

GALOIS SCAFFOLDING IN ONE-DIMENSIONAL ELEMENTARY ABELIAN EXTENSIONS

G. GRIFFITH ELDER

(Communicated by Ted Chinburg)

ABSTRACT. A *Galois scaffold* is defined to be a variant of a normal basis that allows for an easy determination of valuation and thus has implications for the questions of the Galois module structure. We introduce a class of elementary abelian p -extensions of local function fields of characteristic p , which we call *one-dimensional* and which should be considered no more complicated than cyclic degree p extensions, and show that they, just as cyclic degree p extensions, possess a Galois scaffold.

1. INTRODUCTION

The Normal Basis Theorem states that in a finite Galois extension L/K with $G = \text{Gal}(L/K)$, there are elements $\rho \in L$ whose conjugates $\{\sigma\rho : \sigma \in G\}$ provide a basis for L over K . In the setting of local field extensions, the most important property of an element is its valuation, and so we asked the following question in [5] about the valuations of these elements: Is there a valuation (integer certificate) that guarantees that any element bearing this valuation is a normal basis generator? In other words, is there a $v \in \mathbb{Z}$ such that $\rho \in L$ and $v_L(\rho) = v$ implies that $\{\sigma\rho : \sigma \in G\}$ is a basis for L over K ?

In this paper, we ask for more. Let L/K be a fully ramified p -extension of local fields with perfect residue field of characteristic p , and let v_L denote the normalized, additive valuation. We ask, in addition to the existence of an integer certificate v , that there be a set of $t = \log_p |G|$ elements $\theta_i \in K[G]$ which depend on the extension L/K but are independent of ρ with $v_L(\rho) = v$ such that $\{v_L(\prod_{i=1}^t \theta_i^{j_i} \rho) : 0 \leq j_i \leq p-1\}$ is a complete set of residues modulo $|G|$. Of course, this means that $\{\prod_{i=1}^t \theta_i^{j_i} : 0 \leq j_i \leq p-1\}$ is a basis for the group ring $K[G]$ over K . These two ingredients, an integer certificate and a particularly nice basis, make up what we call a *Galois scaffold*.

Cyclic, ramified extensions of degree p form the prototype for our considerations. Suppose now that L/K is cyclic of degree p with $G = \langle \sigma \rangle$. Assume that the ramification break number for L/K is b and $\gcd(p, b) = 1$. This does not restrict the extension when K has characteristic p and is a minor restriction when K has

Received by the editors May 17, 2007, and, in revised form, July 21, 2007, September 12, 2007, and April 8, 2008.

2000 *Mathematics Subject Classification*. Primary 11R33, 11S15.

Key words and phrases. Ramification, Galois module structure.

The author was partially supported by National Science Foundation Grant No. 201080.

©2008 American Mathematical Society
Reverts to public domain 28 years from publication

characteristic 0 [7, III. Prop 2.3]. If $\rho \in L$ with $v_L(\rho) \equiv b \pmod p$, then $v_L((\sigma - 1)^j \rho) \equiv (j + 1)b \pmod p$ for $0 \leq j \leq p - 1$. In particular, $v_L((\sigma - 1)^j \rho)$ is a complete set of residues modulo p . We have a Galois scaffold: Choose any integer $\equiv b \pmod p$ along with $\{(\sigma - 1)^j : 0 \leq j \leq p - 1\}$.

Galois scaffolds are not universally available. Consider, for an example, any unramified extension where there is no integer certificate. Indeed, Galois scaffolds should be viewed as normal bases with an advantage: the valuation of any element expressed in terms of a Galois scaffold can be easily determined. In the example above, since L/K is fully ramified, every $\alpha \in L$ can be expressed as $\alpha = \sum_{i=0}^{p-1} a_i(\sigma - 1)^i \rho$ for some $a_i \in K$. Then $v_L(\alpha) = \min\{v_L(a_i) + ib + v_L(\rho) : 0 \leq i \leq p - 1\}$. We repeat ourselves for emphasis. Normal bases and power bases (polynomial bases) in a prime element are two common bases. The first allows the Galois action to be easily followed. The second allows the valuation to be easily determined. These two properties are in tension. So Galois scaffolds are remarkable for the delicate balance that they achieve.

The Galois scaffold for ramified cyclic extensions of degree p makes the questions of Galois module structure in these extensions tractable [1, 2, 3, 6]. In this paper, we restrict our attention to fully ramified elementary abelian extensions of local function fields that are, in a particular sense, as simple as a ramified cyclic extension of degree p . We call these extensions one-dimensional, respectively near one-dimensional, elementary abelian extensions (see §4), and give, for them, an explicit Galois scaffold.

We will use the following notation throughout the paper. Let p be a prime integer and let \mathbb{F}_p be the finite field with p elements. Let $K = \mathbb{F}((t))$ be a local function field with perfect residue field \mathbb{F} of characteristic p . Let $\varphi : K \rightarrow K$ denote the \mathbb{F}_p -linear map $\varphi(x) = x^p - x$, and let ϕ denote the ring homomorphism $\phi(x) = x^p$. Use subscripts to denote the field of reference. So π_K is a prime element of K , and v_K is the valuation normalized so that $v_K(\pi_K^s) = s$. Let $\mathfrak{O}_K = \{x \in K : v_K(x) \geq 0\}$ be the valuation ring, and let $\mathfrak{P}_K = \pi_K \mathfrak{O}_K$ be its maximal ideal. Let L/K denote a fully ramified Galois p -extension, with $G = \text{Gal}(L/K)$. Define its ramification filtration by

$$G_i = \{\sigma \in G : v_L((\sigma - 1)\pi_L) \geq i + 1\}.$$

Define the binomial coefficient $\binom{X}{i} = X \cdot (X - 1) \cdots (X - i + 1)/i! \in \mathbb{Q}[X]$, and define *truncated exponentiation* by the polynomial that results from the truncation of the binomial series at the p th term:

$$(1) \quad (1 + X)^{[Y]} := \sum_{i=0}^{p-1} \binom{Y}{i} X^i \in \mathbb{Z}_{(p)}[X, Y],$$

where $\mathbb{Z}_{(p)}$ denotes the integers localized at p .

