PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9939(XX)0000-0

INTEGRAL GALOIS MODULE STRUCTURE FOR ELEMENTARY ABELIAN EXTENSIONS WITH A GALOIS SCAFFOLD

NIGEL P. BYOTT AND G. GRIFFITH ELDER

Abstract. This paper justifies an assertion in [Eld09] that Galois scaffolds make the questions of Galois module structure tractable. Let k be a perfect field of characteristic p and let $K = k((T))$. For the class of characteristic p elementary abelian p-extensions L/K with Galois scaffolds described in [Eld09], we give a necessary and sufficient condition for the valuation ring $\mathfrak{O}_L$ to be free over its associated order $\mathfrak{A}_{L/K}$ in $K[\mathrm{Gal}(L/K)]$. Interestingly, this condition agrees with the condition found by Y. Miyata, concerning a class of cyclic Kummer extensions in characteristic zero.

1. Introduction

Let k be a perfect field of characteristic $p > 0$, and let $K = k((T))$ be a local function field over k of dimension 1. For any finite extension L of K, we write $\mathfrak{O}_L$ for the valuation ring of L with maximal ideal $\mathfrak{P}_L$, and write $v_L \colon L \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ for the normalized valuation on L. If L/K is a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$, we write

$$\mathfrak{A}_{L/K} = \{\alpha \in K[G] \mid \alpha \mathfrak{O}_L \subseteq \mathfrak{O}_L\}$$

for the associated order of $\mathfrak{O}_L$ in the group algebra $K[G]$. Then $\mathfrak{A}_{L/K}$ is an $\mathfrak{O}_K$-order in $K[G]$ containing $\mathfrak{O}_K[G]$, and $\mathfrak{O}_L$ is a module over $\mathfrak{A}_{L/K}$. It is natural then to ask whether $\mathfrak{O}_L$ is a free module over $\mathfrak{A}_{L/K}$.

This question was investigated by Aiba [Aib03] and by de Smit and Thomas [dST07] when L/K is an extension of degree p. (For the analogous results in characteristic zero, see [BF72, BBF72].) Ramified cyclic extensions of degree p in characteristic p are special in that they possess a particular property, a Galois scaffold. In [Eld09], a class of arbitrarily large fully ramified elementary abelian p-extensions L/K, the *near one-dimensional elementary abelian extensions*, was introduced. These extensions are similarly special. They too possess a Galois scaffold.

Received by the editors February 12, 2009.
1991 *Mathematics Subject Classification.* 11S15, 11R33.
Key words and phrases. Galois module structure, Associated Order.

Definition. Let $K = k((T))$ as above. An elementary abelian extension $L = K(x_0, \ldots, x_n)$ of K of degree $q = p^{n+1}$ is a *one-dimensional elementary abelian extension* of K if $x_i^p - x_i = \Omega_i^{p^n}\beta$ for elements $\beta, \Omega_0 = 1, \Omega_1, \ldots \Omega_n \in K$ such that $v_K(\beta) = -b < 0$ with $(b,p) = 1$, $v_K(\Omega_n) \leq \ldots \leq v_K(\Omega_1) \leq v_K(\Omega_0) = 0$, and whenever $v_K(\Omega_i) = \cdots = v_K(\Omega_j)$ for $i < j$, the projections of $\Omega_i, \ldots, \Omega_j$ into $\Omega_i\mathfrak{O}_K/\Omega_i\mathfrak{P}_K$ are linearly independent over the field with p elements.

The extension L is a *near one-dimensional elementary abelian extension* of K if β, $\Omega_0, \ldots, \Omega_n$ and x_0 are as above, but for $1 \leq i \leq n$,

$$x_i^p - x_i = \Omega_i^{p^n}\beta + \epsilon_i,$$

for some "error terms" $\epsilon_i \in K$ satisfying

$$v_K(\epsilon_i) > v_K(\Omega_i^{p^n}\beta) + \frac{(p^n-1)b}{p^n} - (p-1)\sum_{j=1}^{n-1} p^j v_K(\Omega_j).$$

The purpose of this paper is to use the existence of Galois scaffolds for near one-dimensional elementary abelian extensions (recalled here as Theorem 2.1) to determine a necessary and sufficient condition for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_{L/K}$. So that we can state our main result (Theorem 1.1), we introduce some further notation.

