SUFFICIENT CONDITIONS FOR LARGE GALOIS SCAFFOLDS

NIGEL P. BYOTT AND G. GRIFFITH ELDER

Abstract. Let L/K be a finite Galois, totally ramified p-extension of complete local fields with perfect residue fields of characteristic $p > 0$. In this paper, we give conditions, valid for any Galois p-group $G = \mathrm{Gal}(L/K)$ (abelian or not) and for K of either possible characteristic (0 or p), that are sufficient for the existence of a Galois scaffold. The existence of a Galois scaffold makes it possible to address questions of integral Galois module structure, which is done in a separate paper [BCE]. But since our conditions can be difficult to check, we specialize to elementary abelian extensions and extend the main result of [Eld09] from characteristic p to characteristic 0. This result is then applied, using a result of Bondarko, to the construction of new Hopf orders over the valuation ring $\mathfrak{O}_K$ that lie in $K[G]$ for G an elementary abelian p-group.

1. Introduction

Let p be prime, κ be a perfect field of characteristic p, and K be a local field with residue field κ. Let L be a totally ramified Galois extension of K with $G = \mathrm{Gal}(L/K)$ of degree p^n for some $n > 0$, and let $\mathfrak{O}_L$ be the ring of integers of L (*i.e.* its valuation ring). *Local integral Galois module theory* asks a question that is a consequence of three classical results: the Normal Basis Theorem, which states that L *is free* over the group algebra $K[G]$; a result of E. Noether [Noe32], which concludes that, because L/K is wildly ramified, $\mathfrak{O}_L$ *is not free* over the group ring $\mathfrak{O}_K[G]$; and a local version of a result of H. W. Leopoldt [Leo59], which states that for absolute abelian extensions of the p-adic numbers (*i.e.* $K = \mathbb{Q}_p$), $\mathfrak{O}_L$ *is free* over its associated order

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

the largest $\mathfrak{O}_K$-order in the group algebra $K[G]$ for which $\mathfrak{O}_L$ is a module.

Question 1.1. When is the ring of integers $\mathfrak{O}_L$ free over its associated order $\mathfrak{A}_{L/K}$?

Restrict for the moment to the situation where K is a finite extension of $\mathbb{Q}_p$. The earliest answers here showed us that unless $K = \mathbb{Q}_p$, $\mathfrak{O}_L$ need not be free over $\mathfrak{A}_{L/K}$, which is why the question is currently asked in this way. Additionally, those early answers suggested a form that we might expect the answers to take. Based upon work of F. Bertrandias and M.-J. Ferton [BF72] when L/K is a C_p-extension, and B. Martel [Mar74] when L/K is a $C_2 \times C_2$-extension, we might expect the answer to Question 1.1, necessary and sufficient conditions for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_{L/K}$, to be expressed in terms of the ramification numbers associated with the extension (integers i such that $G_i \neq G_{i+1}$ where G_i is the ith ramification group

Date: June 8, 2017.
2010 *Mathematics Subject Classification.* Primary 11S15, Secondary 11R33, 16T05.
Key words and phrases. Galois module structure, Hopf order.

[Ser79, IV §1]). There have not been that many further results in this direction. Still,

(1) When L/K is an abelian extension, and the ring of integers is replaced with the inverse different $\mathfrak{D}_{L/K}^{-1}$, [Byo97, Theorem 3.10] determines necessary conditions, in terms of ramification numbers, for the inverse different to be free over its associated order.
(2) When $K/\mathbb{Q}_p$ is unramified and L/K is a totally ramified abelian extension (not necessarily of p-power degree), D. Burns [Bur91] investigated freeness of ideals in $\mathfrak{O}_L$ over their associated orders in $K[G]$. This was extended in [Bur00] to the case where $K/\mathbb{Q}_p$ can be ramified, but associated orders are considered in $\mathbb{Q}_p[G]$ (or, more generally, in $E[G]$, where $E \subseteq K$ and $E/\mathbb{Q}_p$ is unramified). In both these situations, the existence of *any* ideal free over its associated order forces strong restrictions on the extension L/K.
(3) When L/K is a special type of cyclic Kummer extension, namely $L = K(\sqrt[p^n]{1+\beta})$ for some $\beta \in K$ with $p \nmid v_K(\beta) > 0$, where v_K is the normalized valuation on K, Y. Miyata determines necessary and sufficient conditions for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_{L/K}$ in terms of $v_K(\beta)$. These conditions can be restated in terms of ramification numbers [Miy98].
(4) Finally, we move into characteristic p with $K = \kappa((t))$. When L/K is a special type of elementary abelian extension, namely *near one-dimensional*, and thus has a *Galois scaffold* [Eld09], necessary and sufficient conditions for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_{L/K}$ are given in terms of ramification numbers [BE14].

Interestingly, the conditions on the ramification numbers in [BE14] agree with those given in [Miy98] (as translated by [Byo08]).

The purpose of this paper is to extend the setting where Galois scaffolds have been proven to exist, namely [Eld09, BE13]: from characteristic p to characteristic 0, and from elementary abelian (or cyclic of degree p^2) p-groups to all p-groups (abelian or not). We do this, in Theorem 2.10, by determining conditions sufficient for a Galois scaffold to exist that are independent of characteristic and of Galois group. When an extension L/K satisfies the hypotheses of Theorem 2.10 and thus possesses a Galois scaffold, the answer to Question 1.1 is provided in [BCE], where necessary and sufficient conditions are given, not just for $\mathfrak{O}_L$, but for each fractional ideal $\mathfrak{P}_L^i$ of $\mathfrak{O}_L$, to be free over its associated order. Indeed, stronger questions, such as those asked by B. de Smit and L. Thomas in [dST07], are also addressed. Each answer is given in terms of ramification numbers.

On the other hand, given only the generators of an extension, it is not easy to determine whether the extension satisfies the conditions of Theorem 2.10. Thus in §3, we describe, in terms of Artin-Schreier generators, arbitrarily large elementary abelian p-extensions that do satisfy the conditions of Theorem 2.10 and thus possess a Galois scaffold. In characteristic 0, the result is new. These are the analogs of the near one-dimensional elementary abelian extensions of [Eld09]. In §4, to illustrate the level of explicit detail that is then possible when the results of this paper are combined with [BCE], we include results in characteristic 0, on the structure of $\mathfrak{P}_L^i$ over its associated order, for certain families of elementary abelian extensions that are of common interest.

Finally, to illustrate the utility of our results beyond local integral Galois module theory, we explain how the results of this paper combined with [Bon00, BCE] can be used to attack the difficult problem of classifying Hopf orders in the group algebra $K[G]$ for G some p-group. This is an old problem. The first result in this direction is that of Tate and Oort [TO70] for Hopf orders of rank p. And yet, the classifications for $G \cong C_p^3, C_{p^3}$ remain incomplete [CS05, Proposition 15], [UC06, Theorem 5.4]. Notably, the Hopf orders that are missing for $G \cong C_p^3$ include those which are realizable as the associated orders of valuation rings, and it is precisely such Hopf orders that the results of this paper are designed to produce. Indeed, §5 can be viewed as providing a model, given any p-group G, for the construction of such "realizable" Hopf orders in $K[G]$. As such, it provides motivation for future work identifying extensions that satisfy the hypotheses of Theorem 2.10.

We close this introduction by pointing out that our work is somewhat similar in spirit to that of Bondarko [Bon00, Bon02, Bon06], who also considers the existence of ideals free over their associated orders in the context of totally ramified Galois extensions of p-power degree. Bondarko introduces the class of semistable extensions. Any such extension contains at least one ideal free over its associated order, and all such ideals can be determined from numerical data. Moreover, any abelian extension containing an ideal free over its associated order, and satisfying certain additional assumptions, must be semistable. Abelian semistable extensions can be completely characterized in terms of the Kummer theory of (one-dimensional) formal groups. The precise relationship between Bondarko's results and our own remains to be explored.

1.1. **Discussion of our approach.** The existence of a Galois scaffold addresses an issue, which is illustrated in the following two examples. Let v_K, v_L denote the normalized valuations for K, L, respectively. Choose $\pi \in K$ with $v_K(\pi) = 1$.

Example 1.2. Fix a local field K and suppose that L/K is a totally ramified Galois extension of degree p. Let σ generate G. Then L/K has a unique ramification break b, and this is characterized by the property that, for all $\alpha \in L\backslash\{0\}$,

$$v_L((\sigma - 1) \cdot \alpha) \geq v_L(\alpha) + b, \text{ with equality if } p \nmid v_L(\alpha).$$

Let us suppose for simplicity that $b \equiv -1 \bmod p$, say $b = pr - 1$ with $r \geq 1$. Fix a uniformizing parameter π of K, and let $\Psi = (\sigma - 1)/\pi^r \in K[G]$. Pick any $\rho \in L$ with $v_L(\rho) = p - 1$. Then, for $0 \leq j \leq p - 1$, we have $v_L(\Psi^j \cdot \rho) = p - 1 - j$. Thus Ψ typically reduces valuations by 1, and the $\Psi^j \cdot \rho$ for $0 \leq j \leq p - 1$ form an $\mathfrak{O}_K$-basis of $\mathfrak{O}_L$. Two conclusions follow: firstly, that the Ψ^j form an $\mathfrak{O}_K$-basis of the associated order $\mathfrak{A}_{L/K}$, and, secondly, that $\mathfrak{O}_L$ is a free module over $\mathfrak{A}_{L/K}$, generated by any element ρ of valuation $p - 1$.

Example 1.2 in itself is nothing new. Indeed, far more comprehensive treatments of the valuation ring of an extension of degree p are given in [BF72, BBF72] for the characteristic 0 case, and in [Aib03, dST07] for characteristic p. (See also [Fer73] for arbitrary ideals in characteristic 0, and [Huy14] and [Mar14] for the corresponding problem in characteristic p.) We now consider what happens if we try to make the same argument for a larger extension.

Example 1.3. Let L/K be a totally ramified extension of degree p^2. We now have two ramification breaks $b_1 \leq b_2$ (in the lower numbering), and we necessarily have $b_1 \equiv b_2 \bmod p$. For simplicity we assume that $b_i \equiv -1 \bmod p^2$, say $b_i = r_i p^2 - 1$, for $i = 1, 2$. We can then find elements σ_1, σ_2 which generate $\mathrm{Gal}(L/K)$ and for which, setting $\Psi_i' = (\sigma_i - 1)/\pi^{r_i}$, we have

$$v_L(\Psi_i' \cdot \alpha) \geq v_L(\alpha) - 1 \text{ for } i = 1, 2, \text{ with equality if } p \nmid v_L(\alpha)$$

whenever $\alpha \in L \backslash \{0\}$. Thus Ψ_1' and Ψ_2' both typically reduce valuations by 1, but this does not enable us to determine $\mathfrak{A}_{L/K}$. Now suppose that we could replace Ψ_1', Ψ_2' with elements Ψ_1, Ψ_2 such that, for some suitable choice of $\rho \in L$ with $v_L(\rho) = p^2 - 1$, we had

$$v_L(\Psi_1^{j_1}\Psi_2^{j_2} \cdot \rho) = p^2 - 1 - j_1 p - j_2 \text{ for all } 0 \leq j_1, j_2, \leq p - 1. \tag{1}$$

Thus, at least on the family of elements of L of the form $\Psi_i^{i_1}\Psi_2^{i_2} \cdot \rho$, we can say that Ψ_1 typically reduces valuations by p, whilst Ψ_2 typically reduces valuations by 1. We could then deduce that the elements $\Psi_1^{j_1}\Psi_2^{j_2}$ form an $\mathfrak{O}_K$-basis of $\mathfrak{A}_{L/K}$, and that $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$ on the generator ρ. Such elements Ψ_i would essentially constitute a Galois scaffold.

The reason that we cannot determine $\mathfrak{A}_{L/K}$ in Example 1.3 using the original elements Ψ_1' and Ψ_2' is that we have insufficient information about their effect on elements of L whose valuation is divisible by p but not by p^2. It is because of this problem that early attempts to treat other cases in the same manner as degree p extensions achieved only limited success. (See for instance [Fer75] for cyclic extensions of degree p^n, $n \geq 2$, and, temporarily relaxing the condition that L/K has p-power degree, [Fer72, Ber72] for dihedral extensions of degree $2p$. A complete treatment of biquadratic extensions of 2-adic fields was, however, given in [Mar74].)

1.2. **Intuition of a scaffold.** The intuition underlying a scaffold can be explained, as is done in [BCE], somewhat informally. For the convenience of the reader, we replicate it here: Given any positive integers b_i for $1 \leq i \leq n$ such that $p \nmid b_i$ (think of lower ramification numbers), there are elements $X_i \in L$ such that $v_L(X_i) = -p^{n-i}b_i$. Since the valuations, v_L, of the monomials

$$\mathbb{X}^a = X_n^{a_{(0)}} X_{n-1}^{a_{(1)}} \cdots X_1^{a_{(n-1)}} : 0 \leq a_{(i)} < p,$$

provide a complete set of residues modulo p^n and L/K is totally ramified of degree p^n, these monomials provide a convenient K-basis for L. The action of the group ring $K[G]$ on L is clearly determined by its action on the monomials $\mathbb{X}^a$. So if there were $\Psi_i \in K[G]$ for $1 \leq i \leq n$ such that each Ψ_i acts on the monomial basis element $\mathbb{X}^a$ of L as if it were the differential operator d/dX_i and the X_i were independent variables, namely

$$\Psi_i \mathbb{X}^a = a_{(n-i)} \mathbb{X}^a / X_i, \tag{2}$$

then the monomials in the Ψ_i (with exponents bound $< p$) would furnish a convenient basis for $K[G]$ whose effect on the $\mathbb{X}^a$ would be easy to determine. As a consequence, the determination of $\mathfrak{A}_{L/K}$, and of the structure of $\mathfrak{O}_L$ over $\mathfrak{A}_{L/K}$ would be reduced to a purely numerical calculation involving the b_i. This remains true if (2) is loosened to the congruence,

$$\Psi_i \mathbb{X}^a \equiv a_{(n-i)} \mathbb{X}^a / X_i \bmod (\mathbb{X}^a / X_i)\mathfrak{P}_L^{\mathfrak{c}} \tag{3}$$

for a sufficiently large "precision" $\mathfrak{c}$. The Ψ_i, together with the $\mathbb{X}^a$, constitute a Galois scaffold on L.

The formal definition of a scaffold [BCE, Definition 2.3] generalizes this situation. Indeed, given this intuitive connection with differentiation, it is perhaps not surprising that scaffolds can be constructed from higher derivations on an inseparable extension, as is done in [BCE, §5]. Ironically, with this perspective it may now be surprising that they can be constructed for Galois extensions under the action of the action of $K[G]$. Yet, this is where they were first constructed [Eld09].

2. Main Result: Construction of Galois scaffold

Recall that K is a complete local field whose residue field is perfect of characteristic $p > 0$, and that L/K is a totally ramified Galois extension of degree p^n. Relabel now, so that $L/K = K_n/K_0$. Following common practice, we use subscripts to denote field of reference. So $v_n \colon K_n \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ is the normalized valuation, and π_n is a prime element of K_n with $v_n(\pi_n) = 1$. The valuation ring of K_n is denoted by $\mathfrak{O}_n$ with maximal ideal $\mathfrak{P}_n$. Let $G_i = \{\sigma \in G : v_n((\sigma - 1)\pi_n) \geq i + 1\}$ be the ith group in the ramification filtration of the Galois group $G = \mathrm{Gal}(K_n/K_0)$.

In this section we construct a Galois scaffold, in Theorem 2.10, for extensions K_n/K_0 that satisfy three assumptions, which in turn depend upon two choices. For emphasis, we repeat here that K_0 may have characteristic 0 or p. The Galois group G can be nonabelian, as well as abelian. We also point out that, except for Assumption 2.9, all these choices and assumptions appear in [Eld09]. Our first choice organizes the extension.

Choice 2.1. Choose a composition series for G that refines the ramification filtration: $\{H_i\} \supseteq \{G_i\}$ such that $H_0 = G$, $H_n = \{e\}$ and $H_{i-1}/H_i \cong C_p$. Furthermore, choose one element to represent each degree p quotient: $\sigma_i \in H_{i-1} \setminus H_i$.

Let $K_i = K_n^{H_i}$ be the fixed field of H_i, and let $b_i = v_n((\sigma_i - 1)\pi_n) - 1$. Because of Choice 2.1, we can see, using [Ser79, IV§1], that the multiset $B = \{b_i : 1 \leq i \leq n\}$ is the set of lower ramification numbers, namely the set of subscripts i with $G_i \supsetneq G_{i+1}$, with multiplicity $\log_p |G_{b_i}/G_{b_i+1}|$. In particular, $b_1 \leq b_2 \leq \cdots \leq b_n$, $\{b_i : j < i \leq n\}$ is the ramification multiset for K_n/K_j, $\{b_i : 0 < i \leq j\}$ is the ramification multiset for K_j/K_0, and b_j is the lower ramification number for K_j/K_{j-1}. The set of upper ramification numbers $\{u_i\}$ is determined by

$$u_i = b_1 + \frac{b_2 - b_1}{p} + \cdots + \frac{b_i - b_{i-1}}{p^{i-1}} = (p-1)\left(\frac{b_1}{p} + \cdots + \frac{b_i}{p^i}\right) + \frac{b_i}{p^i} \tag{4}$$

[Ser79, IV§3]. Furthermore note that $\{u_i : 0 < i \leq j\}$ is the set of upper ramification numbers for K_j/K_0, but that $\{u_i : j < i \leq n\}$ is not necessarily the set of upper ramification numbers for K_n/K_j.

