NORMAL INTEGRAL BASES OF A CYCLIC QUINTIC FIELD

CHAD DAVIS, DANIEL ELOFF, AND BLAIR K. SPEARMAN

ABSTRACT. Let $K/\mathbb{Q}$ be a finite Galois extension. A normal integral basis for K is an integral basis for K in which all the elements of the basis are conjugate over $\mathbb{Q}$. Let $\theta \in \mathbb{R}$ be a root of the polynomial

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

Set $K = \mathbb{Q}(\theta)$. It is known that K possesses infinitely many normal integral bases. In this paper, we explicitly determine all normal integral bases of K and parametrize them using the Fibonacci and Lucas numbers.

1. INTRODUCTION

Let K be a finite Galois extension of the rational field $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$. An integral basis for K is said to be a *normal integral basis* if all of its elements are conjugate over $\mathbb{Q}$. It is known by the Hilbert-Speiser Theorem that a finite abelian extension $K/\mathbb{Q}$ has a normal integral basis if and only if K is tamely ramified over $\mathbb{Q}$. This result is known not to hold for arbitrary extensions of number fields, thus making the study of normal integral bases of number fields over $\mathbb{Q}$ an interesting problem. For instance, the existence of normal integral bases of a given form in a parametric family of fields was proved in [16]. An element $a \in \mathcal{O}_K$ is said to generate a normal integral basis for K if a and all of its conjugates form an integral basis for K. Generators for normal integral bases in cyclic fields of prime degree were studied in [1]. If K is a finite, tame, abelian, Galois extension of $\mathbb{Q}$, then an asymptotic formula for the number of generators of normal integral bases of K was given in [5].

Consider the polynomial

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

Lehmer studied a parametric family of polynomials that contains f in [12, p. 539], with $n = -1$; this parametric family was also studied by Nakano in [13]. It is known that $f(X)$ is irreducible, that all the roots of $f(X)$ are real, and that $K = \mathbb{Q}(\theta)$ is a cyclic extension of $\mathbb{Q}$ of degree 5 where $\theta \in \mathbb{R}$ is a root of f (see [12, 14]). In [4], the authors exhibited infinitely many normal integral bases of K parametrized by Fibonacci and Lucas numbers. In this paper, we expand upon this result by finding all normal integral bases of K. We are able to show this result by considering the group ring generated by the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ over $\mathbb{Z}$. Moreover, if F_n and L_n denote the nth Fibonacci and Lucas numbers, respectively, we also prove that every normal integral basis of K can be parametrized using F_n and L_n where $n \in \mathbb{Z}$. Our main result is as follows.

Theorem 1.1. *Let K be the cyclic quintic field $\mathbb{Q}(\theta)$ where θ is a root of*

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

Let $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$ and let $\sigma \in \mathcal{G}$ be such that $\mathcal{G} = \langle\sigma\rangle$. Define

$$a_n = \frac{1}{10}(25F_{2n} + (-1)^n L_{2n} - 2) + \frac{1}{2}(-5F_{2n} + (-1)^n L_{2n})\theta - 4F_{2n}\theta^2 + F_{2n}\theta^3 + F_{2n}\theta^4 \quad (1.1)$$

and

$$S = \{\alpha \in \mathcal{O}_K : \alpha \text{ generates a normal integral basis for } K\}.$$

Then $a_n \in \mathcal{O}_K$ *for all* $n \in \mathbb{Z}$, *and furthermore,*

$$S = \{(-1)^i \sigma^j(a_n) : n \in \mathbb{Z}, i = 0, 1, j = 0, \ldots, 4\}.$$

As stated, the proof of the theorem will utilize a certain group ring, the necessary theory of which will be provided in Section 2. Some useful identities regarding Fibonacci and Lucas numbers are given in Section 3. The proof of the theorem is given in Section 4.

2. A Special Group Ring

In this section we explain how group rings are related to generators of normal integral bases. The definition of a group ring can be found in numerous algebra texts, see for instance [15, p. 1], or [8, p. 117]. For a given group G and ring R, we will denote the group ring of G over R by $R[G]$. One shows that $R[G]$ forms a ring with unity under the specified operations with identity element $1_{R[G]} = 1_R e_G$ where 1_R and e_G are the identity elements in R and G, respectively. It is also easy to show that $R[G]$ is commutative if and only if G is abelian. The theory of group rings is rich and the curious reader should consult [15] for more information.

For the rest of this section suppose that K is a finite, abelian, Galois extension of the rational field $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$ and Galois group $\mathcal{G}$. We are concerned with the group ring $\mathbb{Z}[\mathcal{G}]$ and how it relates to $\mathcal{O}_K$. Following the notation given in [5], the next proposition answers our query.