2. CYCLIC EXTENSIONS OF DEGREE p

Consider our prototype now in greater detail: Let L/K be a ramified cyclic extension of degree p . So $L = K(x)$ with $\varphi(x) = x^p - x = \beta$ for some $\beta \in K$, $v_K(\beta) = -b$, $b > 0$ and $\text{gcd}(b, p) = 1$. Let $\text{Gal}(L/K) = \langle \sigma \rangle$ with $\sigma x = x + 1$. Since $\varphi(x) = \beta$ is a statement about the norm of x , namely $N_{L/K}(x) = \beta$, we have $v_L(x) = -b$. Since $v_L((\sigma - 1)x) = 0$, the ramification break number for L/K is b . Write $x^p - x = \beta$ as $x \cdot \binom{x-1}{p-1} = -\beta$, so the binomial coefficient $\binom{x-1}{p-1}$ generates

L/K . Notice, using (1), that $\sigma^{[i]} = \sigma^i$ for $0 \leq i \leq p - 1$. Moreover, there is a striking similarity between

$$\sigma^{[i]} \binom{x - 1}{p - 1} = \binom{x - 1 + i}{p - 1} \text{ for } i \in \mathbb{F}_p$$

and the equation in

Lemma 2.1. *Let L/K be a cyclic, ramified extension of degree p with x and σ as above. Given $A \in L$,*

$$\sigma^{[A]} \binom{x - 1}{p - 1} = \binom{x - 1 + A}{p - 1}.$$

Proof. A nice observation of [6] is that Pascal’s identity $\binom{X-1}{i-1} + \binom{X-1}{i} = \binom{X}{i} \in \mathbb{Q}[X]$ for $1 \leq i \leq p - 1$ means $(\sigma - 1)\binom{x-1}{i} = \binom{x-1}{i-1}$, and therefore $(\sigma - 1)^i \binom{x-1}{p-1} = \binom{x-1}{p-1-i}$. Substituting $X = \sigma - 1$ and $Y = A \in L$ in (1), we find $\sigma^{[A]} \binom{x-1}{p-1} = \sum_{i=0}^{p-1} \binom{A}{i} (\sigma - 1)^i \binom{x-1}{p-1} = \sum_{i=0}^{p-1} \binom{A}{i} \binom{x-1}{p-1-i} \in L$. We now use Vandermonde’s Convolution Identity $\sum_{i=0}^{p-1} \binom{X}{i} \binom{Y}{p-1-i} = \binom{X+Y}{p-1} \in \mathbb{Z}_{(p)}[X, Y]$, which results from considering the coefficient of Z^{p-1} in the identity $(1+Z)^X (1+Z)^Y = (1+Z)^{X+Y} \in \mathbb{Q}[X, Y][[Z]]$. Set $X = A$ and $Y = x - 1$. So $\sum_{i=0}^{p-1} \binom{A}{i} \binom{x-1}{p-1-i} = \binom{x-1+A}{p-1} \in L$. \square

In [4] a refined ramification filtration was introduced, which grew out of the possibility that the natural \mathbb{F}_p -action on σ could be extended to a residue field “action”, a possibility that is certainly suggested by this lemma. In this paper, the lemma motivates a Galois scaffold.

3. A GALOIS SCAFFOLD

In this section, we begin with an abelian p -extension that we organize using the ramification filtration. This “organization” defines a matrix $(\Delta_{i,j})_{0 \leq i,j \leq n}$. If the coefficients of $(\Delta_{i,j})_{0 \leq i,j \leq n}$ lie in our base field K , the extension satisfies a strong assumption, which makes it possible for us to construct a Galois scaffold, but also makes the extension elementary abelian. At the end of the section, one question remains: Are there any elementary abelian extensions that satisfy this strong assumption? In §4, we construct extensions that do.

Let K_n/K be a fully ramified abelian extension of degree p^{n+1} . A Galois scaffold for the case $n = 0$ was given in §1. So assume $n \geq 1$. Let $G = \text{Gal}(K_n/K)$ with break numbers $b_1 < \dots < b_m$ such that $G = G_{b_1}, G_{b_i} \supsetneq G_{b_{i+1}} = G_{b_{i+1}}$ and $G_{b_m+1} = \langle e \rangle$. Because K has characteristic p , $\gcd(b_1, p) = 1$, and by [8, IV, §2, Prop. 11], $b_i \equiv b_1 \pmod p$. Organize the extension by choosing a filtration of $n + 1$ subgroups $G_{(i)} \subseteq G$ that include the ramification groups G_i and satisfy $G_{(i)}/G_{(i+1)} \cong C_p$. So

$$G = G_{(0)} \supsetneq G_{(1)} \supsetneq \dots \supsetneq G_{(n)} \supsetneq G_{(n+1)} = \langle e \rangle.$$

Indeed, since each quotient of consecutive ramification groups is elementary abelian, this is easy to do. Now for each i , pick $\sigma_i \in G_{(i)} \setminus G_{(i+1)}$. So $G_{(i)} = \langle \sigma_i, \sigma_{i+1}, \dots, \sigma_n \rangle$, though $\{\sigma_i, \dots, \sigma_n\}$ is probably not a minimal generating set. For $i \geq 0$, let K_{i-1} be the fixed field of $G_{(i)}$, with $K_{-1} = K$ and define $b_{(i)} = v_n((\sigma_i - 1)\pi_n) - 1$. This means that $b_{(0)} \leq \dots \leq b_{(n)}$ is a list of $n + 1$ integers, which are not necessarily distinct. We get $b_1 < \dots < b_m$ from this list by eliminating repetitions. Since K_n/K is abelian, the Hasse-Arf Theorem states that the upper ramification numbers are

integers [8, IV §3], which is equivalent to $b_i \equiv b_m \pmod{[G : G_{b_{i+1}}]}$ for $1 \leq i \leq m$, and also to

$$(2) \quad b_{(i)} \equiv b_{(n)} \pmod{p^{i+1}} \text{ for } 0 \leq i \leq n.$$

Since $\{b_{(0)}, \dots, b_{(n)}\}$ is the set of ramification break numbers for K_n/K , the ramification break numbers for K_i/K are $\{b_{(0)}, \dots, b_{(i)}\}$ [8, IV, §1, Prop. 3, Cor.]. Therefore K_i/K_{i-1} has ramification break number $b_{(i)}$, $\text{Gal}(K_i/K_{i-1}) = G_{b_{(i)}}/G_{b_{(i+1)}} = \langle \bar{\sigma}_i \rangle \cong C_p$, and there are $X_i \in K_i$ such that $v_i(X_i) = -b_{(i)}$, $\wp(X_i) = X_i^p - X_i \in K_{i-1}$ and $\sigma_i X_i = X_i + 1$. Define

$$\Delta_{i,j} = (\sigma_i - 1)X_j.$$

So $\Delta_{i,j} = 0$ when $i > j$, $\Delta_{i,i} = 1$ for all i and $v_j(\Delta_{i,j}) = v_j((\sigma_i - 1)X_j) = b_{(i)} - b_{(j)} \leq 0$ for $i < j$. Collect these $\Delta_{i,j}$ into a matrix $(\Delta) = (\Delta_{i,j})_{0 \leq i,j \leq n}$. Motivated by the fact that we want a basis for $K[G]$ over K , we impose

Assumption 1. $\Delta_{i,j} \in K$ for all $0 \leq i, j \leq n$.

