ASIAN J. MATH.
Vol. 10, No. 4, pp. 765–772, December 2006

008

INTEGRAL BASES FOR AN INFINITE FAMILY OF CYCLIC QUINTIC FIELDS*

DANIEL ELOFF[†], BLAIR K. SPEARMAN[†§], AND KENNETH S. WILLIAMS[‡§]

Abstract. An explicit integral basis is given for infinitely many cyclic quintic fields.

Key words. Integral basis, family of quintic fields.

AMS subject classifications. 11R04, 11R20, 11R29.

1. Introduction. We denote the set of integers by $\mathbb{Z}$ and the set of positive integers by $\mathbb{N}$. Let $n \in \mathbb{Z}$. The Lehmer quintic $f_n(x) \in \mathbb{Z}[x]$ is defined by

$$\begin{aligned} f_n(x) = x^5 + n^2x^4 &- (2n^3 + 6n^2 + 10n + 10)x^3 \\ &+(n^4 + 5n^3 + 11n^2 + 15n + 5)x^2 + (n^3 + 4n^2 + 10n + 10)x + 1, \end{aligned}$$

see [5, p. 539]. Schoof and Washington [6, p. 548] have shown that $f_n(x)$ is irrreducible for all $n \in \mathbb{Z}$. Let $\theta \in \mathbb{C}$ be a root of $f_n(x) = 0$. Set $K = \mathbb{Q}(\theta)$ so that $[K : \mathbb{Q}] = 5$. It is known that K is a cyclic field [6, p. 548]. We denote the ring of integers of K by O_K. The discriminant $d(K)$ of K has been determined by Jeannin [4, p. 76], see also Spearman and Williams [7, p. 215], namely $d(K) = f(K)^4$, where the conductor $f(K)$ of K is given by

$$f(K) = 5^b \prod_{\substack{p \equiv 1 \pmod 5 \\ v_p(n^4+5n^3+15n^2+25n+25) \not\equiv 0 \pmod 5}} p, \tag{1.1}$$

where $v_p(k)$ denotes the exponent of the largest power of the prime p dividing the nonzero integer k and

$$b = \begin{cases} 0, & \text{if } 5 \nmid n, \\ 2, & \text{if } 5 \mid n. \end{cases} \tag{1.2}$$

Set

$$m = n^4 + 5n^3 + 15n^2 + 25n + 25 \in \mathbb{Z}, \tag{1.3}$$

$$d = n^3 + 5n^2 + 10n + 7 \in \mathbb{Z}, \tag{1.4}$$

$$a = m^3 - 10m^2 + 5m \in \mathbb{Z}. \tag{1.5}$$

From (1.3) we have

$$m = (n+2)(n+1)\left((n+1)^2 + 6\right) + 11$$

*Received November 15, 2005; accepted for publication March 6, 2006.
[†]Department of Mathematics and Statistics, University of British Columbia Okanagan, Kelowna, B.C. Canada V1V 1V7 (dan.eloff@gmail.com; blair.spearman@ubc.ca).
[‡]School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6 (kwilliam@connect.carleton.ca).
[§]The second and third authors were supported by grants from the Natural Sciences and Engineering Research Council of Canada.

and, as $(n+2)(n+1) \geq 0$ for all $n \in \mathbb{Z}$, we deduce that $m \geq 11$ so that

$$m \in \mathbb{N}. \tag{1.6}$$

Then, from (1.5), we obtain $a = m^2(m-10) + 5m \geq 176$ so that

$$a \in \mathbb{N}. \tag{1.7}$$

As $x^3 + 5x^2 + 10x + 7$ is irreducible in $\mathbb{Z}[x]$, we deduce from (1.4) that

$$d \neq 0. \tag{1.8}$$

A MAPLE calculation gives

$$\begin{aligned} a = \; & (n^3 + 5n^2 + 10n + 7)(n^9 + 10n^8 + 60n^7 + 243n^6 + 730n^5 \\ & + 1650n^4 + 2824n^3 + 3520n^2 + 2990n + 1357) + 1. \end{aligned} \tag{1.9}$$

From (1.2) and (1.3) we observe that

$$5^b \parallel m. \tag{1.10}$$

From (1.4) and (1.9) we see that

$$a = 1 + dk, \tag{1.11}$$

where

$$\begin{aligned} k = \; & n^9 + 10n^8 + 60n^7 + 243n^6 + 730n^5 + 1650n^4 \\ & + 2824n^3 + 3520n^2 + 2990n + 1357 \in \mathbb{Z} \setminus \{0\}. \end{aligned} \tag{1.12}$$

