Galois scaffolds for cyclic $p^n$-extensions in characteristic $p$

G. Griffith Elder$^1$ and Kevin Keating$^2$*

*Correspondence: keating@ufl.edu
$^2$Department of Mathematics, University of Florida, Gainesville, FL 32611, USA
Full list of author information is available at the end of the article

Abstract
Let $K$ be a local field of characteristic $p$ and let $L/K$ be a totally ramified Galois extension such that $\text{Gal}(L/K) \cong C_{p^n}$. In this paper we find sufficient conditions for $L/K$ to admit a Galois scaffold, as defined in Byott et al (Ann Inst Fourier 68:965–1010, 2018). This leads to sufficient conditions for the ring of integers $\mathcal{O}_L$ to be free of rank 1 over its associated order $\mathcal{A}$, and to stricter conditions which imply that $\mathcal{A}$ is a Hopf order in the group ring $K[C_{p^n}]$.

1 Introduction
Let $K$ be a field of characteristic $p$. Witt [15] generalized Artin–Schreier theory by proving that cyclic extensions $L/K$ of degree $p^n$ can be described using what is now known as the ring of Witt vectors of length $n$ over $K$, denoted $W_n(K)$. The elements of $W_n(K)$ are indeed vectors with $n$ entries taken from $K$, with nonstandard operations $\oplus$, $\otimes$ which make $W_n(K)$ a commutative ring with 1. Witt showed that for a cyclic extension $L/K$ of degree $p^n$ there exists a vector $\beta \in W_n(K)$ such that $L$ is generated over $K$ by the coordinates of any solution in $W_n(K^{\text{sep}})$ to the equation $\phi(x) = x \oplus \beta$. Here $K^{\text{sep}}$ is a separable closure of $K$ and $\phi : W_n(K^{\text{sep}}) \rightarrow W_n(K^{\text{sep}})$ is the map induced by the $p$-Frobenius on $K^{\text{sep}}$. (See [6] for basic facts about Witt vectors.)

Now suppose that $K$ is a local field of characteristic $p$. In [3] the first author, in collaboration with Byott, considered totally ramified Galois extensions $L/K$ of degree $p^2$. They gave sufficient conditions on $\beta \in W_2(K)$ for the $C_{p^2}$-extension $L/K$ generated by the roots of $\phi(x) = x \oplus \beta$ to admit a Galois scaffold. In this paper we generalize that result by giving sufficient conditions on $\beta \in W_n(K)$ for the $C_{p^n}$-extension $L/K$ generated by the roots of $\phi(x) = x \oplus \beta$ to admit a Galois scaffold.

As explained in [2], a scaffold enables one to answer an array of questions all captured under the heading integral Galois module structure. By the normal basis theorem, $L$ is free of rank 1 over $K[C_{p^n}]$. An integral version of the normal basis theorem would state that the ring of integers $\mathcal{O}_L$ is free over some order $\mathcal{B}$ of $K[C_{p^n}]$. Indeed, if this holds then we must have $\mathcal{B} = \mathcal{A}$, where

$$\mathcal{A} = \{ \gamma \in K[G] : \gamma(\mathcal{O}_L) \subset \mathcal{O}_L \}$$

(1.1)
is the associated order of $\mathcal{O}_L$ in $K[G_{p^n}]$ (see Sect. 4 of [9]). The problem of determining the $\mathfrak{A}$-module structure of $\mathcal{O}_L$ is classical and appears to be difficult in general. However, when $L/K$ has a Galois scaffold with large enough precision (see Definition 1), all that one might reasonably expect is known. Indeed, everything that can be determined about integral Galois module structure in a cyclic extension of degree $p$ can be determined for an extension with a scaffold of sufficiently large precision. For instance, one can give necessary and sufficient conditions in terms of the ramification breaks of $L/K$ for $\mathcal{O}_L$ to be free over $\mathfrak{A}$. In this paper we give sufficient conditions for $\mathcal{O}_L$ to be free over $\mathfrak{A}$ (Corollary 5). We omit the technicalities needed to formulate necessary and sufficient conditions; see Sect. 3 of [2] for details. We also use scaffolds to address a different classical problem: In Corollary 6 we give sufficient conditions for $\mathfrak{A}$ to be a Hopf order in $K[G]$.

Throughout the paper we let $K$ be a field of characteristic $p$ which is complete with respect to a discrete valuation with perfect residue field. Let $K^{\text{sep}}$ be a separable closure of $K$, and for each finite subextension $F/K$ of $K^{\text{sep}}/K$ let $v_F$ be the valuation on $K^{\text{sep}}$ normalized so that $v_F(F^\times) = \mathbb{Z}$. Let $\mathcal{O}_F$ denote the ring of integers of $F$ and let $\mathcal{M}_F$ denote the maximal ideal of $\mathcal{O}_F$.

### 2 Sufficient conditions for a Galois scaffold

In this section we record the definition from [2] of a Galois scaffold for a totally ramified Galois extension $L/K$ of degree $p^n$. We then give some motivation for various technical points that appear in this definition. We conclude by stating the sufficient conditions given in [4] for $L/K$ to admit a Galois scaffold. In later sections we will use Artin–Schreier–Witt theory to construct $C_{p^n}$-extensions $L/K$ in characteristic $p$ which satisfy the conditions from [4], and therefore have Galois scaffolds.

The definition of a Galois scaffold for $L/K$ depends on the ramification data of $L/K$. Set $G = \text{Gal}(L/K)$, and for $\sigma \in G$ define $i(\sigma) = v_L(\sigma (\pi_L) - \pi_L) - 1$. Then $i(\sigma)$ does not depend on the choice of uniformizer $\pi_L$ for $L$. For $x \geq 0$ set $G_x = \{\sigma \in G : i(\sigma) \geq x\}$. Then $G_x \leq G$ is known as the $x$th ramification subgroup of $G$ with respect to the lower numbering. For $H \leq G$ we clearly have $H_x = H \cap G_x$, but the lower numbering of the ramification subgroups is not in general compatible with quotients of Galois groups. Instead we use the upper numbering, defined by $G^\times = G_{(\psi_{L/K}(x))}$, where $\psi_{L/K}$ is a certain continuous piecewise linear function associated to $L/K$. The upper numbering on ramification subgroups is compatible with quotients in the sense that $(G/H)^\times = G^\times H/H$ whenever $H \leq G$.