As observed in [Eld09], any near one-dimensional elementary abelian extension L/K is totally ramified, and its lower ramification numbers are the distinct elements in the sequence

$$b_{(i)} = b + p^n \sum_{j=1}^{i} p^j m_j \tag{1}$$

where $m_j = v_K(\Omega_{j-1}) - v_K(\Omega_j)$. This means that the first ramification number of L/K is b, and that all the (lower) ramification numbers are congruent modulo $q = p^{n+1}$ to $r(b)$, the least non-negative residue of b.

Given any integer $j \geq 0$, let $j_{(s)}$ denote the base-p digits of j:

$$j = \sum_{s=0}^{\infty} j_{(s)} p^s$$

with $0 \leq j_{(s)} < p$ and $j_{(s)} = 0$ for s large enough. Thus $r(b) = \sum_{s=0}^{n} b_{(s)}p^s$. Following [Byo08], we define a set $\mathcal{S}(q)$.

Definition. Given $c \in \mathbb{Z}$ with $(c,p) = 1$, let $h = h_c$ be the unique solution of $hc \equiv -1 \pmod{q}$, $1 \leq h \leq q-1$. Then $\mathcal{S}(q)$ consists of all integers c with $(c,p) = 1$ and $1 \leq c \leq q-1$ satisfying the following property: For all u, $v \geq 1$ with $u + v < c$ there exists $s \in \{0, \ldots, n\}$ with

$$(hu)_{(s)} + (hv)_{(s)} < p - 1.$$

The main result of this paper is the following.

Theorem 1.1. *Let L/K be any near one-dimensional elementary abelian extension L/K of degree $q = p^{n+1}$. Then $\mathfrak{O}_L$ is free over its associated order $\mathfrak{A}_{L/K}$ if and only if $r(b) \in \mathcal{S}(q)$. Moreover, when $r(b) \in \mathcal{S}(q)$, any element $\rho_* \in L$ with $v_L(\rho_*) = r(b)$ is a free generator of $\mathfrak{O}_L$ over $\mathfrak{A}_{L/K}$.*

The definition for $\mathcal{S}(q)$ is difficult to digest, so we state a simpler (but weaker) version of the result.

Corollary 1.2. *Let L/K be as in Theorem 1.1.*

(i) *Suppose that $n \leq 1$. Then $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$ if and only if $r(b)$ divides $q - 1$.*
(ii) *Suppose that $n \geq 2$. Then $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$ if $r(b)$ divides $p^d - 1$ for some $d \in \{1, \ldots, n+1\}$.*

Applying Theorem 1.1 and Corollary 1.2 to the examples of near one-dimensional extensions provided by [Eld09, Lemmas 5.1 and 5.2], we obtain the following Corollaries.

Corollary 1.3. *If k contains the field $\mathbb{F}_q$ of $q = p^{n+1}$ elements with $n \geq 0$, $K = k((T))$, and $L = K(y)$ where*

$$y^q - y = \beta \in K \text{ with } v_K(\beta) = -b < 0, \quad (b, p) = 1, \tag{2}$$

then L/K is a totally ramified elementary abelian extension of degree q, with unique ramification break b. Moreover, if $r(b)$ denotes the least non-negative residue of b modulo q, then $\mathfrak{O}_L$ is free over its associated order $\mathfrak{A}_{L/K}$ if and only if $r(b) \in \mathcal{S}(q)$. In particular, assertion (i) or (ii) of Corollary 1.2 holds for L/K (according as $n \leq 1$ or $n \geq 2$).