Gaál and Pohst [2, p. 1690] have shown that under the condition

$$p^2 \nmid m \text{ for any prime } p \neq 5 \tag{1.13}$$

an integral basis for K is given by

$$\{1, \theta, \theta^2, \theta^3, \omega_5\}, \tag{1.14}$$

where

$$\omega_5 = \frac{1}{d}\left((n+2) + (2n^2 + 9n + 9)\theta + (2n^2 + 4n - 1)\theta^2 + (-3n-4)\theta^3 + \theta^4\right). \tag{1.15}$$

Although it is very likely that there are infinitely many $n \in \mathbb{Z}$ such that (1.13) holds this has not yet been proved. Gaál and Pohst used their integral basis in a search for cyclic quintic fields with a power basis. They proved under the condition that m is squarefree that the field K admits a power basis if and only if $n = -1$ or $n = -2$ [2, Theorem, p. 1695], and noted that these values of n give the same field K [2, p. 1689]. They also observed [2, Remark, p. 1695] that their result is a special case of a theorem of Gras [3], which asserts that there is only one cyclic quintic field with a power basis, namely, the maximal real subfield of the cyclotomic field of 11-th roots of unity.

In this work we give an integral basis for K under the weaker condition

$$m \text{ is cubefree.} \tag{1.16}$$

From now on we assume that (1.16) holds except in Lemma 2.2. In view of (1.6), (1.10) and (1.16), we have

$$m = 5^b P Q^2, \tag{1.17}$$

where b is given by (1.2) and $P, Q \in \mathbb{N}$ are such that

$$5 \nmid P, \quad 5 \nmid Q, \quad (P, Q) = 1, \quad P, Q \text{ squarefree}. \tag{1.18}$$

By [4, Lemme 2.1.1] every prime factor ($\neq 5$) of m is $\equiv 1 \pmod 5$. Hence, by (1.1), we have

$$f(K) = 5^b P Q \tag{1.19}$$

and

$$p \text{ (prime)} \mid PQ \Longrightarrow p \equiv 1 \pmod{5}. \tag{1.20}$$

By (1.17) we have $Q \mid m$. By (1.5) we have $m \mid a$. Hence $Q \mid a$. Then, by (1.11), we have $Q \mid 1 + dk$ from which we deduce

$$(d, Q) = 1. \tag{1.21}$$

We define

$$\upsilon_4 = \frac{1}{Q}\left(\theta - \frac{n^2}{5}(Q-1)\right)^3 \in K \tag{1.22}$$

and

$$\upsilon_5 = \frac{ad\omega_5 + (1-a)Q\upsilon_4\theta}{dQ} \in K. \tag{1.23}$$

We note that (1.8) ensures that υ_5 is well-defined. We prove

Theorem. *Under the assumption* (1.16)

$$\{1, \theta, \theta^2, \upsilon_4, \upsilon_5\}$$

is an integral basis for K.

We note that if (1.13) holds then

$$Q = 1, \;\; \upsilon_4 = \theta^3, \;\; \upsilon_5 = \frac{ad\omega_5 + (1-a)\theta^4}{d}.$$

Appealing to (1.11) we deduce

$$\upsilon_5 = \omega_5 + k(d\omega_5 - \theta^4).$$

As $d\omega_5 - \theta^4$ is a cubic polynomial in θ with coefficients in $\mathbb{Z}$, we deduce from the theorem that $\{1, \theta, \theta^2, \theta^3, \omega_5\}$ is an integral basis for K showing that our theorem includes that of Gaál and Pohst [2, p. 1690].

By a theorem of Erdös [1] there exists an infinite set S of integers n such that $m = n^4 + 5n^3 + 15n^2 + 25n + 25$ is cubefree. For $n \in S$ the integer m has the form (1.17). Clearly S contains an infinite subset S_1 such that the values of $5^b PQ$ are distinct for $n \in S_1$. Thus, by (1.19), the conductors $f(K)$ are distinct for $n \in S_1$ thus ensuring that the cyclic quintic fields K are distinct for $n \in S_1$. Thus our theorem gives an integral basis for infinitely many cyclic quintic fields.

2. Proof of Theorem. We require a number of lemmas.

LEMMA 2.1. *Under the assumption* (1.16), *we have* $\upsilon_4 \in O_K$.

