by four roots of $f_n(x)$ and -1 in the full unit group of K.

(i) for $|n+1| \geq 20$ we have $i < 11$.

(ii) Since 2, 3, 7 and 9 are not norms for $\mathbb{Z}[\zeta_5]$ over $\mathbb{Z}$ (ζ_5 being a fifth primitive root of unity), we have $i \in \{1, 5\}$ for $|n+1| \geq 20$.

(iii) The possibility $i = 5$ is eliminated by considering a prime $p \neq 5$ dividing m (compare Step 2 of [10]). Such a prime exists except for $n = 0$.

(iv) For those n subject to $|n+1| < 20$ for which m is not a prime the unit group is explicitly calculated with Kant (cf. [1]).

The structure of the index form

Denote by $\gamma^{(i)}$ $(1 \leq i \leq 5)$ the conjugates of any $\gamma \in K$ ordered such that (2) maps $\gamma^{(i)}$ onto $\gamma^{(j)}, j = (i \bmod 5) + 1$. For $1 \leq i \leq 5$ we set

$$L^{(i)}(\underline{X}) = \vartheta^{(i)} X_2 + \left(\vartheta^{(i)}\right)^2 X_3 + \left(\vartheta^{(i)}\right)^3 X_4 + \omega_5^{(i)} X_5,$$

and

$$L_{ij}(\underline{X}) = L^{(i)}(\underline{X}) - L^{(j)}(\underline{X}) \ \ (1 \leq i < j \leq 5)$$

in the variables $\underline{X} = (X_2, X_3, X_4, X_5)$. The index form corresponding to the integral basis of Lemma 2 is

$$I(\underline{X}) = \frac{1}{\sqrt{D_K}} \prod_{1 \leq i < j \leq 5} L_{ij}(\underline{X}). \tag{4}$$

This is a homogeneous form of degree 10 with rational integer coefficients.

Lemma 4. *We have*

$$I(\underline{X}) = N_{K/Q}(A(\underline{X}))N_{K/Q}(B(\underline{X}))$$

where

$$A(\underline{X}) = \frac{L_{12}(\underline{X})}{\vartheta^{(1)} - \vartheta^{(3)}} = \frac{\vartheta^{(1)} - \vartheta^{(2)}}{\vartheta^{(1)} - \vartheta^{(3)}} X_2 + \frac{\left(\vartheta^{(1)}\right)^2 - \left(\vartheta^{(2)}\right)^2}{\vartheta^{(1)} - \vartheta^{(3)}} X_3 + \frac{\left(\vartheta^{(1)}\right)^3 - \left(\vartheta^{(2)}\right)^3}{\vartheta^{(1)} - \vartheta^{(3)}} X_4 + \frac{\omega_5^{(1)} - \omega_5^{(2)}}{\vartheta^{(1)} - \vartheta^{(3)}} X_5$$

and

$$B(\underline{X}) = \frac{L_{13}(\underline{X})}{\vartheta^{(1)} - \vartheta^{(3)}} = X_2 + \left(\vartheta^{(1)} + \vartheta^{(3)}\right) X_3 + \left(\left(\vartheta^{(1)}\right)^2 + \vartheta^{(1)}\vartheta^{(3)} + \left(\vartheta^{(3)}\right)^2\right) X_4 + \frac{\omega_5^{(1)} - \omega_5^{(3)}}{\vartheta^{(1)} - \vartheta^{(3)}} X_5$$

and the coefficients of these linear forms are integers of K.

Proof. In view of (3) we have

$$I(\underline{X}) = \frac{1}{m^2} N_{K/Q}(L_{12}(\underline{X})) N_{K/Q}(L_{13}(\underline{X})).$$

We observe that $N_{K/Q}(\vartheta^{(1)} - \vartheta^{(3)}) = -m$. By direct calculations it can be checked that the coefficients of both $L_{12}(\underline{X})$ and $L_{13}(\underline{X})$ are divisible by $\vartheta^{(1)} - \vartheta^{(3)}$.

It is well known that the algebraic integer $\xi = x_1 + \vartheta x_2 + \vartheta^2 x_3 + \vartheta^3 x_4 + \omega_5 x_5$ ($x_i \in \mathbb{Z}, 1 \le i \le 5$) generates a power integral basis $\{1, \xi, \xi^2, \xi^3, \xi^4\}$ in K if and only if (x_2, x_3, x_4, x_5) is a solution of the index form equation

$$I(x_2, x_3, x_4, x_5) = \pm 1 \quad \text{in} \quad (x_2, x_3, x_4, x_5) \in \mathbb{Z}^4. \tag{5}$$

Remark. By direct substitution we get (cf. Corollary)

$$I(\vartheta) = I(1, 0, 0, 0) = d.$$

The unit equation

In the following we suppose that $m = n^4 + 5n^3 + 15n^2 + 25n + 25$ is **square free**. This involves $5 \nmid m$ (or equivalently $5 \nmid n$) hence 5 is invertible modulo m. Also, in view of Lemma 1, d is invertible modulo m.