Lemma 3.1. *Under Assumption 1, K_n/K is elementary abelian.*

Proof. Since $v_n(X_n) = -b_{(n)}$, $\text{gcd}(v_n(X_n), p) = 1$ and thus $K_n = K(X_n)$. Since $\Delta_{i,n} \in K$, $\sigma_i^k X_n = X_n + k\Delta_{i,n}$ for $0 \leq k \leq p$. So $\sigma_i^p X_n = X_n$ for all $0 \leq i \leq n$. \square

Define $\Theta_{(0)} = \sigma_n$ and $\Theta_{(i)} \in K[\sigma_n, \sigma_{n-1}, \dots, \sigma_{n-i}]$ recursively for $1 \leq i \leq n$ by

$$(3) \quad \Theta_{(i)} = \sigma_{n-i} \Theta_{(0)}^{[-\Delta_{n-i,n}]} \Theta_{(1)}^{[-\Delta_{n-i,n-1}]} \dots \Theta_{(i-1)}^{[-\Delta_{n-i,n-(i-1)}]},$$

using truncated exponentiation. Note that each $\Theta_{(i)}$ is a 1-unit, *i.e.* $\Theta_{(i)} \in 1 + (\sigma - 1 : \sigma \in G) \subseteq K[G]$, where $(\sigma - 1 : \sigma \in G)$ is the augmentation ideal. Note that $\alpha^p = 0$ for all $\alpha \in (\sigma - 1 : \sigma \in G)$. So $(\Theta_{(i)} - 1)^p = 0$, and thus $\Theta_{(i)}^{[\Delta_{j,k}]} \Theta_{(i)}^{[-\Delta_{j,k}]} = 1$. As a result, since $\Delta_{n-r,n-r} = 1$, we can rewrite (3) as $\sigma_{n-i} = \Theta_{(0)}^{[\Delta_{n-i,n}]} \Theta_{(1)}^{[\Delta_{n-i,n-1}]} \dots \Theta_{(i-1)}^{[\Delta_{n-i,n-(i-1)}]} \Theta_{(i)}^{[\Delta_{n-i,n-i}]}$. If we replace multiplication by addition and truncated exponentiation by multiplication, a vector of these units, namely $(\Theta_{(n-j)})$, solves the matrix equation

$$\begin{pmatrix} \Delta_{0,0} & \Delta_{0,1} & \cdots & \Delta_{0,n} \\ 0 & \Delta_{1,1} & \cdots & \Delta_{1,n} \\ & & \ddots & \\ 0 & \cdots & 0 & \Delta_{n,n} \end{pmatrix} \cdot \begin{pmatrix} \Theta_{(n)} \\ \Theta_{(n-1)} \\ \vdots \\ \Theta_{(0)} \end{pmatrix} = \begin{pmatrix} \sigma_0 \\ \sigma_1 \\ \vdots \\ \sigma_n \end{pmatrix}.$$

However, truncated exponentiation does not distribute. (It is easy to check that for $p = 2$, the units $(\Theta_{(i)}\Theta_{(j)})^{[\Delta]}$ and $\Theta_{(i)}^{[\Delta]}\Theta_{(j)}^{[\Delta]}$ are not equal.) So we cannot apply the inverse matrix $(\Delta)^{-1}$ to both sides of this equation and preserve the equality. Since the vectors $(\Theta_{(n-j)})$ and $(\Delta)^{-1} \cdot (\sigma_i)$ are unequal, this matrix equation is simply a convenient way to express the recursive definition – no more, no less.

Lemma 3.2. *For $0 \leq i, j \leq n$,*

$$\Theta_{(i)} \begin{pmatrix} X_j \\ p-1 \end{pmatrix} = \begin{cases} \begin{pmatrix} X_j \\ p-1 \end{pmatrix} & \text{if } j \neq n-i, \\ \begin{pmatrix} X_{j+1} \\ p-1 \end{pmatrix} & \text{if } j = n-i. \end{cases}$$

Proof. We use induction on i . For $i = 0$, $\Theta_{(0)} = \sigma_n$ and the result is clear. Now assume the result for $0 \leq i < k$ and consider $\Theta_{(k)} \binom{X_j}{p-1}$. Recall that $\Theta_{(k)}$ is a product (3) and examine the effect of each factor $\Theta_{(i)}^{[-\Delta_{n-k, n-i}]}$ of $\Theta_{(k)}$ on $\binom{X_j}{p-1}$. By induction $(\Theta_{(i)} - 1)^r \binom{X_j}{p-1} = 0$ for $r > 0$ and $j \neq n - i$, and $(\Theta_{(i)} - 1)^r \binom{X_{n-i}}{p-1} = \binom{X_{n-i}}{p-1-r}$ for $0 \leq r \leq p - 1$. Arguing as in Lemma 2.1, we have

$$\Theta_{(i)}^{[-\Delta_{n-k, n-i}]}\binom{X_j}{p-1} = \begin{cases} \binom{X_j}{p-1} & \text{for } j \neq n - i, \\ \binom{X_j - \Delta_{n-k, j}}{p-1} & \text{for } j = n - i. \end{cases}$$

If $j < n - k$, then every factor of $\Theta_{(k)}$ and thus $\Theta_{(k)}$ acts trivially on $\binom{X_j}{p-1}$. If $j = n - k$, then $\sigma_{n-k} = \sigma_j$ is the only factor of $\Theta_{(k)}$ to act nontrivially, and $\sigma_j \binom{X_j}{p-1} = \binom{X_j+1}{p-1}$. If $j > n - k$, then two factors of $\Theta_{(k)}$ act nontrivially, σ_{n-k} and $\Theta_{(n-j)}^{[-\Delta_{n-k, j}]}$. So $\Theta_{(k)} \binom{X_j}{p-1} = \sigma_{n-k} \Theta_{(n-j)}^{[-\Delta_{n-k, j}]}\binom{X_j}{p-1} = \sigma_{n-k} \binom{X_j - \Delta_{n-k, j}}{p-1} = \binom{X_j}{p-1}$. \square