Proposition 2.1. $\mathcal{O}_K$ *is a* $\mathbb{Z}[\mathcal{G}]$*-module under the following action:*

$$a.\left(\sum_{\sigma\in\mathcal{G}} x_\sigma \sigma\right) = \sum_{\sigma\in\mathcal{G}} x_\sigma \sigma(a).$$

The proof of this proposition is straightforward definition checking and is omitted. Furthermore, Proposition 2.1 implies the following important observation: $a \in \mathcal{O}_K$ generates a normal integral basis for K if and only if

$$a.\mathbb{Z}[\mathcal{G}] = \mathcal{O}_K.$$

The next proposition, given in [5, p. 1007], shows that all the generators of normal integral bases of K can be characterized by this action and is pivotal to our main result.

Proposition 2.2. *Let* $a \in \mathcal{O}_K$ *generate a normal integral basis for* K. *Then the set of all generators of normal integral bases for* K *is* $a.\mathbb{Z}[\mathcal{G}]^*$ *where* $\mathbb{Z}[\mathcal{G}]^*$ *is the unit group of* $\mathbb{Z}[\mathcal{G}]$.

The proof of this proposition follows using a standard dual inclusion argument and so is omitted. Notice that Proposition 2.2 reduces the problem of finding generators of normal integral bases to one of finding the unit group in a particular group ring (a single generator can always theoretically be found, see [5, p. 1007]). However, determining the units in a group ring is often an arduous task, and we refer to [3, 7, 10, 11, 15] for more details.

3. Some Useful Identities

In this section we give some identities of Fibonacci numbers F_n, and Lucas numbers L_n, that will be used in the proof of Theorem 1. We recall that the Fibonacci and Lucas numbers are generated via the following recursions

$$F_0 = 0, F_1 = 1, \text{ and } F_n = F_{n-2} + F_{n-1} \text{ for } n \geq 2,$$
$$L_0 = 2, L_1 = 1, \text{ and } L_n = L_{n-2} + L_{n-1} \text{ for } n \geq 2.$$

Proposition 3.1. *Let n be a positive integer. The Fibonacci and Lucas numbers extend to all integers via the following two formulas,*

$$F_{-n} = (-1)^{n+1}F_n, \text{ and } L_{-n} = (-1)^n L_n, \text{ for } n \in \mathbb{N}.$$

Then, for any $n, m \in \mathbb{Z}$, the Fibonacci and Lucas numbers satisfy the following 7 identities.

(1) $F_{2(m+1)} = \frac{1}{2}(3F_{2m} + L_{2m})$,

(2) $L_{2(m+1)} = \frac{1}{2}(5F_{2m} + 3L_{2m})$,

(3) $F_{2(m-1)} = \frac{1}{2}(3F_{2m} - L_{2m})$,

(4) $L_{2(m-1)} = \frac{1}{2}(3L_{2m} - 5F_{2m})$,

(5) $F_{2(m-2)} = \frac{1}{2}(7F_{2m} - 3L_{2m})$,

(6) $L_{2(m-2)} = \frac{1}{2}(7L_{2m} - 15F_{2m})$,

and

(7) $5F_n^2 - L_n^2 = 4(-1)^{n+1}$.

Proof. (1)–(7) can be proved immediately from (15a), (15b), (17a), (17b), and (17c), or from (16a) and (16b) of [17, p. 177]. □

4. Proof of Theorem 1.1

Proof. The field $K = \mathbb{Q}(\theta)$ is a finite, abelian Galois extension of $\mathbb{Q}$ with Galois group $\mathcal{G} \cong \mathbb{Z}/5\mathbb{Z}$ and discriminant 11^4 (see [12, p. 539] with $n = -1$). Let $\sigma \in \mathcal{G}$ with $\mathcal{G} = \langle\sigma\rangle$. From [4, p. 151], the conjugates of θ are

$$\theta, \quad \sigma(\theta) = 2 - 4\theta^2 + \theta^4, \quad \sigma^2(\theta) = -1 + 2\theta + 3\theta^2 - \theta^3 - \theta^4 \tag{4.1}$$

$$\sigma^3(\theta) = -2 + \theta^2, \quad \sigma^4(\theta) = -3\theta + \theta^3. \tag{4.2}$$

Furthermore, by the theorem of [4, p. 152], $a_n \in \mathcal{O}_K$ generates a normal integral basis for all $n \in \mathbb{N}$.

