Journal of Number Theory 278 (2026) 893–923

Contents lists available at ScienceDirect

Journal of Number Theory

journal homepage: www.elsevier.com/locate/jnt

General Section

Galois scaffolds for extraspecial p-extensions in characteristic 0

Kevin Keating [a], Paul Schwartz [b,*]

[a] Department of Mathematics, University of Florida, Gainesville, FL 32611, USA
[b] Department of Mathematical Sciences, Stevens Institute of Technology, Hoboken, NJ 07030, USA

ARTICLE INFO

Article history:
Received 24 July 2024
Received in revised form 8 May 2025
Accepted 11 May 2025
Available online 19 June 2025
Communicated by F. Pellarin

Keywords:
Galois scaffolds
Galois module structure
Hopf algebras
Extraspecial p-groups

ABSTRACT

Let K be a local field of characteristic 0 with residue characteristic $p > 2$. Let G be an extraspecial p-group and let L/K be a totally ramified G-extension. In this paper we find sufficient conditions for L/K to admit a Galois scaffold. This leads to sufficient conditions for the ring of integers $\mathfrak{O}_L$ to be free of rank 1 over its associated order $\mathfrak{A}_{L/K}$, and to stricter conditions which imply that $\mathfrak{A}_{L/K}$ is a Hopf order in the group ring $K[G]$.

1. Introduction

Let L/K be a finite totally ramified extension of local fields and set $G = \mathrm{Gal}(L/K)$. The associated order in $K[G]$ of the ring of integers $\mathfrak{O}_L$ of L is defined to be

$$\mathfrak{A}_{L/K} = \{\lambda \in K[G] : \lambda(\mathfrak{O}_L) \subset \mathfrak{O}_L\}.$$

* Corresponding author.
E-mail addresses: keating@ufl.edu (K. Keating), pschwart@stevens.edu (P. Schwartz).

https://doi.org/10.1016/j.jnt.2025.05.005
0022-314X/

Thus $\mathfrak{A}_{L/K}$ is an $\mathfrak{O}_K$-order in $K[G]$, and $\mathfrak{O}_L$ is a module over $\mathfrak{A}_{L/K}$. It is a classical problem to determine whether $\mathfrak{O}_L$ is free (necessarily of rank 1) over $\mathfrak{A}_{L/K}$. In the case where L/K is tamely ramified we have $\mathfrak{A}_{L/K} = \mathfrak{O}_K[G]$, and E. Noether showed that $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$ [20]. Much less is known about this problem in the case where L/K is wildly ramified. When L/K is a ramified C_p-extension, necessary and sufficient conditions for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_{L/K}$ were given in [3,2] for the case $\mathrm{char}(K) = 0$, and in [1,18] for the case $\mathrm{char}(K) = p$. Sufficient conditions are known for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_{L/K}$ in the cases where G is an elementary abelian p-group [7], $G \cong C_{p^2}$ and $\mathrm{char}(K) = p$ [6], or $G \cong C_{p^2}$ and $\mathrm{char}(K) = 0$ [17]. When $\mathrm{char}(K) = p$, [12] gives sufficient conditions for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_{L/K}$ in the case where G is an arbitrary p-group.

In this paper we give sufficient conditions for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_{L/K}$ in the cases where $\mathrm{char}(K) = 0$ and $G = \mathrm{Gal}(L/K)$ is an extraspecial p-group. As an application we give sufficient conditions for $\mathfrak{A}_{L/K}$ to be a Hopf order. Our proofs are based on constructing extensions L/K which possess a Galois scaffold, as defined in [8]. We focus on the case $\mathrm{char}(K) = 0$, but all the statements and proofs presented here are valid, and often simpler, when $\mathrm{char}(K) = p$.

Let K be a local field of characteristic 0 with residue characteristic p. Then K is complete with respect to a discrete valuation v_K which is normalized so that $v_K(K^\times) = \mathbb{Z}$. The ring of integers of K is $\mathfrak{O}_K = \{x \in K : v_K(x) \geq 0\}$ and the unique maximal ideal of $\mathfrak{O}_K$ is $\mathfrak{M}_K = \{x \in K : v_K(x) \geq 1\}$. Let π_K be a uniformizer for K. Thus π_K is any element of $\mathfrak{O}_K$ that satisfies $v_K(\pi_K) = 1$, or equivalently $\mathfrak{M}_K = (\pi_K)$. We assume that the residue field $\mathfrak{O}_K/\mathfrak{M}_K$ of K is a perfect field of characteristic p. Let $e_K = v_K(p)$ be the absolute ramification index of K and let K^{sep} be a separable closure of K. Then v_K extends uniquely to a valuation on K^{sep}, which we also denote by v_K. We will often work with towers $K_0 \subset K_1 \subset \cdots \subset K_n$ of field extensions of degree p. In this case we usually denote $v_{K_i}, \mathfrak{O}_{K_i}, \mathfrak{M}_{K_i}, \pi_{K_i}, e_{K_i}$ by $v_i, \mathfrak{O}_i, \mathfrak{M}_i, \pi_i, e_i$.

2. Higher ramification theory

In this section we recall some facts about higher ramification theory of finite separable extensions of local fields. We do not assume that our extensions are Galois, but for simplicity we only consider extensions whose degree is a power of p. For more information about higher ramification theory for extensions which are separable, but not necessarily Galois, see [15], [16], the appendix to [10], or Chapter 13 of [9].

Let K be a local field with residue characteristic p and let L/K be a subextension of K^{sep}/K of degree p^n. Let L_0/K be the maximal unramified subextension of L/K. Let Γ denote the set of K-embeddings of L into K^{sep}, and let Γ_0 be the subset of Γ consisting of $\sigma \in \Gamma$ such that $\sigma(L_0) = L_0$ and σ induces the identity map on the residue field of L_0. For real $x > 0$ define

$$\Gamma_x = \{\gamma \in \Gamma_0 : v_L(\gamma(\pi_L) - \pi_L) \geq x + 1\}.$$

Then Γ_x does not depend on the choice of uniformizer π_L for L. Observe that $\Gamma_x \subset \Gamma_y$ for $0 \leq y \leq x$, and $\Gamma_x = \{\mathrm{id}_L\}$ for sufficiently large x. We say that Γ_x is the xth subset in the lower ramification filtration of Γ.

Lemma 2.1. *For each $x > 0$, $|\Gamma_x|$ is a power of p.*

Proof. Let M/K be the Galois closure of L/K. Set $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$. Then Γ can be identified with the coset space G/H. Let $x > 0$ and set

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

Then $H \leq G(x) \leq G$ and Γ_x is identified with $G(x)/H$. The lemma now follows from Lagrange's theorem. □

Say that $b > 0$ is a lower ramification number for L/K if $\Gamma_b \neq \Gamma_{b+\epsilon}$ for all $\epsilon > 0$. Say that $b > 0$ is a lower ramification number with multipicity m if $|\Gamma_b|/|\Gamma_{b+\epsilon}| = p^m$ for all sufficiently small $\epsilon > 0$. Let p^t be the ramification index of L/K. Then L/K has t positive lower ramification numbers, counted with multiplicity. The positive lower ramification numbers of L/K can be viewed either as a multiset or as a nondecreasing sequence $b_1 \leq b_2 \leq \cdots \leq b_t$ of rational numbers. To account for the unramified part of L/K we say that -1 is a lower ramification number of L/K with multipicity $n - t$. Thus L/K has a total of n lower ramification numbers, counted with multiplicity.

We define the positive upper ramification numbers of L/K by setting $u_1 = b_1$ and $u_{i+1} = u_i + p^{-i}(b_{i+1} - b_i)$ for $1 \leq i \leq t - 1$. In addition, if $t < n$ we say that -1 is an upper ramification number of L/K with multipicity $n - t$. For $1 \leq i \leq t$ let $\Gamma^{u_i} = \Gamma_{b_i}$, and for real $x \geq 0$ set

$$\Gamma^x = \begin{cases} \Gamma^{u_1} & \text{if } 0 \leq x \leq u_1, \\ \Gamma^{u_j} & \text{if } u_{j-1} < x \leq u_j \text{ for some } 2 \leq j \leq t, \\ \{\mathrm{id}_L\} & \text{if } x > u_t. \end{cases}$$

Let M/K be a subextension of L/K, and let Δ be the set of K-embeddings of M into K^{sep}. We can define ramification subsets Δ_x and Δ^x of Δ, which give us ramification numbers for M/K. For $x > 0$ we have $\Delta^x = \{\gamma|_M : \gamma \in \Gamma^x\}$ (see for instance Theorem 13.15 in [9]). It follows that the multiset of upper ramification numbers of M/K is contained in the multiset of upper ramification numbers of L/K.

Let L/K be a Galois extension of degree p^n and set $G = \mathrm{Gal}(L/K)$. Then G may be identified with the set of K-embeddings of L into K^{sep}, so the definitions given above are valid with Γ replaced by G. In this setting we find that G_x and G^x are normal subgroups of G for all $x \geq 0$. Let $H \trianglelefteq G$ and set $M = L^H$. Then the upper ramification filtration of $\mathrm{Gal}(M/K) \cong G/H$ is given by $(G/H)^x = G^x H/H$ for $x \geq 0$.

We will need the following technical facts about ramification numbers:

Proposition 2.2. *[7, Example 1.2] Let L/K be a totally ramified C_p-extension of local fields with ramification number b, and let $x \in L \smallsetminus \{0\}$. Then $v_L((\sigma-1)x) \geq v_L(x) + b$, with equality if and only if $p \nmid v_L(x)$.*

Proposition 2.3. *Let L/K be a totally ramified Galois extension of degree p^n, with upper ramification numbers $u_1 \leq \cdots \leq u_{n-2} \leq u_{n-1} < u_n$. Set $G = \mathrm{Gal}(L/K)$, and suppose there is $H \leq Z(G)$ such that $H \cong C_p^2$. Let $M = L^H$ be the fixed field of H, and assume that u_n is not an upper ramification number of M/K. Then there is a unique C_p-subextension F_0/M of L/M such that F_0/K has ramification numbers $u_1, \ldots, u_{n-2}, u_{n-1}$. For all other C_p-subextensions F/M of L/M, u_n is an upper ramification number of F/K.*

Proof. Since u_n is not an upper ramification number of M/K we have $G^{u_n}H/H = (G/H)^{u_n} = \{1\}$, and hence $G^{u_n} \leq H$. Let $A \leq H$ be such that $|A| = p$. Then $(G/A)^{u_n+\epsilon} = G^{u_n+\epsilon}A/A$ is necessarily trivial, and $(G/A)^{u_n} = G^{u_n}A/A$ is trivial if and only if $G^{u_n} \leq A$. Since $|G^{u_n}| = p$ it follows that u_n is an upper ramification number of L^A/K if and only if $A \neq G^{u_n}$. Set $F_0 = L^{G^{u_n}}$. Then u_n is not an upper ramification number of F_0/K, so the upper ramification numbers of F_0/K are $u_1, \ldots, u_{n-2}, u_{n-1}$. □

Proposition 2.4. *Let L/K be a totally ramified extension of degree p^n. Let $b_1 \leq \cdots \leq b_n$ be the lower ramification numbers of L/K and let $u_1 \leq \cdots \leq u_n$ be the upper ramification numbers. Then for $1 \leq i \leq n-1$ and $m \geq i$ we have $b_{i+1} - b_i \leq p^m(u_{i+1} - u_i)$.*

Proof. In fact $b_{i+1} - b_i = p^i(u_{i+1} - u_i) \leq p^m(u_{i+1} - u_i)$. □

Corollary 2.5. *Let L/K be a totally ramified extension of degree p^n. Let $b_1 \leq \cdots \leq b_n$ be the lower ramification numbers of L/K and let $u_1 \leq \cdots \leq u_n$ be the upper ramification numbers. Then*

(a) $b_j - b_i \leq p^{j-1}(u_j - u_i)$ for $1 \leq i \leq j \leq n$.
(b) $b_j \leq p^{j-1}u_j$ for $1 \leq j \leq n$, with equality only if $j = 1$.

Proof. (a) The claim is clear when $i = j$. Now assume $1 \leq i < j \leq n$. Proposition 2.4 gives $b_{h+1} - b_h \leq p^{j-1}(u_{h+1} - u_h)$ for $i \leq h \leq j-1$. Thus

$$\begin{aligned} b_j - b_i &= \sum_{h=i}^{j-1} (b_{h+1} - b_h) \\ &\leq \sum_{h=i}^{j-1} p^{j-1}(u_{h+1} - u_h) \\ &= p^{j-1}(u_j - u_i). \end{aligned}$$

(b) This follows from (a) by setting $i = 1$ and noting that $b_1 = u_1$. □

3. Constructing abelian p-extensions

Let K be a local field of characteristic 0 whose residue field has characteristic p. In this section we use Artin-Schreier polynomials and Witt addition polynomials to construct totally ramified abelian p-extensions L/K. The corresponding constructions for local fields of characteristic p are well-known. The results of this section will be used in Sections 4 and 5 to construct Galois extensions whose Galois groups are extraspecial p-groups.

We will make frequent use of the following basic result of MacKenzie and Whaples:

Theorem 3.1. *Let $a \in K$ satisfy $v_K(a) > -pe_K/(p-1)$ and let $\alpha \in K^{sep}$ be a root of $X^p - X - a$ such that $\alpha \notin K$. Then $K(\alpha)/K$ is a cyclic extension of degree p, and there is $\sigma \in \mathrm{Gal}(K(\alpha)/K)$ such that $\sigma(\alpha) \equiv \alpha + 1 \pmod{\mathfrak{M}_K}$.*

Proof. This follows from Theorem 5 of [19]. □

Let $\mathcal{G}_K = \mathrm{Gal}(K^{sep}/K)$ be the absolute Galois group of K and let $\sigma \in \mathcal{G}_K$. It follows from the above that there is $m_0 \in \mathbb{Z}$ such that $(\sigma - 1)\alpha \equiv m_0 \pmod{\mathfrak{M}_K}$. Define m_σ to be the image of m_0 in $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. Then m_σ does not depend on the choice of root α, so we may define $\chi_a^K : \mathcal{G}_K \to \mathbb{F}_p$ by $\chi_a^K(\sigma) = m_\sigma$. Then χ_a^K is a continuous homomorphism.

Define the Artin-Schreier polynomial $\wp(X) \in \mathbb{F}_p[X]$ by $\wp(X) = X^p - X$.

Proposition 3.2. *Let $a \in K$ satisfy $-pe_K/(p-1) < v_K(a) < 0$ and $p \nmid v_K(a)$. Choose $\alpha \in K^{sep}$ such that $\wp(\alpha) = a$ and set $L = K(\alpha)$. Then L/K is a totally ramified C_p-extension with upper and lower ramification number $-v_K(a)$. Set $H = \ker \chi_a^K \leq \mathcal{G}_K$. Then $L = (K^{sep})^H$ is the fixed field of H.*

Proof. Set $\wp(K) = \{\wp(b) : b \in K\}$. Our hypotheses on a imply that $a \notin \wp(K)$, so χ_a^K is nontrivial. Hence by Theorem 3.1, L/K is a C_p-extension and there is $\tau \in \mathrm{Gal}(L/K)$ such that $(\tau - 1)\alpha \equiv 1 \pmod{\mathfrak{M}_L}$. Since p does not divide $v_K(a) = pv_K(\alpha)$ we see that L/K is totally ramified. In addition, it follows from Proposition 2.5 of [13, III] that the ramification number of L/K is $-v_L(\alpha) = -v_K(a)$. It is clear from Galois theory that $L = (K^{sep})^H$. □

The following is proved as Lemma 3.5 in [17]:

Lemma 3.3. *Let $a \in K \smallsetminus \wp(K)$ be such that $u = -v_K(a)$ satisfies $0 < u < pe_K/(p-1)$. Let α be a root of $f(X) = X^p - X - a$ and set $L = K(\alpha)$.*

(a) If L/K is a totally ramified C_p-extension then there is $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha) = \alpha + 1 + \epsilon$ for some $\epsilon \in L$ with $v_K(\epsilon) \geq e_K - (1 - p^{-1})u$.
(b) If $p \nmid u$, then L/K is a totally ramified C_p-extension and $v_K(\epsilon) = e_K - (1 - p^{-1})u$.