We say that $b$ is a lower ramification break of $L/K$ if $G_b \neq G_{b+\epsilon}$ for all $\epsilon > 0$. We say that the lower break $b$ has multiplicity $m$ if $|G_b : G_{b+\epsilon}| = p^m$. The upper ramification breaks of $L/K$ and their multiplicities are defined similarly. 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 breaks of $L/K$, counted with multiplicity. These are related by the formulas $b_1 = u_1$ and

$$b_{i+1} - b_i = p^i(u_{i+1} - u_i)$$

for $1 \leq i \leq n - 1$. See Chap. IV of [11] for proofs of these facts and more information on this topic.

In order to state the definition of a Galois scaffold we introduce some notation from Sect. 2 of [2]. As above we let $L/K$ be a totally ramified Galois extension with lower ramification breaks $b_1 \leq b_2 \leq \cdots \leq b_n$. Assume that $p \nmid b_i$ for $1 \leq i \leq n$. Set $S_{p^n} = \{0, 1, \ldots, p^n - 1\}$.
and write $s \in \mathbb{S}_{p^n}$ in base $p$ as

$$s = s(0)p^0 + s(1)p^1 + \cdots + s(n-1)p^{n-1}$$

with $0 \leq s(i) < p$. Define $b : \mathbb{S}_{p^n} \to \mathbb{Z}$ by

$$b(s) = s(0)p^0b_n + s(1)p^1b_{n-1} + \cdots + s(n-1)p^{n-1}b_1.$$

Let $r : \mathbb{Z} \to \mathbb{S}_{p^n}$ be the function which maps $t \in \mathbb{Z}$ onto its least nonnegative residue modulo $p^n$. The function $r \circ (-b) : \mathbb{S}_{p^n} \to \mathbb{S}_{p^n}$ is a bijection since $p \nmid b_1$. Therefore we may define $a : \mathbb{S}_{p^n} \to \mathbb{S}_{p^n}$ to be the inverse of $r \circ (-b)$. We extend $a$ to a function from $\mathbb{Z}$ to $\mathbb{S}_{p^n}$ by setting $a(t) = a(r(t))$ for $t \in \mathbb{Z}$.

The following is a specialization of the general definition of “$A$-scaffold” given in Definition 2.3 of [2]:

**Definition 1** ([2], Definition 2.6) Let $c \geq 1$. A Galois scaffold $(\{|\Psi_i\}, \{\lambda_i\})$ for $L/K$ with precision $c$ consists of elements $\Psi_i \in K[G]$ for $1 \leq i \leq n$ and $\lambda_i \in L$ for all $t \in \mathbb{Z}$ such that the following hold:

(i) $\Psi_i(\lambda_i) = t$ for all $t \in \mathbb{Z}$.
(ii) $\lambda_i\lambda_j^{-1} \in K$ whenever $t_1 \equiv t_2 \pmod{p^n}$.
(iii) $\Psi_i(1) = 0$ for $1 \leq i \leq n$.
(iv) For each $1 \leq i \leq n$ and $t \in \mathbb{Z}$ there exists $u_{it} \in O_K^c$ such that the following congruence modulo $\lambda_{t+i}p^n \rightarrow \mathbb{A}_L$ holds:

$$\Psi_i(\lambda_i) \equiv \begin{cases} u_{it}\lambda_i^{p^n-i}b_i & \text{if } a(t)_{(n-t)} \geq 1, \\ 0 & \text{if } a(t)_{(n-t)} = 0. \end{cases}$$

As Definition 1 is technical and it is unclear what the functions $a, b$ represent, we recall and elaborate upon the intuition of a scaffold given in the introduction of [2]. Given integers $\{d_i\}_{1 \leq i \leq n}$ relatively prime to $p$, choose elements $X_i \in L$ such that $\psi_L(X_i) = p^n - d_i$. Then the $L$-valuations of the monomials

$$X^a = X_n^{a(n)}X_{n-1}^{a(n-1)} \cdots X_1^{a(1)}$$

for $0 \leq a_i < p$ provide a complete set of residues modulo $p^n$. Since $L/K$ is totally ramified of degree $p^n$, these monomials form a $K$-basis for $L$. Of course, the action of $K[G]$ on $L$ is determined by its action on any $K$-basis. So if there were elements $\Psi_i \in K[G]$ for $1 \leq i \leq n$ that acted on $X^a$ as differential operators $d/dX_i$ (with $X_i$ independent variables),

$$\Psi_i X^a = a_n(\Psi_iX^a)/X_i$$

then the monomials in the $\Psi_i$ with exponents $< p$ would provide a $K$-basis for $K[G]$ whose effect on $X^a$ (and thus on any element expressed in terms of the $X^a$) would be easy to determine. As a consequence, the determination of $\Psi_i$ and the structure of $O_L$ over $\mathbb{A}$ would be reduced to a purely numerical calculation involving the $d_i$. This remains true if (2.2) is replaced by the congruence

$$\Psi_i X^a \equiv a_n(\Psi_iX^a)/X_i \pmod{(X^a/X_i)M_L}$$

for a sufficiently large precision $c$.

Of course, one cannot expect to find $\Psi_i \in K[G]$ acting in this manner on $X^a$ for arbitrary integers $d_i$ and arbitrary $X_i \in L$ satisfying $\psi_L(X_i) = p^n - d_i$. So for guidance, we turn to
cyclic extensions $L/K$ of degree $p$ where Galois scaffolds arise naturally. In this case we have $\text{Gal}(L/K) = \langle \sigma \rangle$ and $\Psi_l = \sigma - 1$ increases valuations by the ramification break $b_1$ (see Example 2.8 in [2]). Since the intuition suggests that the exponent of $X_1$ should be decreased by application of $\Psi_l$, we set $d_i = -b_i$ and choose $X_1$ to satisfy $v_L(X_1) = -b_1$.