We are now ready to proceed with the proof of the main result. We first show that $a_n \in \mathcal{O}_K$ for all $n \in \mathbb{Z}$. The congruence relations

$$L_n \equiv F_n \pmod 2, \qquad L_{2n} \equiv (-1)^n 2 \pmod 5$$

given in [4, page 152], hold for all $n \in \mathbb{Z}$. Substituting these into the formula for a_n given in equation (1.1), we see that $a_n \in \mathcal{O}_K$ for all $n \in \mathbb{Z}$. Using (7) of Proposition 3.1, the discriminant of $\{a_n, \sigma(a_n), \sigma^2(a_n), \sigma^3(a_n), \sigma^4(a_n)\}$ is

$$11^4 \cdot \frac{1}{256}(5F_{2n}^2 - L_{2n}^2)^4 = 11^4 \cdot \frac{1}{256}(256) = 11^4$$

for all $n \in \mathbb{Z}$. Thus, a_n generates a normal integral basis for all $n \in \mathbb{Z}$. From [2, pp. 2932 and 2934], the unit group of $\mathbb{Z}[\mathcal{G}]$ is $\langle -1, \sigma, \sigma^2 + \sigma^3 - 1\rangle$ where $\langle\cdot\rangle$ denotes the multiplicative group of $\mathbb{Z}[\mathcal{G}]$ generated by these three elements. Fixing $n = 1$ for a_1, Proposition 2.2 implies that

$$S = \{\alpha \in \mathcal{O}_K : \alpha \text{ generates a normal integral basis}\} = a_1.\langle -1, \sigma, \sigma^2 + \sigma^3 - 1\rangle$$

where

$$a_1 = 2 - 4\theta - 4\theta^2 + \theta^3 + \theta^4. \tag{4.3}$$

Hence, a typical element $s \in S$ is of the form

$$s = a_1.((-1)^i\sigma^j(\sigma^2 + \sigma^3 - 1)^m) = (-1)^i\sigma^j((\sigma^2 + \sigma^3 - 1)^m(a_1))$$

where $i = 0, 1, j = 0, \ldots, 4$, and $m \in \mathbb{Z}$. We now prove two lemmas that give formulas for $a_1.(\sigma^2 + \sigma^3 - 1)^m$ for any $m \in \mathbb{Z}$ in terms of a_n.

Lemma 4.1. *Let $m \in \mathbb{N}$. Then $a_1.(\sigma^2 + \sigma^3 - 1)^m = a_{M(m)}$ where $M(m) = (-1)^{m-1}(m-1)$.*

Proof. We use induction on m. If $m = 1$, then we use the identities in (4.1) and (4.2) to get

$$a_1.(\sigma^2 + \sigma^3 - 1) = \sigma^2(a_1) + \sigma^3(a_1) - a_1 = \theta = a_0 = a_{M(1)}.$$

Now suppose that $a_1.(\sigma^2 + \sigma^3 - 1)^{m-1} = a_{M(m-1)}$. By the induction hypothesis,

$$a_1.(\sigma^2 + \sigma^3 - 1)^m = (a_1.(\sigma^2 + \sigma^3 - 1)^{m-1}).(\sigma^2 + \sigma^3 - 1) = a_{M(m-1)}.(\sigma^2 + \sigma^3 - 1).$$

In order to make the proof slightly easier, we now split it into two cases: one where m is even and one where m is odd.

Case 1: Assume m is even. Then $m-1$ is odd, so that $M(m-1) = m-2$ and $M(m) = 1-m$. Equation (1.1) implies

$$\begin{aligned} a_{m-2} = {} & \frac{1}{10}(25F_{2(m-2)} + L_{2(m-2)} - 2) + \frac{1}{2}(-5F_{2(m-2)} + L_{2(m-2)})\theta \\ & - 4F_{2(m-2)}\theta^2 + F_{2(m-2)}\theta^3 + F_{2(m-2)}\theta^4. \end{aligned}$$

Using (4.1) and (4.2), we calculate

$$\begin{aligned} a_{m-2}.(\sigma^2 + \sigma^3 - 1) = {} & -\frac{1}{5}(1 + 20F_{2(m-2)} + 7L_{2(m-2)}) + \frac{1}{2}(5F_{2(m-2)} + L_{2(m-2)})\theta \\ & + 2(3F_{2(m-2)} + L_{2(m-2)})\theta^2 - \frac{1}{2}(3F_{2(m-2)} + L_{2(m-2)})\theta^3 \\ & - \frac{1}{2}(3F_{2(m-2)} + L_{2(m-2)})\theta^4, \end{aligned}$$

and by equation (1.1) and the definitions of F_{-n} and L_{-n} in Proposition 3.1, we have

$$\begin{aligned} a_{1-m} = {} & \frac{1}{10}(-25F_{2(m-1)} - L_{2(m-1)} - 2) + \frac{1}{2}(5F_{2(m-1)} - L_{2(m-1)})\theta \\ & + 4F_{2(m-1)}\theta^2 - F_{2(m-1)}\theta^3 - F_{2(m-1)}\theta^4. \end{aligned}$$

Applying (3)–(6) of Proposition 3.1 to the coefficients of the powers of θ in $a_{m-2}.(\sigma^2 + \sigma^3 - 1)$ and a_{1-m} shows that they are equal. Hence we have $a_1.(\sigma^2 + \sigma^3 - 1)^m = a_{M(m)}$.