Proposition 3.4. *Let L be a local field with residue characteristic p and let $\alpha \in L$ satisfy $v_L(\alpha) = -u$, with $0 < u < e_L/(p-1)$. Let $\beta \in L$ be such that $\wp(\alpha) \equiv \wp(\beta) \pmod{\mathfrak{M}_L}$. Then there is $k \in \mathbb{Z}$ such that $\beta \equiv \alpha + k \pmod{\mathfrak{M}_L}$.*

Proof. Set $\delta = \beta - \alpha$. Then

$$\wp(\beta) - \wp(\alpha) = \delta^p - \delta + \sum_{i=1}^{p-1} \binom{p}{i} \alpha^{p-i} \delta^i. \tag{3.1}$$

If $v_L(\delta) < 0$ then $v_L(\delta^p) < v_L(\binom{p}{i}\alpha^{p-i}\delta^i)$ for $1 \le i \le p-1$ and $v_L(\delta^p) < v_L(\delta)$. This implies $v_L(\wp(\beta) - \wp(\alpha)) = v_L(\delta^p) < 0$, a contradiction. Hence $v_L(\delta) \ge 0$. It now follows from (3.1) and the assumption on $v_L(\alpha)$ that $0 \equiv -\delta + \delta^p \pmod{\mathfrak{M}_L}$. Thus $\delta \equiv k \pmod{\mathfrak{M}_L}$ for some $k \in \mathbb{Z}$. □

We will make frequent use of the following result:

Proposition 3.5. *Let $a, b \in K$ satisfy $v_K(b) \ge v_K(a) > -pe_K/(p-1)$ and $v_K(p^p a^{p-1} b) > 0$. Then*

(a) $\chi^K_{a+b} = \chi^K_a + \chi^K_b$.
(b) For each root α of $X^p - X - a$ and each root β of $X^p - X - b$ there is a unique root γ of $X^p - X - (a+b)$ such that $\gamma \equiv \alpha + \beta \pmod{p\alpha^{p-1}\beta}$. Furthermore, we have $\gamma \in K(\alpha, \beta)$.

Proof. (a) This is proved in Proposition 5 of [19].
(b) By the proof of Proposition 5 in [19] there is a unique root γ of $X^p - X - (a+b)$ such that $\delta := \alpha + \beta - \gamma$ satisfies $v_K(\delta) > 0$. As in the proof of Proposition 3.4 we get

$$\begin{aligned} \delta^p - \delta + \sum_{i=1}^{p-1} \binom{p}{i} \gamma^{p-i} \delta^i &= \wp(\alpha + \beta) - \wp(\gamma) \\ &\equiv \wp(\alpha) + \wp(\beta) - (a+b) \pmod{p\alpha^{p-1}\beta} \\ &\equiv 0 \pmod{p\alpha^{p-1}\beta}. \end{aligned}$$

It follows that $\delta^p - \delta \equiv 0 \pmod{p\alpha^{p-1}\beta}$, and hence that $\delta \equiv 0 \pmod{p\alpha^{p-1}\beta}$. Using (a) we get $\gamma \in K(\alpha, \beta)$. □

Corollary 3.6. *Let $K, a, b, \alpha, \beta, \gamma$ satisfy the conditions of Proposition 3.5. Then for all $\sigma \in \mathrm{Gal}(K(\alpha,\beta)/K)$ we have*

$$(\sigma - 1)(\gamma) \equiv (\sigma - 1)(\alpha) + (\sigma - 1)(\beta) \pmod{p\alpha^{p-1}}.$$

Proof. By Lemma 3.3 there are $k, \ell, m \in \mathbb{Z}$ such that

$$\begin{aligned}(\sigma-1)(\alpha) &\equiv k \pmod{p\alpha^{p-1}}\\ (\sigma-1)(\beta) &\equiv \ell \pmod{p\beta^{p-1}}\\ (\sigma-1)(\gamma) &\equiv m \pmod{p\gamma^{p-1}}.\end{aligned}$$

Since $\chi^K_{a+b}(\sigma) = \chi^K_a(\sigma) + \chi^K_b(\sigma)$ we have $m \equiv k+\ell \pmod p$. Since $v_K(\alpha) \le v_K(\beta)$ and $v_K(\alpha) \le v_K(\gamma)$, the corollary follows from this. □

Corollary 3.7. *Let $a, a' \in K$ satisfy $v_K(a) > -pe_K/(p-1)$ and $a \equiv a' \pmod{\mathfrak{M}_K}$. Then*

(a) $\chi^K_a = \chi^K_{a'}$.
(b) For each root α of $X^p - X - a$ there is a root α' of $X^p - X - a'$ such that $v_K(\alpha - \alpha') > 0$. Furthermore, we have $K(\alpha') = K(\alpha)$.

Proof. We have $a' = a + b$ with $v_K(b) > 0$. Since χ_b is the trivial character, the corollary follows. □

Proposition 3.8. *Let $0 < u < e_K$ be coprime to p. Choose $a_1, \dots, a_r \in \mathfrak{M}_K^{-u}$ such that*

$$\overline{S} = \{a_i + \mathfrak{M}_K^{-u+1} : 1 \le i \le r\}$$

is an $\mathbb{F}_p$-linearly independent subset of $\mathfrak{M}_K^{-u}/\mathfrak{M}_K^{-u+1}$. For $1 \le i \le r$ let $\alpha_i \in K^{sep}$ be a root of $X^p - X - a_i$. Then $L = K(\alpha_1, \dots, \alpha_r)$ is an elementary abelian p-extension of K of rank r, with a single upper and lower ramification number u of multiplicity r.

Proof. It follows from Proposition 3.2 that L/K is an elementary abelian p-extension of degree p^s for some $s \le r$. Let $n_1, \dots, n_r \in \mathbb{Z}$ and set $b = n_1 a_1 + \cdots + n_r a_r$. Then $\chi^K_b = n_1\chi^K_{a_1} + \cdots + n_r\chi^K_{a_r}$ by Proposition 3.5(a) and the bound on u. Therefore χ^K_b induces a character from $\mathrm{Gal}(L/K)$ to $\mathbb{F}_p$. If $n_1', \dots, n_r'$ are integers such that $b' = n_1'a_1 + \cdots + n_r'a_r$ satisfies $\chi^K_{b'} = \chi^K_b$ then $\chi^K_{b'-b}$ is trivial. Hence $b' \equiv b \pmod{\mathfrak{M}_K^{-u}}$, so by the independence of $\overline{S}$ we get $n_i' \equiv n_i \pmod p$ for $1 \le i \le r$. It follows that there are p^r distinct characters from $\mathrm{Gal}(L/K)$ to $\mathbb{F}_p$, so we must have $[L:K] = p^r$. If χ^K_b is nontrivial then $p \nmid n_i$ for at least one i, so $v_K(b) = -u$ by the independence of $\overline{S}$. Hence the C_p-subextension of L/K corresponding to χ^K_b has upper ramification number u. Therefore the only upper ramification number of L/K is u, which has multiplicity r. It follows that the only lower ramification number of L/K is u, again with multiplicity r. □

Motivated by these results we make the following definition:

Definition 3.9. Let K be a local field with residue characteristic p. We say $a_1, \dots, a_n \in K$ are reduced Artin-Schreier constants if all of the following hold:

(i) $-pe_K/(p-1) < v_K(a_n) \leq \cdots \leq v_K(a_1) < 0$.
(ii) $p \nmid v_K(a_i)$ for each $1 \leq i \leq n$.
(iii) If $v_K(a_i) = v_K(a_{i+1}) = \cdots = v_K(a_j) = -u$ then $\{a_h + \mathfrak{M}_K^{-u+1} : i \leq h \leq j\}$ is an $\mathbb{F}_p$-linearly independent subset of $\mathfrak{M}_K^{-u}/\mathfrak{M}_K^{-u+1}$.
(iv) $v_K\left(p^p a_n^{p-1} a_{n-1}\right) > 0$.

Proposition 3.10. *Let $a_1, \ldots, a_n \in K$ be reduced Artin-Schreier constants. For $1 \leq i \leq n$ set $u_i = -v_K(a_i)$ and let $\alpha_i \in K^{sep}$ be a root of $X^p - X - a_i$. Set $L = K(\alpha_1, \ldots, \alpha_n)$. Then L/K is a totally ramified C_p^n-extension with upper ramification numbers $u_1 \leq \cdots \leq u_n$.*

Proof. Let $v_1 < \cdots < v_t$ be the distinct elements of the multiset $\{u_i : 1 \leq i \leq n\}$ and let m_j be the multiplicity of v_j. It follows from Proposition 3.8 that L/K is an elementary abelian p-extension. Furthermore, for $1 \leq j \leq t$, L/K has a subextension L_j/K whose only upper ramification number is v_j, with multiplicity m_j. It follows that $L_1 L_2 \ldots L_t/K$ has upper ramification numbers $v_1, \ldots, v_t$ with multiplicities $m_1, \ldots, m_t$. Since $m_1 + \cdots + m_t = n$ we get $L = L_1 L_2 \ldots L_t$ and $[L : K] = p^n$. □

Remark 3.11. Let L/K be a totally ramified C_p^n-extension with upper ramification numbers $u_1 \leq \cdots \leq u_n$. Then L/K can be constructed using Proposition 3.10 if and only if $p^{-1}u_{n-1} + (1 - p^{-1})u_n < e_K$. This illustrates a general principle about our methods for constructing Galois extensions in characteristic 0: The absolute ramification index e_K of K must be large compared to the upper ramification numbers. This makes our characteristic 0 extensions behave like extensions in characteristic p.

Let $L = K(\alpha_1, \ldots, \alpha_n)$ as in Proposition 3.10. It follows from Lemma 3.3 that for each $1 \leq i \leq n$ there is $\gamma_i \in \mathrm{Gal}(K(\alpha_i)/K)$ such that $\gamma_i(\alpha_i) = \alpha_i + 1 + \delta_i$, where $v_K(\delta_i) = v_K(p\alpha_i^{p-1}) > 0$. We can extend γ_i to an automorphism of L by setting

$$\gamma_i(\alpha_j) = \begin{cases} \alpha_j & \text{if } j \neq i, \\ \alpha_i + 1 + \delta_i & \text{if } j = i. \end{cases} \tag{3.2}$$

Define

$$D(X, Y) = \frac{X^p + Y^p - (X+Y)^p}{p} = -\sum_{i=1}^{p-1} p^{-1} \binom{p}{i} X^i Y^{p-i}.$$

Then $D(X, Y) \in \mathbb{Z}[X, Y]$ and

$$S_1(X_0, X_1, Y_0, Y_1) = X_1 + Y_1 + D(X_0, Y_0)$$

is the second Witt addition polynomial.

Proposition 3.12. *Let $a_1, a_2 \in K$ and set $u_i = -v_K(a_i)$ for $i = 1, 2$. Assume that $p \nmid u_1$, $(p-p^{-1})u_1 < e_K$, and $(1-p^{-1}+p^{-2})u_1 + (1-p^{-1})u_2 < e_K$. Let $\alpha_1, \alpha_2 \in K^{sep}$ satisfy $\alpha_1^p - \alpha_1 = a_1$ and $\alpha_2^p - \alpha_2 = D(\alpha_1, a_1) + a_2$. Set $E = K(\alpha_1, \alpha_2)$. Then*

(a) E/K is a C_{p^2}-extension.
(b) If $u_2 > pu_1$ and $p \nmid u_2$ then the upper ramification numbers of E/K are u_1, u_2.
(c) If $u_2 > (p+1-p^{-1})u_1$ and $p \nmid u_2$ then there is a generator θ for $\mathrm{Gal}(E/K)$ such that $\theta(\alpha_1) \equiv \alpha_1 + 1 \pmod{p\alpha_1^{p-1}}$ and $\theta(\alpha_2) \equiv \alpha_2 + D(1, \alpha_1) \pmod{\mathfrak{M}_E}$.

Proof. For (a) see the remark in Section 3 of [22], or Theorem 2.1 in [17]. For (b) see Proposition 3.4 in [17], and for (c) see Proposition 3.6 in [17]. Propositions 3.4 and 3.6 in [17] are proved under the hypothesis that $a_2 = a_1\mu^p$ for some $\mu \in K^\times$. However, the proofs given in [17] remain valid with this hypothesis replaced by the assumption $p \nmid u_2$. □

4. Generalized Heisenberg extensions

There are two families of extraspecial p-groups: The generalized Heisenberg groups, which have exponent p, and the generalized metacyclic groups, which have exponent p^2. In this section we define the generalized Heisenberg group $H(n)$ of order p^{2n+1}. We then show how to construct totally ramified $H(n)$-extensions of local fields with residue characteristic p. In Section 5 we will define the generalized metacyclic groups $M(n)$ and construct totally ramified $M(n)$-extensions. In Section 9 we will use the results of this section to construct generalized Heisenberg extensions which have a Galois scaffold.

Definition 4.1. Let p be an odd prime. For $n \geq 1$ we define a group $H(n)$ of order p^{2n+1} generated by $g_1, \ldots, g_{2n}, g_{2n+1}$, with $|g_i| = p$ for $1 \leq i \leq 2n+1$. All these generators commute with each other, except for g_i and g_{n+i}, which satisfy $[g_i, g_{n+i}] = g_{2n+1}$ for $1 \leq i \leq n$. Thus $H(1)$ is the Heisenberg p-group and $H(n)$ is an extraspecial p-group with exponent p.

Proposition 4.2. *Let K_0 be a local field with residue characteristic $p > 2$. Let $a_1, \ldots, a_{2n}, a_{2n+1}$ be elements of K_0 such that $a_1, \ldots, a_{2n}$ are reduced Artin-Schreier constants. Set $u_i = -v_0(a_i)$ for $1 \leq i \leq 2n+1$ and assume that*

$$u_n + (1-p^{-1})u_{2n} < e_0, \tag{4.1}$$

$$p^{-1}u_n + p^{-2}u_{2n} + (1-p^{-1})u_{2n+1} < e_0. \tag{4.2}$$

For $1 \leq i \leq 2n$ let α_i satisfy $\alpha_i^p - \alpha_i = a_i$ and define $K_1, \ldots, K_{2n}$ recursively by $K_i = K_{i-1}(\alpha_i)$. Set

$$B = a_1\alpha_{n+1} + a_2\alpha_{n+2} + \cdots + a_n\alpha_{2n},$$

let α_{2n+1} *satisfy* $\alpha_{2n+1}^p - \alpha_{2n+1} = B + a_{2n+1}$, *and define* $K_{2n+1} = K_{2n}(\alpha_{2n+1})$. *Then*

(a) K_{2n+1}/K_0 *is a totally ramified* $H(n)$*-extension. In addition, for* $1 \le i \le 2n+1$ *there are* $\sigma_i \in \mathrm{Gal}(K_{2n+1}/K_{i-1})$ *such that* $\sigma_i|_{K_i}$ *generates* $\mathrm{Gal}(K_i/K_{i-1})$*, with the following properties:*

$$\sigma_i(\alpha_j) = \alpha_j \qquad \text{for } 1 \le i < j \le 2n, \tag{4.3}$$

$$\sigma_i(\alpha_i) \equiv \alpha_i + 1 \pmod{p\alpha_i^{p-1}} \qquad \text{for } 1 \le i \le 2n+1, \tag{4.4}$$

$$\sigma_i(\alpha_{2n+1}) = \alpha_{2n+1} \qquad \text{for } 1 \le i \le n, \tag{4.5}$$

$$\sigma_{n+i}(\alpha_{2n+1}) \equiv \alpha_{2n+1} + \alpha_i \pmod{\mathfrak{M}_{2n+1}} \qquad \text{for } 1 \le i \le n, . \tag{4.6}$$

(b) If $u_{2n+1} \le u_n + u_{2n}$ *then there is* $v \le u_n + u_{2n}$ *such that the upper ramification numbers of* K_{2n+1}/K_0 *are* $u_1, \dots, u_{2n}, v$ *(but not necessarily in that order).*

(c) Suppose $u_{2n+1} > u_n + u_{2n}$ *and* $p \nmid u_{2n+1}$*. Then the upper ramification numbers of* K_{2n+1}/K_0 *are* $u_1 \le \cdots \le u_{2n} < u_{2n+1}$*, and* $v_0(\alpha_i) = -p^{-1}u_i$ *for* $1 \le i \le 2n+1$.