More generally, for $L/K$ of degree $p^n$, we let $d_i = -b_i$ and $v_L(X_i) = -p^{n-1}b_i$. This means that

$$v_L(X_n^s(X_{n-1}^{s(1)} \cdots X_1^{s(n-1)}) = -b(s)$$

where $s = s(0)p^0 + s(1)p^1 + \cdots + s(n-1)p^{n-1}$ is the base-$p$ expression for the exponent. Furthermore, $a(t) = \sum_{i=1}^n a_{(n-i)p^{n-1}}$ is chosen to satisfy

$$v_L(X_n^{a(t)}) = -a(0)bnp^0 - a_1b_{n-1}p^1 - \cdots - a_{(n-1)}b_1p^{n-1} = -b(a(t)) \equiv t \pmod{p^n}.$$ 

The condition $a(t)_{(n-i)} \geq 1$ in Definition 1 can now be interpreted to mean that the element $X_i$ appears with exponent $\geq 1$ in the monomial $X_i^{a(t)}$ that represents $\lambda_i$, and thus is available to be removed. In [4], the monomials $X_i^{a(t)}$ enter explicitly, but they are constructed using falling factorials rather than exponentials.

To prove that certain $C_{p^n}$-extensions admit Galois scaffolds we will use a theorem from [4]. In order to state this theorem we introduce notation from Sect. 2 of [4]. Let $L/K$ be a totally ramified $C_{p^n}$-extension whose lower ramification breaks satisfy $b_i \equiv b_1 \pmod{p^n}$ for $1 \leq i \leq n$. Let $1 \leq j \leq n$. Since $\text{Gal}(L/K)$ is a cyclic $p$-group, $\langle \sigma^j \rangle$ is necessarily a ramification subgroup of $\text{Gal}(L/K)$. Let $K_j$ denote the fixed field of $\langle \sigma^j \rangle$. Then the upper ramification breaks of $K_j/K$ are $u_1, u_2, \ldots, u_j$, and the lower ramification breaks are $b_1, b_2, \ldots, b_j$ (see Sect. 4 in Chap. IV of [11]). Let $Y_j \in K_j$ satisfy $v_{K_j}(Y_j) = -b_j$. Since $p \nmid b_j$ we have $v_{K_j}((\sigma^j - 1)(Y_j)) = b_j - b_j = 0$. Hence there is $c_j \in O_K^\times$ such that $X_j = c_jY_j$ satisfies $(\sigma^{j-1} - 1)(X_j) \equiv 1 \pmod{M_K}$. For $1 \leq j < i \leq n$ we have $(\sigma^{j-1} - 1)(X_j) = 0$. We have $v_{K_j}(X_j) = -b_j$, so for $1 \leq i \leq n$ we get $v_{K_j}((\sigma^{j-1} - 1)(X_j)) = b_i - b_j$. Since $p^n \mid b_i - b_j$ there are $\mu_{ij} \in K$ and $\epsilon_{ij} \in K$ such that

$$(\sigma^{j-1} - 1)(X_j) = \mu_{ij} + \epsilon_{ij}$$

and $b_i - b_j = v_{K_j}(\mu_{ij}) < v_{K_j}(\epsilon_{ij})$. One views $\mu_{ij}$ as the “main term” and $\epsilon_{ij}$ as the “error term” in our representation of $(\sigma^{j-1} - 1)(X_j)$. The following theorem says that if the error terms are sufficiently small compared to the main terms then $L/K$ admits a Galois scaffold.

**Theorem 1** Let $\text{char}(K) = p$ and let $L/K$ be a totally ramified $C_{p^n}$-extension whose lower ramification breaks $b_1 < b_2 < \cdots < b_n$ satisfy $b_i \equiv b_1 \pmod{p^n}$ for $1 \leq i \leq n$. Denote the upper ramification breaks of $L/K$ by $u_1 < u_2 < \cdots < u_n$ and define $\mu_{ij}, \epsilon_{ij}$ as in (2.3). Suppose there is $\epsilon \geq 1$ such that for $1 \leq i \leq j \leq n$ we have

$$v_{L}(\epsilon_{ij}) - v_{L}(\mu_{ij}) \geq p^{n-1}u_i - p^{n-1}b_i + \epsilon.$$ 

Then $L/K$ has a Galois scaffold with precision $\epsilon$.

**Proof** This follows by specializing Theorem 2.10 of [4] to our setting. Note that the hypothesis $p \nmid b_1$ from [4] holds automatically since $\text{char}(K) = p$. \qed
Remark 1 Using Lemma 1 below we get \( p^{n-1}u_i - p^{n-j}b_i \geq p^{n-1}u_i - p^{n-j}b_i \geq 0 \) for \( 1 \leq i \leq j \leq n \). In particular, we have \( p^{n-1}u_i - p^{n-j}b_i = 0 \) if and only if \( i = j = 1 \).

3 A normal basis generator for \( L/K \)

In this section we study a certain class of \( C_{p^n} \)-extensions, which we construct using Artin–Schreier–Witt theory. For each such extension \( L/K \) we give an element \( Y \in L \) that satisfies \( v_L(Y) = -b_j \mod p^n \). Since \( L/K \) is abelian, \( Y^{-1} \) satisfies the “valuation criterion” for a normal basis generator and therefore generates a normal basis for \( L/K \) [13]. In Sects. 4 and 5 we will use \( Y \) (and similar elements associated to the subextensions \( K_j/K \) of \( L/K \)) to show that \( L/K \) admits a Galois scaffold. Our class of extensions is defined by the conditions (3.1), (3.2), and (3.3) given below. These conditions are quite restrictive, which is not surprising since extensions which admit a Galois scaffold are generally quite rare. However, it is easy to produce many examples of \( C_{p^n} \)-extensions which satisfy our conditions, and therefore admit a Galois scaffold.