It is natural to consider a product of these binomial coefficients, such as $\rho = \prod_{j=0}^n \binom{X_j}{p-1}$. So that the valuation of ρ can be described more simply, we use (2) to choose $\alpha_j \in K$ with $v_j(\alpha_j) = b_{(n)} - b_{(j)}$. Therefore $v_j(\alpha_j^{-(p-1)} \binom{X_j}{p-1}) = -(p-1)b_{(n)}$ for $0 \leq j \leq n$. Choose $\alpha \in K$ with $v_K(\alpha) = b_{(n)}$. Define $\mathcal{A} = \alpha \prod_{j=0}^n \alpha_j^{-(p-1)} \in K$, and define

$$\mathbb{X} = \mathcal{A}\rho = \alpha \prod_{j=0}^n \alpha_j^{-(p-1)} \binom{X_j}{p-1},$$

which has valuation $v_n(\mathbb{X}) = p^{n+1}b_{(n)} - (p-1) \sum_{j=0}^n p^{n-j}b_{(n)} = b_{(n)} = b_m$. For $0 \leq r \leq p - 1$, we have $(\Theta_{(i)} - 1)^r \mathbb{X} = \mathbb{X} \binom{X_{n-i}}{p-1-r} \binom{X_{n-i}}{p-1}^{-1}$ and hence $v_n(\alpha_{n-i}^r (\Theta_{(i)} - 1)^r \mathbb{X}) = b_{(n)} + rp^i b_{(n)}$. Therefore given $c_i \in \{0, 1, \dots, p-1\}$, we have

$$(4) \quad v_n \left(\prod_{i=0}^n \alpha_{n-i}^{c_i} (\Theta_{(i)} - 1)^{c_i} \mathbb{X} \right) = v_n(\mathbb{X}) + \sum_{i=0}^n c_i p^i b_{(n)} = \left(1 + \sum_{i=0}^n c_i p^i \right) b_{(n)}.$$

Proposition 3.3. *Under Assumption 1, we have a Galois scaffold. Let $\mathbf{X} \in K_n$ be any element with $v_n(\mathbf{X}) \equiv b_{(n)} = b_m \pmod{p^{n+1}}$. Let $\Theta_{(i)} \in K[G]$ be as defined in (3), let $c_i \in \{0, 1, \dots, p-1\}$, and let $\alpha_j \in K$ with $v_K(\alpha_j) = (b_{(n)} - b_{(j)})/p^{j+1} \in \mathbb{Z}$. Then*

$$v_n \left(\prod_{i=0}^n \alpha_{n-i}^{c_i} (\Theta_{(i)} - 1)^{c_i} \mathbf{X} \right) = v_n(\mathbf{X}) + \sum_{i=0}^n c_i p^i b_m.$$

Proof. Using (4), $\{\prod_{i=0}^n \alpha_{n-i}^{c_i} (\Theta_{(i)} - 1)^{c_i} \mathbb{X} : 0 \leq c_i \leq p-1\}$ is a basis for K_n over K . Express \mathbf{X} as a linear combination of these basis elements. It is enough to show that when we apply $\prod_{i=0}^n \alpha_{n-i}^{d_i} (\Theta_{(i)} - 1)^{d_i}$ with $0 \leq d_i \leq p-1$ to any term in this linear combination, we increase the valuation by at least $\sum_{i=0}^n d_i p^i b_m$. In particular, we need to show that when we apply it to $\prod_{i=0}^n \alpha_{n-i}^{c_i} (\Theta_{(i)} - 1)^{c_i} \mathbb{X}$ we get

$$v_n \left(\prod_{i=0}^n \alpha_{n-i}^{c_i+d_i} (\Theta_{(i)} - 1)^{c_i+d_i} \mathbb{X} \right) \geq v_n \left(\prod_{i=0}^n \alpha_{n-i}^{c_i} (\Theta_{(i)} - 1)^{c_i} \mathbb{X} \right) + \sum_{i=0}^n d_i p^i b_m.$$

If any sum $c_i + d_i \geq p$, then $(\Theta_{(i)} - 1)^{c_i+d_i} = 0$ and the valuation of the left-hand side is infinite. So we are left with the case where all sums $c_i + d_i < p$. But in this case, we can use (4) to determine that we have equality. \square

4. ONE-DIMENSIONAL AND NEAR ONE-DIMENSIONAL
ELEMENTARY ABELIAN EXTENSIONS

In this section, we define one-dimensional and near one-dimensional elementary abelian extensions L/K and organize each such extension by ordering its generators. This defines a matrix (Ω^ϕ) with coefficients in K . The main result of the section is that this “organization” agrees with that of §3. Indeed, we have the matrix equation $(\Delta) \cdot (\Omega^\phi) = I$, where (Δ) is as in §3. Thus L satisfies Assumption 1, (Δ) has coefficients in K , and L possesses a Galois scaffold.

It is a basic observation in Artin-Schreier Theory that elementary abelian extensions of K correspond to finite subspaces of the \mathbb{F}_p -vector space, K/K^\wp , where K^\wp is the image of \wp . Define $K_{(n)} = \phi^n(K) = \mathbb{F}((t^{p^n}))$ with $n \geq 1$. Then $K/K_{(n)}$ is an inseparable field extension, and K is a vector space over $K_{(n)}$. Pick any $\beta \in K$ with $p \nmid v_L(\beta) < 0$. This means that β maps nontrivially into K/K^\wp and $K_{(n)}\beta$ is a one-dimensional subspace of K , one that injects into K/K^\wp . It seems reasonable to call those elementary abelian extensions of K that are associated with finite \mathbb{F}_p -subspaces of the image of $K_{(n)}\beta$ in K/K^\wp one-dimensional. Moreover it seems reasonable to hypothesize that they should closely resemble cyclic extensions of degree p and thus possibly possess a Galois scaffold. This hypothesis is validated below under an assumption on the size of the extension.