Proof. (a) It follows from Proposition 3.10 that K_{2n}/K_0 is a totally ramified C_p^{2n}-extension with upper ramification numbers $u_1, \dots, u_{2n}$. For $1 \le i \le 2n$ let γ_i be the element of $\mathrm{Gal}(K_{2n}/K_0)$ defined by (3.2). Let $1 \le i \le n$. Then $\gamma_i(B+a_{2n+1}) = B+a_{2n+1}$, and by Lemma 3.3 we have

$$\begin{aligned} \gamma_{n+i}(B + a_{2n+1}) - (B + a_{2n+1}) &= a_i(\gamma_{n+i}(\alpha_{n+i}) - \alpha_{n+i}) \\ &\equiv a_i \pmod{pa_i\alpha_{n+i}^{p-1}}. \end{aligned} \tag{4.7}$$

Hence by (4.1) we get

$$\gamma_{n+i}(B + a_{2n+1}) \equiv B + a_{2n+1} + a_i \pmod{\mathfrak{M}_{2n}}. \tag{4.8}$$

Suppose $K_{2n+1} = K_{2n}$, so that $\alpha_{2n+1} \in K_{2n}$. Then for $1 \le i \le n$,

$$\wp(\gamma_i(\alpha_{2n+1})) = \gamma_i(\wp(\alpha_{2n+1})) = \gamma_i(B + a_{2n+1}) = B + a_{2n+1} = \wp(\alpha_{2n+1}).$$

In addition, we have

$$\begin{aligned} v_0(B + a_{2n+1}) &\ge \min\{v_0(B), v_0(a_{2n+1})\} \\ &\ge \min\{-u_n - p^{-1}u_{2n}, -u_{2n+1}\} \\ v_0(\alpha_{2n+1}) &\ge \min\{p^{-1}v_0(B + a_{2n+1}), 0\} \\ &\ge \min\{-p^{-1}u_n - p^{-2}u_{2n}, -p^{-1}u_{2n+1}\}. \end{aligned} \tag{4.9}$$

Hence by (4.8), (4.1), and (4.2) we get

$$\begin{aligned}\wp(\gamma_{n+i}(\alpha_{2n+1})) &= \gamma_{n+i}(B + a_{2n+1}) \\ &\equiv B + a_{2n+1} + a_i \pmod{\mathfrak{M}_{2n}} \\ &\equiv \wp(\alpha_{2n+1}) + \wp(\alpha_i) \pmod{\mathfrak{M}_{2n}} \\ &\equiv \wp(\alpha_{2n+1} + \alpha_i) \pmod{\mathfrak{M}_{2n}}.\end{aligned}$$

Therefore by Proposition 3.4 there are $k, \ell \in \mathbb{Z}$ such that

$$\begin{aligned}\gamma_i(\alpha_{2n+1}) &\equiv \alpha_{2n+1} + k \pmod{\mathfrak{M}_{2n}} \\ \gamma_{n+i}(\alpha_{2n+1}) &\equiv \alpha_{2n+1} + \alpha_i + \ell \pmod{\mathfrak{M}_{2n}}.\end{aligned}$$

It follows that

$$\begin{aligned}\gamma_i\gamma_{n+i}(\alpha_{2n+1}) &\equiv \gamma_i(\alpha_{2n+1} + \alpha_i + \ell) \pmod{\mathfrak{M}_{2n}} \\ &\equiv \alpha_{2n+1} + k + \alpha_i + 1 + \ell \pmod{\mathfrak{M}_{2n}} \\ \gamma_{n+i}\gamma_i(\alpha_{2n+1}) &\equiv \gamma_{n+i}(\alpha_{2n+1} + k) \pmod{\mathfrak{M}_{2n}} \\ &\equiv \alpha_{2n+1} + \alpha_i + \ell + k \pmod{\mathfrak{M}_{2n}}.\end{aligned}$$

Since $\gamma_i\gamma_{n+i} = \gamma_{n+i}\gamma_i$ this is a contradiction. Therefore $K_{2n+1} \neq K_{2n}$. It follows from (4.9), (4.1), and (4.2) that $v_0(B + a_{2n+1}) > -pe_0/(p-1)$. Hence by Theorem 3.1, $K_{2n}(\alpha_{2n+1})/K_{2n}$ is a C_p-extension and there exists $\sigma_{2n+1} \in \mathrm{Gal}(K_{2n+1}/K_{2n})$ such that

$$\sigma_{2n+1}(\alpha_{2n+1}) - \alpha_{2n+1} \equiv 1 \pmod{\mathfrak{M}_{2n+1}}. \tag{4.10}$$

Let $1 \leq i \leq n$. By (4.1), (4.2), and Proposition 3.5(b), $X^p - X - (B + a_{2n+1} + a_i)$ has a root $\delta \in K_{2n+1}$ such that $\delta \equiv \alpha_{2n+1} + \alpha_i \pmod{\mathfrak{M}_{2n+1}}$. Hence by (4.8) and Corollary 3.7(b), $X^p - X - \gamma_{n+i}(B + a_{2n+1})$ has a root $\alpha'_{2n+1} \in K_{2n+1}$ such that $\alpha'_{2n+1} \equiv \alpha_{2n+1} + \alpha_i \pmod{\mathfrak{M}_{2n+1}}$. Therefore we may extend γ_{n+i} to $\sigma_{n+i} \in \mathrm{Aut}(K_{2n+1})$ by setting $\sigma_{n+i}(\alpha_{2n+1}) = \alpha'_{2n+1}$. For $1 \leq i \leq n$ we have $\gamma_i(B + a_{2n+1}) = B + a_{2n+1}$, so we may extend γ_i to $\sigma_i \in \mathrm{Aut}(K_{2n+1})$ by setting $\sigma_i(\alpha_{2n+1}) = \alpha_{2n+1}$. Hence K_{2n+1}/K_0 is a Galois extension.

Statements (4.3), (4.5), and (4.6) follow directly from the definitions of σ_i and σ_{n+i}, while (4.4) follows from the definitions and Lemma 3.3. Since K_{2n}/K_0 is an elementary abelian p-extension we have $[\sigma_i, \sigma_j] \in \mathrm{Gal}(K_{2n+1}/K_{2n})$ and $\sigma_i^p \in \mathrm{Gal}(K_{2n+1}/K_{2n})$ for $1 \leq i, j \leq 2n+1$. By considering how these elements act on α_{2n+1} we easily find that $\sigma_i^p = 1$ for $1 \leq i \leq 2n+1$, and $[\sigma_i, \sigma_j] = 1$ for $1 \leq i \leq j \leq 2n+1$ unless $1 \leq i \leq n$ and $j = n + i$. For instance, if $1 \leq i < j \leq n$ then

$$\begin{aligned}[\sigma_{n+i}, \sigma_{n+j}](\alpha_{2n+1}) &= \sigma_{n+i}\sigma_{n+j}\sigma_{n+i}^{-1}\sigma_{n+j}^{-1}(\alpha_{2n+1}) \\ &\equiv \sigma_{n+i}\sigma_{n+j}\sigma_{n+i}^{-1}(\alpha_{2n+1} - \alpha_j) \pmod{\mathfrak{M}_{2n+1}} \\ &\equiv \sigma_{n+i}\sigma_{n+j}(\alpha_{2n+1} - \alpha_i - \alpha_j) \pmod{\mathfrak{M}_{2n+1}}\end{aligned}$$

$$\begin{aligned} &\equiv \sigma_{n+i}(\alpha_{2n+1} - \alpha_i) && (\mathrm{mod}\ \mathfrak{M}_{2n+1}) \\ &\equiv \alpha_{2n+1} && (\mathrm{mod}\ \mathfrak{M}_{2n+1}). \end{aligned}$$

Hence $[\sigma_{n+i}, \sigma_{n+j}](\alpha_{2n+1}) = \alpha_{2n+1}$, so $[\sigma_{n+i}, \sigma_{n+j}] = 1$. On the other hand, using (4.10) we get

$$\begin{aligned} [\sigma_i, \sigma_{n+i}](\alpha_{2n+1}) &= \sigma_i \sigma_{n+i} \sigma_i^{-1} \sigma_{n+i}^{-1}(\alpha_{2n+1}) \\ &\equiv \sigma_i \sigma_{n+i} \sigma_i^{-1}(\alpha_{2n+1} - \alpha_i) && (\mathrm{mod}\ \mathfrak{M}_{2n+1}) \\ &\equiv \sigma_i \sigma_{n+i}(\alpha_{2n+1} - \alpha_i + 1) && (\mathrm{mod}\ \mathfrak{M}_{2n+1}) \\ &\equiv \sigma_i(\alpha_{2n+1} + 1) && (\mathrm{mod}\ \mathfrak{M}_{2n+1}) \\ &\equiv \alpha_{2n+1} + 1 && (\mathrm{mod}\ \mathfrak{M}_{2n+1}) \\ &\equiv \sigma_{2n+1}(\alpha_{2n+1}) && (\mathrm{mod}\ \mathfrak{M}_{2n+1}). \end{aligned}$$

Therefore $[\sigma_i, \sigma_{n+i}] = \sigma_{2n+1}$ for $1 \le i \le n$. We conclude that $\mathrm{Gal}(K_{2n+1}/K_0) \cong H(n)$.
(b) For $1 \le i \le n$ let $L_{(i)}$ be the extension of $K_0(\alpha_i, \alpha_{n+i})$ generated by the roots of $X^p - X - a_i\alpha_{n+i}$. It follows from (a) that $L_{(i)}/K_0$ is an $H(1)$-extension. Let $M_{(i)}$ be the extension of $K_0(\alpha_{n+i})$ generated by the roots of $X^p - X - a_i\alpha_{n+i}$. Then $M_{(i)}/K_0(\alpha_{n+i})$ is a C_p-extension with ramification number $-v_1(a_i\alpha_{n+i}) = pu_i + u_{n+i}$. Since $K_0(\alpha_{n+i})/K_0$ is a C_p-extension with ramification number u_{n+i}, $M_{(i)}/K_0$ is an extension of degree p^2 with lower ramification numbers $u_{n+i}, pu_i + u_{n+i}$. Hence the upper ramification numbers of $M_{(i)}/K_0$ are $u_{n+i}, u_i + u_{n+i}$. Since $M_{(i)}/K_0$ is a subextension of $L_{(i)}/K_0$, these are also upper ramification numbers of $L_{(i)}/K_0$. Since $K_0(\alpha_i, \alpha_{n+i})/K_0$ is a subextension of $L_{(i)}/K_0$, the upper ramification numbers u_i, u_{n+i} of $K_0(\alpha_i, \alpha_{n+i})/K_0$ are also upper ramification numbers of $L_{(i)}/K_0$. It follows that the upper ramification numbers of $L_{(i)}/K_0$ are $u_i, u_{n+i}, u_i + u_{n+i}$.

Set $L = L_{(1)}L_{(2)} \dots L_{(n)}$. Then $K_{2n} \subset L$. Let $\beta \in K_0^{sep}$ be a root of $X^p - X - a_{2n+1}$. Then $L(\beta)/K_0$ is a compositum of Galois p-extensions, so $L(\beta)/K_0$ is a Galois p-extension. Set $G = \mathrm{Gal}(L(\beta)/K_0)$ and $N_{(i)} = \mathrm{Gal}(L(\beta)/L_{(i)})$ for $1 \le i \le n$. Then $N_{(i)} \trianglelefteq G$ and $\mathrm{Gal}(L_{(i)}/K_0) \cong G/N_{(i)}$. For $x > u_i + u_{n+i}$ we have $G^x N_{(i)}/N_{(i)} = (G/N_{(i)})^x = \{1\}$, and hence $G^x \le N_{(i)}$. Set $H = \mathrm{Gal}(L(\beta)/K_0(\beta))$; then $H \trianglelefteq G$ and $\mathrm{Gal}(K_0(\beta)/K_0) \cong G/H$. For $x > u_n + u_{2n} \ge u_{2n+1}$ we get $G^x H/H = (G/H)^x = \{1\}$, and hence $G^x \le H$. Since $N_{(1)} \cap \dots \cap N_{(n)} \cap H = \{1\}$, it follows that $G^x = \{1\}$ for all $x > u_n + u_{2n}$. Therefore the upper ramification numbers of $L(\beta)/K_0$ are all $\le u_n + u_{2n}$. By (4.1), (4.2), and Proposition 3.5(a) we have

$$\chi_{B+a_{2n+1}}^{K_{2n}} = \chi_{a_1\alpha_{n+1}}^{K_{2n}} + \dots + \chi_{a_n\alpha_{2n}}^{K_{2n}} + \chi_{a_{2n+1}}^{K_{2n}}.$$

Hence $K_{2n+1} \subset L(\beta)$, so the upper ramification numbers of K_{2n+1}/K_0 are bounded above by $u_n + u_{2n}$. Since the subextension K_{2n}/K_0 of K_{2n+1}/K_0 has upper ramification numbers $u_1, \dots, u_{2n}$, we conclude that there is $v \le u_n + u_{2n}$ such that the upper ramification numbers of K_{2n+1}/K_0 are $u_1, \dots, u_{2n}, v$.