Corollary 1.4. *If k has characteristic 2 and $K = k((T))$ and L is any totally ramified biquadratic extension of K (i.e. $\mathrm{Gal}(L/K) \cong C_2 \times C_2$), then $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$.*

Corollary 1.4 should be compared with the more complicated situation in characteristic zero [Mar74].

To close our introduction, we now explain how Theorem 1.1 can be seen to be an analogue of a result of Miyata [Miy98] for certain extensions in characteristic 0, as reformulated in [Byo08]. We will also record in Lemma 1.6 some results from [Byo08] which will be needed to prove Theorem 1.1 and Corollary 1.2.

Let F be a finite extension of the p-adic field $\mathbb{Q}_p$ that contains a primitive $q = p^{n+1}$ root of unity. Again, for any finite Galois extension E/F with Galois group G, we may consider the valuation ring $\mathfrak{O}_E$ as a module over its associated order $\mathfrak{A}_{E/F}$. A nice, natural class of extensions consists of those totally ramified cyclic Kummer extensions $F(\alpha)$ of degree q where

$$\alpha^q = a \in F \text{ with } v_F(a - 1) = t > 0, \quad (t, p) = 1. \tag{3}$$

Miyata [Miy98, Theorem 5] gave the following criterion for $\mathfrak{O}_E$ to be free over $\mathfrak{A}_{E/F}$.

Theorem 1.5 (Miyata)**.** *Let E/F be as above, satisfying* (3)*. Let $t_0 = r(t)$, where, for each $j \in \mathbb{Z}$, we write $r(j)$ for be the least non-negative residue of j mod q. Then $\mathfrak{O}_E$ is free over its associated order $\mathfrak{A}_{E/F}$ if and only if t_0 satisfies the following condition:*

$$t_0 + r(it_0) - r(ht_0) > 0$$

for all integers h, i, j with $0 \le h \le i \le j < n$ such that $i+j = n-1+h$ and $\binom{i}{h} \not\equiv 0 \pmod{p}$.

The lower ramification numbers of E/F are all congruent modulo q to $-t$ [Miy98, Lemma 2 and Proposition 3]. Thus, writing b for the first ramification number of E/F, we may view the condition in Theorem 1.5 as a condition on $r(b) = q - t_0$. Miyata was able to deduce some more explicit results for certain special values of t_0 [Miy98, Theorem 6]; expressed in terms of $r(b)$, his result asserts that if $r(b)$ divides $q-1$ then $\mathfrak{O}_E$ is free over $\mathfrak{A}_{E/F}$, and if $q - r(b)$ divides $q-1$ and $1 < r(b) < q-1$ then $\mathfrak{O}_E$ is not free over $\mathfrak{A}_{E/F}$. Note that these statements are considerably weaker than the corresponding assertions in Corollary 1.2. For further results on the family of Kummer extensions satisfying (3), see [Miy95, Miy04].

The set $\mathcal{S}(q)$ defined above was introduced in [Byo08] to give an alternative formulation of Miyata's condition from which further consequences could be deduced. Indeed, the following results were obtained.

Lemma 1.6. *Let $q = p^{n+1}$, let $1 \le t_0 \le q-1$ with $(t_0, p) = 1$, and let $b_0 = q - t_0$. Then the following conditions are equivalent:*

(i) *$t_0 + r(it_0) - r(ht_0) > 0$ for all integers h, i, j with $0 \le h \le i \le j < n$ such that $i + j = n - 1 + h$ and $\binom{i}{h} \not\equiv 0 \pmod{p}$;*
(ii) *$b_0 \in \mathcal{S}(q)$.*

Moreover, the following assertions hold.