We define L/K to be a *one-dimensional elementary abelian extension* of degree p^{n+1} if $L = K(x_0, \dots, x_n)$ with $\wp(x_i) = x_i^p - x_i = \phi^n(\Omega_i) \cdot \beta$ for some $\beta \in K$ with $p \nmid v_K(\beta) = -b < 0$, and some $\Omega_i \in K$ that span an $(n + 1)$ -dimensional subspace over \mathbb{F}_p . Without loss of generality we may organize these generators by setting $\Omega_0 = 1$, assuming $v_K(\Omega_n) \leq \dots \leq v_K(\Omega_1) \leq v_K(\Omega_0) = 0$, and furthermore assuming that whenever $v_K(\Omega_i) = \dots = v_K(\Omega_j)$ for $i < j$, the projections of $\Omega_i, \dots, \Omega_j$ into $\Omega_i \mathfrak{D}_K / \Omega_i \mathfrak{P}_K$ are linearly independent over \mathbb{F}_p . This final assumption means that $K(x_i, \dots, x_j)$ has one break in its ramification filtration at $-v_K(\phi^n(\Omega_i)\beta)$.

More generally, our Galois scaffold will apply to the broader class of *near one-dimensional elementary abelian extensions*, where $\wp(x_i) \equiv \phi^n(\Omega_i) \cdot \beta + \epsilon_i$ for some error terms $\epsilon_i \in K$ that satisfy a technical bound: For $1 \leq i \leq n$, define $m_i = v_K(\Omega_{i-1}) - v_K(\Omega_i) \geq 0$, and assume that for $1 \leq i \leq n$,

$$\begin{aligned}
 (5) \quad v_K(\epsilon_i) &> -\frac{b}{p^n} - \sum_{j=1}^i p^j m_j + \sum_{j=i+1}^n (p^n - p^j) m_j \\
 &= v_K(\phi^n(\Omega_i)\beta) + \frac{(p^n - 1)b}{p^n} - (p - 1) \sum_{j=1}^{n-1} p^j v_K(\Omega_j).
 \end{aligned}$$

Note that since $v_K(\Omega_j) \leq 0$, this technical bound is stronger than $v_K(\epsilon_i) > v_K(\phi^n(\Omega_i)\beta)$. Thus whenever $v_K(\Omega_i) = \dots = v_K(\Omega_j)$ for $i < j$, it continues to be the case that $K(x_i, \dots, x_j)$ has one break in its ramification filtration at $-v_K(\phi^n(\Omega_i)\beta)$.

4.1. Main Theorem. We define a matrix (Ω^ϕ) : Let $\Omega_j^{(0)} = \Omega_j$, and perform the following elementary row operations on the matrix $\left(\phi^i(\Omega_j^{(0)})\right)_{0 \leq i, j \leq n}$, which resembles the square root of a discriminant matrix. The first column is a column of 1's. So start with the $i = n$ row and work up to the $i = 1$ row, subtracting the $(i - 1)$ st row from the i th row. The $i = 0$ row and $j = 0$ column of our matrix now

agree with (6) below. Ignore them. The result is $(\phi^{i-1}(\wp(\Omega_j^{(0)})))_{1 \leq i, j \leq n}$. Divide each entry in a row by the first entry of the row and get

$$\left(\frac{\phi^{i-1}(\wp(\Omega_j^{(0)}))}{\wp(\Omega_1^{(0)})} \right)_{1 \leq i, j \leq n}.$$

Define $\Omega_j^{(1)} = \wp(\Omega_j^{(0)})/\wp(\Omega_1^{(0)})$ for $1 \leq j \leq n$. Observe that $v_K(\Omega_n^{(1)}) \leq \dots \leq v_K(\Omega_1^{(1)}) = 0$ and that the set $\{\Omega_j^{(1)}\}_{1 \leq j \leq n}$ spans an n -dimensional vector space over \mathbb{F}_p . We have a matrix $(\phi^{i-1}(\wp(\Omega_j^{(1)})))_{1 \leq i, j \leq n}$ whose first column is a column of 1's. Again, starting with the $i = n$ row and working up to the $i = 2$ row, we subtract the $(i - 1)$ st row from the i th row. If we continue, following the same sequence of steps as above, and repeat as often as necessary, we get a matrix over K :

$$(6) \quad (\Omega) = \begin{pmatrix} 1 & \Omega_1^{(0)} & \Omega_2^{(0)} & \dots & \Omega_n^{(0)} \\ 0 & 1 & \Omega_2^{(1)} & \dots & \Omega_n^{(1)} \\ & & \ddots & & \\ 0 & 0 & \dots & 1 & \Omega_n^{(n-1)} \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

with entries in row i that are at or above the diagonal. Moreover $\{\Omega_j^{(i)}\}_{i \leq j \leq n}$ is the set of nonzero entries in row i . It is linearly independent over \mathbb{F}_p , and defined recursively in terms of the nonzero entries in row $i-1$ by $\Omega_j^{(i)} = \wp(\Omega_j^{(i-1)})/\wp(\Omega_i^{(i-1)})$. Let

$$(\Omega^\phi) = (\phi^{n-i-1}(\Omega_j^{(i)}))_{0 \leq i, j \leq n}.$$

In §4.2 we prove that $(\Delta) \cdot (\Omega^\phi) = I$, where (Δ) is as in §3. This means that near one-dimensional elementary abelian extensions satisfy Assumption 1 and that the $\Theta_{(i)}$ defined in (3) can be defined in terms of the Ω_j of this section. Thus using Proposition 3.3, we obtain the main result of the paper.

Theorem 4.1. *Let L/K be a near one-dimensional elementary abelian extension. Let $\Theta_{(i)} \in K[\text{Gal}(L/K)]$ be defined as in (3). For $1 \leq i \leq n$, let $m_i = v_K(\Omega_{i-1}) - v_K(\Omega_i)$, and for $0 \leq j \leq n$ choose $\alpha_j \in K$ with $v_K(\alpha_j) = p^{n-j-1} \sum_{i=j+1}^n p^i m_i$. Let b_m be the largest (lower) ramification break number of L/K . Given any $\rho \in L$ with $v_L(\rho) \equiv b_m \pmod{p^{n+1}}$ and any $a_s \in \{0, \dots, p-1\}$ with $0 \leq s \leq n$,*

$$v_L \left(\prod_{s=0}^n \alpha_{n-s}^{a_s} (\Theta_{(s)} - 1)^{a_s} \rho \right) = v_L(\rho) + \sum_{s=0}^n a_s p^s b_m.$$

As the integers $\sum_{s=0}^n a_s p^s$ run through all possibilities from 0 to $p^{n+1} - 1$, the integers $(\sum_{s=0}^n a_s p^s) b_m$ run through all residues modulo p^{n+1} . This yields

Corollary 4.2. *L has a Galois scaffold.*

Corollary 4.3. *Any element in L of valuation b_m generates a normal field basis.*

This last corollary provides evidence for the Conjecture in [5] that fully ramified, elementary abelian p -extensions in characteristic p possess integer certificates (as in the definition of Galois scaffold).