(c) Let $\widetilde{K}_{2n+1}$ be the extension of K_{2n} generated by the roots of $X^p - X - B$. Then by (a) and (b) $\widetilde{K}_{2n+1}/K_0$ is an $H(n)$-extension whose upper ramification numbers are $u_1, \dots, u_{2n}, v$ for some $v \leq u_n + u_{2n}$. Once again let $\beta \in K_0^{sep}$ be a root of $X^p - X - a_{2n+1}$. Since $p \nmid u_{2n+1}$ we see that u_{2n+1} is an upper ramification number of $K_0(\beta)/K_0$, and hence also of $\widetilde{K}_{2n+1}(\beta)/K_0$. Since $u_{2n+1} > u_n + u_{2n}$, u_{2n+1} is not an upper ramification number of $\widetilde{K}_{2n+1}/K_0$. Therefore $\widetilde{K}_{2n+1}(\beta) \neq \widetilde{K}_{2n+1}$ and $\widetilde{K}_{2n+1}(\beta)/K_{2n}$ is a C_p^2-extension. By (4.2) and Proposition 3.5(a) we have $\chi_{B+a_{2n+1}}^{K_{2n}} = \chi_B^{K_{2n}} + \chi_{a_{2n+1}}^{K_{2n}}$. Hence $K_{2n+1} \subset \widetilde{K}_{2n+1}(\beta)$ and $K_{2n+1} \neq \widetilde{K}_{2n+1}$. The upper ramification numbers of the elementary abelian p-extension $K_{2n}(\beta)/K_0$ are $u_1, \dots, u_{2n}, u_{2n+1}$. Since $u_{2n+1} > u_n + u_{2n} \geq v$, the upper ramification numbers of $\widetilde{K}_{2n+1}(\beta)/K_0$ are $u_1, \dots, u_{2n}, u_{2n+1}, v$. Using Proposition 2.3 we deduce that the upper ramification numbers of K_{2n+1}/K_0 are $u_1, \dots, u_{2n}, u_{2n+1}$. We clearly have $v_0(\alpha_i) = p^{-1}v_0(a_i) = -p^{-1}u_i$ for $1 \leq i \leq 2n$. Since $u_{2n+1} > u_n + u_{2n}$ we also have

$$v_0(\alpha_{2n+1}) = p^{-1}v_0(B + a_{2n+1}) = p^{-1}v_0(a_{2n+1}) = -p^{-1}u_{2n+1}. \quad \square$$

5. Generalized metacyclic extensions

In this section we define the generalized metacyclic group $M(n)$ of order p^{2n+1}. We then show how to construct totally ramified $M(n)$-extensions of local fields with residue characteristic p. In Section 9 we will use these results to construct generalized metacyclic extensions with a Galois scaffold.

Definition 5.1. Let p be an odd prime. For $n \geq 1$ we define a group $M(n)$ of order p^{2n+1} generated by $h_1, \dots, h_{2n}, h_{2n+1}$, with $h_1^p = h_{2n+1}$ and $|h_i| = p$ for $2 \leq i \leq 2n+1$. All these generators commute with each other, except for h_i and h_{n+i}, which satisfy $[h_i, h_{n+i}] = h_{2n+1}$ for $1 \leq i \leq n$. Thus $M(1)$ is the metacyclic group of order p^3 and $M(n)$ is an extraspecial p-group with exponent p^2.

Proposition 5.2. *Let K_0 be a local field with residue characteristic $p > 2$ and let $a_1, a_2, \dots, a_{2n}, a_{2n+1} \in K_0$. For $1 \leq i \leq 2n+1$ set $u_i = -v_0(a_i)$. Assume that $a_1, a_2, \dots, a_{2n}$ are reduced Artin-Schreier constants, $p \nmid u_{2n+1}$, and*

$$u_n + (1 - p^{-1})u_{2n} < e_0 \tag{5.1}$$

$$p^{-1}u_n + p^{-2}u_{2n} + (1 - p^{-1})u_{2n+1} < e_0 \tag{5.2}$$

$$(1 - p^{-1} + p^{-2})u_1 + (1 - p^{-1})u_{2n+1} < e_0 \tag{5.3}$$

$$(p + 1 - p^{-1})u_1 < u_{2n+1} \tag{5.4}$$

$$u_n + u_{2n} < u_{2n+1}. \tag{5.5}$$

For $1 \leq i \leq 2n$ let α_i satisfy $\alpha_i^p - \alpha_i = a_i$. Set

$$B = a_1\alpha_{n+1} + a_2\alpha_{n+2} + \cdots + a_n\alpha_{2n}$$

$$C = D(\alpha_1, a_1) = -\sum_{i=1}^{p-1} p^{-1}\binom{p}{i}\alpha_1^i a_1^{p-i}$$

and let $\widehat{\alpha}_{2n+1} \in K_0^{sep}$ *satisfy* $\widehat{\alpha}_{2n+1}^p - \widehat{\alpha}_{2n+1} = B + C + a_{2n+1}$. *Define* $K_1, \dots, K_{2n}$ *recursively by* $K_i = K_{i-1}(\alpha_i)$ *for* $1 \le i \le 2n$, *and set* $\widehat{K}_{2n+1} = K_{2n}(\widehat{\alpha}_{2n+1})$. *Then*

(a) $\widehat{K}_{2n+1}/K_0$ *is a totally ramified extension with upper ramification numbers* $u_1 \le \cdots \le u_{2n} \le u_{2n+1}$. *Furthermore, we have* $v_0(\alpha_i) = -p^{-1}u_i$ *for* $1 \le i \le 2n+1$.
(b) $\widehat{K}_{2n+1}/K_0$ *is a Galois extension with Galois group* $M(n)$.
(c) For $1 \le i \le 2n+1$ *there are* $\widehat{\sigma}_i \in \mathrm{Gal}(\widehat{K}_{2n+1}/K_{i-1})$ *such that* $\widehat{\sigma}_i|_{K_i}$ *generates* $\mathrm{Gal}(K_i/K_{i-1})$ *for* $1 \le i \le 2n$ *and* $\widehat{\sigma}_{2n+1}$ *generates* $\mathrm{Gal}(\widehat{K}_{2n+1}/K_{2n})$, *with the following properties:*

$$\widehat{\sigma}_i(\alpha_j) = \alpha_j \qquad \text{for } 1 \le i < j \le 2n, \tag{5.6}$$

$$\widehat{\sigma}_i(\alpha_i) \equiv \alpha_i + 1 \pmod{p\alpha_i^{p-1}} \qquad \text{for } 1 \le i \le 2n, \tag{5.7}$$

$$\widehat{\sigma}_1(\widehat{\alpha}_{2n+1}) \equiv \widehat{\alpha}_{2n+1} \pmod{\alpha_1^{p-1}}, \tag{5.8}$$

$$\widehat{\sigma}_i(\widehat{\alpha}_{2n+1}) = \widehat{\alpha}_{2n+1} \qquad \text{for } 2 \le i \le n, \tag{5.9}$$

$$\widehat{\sigma}_{n+i}(\widehat{\alpha}_{2n+1}) \equiv \widehat{\alpha}_{2n+1} \pmod{\alpha_i} \qquad \text{for } 1 \le i \le n, \tag{5.10}$$

$$\widehat{\sigma}_{2n+1}(\widehat{\alpha}_{2n+1}) \equiv \widehat{\alpha}_{2n+1} + 1 \pmod{p\widehat{\alpha}_{2n+1}^{p-1}}. \tag{5.11}$$

Remark 5.3. Note that hypothesis (5.1) is the same as (4.1), (5.2) is the same as (4.2), and (5.5) is one of the hypotheses of Proposition 4.2(c). Also, (5.3) and (5.4) are hypotheses of Proposition 3.12, with u_2 replaced by u_{2n+1}. Inequalities (5.1)–(5.3) say that e_0 is large compared with $u_1, u_2, \dots, u_{2n+1}$ (cf. Remark 3.11), and (5.4)–(5.5) say that u_{2n+1} is large compared with $u_1, u_2, \dots, u_{2n}$.

Proof of Proposition 5.2. (a) Let K_{2n+1} be the extension of K_{2n} generated by the roots of $X^p - X - B$. Thanks to assumptions (5.1) and (5.2) we can apply Proposition 4.2(b), which says that K_{2n+1}/K_0 is an $H(n)$-extension whose upper ramification numbers are $u_1, \dots, u_{2n}, v$ for some $v \le u_n + u_{2n}$. Let E be the extension of K_1 generated by the roots of $X^p - X - (C + a_{2n+1})$. Then by (5.3), (5.4), and Proposition 3.12, E/K_0 is a C_{p^2}-extension with upper ramification numbers u_1, u_{2n+1}. Furthermore, $K_{2n+1} \cap E = K_1$ and $K_{2n+1}E$ is a C_p^2-extension of K_{2n}. Using (5.4), (5.5), (5.2), and Proposition 3.5(a) we get $\chi_{B+C+a_{2n+1}}^{K_{2n}} = \chi_B^{K_{2n}} + \chi_{C+a_{2n+1}}^{K_{2n}}$, and hence $\widehat{K}_{2n+1} \subset K_{2n+1}E$ (see Fig. 1). Therefore by (5.5) and Proposition 2.3 the upper ramification numbers of $\widehat{K}_{2n+1}/K_0$ are $u_1, \dots, u_{2n}, u_{2n+1}$. We clearly have $v_0(\alpha_i) = p^{-1}v_0(a_i) = -p^{-1}u_i$ for $1 \le i \le 2n$. It follows from (5.4) and (5.5) that $v_0(B + C + a_{2n+1}) = v_0(a_{2n+1}) = -u_{2n+1}$. Therefore $v_0(\alpha_{2n+1}) = -p^{-1}u_{2n+1}$.

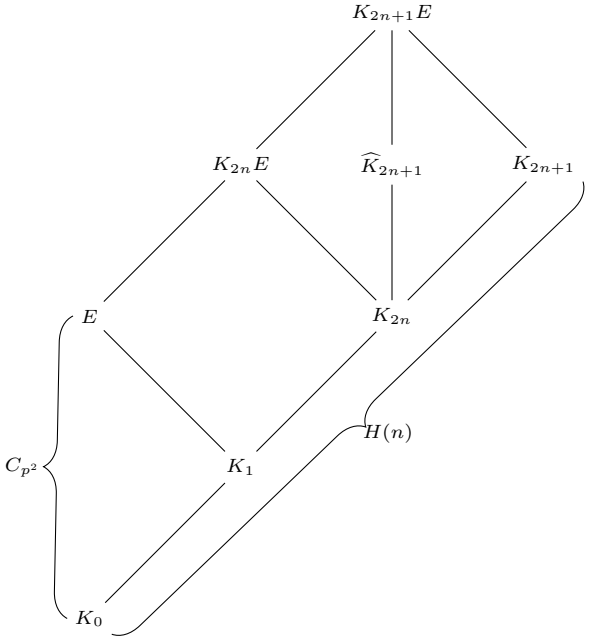

Fig. 1. Field diagram for Proposition 5.2.

(b) Recall the generators $g_1, \dots, g_{2n+1}$ for $H(n)$ given in Definition 4.1, and write $C_{p^2} = \langle k \rangle$. Then

$$\begin{aligned}\mathrm{Gal}(K_{2n+1}E/K_0) &\cong \{(\alpha,\beta) \in \mathrm{Gal}(K_{2n+1}/K_0) \times \mathrm{Gal}(E/K_0) : \alpha|_{K_1} = \beta|_{K_1}\} \\ &\cong \{(g_1^{r_1} g_2^{r_2} \dots g_{2n+1}^{r_{2n+1}}, k^s) \in H(n) \times C_{p^2} : r_1 \equiv s \pmod p\}.\end{aligned}$$

Let $N = \mathrm{Gal}(K_{2n+1}E/\widehat{K}_{2n+1})$. Then the isomorphism above maps N to $\langle (g_{2n+1}^v, k^{-p}) \rangle$ for some $1 \le v \le p-1$. Let $1 \le w \le p-1$ be such that $vw \equiv 1 \pmod p$. Then there is an onto homomorphism $\phi : \mathrm{Gal}(K_{2n+1}E/K_0) \to M(n)$ defined by $\phi(g_1, k) = h_1^v$, $\phi(g_{n+1}, 1) = h_{n+1}^w$, and $\phi(g_i, 1) = h_i$ for $2 \le i \le n$ and $n+2 \le i \le 2n+1$. Since $\ker(\phi) = N$ this gives an isomorphism $\mathrm{Gal}(\widehat{K}_{2n+1}/K_0) \cong M(n)$.

(c) For $1 \le i \le 2n$ let γ_i be the element of $\mathrm{Gal}(K_{2n}/K_0)$ defined by (3.2). Then for $2 \le i \le n$ we have $\gamma_i(B + C + a_{2n+1}) = B + C + a_{2n+1}$. Hence we can extend γ_i to $\widehat{\sigma}_i \in \mathrm{Aut}(\widehat{K}_{2n+1})$ by setting $\widehat{\sigma}_i(\widehat{\alpha}_{2n+1}) = \widehat{\alpha}_{2n+1}$. Let $1 \le i \le n$ and let $\widehat{\alpha}'_{2n+1}$ be a root of $X^p - X - \gamma_{n+i}(B + C + a_{2n+1})$. We extend γ_{n+i} to $\widehat{\sigma}_{n+i} \in \mathrm{Aut}(\widehat{K}_{2n+1})$ by setting $\widehat{\sigma}_{n+i}(\widehat{\alpha}_{2n+1}) = \widehat{\alpha}'_{2n+1}$. By (4.7) and (5.1) we have

$$\gamma_{n+i}(B + C + a_{2n+1}) \equiv B + C + a_{2n+1} \pmod{a_i}.$$

Hence by (5.2) and Proposition 3.5(b) we get $\widehat{\alpha}'_{2n+1} \equiv \widehat{\alpha}_{2n+1} \pmod{\alpha_i}$. It follows from Lemma 3.3 that there is a generator $\widehat{\sigma}_{2n+1}$ for $\mathrm{Gal}(\widehat{K}_{2n+1}/K_{2n})$ such that

$$\widehat{\sigma}_{2n+1}(\widehat{\alpha}_{2n+1}) \equiv \widehat{\alpha}_{2n+1} + 1 \pmod{p\widehat{\alpha}_{2n+1}^{p-1}}.$$

Statements (5.6), (5.9), (5.10), and (5.11) follow directly from these constructions, and (5.7) is a consequence of Lemma 3.3.

In order to extend γ_1 to an automorphism of $\widehat{K}_{2n+1}$ we let $\eta \in E$ be a root of $X^p - X - (C + a_{2n+1})$ and let θ be a generator of $\mathrm{Gal}(E/K_0)$ such that $\theta(\alpha_1) \equiv \alpha_1 + 1 \pmod{p\alpha_1^{p-1}}$ and $\theta(\eta) \equiv \eta + D(1, \alpha_1) \pmod{\mathfrak{M}_E}$. Such θ exists by (5.3), (5.4), and Proposition 3.12(c). Let $\sigma_1 \in \mathrm{Gal}(K_{2n+1}/K_0)$ be defined as in Proposition 4.2. Then $\theta|_{K_1} = \sigma_1|_{K_1}$, so there is $\rho \in \mathrm{Gal}(K_{2n+1}E/K_0)$ such that $\rho|_E = \theta$ and $\rho|_{K_{2n+1}} = \sigma_1$. Define $\widehat{\sigma}_1 = \rho|_{\widehat{K}_{2n+1}}$. Then $\widehat{\sigma}_1|_{K_{2n}} = \sigma_1|_{K_{2n}} = \gamma_1$. By (5.5), (5.2), and Proposition 3.5(b) there is a root α_{2n+1} of $X^p - X - B$ such that $\widehat{\alpha}_{2n+1} \equiv \alpha_{2n+1} + \eta \pmod{p\eta^{p-1}\alpha_{2n+1}}$. By Corollary 3.6 and (4.5) we get

$$\begin{aligned}
(\rho - 1)\widehat{\alpha}_{2n+1} &\equiv (\rho - 1)\alpha_{2n+1} + (\rho - 1)\eta && \pmod{p\eta^{p-1}} \\
(\widehat{\sigma}_1 - 1)\widehat{\alpha}_{2n+1} &\equiv (\sigma_1 - 1)\alpha_{2n+1} + (\theta - 1)\eta && \pmod{p\eta^{p-1}} \\
&\equiv D(1, \alpha_1) && \pmod{\mathfrak{M}_{\widehat{K}_{2n+1}}} \\
&\equiv 0 && \pmod{\alpha_1^{p-1}}.
\end{aligned}$$

This proves (5.8). □

Remark 5.4. Henceforth we will denote the $M(n)$-extensions constructed using Proposition 5.2 by K_{2n+1}/K_0, rather than $\widehat{K}_{2n+1}/K_0$. In addition, we will denote the generator of K_{2n+1} over K_{2n} by α_{2n+1} rather than $\widehat{\alpha}_{2n+1}$, and we will denote the generators of $\mathrm{Gal}(K_{2n+1}/K_0)$ by σ_i rather than $\widehat{\sigma}_i$.