(iii) *Suppose that $n \le 1$. Then $b_0 \in \mathcal{S}(q)$ if and only if b_0 divides $q-1$.*
(iv) *Suppose that $n \ge 2$. Then $b_0 \in \mathcal{S}(q)$ if b_0 divides $p^d - 1$ for some $d \in \{1, \dots, n+1\}$.*

Proof. The equivalence of (i) and (ii) is shown on pp. 153–154 of [Byo08]; see specifically Propositions 2.1 and 2.2 and the paragraph headed *Proof of Theorem 1.8*. Assertion (iii) is [Byo08, Lemma 2.3(ii)], and (iv) follows [Byo08, Lemma 2.3(i) and Lemma 2.4(ii)] as in [Byo08, p. 155, Proof of Theorem 1.6]. □

Note that Lemma 1.6 asserts properties of the set of integers $\mathcal{S}(q)$, whose definition depends only on the prime power q and is otherwise independent of the field extensions under consideration.

Combining Theorem 1.5 with Lemma 1.6, we obtain the fact, previously recorded as [Byo08, Theorem 1.8], that $\mathfrak{O}_E$ is free over $\mathfrak{A}_{E/F}$ if and only if $r(b) \in \mathcal{S}(q)$. Also, returning to the characteristic p situation, Corollary 1.2 follows immediately from Theorem 1.1 and Lemma 1.6.

It is shown in [Byo08, §3] that the converse of Lemma 1.6(iv) does not always hold. Hence the converse of assertion (ii) in Corollary 1.2 (and so also in Corollary 1.3) does not always hold.

The appearance of the same necessary and sufficient condition for freeness of the valuation ring over its associated order, both in the case of Miyata's cyclic extensions in characteristic 0 and in the case of the near one-dimensional elementary abelian extensions in characteristic p, is unexpected. It suggests that we should regard near one-dimensional extensions as somehow analogous to Miyata's cyclic characteristic 0 extensions. In particular, it seems natural to regard the families of extensions in Corollary 1.3 and Theorem 1.5 (both defined by a single equation) to be analogous. If this analogy has merit, then Theorem 1.1 suggests that there should be a larger family of Kummer extensions, "deformations" of Miyata's family, for which, in some appropriate sense, Miyata's criterion holds.

2. Proof of Theorem 1.1

In §2.1 and §2.2, we introduce the Galois scaffold constructed in [Eld09] for near one-dimensional elementary abelian extensions, and then use this scaffold to provide $\mathfrak{O}_K$-bases for both $\mathfrak{O}_L$ and $K[G]$. In §2.3, we use these bases to prove Theorem 1.1.

2.1. **Galois scaffold.**

The definition of Galois scaffold in [Eld09] has been clarified in [BE]. There are two ingredients: a valuation criterion for a normal basis generator and a generating set for a particularly nice K-basis of the group algebra $K[G]$.

In our setting, where L/K is a near one-dimensional elementary abelian extension of degree $q = p^{n+1}$, the valuation criterion is $v_L(\rho) \equiv r(b) \bmod q$, which means that if $v_L(\rho) \equiv r(b) \bmod q$ then $L = K[G]\rho$.

The second ingredient is a generating set of $\log_p |G| = n+1$ elements $\{\Psi_i\}$ from the augmentation ideal $(\sigma - 1 : \sigma \in G)$ of $K[G]$ that satisfy a regularity condition, namely $v_L(\Psi_i^j \rho) - v_L(\rho) = j \cdot ((v_L(\Psi_i \rho') - v_L(\rho'))$ for $0 \le j < p$, and for all $\rho, \rho' \in L$ satisfying the valuation criterion, $v_L(\rho), v_n(\rho') \equiv r(b) \bmod q$. Furthermore, if we define $\Psi^{(a)} = \prod_{s=0}^{n} \Psi_s^{a_{(s)}}$ for $a = \sum_s a_{(s)} p^s$, then $\{v_L(\Psi^{(a)}\rho) : 0 \le a < q\}$ is a complete set of residues modulo q.

The main result of [Eld09], restated here as Theorem 2.1, is that a Galois scaffold exists for L/K.