4.2. **Proof of $(\Delta) \cdot (\Omega^\phi) = I$.** Choose $\sigma_i \in G = \text{Gal}(L/K)$, based upon our choice of generators, so that we have the equality of matrices: $((\sigma_i - 1)x_j)_{0 \leq i, j \leq n} = (\delta_{ij})_{0 \leq i, j \leq n} = I$ (i.e. $\sigma_i x_i = x_i + 1$ and $\sigma_i x_j = x_j$ for $j \neq i$). This gives a filtration $H_{(i)} = \langle \sigma_i, \dots, \sigma_n \rangle$ of G . Let $K_{i-1} = K(x_0, \dots, x_{i-1})$ be the fixed field of $H_{(i)}$. So $K_{-1} = K$ and $K_n = L$. Then

$$u_{(i)} = b + p^n \sum_{j=1}^i m_j = -v_K(\phi^n(\Omega_i)\beta)$$

is the ramification number of $K(x_i)/K$, and is therefore an upper ramification number of L/K . Our assumptions on the Ω_i mean that $\{u_{(0)}, \dots, u_{(n)}\}$ is the set of upper ramification numbers. Use the Herbrand function $\psi(x)$ [8, IV, §3] to pass to the lower ramification numbers. Again, our assumptions on the Ω_i mean that $\{b_{(0)}, \dots, b_{(n)}\}$ with

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

is the set of lower ramification numbers. Moreover, $b_{(i)}$ is the ramification number of K_i/K_{i-1} . The groups $H_{(i)}$ can now be identified with the $G_{(i)}$ defined in §3, and we begin to see that the two organizations (by ramification groups in §3 and by generators in §4) might agree.

To see that the two organizations actually agree, we proceed to construct the $X_j \in K_j$ of §3 as follows: First, in §4.2.1, we construct $X_j \in K_j$ such that $((\sigma_i - 1)X_j)_{0 \leq i, j \leq n} \cdot (\Omega^\phi) = I$. Then in §4.2.2, using (5), we prove that $v_j(X_j) = -b_{(j)}$. Therefore $(\Delta) = ((\sigma_i - 1)X_j)_{0 \leq i, j \leq n}$, and thus $(\Delta) \cdot (\Omega^\phi) = I$.

4.2.1. *Construction of the $X_j \in K_j$.* Let $X_j^{(0)} = x_j$. Recall the definition of the $\Omega_j^{(i)}$, and for $j \geq i$, recursively define

$$(7) \quad X_j^{(i)} = X_j^{(i-1)} - \phi^{n-i}(\Omega_j^{(i-1)})X_{i-1}^{(i-1)}.$$

If we use this definition to replace $X_j^{(i-1)}$ in (7) with $X_j^{(i-2)} - \phi^{n-i+1}(\Omega_j^{(i-2)})X_{i-2}^{(i-2)}$, we find $X_j^{(i)} = X_j^{(i-2)} - \phi^{n-i+1}(\Omega_j^{(i-2)})X_{i-2}^{(i-2)} - \phi^{n-i}(\Omega_j^{(i-1)})X_{i-1}^{(i-1)}$. Continue in this way until $X_j^{(i)} = X_j^{(0)} - \sum_{k=0}^{i-1} \phi^{n-k-1}(\Omega_j^{(k)})X_k^{(k)}$. Consider $i = j$. Since $x_j = X_j^{(0)}$ and $\Omega_j^{(j)} = 1$, this becomes $x_j = \sum_{k=0}^j \phi^{n-k-1} \Omega_j^{(k)} X_k^{(k)}$.

Let $X_j = X_j^{(j)}$, for $0 \leq j \leq n$. Clearly $K_j = K(x_0, \dots, x_j) = K(X_0^{(0)}, \dots, X_j^{(j)}) = K(X_0, \dots, X_j)$. Moreover the collection of equations,

$$x_j = \sum_{k=0}^j \phi^{n-k-1} \Omega_j^{(k)} X_k^{(k)} = \sum_{k=0}^j \phi^{n-k-1} \Omega_j^{(k)} X_k,$$

can be rewritten as the matrix equation

$$(X_0, X_1, \dots, X_n) \cdot (\Omega^\phi) = (x_0, x_1, x_2, \dots, x_n).$$

Since $I = ((\sigma_i - 1)x_j)_{0 \leq i, j \leq n}$, we have

$$(8) \quad ((\sigma_i - 1)X_j)_{0 \leq i, j \leq n} \cdot (\Omega^\phi) = I.$$

4.2.2. *Proof that $v_j(X_j) = -b_{(j)}$.* Since the $\Omega_j^{(i)}$ are an important ingredient in $X_j = X_j^{(j)}$, we begin with

Lemma 4.4. *For $0 \leq i < j \leq n$,*

$$v_K(\Omega_j^{(i)}) = -p^i \sum_{k=i+1}^j m_k.$$

Proof. We use induction on i . Since $m_k = v_K(\Omega_{k-1}^{(0)}) - v_K(\Omega_k^{(0)})$, the result holds for $i = 0$. For $i \geq 1$, assume the result for $i-1$. Recall (6) and the fact that the elements of $\Omega_{i-1}^{(i-1)} = 1, \Omega_i^{(i-1)}, \dots, \Omega_n^{(i-1)}$ are linearly independent over \mathbb{F}_p . In particular, $\Omega_j^{(i-1)} \notin \mathbb{F}_p$ for $i \leq j \leq n$. Since $v_K(\Omega_n^{(i-1)}) \leq \dots \leq v_K(\Omega_i^{(i-1)}) \leq v_K(\Omega_{i-1}^{(i-1)}) = 0$, we have $v_K(\wp(\Omega_j^{(i-1)})) = pv_K(\Omega_j^{(i-1)})$. Using the recursive definition for $\Omega_j^{(i)}$, we find $v_K(\Omega_j^{(i)}) = pv_K(\Omega_j^{(i-1)}) - pv_K(\Omega_i^{(i-1)})$. \square

To assist in our analysis of $v_j(X_j^{(j)})$, define $B_0 = \beta$, $E_j^{(0)} = \epsilon_j$ for $j > 0$. Then for $0 < i < j$ define $E_i^{(i)} = 0$, and recursively define $E_j^{(i)} = E_j^{(i-1)} - \phi^{n-i}(\Omega_j^{(i)})E_i^{(i-1)}$ along with

$$(9) \quad B_i = -\phi^{n-i}(\wp(\Omega_i^{(i-1)}))X_{i-1}^{(i-1)} + E_i^{(i-1)}.$$

The significance of these elements lies in the following result.