Our first assumption is weak, as it does not eliminate any extension in characteristic p. In characteristic 0, it eliminates only maximally ramified extensions, *i.e.* those cyclic extensions K_n/K_0 where K_0 contains the pth roots of unity and $K_1 = K_0(\sqrt[p]{\pi_0})$ for some prime element $\pi_0 \in K_0$ [Ser79, IV§2 Exercise 3].

Assumption 2.2. $p \nmid b_1$.

Now we choose generators for K_n/K_0 based upon Choice 2.1. Since the valuation v_j is normalized so that $v_j(K_j^\times) = \mathbb{Z}$, there are $Y_j \in K_j$ with $v_j(Y_j) = -b_j$. Since $v_j((\sigma_j - 1)Y_j) = 0$, a unit $u \in K_0$ exists such that $v_j(\sigma_j - 1)u^{-1}Y_j - 1) > 0$.

Choice 2.3. For each $1 \leq j \leq n$, choose $X_j \in K_j$ such that $v_j(X_j) = -b_j$ and $v_j((\sigma_j - 1)X_j - 1) > 0$.

Since $b_j \equiv b_1 \bmod p$ [Ser79, IV§2], we have $p \nmid b_j$ and therefore $K_j = K_{j-1}(X_j)$.

Remark 2.4. Since $p \nmid b_j$, we could choose X_j so that, additionally, it satisfies an Artin-Schreier equation $X_j^p - X_j \in K_{j-1}$ [FV02, III §2 Proposition 2.4]. In characteristic 0, this is a result of MacKenzie and Whaples. We do not make this a requirement however, since we do not need to use this fact.

Define the binomial coefficient

$$\binom{Y}{i} = \frac{Y(Y-1)\cdots(Y-i+1)}{i!} \in \mathbb{Q}[Y]$$

for $i \geq 0$, and $\binom{Y}{i} = 0$ for $i < 0$. For integers $-p < v_{(i)} < p$ form the n-tuple, $\vec{v} = (v_{(n-1)}, \dots, v_{(0)})$. Define $\rho_{\vec{v}} = \prod_{i=1}^{n} \binom{X_i}{v_{(n-i)}} \in K_n$. Thus $\rho_{\vec{v}} = 0$, if there is an $0 \leq i < n$ with $v_{(i)} < 0$. Define the partial order $\preceq$ on n-tuples: Given $\vec{v}$, $\vec{w}$,

$$\vec{v} \preceq \vec{w} \iff v_{(i)} \leq w_{(i)} \text{ for all } 0 \leq i < n.$$

Thus $\rho_{\vec{v}} \neq 0$ if and only if $\vec{0} \preceq \vec{v}$. Now restrict to vectors $(a_{(n-1)}, \dots, a_{(0)})$ of the base-p coefficients of integers $0 \leq a < p^n$, and identify each $a = \sum_{i=1}^{n} a_{(n-i)} p^{n-i}$ where $0 \leq a_{(s)} < p$ with its corresponding vector. (It is convenient to index the base-p digits as $a_{(n-i)}$, where increasing values of i correspond to decreasing powers of p.) Define

$$\rho_a = \prod_{i=1}^{n} \binom{X_i}{a_{(n-i)}} \in K_n.$$

Furthermore, define

$$\mathfrak{b}(a) := -v_n(\rho_a) = -\sum_{i=1}^{n} a_{(n-i)} p^{n-i} b_i.$$

Because the b_i are relatively prime to p, $\{-\mathfrak{b}(a) : 0 \leq a < p^n\}$ is a complete set of residues modulo p^n. As a result, $\{\rho_a : 0 \leq a < p^n\}$ is a K_0-basis for K_n. Since $-\mathfrak{b}$ maps the residues modulo p^n onto the residues modulo p^n, it has an inverse $\mathfrak{a}$: For each $t \in \mathbb{Z}$, we define $\mathfrak{a}(t)$ to be the unique integer satisfying

$$0 \leq \mathfrak{a}(t) < p^n, \qquad t = -\mathfrak{b}(\mathfrak{a}(t)) + p^n f_t \text{ for some } f_t \in \mathbb{Z}.$$

Note that $\mathfrak{a}(0) = 0$. Using this notation, we normalize our K_0-basis for K_n as follows.

Definition 2.5. Let $\lambda_t = \pi_0^{f_t} \rho_{\mathfrak{a}(t)}$, where π_0 is a fixed prime element in K_0. Thus $v_n(\lambda_t) = t$ for all t, $\lambda_{t+p^n} = \pi_0 \lambda_t$, and $\{\lambda_t : 0 \leq t < p^n\}$ is an $\mathfrak{O}_0$-basis for $\mathfrak{O}_n$.

We need to discuss Galois action. Choice 2.3 means that $v_j((\sigma_i - 1)X_j) = b_i - b_j$ for $1 \leq i \leq j \leq n$. Recall that $b_i - b_j \equiv 0 \bmod p$ [Ser79, IV§2]. Since K_j/K_{j-1} is ramified, there are elements $\mu_{i,j} \in K_{j-1}$ and $\epsilon_{i,j} \in K_j$ such that

$$(\sigma_i - 1)X_j = \mu_{i,j} + \epsilon_{i,j} \tag{5}$$

with $v_j(\mu_{i,j}) = b_i - b_j < v_j(\epsilon_{i,j})$. We consider $\mu_{i,j}$ to be the *main term*, with $\epsilon_{i,j}$ the *error term*. Observe that $v_j([(\sigma_i - 1) - \mu_{i,j}(\sigma_j - 1)]X_j) > v_j((\sigma_i - 1)X_j)$. We would like this observation to be a statement about an element $\mu_{i,j}(\sigma_j - 1) \in K_0[G]$ that approximates the effect of $(\sigma_i - 1)$. So observe that if $p^j \mid v_j(\mu_{i,j}) = b_i - b_j$, then we may choose $\mu_{i,j} \in K_0$. The condition $p^j \mid b_i - b_j$ for all $1 \leq i \leq j \leq n$ is equivalent to

Assumption 2.6. There is one residue class modulo p^n, represented by $b \in \mathbb{Z}$ with $0 \leq b < p^n$, such that $b_i \equiv b \bmod p^n$ for $1 \leq i \leq n$.

Under this assumption $\mathfrak{b}(a) \equiv ab \bmod p^n$. Furthermore, $\mathfrak{a}(t) \equiv -b^{-1}t \bmod p^n$. Restated in terms of upper ramification numbers, Assumption 2.6 becomes $u_{i+1} \equiv u_i \bmod p^{n-i}$ for $1 \leq i < n$. Since $u_1 = b_1 \in \mathbb{Z}$, this implies the conclusion of the Theorem of Hasse-Arf, namely that the upper ramification numbers are integers. But Assumption 2.6 is stronger than the conclusion of Hasse-Arf, since it implies that the upper ramification numbers are integers congruent modulo p.

Define *truncated exponentiation* by

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

where $\mathbb{Z}_{(p)}$ is the integers localized at p. Motivated by [Eld09], we define:

Definition 2.7. Let $\Psi_i = \Theta_i - 1$ where $\Theta_n = \sigma_n$, and for $1 \leq i \leq n-1$,

$$\Theta_i = \sigma_i \Theta_n^{[-\mu_{i,n}]} \Theta_{n-1}^{[-\mu_{i,n-1}]} \cdots \Theta_{i+1}^{[-\mu_{i,i+1}]}.$$

Remark 2.8. If K_0 has characteristic p and K_n/K_0 is elementary abelian, it was observed in [Eld09] that the elements in Definition 2.7 solve the matrix equation:

$$\begin{pmatrix} \mu_{1,1} & \mu_{1,2} & \cdots & \mu_{1,n} \\ 0 & \mu_{2,2} & \cdots & \mu_{2,n} \\ & & \ddots & \\ 0 & \cdots & 0 & \mu_{n,n} \end{pmatrix} \cdot \begin{pmatrix} \Theta_1 \\ \Theta_2 \\ \vdots \\ \Theta_n \end{pmatrix} = \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_n \end{pmatrix}$$

where the usual vector space operations of addition and scalar multiplication have been replaced by multiplication and scalar truncated exponentiation, respectively. Note $\alpha^p = 0$ for all α in the augmentation ideal $(\sigma - 1 : \sigma \in G) \subset K_0[G]$. So, since $\Theta_j - 1 \in (\sigma - 1 : \sigma \in G)$ satisfies $(\Theta_j - 1)^p = 0$, we find $\Theta_j^{[-\mu_{i,j}]} \cdot \Theta_j^{[\mu_{i,j}]} = 1$. A cautionary remark is important here: Since scalar truncated exponentiation does not distribute (it is easy to check for $p = 2$ that the units $(\Theta_i\Theta_j)^{[\mu]}$ and $\Theta_i^{[\mu]}\Theta_j^{[\mu]}$ are not equal), applying the inverse matrix $(\mu_{i,j})^{-1}$ to both sides of this equation does not preserve equality.

The following assumption will enable us to ignore the error terms in (5).

Assumption 2.9. Given an integer $\mathfrak{c} \geq 1$, assume that for $1 \leq i \leq j \leq n$,

$$v_n(\epsilon_{i,j}) - v_n(\mu_{i,j}) \geq (p-1) \sum_{k=1}^{i-1} p^{n-k-1} b_k + (p^{n-i} - p^{n-j}) b_i + \mathfrak{c},$$

which because of (4), is equivalent to $v_n(\epsilon_{i,j}) - v_n(\mu_{i,j}) \geq p^{n-1}u_i - p^{n-j}b_i + \mathfrak{c}$.

We state the main result of this paper.

Theorem 2.10. *Given a totally ramified Galois p-extension K_n/K_0 with ramification multiset $\{b_i : 1 \leq i \leq n\}$ satisfying Assumption 2.2 and 2.6. Thus there is one congruence class modulo p^n, represented by $0 \leq b < p^n$, that contains all the ramification numbers. Given an integer $\mathfrak{c} \geq 1$, assume that it is possible to make Choices 2.1 and 2.3 so that Assumption 2.9 holds. Then a $K_0[G]$-scaffold on K_n, as defined in* [BCE, Definition 2.3], *exists with precision $\mathfrak{c}$ and shift parameters $b_1, \ldots, b_n$. Namely, there are:*

(i) *$\lambda_t \in K_n$ defined in Definition 2.5 satisfying $v_n(\lambda_i) = i$ and $\lambda_{i+p^n} = \pi_0\lambda_i$ for some fixed prime element $\pi_0 \in K_0$.*

(ii) $\Psi_i \in K_0[G]$ *defined in Definition 2.7, satisfying* $\Psi_i 1 = 0$, *such that for all* $1 \le i \le n$ *and* $j \in \mathbb{Z}$, *modulo* $\lambda_{j+p^{n-i}b_i}\mathfrak{P}_n^{\mathfrak{c}}$,

$$\Psi_i \lambda_j \equiv \begin{cases} \lambda_{j+p^{n-i}b_i} & \text{if } \mathfrak{a}(j)_{(n-i)} \ge 1, \\ 0 & \text{if } \mathfrak{a}(j)_{(n-i)} = 0, \end{cases}$$

where $\mathfrak{a}$ *is the function defined on the integers by* $\mathfrak{a}(j) \equiv -jb^{-1} \bmod p^n$ *and* $0 \le \mathfrak{a}(j) < p^n$, *and* $\mathfrak{a}(j)_{(n-i)}$ *is the coefficient of* p^{n-i} *in the base* p *expansion of* $\mathfrak{a}(j)$.

Before we prove this theorem, some discussion of the elements $\Psi_j \in K_0[G]$ is warranted. Suppose $\psi_j \in K_0[G]$ satisfies $\mathrm{Tr}_{n,j}\psi_j = (\sigma_j - 1)\mathrm{Tr}_{n,j}$ where $\mathrm{Tr}_{n,j} = \sum_{\sigma \in H_j} \sigma$ is the element of $K[G]$ that gives the trace from K_n to K_j. In this case, we will say that ψ_j is a *lift* of $(\sigma_j - 1)$. Thus Ψ_j can be considered to be one among many lifts of $(\sigma_j - 1)$. Now observe that $v_j((\sigma_j - 1)\alpha) - v_j(\alpha) = b_j$ for $\alpha \in K_j$ with $p \nmid v_j(\alpha)$ and thus $v_n((\sigma_j - 1)\alpha) - v_n(\alpha) = p^{n-j}b_j$. The following result states that $p^{n-j}b_j$ is a natural upper bound on $v_n(\psi_j\alpha) - v_n(\alpha)$ for a lift ψ_j of $(\sigma_j - 1)$. From this perspective, Theorem 2.10 states that the lifts Ψ_j, provided by Definition 2.7, are special in that they achieve a natural upper bound.

Proposition 2.11. *Let* K_n/K_0 *be a totally ramified Galois* p*-extension satisfying Assumptions 2.2 and 2.6. Let* $1 \le j \le n$ *and let* ψ_j *be any element of* $K_0[G]$ *such that* $\mathrm{Tr}_{n,j}\psi_j = (\sigma_j - 1)\mathrm{Tr}_{n,j}$. *If* $\rho \in K_n$ *with* $v_n(\rho) \equiv b_n \bmod p^{n-j}$ *but* $v_n(\rho) \not\equiv b_n(1 - p^{n-j}) \bmod p^{n-j+1}$ *(which is equivalent to* $p \nmid v_j(\mathrm{Tr}_{n,j}\rho)$*), then*

$$v_n(\psi_j\rho) \le v_n(\rho) + p^{n-j}b_j.$$

Proof. The case $j = n$ is trivial since we necessarily have $\psi_n = \sigma_n - 1$. Fix $j < n$ and consider the different $\mathfrak{D}_{K_n/K_j}$ of the extension K_n/K_j. Hilbert's formula for the exponent of the different [Ser79, IV§1 Proposition 4] gives $\mathfrak{D}_{K_n/K_j} = \mathfrak{P}_n^m$ where $m = (b_{j+1} + 1)(p^{n-j} - 1) + \sum_{i=j+1}^{n-1}(b_{i+1} - b_i)(p^{n-i} - 1)$. For any $r \in \mathbb{Z}$, we have $\mathrm{Tr}_{n,j}(\mathfrak{P}_n^r) = \mathfrak{P}_j^{s_r}$ where $s_r = \lfloor (m + r)/p^{n-j} \rfloor$ and $\lfloor x \rfloor$ denotes the greatest integer $\le x$. Since $p^{i+1} \mid (b_{i+1} - b_i)$ by Assumption 2.6, it follows that

$$s_r = (b_{j+1} + 1) + \sum_{i=j+1}^{n-1} (b_{i+1} - b_i)p^{j-i} + \left\lfloor \frac{-1 - b_n + r}{p^{n-j}} \right\rfloor.$$

In particular, if $r = b_n + kp^{n-j}$ for some $k \in \mathbb{Z}$, we find that $s_{r+1} > s_r$ and $s_r \equiv b_{j+1} + k \bmod p$. Let $\rho \in K_n$ with $v_n(\rho) = r$. We may write an arbitrary element $\alpha \in \mathfrak{P}_n^r$ as $\alpha = x\rho + \nu$ with $x \in \mathfrak{O}_j$ and $\nu \in \mathfrak{P}_n^{r+1}$. Since $s_{r+1} > s_r$, it follows that $v_j(\mathrm{Tr}_{n,j}\rho) = s_r$, and hence that $v_j((\sigma_j - 1)\mathrm{Tr}_{n.j}\rho) = s_r + b_j$ provided that $k \not\equiv -b_{j+1} \bmod p$. Recalling Assumption 2.2, we have therefore shown that if $v_n(\rho) = r \equiv b_n \bmod p^{n-j}$ but $r \not\equiv b_n(1 - p^{n-j}) \bmod p^{n-j+1}$ then $v_n((\sigma_j - 1)\mathrm{Tr}_{n,j}\rho) = s_r + b_j$.

Now, with ρ as above, suppose that ψ_j is any element of $K_0[G]$ with $v_n(\psi_j\rho) > r' := r + p^{n-j}b_j$. Since $r' \equiv b_n \bmod p^{n-j}$, we have $s_{r'+1} > s_{r'} = s_r + b_j$, so that $v_j(\mathrm{Tr}_{n,j}\psi_j\rho) > s_r + b_j = v_n((\sigma_j - 1)\mathrm{Tr}_{n,j}\rho)$. Hence $\mathrm{Tr}_{n,j}\psi_j \ne (\sigma_j - 1)\mathrm{Tr}_{n,j}$. □

We conclude this section by recording a technical question.

Question 2.12. A bijection exists between the one-units of $\mathfrak{O}_j$ and the choices possible in Choice 2.3. Namely, given X_j satisfying Choice 2.3 and any $u_j \in 1 + \mathfrak{P}_j$, then u_jX_j will also satisfy Choice 2.3. So how does one optimize the choice of X_j in Choice 2.3 to maximize the precision $\mathfrak{c}$ available in Assumption 2.9?

We do not address this question here. Neither was it addressed in [Eld09, BE13]. Thus far, in all these cases, naive choices were made that turned out to be good enough for a determination of Galois module structure. There has been no need.