In the notation of Sect. 2 we could write \( L = K_n \), in which case it would make sense to call our normal basis generator \( Y_n \). We have chosen not to do this in order to simplify the notation.

Let \( L/K \) be a finite totally ramified Galois subextension of \( K_{sep}/K \), with \( \text{Gal}(L/K) \cong C_{p^n} \). Let \( W_n(K) \) denote the ring of Witt vectors of length \( n \) over \( K \) and let \( \beta \in W_n(K) \) be a Witt vector which corresponds to \( L/K \) under Artin–Schreier–Witt theory. For \( 0 \leq i \leq n - 1 \) let \( \beta_i \) denote the \( i \)th coordinate of \( \beta \). We may assume without loss of generality that \( \beta \) is reduced in the sense of Proposition 4.1 from [12]. This means that for each \( 0 \leq i \leq n - 1 \) we have either \( v_K(\beta_i) \geq 0 \) or \( p \nmid v_K(\beta_i) \). Define \( \phi : K_{sep} \to K_{sep} \) by \( \phi(x) = x^p \). Then \( \phi \) induces a map from \( W_n(K) \) to itself by acting on coordinates. Let \( x \in W_n(K_{sep}) \) satisfy \( \phi(x) = x \oplus \beta \), where \( \oplus \) denotes Witt vector addition. Then \( L = K(x_0, x_1, \ldots, x_{n-1}) \) and there is a generator \( \sigma \) for \( \text{Gal}(L/K) \cong C_{p^n} \) such that \( \sigma(x) = x \oplus 1 \), where \( 1 \in W_n(K) \) is the multiplicative identity.

Since \( L/K \) is a totally ramified \( C_{p^n} \)-extension we have \( v_K(\beta_0) < 0 \). Set \( \beta = \beta_0 \) and assume there are \( \omega_i, \delta_i \in K \) such that

\[
\beta_i = \beta \omega_i^{p^{n-1}} + \delta_i, \quad v_K(\delta_i) > v_K(\beta_i)
\]

(3.1)

for \( 0 \leq i \leq n - 1 \). Note that \( \omega_0 = 1 \) and \( \delta_0 = 0 \). As in [3,7] we view \( \beta \omega_i^{p^{n-1}} \) as the “main term” of \( \beta_i \), and \( \delta_i \) as the “error term”. Let \( \omega \in K^n \) be the vector of \( \omega_i \)'s, let \( \delta \in K^n \) be the vector of \( \delta_i \)'s, and set \( d = (x \oplus \beta) - x - \beta \). We get \( \beta = \beta \phi^{n-1}(\omega) + \delta + d \) and

\[
\begin{align*}
\beta & = \begin{bmatrix}
\beta_0 \\
\beta_1 \\
\vdots \\
\beta_{n-1}
\end{bmatrix} \\
\beta_0 & = \beta \omega_0^{p^{n-1}} + \delta_0 \\
\beta_1 & = \beta \omega_1^{p^{n-1}} + \delta_1 \\
\vdots & = \vdots \\
\beta_{n-1} & = \beta \omega_{n-1}^{p^{n-1}} + \delta_{n-1}
\end{align*}
\]

\[
\omega = \begin{bmatrix}
\omega_0 \\
\omega_1 \\
\vdots \\
\omega_{n-1}
\end{bmatrix} \\
\delta = \begin{bmatrix}
\delta_0 \\
\delta_1 \\
\vdots \\
\delta_{n-1}
\end{bmatrix}
\]

\[
dx = \begin{bmatrix}
x_0 \\
x_1 \\
\vdots \\
x_{n-1}
\end{bmatrix} \\
d = \begin{bmatrix}
d_0 \\
d_1 \\
\vdots \\
d_{n-1}
\end{bmatrix}
\]

Since \( \phi(x) = x + \beta \phi^{n-1}(\omega) + \delta + d \) we have \( x_i^p - x_i = \beta \omega_i^{p^{n-1}} + \delta_i + d_i \) for \( 0 \leq i \leq n - 1 \).
We assume throughout that the following hold for $1 \leq i \leq n - 1$:

\begin{align*}
    b_{i+1}^j > p^ju_i \quad (3.2) \\
    b_{i+1}^j > -p^{n-1}v_K(\delta_i) \quad (3.3)
\end{align*}

It follows from the (well-known) Lemma 1 below that $p^ju_{i+1}^j \geq b_{i+1}^j$. Hence $(3.2)$ implies the weaker condition

\begin{equation}
    u_{i+1}^j > pu_i^j, \quad (3.4)
\end{equation}

which is sufficient for most of the steps of our argument. This last inequality is equivalent to the statement that the sequence $(p^ju_i^j)_{0 \leq i \leq n-1}$ is strictly increasing.

**Lemma 1** Let $1 \leq j \leq n$. Then $b_j \leq p^j u_j$, with equality if and only if $j = 1$.

**Proof** If $j > 1$ then by $(2.1)$ we get

\begin{align*}
    p^j u_j^j - b_j &= p^j u_j^j - b_1 - \sum_{h=1}^{j-1} (b_{h+1}^j - b_h) \\
    &= p^j u_j^j - u_1 - \sum_{h=1}^{j-1} p^h (u_{h+1}^j - u_h) \\
    &= \sum_{h=1}^{j-1} (p^h - p^{h-1})u_h > 0.
\end{align*}

\[\square\]