Proof. The asserted result is immediate if $Q = 1$. Hence we may assume that $Q > 1$. By (1.19) we see that $Q \mid f(K)$. Hence all the prime divisors q of Q ramify in O_K. Moreover, as K is a cyclic quintic field, each prime factor q ramifies totally. Hence there is a prime ideal $\wp$ of O_K such that $< q >= \wp^5$ and $N(\wp) = q$. Let $g_n(x) \in \mathbb{Z}[x]$ be the minimal polynomial of $5\theta + n^2$. Using MAPLE we find

$$g_n(0) = m(4n^6 + 30n^5 + 65n^4 - 200n^2 - 125n + 125). \tag{2.1}$$

From (1.17) and (2.1) we deduce that

$$Q^2 \mid g_n(0) = \pm N(5\theta + n^2). \tag{2.2}$$

Let

$$< 5\theta + n^2 >= P_1^{a_1} \cdots P_r^{a_r} \tag{2.3}$$

be the prime ideal decomposition of $< 5\theta + n^2 >$ into distinct prime ideals of O_K so

$$\left|N(5\theta + n^2)\right| = N(< 5\theta + n^2 >) = N(P_1)^{a_1} \cdots N(P_r)^{a_r}. \tag{2.4}$$

From (2.2) and (2.4) we see that

$$q^2 \mid N(P_1)^{a_1} \cdots N(P_r)^{a_r}. \tag{2.5}$$

Thus $P_i = \wp$ and $a_i \geq 2$ for some $i \in \{1, 2, \ldots, r\}$. Hence by (2.3) we have

$$\wp^2 \mid < 5\theta + n^2 > . \tag{2.6}$$

Since $\wp^5 \mid Q$ we deduce from (2.6) that

$$\wp^2 \mid < 5\theta + n^2 - n^2 Q > . \tag{2.7}$$

As $5 \nmid Q$ we have $\wp \nmid < 5 >$. Also by (1.20) we have $Q \equiv 1 \pmod 5$. Thus

$$\wp^2 \mid < \theta - n^2 \left(\frac{Q-1}{5}\right) > .$$

Hence

$$\wp^5 \mid < \theta - n^2 \left(\frac{Q-1}{5}\right) >^3 . \tag{2.8}$$

As (2.8) is true for each prime divisor q of Q we have

$$Q \mid < \theta - n^2 \left(\frac{Q-1}{5}\right) >^3 .$$

This proves that

$$\upsilon_4 = \frac{1}{Q}\left(\theta - \frac{n^2}{5}(Q-1)\right)^3 \in O_K$$

as asserted. □

LEMMA 2.2. *For all* $n \in \mathbb{Z}$ *we have* $\omega_5 \in O_K$.

Proof. The proof is given in [2, pp. 1690-1691], where the case $n = -2$ should be dealt with separately. □

LEMMA 2.3. *Under the assumption* (1.16), *we have* $\upsilon_5 \in O_K$.

Proof. Let

$$\alpha = ad\omega_5 + (1-a)Q\upsilon_4\theta. \tag{2.9}$$

By Lemmas 2.1 and 2.2 we have $\upsilon_4 \in O_K$ and $\omega_5 \in O_K$ so

$$\alpha \in O_K.$$

From (1.5) and (1.17) we have $Q \mid a$. Hence

$$\alpha \equiv 0 \pmod{Q}$$

in O_K. From (1.11) we have $d \mid 1-a$. Hence

$$\alpha \equiv 0 \pmod{d}$$

in O_K. Then, by (1.21), we deduce that

$$\alpha \equiv 0 \pmod{dQ}$$

in O_K so that by (1.23) and (2.9)

$$\upsilon_5 = \frac{\alpha}{dQ} \in O_K$$

as claimed. □

Proof of Theorem. We have

$$\begin{aligned}\alpha = dQ\upsilon_5 &= ad\omega_5 + (1-a)Q\upsilon_4\theta \\ &= a\left(\theta^4 + c(\theta)\right) + (1-a)\theta\left(\theta - \frac{n^2}{5}(Q-1)\right)^3,\end{aligned}$$

where

$$c(\theta) \in \mathbb{Z}[\theta], \ \ \deg c(\theta) = 3.$$

Thus

$$\alpha = \theta^4 + d(\theta),$$

where

$$d(\theta) \in \mathbb{Z}[\theta], \ \ \deg d(\theta) \leq 3.$$

Similarly

$$Q\upsilon_4 = \theta^3 + e(\theta),$$

where

$$e(\theta) \in \mathbb{Z}[\theta], \ \ \deg e(\theta) \leq 2.$$

Thus

$$\mathrm{disc}(1,\theta,\theta^2,Q\upsilon_4,\alpha) = \mathrm{disc}(1,\theta,\theta^2,\theta^3,\alpha) = \mathrm{disc}(1,\theta,\theta^2,\theta^3,\theta^4) = m^4 d^2,$$

by [2, p. 1691]. Therefore

$$\mathrm{disc}(1,\theta,\theta^2,\upsilon_4,\upsilon_5) = \frac{\mathrm{disc}(1,\theta,\theta^2,Q\upsilon_4,\alpha)}{Q^2(dQ)^2} = \frac{m^4}{Q^4} = 5^{4b}P^4Q^4 = f(K)^4 = d(K).$$