Lemma 5. *If $\underline{x} = (x_2, x_3, x_4, x_5) \in \mathbb{Z}^4$ is a solution of (5), then there exist units ε, η in K such that*

$$\varepsilon + \left(\frac{\vartheta^{(2)} - \vartheta^{(4)}}{\vartheta^{(1)} - \vartheta^{(3)}}\right) \varepsilon' - \eta = 0 \tag{6}$$

where ε' denotes the conjugate of ε under (2).

Proof. Obviously, we have

$$\frac{L_{12}(\underline{x})}{\vartheta^{(1)} - \vartheta^{(3)}} + \frac{L_{23}(\underline{x})}{\vartheta^{(1)} - \vartheta^{(3)}} - \frac{L_{13}(\underline{x})}{\vartheta^{(1)} - \vartheta^{(3)}} = 0. \tag{7}$$

By Lemma 4

$$\varepsilon = \frac{L_{12}(\underline{x})}{\vartheta^{(1)} - \vartheta^{(3)}} = A(\underline{x}) \tag{8}$$

and

$$\eta = \frac{L_{13}(\underline{x})}{\vartheta^{(1)} - \vartheta^{(3)}} = B(\underline{x})$$

are units in K. The conjugate of ε under the mapping (2) is

$$\varepsilon' = \left(\frac{L_{12}(\underline{x})}{\vartheta^{(1)} - \vartheta^{(3)}}\right)' = \frac{L_{23}(\underline{x})}{\vartheta^{(2)} - \vartheta^{(4)}},$$

hence the second term of (7) can be rewritten in the required form (6).

Remark. Equation (6) leads to the unit equation in two variables

$$\left(\varepsilon(\eta)^{-1}\right) + \frac{\vartheta^{(2)} - \vartheta^{(4)}}{\vartheta^{(1)} - \vartheta^{(3)}} \left(\varepsilon'(\eta)^{-1}\right) = 1. \tag{9}$$

Lemma 6. *Let*

$$\begin{aligned} e_0 &= 1, \\ e_1 &= \frac{-n^2}{5}, \\ e_2 &= -\frac{n^3}{5} - \frac{3n^2}{5} - n - 1, \\ e_3 &= \frac{2n^2}{5} + n + 2, \\ e_4 &= \frac{n^3}{5} + \frac{4n^2}{5} + 2n + 2. \end{aligned} \tag{10}$$

Any unit of the field K is congruent to e_k or $-e_k$ for a suitable index k $(0 \le k \le 4)$ modulo the ideal (m) of $\mathbb{Z}_K$, where divison by 5 yields multiplication by the inverse of 5 $\bmod m$. *Moreover, for any unit ε of K and its conjugate ε' we have*

$$\varepsilon \equiv \varepsilon' \bmod m. \tag{11}$$

Proof. Because of

$$f_n(x) \equiv \left(x + \frac{n^2}{5}\right)^5 \bmod m$$

all roots η_i of f_n satisfy

$$\eta_i \equiv -\frac{n^2}{5} \bmod m \ \ (1 \le i \le 5). \tag{12}$$

Moreover, we have $\eta_1\eta_2\eta_3\eta_4\eta_5 = -1$, hence

$$\left(\frac{-n^2}{5}\right)^5 \equiv -1 \bmod m. \tag{13}$$

Lemma 3 implies that $\{\eta_1, \eta_2, \eta_3, \eta_4\}$ is a set of fundamental units in K, hence any unit ε can be written as a power product of these elements and possibly -1. Now (12) and (13) imply, that for any unit ε there exists an exponent k $(0 \le k \le 4)$ such that

$$\varepsilon \equiv \pm \left(\frac{-n^2}{5}\right)^k \bmod m.$$

The remainder of $(-n^2/5)^k \bmod m$ is just e_k $(0 \le k \le 4)$ which implies the first assertion of the lemma. (11) follows from

$$\eta_i \equiv \eta_i' \equiv \frac{-n^2}{5} \bmod m \ (1 \le i \le 5).$$

Lemma 7. *If there exists a solution $\underline{x} = (x_2, x_3, x_4, x_5) \in \mathbb{Z}^4$ of equation (5), then there is an index k $(0 \le k \le 4)$ such that*

$$\pm e_k(1 + a) - 1 \equiv 0 \bmod m, \tag{14}$$

with a suitable sign, where

$$a = \frac{n^3}{5} + \frac{4n^2}{5} + 2n + 2. \tag{15}$$

Proof. By Lemma 5 there exist units ε and η such that (6) holds. We calculate

$$\frac{\vartheta^{(2)} - \vartheta^{(4)}}{\vartheta^{(1)} - \vartheta^{(3)}} \equiv a \bmod (m).$$

Using (11) and (6) we obtain

$$\varepsilon(1 + a) - \eta \equiv 0 \bmod m$$

whence

$$(\eta)^{-1}\varepsilon(1 + a) - 1 \equiv 0 \bmod m.$$

This implies (14) because of Lemma 6.