For $0 \leq i \leq n - 1$ let $S_i \in \mathbb{Z}[X_0, \ldots, X_i, Y_1, \ldots, Y_i]$ be the $i$th Witt vector addition polynomial. Then addition in $W_n$ is given by

\[
\begin{bmatrix}
    X_0 \\
    X_1 \\
    \vdots \\
    X_{n-1}
\end{bmatrix}
\oplus
\begin{bmatrix}
    Y_0 \\
    Y_1 \\
    \vdots \\
    Y_{n-1}
\end{bmatrix}
= 
\begin{bmatrix}
    S_0 \\
    S_1 \\
    \vdots \\
    S_{n-1}
\end{bmatrix}
\]

and $S_i$ is defined in terms of $S_0, \ldots, S_{i-1}$ by the recursion formula

\begin{equation}
    S_i = p^{-i} \left( \sum_{j=0}^{i} p^j (X_j^{p^j} + Y_j^{p^j}) - \sum_{j=0}^{i-1} p^j S_j^{p^j} \right). \quad (3.5)
\end{equation}

Hence $S_i = X_i + Y_i + D_i$, with $D_i \in \mathbb{Z}[X_0, \ldots, X_{i-1}, Y_0, \ldots, Y_{i-1}]$. In particular, $S_0 = X_0 + Y_0$ and $D_0 = 0$. We will use the following elementary fact about $D_i$:

**Lemma 2** Every monomial in $D_i$ has a factor $X_h$ for some $0 \leq h \leq i - 1$, and a factor $Y_h$ for some $0 \leq h \leq i - 1$.

**Proof** Since $0$ is the identity element for the operation $\oplus$ on $W_n$, the only term of $S_i$ not divisible by some $X_h$ is $Y_i$, and the only term of $S_i$ not divisible by some $Y_h$ is $X_i$. \[\square\]

**Lemma 3** Let $K'/K$ be a ramified $C_p$-extension and let $L/K$ be a finite totally ramified Galois extension of degree $p^i$ such that $K' \not\subseteq L$. Let $w$ be the upper ramification break of
\( K' / K \) and let \( u_1 \leq \cdots \leq u_i \) be the upper ramification breaks of \( L / K \). Set \( L' = K' L \) and assume that the upper ramification breaks of \( L' / K \) have the form \( u_1 \leq \cdots \leq u_i < u_{i+1} \). Then \( w = u_{i+1} \).

**Proof** Since the upper break \( w \) of \( K' / K \) is inherited by \( L' / K \) we have \( w \leq u_{i+1} \). Suppose \( w < u_{i+1} \). Set \( G = \text{Gal}(L'/K), H = \text{Gal}(L'/K) \), and \( N = \text{Gal}(L'/L) \). Then \( G = H \times N \). Using our assumptions about the upper breaks and basic facts about ramification groups we get

\[
[1] = (G/H)^{u_{i+1}} = G^{u_{i+1}} H / H
\]

\[
[1] = (G/N)^{u_{i+1}} = G^{u_{i+1}} N / N.
\]

Therefore \( G^{u_{i+1}} \subset H \cap N = \{1\} \), so \( G^{u_{i+1}} = \{1\} \). This contradicts the assumption that \( u_{i+1} \) is an upper ramification break of \( L' / K \), so we must have \( u_{i+1} = w \). \( \square \)

For the proof of the next lemma we let \( \overline{S}_i, \overline{D}_i \) denote the reductions modulo \( p \) of \( S_i, D_i \). Recall that \( K_i \) denotes the fixed field of \( \langle \sigma^p \rangle \) acting on \( L \). Thus \( K_0 = K \), \( K_n = L \), and \( K_i = K(x_0, x_1, \ldots, x_{i-1}) \) for \( 0 \leq i \leq n \).

**Lemma 4** (a) \( v_K(d_i) > -pu_i \) for \( 1 \leq i \leq n - 1 \).
(b) \( v_K(\beta_i) = -u_{i+1} \) and \( v_K(x_i) = -p^{-1} u_{i+1} \) for \( 0 \leq i \leq n - 1 \).

**Proof** We use strong induction on \( i \). Let \( 1 \leq i \leq n - 1 \) and assume the lemma holds for \( 0 \leq j < i \). In \( W_i(k_{sep}) \) we have \( d = x \oplus \beta - x - \beta \), and hence

\[
d_i = \overline{D}_i(x_0, x_1, \ldots, x_{i-1}, \beta_0, \beta_1, \ldots, \beta_{i-1}).
\]

Let \( 0 \leq j \leq i - 1 \). Then by the inductive hypotheses and (3.4) we get

\[
v_K(\beta_i) = -u_{i+1} \geq -p^{j+i+1} u_j = p^{-j-i} (-pu_i).
\]

\[
v_K(x_i) = -p^{-1} u_{i+1} \geq -p^{j-i} u_j > p^{-j-i} (-pu_i).
\]

If we assign \( X_j \) and \( Y_j \) the weight \( p^j \) then an inductive argument based on (3.5) shows that \( \overline{S}_i \) and \( \overline{D}_i \) are isobaric of weight \( p^j \). Using (3.6), (3.7), and Lemma 2 we deduce that each term of \( d_i \) has \( K \)-valuation greater than \(-pu_i \). It follows that \( v_K(d_i) > -pu_i \), which proves (a).