2.1. **Proof of Theorem 2.10.** We are interested in analyzing the expression $\Psi_i\lambda_j$ for $1 \le i \le n$ and $j \in \mathbb{Z}$, where λ_j is as in Definition 2.5 and Ψ_i is as in Definition 2.7. So observe that $\Psi_i\lambda_j = \pi_0^{f_j} \cdot \Psi_i\rho_{\mathfrak{a}(j)}$ where

$$\Psi_i\rho_{\mathfrak{a}(j)} = \Psi_i\binom{X_n}{a_{(0)}}\binom{X_{n-1}}{a_{(1)}}\cdots\binom{X_1}{a_{(n-1)}},$$

for $\mathfrak{a}(j) = a = \sum_{i=1}^n a_{(n-i)}p^{n-i}$ with $0 \le a_{(n-i)} < p$. Our analysis is technical. To motivate it, we begin by considering the special case treated in [Eld09] where $\epsilon_{i,j} = 0$ for all $1 \le i, j \le n$. This gives us the opportunity to more fully justify [Eld09, (4)]. Observe that Theorem 2.10 with $\mathfrak{c} = \infty$ follows from Proposition 2.13 setting $\kappa_i = 0$.

Proposition 2.13. *Suppose that Assumptions 2.2 and 2.6 hold, and that $\epsilon_{i,j} = 0$ for all $1 \le i, j \le n$ so that Assumption 2.9 holds vacuously. Then for all $0 \le a_{(i)} < p$ and $\kappa_i \in K_0$,*

$$\Psi_j\prod_{i=1}^n\binom{X_i+\kappa_i}{a_{(n-i)}} = \binom{X_j+\kappa_j}{a_{(n-j)}-1}\prod_{i\ne j}\binom{X_i+\kappa_i}{a_{(n-i)}}$$

Proof. Note that Θ_j fixes X_i for $i < j$. So it is sufficient to prove by inducting down from $j = n$ to $j = 1$ that $\Psi_j\prod_{i=j}^n\binom{X_i+\kappa_i}{a_{(n-i)}} = \binom{X_j+\kappa_j}{a_{(n-j)}-1}\prod_{i=j+1}^n\binom{X_i+\kappa_i}{a_{(n-i)}}$. Recall $\Theta_n = \sigma_n$. Pascal's Identity states that $\binom{X_n+\kappa_n}{a_{(0)}-1} + \binom{X_n+\kappa_n}{a_{(0)}} = \binom{X_n+\kappa_n+1}{a_{(0)}}$. Thus $\Psi_n\binom{X_n+\kappa_n}{a_{(0)}} = \binom{X_n+\kappa_n}{a_{(0)}-1}$ for $1 \le a_{(0)} < p$. Recall $\Theta_{n-1} = \sigma_{n-1}\Theta_n^{[-\mu_{n-1,n}]}$. Observe that

$$\begin{aligned}\Theta_n^{[-\mu_{n-1,n}]}&\binom{X_n+\kappa_n}{a_{(0)}}\binom{X_{n-1}+\kappa_{n-1}}{a_{(1)}}\\ &=\sum_{s=0}^{p-1}\binom{-\mu_{n-1,n}}{s}\Psi_n^s\binom{X_n+\kappa_n}{a_{(0)}}\binom{X_{n-1}+\kappa_{n-1}}{a_{(1)}}\\ &=\sum_{s=0}^{a_{(0)}}\binom{-\mu_{n-1,n}}{s}\binom{X_n+\kappa_n}{a_{(0)}-s}\binom{X_{n-1}+\kappa_{n-1}}{a_{(1)}}\\ &=\binom{X_n+\kappa_n-\mu_{n-1,n}}{a_{(0)}}\binom{X_{n-1}+\kappa_{n-1}}{a_{(1)}}\end{aligned}$$

where the last equality is a consequence of Vandermonde's Convolution identity, $\sum_{i=0}^m\binom{a}{i}\binom{b}{m-i} = \binom{a+b}{m}$. Thus because $\sigma_{n-1}X_n = X_n + \mu_{n-1,n}$ we have

$$\sigma_{n-1}\Theta_n^{[-\mu_{n-1,n}]}\binom{X_n+\kappa_n}{a_{(0)}}\binom{X_{n-1}+\kappa_{n-1}}{a_{(1)}} = \binom{X_n+\kappa_n}{a_{(0)}}\binom{X_{n-1}+\kappa_{n-1}+1}{a_{(1)}}.$$

So $\Psi_{n-1}\binom{X_n+\kappa_n}{a_{(0)}}\binom{X_{n-1}+\kappa_{n-1}}{a_{(1)}} = \binom{X_n+\kappa_n}{a_{(0)}}\binom{X_{n-1}+\kappa_{n-1}}{a_{(1)}-1}$, based upon Pascal's Identity. Note the role of Pascal's Identity and Vandermonde's Convolution Identity. These two identities will be used repeatedly and without mention in the induction step.

Assume that the proposition holds for all j such that $k < j \leq n$. Thus for each j with $k < j \leq n$,

$$\Theta_j^{[-\mu_{k,j}]} \prod_{i=1}^{n} \binom{X_i+\kappa_i}{a_{(n-i)}} = \sum_{s=0}^{p-1} \binom{-\mu_{k,j}}{s} \Psi_j^s \prod_{i=1}^{n} \binom{X_i+\kappa_i}{a_{(n-i)}} \tag{6}$$

$$= \sum_{s=0}^{a_{(n-j)}} \binom{-\mu_{k,j}}{s} \binom{X_j+\kappa_j}{a_{(n-j)}-s} \prod_{i\neq j} \binom{X_i+\kappa_i}{a_{(n-i)}} = \binom{X_j+\kappa_j-\mu_{k,j}}{a_{(n-j)}} \prod_{i\neq j} \binom{X_i+\kappa_i}{a_{(n-i)}}.$$

Since $\kappa_j' = \kappa_j - \mu_{k,j}$ is just another element of K_0, we find, by applying (6) repeatedly that

$$\prod_{s=k+1}^{n} \Theta_s^{[-\mu_{k,s}]} \cdot \prod_{i=1}^{n} \binom{X_i+\kappa_i}{a_{(n-i)}} = \prod_{i=k+1}^{n} \binom{X_i+\kappa_i-\mu_{k,i}}{a_{(n-i)}} \cdot \prod_{i=1}^{k} \binom{X_i+\kappa_i}{a_{(n-i)}}.$$

Thus $\Theta_k \prod_{i=1}^n \binom{X_i+\kappa_i}{a_{(n-i)}} = \prod_{i=k+1}^n \binom{X_i+\kappa_i}{a_{(n-i)}} \cdot \binom{X_k+\kappa_k+1}{a_{(n-k)}} \cdot \prod_{i=1}^{k-1} \binom{X_i+\kappa_i}{a_{(n-i)}}$, which means that for $0 \leq a_{(n-k)} < p$, $\Psi_k \prod_{i=1}^n \binom{X_i+\kappa_i}{a_{(n-i)}} = \binom{X_k+\kappa_k}{a_{(n-k)}-1} \prod_{i\neq k} \binom{X_i+\kappa_i}{a_{(n-i)}}$. □

2.1.1. *Preliminary results for Theorem 2.10.* For $1 \leq r \leq s \leq n$, set

$$M_r^s = \prod_{i=r}^{s-1} \mu_{i,i+1},$$

and define an ideal I_r of $\mathfrak{O}_n$ by its generators:

$$I_r = \Big(M_r^s \cdot \epsilon_{s,t} \cdot X_t^{-1} : r \leq s \leq t \leq n\Big).$$

Lemma 2.14.

$$I_r = \sum_{i=r}^{n} \epsilon_{r,i} X_i^{-1} \mathfrak{O}_n + \sum_{s=0}^{n-r-1} \mu_{r,n-s} I_{n-s}.$$

Proof. We can partition the generators of I_r into those with $r = s$ and those with $r < s$. When $r = s$ we have $M_r^s = 1$. When $r < s$ we have $M_r^s = \mu_{r,r+1} M_{r+1}^s$. As a result,

$$I_r = \sum_{i=r}^{n} \epsilon_{r,i} X_i^{-1} \mathfrak{O}_n + \mu_{r,r+1} I_{r+1}.$$

Given $i-1 \geq r$ we have $b_{i-1} \geq b_r$ and thus $v_n(\mu_{r,i}) \geq v_n(\mu_{r,i-1}\mu_{i-1,i})$. This means that $\mu_{r,i} \cdot M_i^s \epsilon_{s,t} X_t^{-1} \mathfrak{O}_n \subseteq \mu_{r,i-1} \cdot M_{i-1}^s \epsilon_{s,t} X_t^{-1} \mathfrak{O}_n$, and so $\mu_{r,i} I_i \subseteq \mu_{r,i-1} I_{i-1}$. As a result, for $1 \leq r \leq n$, we have $\mu_{r,n} I_n \subseteq \mu_{r,n-1} I_{n-1} \subseteq \cdots \subseteq \mu_{r,r+1} I_{r+1}$, and thus

$$\sum_{s=0}^{n-r-1} \mu_{r,n-s} I_{n-s} = \mu_{r,r+1} I_{r+1}.$$

□

Lemma 2.15. $I_r \subseteq X_r^{-1} \mathfrak{P}_n^{\mathfrak{c}}$ *if and only if for all* $1 \leq r \leq s \leq t \leq n$,

$$v_n(\epsilon_{s,t}) - v_n(\mu_{s,t}) \geq (p-1) \sum_{i=r}^{s-1} p^{n-i-1} b_i + (p^{n-s} - p^{n-t}) b_s + \mathfrak{c}.$$

Proof. Observe that $v_n(M_r^s\epsilon_{s,t}X_t^{-1}) \geq v_n(X_r^{-1}\pi_n^{\mathfrak{c}})$ is equivalent to $\sum_{i=r}^{s-1} p^{n-i-1}(b_i - b_{i+1}) + v_n(\epsilon_{s,t}) + p^{n-t}b_t \geq p^{n-r}b_r + \mathfrak{c}$, and that this is equivalent to $v_n(\epsilon_{s,t}) - v_n(\mu_{s,t}) \geq p^{n-r}b_r - p^{n-t}b_t - \sum_{i=r}^{s-1} p^{n-i-1}(b_i - b_{i+1}) - p^{n-t}(b_s - b_t) + \mathfrak{c} = (p-1)\sum_{i=r}^{s-1} p^{n-i-1}b_i + (p^{n-s} - p^{n-t})b_s + \mathfrak{c}$. $\square$

Corollary 2.16. *Assumption 2.9 holds with precision* $\mathfrak{c}$ *if and only if* $I_r \subseteq X_r^{-1}\mathfrak{P}_n^{\mathfrak{c}}$ *for all* $1 \leq r \leq n$.

2.1.2. *Main result for Theorem 2.10.* Since Θ_j fixes X_i for $i < j$, Theorem 2.10 follows from Corollary 2.16 and Proposition 2.17 below by specializing to the case $\kappa_i = 0$.

Proposition 2.17. *Suppose that Assumptions 2.2 and 2.6 hold, and that Assumption 2.9 holds with precision* $\mathfrak{c} \geq 1$. *Then for all* $0 \leq a_{(i)} < p$ *and any* $\kappa_i \in K_0$ *with* $v_i(X_i) < v_i(\kappa_i)$,

$$\Psi_j \prod_{i=j}^{n} \binom{X_i + \kappa_i}{a_{(n-i)}} \equiv \binom{X_j + \kappa_j}{a_{(n-j)} - 1} \cdot \prod_{i=j+1}^{n} \binom{X_i + \kappa_i}{a_{(n-i)}} \bmod \prod_{i=j}^{n} \binom{X_i}{a_{(n-i)}} \cdot I_j.$$

Proof. We induct down from $j = n$ to $j = 1$. Note $\Theta_n = \sigma_n$, and observe that

$$\sigma_n \binom{X_n + \kappa_n}{a_{(0)}} = \binom{X_n + \kappa_n + 1 + \epsilon_{n,n}}{a_{(0)}} \equiv \binom{X_n + \kappa_n + 1}{a_{(0)}} \bmod \epsilon_{n,n}X_n^{-1}\binom{X_n}{a_{(0)}}.$$

Using Pascal's Identity and the definition of I_n, this means

$$(\sigma_n - 1)\binom{X_n + \kappa_n}{a_{(0)}} \equiv \binom{X_n + \kappa_n}{a_{(0)} - 1} \bmod \binom{X_n}{a_{(0)}} \cdot I_n.$$

We have proven the case $j = n$.

Assume that Proposition 2.17 holds for all j with $k < j \leq n$. We aim to prove that it continues to hold for $j = k$. Since

$$\left\{ \prod_{i=j}^{n} \binom{X_j + \kappa_i}{a_{(n-i)}} : 0 \leq a_{(n-i)} < p \right\}$$

is a basis for K_n over K_{j-1}, we can express any element of K_n in terms of this basis. Our assumption that Proposition 2.17 holds for $k < j \leq n$, together with Corollary 2.16, means that $v_n((\Theta_j - 1)\alpha) \geq v_n(\alpha) + p^{n-j}b_j$ for all $\alpha \in K_n$. As a result, we see that for $1 \leq s \leq p-1$,

$$v_n\left(\binom{-\mu_{k,j}}{s}(\Theta_j - 1)^{s-1} I_j \prod_{i=j}^{n}\binom{X_i + \kappa_i}{a_{(n-i)}}\right) \geq$$
$$sp^{n-j}(b_k - b_j) + (s-1)p^{n-j}b_j + v_n(I_j) + v_n\left(\prod_{i=j}^{n}\binom{X_i + \kappa_i}{a_{(n-i)}}\right).$$

Note the right-hand side is minimized by $s = 1$. As a result, using Proposition 2.17 for each $k < j$, we have

$$\Theta_j^{[-\mu_{k,j}]} \prod_{i=j}^{n} \binom{X_i + \kappa_i}{a_{(n-i)}} = \sum_{s=0}^{p-1} \binom{-\mu_{k,j}}{s} \Psi_j^s \prod_{i=j}^{n} \binom{X_i + \kappa_i}{a_{(n-i)}}$$

$$\equiv \prod_{i=j+1}^{n} \binom{X_i + \kappa_i}{a_{(n-i)}} \sum_{s=0}^{a_{(n-j)}} \binom{-\mu_{k,j}}{s} \binom{X_j + \kappa_j}{a_{(n-j)} - s} \bmod \binom{-\mu_{k,j}}{1} I_j \prod_{i=j}^{n} \binom{X_i}{a_{(n-i)}}.$$

Vandermonde's Convolution Identity yields, modulo $\mu_{k,j} I_j \prod_{i=j}^{n} \binom{X_i}{a_{(n-i)}}$,

$$\Theta_j^{[-\mu_{k,j}]} \prod_{i=j}^{n} \binom{X_i + \kappa_i}{a_{(n-i)}} \equiv \prod_{i=j+1}^{n} \binom{X_i + \kappa_i}{a_{(n-i)}} \cdot \binom{X_j + \kappa_j - \mu_{k,j}}{a_{(n-j)}},$$

which holds for all $k < j \leq n$. Since Θ_j fixes X_i for $i < j$, this means that

$$\Theta_j^{[-\mu_{k,j}]} \prod_{i=k}^{n} \binom{X_i + \kappa_i}{a_{(n-i)}} \equiv \prod_{i=j+1}^{n} \binom{X_i + \kappa_i}{a_{(n-i)}} \cdot \binom{X_j + \kappa_j - \mu_{k,j}}{a_{(n-j)} - i} \cdot \prod_{i=k}^{j-1} \binom{X_i + \kappa_i}{a_{(n-i)}} \bmod \mu_{k,j} I_j \prod_{i=k}^{n} \binom{X_i}{a_{(n-i)}}. \tag{7}$$

Note that, in general, we may consider $\kappa_i' = \kappa_i - \mu_{k,i}$ to be another κ_i. As a result, by repeated use of (7), once for each value of j in $k < j \leq n$, we find that

$$\prod_{j=k+1}^{n} \Theta_j^{[-\mu_{k,j}]} \cdot \prod_{i=k}^{n} \binom{X_i + \kappa_i}{a_{(n-i)}} \equiv \prod_{j=k+1}^{n} \binom{X_j + \kappa_j - \mu_{k,j}}{a_{(n-j)}} \cdot \binom{X_k + \kappa_k}{a_{(n-k)}} \bmod \left(\sum_{j=k+1}^{n} \mu_{k,j} I_j \right) \prod_{i=k}^{n} \binom{X_i}{a_{(n-i)}}$$

Notice that the order in which we apply these $\Theta_j^{[-\mu_{k,j}]}$ does not matter. See Remark 2.18. In any case, if we keep the ordering used in Definition 2.7, we find

$$\Theta_k \prod_{i=k}^{n} \binom{X_i + \kappa_i}{a_{(n-i)}} \equiv \prod_{j=k+1}^{n} \binom{X_j + \kappa_j + \epsilon_{k,j}}{a_{(n-j)}} \cdot \binom{X_k + \kappa_k + 1 + \epsilon_{k,k}}{a_{(n-k)}} \bmod \left(\sum_{j=k+1}^{n} \mu_{k,j} I_j \right) \prod_{i=k}^{n} \binom{X_i}{a_{(n-i)}},$$

$$\equiv \prod_{j=k+1}^{n} \binom{X_j + \kappa_j}{a_{(n-j)}} \cdot \binom{X_k + \kappa_k + 1}{a_{(n-k)}} \bmod \left(\sum_{j=k}^{n} \epsilon_{k,j} X_j^{-1} \mathfrak{O}_n + \sum_{j=k+1}^{n} \mu_{k,j} I_j \right) \prod_{i=k}^{n} \binom{X_i}{a_{(n-i)}}.$$

Using $\Psi_k = \Theta_k - 1$, Lemma 2.14 and Pascal's Identity, the result holds for $j = k$. $\square$

Remark 2.18. The proof of Proposition 2.17 does not depend upon the ordering of the factors in Θ_j. Since the Galois group may be nonabelian, this is noteworthy.