As $\upsilon_4 \in O_K$ and $\upsilon_5 \in O_K$ by Lemmas 2.1 and 2.3 respectively, we deduce that $\{1,\theta,\theta^2,\upsilon_4,\upsilon_5\}$ is an integral basis for K. □

We conclude with an example.

EXAMPLE. Let $n = 14$ so that

$$K = \mathbb{Q}(\theta), \ \ \theta^5 + 196\theta^4 - 6814\theta^3 + 54507\theta^2 + 3678\theta + 1 = 0.$$

We use the theorem to determine an integral basis for K. Here

$$\begin{aligned} & m = 11 \times 71^2,\ b = 0,\ P = 11,\ Q = 71, \\ & d = 7^2 \times 79, \\ & a = 2^4 \times 11 \times 71^2 \times 192141181, \\ & k = 5 \times 8807580989, \\ & \upsilon_4 = \frac{1}{71}(\theta - 2744)^3, \ \ \upsilon_4 \equiv \frac{5 + 29\theta + 4\theta^2 + \theta^3}{71} (\mathrm{mod}\ 1), \\ & \omega_5 = \frac{16 + 527\theta + 447\theta^2 - 46\theta^3 + \theta^4}{3871}, \end{aligned}$$

and

$$\upsilon_5 = \frac{r + s\theta - t\theta^2 + u\theta^3 + \theta^4}{274841}$$

with

$$r = 2727531680673536, \ \ s = 352210381854043381655 7072,$$

$$t = 3850620295978378636848, \ \ u = 1395473396124589624,$$

so that

$$\upsilon_5 \equiv \frac{50339 + 276624\theta + 112706\theta^2 + 220601\theta^3 + \theta^4}{274841} (\mathrm{mod}\ 1).$$

Thus by the theorem

$$\left\{1,\theta,\theta^2, \frac{5 + 29\theta + 4\theta^2 + \theta^3}{71}, \frac{50339 + 276624\theta + 112706\theta^2 + 220601\theta^3 + \theta^4}{274841}\right\}$$

is an integral basis for K. As

$$\begin{aligned}
&\frac{65823+624463\theta+70125\theta^2+3825\theta^3+\theta^4}{274841}\\
&\quad=\frac{50339+276240\theta+112706\theta^2+220601\theta^3+\theta^4}{274841}\\
&\qquad-56\left(\frac{5+29\theta+4\theta^2+\theta^3}{71}\right)+\left(4+23\theta+3\theta^2\right),
\end{aligned}$$

we see that

$$\left\{1,\theta,\theta^2,\frac{5+29\theta+4\theta^2+\theta^3}{71},\frac{65823+624463\theta+70125\theta^2+3825\theta^3+\theta^4}{274841}\right\}$$

is also an integral basis for K in agreement with MAPLE.

We close by remarking that when m is not cubefree the cyclic quintic field K may not have an integral basis of the type given in our theorem. To see this take $n=44$ so that $m=41^3\times 61$. In this case $(18+20\theta+\theta^2)/41$ is an integer of K and so θ^2 is not a minimal integer of degree 2. Hence K cannot have an integral basis of the type $\{1,\theta,\theta^2,*,*\}$.

REFERENCES

[1] P. Erdös, *Arithmetic properties of polynomials,* J. London Math. Soc., 28 (1953), pp. 416–425.
[2] I. Gaál and M. Pohst, *Power integral bases in a parametric family of totally real cyclic quintics,* Math. Comp., 66 (1997), pp. 1689–1696.
[3] 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), pp. 347–353.
[4] S. Jeannin, *Nombre de classes et unités des corps de nombres cycliques quintiques d'E. Lehmer,* J. Théor. Nombres Bordeaux, 8 (1996), pp. 75–92.
[5] E. Lehmer, *Connection between Gaussian periods and cyclic units,* Math. Comp., 50 (1988), pp. 535–541.
[6] R. Schoof and L. C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers,* Math. Comp., 50 (1988), pp. 543–556.
[7] B. K. Spearman and K. S. Williams, *Normal integral bases for Emma Lehmer's parametric family of cyclic quintics,* J. Théor. Nombres Bordeaux, 16 (2004), pp. 215–220.