Theorem 2.1. *Let L/K be a near one-dimensional elementary abelian extension of degree $q = p^{n+1}$, let $G = \mathrm{Gal}(L/K)$ and let $b_{\max}$ be the*

largest lower ramification number of L/K. Then for $0 \le i \le n$ there exist elements Ψ_i in the augmentation ideal $(\sigma - 1 : \sigma \in G)$ of $K[G]$ such that $\Psi_i^p = 0$ and, for any $\rho \in L$ with $v_L(\rho) \equiv b_{\max} \pmod q$ and any $0 \le a < q$, we have

$$v_L\left(\Psi^{(a)}\rho\right) = v_L\left(\prod_{i=0}^{n} \Psi_i^{a_{(i)}} \cdot \rho\right) = v_L(\rho) + \sum_{i=0}^{n} a_{(i)} p^i b_{\max} = v_L(\rho) + a \cdot b_{\max}.$$

Proof. In [Eld09, Theorem 4.1], take $\Psi_i = \alpha_{n-i}(\Theta_{(i)} - 1)$. □

In the next two sections, we describe the associated order $\mathfrak{A}_{L/K}$ in terms of these Ψ_i, and show that $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$ if and only if $r(b) \in \mathcal{S}(q)$. To do so, we require nothing more than the existence of the Ψ_i described in Theorem 2.1, and the fact that, from (1), the parameter b in Theorem 1.1 satisfies $b \equiv b_{\max} \bmod q$.

2.2. **Associated order.** For the fixed prime power $q = p^{n+1}$, there is a partial order $\preceq$ on the integers $x \ge 0$ defined as follows. Recall the p-adic expansion of an integer: $x = \sum_{s=0}^{\infty} x_{(s)} p^s$ with $x_{(s)} \in \{0, \dots, p-1\}$. Define

$$x \preceq y \Leftrightarrow x_{(s)} \le y_{(s)} \text{ for } 0 \le s \le n.$$

Write $y \succeq x$ for $x \preceq y$. Note that $\preceq$ does not respect addition: if $0 \le x, y \le q-1$ then $x \preceq q-1-y$ is equivalent to $y \preceq q-1-x$ (both say that no carries occur in the base-p addition of x and y) but these are not equivalent to $x + y \preceq q - 1$ (which always holds).

Recall that for $a = \sum_s a_{(s)} p^s$, we have defined $\Psi^{(a)} = \prod_{s=0}^{n} \Psi_s^{a_{(s)}}$. Since $\Psi_s^p = 0$ for all s we have

$$\Psi^{(a)}\Psi^{(j)} = \begin{cases} \Psi^{(a+j)} & \text{if } a \preceq q-1-j; \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

Now set $d_a = \lfloor (1+a) b_{\max}/q \rfloor$ for $0 \le a \le q-1$. This means that $(1+a)b_{\max} = d_a q + r((1+a)b_{\max})$ with $0 \le r((1+a)b_{\max}) < q$. Let $\rho_* \in L$ be any element with valuation $v_L(\rho_*) = r(b) = r(b_{\max})$. Recall that $K = k((T))$ with $v_K(T) = 1$, so that $v_L(T) = q$. Set $\rho = T^{d_0}\rho_*$, so $v_L(\rho) = b_{\max}$, and set

$$\rho_a = T^{-d_a}\Psi^{(a)} \cdot \rho.$$

This means that, based upon Theorem 2.1, we have $v_L(\rho_a) = -qd_a + v_L(\rho) + ab_{\max} = -qd_a + (1+a)b_{\max} = r((1+a)b_{\max})$. Using (4), we also have

$$\Psi^{(j)} \cdot \rho_a = \begin{cases} T^{d_{a+j} - d_a}\rho_{j+a} & \text{if } a \preceq q-1-j \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

Lemma 2.2. *$\{\rho_a\}_{0 \le a \le q-1}$ is an $\mathfrak{O}_K$-basis for $\mathfrak{O}_L$. Moreover $\{\Psi^{(a)}\}_{0 \le a \le q-1}$ is a K-basis for the group algebra $K[G]$, and ρ generates a normal basis for the extension L/K.*