3. Elementary abelian p-extensions with Galois scaffold

In this section, we determine conditions that are sufficient for a totally ramified, elementary abelian extension L/K of degree p^n to satisfy Theorem 2.10 and thus have a $K[G]$-scaffold on L. The main result of this section, Theorem 3.5, extends, from characteristic p to characteristic 0, the main result of [Eld09].

3.1. **Cyclic extensions of degree p in characteristic 0.**

Theorem 3.1. *Let K be a characteristic 0 local field with perfect residue field of characteristic p, and let L/K be a totally ramified cyclic extension of degree p. Let the ramification number u for L/K be relatively prime to p. (Recall the discussion preceding Assumption 2.2.) Then the hypotheses of Theorem 2.10 hold and there is a Galois scaffold with precision $\mathfrak{c} = pv_K(p) - (p-1)u \geq 1$.*

Proof. Since there is only one break in the ramification filtration, the lower and upper ramification numbers are the same $b = u$. Since $\gcd(p, u) = 1$, $L = K(x)$ for some x with $-pv_K(p)/(p-1) < v_L(x) = -u < 0$ satisfying an Artin-Schreier equation $\wp(x) := x^p - x \in K$ with $(\sigma - 1)x - 1 = \delta \in \mathfrak{P}_L$ [FV02, III §2.5 Prop]. Expand $\wp(\sigma x) = \wp(x)$ to find that $\sum_{k=1}^{p-1}\binom{p}{k}x^k(1+\delta)^{p-k} \equiv \delta \bmod \delta\mathfrak{P}_L$. Since $v_L(x) = -u < 0$, this means that $v_L((\sigma-1)x-1) = v_L(\delta) = v_L(px^{p-1}) = pv_K(p) - (p-1)u$. In the notation of §2, we have $K_1 = L$, $K_0 = K$, $X_1 = x$ and $\sigma_1 = \sigma$ where $(\sigma_1 - 1)X_1 = \mu_{1,1} + \epsilon_{1,1}$ with $\mu_{1,1} = 1$ and $\epsilon_{1,1} = \delta$. The extension satisfies Assumptions 2.2, 2.6 and 2.9 with precision $\mathfrak{c} = v_L(\delta)$. □

3.2. **Elementary abelian p-extensions.**

Since the description of the extensions requires a few paragraphs to develop, we introduce the extensions and state the main theorem first. We leave the proofs till §3.3 and §3.4.

Let K be a complete local field whose residue field is perfect of characteristic $p > 0$. Let L/K be a totally ramified, elementary abelian extension of degree p^n, $n > 1$. Again we change notation so that $L/K = K_n/K_0$. Fix a composition series $\{H_i\}$ that refines the ramification filtration of the elementary abelian group $G = \mathrm{Gal}(K_n/K_0) \cong C_p^n$. Thus $\{H_i\}$ yields elements $\sigma_i \in G$, lower ramification numbers b_i, and upper ramification numbers u_i via (4), as in §2. Restrict these upper ramification numbers as follows.

Assumption 3.2. $p \nmid u_1$ and $u_i \equiv u_1 \bmod p^{n-1}$ for all $1 \leq i \leq n$.

Our extension now satisfies Assumptions 2.2 and 2.6 from §2, and restrictions are imposed on the Artin-Schreier generators of the extension: Let $K_{(i)}$ be the subfield that is fixed by $\langle \sigma_j : j \neq i\rangle$. Then because u_i is the ramification number for $K_{(i)}/K_0$ and $p \nmid u_i$, we have $K_{(i)} = K_0(x_i)$ where x_i satisfies an Artin-Schreier equation $\wp(x_i) = x_i^p - x_i = \alpha_i \in K_0$, with $v_{(i)}(x_i) = -u_i$ and $v_{(i)}((\sigma_i - 1)x_i - 1) > 0$ [FV02, III §2.5 Prop]. Following the proof of Theorem 3.1,

$$v_{(i)}((\sigma_i - 1)x_i - 1) = pv_0(p) - (p-1)u_i. \tag{8}$$

Let $\beta = \alpha_1$. So $v_0(\beta) = -u_1 = -b_1$. Since $v_0(\alpha_i) = -u_i \equiv -u_j = v_0(\alpha_j) \bmod p^{n-1}$ for all i, j, there are $\omega_i \in K_0$ with $\omega_1 = 1$ and $v_0(\omega_n) \leq v_0(\omega_{n-1}) \leq \cdots \leq$

$v_0(\omega_1) = 0$, such that $\omega_i^{p^{n-1}}\beta \equiv \alpha_i \bmod \alpha_i\mathfrak{P}_0$ for $2 \le i \le n$. (Here we have used the fact that the residue field of K_0 is perfect.) Thus

$$\wp(x_i) = \omega_i^{p^{n-1}}\beta + \epsilon_i \tag{9}$$

for some "error terms" $\epsilon_i \in K_0$ with $\epsilon_1 = 0$ and $v_0(\epsilon_i) > -u_i$. Note that whenever $v_0(\omega_i) = v_0(\omega_{i+1}) = \cdots = v_0(\omega_j)$ with $i < j$, $K_0(x_i, \dots, x_j)/K_0$ has only one ramification number $u_i = u_j$. As a result, the projections of $\omega_j, \dots, \omega_i$ into $\omega_i\mathfrak{O}_0/\omega_i\mathfrak{P}_0$ must be linearly independent over $\mathbb{F}_p$, the finite field with p elements. Conversely, given any β, ω_i, ϵ_i as above, and x_i satisfying (9), $K_n = K_0(x_1, x_2, \dots, x_n)$ will be a totally ramified elementary abelian extension of degree p^n with upper ramification numbers $\{u_j : 1 \le j \le n\}$ satisfying Assumption 3.2.

We now need to subject our extension K_n/K_0 to two further restrictions: First, we ask that the error terms be negligible. Second, we ask that the absolute ramification be relatively large. To make this precise, we need further notation: Let $m_i = v_0(\omega_{i-1}) - v_0(\omega_i) \ge 0$ for $i \ge 2$. So $v_0(\omega_i) = -\sum_{k=2}^{i} m_k$. Note $u_i = b_1 + p^{n-1}\sum_{k=2}^{i} m_k$ and $b_i = b_1 + p^n \sum_{k=2}^{i} p^{k-2}m_k$. Set $C_0 = 0$, and for $1 \le i \le n$, define

$$C_i = u_i - b_i/p^i.$$

Check that $C_i = u_{i+1} - b_{i+1}/p^i$ for $0 \le i \le n-1$. Since $C_i = u_{i+1} - b_{i+1}/p^i < u_{i+1} - b_{i+1}/p^{i+1} = C_{i+1}$, the sequence $\{C_i : 0 \le i \le n\}$ is increasing. The two further restrictions are:

Assumption 3.3. $v_0(\epsilon_i) > -u_i + C_{n-1}$.

Assumption 3.4. $v_0(p) \ge C_n + \mathfrak{c}/p^n$ with $\mathfrak{c} \ge 1$.

These assumptions enable us to prove:

Theorem 3.5. *Let K_0 be a complete local field whose residue field is perfect of characteristic $p > 0$. Let K_n/K_0 be a totally ramified, elementary abelian extension of degree p^n, $n > 1$ that satisfies Assumptions 3.2, 3.3, 3.4 with $\mathfrak{c} \ge 1$, and has ramification multiset $\{b_1, b_2, \dots, b_n\}$. Then the hypotheses of Theorem 2.10 hold and we have a scaffold for the $K_0[G]$-action on K_n/K_0 of precision $\mathfrak{c}$, with shift parameters $b_1, b_2, \dots, b_n$.*

To prove this theorem we must, in the notation of §2, choose elements $X_j \in K_j$ with $v_j(X_j) = -b_j$, as required for Choice 2.3 so that the difference $v_j(\epsilon_{i,j}) - v_j(\mu_{i,j})$, where $(\sigma_i - 1)X_j = \mu_{i,j} + \epsilon_{i,j}$ as in (5), satisfies Assumption 2.9 with precision $\mathfrak{c} \ge 1$. We define the X_j in §3.3. Interestingly, if we assume $v_j(X_j) = -b_j$, the proof that Assumption 2.9 is satisfied with precision $\mathfrak{c} \ge 1$ is relatively easy. It appears in §3.3, as Lemma 3.8. The proof that $v_j(X_j) = -b_j$ is much more involved and appears afterwards, in §3.4.

Remark 3.6. In characteristic p, Assumption 3.4 is vacuous, which is why it did not appear in [Eld09]. Otherwise, everything in §3.2 is consistent with [Eld09]. Indeed, Assumption 3.3 is, after small changes in notation, exactly [Eld09, (5)].

3.3. **Candidate for Choice 2.3.** Let $\Omega_{1,j} = \omega_j$, $X_{1,j} = x_j$. For $2 \le i \le j \le n$, recursively define

$$\Omega_{i,j} = \wp(\Omega_{i-1,j})/\wp(\Omega_{i-1,i}) \in K_0; \text{ in particular, } \Omega_{j,j} = 1 \text{ for all } j; \tag{10}$$

$$X_{i,j} = X_{i-1,j} - \Omega_{i-1,j}^{p^{n-i}} X_{i-1,i-1} \in K_{i-1}(x_j) \subseteq K_j; \tag{11}$$

The following result proves that the $\Omega_{i,j}$, and thus the $X_{i,j}$, are well-defined.

Lemma 3.7. *For $2 \le i \le n$ we have $\wp(\Omega_{i-1,i}) \ne 0$. Furthermore, for $1 \le i \le j \le n$*

$$v_0(\Omega_{i,j}) = -p^{i-1} \sum_{k=i+1}^{j} m_k = p^{i-n}(u_i - u_j).$$

Proof. To obtain the first assertion, we show that for $1 \le i \le n$ we have $v_0(\Omega_{i,n}) \le v_0(\Omega_{i,n-1}) \le \cdots \le v_0(\Omega_{i,i}) = 0$, and that if $v_0(\Omega_{i,j}) = 0$ for some $j > i$, then the projections $\overline{\Omega}_{i,j}, \dots, \overline{\Omega}_{i,i}$ of $\Omega_{i,j}, \dots, \Omega_{i,i}$ in $\mathfrak{O}_n/\mathfrak{P}_n$ are linearly independent over $\mathbb{F}_p$. These assertions hold for $i = 1$ since $\Omega_{1,j} = \omega_j$ with $\omega_1 = 1$. Assume inductively that they hold for $i = k-1 \ge 1$. Since $\Omega_{k-1,k-1} = 1$, either $v_0(\Omega_{k-1,k}) < 0$, or $v_0(\Omega_{k-1,k}) = 0$ with $\overline{\Omega}_{k-1,k} \notin \mathbb{F}_p$. In either case, $\wp(\Omega_{k-1,k}) \ne 0$, and indeed $v_0(\wp(\Omega_{j,k})) = pv_0(\Omega_{j,k})$ for all $j < k$. Furthermore, if $v_0(\Omega_{k-1,j}) = 0$ with $j > k-1$ then $v_0(\wp(\Omega_{k-1,j})) = \cdots = v_0(\wp(\Omega_{k-1,k})) = 0$. Also, $\wp(\overline{\Omega}_{k-1,j}), \dots, \wp(\overline{\Omega}_{k-1,k})$ are linearly independent over $\mathbb{F}_p$ because $\overline{\Omega}_{k-1,j}, \dots, \overline{\Omega}_{k-1,k-1} = 1$ are linearly independent and $\wp$ is $\mathbb{F}_p$-linear with kernel $\mathbb{F}_p$. It then follows from (10) that our assertions hold for $i = k$. This completes the proof that $\wp(\Omega_{i-1,i}) \ne 0$ for $2 \le i \le n$. The formula for $v_0(\Omega_{i,j})$ is then easily verified by induction, using (10), the definition of the m_k, and the fact that $v_0(\wp(\Omega_{j,k})) = pv_0(\Omega_{j,k})$ if $j < k$. $\square$

Using (11) repeatedly, we find that $X_{j,j} = X_{1,j} - \sum_{s=1}^{j-1} \Omega_{s,j}^{p^{n-s-1}} X_{s,s}$, or $x_j = X_{1,j} = X_{j,j} + \sum_{s=1}^{j-1} \Omega_{s,j}^{p^{n-s-1}} X_{s,s}$. In other words, we have the matrix equation $(X_{1,1}, X_{2,2}, \dots, X_{n,n}) \cdot (\mathbf{\Omega}) = (x_1, x_2, \dots, x_n)$ with

$$(\mathbf{\Omega}) = \begin{pmatrix} 1 & \Omega_{1,2}^{p^{n-2}} & \Omega_{1,3}^{p^{n-2}} & \cdots & \Omega_{1,n}^{p^{n-2}} \\ 0 & 1 & \Omega_{2,3}^{p^{n-3}} & \cdots & \Omega_{2,n}^{p^{n-3}} \\ & & \ddots & & \\ 0 & 0 & \cdots & 1 & \Omega_{n-1,n}^{p^0} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}. \tag{12}$$

Clearly, $K_i = K_0(x_1, \dots, x_i) = K_0(X_{1,1}, \dots, X_{i,i})$. In the next section we will prove that $v_j(X_{j,j}) = -b_j$ for $1 \le j \le n$, so that $X_j = X_{j,j}$ provide candidates for Choice 2.3. But first we derive an important consequence.

Lemma 3.8. *If $v_j(X_{j,j}) = -b_j$ for $1 \le j \le n$, then we may use $X_j = X_{j,j}$ for Choice 2.3. If we do so, then Assumption 3.4 ensures that Assumption 2.9 holds with precision $\mathfrak{c} \ge 1$.*

Proof. Using (12) we find $((\sigma_i - 1)X_{j,j})_{1 \le i,j \le n} = ((\sigma_i - 1)x_j)_{1 \le i,j \le n}(\mathbf{\Omega})^{-1}$. Recall that $(\sigma_i - 1)X_{j,j} = 0 = (\sigma_i - 1)x_j$ for $i > j$. Express the upper triangular matrix $(\mathbf{\Omega})^{-1} = (\alpha_{i,j})$ for some $\alpha_{i,j} \in K_0$. So then for $i \le j$, $(\sigma_i - 1)X_{j,j} = \alpha_{i,j}(\sigma_i - 1)x_i$ where $(\sigma_i - 1)x_i \in K_{(i)}$ is a 1-unit. Recall from (8) that $v_{(i)}((\sigma_i - 1)x_i - 1) = pv_0(p) - (p-1)u_i$. Note that $\alpha_{i,i} = 1$.

Since $v_j(X_{j,j}) = -b_j$, $v_j((\sigma_i - 1)X_{j,j}) = b_i - b_j$. Since $(\sigma_i - 1)x_i$ is a unit, $v_0(\alpha_{i,j}) = (b_i - b_j)/p^j$. Let $\mu_{i,j} = \alpha_{i,j}$ in (5). Then $\epsilon_{i,j} = \mu_{i,j}((\sigma_i - 1)x_i - 1)$ and $v_j(\epsilon_{i,j}) = v_j(\mu_{i,j}) + p^{j-1}(pv_0(p) - (p-1)u_i)$, which is equivalent to $v_n(\epsilon_{i,j}) - v_n(\mu_{i,j}) = p^n v_0(p) - (p-1)p^{n-1}u_i$.