Lemma 4.5. *For $j \geq i$,*

$$\wp(X_j^{(i)}) = \phi^{n-i}(\Omega_j^{(i)})B_i + E_j^{(i)}.$$

Proof. We use induction on i . For $i = 0$, this is clear. So we assume $\wp(X_j^{(i-1)}) = \phi^{n-i+1}(\Omega_j^{(i-1)})B_{i-1} + E_j^{(i-1)}$ and in particular, $\wp(X_{i-1}^{(i-1)}) = B_{i-1}$. Consider $\wp(X_j^{(i)})$. Notice $\wp(aX) = \phi(a)\wp(X) + \wp(a)X$. So using (7) we find that

$$\begin{aligned} \wp(X_j^{(i)}) &= \wp(X_j^{(i-1)}) - \phi^{n-i+1}(\Omega_j^{(i-1)})\wp(X_{i-1}^{(i-1)}) - \phi^{n-i}(\wp(\Omega_j^{(i-1)}))X_{i-1}^{(i-1)} \\ &= \phi^{n-i+1}(\Omega_j^{(i-1)})B_{i-1} + E_j^{(i-1)} - \phi^{n-i+1}(\Omega_j^{(i-1)})B_{i-1} \\ &\quad - \phi^{n-i}(\wp(\Omega_j^{(i-1)}))X_{i-1}^{(i-1)} = E_j^{(i-1)} - \phi^{n-i}(\wp(\Omega_j^{(i-1)}))X_{i-1}^{(i-1)}, \end{aligned}$$

which, using (9) and the definition of $\Omega_j^{(i)}$, agrees with the statement for i . \square

Lemma 4.6. *Assume the bounds given in (5). Then for $1 \leq i \leq n$, we have*

$$v_K(E_i^{(i-1)}) > -b_{(i)}/p^i.$$

Proof. Use Lemma 4.4 to determine that (5) is equivalent to $v_K(\phi^{n-i}(\Omega_n^{(i)})\epsilon_i) > -b_{(n)}/p^n$. We are interested in $v_K(E_i^{(i-1)})$. Recall $E_j^{(i)} = E_j^{(i-1)} - \phi^{n-i}(\Omega_j^{(i)})E_i^{(i-1)}$ for $j > i$, which means that $E_j^{(i)} = E_j^{(0)} - \sum_{k=1}^i \phi^{n-k}(\Omega_j^{(k)})E_k^{(k-1)}$, and so

$$(10) \quad E_i^{(i-1)} = \epsilon_i - \sum_{k=1}^{i-1} \phi^{n-k}(\Omega_i^{(k)})E_k^{(k-1)}.$$

In order that $v_K(E_i^{(i-1)}) > -b_{(i)}/p^i$ for $1 \leq i \leq n$, it is sufficient to prove

$$(11) \quad v_K(\epsilon_i) > -b_{(i)}/p^i \text{ for } 1 \leq i \leq n, \text{ and}$$

$$(12) \quad v_K(\phi^{n-k}(\Omega_i^{(k)})E_k^{(k-1)}) > -b_{(i)}/p^i \text{ for } 1 \leq k \leq i-1 \leq n-1.$$

Let $c_i = -b_{(i)}/p^i + v_K(\phi^{n-i}(\Omega_n^{(i)}))$. Using Lemma 4.4, we find that $-b_{(i)}/p^i + v_K(\phi^{n-i}(\Omega_n^{(i)})) = -b_{(i-1)}/p^i + v_K(\phi^{n-i+1}(\Omega_n^{(i-1)}))$. As a result, $c_i > c_{i-1}$, since $-b_{(i-1)}/p^i > -b_{(i-1)}/p^{i-1}$. Using (5), $v_K(\phi^{n-i}(\Omega_n^{(i)})\epsilon_i) > -b_{(n)}/p^n = c_n$. So $v_K(\phi^{n-i}(\Omega_n^{(i)})\epsilon_i) > c_j$ for all j , including $j = i$. Therefore (11) follows from (5). Focus now on (12), which is equivalent to $v_K(E_k^{(k-1)}) > d_i^k$, where $d_i^k = -b_{(i)}/p^i - v_K(\phi^{n-k}(\Omega_i^{(k)}))$. Since $-b_{(i)}/p^i - v_K(\phi^{n-k}(\Omega_i^{(k)})) = -b_{(i-1)}/p^i - v_K(\phi^{n-k}(\Omega_{i-1}^{(k)}))$, we have $d_i^k > d_{i-1}^k$. Thus (12) is equivalent to

$$(13) \quad v_K(\phi^{n-k}(\Omega_n^{(k)})E_k^{(k-1)}) > -b_{(n)}/p^n \text{ for } 1 \leq k \leq n-1.$$

Switch i and k in (10) and apply $\phi^{n-k}(\Omega_n^{(k)})$ to both sides: $\phi^{n-k}(\Omega_n^{(k)})E_k^{(k-1)} = \phi^{n-k}(\Omega_n^{(k)})\epsilon_k - \sum_{i=1}^{k-1} \phi^{n-k}(\Omega_n^{(k)})\phi^{n-i}(\Omega_k^{(i)})E_i^{(i-1)}$. By Lemma 4.4, $v_K(\phi^{n-i}(\Omega_n^{(i)})) = v_K(\phi^{n-k}(\Omega_n^{(k)})\phi^{n-i}(\Omega_k^{(i)}))$. Therefore (13) follows from (5) by induction on k . \square

Lemma 4.7. *Assume the bounds in (5). Then for $0 \leq j \leq n$, $v_j(X_j^{(j)}) = -b_{(j)}$.*