6. Valuations of determinants

To construct $H(n)$-extensions and $M(n)$-extensions with Galois scaffolds we use an approach which is similar to that used in [11] and [12], with the significant difference that our fields have characteristic 0 rather than characteristic p. For a local field F with residue characteristic p define $\phi : F \to F$ by $\phi(x) = x^p$; then ϕ can also be applied to matrices and vectors over F by acting on the entries. If $\mathrm{char}(F) = 0$ then we don't necessarily have $\phi(x + y) = \phi(x) + \phi(y)$. However, if $w, x, y, z \in F$ satisfy $v_F(x) \leq v_F(y)$ and $x + y \equiv w \pmod{z}$ then we do have $\phi(x) + \phi(y) \equiv \phi(w) \pmod{(px^p, z^p)}$. Therefore we get the following:

Lemma 6.1. *Let $A = (a_{ij}) \in M_k(F)$ and let τ be a permutation of $\{1, 2, \ldots, k\}$ chosen so that $\gamma = \prod_{i=1}^{k} a_{i,\tau(i)}$ has minimum valuation among the $k!$ terms in the Leibniz expansion of $\det(A)$. Then*

(a) $\det(\phi(A)) \equiv \phi(\det(A)) \pmod{p\gamma^p}$.
(b) If $d, \mu \in F$ satisfy $\det(A) \equiv d \pmod{\mu}$ then

$$\det(\phi(A)) \equiv \phi(d) \pmod{(p\gamma^p, \mu^p)}.$$

In the next section we will need to know the valuations of the determinants of certain square matrices with entries in K_0. The following lemma will allow us to compute these valuations:

Lemma 6.2. *Let F be a local field with residue characteristic p, let $\beta_1, \dots, \beta_k \in F^\times$, and set $r_i = -v_F(\beta_i)$. Assume that $r_1 \le r_1 \le \cdots \le r_k$, and for every $1 \le i < j \le k$ such that $r_i = r_j$ the images of $\beta_i, \dots, \beta_j$ in $\mathfrak{M}_F^{-r_i}/\mathfrak{M}_F^{-r_i+1}$ are linearly independent over $\mathbb{F}_p$. Set*

$$M = \begin{bmatrix} \beta_1 & \beta_1^p & \cdots & \beta_1^{p^{k-1}} \\ \beta_2 & \beta_2^p & \cdots & \beta_2^{p^{k-1}} \\ \vdots & \vdots & & \vdots \\ \beta_k & \beta_k^p & \cdots & \beta_k^{p^{k-1}} \end{bmatrix}.$$

Then $v_F(\det(M))$ is equal to the minimum of the valuations of the $k!$ terms in the Leibniz expansion of $\det(M)$. More precisely,

$$\begin{aligned} v_F(\det(M)) &= v_F(\beta_1\beta_2^p \dots \beta_k^{p^{k-1}}) \\ &= -(r_1 + pr_2 + \cdots + p^{k-1}r_k). \end{aligned}$$

Proof. Let $s_1 < \cdots < s_\ell$ be the distinct elements of $\{r_1, \dots, r_k\}$ and set

$$m_j = |\{1 \le i \le k : r_i = s_j\}|.$$

For $1 \le j \le \ell$ set $c_j = m_1 + \cdots + m_{j-1}$. Then $r_{c_j+1} = \cdots = r_{c_j+m_j} = s_j$. Set

$$M_j = \begin{bmatrix} \beta_{c_j+1}^{p^{c_j}} & \beta_{c_j+1}^{p^{c_j+1}} & \cdots & \beta_{c_j+1}^{p^{c_j+m_j-1}} \\ \beta_{c_j+2}^{p^{c_j}} & \beta_{c_j+2}^{p^{c_j+1}} & \cdots & \beta_{c_j+2}^{p^{c_j+m_j-1}} \\ \vdots & \vdots & & \vdots \\ \beta_{c_j+m_j}^{p^{c_j}} & \beta_{c_j+m_j}^{p^{c_j+1}} & \cdots & \beta_{c_j+m_j}^{p^{c_j+m_j-1}} \end{bmatrix}$$

$$M' = \begin{bmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M_\ell \end{bmatrix}.$$

Thus M' is obtained from M by replacing all entries outside the diagonal blocks with 0. Since $s_1 < \cdots < s_\ell$ we get

$$\begin{aligned} \det(M) &\equiv \det(M') && (\text{mod } \beta_1\beta_2^p \dots \beta_k^{p^{k-1}}\mathfrak{M}_F) \\ &\equiv \det(M_1)\det(M_2)\dots\det(M_\ell) && (\text{mod } \beta_1\beta_2^p \dots \beta_k^{p^{k-1}}\mathfrak{M}_F). \end{aligned} \tag{6.1}$$

We have

$$\det(M_j) = \beta_{c_j+1}^{p^{c_j}+p^{c_j+1}+\cdots+p^{c_j+m_j-1}} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \mu_2 & \mu_2^p & \cdots & \mu_2^{p^{m_j-1}} \\ \vdots & \vdots & & \vdots \\ \mu_{m_j} & \mu_{m_j}^p & \cdots & \mu_{m_j}^{p^{m_j-1}} \end{vmatrix}, \tag{6.2}$$

where $\mu_h = \beta_{c_j+h}^{p^{c_j}} \beta_{c_j+1}^{-p^{c_j}} \in \mathfrak{O}_F^\times$. Since the images of $\beta_{c_j+1}, \beta_{c_j+2}, \ldots, \beta_{c_j+m_j}$ in $\mathfrak{M}_F^{-s_j}/\mathfrak{M}_F^{-s_j+1}$ are linearly independent over $\mathbb{F}_p$, the images of $1, \mu_2, \ldots, \mu_{m_j}$ in $\mathfrak{O}_F/\mathfrak{M}_F$ are also linearly independent over $\mathbb{F}_p$. It follows from the theory of the Moore determinant [14, Lemma 1.3.3] that the determinant on the right side of (6.2) is a unit. Hence

$$\begin{aligned} v_F(\det(M_j)) &= (p^{c_j} + p^{c_j+1} + \cdots + p^{c_j+m_j-1}) v_F(\beta_{c_j+1}) \\ &= -(p^{c_j} + p^{c_j+1} + \cdots + p^{c_j+m_j-1}) s_j \\ &= -(p^{c_j} r_{c_j+1} + p^{c_j+1} r_{c_j+2} + \cdots + p^{c_j+m_j-1} r_{c_j+m_j}). \end{aligned}$$

Combining this formula with (6.1) gives the desired result. □

7. Field extensions with a generator

In Proposition 4.2 we constructed a tower of Galois extensions

$$K_0 \subset K_1 \subset \cdots \subset K_{2n} \subset K_{2n+1}$$

such that $\mathrm{Gal}(K_i/K_0) \cong C_p^i$ for $1 \le i \le 2n$ and $\mathrm{Gal}(K_{2n+1}/K_0) \cong H(n)$. In Proposition 5.2 (with the notational adjustment described in Remark 5.4) we constructed a similar tower, but with $\mathrm{Gal}(K_{2n+1}/K_0) \cong M(n)$. In this section we specialize these constructions to produce $H(n)$-extensions and $M(n)$-extensions K_{2n+1}/K_0 together with $Y \in K_{2n+1}$ such that $v_{2n+1}(Y) \equiv -b_1 \pmod{p^{2n+1}}$, where b_1 is the smallest lower ramification number of K_{2n+1}/K_0. Since $p \nmid b_1$ it follows that $K_{2n+1} = K_0(Y)$. In the next section we will use the generator Y to construct Galois scaffolds for these extensions.

The extensions constructed in Propositions 4.2 and 5.2 depend on the choice of elements $a_1, \ldots, a_{2n+1}$ in K_0 satisfying certain conditions on the valuations $v_0(a_i) = -u_i$. In this section we retain these hypotheses; in particular, in the cases where K_{2n+1}/K_0 is an $H(n)$-extension we assume that the condition $u_{2n+1} > u_n + u_{2n}$ from Proposition 4.2(c) holds. We impose further constraints on the a_i by requiring that there are $c, \omega_i \in K_0$ such that $a_i = c\omega_i^{p^{2n}}$ for $1 \le i \le 2n+1$. Set $r = -v_0(c)$ and $m_i = -v_0(\omega_i)$ for $1 \le i \le 2n+1$. Then $u_i = -v_0(a_i) = r + p^{2n} m_i$.

For $1 \le i \le 2n$ let $\alpha_i \in K^{sep}$ satisfy $\alpha_i^p - \alpha_i = a_i$. Recall from Propositions 4.2 and 5.2 that we defined

$$B = a_1\alpha_{n+1} + a_2\alpha_{n+2} + \cdots + a_n\alpha_{2n}$$

$$C = -\sum_{i=1}^{p-1} p^{-1}\binom{p}{i}\alpha_1^i a_1^{p-i}.$$

Set $E = B$ in the case where K_{2n+1}/K_0 is an $H(n)$-extension, and $E = B + C$ in the case where K_{2n+1}/K_0 is an $M(n)$-extension. Let $\alpha_{2n+1} \in K^{sep}$ satisfy

$$\alpha_{2n+1}^p - \alpha_{2n+1} = E + a_{2n+1}.$$

We define the following elements of K_{2n+1}^{2n+1}:

$$\vec{E} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ E \end{bmatrix} \quad \vec{\omega} = \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_{2n} \\ \omega_{2n+1} \end{bmatrix} \quad \vec{\alpha} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_{2n} \\ \alpha_{2n+1} \end{bmatrix}.$$

Then we can write our system of Artin-Schreier equations as $\phi(\vec{\alpha}) - \vec{\alpha} = c\phi^{2n}(\vec{\omega}) + \vec{E}$. Now define

$$Y = \det([\vec{\alpha}, \vec{\omega}, \phi(\vec{\omega}), \ldots, \phi^{2n-1}(\vec{\omega})]). \tag{7.1}$$

Then $Y \in K_{2n+1}$. By expanding the right side of (7.1) in cofactors along the first column we get

$$Y = t_1\alpha_1 + t_2\alpha_2 + \cdots + t_{2n+1}\alpha_{2n+1} \tag{7.2}$$

with $t_i \in K_0$.

Since $a_1, \ldots, a_{2n}$ are reduced Artin-Schreier constants, it follows from Lemma 6.2 that

$$\begin{aligned} v_0(t_i) &= v_0(\omega_1\omega_2^p \ldots \omega_{i-1}^{p^{i-2}} \omega_{i+1}^{p^{i-1}} \omega_{i+2}^{p^i} \ldots \omega_{2n+1}^{p^{2n-1}}) \\ &= -(m_1 + pm_2 + \cdots + p^{i-2}m_{i-1} + p^{i-1}m_{i+1} + p^i m_{i+2} + \cdots + p^{2n-1}m_{2n+1}). \end{aligned}$$

Hence for $1 \le i \le 2n$ we have

$$\begin{aligned} v_0(t_{i+1}) - v_0(t_i) &= p^{i-1}m_{i+1} - p^{i-1}m_i \\ v_{2n+1}(t_{i+1}) - v_{2n+1}(t_i) &= p^{2n+i}(m_{i+1} - m_i) \\ &= p^i(u_{i+1} - u_i) \\ &= b_{i+1} - b_i, \end{aligned}$$

where $b_1, \ldots, b_{2n+1}$ are the lower ramification numbers of K_{2n+1}/K_0. For $1 \le i, j \le 2n+1$ we get

$$v_{2n+1}(t_j) - v_{2n+1}(t_i) = b_j - b_i. \tag{7.3}$$

By Propositions 4.2(c) and 5.2(c) we have $v_0(\alpha_i) = -p^{-1}u_i$ for $1 \le i \le 2n+1$. It follows that for $1 \le j \le 2n$ and $i \ge 0$ we have

$$\begin{aligned} v_0(t_{j+1}^{p^i}\alpha_{j+1}) - v_0(t_j^{p^i}\alpha_j) &= p^{i-2n-1}(b_{j+1} - b_j) - p^{-1}(u_{j+1} - u_j) \\ &= (p^{i+j-2n-1} - p^{-1})(u_{j+1} - u_j). \end{aligned} \tag{7.4}$$

Proposition 7.1. *Let K_{2n+1}/K_0 be an extension constructed as in Proposition 4.2 or Proposition 5.2 using $a_1, a_2, \dots, a_{2n+1} \in K_0$. Assume that there are $c, \omega_i \in K_0$ such that $a_i = c\omega_i^{p^{2n}}$ for $1 \le i \le 2n+1$. Set $u_i = -v_0(a_i)$, and assume $u_{2n} < e_0$ and*

$$p^{2n}u_n + p^{2n-1}u_{2n} < b_{2n+1}.$$

If K_{2n+1}/K_0 is an $H(n)$-extension assume (4.1), (4.2), and $u_{2n+1} > u_n + u_{2n}$, while if K_{2n+1}/K_0 is an $M(n)$-extension assume (5.1)–(5.5) and

$$p^{2n+1}(1 - p^{-1} + p^{-2})u_1 < b_{2n+1}.$$

Define Y as in (7.1). Then for $0 \le i \le 2n$ we have the following congruences modulo $pt_{2n+1-i}^{p^i}\alpha_{2n+1-i}^{p}$:

$$\phi^i(Y) \equiv \det([\vec{\alpha} + \vec{E} + \phi(\vec{E}) + \cdots + \phi^{i-1}(\vec{E}), \phi^i(\vec{\omega}), \dots, \phi^{2n-1+i}(\vec{\omega})]). \tag{7.5}$$

Proof. If K_{2n+1}/K_0 is an $H(n)$-extension then $v_0(E) \ge -u_n - p^{-1}u_{2n}$, while if K_{2n+1}/K_0 is an $M(n)$-extension then

$$v_0(E) \ge \min\{-u_n - p^{-1}u_{2n}, -(p - 1 + p^{-1})u_1\}.$$

In either case it follows from the hypotheses that

$$b_{2n+1} > -p^{2n}v_0(E). \tag{7.6}$$

We use induction on i. The case $i = 0$ follows from (7.1). Let $0 \le i \le 2n-1$ and assume that the claim holds for i. Then we have

$$\phi^i(Y) \equiv \det([\vec{\alpha} + \vec{E} + \phi(\vec{E}) + \cdots + \phi^{i-1}(\vec{E}), \phi^i(\vec{\omega}), \dots, \phi^{2n-1+i}(\vec{\omega})]) \pmod{\mu}, \tag{7.7}$$

where $\mu = pt_{2n+1-i}^{p^i}\alpha_{2n+1-i}^{p}$. It follows from the hypotheses that $u_1 \le \cdots \le u_{2n+1}$, and hence that $-v_0(\omega_1) \le \cdots \le -v_0(\omega_{2n+1})$. Therefore by Lemma 6.2 the minimum valuation of the $(2n+1)!$ terms in the Leibniz expansion of the determinant in (7.5) is equal either to $v_0(t_j^{p^i}\alpha_j)$ for some $1 \le j \le 2n+1$, or to $v_0(t_{2n+1}^{p^i}E^{p^{i-1}})$. By (7.4) we get

$$\begin{aligned} v_0(t_{j+1}^{p^i}\alpha_{j+1}) - v_0(t_j^{p^i}\alpha_j) &\le 0 \text{ for } 1 \le j \le 2n - i \\ v_0(t_{j+1}^{p^i}\alpha_{j+1}) - v_0(t_j^{p^i}\alpha_j) &\ge 0 \text{ for } 2n - i \le j \le 2n. \end{aligned}$$