Recall that Assumption 2.9 with precision $\mathfrak{c} \ge 1$, is equivalent to $v_n(\epsilon_{i,j}) - v_n(\mu_{i,j}) \ge p^{n-1}u_i - p^{n-j}b_i + \mathfrak{c}$. So Assumption 2.9 follows from $p^n v_0(p) - (p -$

$1)p^{n-1}u_i \geq p^{n-1}u_i - p^{n-j}b_i + \mathfrak{c}$, or $v_0(p) \geq u_i - b_i/p^{-j} + \mathfrak{c}/p^n$ for all $1 \leq i \leq j \leq n$. Since $C_i = u_i - b_i/p^{-i} \geq u_i - b_i/p^{-j}$ and $\{C_i\}$ is an increasing sequence, this means that Assumption 2.9 with precision $\mathfrak{c} \geq 1$ follows from Assumption 3.4. $\square$

3.4. **Candidate has correct valuation.** First we define some auxiliary elements. Let $B_1 = \beta$ and $E_{1,j} = \epsilon_j$, and for $2 \leq i \leq j \leq n$ define

$$B_i = \wp(X_{i,i}); \tag{13}$$

$$E_{i,j} = \wp(X_{i,j}) - \Omega_{i,j}^{p^{n-i}} B_i. \tag{14}$$

$$M_{i-1,j} = X_{i,j}^p - X_{i-1,j}^p + \Omega_{i-1,j}^{p^{n-i+1}} X_{i-1,i-1}^p \in K_{i-1}(x_j), \tag{15}$$

$$L_{i-1,j} = \wp\left(\Omega_{i-1,i}^{p^{n-i}}\right)\Omega_{i,j}^{p^{n-i}} - \wp\left(\Omega_{i-1,j}^{p^{n-i}}\right) \in K_0. \tag{16}$$

Observe that (9) together with (14) can be restated as $\wp(X_{i,j}) = \Omega_{i,j}^{p^{n-i}} B_i + E_{i,j}$ for $1 \leq i \leq j \leq n$. Using (11), (14) and (15), we calculate

$$\begin{aligned}\wp(X_{i,j}) = X_{i,j}^p - X_{i,j} &= \left(M_{i-1,j} + X_{i-1,j}^p - \Omega_{i-1,j}^{p^{n-i+1}} X_{i-1,i-1}^p\right) - X_{i,j}\\ &= M_{i-1,j} + \wp(X_{i-1,j}) - \Omega_{i-1,j}^{p^{n-i+1}} X_{i-1,i-1}^p + \Omega_{i-1,j}^{p^{n-i}} X_{i-1,i-1}\\ &= M_{i-1,j} + \left(\Omega_{i-1,j}^{p^{n-i+1}} B_{i-1} + E_{i-1,j}\right) - \Omega_{i-1,j}^{p^{n-i+1}} (B_{i-1} + X_{i-1,i-1}) + \Omega_{i-1,j}^{p^{n-i}} X_{i-1,i-1}\\ &= E_{i-1,j} + M_{i-1,j} - \wp(\Omega_{i-1,j}^{p^{n-i}}) X_{i-1,i-1}.\end{aligned} \tag{17}$$

Using (17) with $j = i$, (13) becomes

$$B_i = E_{i-1,i} + M_{i-1,i} - \wp\left(\Omega_{i-1,i}^{p^{n-i}}\right) X_{i-1,i-1}. \tag{18}$$

Use (17) to replace $\wp(X_{i,j})$ in (14), and then use (18) to replace B_i. The result is

$$E_{i,j} = E_{i-1,j} + M_{i-1,j} - \Omega_{i,j}^{p^{n-i}}(E_{i-1,i} + M_{i-1,i}) + L_{i-1,j} X_{i-1,i-1} \tag{19}$$

We now define $\Omega_k^{\pi(i,j)} \in K_0$ for integers $1 \leq i \leq j \leq k \leq n$. Let $(\mathbf{\Omega}^p)$ be the matrix formed by replacing each coefficient in $(\mathbf{\Omega})$ with its pth power. The $\Omega_k^{\pi(i,j)} \in K_0$ generalize the coefficients that appear in the inverse of $(\mathbf{\Omega}^p)$. Given integers $i \leq j$, let $\pi(i,j) = \{(a_1, a_2, \dots, a_t) : i = a_1 < a_2 < \cdots < a_t \leq j\}$ denote the set of increasing integer sequences that begin at i and end at or before j. Given $k \geq j$, associate to each sequence $(a_1, a_2, \dots, a_t) \in \pi(i,j)$ the product $(-1)^t \Omega_{a_1,a_2}^{p^{n-a_1}} \Omega_{a_2,a_3}^{p^{n-a_2}} \Omega_{a_3,a_4}^{p^{n-a_3}} \cdots \Omega_{a_t,k}^{p^{n-a_t}}$. Let

$$\Omega_k^{\pi(i,j)} = \sum_{(a_1,\dots,a_t)\in\pi(i,j)} (-1)^t \Omega_{a_1,a_2}^{p^{n-a_1}} \Omega_{a_2,a_3}^{p^{n-a_2}} \Omega_{a_3,a_4}^{p^{n-a_3}} \cdots \Omega_{a_t,k}^{p^{n-a_1}}.$$

In particular,

$$\Omega_j^{\pi(i,i)} = -\Omega_{i,j}^{p^{n-i}}. \tag{20}$$

Observe that for $i < j < k$,

$$\Omega_k^{\pi(i,j)} = \Omega_j^{\pi(i,j-1)} \Omega_k^{\pi(j,j)} + \Omega_k^{\pi(i,j-1)}. \tag{21}$$

Furthermore, for $i < j$,

$$\Omega_j^{\pi(i,j-1)} = -\left(\Omega_{i,i+1}^{p^{n-i}} \Omega_j^{\pi(i+1,j-1)} + \cdots + \Omega_{i,j-1}^{p^{n-i}} \Omega_j^{\pi(j-1,j-1)} + \Omega_{i,j}^{p^{n-i}}\right),$$

which can be seen as the dot product of the ith row of $(\mathbf{\Omega}^p)$ and the jth column of

$$(\mathbf{\Omega}^p)^{-1} = \begin{pmatrix} 1 & \Omega_2^{\pi(1,1)} & \Omega_3^{\pi(1,2)} & \cdots & \Omega_n^{\pi(1,n-1)} \\ 0 & 1 & \Omega_3^{\pi(2,2)} & \cdots & \Omega_n^{\pi(2,n-1)} \\ & & \ddots & & \\ 0 & 0 & \cdots & 1 & \Omega_n^{\pi(n-1,n-1)} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Now check, using Lemma 3.7, that for $(a_1, \ldots, a_t) \in \pi(i,j)$

$$v_0\left((-1)^t \Omega_{a_1,a_2}^{p^{n-a_1}} \Omega_{a_2,a_3}^{p^{n-a_2}} \Omega_{a_3,a_4}^{p^{n-a_3}} \cdots \Omega_{a_t,k}^{p^{n-a_t}}\right) = -p^{n-1} \sum_{s=i+1}^{k} m_s.$$

Thus

$$v_0\left(\Omega_k^{\pi(i,j)}\right) \geq -p^{n-1} \sum_{s=i+1}^{k} m_s = u_i - u_k = v_0\left(\Omega_{i,k}^{p^{n-i}}\right). \tag{22}$$

Lemma 3.9. *$E_{i,j} = E_{1,j} + \sum_{s=2}^{i} \Omega_j^{\pi(s,i)} E_{1,s} + \sum_{r=1}^{i-1}\left(M_{r,j} + \sum_{s=r+1}^{i} \Omega_j^{\pi(s,i)} M_{r,s}\right)$ $+ \sum_{r=1}^{i-1}\left(L_{r,j} + \sum_{s=r+2}^{i} \Omega_j^{\pi(s,i)} L_{r,s}\right) X_{r,r}$ for $1 \leq i < j \leq n$.*

Proof. This is clear for $i = 1$. For $i = 2$ the statement follows directly from (19) and (20). Assume that the Lemma holds for $(i,j) = (i_0 - 1, j), (i_0 - 1, i_0)$. Using (20), we can write (19) as $E_{i_0,j} = E_{i_0-1,j} + \Omega_j^{\pi(i_0,i_0)} E_{i_0-1,i_0} + L_{i_0-1,j} X_{i_0-1,i_0-1} + M_{i_0-1,j} + \Omega_j^{\pi(i_0,i_0)} M_{i_0-1,i_0}$. Using induction, replace $E_{i_0-1,j}$ and E_{i_0-1,i_0}. Then (19) becomes

$$\begin{aligned} E_{i_0,j} = E_{1,j} &+ \sum_{s=2}^{i_0-1} \Omega_j^{\pi(s,i_0-1)} E_{1,s} + \Omega_j^{\pi(i_0,i_0)}\left(E_{1,i_0} + \sum_{s=2}^{i_0-1} \Omega_{i_0}^{\pi(s,i_0-1)} E_{1,s}\right) \\ &+ M_{i_0-1,j} + \sum_{r=1}^{i_0-2}\left(M_{r,j} + \sum_{s=r+1}^{i_0-1} \Omega_j^{\pi(s,i_0-1)} M_{r,s}\right) \\ &+ \Omega_j^{\pi(i_0,i_0)} M_{i_0-1,i_0} + \Omega_j^{\pi(i_0,i_0)} \sum_{r=1}^{i_0-2}\left(M_{r,i_0} + \sum_{s=r+1}^{i_0-1} \Omega_{i_0}^{\pi(s,i_0-1)} M_{r,s}\right) \\ &+ L_{i_0-1,j} X_{i_0-1,i_0-1} + \sum_{r=1}^{i_0-2}\left(L_{r,j} + \sum_{s=r+2}^{i_0-1} \Omega_j^{\pi(s,i_0-1)} L_{r,s}\right) X_{r,r} \\ &+ \Omega_j^{\pi(i_0,i_0)} \sum_{r=1}^{i_0-2}\left(L_{r,i_0} + \sum_{s=r+2}^{i_0-1} \Omega_{i_0}^{\pi(s,i_0-1)} L_{r,s}\right) X_{r,r}. \end{aligned}$$

As a result,

$$E_{i_0,j} = E_{1,j} + \Omega_j^{\pi(i_0,i_0)} E_{1,i_0} + \sum_{s=2}^{i_0-1} \left(\Omega_j^{\pi(s,i_0-1)} + \Omega_j^{\pi(i_0,i_0)} \Omega_{i_0}^{\pi(s,i_0-1)}\right) E_{1,s} + \sum_{r=1}^{i_0-1} M_{r,j}$$
$$+ \Omega_j^{\pi(i_0,i_0)} \sum_{r=1}^{i_0-1} M_{r,i_0} + \sum_{r=1}^{i_0-2} \sum_{s=r+1}^{i_0-1} \left(\Omega_j^{\pi(s,i_0-1)} + \Omega_j^{\pi(i_0,i_0)} \Omega_{i_0}^{\pi(s,i_0-1)}\right) M_{r,s} + \sum_{r=1}^{i_0-1} L_{r,j} X_{r,r}$$
$$+ \Omega_j^{\pi(i_0,i_0)} \sum_{r=1}^{i_0-2} L_{r,i_0} X_{r,r} + \sum_{r=1}^{i_0-2} \sum_{s=r+2}^{i_0-1} \left(\Omega_j^{\pi(s,i_0-1)} + \Omega_j^{\pi(i_0,i_0)} \Omega_{i_0}^{\pi(s,i_0-1)}\right) L_{r,s} X_{r,r}.$$

Using (21) , we find that

$$\begin{aligned} E_{i_0,j} = E_{1,j} &+ \Omega_j^{\pi(i_0,i_0)} E_{1,i_0} + \sum_{s=2}^{i_0-1} \Omega_j^{\pi(s,i_0)} E_{1,s} \\ &+ \sum_{r=1}^{i_0-1} M_{r,j} + \sum_{r=1}^{i_0-1} \Omega_j^{\pi(i_0,i_0)} M_{r,i_0} + \sum_{r=1}^{i_0-2} \sum_{s=r+1}^{i_0-1} \Omega_j^{\pi(s,i_0)} M_{r,s} \\ &+ \sum_{r=1}^{i_0-1} L_{r,j} X_{r,r} + \sum_{r=1}^{i_0-2} \Omega_j^{\pi(i_0,i_0)} L_{r,i_0} X_{r,r} + \sum_{r=1}^{i_0-2} \sum_{s=r+2}^{i_0-1} \Omega_j^{\pi(s,i_0)} L_{r,s} X_{r,r}, \end{aligned}$$

from which the result for $i = i_0$ follows. □

Lemma 3.10. *If $v_0(p) \geq C_n$ then $v_0(L_{r,s}) \geq v_0(p) + u_r - u_s$ for $1 \leq r < s \leq n$.*

Proof. The formula for $L_{r,s}$, namely (16), compared with (10) leads to an interest in $\wp(\Omega_{r,s})^{p^t} - \wp(\Omega_{r,s}^{p^t})$ or $\Omega_{r,s}^{p^{t+1}} \left((1-y)^{p^t} - 1 + y^{p^t}\right)$ where $t = n - r - 1$ and $y = \Omega_{r,s}^{1-p} \in \mathfrak{O}_0$. Note that from Lemma 3.7 we have $v_0(y) = p^{r-1}(p-1) \sum_{v=r+1}^{s} m_v \geq 0$. So we begin by proving the following:

Given any prime p, integer $t \geq 1$ and indeterminate y, the polynomial $(1-y)^{p^t} - 1 + y^{p^t}$ is contained in the ideal of the polynomial ring $\mathbb{Z}[y]$:

$$(p^i y^{p^{t-i}} : 1 \leq i \leq t). \tag{23}$$

Although this can be proven by induction, we prefer an alternate proof using the Binomial Theorem: $(1-y)^{p^t} - 1 + y^{p^t} = \sum_{a=1}^{p^t-1} \binom{p^t}{a} (-y)^a + (-y)^{p^t} + y^{p^t}$. It is a result of Kummer that the exact power of p dividing $\binom{a+b}{a}$ is equal to the number of "carries" when performing the addition of a and b, written in base p [Rib89, pg 24]. Given i, we are interested in identifying the smallest integer exponent a such that a plus $p^t - a$ involves exactly i "carries". This occurs at $a = p^{t-i}$. Note that p^{t-i} plus $p^t - p^{t-i} = (p-1)p^{t-1} + (p-1)p^{t-2} + \cdots + (p-1)p^{t-i}$ is p^t.

Return to the situation where $y = \Omega_{r,s}^{1-p} \in \mathfrak{O}_0$ and (23) is an ideal of $\mathfrak{O}_0$. We now prove that under $v_0(p) \geq C_n$, this ideal is generated by $py^{p^{t-1}}$. In other words, we prove that $v_0(p^i y^{p^{t-i}}) = iv_0(p) + p^{t-i} v_0(y) \geq v_0(py^{p^{t-1}})$ for $1 \leq i \leq t$. Observe that because $b_1 > 0$ and $m_k \geq 0$ we have $b_1 + p^{n-2} \sum_{k=2}^{n} m_k \geq b_1/p^n + \sum_{k=2}^{n} p^{k-2} m_k$, which is equivalent to $b_1 + u_n/p \geq b_1/p + b_n/p^n$ and thus to $u_n - b_n/p^n \geq (p-1)(u_n - b_1)/p$. As a consequence, $u_n - b_n/p^n \geq (p-1)(u_n - b_1)/p \geq (p-1)(u_n - b_1)/p^2$. Our assumption, $v_0(p) \geq C_n$, therefore means that $v_0(p) \geq (p-1)(u_n - b_1)/p^2$. In other words, $v_0(p) \geq p^{n-3}(p-1) \sum_{k=2}^{n} m_k$. Thus $v_0(p) \geq p^{n-3}(p-1) \sum_{v=r+1}^{s} m_v$

for all $1 \le r < s \le n$, and thus $v_0(p) \ge p^{n-r-2}v_0(y)$. We have shown that $v_0(p) \ge p^{t-1}v_0(y)$. As a result, for $2 \le i$, $(i-1)v_0(p) \ge v_0(p) \ge p^{t-1}v_0(y) \ge (1/p - 1/p^i)p^t v_0(y)$ from which $v_0(p^i y^{p^{t-i}}) \ge v_0(py^{p^{t-1}})$ follows.

This implies

$$\wp(\Omega_{r,s})^{p^t} - \wp\left(\Omega_{r,s}^{p^t}\right) \in p\Omega_{r,s}^{p^{t-1}(p^2-p+1)}\mathfrak{O}_0. \tag{24}$$

In particular, by setting $s = r+1$, we see that (24) implies

$$\frac{\wp(\Omega_{r,r+1}^{p^t})}{\wp(\Omega_{r,r+1})^{p^t}} \in 1 + p\Omega_{r,r+1}^{-p^{t-1}(p-1)}\mathfrak{O}_0. \tag{25}$$

Replace $\Omega_{r+1,s}$ in the expression for $L_{r,s}$ using (10). Thus, using (25) and (10), we see that $L_{r,s} \in \wp(\Omega_{r,s})^{p^t}(1 + p\Omega_{r,r+1}^{-p^{t-1}(p-1)}\mathfrak{O}_0) - \wp(\Omega_{r,s}^{p^t})$. Using (24),

$$L_{r,s} \in p\Omega_{r,s}^{p^{t-1}(p^2-p+1)}\mathfrak{O}_0 + p\wp(\Omega_{r,s})^{p^t}\Omega_{r,r+1}^{-p^{t-1}(p-1)}\mathfrak{O}_0.$$

Since $v_0(\wp(\Omega_{r,s})) = v_0(\Omega_{r,s}^p)$ and $v_0(\Omega_{r,s}) \le v_0(\Omega_{r,r+1})$, $v_0(\wp(\Omega_{r,s})^{p^t}\Omega_{r,r+1}^{-p^{t-1}(p-1)}) \le v_0(\Omega_{r,s}^{p^{t-1}(p^2-p+1)})$. Therefore $v_0(L_{r,s}) \ge v_0(p\wp(\Omega_{r,s})^{p^t}\Omega_{r,r+1}^{-p^{t-1}(p-1)})$, which implies $v_0(L_{r,s}) \ge v_0(p) - p^{n-1}\sum_{k=r+2}^{s} m_k - p^{n-3}(p^2-p+1)m_{r+1} \ge v_0(p) + u_r - u_s$. $\square$

Proposition 3.11. *Under Assumption 3.3, if $v_0(p) > C_n$ then $v_j(X_{j,j}) = -b_j$ for $1 \le j \le n$.*

Proof. We point out to the reader that we do not use Assumption 3.3 until the last third of the proof where we verify (31) for $E_{1,s}$.

Define $v_i^*(x) = p^{i-n}v_n(x)$ for $x \in K_n$, so that for $x \in K_i$ we have $v_i^*(x) = v_i(x)$. For $1 \le i \le j \le n$, define

$$\mathfrak{c}_{i,j} = -b_i - p^{n+i-2}\sum_{k=i+1}^{j} m_k = p^{i-1}(u_i - u_j) - b_i = v_{i-1}(\Omega_{i,j}^{p^{n-i}}) - b_i. \tag{26}$$

Our goal is to prove, by induction on i, that for $1 \le i \le j \le n$, we have

$$v_{i-1}^*(B_i) = \mathfrak{c}_{i,i} = -b_i \tag{27}$$

$$v_{i-1}^*(E_{i,j}) > v_i^*(X_{i,j}) = \mathfrak{c}_{i,j}. \tag{28}$$

The case $i = 1$ is immediate from $B_1 = \beta$, $X_{1,j} = x_j$ and $E_{1,j} = \epsilon_j$ since $v_0(B_1) = v_0(\beta) = -b_1$, $v_1^*(X_{1,j}) = v_{(1)}(x_j) = -u_j = -b_1 - p^{n-1}\sum_{k=2}^{j} m_k = \mathfrak{c}_{1,j}$, and $v_0(\epsilon_j) > -u_j$.