Proof. It is clear that $v_0(X_0^{(0)}) = -b_{(0)}$. So for $i > 0$, assume that $v_{i-1}(X_{i-1}^{(i-1)}) = -b_{(i-1)} = -b - p^n \sum_{j=1}^{i-1} p^j m_j$. Using Lemma 4.4, we see that $v_K(\wp(\Omega_i^{(i-1)})) = -p^i m_i$. So $v_K(\phi^{n-i}(\wp(\Omega_i^{(i-1)}))) = -p^n m_i$ and therefore $v_{i-1}(\phi^{n-i}(\wp(\Omega_i^{(i-1)}))) = -p^n \cdot p^i m_i$. So $v_{i-1}(\phi^{n-i}(\wp(\Omega_i^{(i-1)})X_{i-1}^{(i-1)})) = -b_{(i)}$. By Lemma 4.6, $v_{i-1}(E_i^{(i-1)}) > -b_{(i)}$. Therefore $v_{i-1}(B_i) = -b_{(i)}$. Lemma 4.5 implies that in particular the norm $N_{K_i/K_{i-1}}(X_i^{(i)}) = \wp(X_i^{(i)}) = B_i$, which means that $v_i(X_i^{(i)}) = -b_{(i)}$. \square

5. EXAMPLES OF NEAR ONE-DIMENSIONAL
ELEMENTARY ABELIAN EXTENSIONS

Lemma 5.1. *Fully ramified biquadratic extensions (so $p = 2$) are near one-dimensional elementary abelian extensions.*

Proof. Let $L = K(x_0, x_1)$ with $x_0^2 - x_0 = \beta$, $x_1^2 - x_1 = \beta_1$, $v_K(\beta_1) \leq v_K(\beta) < 0$ and both of $v_K(\beta_1)$ and $v_K(\beta)$ odd. Because $v_K(\beta) - v_K(\beta_1)$ is even, there is a $\mu_0 \in K$ such that $\mu_0^2 \beta_1 \equiv \beta \pmod{\beta \mathfrak{P}_K}$. So $\beta = \mu_0^2 \beta_1 + \tau_0$ for some $v_K(\tau_0) > v_K(\beta)$. We can replace β by any element in $\beta + K^\wp$. So $v_K(\tau_0) \geq 0$, or $v_K(\tau_0) < 0$ with $v_K(\tau_0)$ odd. If $v_K(\tau_0)$ odd, there is a $\mu_1 \in K$ such that $\mu_1^2 \beta_1 \equiv \tau_0 \pmod{\tau_0 \mathfrak{P}_K}$, and thus $\beta = (\mu_0 + \mu_1)^2 \beta_1 + \tau_1$ for $v_K(\tau_1) > v_K(\tau_0)$. Continue until $\beta = \mu^2 \beta_1 + \tau$ for $\mu \in K$ and either $\tau = 0$ or $v_K(\tau) = 0$. If $\tau = 0$, L/K is one-dimensional. If $v_K(\tau) = 0$, then $\beta_1 = \Omega_1^2 \beta + \epsilon_1$, where $\epsilon_1 = \tau \mu^{-2}$ and $\Omega_1 = \mu^{-1}$. So $b = -v_K(\beta)$, $m_1 = -v_K(\Omega_1) = v_K(\mu)$, and $v_K(\epsilon_1) = -2m_1 > -b/2 - 2m_1$ satisfies (5). \square

Lemma 5.2. *Let $\mathbb{F}_q \subseteq \mathbb{F}$ for some $q = p^f$, and suppose that $\beta \in K$ with $v_K(\beta) < 0$ and $\gcd(v_K(\beta), p) = 1$. Then $L = K(y)$ with $y^q - y = \beta$ is a one-dimensional elementary abelian extension of K .*

Proof. Let $q = p^f$ and $\{1 = \omega_0, \omega_1, \dots, \omega_{f-1}\}$ be a basis for \mathbb{F}_q over \mathbb{F}_p . Then $x_i = \sum_{r=0}^{f-1} \phi^r(\omega_i y)$ satisfies $x_i^p - x_i = \omega_i \beta$. Set $\Omega_i = \phi^{-f+1}(\omega_i)$. \square

Lemma 5.3. *Let L/K be a noncyclic, fully and weakly ramified p -extension. Then L/K is a near one-dimensional elementary abelian extension.*

Proof. Weakly ramified means $G_2 = \{e\}$. Since $G = G_1$, L/K is elementary abelian [8, IV §2]. The one ramification break is 1. So $L = K(x_0, \dots, x_n)$ with $v_K(\wp(x_i)) = -1$. Let $\beta = \wp(x_0)$. So $\wp(x_i) \equiv \omega_i \beta \pmod{\mathfrak{D}_K}$ for some $\omega_i \in \mathbb{F}$. Since ϕ is an automorphism of \mathbb{F} , set $\Omega_i = \phi^{-n}(\omega_i)$. So $\wp(x_i) = \phi^n(\Omega_i)\beta + \epsilon_i$ with $v_K(\epsilon_i) \geq 0 > -1/p^n = -b/p^n$, and (5) holds. \square

REFERENCES

1. Akira Aiba, *Artin-Schreier extensions and Galois module structure*, J. Number Theory **102** (2003), no. 1, 118–124. MR1994476 (2004f:11127)
2. 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. MR0296047 (45:5108)
3. Z. I. Borevič and S. V. Vostokov, *The ring of integral elements of an extension of prime degree of a local field as a Galois module*, Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **31** (1973), 24–37. MR0330112 (48:8450)
4. Nigel P. Byott and G. Griffith Elder, *New ramification breaks and additive Galois structure*, J. Théor. Nombres Bordeaux **17** (2005), no. 1, 87–107, Les XXIIIèmes Journées Arithmétiques (Graz, 2003). MR2152213 (2006b:11149)
5. ———, *A valuation criterion for normal bases in elementary abelian extensions*, Bull. Lond. Math. Soc. **39** (2007), no. 5, 705–708. MR2365217
6. 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. MR2305599 (2008b:11120)
7. I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions*, second ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, Providence, RI, 2002. MR1915966 (2003c:11150)
8. J-P. Serre, *Local fields*, Springer-Verlag, New York, 1979. MR554237 (82e:12016)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF NEBRASKA AT OMAHA, OMAHA, NEBRASKA
68182-0243

E-mail address: elder@unomaha.edu