Proof. The first assertion follows from the fact that since $p \nmid b_{\max}$, $v_L(\rho_a) = r((1+a)b_{\max})$ takes all values in $\{0, \dots, q-1\}$ as a does. From the definition of the ρ_a, we then deduce that the elements $\Psi^{(a)} \cdot \rho$ span L over K. Comparing dimensions, it follows that ρ generates a normal basis, and that the $\Psi^{(a)}$ form a K-basis for $K[G]$. □

2.3. **Freeness over associated order.** Let $q = p^{n+1}$ and define

$$w_j = \min\{d_{a+j} - d_a \mid 0 \le a \le q-1, a \preceq q-1-j\}.$$

Then $w_0 = 0$ and (taking $a = 0$), we have $w_j \le d_j - d_0$ for all $0 \le j < q$.

We now give an overview of the remainder of the proof of Theorem 1.1. In Theorem 2.3, we will provide a necessary and sufficient condition, in terms of the w_j, for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_{L/K}$. We will also show that, when this condition holds, any $\rho_* \in L$ with $v_L(\rho_*) = r(b_{\max}) = r(b)$ is a free generator of $\mathfrak{O}_L$ over $\mathfrak{A}_{L/K}$. We will then show in Lemma 2.4 that this condition is equivalent to Miyata's condition, which appears as (i) in Lemma 1.6. Theorem 1.1 will then be an immediate consequence of Theorem 2.3, Lemma 2.4, and the equivalence of (i) and (ii) in Lemma 1.6.

Theorem 2.3. *Let L/K be any near one-dimensional elementary abelian extension L/K of degree $q = p^{n+1}$, with largest ramification number $b_{\max}$. The associated order $\mathfrak{A}_{L/K}$ of $\mathfrak{O}_L$ has $\mathfrak{O}_K$-basis $\{T^{-w_j}\Psi^{(j)}\}_{0 \le j \le q-1}$. Moreover $\mathfrak{O}_L$ is a free module over $\mathfrak{A}_{L/K}$ if and only if $w_j = d_j - d_0$ for all $0 \le j < q$, and in this case any element $\rho_* \in L$ with $v_L(\rho_*) = r(b_{\max})$ is a free generator of $\mathfrak{O}_L$ over $\mathfrak{A}_{L/K}$.*

Proof. Since $\{\Psi^{(j)}\}_{0 \le j \le q-1}$ is a K-basis of $K[G]$, any element α of $K[G]$ may be written $\alpha = \sum_{j=0}^{q-1} c_j \Psi^{(j)}$ with $c_j \in K$. Let ρ_* be as in the statement, and define ρ_a for $0 \le a \le q-1$ as in §2.2 above. Using (5) we have

$$\begin{aligned}
\alpha \in \mathfrak{A}_{L/K} &\Leftrightarrow \alpha \cdot \rho_a \in \mathfrak{O}_L \text{ for all } a \\
&\Leftrightarrow \sum_{j \preceq q-1-a} c_j T^{d_{j+a}-d_a} \rho_{j+a} \in \mathfrak{O}_L \text{ for all } a \\
&\Leftrightarrow c_j T^{d_{j+a}-d_a} \in \mathfrak{O}_K \text{ if } j \preceq q-1-a \\
&\Leftrightarrow v_K(c_j) \ge d_a - d_{j+a} \text{ if } j \preceq q-1-a \\
&\Leftrightarrow -v_K(c_j) \le w_j \text{ for all } j.
\end{aligned}$$

Hence the elements $T^{-w_j}\Psi^{(j)}$ form an $\mathfrak{O}_K$-basis of $\mathfrak{A}_{L/K}$.

Now suppose that $w_j = d_j - d_0$ for all j. As $\rho_* = \rho_0$, the definition of ρ_j yields $T^{-w_j}\Psi^{(j)} \cdot \rho_* = \rho_j$, so the basis elements $\{T^{-w_j}\Psi^{(j)}\}_{0 \le j \le q-1}$ of $\mathfrak{A}_{L/K}$ take ρ_* to the basis elements of $\{\rho_j\}_{0 \le j \le q-1}$ of $\mathfrak{O}_L$. Hence $\mathfrak{O}_L$ is a free $\mathfrak{A}_{L/K}$-module on the generator ρ_*.