Therefore the minimum of $v_0(t_j^{p^i}\alpha_j)$ is achieved when $j = 2n - i$. By (7.3), (7.6), and Corollary 2.5(b) we get

$$\begin{aligned} v_0(t_{2n+1}^{p^i}E^{p^{i-1}}) - v_0(t_{2n-i}^{p^i}\alpha_{2n-i}) &= p^{i-2n-1}(b_{2n+1} - b_{2n-i}) + p^{i-1}v_0(E) + p^{-1}u_{2n-i} \\ &> -p^{i-2n-1}b_{2n-i} + p^{-1}u_{2n-i} \geq 0. \end{aligned}$$

Hence the term with minimum valuation in the Leibniz expansion of (7.5) is $\gamma := t_{2n-i}^{p^i}\alpha_{2n-i}$. For $1 \leq i \leq 2n-1$ it follows from (7.3) and the assumption $u_{2n} < e_0$ that

$$\begin{aligned} v_0(\mu^p) - v_0(p\gamma^p) &= v_0((pt_{2n+1-i}^{p^i}\alpha_{2n+1-i}^p)^p) - v_0(p(t_{2n-i}^{p^i}\alpha_{2n-i})^p) \\ &= (p-1)e_0 + p^{i-2n}(b_{2n+1-i} - b_{2n-i}) - pu_{2n+1-i} + u_{2n-i} \\ &= (p-1)e_0 + (u_{2n+1-i} - u_{2n-i}) - pu_{2n+1-i} + u_{2n-i} \\ &= (p-1)(e_0 - u_{2n+1-i}) > 0. \end{aligned}$$

Using equation (7.1) and Lemma 6.1(a) (for the case $i = 0$), or equation (7.7) and Lemma 6.1(b) (for the cases $1 \leq i \leq 2n-1$) we get the following congruences modulo $p\gamma^p = pt_{2n-i}^{p^{i+1}}\alpha_{2n-i}^p$:

$$\begin{aligned} \phi^{i+1}(Y) &\equiv \det([\phi(\vec{\alpha}) + \phi(\vec{E}) + \phi^2(\vec{E}) + \cdots + \phi^i(\vec{E}), \phi^{i+1}(\vec{\omega}), \ldots, \phi^{2n+i}(\vec{\omega})]) \\ &\equiv \det([\vec{\alpha} + c\phi^{2n}(\omega) + \vec{E} + \phi(\vec{E}) + \cdots + \phi^i(\vec{E}), \phi^{i+1}(\vec{\omega}), \ldots, \phi^{2n+i}(\vec{\omega})]) \\ &\equiv \det([\vec{\alpha} + \vec{E} + \phi(\vec{E}) + \cdots + \phi^i(\vec{E}), \phi^{i+1}(\vec{\omega}), \ldots, \phi^{2n+i}(\vec{\omega})]). \end{aligned}$$

Note that the last congruence holds because $i + 1 \leq 2n \leq 2n + i$. □

Corollary 7.2. *Let K_{2n+1}/K_0 be an extension which satisfies the hypotheses of Proposition 7.1, and define Y as in (7.1). Then $v_{2n+1}(Y) = -b_1 + v_{2n+1}(t_1)$ and $K_{2n+1} = K_0(Y)$.*

Proof. The case $i = 2n$ of Proposition 7.1 gives

$$\phi^{2n}(Y) \equiv \det([\vec{\alpha} + \vec{E} + \phi(\vec{E}) + \cdots + \phi^{2n-1}(\vec{E}), \phi^{2n}(\vec{\omega}), \ldots, \phi^{4n-1}(\vec{\omega})]) \pmod{pt_1^{p^{2n}}\alpha_1^p}.$$

It follows from (7.3) and (7.6) that $v_0(E^{p^{2n-1}}t_{2n+1}^{p^{2n}}) > v_0(t_1^{p^{2n}}\alpha_1)$. Hence by (7.4) we get

$$v_0(\det([\vec{\alpha} + \vec{E} + \cdots + \phi^{2n-1}(\vec{E}), \phi^{2n}(\vec{\omega}), \ldots, \phi^{4n-1}(\vec{\omega})])) = v_0(t_1^{p^{2n}}\alpha_1).$$

Since $a_1, \ldots, a_{2n}$ are reduced Artin-Schreier constants we have $v_0(t_1^{p^{2n}}\alpha_1) < v_0(pt_1^{p^{2n}}\alpha_1^p)$. Therefore it follows from the above that

$$v_0(\phi^{2n}(Y)) = v_0(t_1^{2n}\alpha_1) = -p^{-1}u_1 + p^{2n}v_0(t_1)$$
$$v_{2n+1}(Y) = -b_1 + v_{2n+1}(t_1).$$

Since $t_1 \in K_0$ we get $v_{2n+1}(Y) \equiv -b_1 \pmod{p^{2n+1}}$. It follows that $p \nmid v_{2n+1}(Y)$, and hence that $K_{2n+1} = K_0(Y)$. □

8. Galois scaffolds

A Galois scaffold is a structure that can be attached to certain totally ramified Galois p-extensions. A Galois scaffold for L/K can be used to answer questions about the Galois module structure of $\mathfrak{O}_L$ and its ideals which are in general difficult to address. In [7], Byott and Elder gave sufficient conditions for a totally ramified Galois p-extension L/K to admit a Galois scaffold. In this section we define Galois scaffolds and state the Byott-Elder criterion for the existence of a Galois scaffold. In Section 10 we will use Galois scaffolds to get information about Galois module theory.

For $n \geq 1$ set $\mathbb{S}_{p^n} = \{0, 1, \ldots, p^n - 1\}$. Write the base-$p$ expansion of $s \in \mathbb{S}_{p^n}$ as $s = \sum_{i=0}^{n-1} s_{(i)}p^i$, with $0 \leq s_{(i)} < p$. Let K be a local field with residue characteristic p, let L/K be a totally ramified Galois extension of degree p^n, and set $G = \mathrm{Gal}(L/K)$. Assume that the lower ramification numbers $b_1 \leq \ldots \leq b_n$ of L/K are relatively prime to p. Associated to the extension L/K there is a function $\mathfrak{b} : \mathbb{S}_{p^n} \to \mathbb{Z}$ defined by

$$\mathfrak{b}(s) = \sum_{i=1}^{n} s_{(n-i)}p^{n-i}b_i.$$

Let $r : \mathbb{Z} \to \mathbb{S}_{p^n}$ be the residue function, defined by $r(a) \in \mathbb{S}_{p^n}$ and $r(a) \equiv a \pmod{p^n}$. The assumption $p \nmid b_i$ for $1 \leq i \leq n$ implies that $r \circ (-\mathfrak{b}) : \mathbb{S}_{p^n} \to \mathbb{S}_{p^n}$ is a bijection. Let $\mathfrak{a} : \mathbb{S}_{p^n} \to \mathbb{S}_{p^n}$ be the inverse of $r \circ (-\mathfrak{b})$. We may extend $\mathfrak{a}$ to a function from $\mathbb{Z}$ to $\mathbb{S}_{p^n}$ by setting $\mathfrak{a}(t) = \mathfrak{a}(r(t))$ for $t \in \mathbb{Z}$.

Definition 8.1. Let L/K, $b_1, \ldots, b_n$, $\mathfrak{b}$ and $\mathfrak{a}$ be as above, and let $\mathfrak{c} \geq 1$. Then a Galois scaffold for L/K with precision $\mathfrak{c}$ consists of:

(i) Elements $\lambda_t \in L$ for each $t \in \mathbb{Z}$ such that $v_L(\lambda_t) = t$ and $\lambda_t\lambda_s^{-1} \in K$ whenever $t \equiv s \pmod{p^n}$.

(ii) Elements $\Psi_1, \ldots, \Psi_n$ in the augmentation ideal $(\sigma - 1 : \sigma \in G)$ of $K[G]$ such that for each $1 \leq i \leq n$ and $t \in \mathbb{Z}$,

$$\Psi_i\lambda_t \equiv u_{i,t}\lambda_{t+p^{n-i}b_i} \pmod{\lambda_{t+p^{n-i}b_i}\mathfrak{M}_L^{\mathfrak{c}}} \quad \text{if } \mathfrak{a}(t)_{(n-i)} \geq 1$$
$$\Psi_i\lambda_t \equiv 0 \pmod{\lambda_{t+p^{n-i}b_i}\mathfrak{M}_L^{\mathfrak{c}}} \quad \text{if } \mathfrak{a}(t)_{(n-i)} = 0$$

for some $u_{i,t} \in \mathfrak{O}_K^{\times}$.

We now describe the sufficient conditions for the existence of a Galois scaffold given in [7]. Let K_n/K_0 be a totally ramified Galois extension of degree p^n. Set $G = \mathrm{Gal}(K_n/K_0)$ and let

$$\{1\} = G^{(n)} \leq G^{(n-1)} \leq \cdots \leq G^{(1)} \leq G^{(0)} = G$$

be a refinement of the ramification filtration of G by normal subgroups of G such that $|G^{(i)}| = p^{n-i}$. For $1 \leq i \leq n$ let K_i be the fixed field of $G^{(i)}$ and choose $\sigma_i \in G^{(i-1)} \smallsetminus G^{(i)}$. Then $\sigma_i|_{K_i}$ is a generator for $\mathrm{Gal}(K_i/K_{i-1}) \cong G^{(i-1)}/G^{(i)} \cong C_p$.

Let $b_1 \leq b_2 \leq \cdots \leq b_n$ and $u_1 \leq u_2 \leq \cdots \leq u_n$ be the lower and upper ramification numbers of K_n/K_0, counted with multiplicities. Using Proposition 3 of [21, IV §1] we find that K_i/K_0 has lower ramification numbers $b_1 \leq \cdots \leq b_i$ and upper ramification numbers $u_1 \leq \cdots \leq u_i$. Assume that the lower numbers satisfy $p \nmid b_1$ and $b_i \equiv b_1 \pmod{p^n}$ for $1 \leq i \leq n$. Let $X_j \in K_j$ be such that $v_j(X_j) = -b_j$. By Lemma 4 of [21, IV §3] we have $v_j((\sigma_i - 1)X_j) = b_i - b_j$ for $1 \leq i \leq j$. It follows that $(\sigma_i - 1)X_j = \mu_{ij} + \epsilon_{ij}$ for some $\mu_{ij} \in K_0$ and $\epsilon_{ij} \in K_j$ such that $v_j(\mu_{ij}) = b_i - b_j$ and $v_j(\epsilon_{ij}) > b_i - b_j$.

Theorem 8.2. *Let K_n/K_0, u_i, b_i, σ_i, X_i, μ_{ij}, and ϵ_{ij} be as above. Set*

$$\mathfrak{c} = \min_{1 \leq i \leq j \leq n} \{v_n(\epsilon_{ij}) - v_n(\mu_{ij}) - p^{n-1}u_i + p^{n-j}b_i\}.$$

If $\mathfrak{c} \geq 1$ then K_n/K_0 admits a Galois scaffold with precision $\mathfrak{c}$.

Proof. This is proved as Theorem 2.10 in [7]. □

9. Extensions with a Galois scaffold

In Section 7 we constructed totally ramified $H(n)$-extensions and $M(n)$-extensions K_{2n+1}/K_0 together with elements $Y \in K_{2n+1}$ such that $K_{2n+1} = K_0(Y)$. In this section we specialize these constructions to produce $H(n)$-extensions and $M(n)$-extensions which satisfy the conditions of Theorem 8.2, and therefore have Galois scaffolds.

To apply Theorem 8.2 we need to find elements $X_j \in K_j$ which have the properties specified in the theorem. Since K_{2n}/K_0 is an elementary abelian p-extension we can use known results to get X_j for $1 \leq j \leq 2n$:

Proposition 9.1. *Let K_{2n+1}/K_0 be an extension constructed using Proposition 7.1. Then for $1 \leq j \leq 2n$ there are $X_j \in K_j$ such that $v_j(X_j) = -b_j$ with the following property: For $1 \leq i \leq j$ we have $(\sigma_i - 1)X_j = \mu_{ij} + \epsilon_{ij}$ with $\mu_{ij} \in K_0$, $\epsilon_{ij} \in K_j$, $v_j(\mu_{ij}) = b_i - b_j$, and*

$$v_{2n+1}(\epsilon_{ij}) - v_{2n+1}(\mu_{ij}) = p^{2n+1}e_0 - (p-1)p^{2n}u_i.$$

Furthermore, we have $\mu_{jj} = 1$.

Proof. See the proof of Lemma 3.8 in [7]. □

It follows from Proposition 9.1 and Corollary 2.5(b) that

$$\begin{aligned}
&\min_{1\le i\le j\le 2n}\{v_{2n+1}(\epsilon_{ij}) - v_{2n+1}(\mu_{ij}) - p^{2n}u_i + p^{2n+1-j}b_i\}\\
&\quad = \min_{1\le i\le j\le 2n}\{p^{2n+1}e_0 - p^{2n+1}u_i + p^{2n+1-j}b_i\}\\
&\quad = \min_{1\le i\le 2n}\{p^{2n+1}e_0 - p^{2n+1}u_i + pb_i\}\\
&\quad = p^{2n+1}e_0 - p^{2n+1}u_{2n} + pb_{2n}. \qquad (9.1)
\end{aligned}$$

Suppose $p^{2n+1}e_0 - p^{2n+1}u_{2n} + pb_{2n} > 0$. In order to apply Theorem 8.2 to get a Galois scaffold for K_{2n+1}/K_0 we need to choose an appropriate $X_{2n+1} \in K_{2n+1}$. The remainder of this section is devoted to showing that, under suitable assumptions on ramification data, $X_{2n+1} = t_{2n+1}^{-1}Y$ satisfies the conditions of Theorem 8.2 and thus can be used to construct $H(n)$-extensions and $M(n)$-extensions with Galois scaffolds.