To prove (b), let \( y \) be a root of \( X^p - X - d_i \) and let \( z \) be a root of \( X^p - X - \beta_i \) such that \( y + z = x_i \). Then \( K_i(y) \), like \( K_i(x_i) = K_{i+1} \), is a \( C_{p^{i+1}} \)-extension of \( K \). The unique (lower and upper) ramification break of the \( C_p \)-extension \( K_i(x_i)/K_i \) is \( b_{i+1} \), while the ramification break \( b'_{i+1} \) of \( K_i(y)/K_i \) satisfies \( b'_{i+1} \leq -v_{K_i}(d_i) \). Using (a) and (3.2) we get \( b'_{i+1} < p^{j+i+1} u_i < b_{i+1} \). Therefore \( K_i(y, z)/K_i \) is a \( C_{p^2} \)-extension with upper ramification breaks \( b'_{i+1}, b_{i+1} \). It follows from Lemma 3 that the ramification break of \( K_i(z)/K_i \) is \( b_{i+1} \). Since \( u_{i+1} = u_i + p^{-i} (b_{i+1} - b_i) \) we deduce that \( K_i(z)/K \) has upper ramification breaks \( u_1 < \cdots < u_i < u_{i+1} \). It follows from Lemma 3 that the ramification break of the \( C_p \)-extension \( K(z)/K \) is \( u_{i+1} \). Hence \( v_K(\beta_i) = -u_{i+1} \). Using (a) and (3.4) we get \( v_K(d_i) > -pu_i > -u_{i+1} = v_K(\beta_i) \), and hence \( v_K(d_i + \beta_i) = v_K(\beta_i) < 0 \). Therefore \( v_K(x_i) = p^{-1} v_K(\beta_i) = -p^{-1} u_{i+1} \). \( \square \)
It follows from the assumption $v_K(\delta_{i-1}) > v_K(\beta_{i-1})$ that $v_K(\beta_0\omega_{i-1}^n) = v_K(\beta_{i-1}) = -u_i$ for $1 \leq i \leq n$. Setting $v_K(\omega_i) = -m_i$ we get $u_1 = b_1$ and $u_i = b_1 + p^{n-1}m_{i-1}$ for $2 \leq i \leq n$. It follows that
\[
-v_K(\omega_i) = m_i = p^{-n+1}(u_{i+1} - u_1) > 0
\]
for $0 \leq i \leq n - 1$. Define
\[
Y = \det([x, \omega, \phi(\omega), \ldots, \phi^{n-2}(\omega)]).
\]

**Lemma 5** For $0 \leq i < n$ let $t_i \in K$ be the $(i, 0)$ cofactor of $(3.9)$. Then

(a) $Y = t_0x_0 + t_1x_1 + \cdots + t_{n-1}x_{n-1}$.
(b) $v_K(t_0) = -m_1 - pm_2 - \cdots - p^{n-2}m_{n-1}$.
(c) For $0 \leq i < j \leq n - 1$ we have $v_K(t_j) - v_K(t_i) = p^{-n}(b_{j+1} - b_{i+1})$.

**Proof** Statement (a) is just the expansion of $Y$ in cofactors along column 0. Keeping in mind that $\omega_0 = 1$ and $0 = m_0 < m_1 < \cdots < m_{n-1}$ we see that for $0 \leq i \leq n - 1$ we have
\[
v_K(t_i) = v_K(\omega_0\omega_1^1 \omega_2^2 \cdots \omega_{i-1}^{i-1} \omega_{i+1} \cdots \omega_{n-1}^{n-2})
\]
\[
= -m_0 - pm_1 - p^2m_2 - \cdots - p^{i-1}m_{i-1} - p^im_{i+1} - \cdots - p^{n-2}m_{n-1}.
\]

(3.10)

In particular, we have
\[
v_K(t_0) = -m_1 - pm_2 - \cdots - p^{n-2}m_{n-1},
\]
which is (b). Using (3.10), (3.8), and (2.1) we get
\[
v_K(t_j) - v_K(t_{j-1}) = p^{j-1}(m_j - m_{j-1})
\]
\[
= p^{-n}(u_{j+1} - u_j)
\]
\[
= p^{-n}(b_{j+1} - b_j).
\]

It follows that for $0 \leq i < j \leq n - 1$ we have $v_K(t_j) - v_K(t_i) = p^{-n}(b_{j+1} - b_{i+1})$, which gives (c).

By Lemmas 5(c) and 4(b), for $1 \leq i \leq n - 1$ we get
\[
v_L(t_{i-1}x_{i-1}) - v_L(t_ix_i) = -(b_{i+1} - b_i) + p^{n-1}(u_{i+1} - u_i)
\]
\[
= -p^i(u_{i+1} - u_i) + p^{n-1}(u_{i+1} - u_i)
\]
\[
\geq 0,
\]
with equality if and only if $i = n - 1$. It follows that
\[
v_L(t_{n-1}x_{n-1}) = v_L(t_{n-2}x_{n-2}) < v_L(t_{n-3}x_{n-3}) < \cdots < v_L(t_0x_0).
\]

Therefore we cannot compute $v_L(Y)$ directly from Lemma 5(a). Instead we use an inductive argument based on properties of the determinant:

**Proposition 1** Let $L/K$ be a $C_{p^n}$-extension which satisfies assumptions (3.1), (3.2), and (3.3), and define $Y$ as in (3.9). Then $L = K(Y)$ and
\[
v_L(Y) = -b_1 - p^nm_1 - p^{n+1}m_2 - \cdots - p^{2n-2}m_{n-1}.
\]
Proof. Since \( x_i \in L \) and \( \omega_i \in K \) for \( 0 \leq i \leq n - 1 \) we have \( Y \in L \). We claim that for \( 0 \leq i \leq n - 1 \) we have
\[
\phi^i(Y) = \det([x + d + \ldots + \phi^i(d) + \delta + \ldots + \phi^i(\delta), \phi(\omega), \ldots, \phi^{i+n-2}(\omega)]).
\]  
(3.12)

The case \( i = 0 \) is given by (3.9). Let \( 0 \leq i \leq n - 2 \) and assume that (3.12) holds for \( i \). Then
\[
\phi^{i+1}(Y) = \phi(\det([x + d + \ldots + \phi^i(d) + \delta + \ldots + \phi^i(\delta), \phi(\omega), \ldots, \phi^{i+n-2}(\omega)]))
= \det([\phi(x) + \phi(d) + \ldots + \phi^i(d) + \phi(\delta) + \ldots + \phi^i(\delta), \phi^i(\omega), \ldots, \phi^{i+n-1}(\omega)])
= \det([x + \beta \phi^{i-1}(\omega) + \delta + d + \phi(d) + \ldots + \phi^i(d) + \phi(\delta) + \ldots + \phi^i(\delta),
\phi^{i+1}(\omega), \ldots, \phi^{i+n-1}(\omega)]).
\]