Given $2 \le i_0 \le n$, assume that (27) and (28) hold for all $i = i_0 - 1 \le j \le n$. We need to prove that (27) and (28) hold for $i = i_0$. Observe that once we have proven $v_{i_0-1}^*(B_{i_0}) = \mathfrak{c}_{i_0,i_0}$ and for $i_0 \le j \le n$ that $v_{i_0-1}^*(E_{i_0,j}) > \mathfrak{c}_{i_0,j}$, then it is immediate from (14) and Lemma 3.7 that $v_{i_0}^*(X_{i_0,j}) = \mathfrak{c}_{i_0,j}$. Thus we focus on proving that $v_{i_0-1}^*(B_{i_0}) = \mathfrak{c}_{i_0,i_0}$ and for $i_0 \le j \le n$ that $v_{i_0-1}^*(E_{i_0,j}) > \mathfrak{c}_{i_0,j}$.

Consider the expression for B_{i_0} in (18). By induction, $v_{i_0-1}(X_{i_0-1,i_0-1}) = -b_{i_0-1}$. Thus, using Lemma 3.7, we have $v_{i_0-1}(\wp(\Omega_{i_0-1,i_0}^{p^{n-i_0}})X_{i_0-1,i_0-1}) = \mathfrak{c}_{i_0,i_0} =$

$-b_{i_0}$. Use Lemma 3.9 to expand E_{i_0-1,i_0} so that the other terms in B_{i_0} are

$$(29)\quad E_{i_0-1,i_0}+M_{i_0-1,i_0}=E_{1,i_0}+\sum_{s=2}^{i_0-1}\Omega_{i_0}^{\pi(s,i_0-1)}E_{1,s}+M_{i_0-1,i_0}$$
$$+\sum_{r=1}^{i_0-2}\left(M_{r,i_0}+\sum_{s=r+1}^{i_0-1}\Omega_{i_0}^{\pi(s,i_0-1)}M_{r,s}\right)+\sum_{r=1}^{i_0-2}\left(L_{r,i_0}+\sum_{s=r+2}^{i_0-1}\Omega_{i_0}^{\pi(s,i_0-1)}L_{r,s}\right)X_{r,r}.$$

We will have proven $v_{i_0-1}^*(B_{i_0})=\mathfrak{c}_{i_0,i_0}$ as soon as we prove that the valuation in $v_{i_0-1}^*$ of each term in the right-hand-side of (29) exceeds $-b_{i_0}=\mathfrak{c}_{i_0,i_0}$. Similarly, $v_{i_0-1}^*(E_{i_0,j})>\mathfrak{c}_{i_0,j}$ will follow if each term in the right-hand-side of

$$(30)\quad E_{i_0,j}=E_{1,j}+\sum_{s=2}^{i_0}\Omega_j^{\pi(s,i_0)}E_{1,s}+\sum_{r=1}^{i_0-1}\left(M_{r,j}+\sum_{s=r+1}^{i_0}\Omega_j^{\pi(s,i_0)}M_{r,s}\right)$$
$$+\sum_{r=1}^{i_0-1}\left(L_{r,j}+\sum_{s=r+2}^{i_0}\Omega_j^{\pi(s,i_0)}L_{r,s}\right)X_{r,r}$$

has valuation in $v_{i_0-1}^*$ that exceeds $\mathfrak{c}_{i_0,j}$. We claim that both of these statements follow if, for $1\le r<i_0, s\le n$, we prove that

$$(31)\quad v_{i_0-1}^*(E_{1,s}),v_{i_0-1}^*(M_{r,s}),v_{i_0-1}^*(L_{r,s}X_{r,r})>$$
$$p^{i_0-1}(u_{i_0}-u_s)-b_{i_0}=-b_{i_0}+p^{n+i_0-2}\begin{cases}\sum_{k=s+1}^{i_0}m_k & \text{if } s\le i_0,\\ -\sum_{k=i_0+1}^{s}m_k & \text{if } i_0<s.\end{cases}$$

To prove this claim we begin by noticing that the terms $E_{1,s}$, $M_{r,s}$, $L_{r,s}X_{r,r}$ with $s=j$ and $1\le r<i_0<j\le n$ only appear in (30). The fact that the valuation in $v_{i_0-1}^*$ of these terms exceeds $\mathfrak{c}_{i_0,j}=\mathfrak{c}_{i_0,s}=-b_{i_0}-p^{n+i_0-2}\sum_{k=i_0+1}^{s}m_k$ is equivalent to (31) for $i_0<s$. The other terms, $E_{1,s}$ with $1<s\le i_0$, $M_{r,s}$ with $1\le r<s\le i_0$, $L_{r,s}X_{r,r}$ with $1\le r<r+2\le s\le i_0$, appear in both (29) and (30). So that we can treat these terms uniformly, let T_s with $s\le i_0$ denote one such term (either $E_{1,s}$, $M_{r,s}$ or $L_{r,s}X_{r,r}$), and notice that (31) concerning $v_{i_0-1}^*(T_s)$ can be rewritten using Lemma 3.7 as

$$(32)\qquad v_{i_0-1}^*(\Omega_{s,j}^{p^{n-s}}T_s)>\mathfrak{c}_{i_0,j},$$

where j is any integer $i_0\le j\le n$. Let T_s be a term in (29). We treat the two cases, $s=i_0$ and $s<i_0$, separately. If $s=i_0$, we need $v_{i_0-1}^*(T_s)>\mathfrak{c}_{i_0,i_0}$, which since $\Omega_{i_0,i_0}^{p^{n-i_0}}=1$ is equivalent to (32) with $j=i_0$. If $s<i_0$, we need $v_{i_0-1}^*(\Omega_{i_0}^{\pi(s,i_0-1)}T_s)>\mathfrak{c}_{i_0,i_0}$. This follows from (32) with $j=i_0$, using (22), namely $v_{i_0-1}^*(\Omega_{i_0}^{\pi(s,i_0-1)}T_s)\ge v_{i_0-1}^*(\Omega_{s,i_0}^{p^{n-s}}T_s)$. Now let T_s be a term in (30), with $s\le i_0$. We need $v_{i_0-1}^*(\Omega_j^{\pi(s,i_0)}T_s)>\mathfrak{c}_{i_0,j}$. This follows from (32), again using (22), $v_{i_0-1}^*(\Omega_j^{\pi(s,i_0)}T_s)\ge v_{i_0-1}^*(\Omega_{s,j}^{p^{n-s}}T_s)$.

Now we prove, for each of $E_{1,s}$, $M_{r,s}$ and $L_{r,s}X_{r,r}$, that the inequalities in (31) hold. Consider (31) for $E_{1,s}$. Since $\{C_i\}$ is an increasing sequence, $C_{i_0-1}\le C_{n-1}$. So, using Assumption 3.3, we have $v_0(E_{1,s})>C_{n-1}-u_s\ge C_{i_0-1}-u_s=u_{i_0}-b_{i_0}/p^{i_0-1}-u_s$, which is equivalent to (31).

Consider (31) for $M_{r,s}$, namely $v_0^*(M_{r,s})>(u_{i_0}-u_s)-b_{i_0}/p^{i_0-1}$. Since $v_0(p)>C_{n-1}$ and $\{C_i\}$ is an increasing sequence, $v_0(p)>C_{i_0-1}-C_{r-1}$. This means that

$v_0(p) + (u_r - u_s) - b_r/p^{r-1} > (u_{i_0} - u_s) - b_{i_0}/p^{i_0-1}$. Therefore, it is sufficient to prove $v_0^*(M_{r,s}) \geq v_0(p) + (u_r - u_s) - b_r/p^{r-1}$, or equivalently $v_r^*(M_{r,s}) \geq v_r(p) + p^r(u_r - u_s) - pb_r = v_r(p) + p\mathfrak{c}_{r,s}$. By induction $v_r^*(X_{r,s}) = \mathfrak{c}_{r,s}$ for $1 \leq r < i_0$ and all $r \leq s \leq n$. Thus it is sufficient to prove $v_r^*(M_{r,s}) \geq v_r^*(pX_{r,s}^p) = v_r^*(p\Omega_{r,s}^{p^{n-r}} X_{r,r}^p)$. Recall using (15) that $M_{r,s} = X_{r+1,s}^p - X_{r,s}^p + \Omega_{r,s}^{p^{n-r}} X_{r,r}^p$. Use (11) to replace $X_{r+1,s}$. As a result,

$$M_{r,s} = \sum_{i=1}^{p-1} \binom{p}{i} X_{r,s}^i \left(-\Omega_{r,s}^{p^{n-r-1}} X_{r,r}\right)^{p-i} + \left(\left(-\Omega_{r,s}^{p^{n-r-1}}\right)^p + \Omega_{r,s}^{p^{n-r}}\right) X_{r,r}^p.$$

It is sufficient to prove that each nonzero term in this sum has valuation $v_r^*(pX_{r,s}^p)$. So note

$$((-\Omega_{r,s}^{p^{n-r-1}})^p + \Omega_{r,s}^{p^{n-r}})X_{r,r}^p = \begin{cases} p\Omega_{r,s}^{p^{n-r}} X_{r,r}^p & \text{for } p = 2, \\ 0 & \text{for } p > 2. \end{cases}$$

Furthermore, $v_r^*(\binom{p}{i} X_{r,s}^i (-\Omega_{r,s}^{p^{n-r-1}} X_{r,r})^{p-i}) = v_r^*(pX_{r,s}^p)$ for $1 \leq i \leq p$, since we have $v_r^*(X_{r,s}) = v_r^*(\Omega_{r,s}^{p^{n-r-1}} X_{r,r})$.

Consider (31) for $L_{r,s}X_{r,r}$, namely $v_0^*(L_{r,s}X_{r,r}) > (u_{i_0} - u_s) - b_{i_0}/p^{i_0-1}$. From Lemma 3.10, assuming $v_0(p) > C_n$, we have $v_0(L_{r,s}) \geq v_0(p) + u_r - u_s$. Since $v_0(p) > C_{i_0-1} - C_r$, this means that $v_0(L_{r,s}) > C_{i_0-1} - C_r + u_r - u_s = (u_{i_0} - u_s) - b_{i_0}/p^{i_0-1} + b_r/p^r$. Since $r < i_0$, $v_r^*(X_{r,r}) = -b_r$, and so $v_0^*(L_{r,s}X_{r,r}) > (u_{i_0} - u_s) - b_{i_0}/p^{i_0-1}$. □

Proposition 3.11 completes the proof of Theorem 3.5.

4. Elementary abelian examples and explicit Galois module structure

In this section, we illustrate the explicit nature of what is possible when one combines the results of this paper with those of [BCE]. We choose to do so in the context of two classes of totally ramified extensions, biquadratic and weakly ramified, that have a long history and for which explicit results already exist. Furthermore, since it can be done quickly, we also apply our results to V. Abrashkin's "elementary extensions" [Abr87]. All these results are in characteristic 0. For analogous results in characteristic p, see [BCE, §4].

4.1. **Biquadratic extensions.** Let K_0 be a local field of characteristic 0 with perfect residue field of characteristic 2, and let K_2 be a totally ramified Galois extension of K_0 with $G = \mathrm{Gal}(K_2/K_0) \cong C_2 \times C_2$. The structure of $\mathfrak{O}_2$ over its associated order $\mathfrak{A}_{K_2/K_0}$ in $K_0[G]$ was investigated by B. Martel [Mar74]. Here, we use [BCE, Thm 3.1] to recover a large part of Martel's result, but also extend his result to arbitrary ideals $\mathfrak{P}_2^h$. Exclude the case where K_2/K_0 contains a maximally ramified quadratic subextension. (Martel's results include this case, and also the case where K_2/K_0 is not totally ramified.) Then the upper ramification numbers $u_1 \leq u_2$ are both odd, and the lower ramification numbers $b_1 \leq b_2$ are congruent modulo 4. We then have $2b_1 + b_2 = u_1 + 2u_2 \leq 6v_0(2) - 3$. Define

$$\mathfrak{A}_h = \{\alpha \in K_0[G] : \alpha\mathfrak{P}_2^h \subseteq \mathfrak{P}_2^h\}.$$

Note that $\mathfrak{A}_0 = \mathfrak{A}_{K_2/K_0}$. Martel's result is that $\mathfrak{O}_2$ is free over $\mathfrak{A}_0$ if and only if

$$2b_1 + b_2 \leq 4v_0(2) + 3(-1)^{(b_1-1)/2}. \tag{33}$$

In other words, [Mar74] finds that $\mathfrak{O}_2$ is always free over $\mathfrak{A}_0$ when $v_0(2)$ is sufficiently large relative to b_1 and b_2. In Proposition 4.2 below, we find, also assuming $v_0(2)$ is sufficiently large, that $\mathfrak{P}_2^3$ is always free over $\mathfrak{A}_3$, that $\mathfrak{P}_2$ is free over $\mathfrak{A}_1$ if and only if $b_1 \equiv 1 \bmod 4$, and that $\mathfrak{P}_2^2$ is free over $\mathfrak{A}_2$ if and only if $b_1 \equiv 3 \bmod 4$. In each case, what we mean by "sufficiently large" is determined by Proposition 4.1 and the value of h in $\mathfrak{P}_2^h$. When $h = 0$, our result excludes only one case covered by (33), namely the case $2b_1 + b_2 = 4v_0(2) + 3$ when $b_1 \equiv 1 \bmod 4$.

Proposition 4.1. *Let K_2/K_0 be a totally ramified biquadratic extension in characteristic 0 whose lower ramification numbers satisfy $2b_1 + b_2 < 4v_0(2)$. Then K_2/K_0 has a Galois scaffold of precision $\mathfrak{c} = 4v_0(2) - 2b_1 - b_2 \geq 1$.*

Proof. The condition $2b_1 + b_2 < 4v_0(2)$ ensures that $u_2 < 2v_0(2)$, so that u_1, u_2 are indeed odd. We have $b_1 = u_1$, $b_2 = b_1 + 4m$, $u_2 = u_1 + 2m$ for some integer $m \geq 0$. Then $K_2 = K_0(x_1, x_2)$ with $\wp(x_1) = \beta \in K_0$ where $v_0(\beta) = -b_1$ and $\wp(x_2) = \omega^2\beta + \epsilon$ where $\omega, \epsilon \in K_0$ with $v_0(\omega) = -m$ and $v_0(\epsilon) > -u_2$.

We now show that without loss of generality we may assume $v_0(\epsilon) \geq -2m$. If $v_0(\epsilon) < -2m$, there are two cases: If $v_0(\epsilon)$ is even, take $\eta \in K_0$ with $\eta^2\omega^2 \equiv \epsilon \bmod \mathfrak{P}_0\epsilon$. Then $-u_1/2 < v_0(\eta) = v_0(\epsilon)/2 + m < 0$, and $v_0(2\eta) > v_0(2) - u_1/2 > 0$. Set $x_1' = (1 + 2\eta)x_1 - \eta$. Then $v_1(x_1') = v_1(x_1) = -u_1$, and we calculate $\wp(x_1') = \beta'$ where $\beta' = \beta + \eta(\eta + 1)(1 + 4\beta) \in K_0$. We may therefore replace x_1 by x_1', β by $\beta' = \wp(x_1')$, and ϵ by $\epsilon' = \wp(x_2) - \beta'\omega^2$ and find $v_0(\epsilon') > v_0(\epsilon)$. If $v_0(\epsilon)$ is odd, take $\phi \in K_0$ so that $\beta\phi^2 \equiv \epsilon \bmod \mathfrak{P}_0\epsilon$. Then $v_0(\phi) = (v_0(\epsilon) + u_1)/2 > -m$ and also $v_0(2\beta\omega\phi) > v_0(\beta\phi^2)$ since $v_0(\epsilon) < -2m \leq 0 < 2v_0(2) - u_2$. Then $\wp(x_2) = \beta(\omega + \phi)^2 + \epsilon'$ with $\epsilon' = \epsilon - \beta\phi^2 - 2\beta\omega\phi$ where $v_0(\epsilon') > v_0(\epsilon)$. We may therefore replace ω by $\omega + \phi$ and ϵ by ϵ' and find $v_0(\epsilon') > v_0(\epsilon)$. Repeat these steps as necessary until $v_0(\epsilon) \geq -2m$.