Conversely, suppose that $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$, say $\mathfrak{O}_L = \mathfrak{A}_{L/K} \cdot \eta$ where $\eta = \sum_{r=0}^{q-1} x_r \rho_r$ with $x_r \in \mathfrak{O}_K$. Then $\{T^{-w_i}\Psi^{(i)} \cdot \eta\}_{0 \le i \le q-1}$

is an $\mathfrak{O}_K$-basis for $\mathfrak{O}_L$, and using (5) we have $T^{-w_i}\Psi^{(i)} \cdot \eta = \sum_{0\le r\preceq q-1-i} x_r T^{-w_i+d_{i+r}-d_r}\rho_{i+r}$, which is an $\mathfrak{O}_K$-linear combination of the ρ_j with $j \ge i$. In other words, there is an upper triangular matrix $(c_{i,j})$ with $c_{i,j} \in \mathfrak{O}_K$ such that $T^{-w_i}\Psi^{(i)} \cdot \eta = \sum_{j=i}^{q-1} c_{i,j}\rho_j$. This matrix is invertible, since $\{\rho_j\}_{0\le j\le q-1}$ is also an $\mathfrak{O}_K$-basis for $\mathfrak{O}_L$. Thus $v_K(c_{i,i}) = 0$ for $0 \le i < q$, which means that $v_K(x_0 T^{-w_i+d_{i+0}-d_0}) = 0$, and thus $w_j = d_j - d_0$ for all j, as required. □

Lemma 2.4. *$w_j = d_j - d_0$ for all $0 \le j < q$ if and only if condition (i) of Lemma 1.6 holds with $b_0 = r(b)$.*

Proof. The condition on the w_j can be restated as

$$d_{x+y} - d_x \ge d_y - d_0 \text{ if } x \preceq q-1-y. \tag{6}$$

As this is symmetric in x and y, we may assume $x \ge y$.

Let $i = q-1-x$, $j = q-1-y$ and $h = q-1-x-y$. So $i+j = q-1+h$. The first step is to prove that $0 \le y \le x \le q-1$ and $x \preceq q-1-y$ if and only if $0 \le h \le i \le j \le q-1$ and $\binom{i}{h} \not\equiv 0 \pmod p$. Observe that $\binom{i}{h} \not\equiv 0 \pmod p$ holds if and only if there are no carries in the base-p addition of h and $i-h = y$ (see for example [Rib89, p. 24]).

Observe that $x \preceq q-1-y$ means that $x_{(s)} + y_{(s)} \le p-1$ for all $0 \le s \le n$. Using the definition of h, this means that $h \ge 0$ and $h_{(s)} = p-1-x_{(s)}-y_{(s)}$ for all $0 \le s \le n$. So $0 \le y \le x \le q-1$ and $x \preceq q-1-y$ means that $0 \le h \le i \le j \le q-1$ and $h_{(s)} + y_{(s)} \le p-1$ for all $0 \le s \le n$. No carries occur in the base-p addition of h and y.

On the other hand, assume that $0 \le h \le i \le j \le q-1$, $h_{(s)} + y_{(s)} \le p-1$ for all $0 \le s \le n$, and for a contradiction that there is an s such that $x_{(s)} + y_{(s)} \ge p$. We may assume that s is the smallest such subscript. Thus $x_{(r)} + y_{(r)} \le p-1$ for all $0 \le r < s$ and $x_{(s)} + y_{(s)} = p + c_s$ where $0 \le c_s \le p-1$. This means that $h_{(r)} = p-1-x_{(r)}-y_{(r)}$ for all $0 \le r < s$, and $h_{(s)} = p-1-c_s$. So $h_{(r)} + y_{(r)} \le p-1$ for all $0 \le r < s$ and $h_{(s)} + y_{(s)} = p-1-c_s+y_{(s)} = 2p-1-x_{(s)} \ge p$.