Theorem 9.2. *Let K_0 be a local field with residue characteristic $p > 2$. Let $c, \omega_1, \dots, \omega_{2n+1}$ be elements of K_0 such that $p \nmid v_0(c)$, and set $a_i = c\omega_i^{p^{2n}}$ for $1 \le i \le 2n+1$. Set $u_i = -v_0(a_i)$ for $1 \le i \le 2n+1$ and define $b_1, \dots, b_{2n+1}$ recursively by $b_1 = u_1$ and $b_{i+1} - b_i = p^i(u_{i+1} - u_i)$ for $1 \le i \le 2n$. Assume that $a_1, \dots, a_{2n}$ are reduced Artin-Schreier constants, and that*

$$u_n + (1-p^{-1})u_{2n} < e_0 \qquad (9.2)$$

$$p^{-1}u_n + p^{-2}u_{2n} + (1-p^{-1})u_{2n+1} < e_0 \qquad (9.3)$$

$$u_{2n} < e_0 \qquad (9.4)$$

$$u_{2n+1} - p^{-2n-1}b_{2n+1} < e_0 \qquad (9.5)$$

$$p^{2n}u_n + p^{2n}u_{2n} < b_{2n+1}. \qquad (9.6)$$

For $1 \le i \le 2n$ let α_i satisfy $\alpha_i^p - \alpha_i = a_i$ and define $K_i = K_{i-1}(\alpha_i)$. Set

$$B = a_1\alpha_{n+1} + a_2\alpha_{n+2} + \cdots + a_n\alpha_{2n},$$

let α_{2n+1} satisfy $\alpha_{2n+1}^p - \alpha_{2n+1} = B + a_{2n+1}$, and define $K_{2n+1} = K_{2n}(\alpha_{2n+1})$. Then K_{2n+1}/K_0 is an $H(n)$-extension with upper ramification numbers $u_1 \le \cdots \le u_{2n+1}$ and lower ramification numbers $b_1 \le \cdots \le b_{2n+1}$. Furthermore, K_{2n+1}/K_0 has a Galois scaffold with precision

$$\mathfrak{c} = \min\{b_{2n+1} - p^{2n}u_n - p^{2n}u_{2n}, p^{2n+1}e_0 - p^{2n+1}u_{2n+1} + b_{2n+1}\}.$$

Proof. By (9.6) and Corollary 2.5(b) we get $u_n + u_{2n} < u_{2n+1}$. Therefore by Proposition 4.2(c), K_{2n+1}/K_0 is an $H(n)$-extension with upper ramification numbers $u_1 \leq \cdots \leq u_{2n+1}$ and lower ramification numbers $b_1 \leq \cdots \leq b_{2n+1}$. By (9.4), (9.6), and Corollary 7.2 we get $v_{2n+1}(Y) = -b_1 + v_{2n+1}(t_1)$ and $K_{2n+1} = K_0(Y)$. Set $X_{2n+1} = t_{2n+1}^{-1}Y$. Then by (7.3) we get

$$v_{2n+1}(X_{2n+1}) = -v_{2n+1}(t_{2n+1}) - b_1 + v_{2n+1}(t_1) = -b_{2n+1}.$$

Let $1 \leq i \leq n$. Then by (7.2), (4.3), and (4.5) we have

$$\begin{aligned}(\sigma_i - 1)(X_{2n+1}) &= t_{2n+1}^{-1} t_i (\sigma_i - 1)(\alpha_i)\\ (\sigma_{n+i} - 1)(X_{2n+1}) &= t_{2n+1}^{-1} t_{n+i} (\sigma_{n+i} - 1)(\alpha_{n+i}) + (\sigma_{n+i} - 1)(\alpha_{2n+1})\\ (\sigma_{2n+1} - 1)(X_{2n+1}) &= (\sigma_{2n+1} - 1)(\alpha_{2n+1}).\end{aligned}$$

For $1 \leq i \leq 2n+1$ set $\mu_{i,2n+1} = t_{2n+1}^{-1} t_i \in K_0$. Then $v_{2n+1}(\mu_{i,2n+1}) = b_i - b_{2n+1}$ by (7.3). Write $(\sigma_i - 1)(X_{2n+1}) = \mu_{i,2n+1} + \epsilon_{i,2n+1}$ with $\epsilon_{i,2n+1} \in K_{2n+1}$. Then by (4.4) and (4.6) we have

$$\begin{aligned}v_{2n+1}(\epsilon_{i,2n+1}) - v_{2n+1}(\mu_{i,2n+1}) &\geq p^{2n+1}e_0 - (p-1)p^{2n}u_i\\ v_{2n+1}(\epsilon_{n+i,2n+1}) - v_{2n+1}(\mu_{n+i,2n+1}) &\geq \min\{p^{2n+1}e_0 - (p-1)p^{2n}u_{n+i}, b_{2n+1}\\ &\qquad - b_{n+i} - p^{2n}u_i\}\\ v_{2n+1}(\epsilon_{2n+1,2n+1}) - v_{2n+1}(\mu_{2n+1,2n+1}) &\geq p^{2n+1}e_0 - (p-1)p^{2n}u_{2n+1}\end{aligned}$$

for $1 \leq i \leq n$. It follows that

$$\begin{aligned}&v_{2n+1}(\epsilon_{i,2n+1}) - v_{2n+1}(\mu_{i,2n+1}) - p^{2n}u_i + b_i \geq p^{2n+1}e_0 - p^{2n+1}u_i + b_i\\ &v_{2n+1}(\epsilon_{n+i,2n+1}) - v_{2n+1}(\mu_{n+i,2n+1}) - p^{2n}u_{n+i} + b_{n+i}\\ &\quad \geq \min\{p^{2n+1}e_0 - p^{2n+1}u_{n+i} + b_{n+i}, b_{2n+1} - p^{2n}u_i - p^{2n}u_{n+i}\}\\ &v_{2n+1}(\epsilon_{2n+1,2n+1}) - v_{2n+1}(\mu_{2n+1,2n+1}) - p^{2n}u_{2n+1} + b_{2n+1}\\ &\quad \geq p^{2n+1}e_0 - p^{2n+1}u_{2n+1} + b_{2n+1}.\end{aligned}$$

Using Corollary 2.5(a) we get

$$p^{2n+1}e_0 - p^{2n+1}u_i + b_i \geq p^{2n+1}e_0 - p^{2n+1}u_{2n+1} + b_{2n+1} \tag{9.7}$$

for $1 \leq i \leq 2n$. It follows that

$$\begin{aligned}&\min_{1\leq i\leq 2n+1}\{v_{2n+1}(\epsilon_{i,2n+1}) - v_{2n+1}(\mu_{i,2n+1}) - p^{2n}u_i + b_i\}\\ &\quad \geq \min\{b_{2n+1} - p^{2n}u_n - p^{2n}u_{2n}, p^{2n+1}e_0 - p^{2n+1}u_{2n+1} + b_{2n+1}\}.\end{aligned}$$

Using the relation $b_{2n+1} - b_{2n} = p^{2n}(u_{2n+1} - u_{2n})$ we get

$$p^{2n+1}e_0 - p^{2n+1}u_{2n} + pb_{2n} > p^{2n+1}e_0 - p^{2n+1}u_{2n+1} + b_{2n+1}. \tag{9.8}$$

Hence by (9.1) and Theorem 8.2 we deduce that K_{2n+1}/K_0 has a Galois scaffold with precision

$$\mathfrak{c} = \min\{b_{2n+1} - p^{2n}u_n - p^{2n}u_{2n},\ p^{2n+1}e_0 - p^{2n+1}u_{2n+1} + b_{2n+1}\}.$$

Note that $\mathfrak{c} \geq 1$ by (9.6) and (9.5). □

By replacing (9.2)–(9.5) with the single inequality $u_{2n+1} \leq e_0$ we get the following simpler, but weaker, version of Theorem 9.2:

Corollary 9.3. *Let K_{2n+1}/K_0 be an extension constructed as in Theorem 9.2, but with (9.2)–(9.5) replaced with the single assumption $u_{2n+1} \leq e_0$. Then K_{2n+1}/K_0 is an $H(n)$-extension which has a Galois scaffold with precision $\mathfrak{c} = b_{2n+1} - p^{2n}u_n - p^{2n}u_{2n}$.*

Proof. As in the proof of Theorem 9.2, (9.6) implies $u_n + u_{2n} < u_{2n+1}$. Combining this with the assumption $u_{2n+1} \leq e_0$ we find that the assumptions (9.2)–(9.5) from Theorem 9.2 all hold. Since $u_{2n+1} \leq e_0$ we have

$$b_{2n+1} - p^{2n}u_n - p^{2n}u_{2n} < p^{2n+1}e_0 - p^{2n+1}u_{2n+1} + b_{2n+1}. \tag{9.9}$$

Hence by Theorem 9.2 K_{2n+1}/K_0 is an $H(n)$-extension which admits a Galois scaffold with precision $\mathfrak{c} = b_{2n+1} - p^{2n}u_n - p^{2n}u_{2n}$. □

Theorem 9.4. *Let K_0 be a local field with residue characteristic $p > 2$. Let $c, \omega_1, \dots, \omega_{2n+1}$ be elements of K_0 such that $p \nmid v_0(c)$, and set $a_i = c\omega_i^{p^{2n}}$ for $1 \leq i \leq 2n+1$. Set $u_i = -v_0(a_i)$ for $1 \leq i \leq 2n+1$ and define $b_1, \dots, b_{2n+1}$ recursively by $b_1 = u_1$ and $b_{i+1} - b_i = p^i(u_{i+1} - u_i)$ for $1 \leq i \leq 2n$. Assume that $a_1, \dots, a_{2n}$ are reduced Artin-Schreier constants, and that*

$$u_n + (1 - p^{-1})u_{2n} < e_0 \tag{9.10}$$

$$p^{-1}u_n + p^{-2}u_{2n} + (1 - p^{-1})u_{2n+1} < e_0 \tag{9.11}$$

$$(1 - p^{-1} + p^{-2})u_1 + (1 - p^{-1})u_{2n+1} < e_0 \tag{9.12}$$

$$u_{2n} < e_0 \tag{9.13}$$

$$u_{2n+1} - p^{-2n-1}b_{2n+1} < e_0 \tag{9.14}$$

$$p^{2n}u_n + p^{2n}u_{2n} < b_{2n+1} \tag{9.15}$$

$$p^{2n+1}u_1 < b_{2n+1}. \tag{9.16}$$

For $1 \leq i \leq 2n$ let α_i satisfy $\alpha_i^p - \alpha_i = a_i$ and define $K_i = K_{i-1}(\alpha_i)$. Set

$$B = a_1\alpha_{n+1} + a_2\alpha_{n+2} + \cdots + a_n\alpha_{2n},$$
$$C = D(\alpha_1, a_1) = -\sum_{i=1}^{p-1} p^{-1}\binom{p}{i}\alpha_1^i a_1^{p-i},$$

let α_{2n+1} satisfy $\alpha_{2n+1}^p - \alpha_{2n+1} = B + C + a_{2n+1}$, and define $K_{2n+1} = K_{2n}(\alpha_{2n+1})$. Then K_{2n+1}/K_0 is an $M(n)$-extension with upper ramification numbers $u_1 \le \cdots \le u_{2n+1}$ and lower ramification numbers $b_1 \le \cdots \le b_{2n+1}$. Furthermore, K_{2n+1}/K_0 has a Galois scaffold with precision

$$\mathfrak{c} = \min\{b_{2n+1} - p^{2n+1}u_1,\ b_{2n+1} - p^{2n}u_n - p^{2n}u_{2n},\ p^{2n+1}e_0 - p^{2n+1}u_{2n+1} + b_{2n+1}\}.$$

Proof. As in the proof of Theorem 9.2, (9.15) implies $u_n + u_{2n} < u_{2n+1}$. In addition, by (9.16) and Corollary 2.5(a) we get $(p + 1 - p^{-1})u_1 < u_{2n+1}$. Hence by Proposition 5.2, K_{2n+1}/K_0 is an $M(n)$-extension with upper ramification numbers $u_1 \le \cdots \le u_{2n+1}$ and lower ramification numbers $b_1 \le \cdots \le b_{2n+1}$. By (9.13), (9.15), (9.16), and Corollary 7.2 we get $v_{2n+1}(Y) = -b_1 + v_{2n+1}(t_1)$ and $K_{2n+1} = K_0(Y)$. Set $X_{2n+1} = t_{2n+1}^{-1}Y$; then $v_{2n+1}(X_{2n+1}) = -b_{2n+1}$. By (7.2), (5.6), and (5.9) we get

$$\begin{aligned}
(\sigma_1 - 1)(X_{2n+1}) &= t_{2n+1}^{-1}t_1(\sigma_1 - 1)(\alpha_1) + (\sigma_1 - 1)(\alpha_{2n+1}),\\
(\sigma_i - 1)(X_{2n+1}) &= t_{2n+1}^{-1}t_i(\sigma_i - 1)(\alpha_i) && (2 \le i \le n),\\
(\sigma_{n+i} - 1)(X_{2n+1}) &= t_{2n+1}^{-1}t_{n+i}(\sigma_{n+i} - 1)(\alpha_{n+i}) + (\sigma_{n+i} - 1)(\alpha_{2n+1}) && (1 \le i \le n),\\
(\sigma_{2n+1} - 1)(X_{2n+1}) &= (\sigma_{2n+1} - 1)(\alpha_{2n+1}).
\end{aligned}$$

For $1 \le i \le 2n+1$ set $\mu_{i,2n+1} = t_{2n+1}^{-1}t_i$; then $v_{2n+1}(\mu_{i,2n+1}) = b_i - b_{2n+1}$. Write $(\sigma_i - 1)(X_{2n+1}) = \mu_{i,2n+1} + \epsilon_{i,2n+1}$ with $\epsilon_{i,2n+1} \in K_{2n+1}$. Then by (5.7), (5.8), (5.10), and (5.11) we have

$$\begin{aligned}
v_{2n+1}(\epsilon_{1,2n+1}) - v_{2n+1}(\mu_{1,2n+1}) &\ge \min\{p^{2n+1}e_0 - (p-1)p^{2n}u_1,\\
&\qquad b_{2n+1} - b_1 - (p-1)p^{2n}u_1\},\\
v_{2n+1}(\epsilon_{i,2n+1}) - v_{2n+1}(\mu_{i,2n+1}) &\ge p^{2n+1}e_0 - (p-1)p^{2n}u_i && (2 \le i \le n),\\
v_{2n+1}(\epsilon_{n+i,2n+1}) - v_{2n+1}(\mu_{n+i,2n+1}) &\ge \min\{p^{2n+1}e_0 - (p-1)p^{2n}u_{n+i},\\
&\qquad b_{2n+1} - b_{n+i} - p^{2n}u_i\} && (1 \le i \le n),\\
v_{2n+1}(\epsilon_{2n+1,2n+1}) - v_{2n+1}(\mu_{2n+1,2n+1}) &\ge p^{2n+1}e_0 - (p-1)p^{2n}u_{2n+1}.
\end{aligned}$$

It follows that

$$\begin{aligned}
v_{2n+1}(\epsilon_{1,2n+1}) - v_{2n+1}(\mu_{1,2n+1}) - p^{2n}u_1 + b_1 \ge \min\{&p^{2n+1}e_0 - p^{2n+1}u_1\\
&+ b_1,\\
&b_{2n+1} - p^{2n+1}u_1\},
\end{aligned}$$

$$v_{2n+1}(\epsilon_{2n+1,2n+1}) - v_{2n+1}(\mu_{2n+1,2n+1}) - p^{2n}u_{2n+1} + b_{2n+1} \geq p^{2n+1}e_0 - p^{2n+1}u_{2n+1} + b_{2n+1}.$$

In addition, for $2 \leq i \leq n$ we have

$$v_{2n+1}(\epsilon_{i,2n+1}) - v_{2n+1}(\mu_{i,2n+1}) - p^{2n}u_i + b_i \geq p^{2n+1}e_0 - p^{2n+1}u_i + b_i$$

and for $1 \leq i \leq n$ we have

$$\begin{aligned} &v_{2n+1}(\epsilon_{n+i,2n+1}) - v_{2n+1}(\mu_{n+i,2n+1}) - p^{2n}u_{n+i} + b_{n+i} \\ &\quad \geq \min\{p^{2n+1}e_0 - p^{2n+1}u_{n+i} + b_{n+i}, b_{2n+1} - p^{2n}u_i - p^{2n}u_{n+i}\}. \end{aligned}$$

Clearly $b_{2n+1} - p^{2n}u_i - p^{2n}u_{n+i}$ is minimized for $1 \leq i \leq n$ by taking $i = n$. It now follows from (9.7), (9.8), (9.1), and Theorem 8.2 that K_{2n+1}/K_0 has a Galois scaffold with the precision $\mathfrak{c}$ given in the statement of the theorem. □

Theorem 9.4, like Theorem 9.2, can be simplified by strengthening the hypotheses:

Corollary 9.5. *Let K_{2n+1}/K_0 be an extension constructed as in Theorem 9.4, but with (9.10)–(9.14) replaced with the single assumption $u_{2n+1} \leq e_0$. Then K_{2n+1}/K_0 is an $M(n)$-extension which has a Galois scaffold with precision*

$$\mathfrak{c} = \min\{b_{2n+1} - p^{2n+1}u_1,\ b_{2n+1} - p^{2n}u_n - p^{2n}u_{2n}\}.$$

Proof. As in the proof of Theorem 9.2, (9.15) implies $u_n + u_{2n} < u_{2n+1}$. In addition, using Corollary 2.5(b) and (9.16) we get $pu_1 < u_{2n+1}$. Combining these inequalities with $u_{2n+1} \leq e_0$ gives assumptions (9.10)–(9.14) of Theorem 9.4. Since $u_{2n+1} \leq e_0$, the inequality (9.9) holds. Therefore by Theorem 9.4 K_{2n+1}/K_0 is an $M(n)$-extension which admits a Galois scaffold with the given precision. □

Remark 9.6. Suppose $\mathrm{char}(K) = p$. In this setting, Theorem 9.2 reduces to Corollary 9.3, and Theorem 9.4 reduces to Corollary 9.5. In [12], G-extensions L/K with a Galois scaffold were constructed for an arbitrary finite p-group G. In the cases where G is an extraspecial p-group, the methods used in this paper can be used to construct all the G-extensions and scaffolds from [12], as well as many others. When a G-extension with a scaffold can be constructed by either method, the theorems in this paper assign a larger precision to the scaffold than do the theorems in [12].