Case 2: Assume m is odd. Then $m-1$ is even, and $M(m-1) = 2-m$ and $M(m) = m-1$. The proof then follows in the same way as Case 1. □

Lemma 4.2. *Let $m \in \mathbb{N}$. Then $a_1.(\sigma^2 + \sigma^3 - 1)^{-m} = a_{N(m)}$ where $N(m) = (-1)^m(m+1)$.*

Proof. The proof follows in the same fashion as that of Lemma 4.1, using (1) and (2) of Proposition 3.1, and noting that $(\sigma^2 + \sigma^3 - 1)^{-1} = \sigma + \sigma^4 - 1$. □

Lemmas 1 and 2 imply immediately that $S \subseteq \{(-1)^i\sigma^j(a_n) : n \in \mathbb{Z}, i = 0, 1, j = 0, \ldots, 4\}$. Equality follows from noting that, for any $n \in \mathbb{Z}$, we have $M(n+1) = n$ if n is even and $N(n-1) = n$ if n is odd. □

Acknowledgement

The authors would like to thank the anonymous referee for their useful comments and critiques on the first draft of this paper.

References

[1] V. Acciaro and C. Fieker, *Finding normal integral bases of cyclic number fields of prime degree*, J. Symbolic Computation, **30** (2000), 129–136.
[2] V. A. Artamonov and A. A. Bovdi, *Integral group rings: groups of invertible elements and classical K-theory*, (Russian) Translated in J. Soviet Math., **57.2** (1991), 2931–2958.
[3] A. K. Bhandari, *Some remarks on the unit groups of integral group rings*, Arch. Math., **44** (1985), 319–322.
[4] D. Eloff, B. K. Spearman, and K. S. Williams, *A number field with infinitely many normal integral bases*, The Fibonacci Quarterly, **45.2** (2007), 151–154.
[5] G. R. Everest, *Counting generators of normal integral bases*, American Journal of Mathematics, **120** (1998), 1007–1018.
[6] I. Gaál and M. Pohst, *Power integral bases in a parametric family of totally real cyclic quintic fields*, Mathematics of Computation, **66.220** (1997), 1689–1696.
[7] G. Higman, *The units of group rings*, Proc. London Math Soc., **46.2**, (1940), 231–248.
[8] T. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.
[9] S. Jeannin, *Nombre de classes et unités des corps de nombres cycliques quintiques d'E. Lehmer*, Journal de Théorie des Nombres de Boredeaux, **8** (1996), 75–92.
[10] E. Jespers and G. Leal, *Generators of large subgroups of the unit group of integral group rings*, Manuscripta Math., **78** (1993), 303–315.
[11] E. Jespers and C. Polinco Milies, *Units of group rings*, Journal of Pure and Applied Algebra, **107** (1996), 233–251.
[12] E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp., **50** (1988), 535–541.
[13] S. Nakano, *A family of quintic cyclic fields with even class number parametrized by rational points on an elliptic curve*, J. Number Theory, **129.12** (2009), 2943–2951.
[14] R. Schoof and L. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp., **50** (1988), 543–566.
[15] S. K. Sehgal, *Topics in Group Rings*, Marcel Dekker Inc., New York, 1978.
[16] B. K. Spearman and K. S. Williams, *Normal integral bases for Emma Lehmer's parametric family of cyclic quintics*, Journal de Théorie des Nombres de Bordeux, **16** (2004), 215–220.
[17] S. Vajda, *Fibonacci & Lucas Numbers, and the Golden Section: Theory and Applications*, Ellis Horwood Limited, West Sussex England, 1989.

MSC2010: 11R33, 20C05

Department of Mathematics and Statistics, University of British Columbia - Okanagan, Kelowna, British Columbia, V1V 1V7, Canada
E-mail address: cghost21@gmail.com

Department of Mathematics and Statistics, University of British Columbia - Okanagan, Kelowna, British Columbia, V1V 1V7, Canada
E-mail address: dan.eloff@gmail.com

Department of Mathematics and Statistics, University of British Columbia - Okanagan, Kelowna, British Columbia, V1V 1V7, Canada
E-mail address: blair.spearman@ubc.ca