The existence of a Galois scaffold follows from Theorem 3.5 once we verify Assumptions 3.2, 3.3 and 3.4. Assumption 3.2 is clear, and Assumption 3.3 is the statement that $v_0(\epsilon) > -u_2 + C_1 = -u_1/2 - 2m$, which holds since $v_0(\epsilon) \geq -2m$. Assumption 3.4 for $\mathfrak{c} \geq 1$ is equivalent to $4v_0(2) \geq 2b_1 + b_2 + \mathfrak{c}$. □

Proposition 4.2. *Let K_2 be a totally ramified biquadratic extension of K_0, with lower ramification numbers satisfying $2b_1 + b_2 < 4v_0(2)$.*

(i) *If $b_1 \equiv 1 \bmod 4$ then $\mathfrak{P}_2^h$ is free over $\mathfrak{A}_h$ when $h \equiv 0, 1 \bmod 4$ and $2b_1 + b_2 \leq 4v_0(2) - 1$, or when $h \equiv 3 \bmod 4$ and $2b_1 + b_2 \leq 4v_0(2) - 5$. Moreover, $\mathfrak{P}_2^h$ is not free over $\mathfrak{A}_h$ when $h \equiv 2 \bmod 4$ and $2b_1 + b_2 \leq 4v_0(2) - 9$.*

(ii) *If $b_1 \equiv 3 \bmod 4$ then $\mathfrak{P}_2^h$ is free over $\mathfrak{A}_h$ when $h \equiv 0, 2, 3 \bmod 4$ and $2b_1 + b_2 \leq 4v_0(2) - 3$. Moreover, $\mathfrak{P}_2^h$ is not free over $\mathfrak{A}_h$ when $h \equiv 1 \bmod 4$ and $2b_1 + b_2 \leq 4v_0(2) - 7$.*

Proof. The bounds on $2b_1 + b_2$ ensure that we always have $b_1 \equiv b_2 \equiv 1, 3 \bmod 4$. So let $b \in \{1, 3\}$ with $b \equiv b_2 \bmod 4$. Freeness of $\mathfrak{P}_2^h$ over $\mathfrak{A}_h$ depends only on the residue of $h \bmod 4$. So we may assume $0 \leq b - h < 4$. This choice of b and h is consistent with the notation of [BCE, §3.1]. The values of $L_1 := 4 + b - h$ and $L_2 := \max(1, b - h)$ are as shown in Table 4.1. A brute force check, as in the proof of [BCE, Thm 4.4], determines that the condition $w(s) = d(s)$ of [BCE, Thm 3.1] holds for all s except when $b = 1$, $h = -2$ or $b = 3$, $h = 1$. This gives the result; the bounds on $2b_1 + b_2$ in each case come from the fact that $\mathfrak{c}$ in Proposition 4.1 must be bounded below by either L_1 (for the assertion that $\mathfrak{P}_2^h$ is not free) or L_2

b	h	L_1	L_2
1	1	4	1
1	0	5	1
1	-1	6	2
1	-2	7	3
3	3	4	1
3	2	5	1
3	1	6	2
3	0	7	3

TABLE 1. Values of the bounds bounds on $\mathfrak{c}$ in the biquadratic case.

(for the assertion that it is free), together with the observation that $2b_1 + b_2 \equiv 3$ (respectively, 1) mod 4 if $b \equiv 1$ (respectively, 3) mod 4. $\square$

4.2. **Weakly ramified extensions.** A Galois extension of local fields is said to be weakly ramified if its second ramification group is trivial. An extension of global fields is weakly ramified if all its completions are. In a weakly ramified extension L/K of odd degree, there is a fractional ideal of $\mathfrak{O}_L$ whose square is the inverse different. It was shown by B. Erez [Ere91] that this ideal is locally free over the group ring $\mathfrak{O}_K[\mathrm{Gal}(L/K)]$. This led several subsequent authors (see for example [Vin03], [Pic09]) to investigate the square root of the inverse different in weakly ramified extensions, both of number fields and of local fields. The valuation ring, and its maximal ideal, in a weakly ramified (but not necessarily totally ramified) extension of local fields are studied as Galois modules in [Joh15].

Here we consider totally and weakly ramified Galois extensions K_n/K_0 of degree p^n, where K_0 is a local field whose residue field is perfect of characteristic p. Thus K_n/K_0 is necessarily elementary abelian. It is known that the valuation ring $\mathfrak{O}_n$ is free over its associated order. This can be proved using Lubin-Tate theory [Byo99, Cor 4.3] when the residue field is finite, but can also be deduced directly from Erez' result; see also [Joh15]. In this section, we will use [BCE, Thm 3.1] to give an alternative proof of this result, while at the same time determining the structure of the other ideals. Thus we define

$$\mathfrak{A}_h = \{\alpha \in K_0[G] : \alpha\mathfrak{P}_n^h \subseteq \mathfrak{P}_n^h\}.$$

Again, note that $\mathfrak{A}_0 = \mathfrak{A}_{L/K}$. We begin with the fact that a Galois scaffold exists. Note that in characteristic p, K_n/K_0 has a Galois scaffold of precision ∞ [Eld09].

Proposition 4.3. *Let K_0 be a local field of characteristic 0 whose residue field is perfect of characteristic p, and let K_n/K_0 be a totally and weakly ramified Galois extension of K_0 of degree p^n. Then K_n/K_0 has a Galois scaffold of precision $\mathfrak{c} = p^n v_0(p) - (p^n - 1)$.*

Proof. The hypothesis means that K_n/K_0 is elementary abelian of degree p^n, with $b_i = u_i = 1$ for $1 \le i \le n$. When $n = 1$, the result follows from Theorem 3.1. When $n \ge 2$, the result will follow from Theorem 3.5 provided that Assumptions 3.2, 3.3 and 3.4 hold. Using [FV02, III §2.5 Prop], $K_n = K_0(x_1, \dots, x_n)$ where $\wp(x_i) = \omega_i^{p^{n-1}}\beta + \epsilon_i$ for some $\beta \in K_0$ with $v_0(\beta) = -1$, some $\omega_i \in \mathfrak{O}_0 \setminus \mathfrak{P}_0$ which, in the residue field $\mathfrak{O}_0/\mathfrak{P}_0$, are linearly independent over $\mathbb{F}_p$, and some $\epsilon_i \in \mathfrak{O}_0$. Since $b_i = u_i = 1$ for all i, Assumptions 3.2 and 3.3 hold. Furthermore Assumption 6 holds since by choice of $\mathfrak{c}$, $v_0(p) = 1 - 1/p^n + \mathfrak{c}/p^n = C_n + \mathfrak{c}/p^n$. □

We now give a new proof of the fact that the valuation ring of a totally and weakly ramified extension is free over its associated order, and that the square root of the inverse different is free over the group ring. Our proof depends on the existence of a Galois scaffold, and works both in characteristic p and characteristic 0, with no hypothesis on $v_0(p)$.

Proposition 4.4. *Let K_n/K_0 be a totally and weakly ramified Galois extension of local fields, and let $G = \mathrm{Gal}(K_n/K_0)$. Then $\mathfrak{P}_n$ (respectively, $\mathfrak{O}_n$) is free over $\mathfrak{O}_0[G]$ (respectively, over $\mathfrak{O}_0[G][\pi_0^{-1}\mathrm{Tr}_{n,0}]$, where $\mathrm{Tr}_{n,0} = \sum_{g\in G} g$ is the trace element in $K_0[G]$), and any element of K_n of valuation 1 is a generator.*

Proof. We are interested in the Galois module structure of $\mathfrak{P}_n^h$ for $h = 0$ and $h = 1$. Since $b_i = 1$ for all i, we may assume that $b = 1$. Our notation, namely h, b, is consistent with the notation in [BCE, §3.1]. Using Proposition 4.3, K_n/K_0 has a Galois scaffold of precision $\mathfrak{c} \geq 1 = \max(b - h, 1)$. The numbers $d(s)$ and $w(s)$ occurring in [BCE, Thm 3.1] are easy to determine in this case (as in the proof of [BCE, Thm 4.5]); we find when $h = 1$ that $d(s) = w(s) = 0$ for all $s \in \mathbb{S}_{p^n} = \{s : 0 \leq s < p^n\}$, and when $h = 0$ that $d(s) = w(s) = 0$ for all $s \neq p^n - 1$ and $d(p^n - 1) = w(p^n - 1) = 1$. Since $d(s) = w(s)$ for all s, both $\mathfrak{P}_n$ and $\mathfrak{O}_n$ are free over their associated orders by [BCE, Thm 3.1(iv)]. We now identify those associated orders. For $h = 1$, we have $w(s) = 0$ for all s, so $\mathfrak{A}_1 = \mathfrak{O}_0[\Psi_1, \dots, \Psi_n]$. Since in the proof of Proposition 4.3 and in [Eld09, Prop 5.3], we have $\omega_i \in \mathfrak{O}_0$ for all i, it follows from the construction of the Galois scaffold that $\Psi_i \in \mathfrak{O}_0[G]$ for all i. Hence $\mathfrak{A}_1 \subseteq \mathfrak{O}_0[G]$. Since the reverse inclusion certainly holds, we have $\mathfrak{A}_1 = \mathfrak{O}_0[G]$ when $h = 1$. When $h = 0$, we have $w(s) = 0$ for $s \neq p^n - 1$ and $w(p^n - 1) = 1$, so $\mathfrak{A}_0 = \mathfrak{O}_0[G] + \mathfrak{O}_0\pi_0^{-1}\Psi^{(p^n-1)}$. Thus $\mathfrak{A}_0/\mathfrak{O}_0[G]$ has dimension 1 over $\mathfrak{O}_0/\mathfrak{P}_0$. But $\pi_0^{-1}\mathrm{Tr}_{n,0} \in \mathfrak{A}_0$ since $\mathrm{Tr}_{K_n/K_0}(\mathfrak{O}_n) \subsetneq \mathfrak{O}_0$ because K_n/K_0 is wildly ramified. It follows that $\mathfrak{A}_0 = \mathfrak{O}_0[G] + \mathfrak{O}_0\pi_0^{-1}\mathrm{Tr}_{n,0}$.

We next show that any $\pi_n \in K_n$ of valuation 1 is a free generator for $\mathfrak{P}_n$ and $\mathfrak{O}_n$. This follows from [BCE, Thm 3.1(ii)] if $v_0(p) \geq 2$, because then $\mathfrak{c} \geq p^n + b - h$. So we need only consider the case $v_0(p) = 1$, when K_0 has characteristic 0 and is unramified over the p-adic numbers. We nevertheless give a proof which works more generally. We may write $\pi_n = \sum_{i=1}^{p^n} a_i\lambda_i$ for some $a_i \in \mathfrak{O}_0$ with $v_0(a_0) = 0$. Since, by Theorem 2.10, the Ψ_j are K_0-linear maps, we observe as in [BCE, (5)] that $v_n(\Psi^{(j)}\lambda_i) \geq i + j$ with $v_n(\Psi^{(j)}\lambda_1) = 1 + j$. It follows that $v_n(\Psi^{(s)}\pi_n) = s + 1$ for all $s \in \mathbb{S}_{p^n}$. Thus $\mathfrak{O}_0[G]\pi_n = \mathfrak{P}_n$ and $(\mathfrak{O}_0[G] + \mathfrak{O}_0\pi_0^{-1}\mathrm{Tr}_{n,0})\pi_n = \mathfrak{O}_n$, as required. □

Remark 4.5. The valuation of the different of K_n/K_0 is $2(p^n - 1)$, so the square root of the inverse different is $\mathfrak{P}_n^{1-p^n}$, which is isomorphic to $\mathfrak{P}_n$. The fact that the square root of the inverse different is free over the group ring $\mathfrak{O}_0[G]$ therefore follows from the case $h = 1$ in Proposition 4.4.

We now use the Galois scaffold of Proposition 4.3 to determine which other ideals $\mathfrak{P}_n^h$ are free over their associated orders.

Proposition 4.6. *Let K_n/K_0 be as in Proposition 4.3 with $v_0(p) \geq 3$. Then $\mathfrak{P}_L^h$ is free over its associated order if and only if $h \equiv h' \bmod p^n$ where $h' = 0$, $h' = 1$, or $\frac{1}{2}(p^n + 1) < h' < p^n$.*

Proof. The condition $v_0(p) \geq 3$ ensures that K_n/K_0 has a Galois scaffold of precision $\mathfrak{c} \geq 2p^n - 1$. We can therefore apply [BCE, Thm 3.1(ii)]. The condition on h then follows as in [BCE, Thm 4.5]. □

4.3. **Abrashkin's elementary extensions.** Let K_0 be a local field of characteristic 0 with perfect residue field of characteristic p containing the field of p^n elements. Following [FV02, III§2 Ex.4], we define K_n to be an elementary extension of K_0 if $K_n = K_0(x)$ where $x^{p^n} - x = \tau$ with $\tau \in K_0$ and $v_0(\tau) > -p^n v_0(p)/(p^n - 1)$.

In the case that K_0 is unramified over $\mathbb{Q}_p$, the elementary extensions were introduced by V. Abrashkin [Abr87], who used them in his proof that there are no abelian schemes over $\mathbb{Z}$.

We set $u = -v_0(\tau)$, and make the further assumptions that $u > 0$, $\gcd(u, p) = 1$. Then K_n/K_0 is a totally ramified elementary abelian extension of degree p^n, with unique ramification break u. Furthermore K_n/K_0 has a Galois scaffold, directly generalizing Theorem 3.1, which concerns the case $n = 1$.

Proposition 4.7. *If K_n/K_0 is an elementary abelian extension as above, then K_n/K_0 has a Galois scaffold of precision $\mathfrak{c} = p^n v_0(p) - (p^n - 1)u \geq 1$.*

Proof. Let $\mathbb{F}_p$ be the finite field with p elements and $\mathbb{F}_{p^n}$ the finite field with p^n elements contained in the residue field $\mathfrak{O}_0/\mathfrak{P}_0$. Let $\omega_1 = 1, \omega_2, \ldots, \omega_n \in \mathfrak{O}_0$ be Teichmüller representatives for an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^n}$. So $\omega_i^{p^n} = \omega_i$. We prove that $K_n = K_0(x_1, \ldots, x_n)$ where $x_i^p - x_i = \omega_i \tau$. But this follows if we prove that for each i, $z^p - z = \omega_i \tau$ has p solutions in K_n. Consider the polynomial

$$f(y) = \left(\sum_{r=0}^{n-1} (\omega_i x)^{p^r} + y\right)^p - \left(\sum_{r=0}^{n-1} (\omega_i x)^{p^r} + y\right) - \omega_i \tau \in K_n[y].$$

The bound on t means that $f(y) \equiv y^p - y \bmod \mathfrak{P}_n$, so $f(y)$ has p roots in K_n by Hensel's Lemma.

We have ramification numbers $b_i = u_i = u$ for all i. As $\gcd(u, p) = 1$, Assumption 3.2 is satisfied, and Assumption 3.3 is satisfied since $\epsilon_i = 0$ for all i. Finally, Assumption 6 with precision $\mathfrak{c}$ is equivalent to $p^n v_0(p) \geq (p^n - 1)u + \mathfrak{c}$. This holds for $\mathfrak{c} = p^n v_0(p) - (p^n - 1)u$, and then $\mathfrak{c} \geq 1$ by the condition on $v_0(\tau)$. □

Corollary 4.8. *Let K_n/K_0 be an elementary extension as above with $u > 0$, $\gcd(u, p) = 1$, and suppose that u satisfies the slightly more restrictive condition*

$$u < \frac{p^n v_0(p)}{p^n - 1} - 2.$$

Then the freeness or otherwise of any fractional ideal $\mathfrak{P}_n^h$ of $\mathfrak{O}_n$ is determined by the numerical data $d(s)$, $w(s)$ as in [BCE, Thm 3.1]. *In particular, $\mathfrak{O}_n$ itself is free over its associated order $\mathfrak{A}_0 = \mathfrak{A}_{L/K}$ if the least non-negative residue b of u mod p^n divides $p^m - 1$ for some $m \leq n$. For $n = 2$, $\mathfrak{O}_n$ is free over $\mathfrak{A}_0$ if and only if b divides $p^2 - 1$.*

Proof. The condition on u ensures that there is a Galois scaffold of precision $\mathfrak{c} \geq 2p^n - 1$, so that all parts of [BCE, Thm 3.1] apply. The statements about $\mathfrak{O}_n$ follow from [BCE, Cor 3.3]. □

Remark 4.9. The corresponding extensions in characteristic p have a Galois scaffold of precision ∞ [Eld09, Lemma 5.2]. Hence the conclusions of Corollary 4.8 hold for these extensions as well.

5. New directions: Constructing Hopf orders in $K[G]$

The purpose of this section is to illustrate how the results of this paper can be used to construct commutative and cocommutative Hopf algebras over valuation rings of local fields and thus shed light on the construction of finite abelian group schemes over such rings. Our purpose here is not to be exhaustive, but simply to illustrate the utility of a Galois scaffold outside of the Galois module structure of ideals in local field extensions.

5.1. **Background.** Let K be a local field of residue characteristic $p > 0$, and let G be a finite abelian p-group. There are not many results that classify Hopf algebras defined over $\mathfrak{O}_K$ within $K[G]$ (*i.e.* Hopf orders). If G has order p, the classification of Hopf orders follows from work of Tate and Oort on group schemes of rank p [TO70]. If $\mathrm{char}(K) = 0$ and K contains the p roots of unity, Greither classified a family of Hopf orders for $G \cong C_{p^2}$ [Gre92]. Under the same assumptions, Byott classified all Hopf orders for $G \cong C_p \times C_p$, and assuming that K contains the p^2 roots of unity, all Hopf orders for $G \cong C_{p^2}$ [Byo93a, Byo93b]. More recently, Tossici classified all Hopf orders for G of order p^2 without any restriction on the field K [Tos10]. Motivated by the construction in this section, specifically Example 5.2, the classification for $G \cong C_p \times C_p$ and $\mathrm{char}(K) = p$ was reproven using Greither's approach [EU17]. For G of order p^n, $n \geq 3$ there are families of Hopf orders for G cyclic [Und96, CU03, CU04, UC06] and for G elementary abelian [CS98, GC98, CS05]. For $n = 3$, these families are known to be incomplete. More recently, Mézard, Romagny and Tossici produce a family of Hopf orders for G cyclic that they conjecture is complete [MRT13]. Still for $p = 3$, the conjecture is unproven. Additional methods are needed.

