A NUMBER FIELD WITH INFINITELY MANY NORMAL INTEGRAL BASES

Daniel Eloff
Dept. of Math. and Statistics, University of British Columbia Okanagan, Kelowna, B.C., Canada V1V 1V7
e-mail: dan.eloff@gmail.com

Blair K. Spearman
Dept. of Math. and Statistics, University of British Columbia Okanagan, Kelowna, B.C., Canada V1V 1V7
e-mail: blair.spearman@ubc.ca

Kenneth S. Williams
School of Math. and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6
e-mail: kwilliam@connect.carleton.ca

(Submitted June 2006-Final Revision July 2007)

ABSTRACT

A cyclic quintic field possessing infinitely many normal integral bases is exhibited. The bases provided are parametrized by Fibonacci numbers.

1. INTRODUCTION AND MAIN THEOREM

Let K be a finite normal extension of the rational field $\mathbb{Q}$. A normal integral basis of K is an integral basis for K all of whose elements are conjugate over $\mathbb{Q}$. Now suppose that K is cyclic of degree $d \geq 2$ over $\mathbb{Q}$. Then K possesses a normal integral basis if and only if K is tamely ramified [3, Corollary, p. 422] or equivalently K has a squarefree conductor [3, p. 175]. If K is a tamely ramified cyclic extension of $\mathbb{Q}$, it follows from results of Newman and Taussky [4], as well as Thompson [7], that K has a unique (up to order and change of sign) normal integral basis if and only if $d = 2, 3, 4$ or 6. Thus if K is a tamely ramified, cyclic, quintic extension of $\mathbb{Q}$ then K has at least two normal integral bases. In this paper we exhibit such a field K that possesses infinitely many normal integral bases. Indeed we exhibit infinitely many normal integral bases parametrized by Fibonacci numbers.

We let

$$f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1.$$

It is known that $f(x)$ is irreducible [5, p. 548 (with $n = -1$)]. Let $\theta \in \mathbb{C}$ be a root of $f(x)$. Set $K = \mathbb{Q}(\theta)$. Then K is a cyclic extension of degree 5 over $\mathbb{Q}$ [5, p. 548 (with $n = -1$)]. The discriminant of K is 11^4 and its conductor is 11 [2, Théorème 1, p. 76 (with $t = -1$)]. Thus K is the unique quintic subfield of the cyclotomic field of 11th roots of unity.

By a result of Gaál and Pohst [1, Lemma 2, p. 1690 (with $n = -1$)] an integral basis for K is $\{1, \theta, \theta^2, \theta^3, \omega\}$, where $\omega = 1 + 2\theta - 3\theta^2 - \theta^3 + \theta^4$. Thus $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ is an integral basis for K. The roots of $f(x)$ in cyclic order are

$$\begin{aligned} &\theta,\ \sigma(\theta) = 2 - 4\theta^2 + \theta^4,\ \sigma^2(\theta) = -1 + 2\theta + 3\theta^2 - \theta^3 - \theta^4, \\ &\sigma^3(\theta) = -2 + \theta^2,\ \sigma^4(\theta) = -3\theta + \theta^3, \end{aligned} \tag{1.1}$$

see for example [6, Proposition, p. 217 (with $n = -1$)].

We prove the following result, where F_n $(n \in \mathbb{Z})$ denotes the n-th Fibonacci number and L_n $(n \in \mathbb{Z})$ denotes the n-th Lucas number.

Theorem: Let K be the cyclic quintic field given by $K = \mathbb{Q}(\theta)$, where $\theta^5 + \theta^4 - 4\theta^3 - 3\theta^2 + 3\theta + 1 = 0$. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$ be given by

$$\sigma(\theta) = 2 - 4\theta^2 + \theta^4.$$

Set

$$\alpha_n = \frac{1}{10}(25F_{2n} + (-1)^n L_{2n} - 2) + \frac{1}{2}(-5F_{2n} + (-1)^n L_{2n})\theta \\ - 4F_{2n}\theta^2 + F_{2n}\theta^3 + F_{2n}\theta^4, \quad n \in \mathbb{N}. \tag{1.2}$$