Since \( i + 1 \leq n - 1 \) it follows that
\[
\phi^{i+1}(Y) = \det([x + d + \phi(d) + \ldots + \phi^i(d) + \delta + \phi(\delta) + \ldots
+ \phi^i(\delta), \phi^{i+1}(\omega), \ldots, \phi^{i+n-1}(\omega)]).
\]
Hence (3.12) holds with \( i \) replaced by \( i + 1 \). It follows by induction that (3.12) holds for \( i = n - 1 \). Therefore we have
\[
\phi^n(Y) = \phi(\det([x + d + \ldots + \phi^{n-2}(d) + \delta + \ldots + \phi^{n-2}(\delta), \phi^{n-1}(\omega), \ldots, \phi^{2n-3}(\omega)]))
= \det([\phi(x) + \phi(d) + \ldots + \phi^{n-1}(d) + \phi^{n-1}(\delta), \phi^n(\omega), \ldots, \phi^{2n-2}(\omega)])
= \det([x + \beta \phi^{n-1}(\omega) + d + \phi(d) + \ldots + \phi^{n-1}(d) + \delta + \phi(\delta) + \ldots + \phi^{n-1}(\delta),
\phi^n(\omega), \ldots, \phi^{2n-2}(\omega)]).
\]  
(3.13)

Observe that the \((i, 0)\) cofactor of (3.13) is \( t_i^n \), where \( t_i \) is the \((i, 0)\) cofactor of (3.9), as in Lemma 5. Therefore
\[
Y^{p^n} = t_0^{p^n}(x_0 + \beta) + \sum_{i=1}^{n-1} t_i^{p^n} \left( x_i + \beta \omega_i^{p^n-1} + \sum_{j=0}^{n-1} (\delta_i^p + \delta_i^{p^n}) \right).
\]  
(3.14)

Using Lemma 5(b) we get
\[
v_K(t_0^{p^n} \beta) = v_K(\beta) + p^n v_K(0)
= -b_1 - p^n m_1 - p^{n+1} m_2 - \ldots - p^{2n-2} m_{n-1}.
\]

To prove the proposition it suffices to show that the other terms in (3.14) all have \( K \)-valuation greater than \( v_K(t_0^{p^n} \beta) \).

We begin by showing that \( v_K(t_i^{p^n} \cdot \beta \omega_i^{p^n-1}) > v_K(t_0^{p^n} \beta) \) for \( 1 \leq i \leq n - 1 \). In fact, by Lemma 5(c) and (3.8) we have
\[
v_K(t_i^{p^n} \omega_i^{p^n-1}) - v_K(t_0^{p^n}) = p^n(v_K(t_i) - v_K(t_0)) + p^{n-1} v_K(\omega_i)
= (b_{i+1} - b_1) - (u_{i+1} - u_1)
= b_{i+1} - u_{i+1} > 0.
\]

Hence \( v_K(t_i^{p^n} \cdot \beta \omega_i^{p^n-1}) > v_K(t_0^{p^n} \beta) \).
Let $0 \leq i \leq n - 1$. By Lemma 4(b) we have $v_K(x_i) = p^{-1}v_K(\beta_i) > v_K(\beta_i)$. It follows from the preceding paragraph that

$$v_K(t_i^m x_i) > v_K(t_i^m \beta_i) = v_K(t_i^m : \beta \omega_i^{p^{m-1}}) > v_K(t_0^m \beta).$$

By Lemma 5(c) and assumption (3.3) we get

$$v_K(t_i^m \delta_i^j) - v_K(t_0^m \beta) = p^n(v_K(t_i) - v_K(t_0)) + p^i v_K(\delta_i) - v_K(\beta)
\quad = b_{i+1} - b_1 + p^i v_K(\delta_i) - (-b_1)
\quad = b_{i+1} + p^i v_K(\delta_i) > 0$$

for $0 \leq i, j \leq n - 1$. Hence $v_K(t_i^m \delta_i^j) > v_K(t_0^m \beta)$.

It remains to show that $v_K(t_i^m \delta_i^j) > v_K(t_0^m \beta)$ for $1 \leq i, j \leq n - 1$. By Lemma 5(c), Lemma 4(a), and assumption (3.2) we have

$$v_K(t_i^m \delta_i^j) - v_K(t_0^m \beta) = p^n(v_K(t_i) - v_K(t_0)) + p^i v_K(\delta_i) - v_K(\beta)
\quad > (b_{i+1} - b_1) - p^{i+1}u_i + b_1
\quad = b_{i+1} - p^{i+1}u_i > 0.$$

Hence $v_K(t_i^m \delta_i^j) > v_K(t_0^m \beta)$. It follows that

$$v_L(Y) = p^n v_K(Y) = v_K(Y^m) = v_K(t_0^m \beta).$$

The formula for $v_L(Y)$ given in the statement of the proposition now follows from (3.11). Since $p \nmid v_L(Y)$ we get $L = K(Y)$. □

For later use we record the following variant of Proposition 1:

**Corollary 1** $v_L(Y) = v_L(t_n - 1) - b_n$

**Proof** By (3.15) and Lemma 5(c) we have

$$v_L(Y) - v_L(t_n - 1) = p^n v_K(t_0) + v_K(\beta) - v_L(t_n - 1)
\quad = v_K(\beta) + p^n v_K(t_0) - p^n v_K(t_n - 1)
\quad = -b_1 - (b_n - b_1) = -b_n.$$

□

It follows from the proposition that $Y^{-1}$ is a “valuation criterion” element of $L$, and hence generates a normal basis for $L/K$.

**Corollary 2** \{ $\sigma(Y^{-1}) : \sigma \in \text{Gal}(L/K)$ \} is a $K$-basis for $L$.

**Proof** Since $t_{n-1} \in K$ the previous corollary implies that $v_L(Y) \equiv -b_n$ (mod $p^n$). Hence $v_L(Y^{-1}) \equiv b_n$ (mod $p^n$), so the claim follows from Theorem 2 of [13]. □
4 The Galois action on $Y$

The goal of this section is to approximate $(\sigma^p - 1)(Y)$ for $0 \leq i \leq n - 1$. In the next section we will use these approximations together with Theorem 1 to get a Galois scaffold for $L/K$.