5.2. **A method for constructing Hopf orders.** Let K be a local field with residue characteristic $p > 0$. In particular, K can have characteristic 0 or p. Let L/K be a totally ramified extension of degree p^n, $n > 1$ with abelian Galois group G, and let the lower ramification numbers b_i satisfy $b_i \equiv -1 \bmod p^n$ (thus Assumptions 2.2 and 2.6 hold with $b = p^n - 1$). Assume now that it is possible to make Choices 2.1 and 2.3 so that Assumption 2.9 holds with $\mathfrak{c} \geq p^n - 1$. Under these circumstances, Theorem 2.10 states that a scaffold exists for the action of $K[G]$ on L/K. As explained in [BCE, Remark 3.5], it then follows from [BCE, Theorem 3.1] that the ring of integers $\mathfrak{O}_L$ is free over its associated order $\mathfrak{A}_{L/K}$, and also that this associated order takes a particularly simple form:

$$\mathfrak{A}_{L/K} = \mathfrak{O}_K \left[\frac{\Theta_n - 1}{\pi_K^{M_n}}, \dots, \frac{\Theta_2 - 1}{\pi_K^{M_2}}, \frac{\Theta_1 - 1}{\pi_K^{M_1}} \right], \tag{34}$$

for integers $M_i \geq 0$ satisfying $M_i = (b_i + 1)/p^i$. Furthermore, the Θ_i are as defined in Definition 2.7, with

$$v_K(\mu_{i,j}) = (b_i - b_j)/p^j = p^{i-j} M_i - M_j. \tag{35}$$

Now assume the very weak condition that largest lower ramification number b_n satisfies $b_n - \lfloor b_n/p \rfloor \leq p^{n-1} v_K(p)$, where $\lfloor \cdot \rfloor$ denotes the greatest integer function.

This condition is empty in characteristic p, and because of the congruences on b_i, it eliminates only certain cyclic extensions in characteristic 0 [Byo97, Proposition 3.7]. Under this assumption, $\mathfrak{A}_{L/K}$ is a local ring (equivalently, $\mathfrak{O}_L$ is indecomposable as an $\mathfrak{O}_K[G]$-module) [Vos74, Theorem 3], [Vos76, Theorem 4]. The congruence conditions on the b_i can then be used together with [Ser79, IV §2 Proposition 4] to see that the different satisfies $\mathfrak{D}_{L/K} = \delta\mathfrak{O}_L$ for some $\delta \in K$. We are now in a position to use a result of Bondarko, and so, since $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$, the associated order $\mathfrak{A}_{L/K}$ is a Hopf order [Bon00, Thm A, Prop 3.4.1].

Remark 5.1. A Hopf order $\mathfrak{H}$ in a group algebra $K[G]$ is said to be realizable if there is an extension L/K such that $\mathfrak{O}_L$ is an $\mathfrak{H}$-Hopf Galois extension of $\mathfrak{O}_K$. When $\mathfrak{H}$ is itself a commutative local ring, this is equivalent to saying that $\mathfrak{H}$ arises as the associated order of some valuation ring $\mathfrak{O}_L$. Moreover, in this case, $\mathfrak{H}$ is realizable if and only if its dual Hopf order is monogenic as an $\mathfrak{O}_K$-algebra [Byo04]. The Hopf orders $\mathfrak{A}_{L/K}$ we consider here are, by construction, associated orders of valuation rings, and hence are realizable.

5.3. **Hopf orders in $K[C_p^n]$.** In the case that K has characteristic 0 and G is elementary abelian, several families of Hopf orders have been described [CS98, GC98, CS05]. It is therefore of interest to describe the elementary abelian Hopf orders that result from this paper in a little more detail. But, although we provide some superficial comments regarding our Hopf orders and those in [CS05], we leave a careful comparison of the families of Hopf orders for a later paper.

We first construct some elementary abelian extensions. Again, K may be of either characteristic. Choose an integer $m_1 \geq 1$ and integers $m_i \geq 0$ for $i \geq 2$ so that

$$v_K(p) \geq m_1(p^n - 1) + \sum_{k=2}^{n}(p^{n-1} - p^{k-2})m_k. \tag{36}$$

No such integers are possible unless $v_K(p)$ is big enough, namely $v_K(p) \geq p^n - 1$. The restriction is vacuous if K has characteristic p. Note that if we can now arrange for our extension to have upper and lower ramification numbers as in §3.2 with $b_1 = p^n m_1 - 1$, then (36) is equivalent to $v_K(p) \geq u_n - b_n/p^n + \mathfrak{c}/p^n$, Assumption 3.4, with $\mathfrak{c} = p^n - 1$.

Choose $\beta \in K$ with $v_K(\beta) = -b_1 = 1 - m_1 p^n$. Thus Assumption 3.2 holds. Choose elements $\omega_i \in K$ for $i \geq 2$ such that $v_K(\omega_i) = -\sum_{k=2}^{i} m_i$, and furthermore assume that, whenever $v_K(\omega_i) = \cdots = v_K(\omega_j)$ with $i < j$, the projections of $\omega_i, \ldots, \omega_j$ into $\omega_i\mathfrak{O}_K/\omega_i\mathfrak{P}_K$ are linearly independent over $\mathbb{F}_p$, the finite field with p elements. This last assumption requires $[\mathfrak{O}_K/\mathfrak{P}_K : \mathbb{F}_p]$ to be strictly larger than the longest string of consecutive zeros in $(m_2, \ldots, m_n)$. Let $L = K(x_1, \ldots, x_n)$ where $\wp(x_1) = \beta$ and $\wp(x_i) = \omega_i^{p^{n-1}}\beta$ for $2 \leq i \leq n$. All this is in agreement with §3.2, except that because we have chosen $\epsilon_i = 0$, Assumption 3.3 is vacuous.

At this point, we have L/K, a totally ramified elementary abelian extension of degree p^n with $\mathrm{Gal}(L/K) = \langle\sigma_1, \ldots, \sigma_n\rangle$ where $(\sigma_i - 1)x_j \equiv \delta_{ij} \bmod \mathfrak{P}_L$. This extension has a Galois scaffold of precision $\mathfrak{c} = p^n - 1$ in characteristic 0 and $\mathfrak{c} = \infty$ in characteristic p. And based upon §5.2, we have a Hopf order of the form (34).

An explicit description of this Hopf order however, requires that we describe the integers M_i, as well as the elements $\mu_{i,j} \in K$ that are used to define the Θ_i in

Definition 2.7. Since

$$p^i M_i = b_i + 1 = p^n(m_1 + \sum_{k=2}^{i} p^{k-2} m_k), \tag{37}$$

these nonnegative integers satisfy

$$p^r M_r \le p^s M_s, \tag{38}$$

for all $1 \le r \le s \le n$. (Note that $i_j = M_{n-j+1}$ translates our notation into analogous notation, namely *valuation parameters*, in [CS05, p. 491]. In their terms, our condition becomes $p^{s-r} i_r \ge i_s$ for $r \le s$, which is weaker that their requirement, $pi_r \ge i_s$ for $r < s$.) Meanwhile, (36), which is vacuous in characteristic p, can be rewritten, using (37):

$$\frac{v_K(p)}{p-1} \ge \sum_{i=1}^{n} M_i. \tag{39}$$

(This is stronger than the condition $v_K(p)/(p-1) > i_j$ in [CS05].) We note that there are also congruence conditions imposed by (37), which we ignore, recalling Remark 3.6, until we can say which are an artifact of our scaffold construction, and which are not.

Turning to the $\mu_{i,j}$, superficial comparisons with analogous expressions in [CS05] become impossible. A detailed translation would greatly expand the scope of the paper. So we close with two examples, $n = 2, 3$, where we include all the details.

Example 5.2. Let $C_p^2 = \langle \sigma_2, \sigma_1 \rangle$. Choose any integers $M_i \ge 0$ such that $M_1 \le pM_2$ and $p \mid M_1$, and let $\mu_{1,2} \in K$ be any element with $v_K(\mu_{1,2}) = M_1/p - M_2$. Then

$$\mathfrak{O}_K \left[\frac{\sigma_2 - 1}{\pi_K^{M_2}}, \frac{\sigma_1 \sigma_2^{[-\mu_{1,2}]} - 1}{\pi_K^{M_1}} \right]$$

is a Hopf order in $K[C_p^2]$ when K has characteristic p. It is a Hopf order in $K[C_p^2]$ when K has characteristic 0 under the additional assumption that $v_K(p)/(p-1) \ge M_1 + M_2$. Note that the valuation of $\mu_{1,2}$ makes $p \mid M_1$ redundant.

Example 5.3. Let $C_p^3 = \langle \sigma_3, \sigma_2, \sigma_1 \rangle$. Choose any integers $M_i \ge 0$ such that $pM_1 \le p^2 M_2 \le p^3 M_3$ and $p^{3-i} \mid M_i$, but $p \mid M_3$. Let $\mu_{i,j} \in K$ be elements with $v_K(\mu_{i,j}) = p^{i-j} M_i - M_j$ that arise from elements $\omega_1, \omega_2 \in K$ via the matrix $(\mathbf{\Omega})$ defined in (12), as explained in the proof of Lemma 3.8. In other words,

$$\mu_{1,2} = -\omega_2^p, \quad \mu_{2,3} = -\frac{\omega_3^p - \omega_3}{\omega_2^p - \omega_2}, \quad \mu_{1,3} = -\frac{\omega_3 \omega_2^p - \omega_2 \omega_3^p}{\omega_2^p - \omega_2}. \tag{40}$$

Then

$$\mathfrak{O}_K \left[\frac{\sigma_3 - 1}{\pi_K^{M_3}}, \frac{\sigma_2 \sigma_3^{[-\mu_{2,3}]} - 1}{\pi_K^{M_2}}, \frac{\sigma_1 \sigma_3^{[-\mu_{1,3}]} (\sigma_2 \sigma_3^{[-\mu_{2,3}]})^{[-\mu_{1,2}]} - 1}{\pi_K^{M_1}} \right]$$

is a Hopf order in $K[C_p^3]$ when K has characteristic p. It is a Hopf order in $K[C_p^3]$ when K has characteristic 0 under the additional assumption that $v_K(p)/(p-1) \ge M_1 + M_2 + M_3$. Note that the valuation of $\mu_{i,j}$ makes $p^{3-i} \mid M_i$, but not $p \mid M_3$, redundant. Thus we suspect $p \mid M_3$ to be an artifact of our scaffold construction. We are uncertain as to the the significance of (40).

Remark 5.4. Although we are not yet prepared to carefully analyze the Hopf orders described in this section in comparison with those that appear in [CS98, GC98, CS05], we can say that the Hopf orders in Example 5.3 do not appear in [CS05]. The Hopf orders in Example 5.3 are realizable, while the Hopf orders with $n = 3$ in [CS05] are not. See [CS05, Proposition 15].

References

[Abr87] Victor A. Abrashkin, *Galois modules of group schemes of period p over the ring of Witt vectors*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 4, 691–736, 910, English transl. in Math. USSR-Izv. **31** (1988), no. 1, 1-46.

[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.

[BCE] Nigel P. Byott, Lindsay N. Childs, and G. Griffith Elder, *Scaffolds and generalized integral Galois modules structure*, Preprint, April 2014, available at arXiv:1308.2088 [math.NT].

[BE13] Nigel P. Byott and G. Griffith Elder, *Galois scaffolds and Galois module structure in extensions of characteristic p local fields of degree* p^2, J. Number Theory **133** (2013), no. 11, 3598–3610.

[BE14] ———, *Integral Galois module structure for elementary abelian extensions with a Galois scaffold*, Proc. Amer. Math. Soc. **142** (2014), no. 11, 3705–3712.

[Ber72] Anne-Marie Bergé, *Sur l'arithmétique d'une extension diédrale*, Ann. Inst. Fourier (Grenoble) **22** (1972), 31–59.

[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.

[Bon00] Mikhail V. Bondarko, *Local Leopoldt's problem for rings of integers in abelian p-extensions of complete discrete valuation fields*, Doc. Math. **5** (2000), 657–693 (electronic).

[Bon02] ———, *Local Leopoldt's problem for ideals in totally ramified p-extensions of complete discrete valuation fields*, Algebraic number theory and algebraic geometry, Contemp. Math., vol. 300, Amer. Math. Soc., Providence, RI, 2002, pp. 27–57.

[Bon06] ———, *Leopoldt's problem for abelian totally ramified extensions of complete discrete valuation fields*, Algebra i Analiz **18** (2006), no. 5, 99–129, English transl. in St. Petersburg Math. J. **18** (2007) no. 5, 757–778.

[Bur91] David J. Burns, *Factorisability and wildly ramified Galois extensions*, Ann. Inst. Fourier (Grenoble) **41** (1991), no. 2, 393–430.

[Bur00] David Burns, *On the equivariant structure of ideals in abelian extensions of local fields*, Comment. Math. Helv. **75** (2000), no. 1, 1–44, With an appendix by W. Bley.

[Byo93a] Nigel P. Byott, *Cleft extensions of Hopf algebras*, J. Algebra **157** (1993), no. 2, 405–429.

[Byo93b] ———, *Cleft extensions of Hopf algebras. II*, Proc. London Math. Soc. (3) **67** (1993), no. 2, 277–304.

[Byo97] ———, *Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications*, J. Théor. Nombres Bordeaux **9** (1997), no. 1, 201–219.

[Byo99] ———, *Integral Galois module structure of some Lubin-Tate extensions*, J. Number Theory **77** (1999), no. 2, 252–273.

[Byo04] ———, *Monogenic Hopf orders and associated orders of valuation rings*, J. Algebra **275** (2004), no. 2, 575–599.

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

[CS98] Lindsay Childs and Jim Sauerberg, *Degree 2 formal groups and Hopf algebras*, Mem. Amer. Math. Soc. **136** (1998), no. 651, 55–90.

[CS05] Lindsay N. Childs and Harold H. Smith, III, *Dual Hopf orders in group rings of elementary abelian p-groups*, J. Algebra **294** (2005), no. 2, 489–518.

[CU03] Lindsay N. Childs and Robert G. Underwood, *Cyclic Hopf orders defined by isogenies of formal groups*, Amer. J. Math. **125** (2003), no. 6, 1295–1334.

[CU04] ———, *Duals of formal group Hopf orders in cyclic groups*, Illinois J. Math. **48** (2004), no. 3, 923–940.

[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.

[Ere91] Boas Erez, *The Galois structure of the square root of the inverse different*, Math. Z. **208** (1991), no. 2, 239–255.

[EU17] G. Griffith Elder and Robert G. Underwood, *Finite group scheme extensions, and Hopf orders in KC_p^2 over a characteristic p discrete valuation ring*, New York J. Math. **23** (2017), 11–39.

[Fer72] Marie-Josée Ferton, *Sur l'anneau des entiers d'une extension diédrale de degré $2p$ d'un corps local*, C. R. Acad. Sci. Paris Sér. A-B **274** (1972), A1529–A1532.

[Fer73] ———, *Sur les idéaux d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sci. Paris Sér. A-B **276** (1973), A1483–A1486.

[Fer75] ———, *Sur l'anneau des entiers de certaines extensions cycliques d'un corps local*, Astérisque **24–25** (1975), 21–28.

[FV02] Ivan B. Fesenko and Sergei V. Vostokov, *Local fields and their extensions*, second ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, Providence, RI, 2002, With a foreword by I. R. Shafarevich.

[GC98] Cornelius Greither and Lindsay Childs, *p-elementary group schemes – constructions, and Raynaud's theory*, Mem. Amer. Math. Soc. **136** (1998), no. 651, 91–117.

[Gre92] Cornelius Greither, *Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring*, Math. Z. **210** (1992), no. 1, 37–67.

[Huy14] Duc Van Huynh, *Artin-Schreier extensions and generalized associated orders*, J. Number Theory **136** (2014), 28–45.

[Joh15] Henri Johnston, *Explicit integral Galois module structure of weakly ramified extensions of local fields*, Proc. Amer. Math. Soc. **143** (2015), no. 12, 5059–5071.

[Leo59] Heinrich-Wolfgang Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. **201** (1959), 119–149.

[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.

[Mar14] Maria L. Marklove, *Local Galois module structure in characteristic p*, Ph.D. thesis, University of Exeter, 2014, `https://ore.exeter.ac.uk/repository/handle/10871/14743`.

[Miy98] Yoshimasa Miyata, *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.

[MRT13] A. Mézard, M. Romagny, and D. Tossici, *Models of group schemes of roots of unity*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 1055–1135.

[Noe32] Emmy Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. Reine Angew. Math. **167** (1932), 147–152.

[Pic09] Erik Jarl Pickett, *Explicit construction of self-dual integral normal bases for the square-root of the inverse different*, J. Number Theory **129** (2009), no. 7, 1773–1785.

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

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[TO70] John Tate and Frans Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21.

[Tos10] Dajano Tossici, *Models of $\mu_{p^2,K}$ over a discrete valuation ring*, J. Algebra **323** (2010), no. 7, 1908–1957, With an appendix by Xavier Caruso.

[UC06] Robert G. Underwood and Lindsay N. Childs, *Duality for Hopf orders*, Trans. Amer. Math. Soc. **358** (2006), no. 3, 1117–1163.

[Und96] Robert Underwood, *The valuative condition and R-Hopf algebra orders in KC_{p^3}*, Amer. J. Math. **118** (1996), no. 4, 701–743.

[Vin03] Stéphane Vinatier, *Sur la racine carrée de la codifférente*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 393–410, Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[Vos74] Sergei V. Vostokov, *Ideals of the abelian p-extension of an irregular local field as Galois modules*, Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **46** (1974), 14–35, 140, Modules and representations.

[Vos76] ———, *Ideals of an Abelian p-extension of a local field as Galois modules*, Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **57** (1976), 64–84, 177, Modules in representation theory and algebraic geometry.

Department of Mathematics, University of Exeter, Exeter EX4 4QF U.K.
E-mail address: `N.P.Byott@exeter.ac.uk`

Department of Mathematics, University of Nebraska at Omaha, Omaha NE 68182-0243 U.S.A.
E-mail address: `elder@unomaha.edu`