Theorem. *Assume as before that m is square free. The field K admits a power integral basis if and only if $n = -1$ or $n = -2$.*

Proof. The field K has a power integral basis if and only if the index form equation (5) is solvable. By Lemma 7 this implies the solvability of (14).

We calculate the remainders modulo m of the left-hand sides of (14) for $0 \le k \le 4$ and for both possible signs. These remainders are cubic polynomials in n. It is easy to see, that for $|n| > 250$ they are non–zero and in absolute value less that m. For $|n| \le 250$ we test all these congruences and the only solutions found are $n = -1, -2$. This case is considered in detail in the next section.

Remark. This theorem is a special case of the result of M. N. Gras [7] which she obtains in a completely different non–constructive way.

The case $n = -1, -2$

For $n = -1, -2$ the fields K_n coincide, which is easily checked by KANT (cf. [1]). To fix our notation we set $n = -1, \quad K = K_{-1}$ and $\vartheta = \vartheta_{-1}$ in this section. We note that K is the totally real quintic number field of minimum discriminant. We have $m = 11, d = 1$ hence by Lemma 2 $\{1, \vartheta, \vartheta^2, \vartheta^3, \vartheta^4\}$ is an integral basis of K. Now using standard arguments, by combining Baker's method with reduction algorithms and sieving procedures (cf. e.g. [3] for the basic ideas of the algorithm) we solved the unit equation (9) corresponding to the index form equation (5). The solutions allow to express ε/ε' and hence also ε, which gives (x_2, x_3, x_4, x_5) in view of (8), by taking conjugates and solving the corresponding system of linear equations.

We obtained the following solutions (if (x_2, x_3, x_4, x_5) is a solution, then so is $(-x_2, -x_3, -x_4, -x_5)$ but we list only one of them):

$$\begin{aligned}
&(x_2, x_3, x_4, x_5) = (0,1,0,0), (0,3,0,-1), (0,4,0,-1), (1,-4,0,1),\\
&(1,-3,0,1), (1,-2,-1,1), (1,-1,-1,0), (1,0,0,0), (1,1,0,0),\\
&(2,-1,-1,0), (2,0,-1,0), (2,1,-2,-1), (2,1,-1,0), (2,3,-1,-1),\\
&(2,4,-1,-1), (2,8,-1,-2), (3,-1,-1,0), (3,0,-1,0), (3,3,-1,-1),\\
&(3,4,-1,-1), (4,-4,-1,1), (5,-11,-1,3), (5,2,-2,-1), (5,13,-2,-3),\\
&(11,5,-4,-2).
\end{aligned}$$

Hence, α generates a power integral basis if and only if $\alpha = x_1 \pm (x_2\vartheta + x_3\vartheta^2 + x_4\vartheta^3 + x_5\vartheta^4)$ with an arbitrary $x_1 \in \mathbb{Z}$ and with a solution (x_2, x_3, x_4, x_5) of the index form equation.

We remark, that using KANT [1] the complete resolution of the unit equation (9) requires less than one minute by a medium fast workstation.

References

1. M.Daberkow, C.Fieker, J.Klüners, M.Pohst, K.Roegner, M.Schörnig & K.Wildanger, *Kant V4*, J. Symbolic Comp., to appear..
2. H.Darmon, *Note on a polynomial of Emma Lehmer*, Math. Comp. **56** (1991), 795–800. MR **91i:**11149
3. I.Gaál, *Computing all power integral bases in orders of totally real cyclic sextic number fields*, Math. Comp. **65** (1996), 801–822. MR **96g:**11155
4. 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. MR **96m:**11026
5. I.Gaál & M.Pohst, *On the resolution of index form equations in sextic fields with an imaginary subfield*, J.Symbolic Comp., to appear.
6. I.Gaál and N.Schulte, *Computing all power integral bases of cubic number fields*, Math. Comp. **53** (1989), 689–696. MR **90b:**11108
7. M.N.Gras, *Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$*, J.Number Theory **23** (1986), 347–353. MR **87g:**11116
8. E.Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988), 535–541. MR **89h:**11067a
9. M.Pohst & H.Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, Cambridge, 1989. MR **92b:**11074
10. R.Schoof & L.Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988), 543–556. MR **89h:**11067b
11. B.W.Char, K.O.Geddes, G.H.Gonnet, M.B.Monagan, S.M.Watt (eds.), *MAPLE, Reference Manual*, Watcom Publications, Waterloo, Canada, 1988.

Kossuth Lajos University, Mathematical Institute, H–4010 Debrecen Pf.12., Hungary
E-mail address: igaal@math.klte.hu

Technische Universität Berlin, Fachbereich 3 Mathematik, Strasse des 17. Juni 136, 10623 Germany
E-mail address: pohst@math.tu-berlin.de