10. Applications and examples

The results of the previous section can be used to get information about the Galois module structure of rings of integers. Let L/K be a finite Galois extension of local fields

and set $G = \mathrm{Gal}(L/K)$. Recall that the associated order of the ring of integers $\mathfrak{O}_L$ of L is defined to be

$$\mathfrak{A}_{L/K} = \{\lambda \in K[G] : \lambda(\mathfrak{O}_L) \subset \mathfrak{O}_L\}.$$

Theorem 10.1. *Let G be equal to either $H(n)$ or $M(n)$ for some $n \geq 1$. Let K_{2n+1}/K_0 be a totally ramified G-extension constructed using Theorem 9.2 or Theorem 9.4, so that K_{2n+1}/K_0 has a Galois scaffold with precision $\mathfrak{c}$ for some $\mathfrak{c} \geq 1$. Let $u_1 \leq \cdots \leq u_{2n+1}$ be the upper ramification numbers and $b_1 \leq \cdots \leq b_{2n+1}$ the lower ramification numbers of K_{2n+1}/K_0. Let $r(u_1)$ denote the least nonnegative residue of u_1 modulo p^{2n+1}.*

(a) If $\mathfrak{c} \geq r(u_1)$ and $r(u_1) \mid p^m - 1$ for some $1 \leq m \leq 2n+1$ then $\mathfrak{O}_{2n+1}$ is free over its associated order $\mathfrak{A}_{K_{2n+1}/K_0}$.

(b) If $\mathfrak{c} \geq 2p^{2n+1} - 1$ and $r(u_1) = p^{2n+1} - 1$ then $\mathfrak{O}_{2n+1}$ is free over $\mathfrak{A}_{K_{2n+1}/K_0}$ and $\mathfrak{A}_{K_{2n+1}/K_0}$ is a Hopf order in $K_0[G]$. Furthermore, $\mathfrak{A}_{K_{2n+1}/K_0}$ is a noncommutative local ring whose only idempotents are 0 and 1.

Proof. (a) Since $b_{2n+1} \equiv b_1 \pmod{p^{2n+1}}$ and $b_1 = u_1$ we have $r(b_{2n+1}) = r(u_1)$. Therefore the claim follows from Theorem 4.8 of [8].

(b) It follows from (a) that $\mathfrak{O}_{2n+1}$ is free over $\mathfrak{A}_{K_{2n+1}/K_0}$. Using the bound $\mathfrak{c} \geq p^{2n+1} + r(u_1)$, it is shown in the proof of Theorem 3.6 of [8] (pp. 985–6) that $\mathfrak{A}_{K_{2n+1}/K_0}$ has a unique maximal ideal $\mathfrak{M}$, that $\mathfrak{A}_{K_{2n+1}/K_0}/\mathfrak{M} \cong \mathfrak{O}_0/\mathfrak{M}_0$, and that there is $d \geq 1$ such that $\mathfrak{M}^d \subset \pi_0\mathfrak{A}_{K_{2n+1}/K_0}$. It follows that every element of $\mathfrak{A}_{K_{2n+1}/K_0} \smallsetminus \mathfrak{M}$ is a unit. Let $e \in \mathfrak{A}_{K_{2n+1}/K_0}$ be idempotent, with $e \neq 1$. Then $e \notin \mathfrak{A}^{\times}_{K_{2n+1}/K_0}$, so $e \in \mathfrak{M}$. Hence for all $t \geq 1$ we have $e = e^{td} \in \pi_0^t\mathfrak{A}_{K_{2n+1}/K_0}$. Since $\mathfrak{A}_{K_{2n+1}/K_0}$ is a free $\mathfrak{O}_0$-module, this implies $e = 0$. Therefore the only idempotents of $\mathfrak{A}_{K_{2n+1}/K_0}$ are 0 and 1, so $\mathfrak{A}_{K_{2n+1}/K_0}$ is indecomposable as a left $\mathfrak{A}_{K_{2n+1}/K_0}$-module. Since $\mathfrak{A}_{K_{2n+1}/K_0}$ is a free $\mathfrak{O}_0$-module and $\mathfrak{A}_{K_{2n+1}/K_0}/\mathfrak{O}_0[G]$ is a torsion $\mathfrak{O}_0$-module, it follows that $\mathfrak{A}_{K_{2n+1}/K_0}$ is indecomposable as a left $\mathfrak{O}_0[G]$-module. In addition, since $b_i \equiv -1 \pmod{p^{2n+1}}$ for $1 \leq i \leq 2n+1$, the different of K_{2n+1}/K_0 is generated by an element of K. It now follows from Proposition 4.5.2 of [4] that $\mathfrak{A}_{K_{2n+1}/K_0}$ is a Hopf order in $K_0[G]$. □

Example 10.2. Let $n \geq 1$ and let K_0 be a local field of characteristic 0 whose residue field $\mathfrak{O}_0/\mathfrak{M}_0$ has characteristic $p > 2$ and cardinality $\geq p^{2n}$. Let $u \geq 1$ with $p \nmid u$ and let $c \in K_0$ satisfy $v_0(c) = -u$. Let $\omega_1, \ldots, \omega_{2n}$ be elements of $\mathfrak{O}_0$ whose images in $\mathfrak{O}_0/\mathfrak{M}_0$ are linearly independent over $\mathbb{F}_p$. For $1 \leq i \leq 2n$ set $a_i = c\omega_i^{p^{2n}}$ and let α_i be a root of $X^p - X - a_i$. Define $K_1, \ldots, K_{2n}$ recursively by $K_i = K_{i-1}(\alpha_i)$ for $1 \leq i \leq 2n$. Let $t \geq 1$ and let $\omega_{2n+1} \in K_0$ satisfy $v_0(\omega_{2n+1}) = -t$. Set $a_{2n+1} = c\omega_{2n+1}^{p^{2n}}$. Then in the notation of Theorems 9.2 and 9.4 we have $u_i = b_i = u$ for $1 \leq i \leq 2n$, $u_{2n+1} = tp^{2n} + u$, and $b_{2n+1} = tp^{4n} + u$.

Now assume that $tp^{2n} + u \leq e_0$ and $2u \leq tp^{2n}$. Define B as in Theorem 9.2, let α_{2n+1} be a root of $X^p - X - (B + a_{2n+1})$, and set $K_{2n+1} = K_{2n}(\alpha_{2n+1})$. Then by

Corollary 9.3, K_{2n+1}/K_0 is an $H(n)$-extension which has a Galois scaffold with precision $\mathfrak{c} = tp^{4n} + u - 2up^{2n}$. Hence by Theorem 10.1(a) if $r(u) \mid p^m - 1$ for some m such that $1 \leq m \leq 2n+1$ then $\mathfrak{O}_{2n+1}$ is free over its associated order $\mathfrak{A}_{K_{2n+1}/K_0}$. In addition, if $r(u) = p^{2n+1} - 1$ and $2u + 2p \leq tp^{2n}$ then $\mathfrak{A}_{K_{2n+1}/K_0}$ is a Hopf order by Theorem 10.1(b). For instance, if $u = t = 1$ and $e_0 \geq p^{2n} + 1$ then $\mathfrak{O}_{2n+1}$ is free over $\mathfrak{A}_{K_{2n+1}/K_0}$, while if $u = p^{2n+1} - 1$, $t = 2p + 1$, and $e_0 \geq 3p^{2n+1} + p^{2n} - 1$ then $\mathfrak{A}_{K_{2n+1}/K_0}$ is a Hopf order.

Alternatively, we can assume that $tp^{2n} + u \leq e_0$ and $pu \leq tp^{2n}$, and define B and C as in Theorem 9.4. We let α_{2n+1} be a root of $X^p - X - (B + C + a_{2n+1})$ and set $K_{2n+1} = K_{2n}(\alpha_{2n+1})$. Then by Corollary 9.5, K_{2n+1}/K_0 is an $M(n)$-extension which has a Galois scaffold with precision $\mathfrak{c} = tp^{4n} + u - up^{2n+1}$. If $r(u) \mid p^m - 1$ for some m such that $1 \leq m \leq 2n+1$ then $\mathfrak{O}_{K_{2n+1}}$ is free over its associated order $\mathfrak{A}_{K_{2n+1}/K_0}$. In particular, if $r(u) = p^{2n+1} - 1$ and $p(u+2) \leq tp^{2n}$ then $\mathfrak{A}_{K_{2n+1}/K_0}$ is a Hopf order. For instance, if $u = t = 1$ and $e_0 \geq p^{2n} + 1$, then $\mathfrak{O}_{K_{2n+1}}$ is free over $\mathfrak{A}_{K_{2n+1}/K_0}$, while if $u = p^{2n+1} - 1$, $t = p^2 + 1$, and $e_0 \geq p^{2n+2} + p^{2n+1} + p^{2n} - 1$ then $\mathfrak{A}_{K_{2n+1}/K_0}$ is a Hopf order.

Remark 10.3. Let K be a local field of characteristic 0 with residue characteristic p, let G be a finite noncyclic p-group, and let $\mathfrak{A}$ be an $\mathfrak{O}_K$-order in $K[G]$. In Theorem 3.11 of [5] it is proved that the following are equivalent:

(i) $\mathfrak{A}$ is a Hopf algebra over $\mathfrak{O}_K$ whose $\mathfrak{O}_K$-dual $\mathfrak{A}^*$ is a local ring and a monogenic $\mathfrak{O}_K$-algebra.
(ii) $\mathfrak{A}$ contains no nontrivial idempotents and there exists a totally ramified G-extension L/K such that the different of L/K is generated by an element of K, $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$, and the associated order $\mathfrak{A}_{L/K}$ of $\mathfrak{O}_L$ is isomorphic to $\mathfrak{A}$.

It follows that if K_{2n+1}/K_0 satisfies the conditions of Theorem 10.1(b) then $\mathfrak{A}^*_{K_{2n+1}/K_0}$ is a local ring and a monogenic $\mathfrak{O}_0$-algebra. In Section 4 of [5] a method is given for constructing $H(1)$-extensions K_3/K_0 which satisfy these equivalent conditions. For every $n \geq 1$, Example 10.2 gives explicit constructions of $H(n)$-extensions and $M(n)$-extensions which satisfy these conditions.

Data availability

No data was used for the research described in the article.

References

[1] Akira Aiba, Artin-Schreier extensions and Galois module structure, J. Number Theory 102 (1) (2003) 118–124, MR 1994476.
[2] Françoise Bertrandias, Jean-Paul Bertrandias, 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, MR 296048.

[3] Françoise Bertrandias, 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, MR 296047.
[4] M.V. Bondarko, Local Leopoldt's problem for ideals in totally ramified p-extensions of complete discrete valuation fields, in: Algebraic number theory and algebraic geometry, in: Contemp. Math., vol. 300, Amer. Math. Soc., Providence, RI, 2002, pp. 27–57, MR 1936366.
[5] M.V. Bondarko, A.V. Dievskiĭ, Nonabelian associated orders in the case of wild ramification, Zap. Nauč. Semin. POMI 356 (2008), no. Voprosy Teorii Predstavleniĭ Algebr i Grupp. 17, 5–45, 189, MR 2760364.
[6] Nigel P. Byott, G. Griffith Elder, Galois scaffolds and Galois module structure in extensions of characteristic p local fields of degree p^2, J. Number Theory 133 (11) (2013) 3598–3610, MR 3084290.
[7] Nigel P. Byott, G. Griffith Elder, Sufficient conditions for large Galois scaffolds, J. Number Theory 182 (2018) 95–130, MR 3703934.
[8] Nigel P. Byott, Lindsay N. Childs, G. Griffith Elder, Scaffolds and generalized integral Galois module structure, Ann. Inst. Fourier (Grenoble) 68 (3) (2018) 965–1010, MR 3805766.
[9] Lindsay N. Childs, Cornelius Greither, Kevin P. Keating, Alan Koch, Timothy Kohl, Paul J. Truman, Robert G. Underwood, Hopf algebras and Galois module theory, Mathematical Surveys and Monographs, vol. 260, American Mathematical Society, Providence, RI, 2021, ©2021, MR 4390798.
[10] P. Deligne, Les corps locaux de caractéristique p, limites de corps locaux de caractéristique 0, Representations of reductive groups over a local field, in: Travaux en Cours, Hermann, Paris, 1984, pp. 119–157, MR 771673.
[11] G. Griffith Elder, Kevin Keating, Galois scaffolds for cyclic p^n-extensions in characteristic p, Res. Number Theory 8 (4) (2022) 75, MR 4491490.
[12] G. Griffith Elder, Kevin Keating, Galois scaffolds for p-extensions in characteristic p, Ann. Inst. Fourier (Grenoble) (2025), https://doi.org/10.5802/aif.3712.
[13] I.B. Fesenko, S.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, MR 1915966.
[14] David Goss, Basic structures of function field arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas, vol. (3), vol. 35, Springer-Verlag, Berlin, 1996, MR 1423131.
[15] Charles Helou, Non-Galois ramification theory of local fields, Algebra Berichte [Algebra Reports], vol. 64, Verlag Reinhard Fischer, Munich, 1990, MR 1076620.
[16] Charles Helou, On the ramification breaks, Commun. Algebra 19 (8) (1991) 2267–2279, MR 1123123.
[17] Kevin Keating, Paul Schwartz, Galois scaffolds and Galois module structure for totally ramified C_{p^2}-extensions in characteristic 0, J. Number Theory 239 (2022) 113–136, MR 4434489.
[18] Günter Lettl, Note on a theorem of A. Aiba, J. Number Theory 115 (1) (2005) 87–88, MR 2176484.
[19] R.E. MacKenzie, G. Whaples, Artin-Schreier equations in characteristic zero, Am. J. Math. 78 (1956) 473–485, MR 90584.
[20] Emmy Noether, Normalbasis bei Körpern ohne Höhere Verzweigung, J. Reine Angew. Math. 167 (1932) 147–152, MR 1581331.
[21] Jean-Pierre Serre, Local fields, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg, MR 554237.
[22] S.V. Vostokov, I.B. Zhukov, Some approaches to the construction of abelian extensions for $\mathfrak{p}$-adic fields, in: Proceedings of the St. Petersburg Mathematical Society, Vol. III, in: Amer. Math. Soc. Transl. Ser. 2, vol. 166, Amer. Math. Soc., Providence, RI, 1995, pp. 157–174, MR 1363296.