Then α_n $(n \in \mathbb{N})$ is an integer of K and

$$\left\{\alpha_n, \sigma(\alpha_n), \sigma^2(\alpha_n), \sigma^3(\alpha_n), \sigma^4(\alpha_n)\right\}, \quad n \in \mathbb{N}, \tag{1.3}$$

is a normal integral basis for K. Moreover the bases (1.3) are distinct in the sense that if, for some $n_1, n_2 \in \mathbb{N}$, $j_1, j_2 \in \{0,1,2,3,4\}$, and $\varepsilon = \pm 1$, we have

$$\sigma^{j_1}(\alpha_{n_1}) = \varepsilon \sigma^{j_2}(\alpha_{n_2})$$

then

$$j_1 = j_2, \quad n_1 = n_2, \text{ and } \epsilon = +1.$$

2. PROOF OF THEOREM

The congruences

$$L_n \equiv F_n \pmod 2, \quad L_{2n} \equiv (-1)^n 2 \pmod 5, \quad n \in \mathbb{N},$$

follow immediately from the easily proved relations $L_n^2 - 5F_n^2 = (-1)^n 4$ and $L_{2n} - 5F_n^2 = (-1)^n 2$. Hence, for $n \in \mathbb{N}$, we have

$$\begin{aligned} 25F_{2n} + (-1)^n L_{2n} - 2 &\equiv F_{2n} - L_{2n} &&\equiv 0 \pmod 2, \\ 25F_{2n} + (-1)^n L_{2n} - 2 &\equiv (-1)^n L_{2n} - 2 &&\equiv 0 \pmod 5, \\ -5F_{2n} + (-1)^n L_{2n} &\equiv F_{2n} - L_{2n} &&\equiv 0 \pmod 2. \end{aligned}$$

Thus, for $n \in \mathbb{N}$, we can define integers r_n, s_n and t_n by

$$r_n = \frac{25F_{2n} + (-1)^n L_{2n} - 2}{10}, \quad s_n = \frac{-5F_{2n} + (-1)^n L_{2n}}{2}, \quad t_n = -F_{2n}. \tag{2.1}$$

Hence

$$-5r_n + s_n - 15t_n = 1, \quad n \in \mathbb{N}, \tag{2.2}$$

and (as $L_{2n}^2 - 5F_{2n}^2 = 4$)

$$s_n^2 - 5s_nt_n + 5t_n^2 = 1, \quad n \in \mathbb{N}. \tag{2.3}$$

Now let

$$\alpha_n = r_n + s_n\theta + 4t_n\theta^2 - t_n\theta^3 - t_n\theta^4, \ n \in \mathbb{N}. \tag{2.4}$$

Clearly α_n is an integer of K. By (1.1) the conjugates of α_n ($n \in \mathbb{N}$) over $\mathbb{Q}$ are

$$\begin{aligned}
\sigma(\alpha_n) &= (r_n + 2s_n - 3t_n) - 3t_n\theta + (-4s_n + 9t_n)\theta^2 + t_n\theta^3 + (s_n - 2t_n)\theta^4, \\
\sigma^2(\alpha_n) &= (r_n - s_n + 5t_n) + (2s_n - 6t_n)\theta + (3s_n - 6t_n)\theta^2 + (-s_n + 3t_n)\theta^3 \\
&\quad + (-s_n + 2t_n)\theta^4, \\
\sigma^3(\alpha_n) &= (r_n - 2s_n + 9t_n) + t_n\theta + (s_n - 6t_n)\theta^2 + t_n\theta^4, \\
\sigma^4(\alpha_n) &= (r_n + 4t_n) + (-3s_n + 8t_n)\theta - t_n\theta^2 + (s_n - 3t_n)\theta^3.
\end{aligned}$$

Using MAPLE, together with (2.2) and (2.3), we obtain

$$\begin{aligned}
&\operatorname{disc}(\{\alpha_n, \sigma(\alpha_n), \sigma^2(\alpha_n), \sigma^3(\alpha_n), \sigma^4(\alpha_n)\}) \\
&\quad = 11^4(-5r_n + s_n - 15t_n)^2(s_n^2 - 5s_nt_n + 5t_n^2)^4 = 11^4 = \operatorname{disc}(K),
\end{aligned}$$

so that for all $n \in \mathbb{N}$

$$\left\{\alpha_n, \sigma(\alpha_n), \sigma^2(\alpha_n), \sigma^3(\alpha_n), \sigma^4(\alpha_n)\right\} \tag{2.5}$$

is a normal integral basis for K.

Finally we show that the infinitely many normal integral bases in (2.5) are all distinct. Suppose that $m(\in \mathbb{N})$ and $n(\in \mathbb{N})$ are such that

$$\begin{aligned}
&\left\{\alpha_m, \sigma(\alpha_m), \sigma^2(\alpha_m), \sigma^3(\alpha_m), \sigma^4(\alpha_m)\right\} \\
&= \pm \left\{\alpha_n, \sigma(\alpha_n), \sigma^2(\alpha_n), \sigma^3(\alpha_n), \sigma^4(\alpha_n)\right\}.
\end{aligned}$$

Then

$$\alpha_m = \pm\sigma^j(\alpha_n) \text{ for some } j \in \{0, 1, 2, 3, 4\}.$$

If $j = 0$ then $\alpha_m = \pm\alpha_n$ and so, by (2.4), we have

$$\begin{aligned}
&r_m + s_m\theta + 4t_m\theta^2 - t_m\theta^3 - t_m\theta^4 \\
&\quad = \pm(r_n + s_n\theta + 4t_n\theta^2 - t_n\theta^3 - t_n\theta^4).
\end{aligned}$$

Equating coefficients of θ^3, we obtain $t_m = \pm t_n$. Appealing to (2.1), we deduce $F_{2m} = \pm F_{2n}$, so that $F_{2m} = F_{2n}$ and $m = n$.