Since $b_0 = r(b)$, we have $t_0 = q - r(b) = r(-b)$. It therefore only remains to show that the inequality $d_{x+y} - d_x \ge d_y - d_0$ corresponds to $r(-b) + r(-ib) - r(-hb) > 0$. For any $j \in \mathbb{Z}$, we have $r(jb_{\max}) = r(jb)$. Thus, for $0 \le m \le q-1$, we have $(m+1)b_{\max} = qd_m + r((m+1)b)$, so that $q(d_{x+y} - d_x) = yb_{\max} - r((x+y+1)b) + r((x+1)b)$. Hence

$$\begin{aligned} & d_{x+y} - d_x \ge d_y - d_0 \\ & \quad \Leftrightarrow \quad yb_{\max} - r((x+y+1)b) + r((x+1)b) \ge yb_{\max} - r((y+1)b) + r(b) \\ & \quad \Leftrightarrow \quad -r(-hb) + r(-ib) \ge -r(-jb) + q - r(-b) \\ & \quad \Leftrightarrow \quad r(-b) + r(-ib) - r(-hb) \ge q - r(-jb). \end{aligned}$$

Now $r(-b)+r(-ib)-r(-hb) \equiv -r(-jb) \pmod q$ since $i+j = q-1+h$, and $1 \le q - r(-jb) \le q$. Thus the last inequality is equivalent to $r(-b) + r(-ib) - r(-hb) > 0$, as required. □

References

[Aib03] Akira Aiba, *Artin-Schreier extensions and Galois module structure*, J. Number Theory **102** (2003), no. 1, 118–124.

[BBF72] Françoise Bertrandias, Jean-Paul Bertrandias, and Marie-Josée Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sci. Paris Sér. A-B **274** (1972), A1388–A1391.

[BE] Nigel P. Byott and G. Griffith Elder, *Galois scaffolds and Galois module structure in extensions of characteristic p local fields of degree p^2*, arXiv:1106.3577 [math.NT].

[BF72] Françoise Bertrandias and Marie-Josée Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sci. Paris Sér. A-B **274** (1972), A1330–A1333.

[Byo08] Nigel P. Byott, *On the integral Galois module structure of cyclic extensions of p-adic fields*, Q. J. Math. **59** (2008), no. 2, 149–162.

[dST07] Bart de Smit and Lara Thomas, *Local Galois module structure in positive characteristic and continued fractions*, Arch. Math. (Basel) **88** (2007), no. 3, 207–219.

[Eld09] G. Griffith Elder, *Galois scaffolding in one-dimensional elementary abelian extensions*, Proc. Amer. Math. Soc. **137** (2009), no. 4, 1193–1203.

[Mar74] Bruno Martel, *Sur l'anneau des entiers d'une extension biquadratique d'un corps 2-adique*, C. R. Acad. Sci. Paris Sér. A **278** (1974), 117–120.

[Miy95] Yoshimasa Miyata, *On the Galois module structure of ideals and rings of all integers of $\mathfrak{P}$-adic number fields*, J. Algebra **177** (1995), no. 3, 627–646.

[Miy98] ———, *On the module structure of rings of integers in $\mathfrak{P}$-adic number fields over associated orders*, Math. Proc. Cambridge Philos. Soc. **123** (1998), no. 2, 199–212.

[Miy04] ———, *Maximal tame extensions over Hopf orders in rings of integers of $\mathfrak{P}$-adic number fields*, J. Algebra **276** (2004), no. 2, 794–825.

[Rib89] Paulo Ribenboim, *The book of prime number records*, second ed., Springer-Verlag, New York, 1989.

College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter EX4 4QE U.K.

E-mail address: N.P.Byott@ex.ac.uk

Department of Mathematics, University of Nebraska at Omaha, Omaha, NE 68182-0243 U.S.A.

E-mail address: elder@unomaha.edu