Next we show that if $j \neq 0$ then $t_n = 0$, which is impossible for $n > 0$ as $t_n = -F_{2n}$.

If $j = 1$ then $\alpha_m = \pm\sigma(\alpha_n)$ and we have

$$\begin{aligned}
&r_m + s_m\theta + 4t_m\theta^2 - t_m\theta^3 - t_m\theta^4 \\
&\quad = \pm((r_n + 2s_n - 3t_n) - 3t_n\theta + (-4s_n + 9t_n)\theta^2 + t_n\theta^3 + (s_n - 2t_n)\theta^4).
\end{aligned}$$

Equating coefficients of θ^3, we obtain $-t_m = \pm t_n$, so by (2.1) we have $F_{2m} = \mp F_{2n}$ and thus $F_{2m} = F_{2n}$ and $m = n$. Hence

$$\begin{aligned} & r_n + s_n\theta + 4t_n\theta^2 - t_n\theta^3 - t_n\theta^4 \\ &= -(r_n + 2s_n - 3t_n) + 3t_n\theta - (-4s_n + 9t_n)\theta^2 - t_n\theta^3 - (s_n - 2t_n)\theta^4. \end{aligned}$$

Equating coefficients of θ and θ^2, we have $s_n = 3t_n$ and $4t_n = 4s_n - 9t_n$, so $t_n = 0$.

If $j = 2$ then $\alpha_m = \pm\sigma^2(\alpha_n)$ and we have

$$\begin{aligned} & r_m + s_m\theta + 4t_m\theta^2 - t_m\theta^3 - t_m\theta^4 \\ &= \pm((r_n - s_n + 5t_n) + (2s_n - 6t_n)\theta + (3s_n - 6t_n)\theta^2 \\ &\quad + (-s_n + 3t_n)\theta^3 + (-s_n + 2t_n)\theta^4). \end{aligned}$$

Equating coefficients of θ^3 and θ^4, we obtain $-s_n + 3t_n = \pm(-t_m) = -s_n + 2t_n$ so $t_n = 0$.

If $j = 3$ then $\alpha_m = \pm\sigma^3(\alpha_n)$ and we have

$$\begin{aligned} & r_m + s_m\theta + 4t_m\theta^2 - t_m\theta^3 - t_m\theta^4 \\ &= \pm((r_n - 2s_n + 9t_n) + t_n\theta + (s_n - 6t_n)\theta^2 + t_n\theta^4). \end{aligned}$$

Equating coefficients of θ^3, we obtain $t_m = 0$.

If $j = 4$ then $\alpha_m = \pm\sigma^4(\alpha_n)$ and we have

$$\begin{aligned} & r_m + s_m\theta + 4t_m\theta^2 - t_m\theta^3 - t_m\theta^4 \\ &= \pm((r_n + 4t_n) + (-3s_n + 8t_n)\theta - t_n\theta^2 + (s_n - 3t_n)\theta^3). \end{aligned}$$

Equating coefficients of θ^4, we obtain $t_m = 0$.

This completes the proof.

ACKNOWLEDGMENTS

The authors wish to thank the referee whose suggestions shortened and improved the paper.

REFERENCES

[1] I. Gaál and M. Pohst. "Power Integral Bases in a Parametric Family of Totally Real Cyclic Quintics." *Math Comp.* **66** (1997): 1689-1696.

[2] S. Jeannin. "Nombre de Classes et unités Des Corps de Nombres Cycliques Quintiques d'E. Lehmer." *J. Théor. Nombres Bordeaux* **8** (1996): 75-92.

[3] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers.* Second Edition, Springer-Verlag, Berlin Heidelberg New York, 1990.

[4] M. Newman and O. Taussky. "On a Generalization of the Normal Basis in Abelian Algebraic Number Fields." *Comm. Pure Appl. Math.* **9** (1956): 85-91.

[5] R. Schoof and L. Washington. "Quintic Polynomials and Real Cyclotomic Fields with Large Class Numbers." *Math. Comp.* **50** (1988): 543-556.

[6] 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): 215-220.

[7] R. C. Thompson. "Normal Matrices and the Normal Basis in Abelian Number Fields." *Pacific J. Math.* **12** (1962): 1115-1124.

AMS Classification Numbers: 11R20

✠ ✠ ✠