Since $(\sigma^p - 1)(x_i) = 0$ for $0 \leq j \leq i - 1$, it follows from Lemma 5(a) that

$$(\sigma^p - 1)(Y) = (\sigma^p - 1)(t_0x_0 + t_1x_1 + \cdots + t_{n-1}x_{n-1}) = t_i(\sigma^p - 1)(x_i) + \cdots + t_{n-1}(\sigma^p - 1)(x_{n-1}). \quad (4.1)$$

Therefore to approximate $(\sigma^p - 1)(Y)$ it suffices to approximate $(\sigma^p - 1)(x_i)$ for $i \leq j \leq n - 1$. To do this we will use the following two facts about Witt vectors.

**Lemma 6** For $0 \leq i \leq j$, let $S_j$ be the $j$th Witt addition polynomial over $\mathbb{Z}$. Then the coefficient of $X_i^{p-1}X_{i+1}^{p-1} \cdots X_{j-1}^{p-1}Y_i$ in $S_j$ is $(-1)^{j-i}$.

**Proof** We fix $i$ and use induction on $j$. For $j = i$ the coefficient of $Y_i$ in $S_i$ is $1 = (-1)^{i-i}$.

Let $j \geq i + 1$ and assume that the claim holds for $j - 1$. Since $S_j$ does not depend on $X_j$ for $0 \leq h \leq j - 2$, the only summand in the recursion formula

$$S_j = p^{-j}\left( \sum_{h=0}^{j} p^h(X_i^{p-h} + Y_i^{p-h}) - \sum_{h=0}^{j-1} p^h S_j^{p-h} \right), \quad (4.2)$$

that can include the term $X_i^{p-1}X_{i+1}^{p-1} \cdots X_{j-1}^{p-1}Y_i$ is $-p^{-1}S_{j-1}$. We have $S_{j-1} = X_{j-1} + \gamma$, where $\gamma$ does not depend on $X_{j-1}$. Hence

$$S_{j-1}^p = \sum_{h=0}^{p} \binom{p}{h} X_{j-1}^{h} \gamma^{p-h},$$

and the only summand on the right that can include the term $X_i^{p-1}X_{i+1}^{p-1} \cdots X_{j-1}^{p-1}Y_i$ is $\left( \binom{p}{p-1} \right) X_{j-1}^{p-1} \gamma^1$. By the inductive assumption, the coefficient of $X_i^{p-1}X_{i+1}^{p-1} \cdots X_{j-2}^{p-1}Y_i$ in $\gamma$ is $(-1)^{j-1-i}$. Hence the coefficient of $X_i^{p-1}X_{i+1}^{p-1} \cdots X_{j-1}^{p-1}Y_i$ in $S_j$ is

$$-\frac{1}{p} \left( \binom{p}{p-1} \right) (-1)^{j-1-i} = (-1)^{j-i}.$$

$$\square$$

**Lemma 7** For $0 \leq i \leq j$, let $E_{ij}$ be the polynomial obtained from

$$D_j = S_j - X_j - Y_j$$

by setting $Y_h = 0$ for $0 \leq h \leq i - 1$. Then

$$E_{ij} \in \mathbb{Z}[X_i, X_{i+1}, \ldots, X_{j-1}, Y_0, Y_{i+1}, \ldots, Y_{j-1}].$$

**Proof** Let $T_{ij}$ be the polynomial obtained from $S_j$ by setting $Y_h = 0$ for $0 \leq h \leq i - 1$. Then $T_{ij} = X_j + Y_j + E_{ij}$ for $0 \leq i \leq j$, and by Lemma 2 we have $T_{ij} = X_j$ for $0 \leq j < i$. It follows from (4.2) that for $j \geq i$,

$$T_{ij} = p^{-j}\left( \sum_{h=i}^{j} p^h(X_i^{p-h} + Y_i^{p-h}) - \sum_{h=i}^{j-1} p^h T_{ih}^{p-h} \right).$$

In particular, $T_{ij} = X_j + Y_j$. Using induction on $j$ we get $T_{ij} \in \mathbb{Q}[X_0, \ldots, X_j, Y_0, \ldots, Y_j]$ for $j \geq i$. Since $D_j \in \mathbb{Z}[X_0, \ldots, X_{j-1}, Y_0, \ldots, Y_{j-1}]$ the lemma follows from this. $\square$
Proposition 2 Let $L/K$ be a $C_p$-extension which satisfies assumptions (3.1), (3.2), and (3.3). Let $\sigma$ be a generator for $\text{Gal}(L/K)$ such that $\sigma(x) = x \oplus 1$, where $1 \in W_n(K)$ is the multiplicative identity. Then the following hold:

(a) For $0 \leq i \leq n - 1$ we have $(\sigma^i - 1)(x_i) = 1$.

(b) For $0 \leq i < j \leq n - 1$ we have

\[ v_K((\sigma^i - 1)(x_j)) = -(1 - p^{-1})(u_{i+1} + \cdots + u_j). \]

Proof (a) It follows from the assumption on $\sigma$ that $\sigma^i(x) = x \oplus p^i$, where $p^i = p^i \cdot 1$ is the element of $W_n(K)$ which has a 1 in position $i$ and 0 in all other positions. Hence by Lemma 2 we get

\[ \sigma^i(x_i) = x_i + 1 + D_i(x_0, \ldots, x_{i-1}, 0, \ldots, 0) = x_i + 1. \]

(b) Let $\tau_j$ denote the $j$th entry of $x \oplus p^i$. It follows from Lemma 7 that $\tau_j - x_j$ can be expressed as a polynomial in $x_i, \ldots, x_{j-1}$ with coefficients in $\mathbb{F}_p$. In fact, letting $E_{ij}$ be the image of $E_{ij}$ in $\mathbb{F}_p[X_i, \ldots, X_j, Y_i, \ldots, Y_j]$ we get

\[ \tau_j - x_j = E_{ij}(x_i, \ldots, x_{j-1}, 1, 0, \ldots, 0). \]  

(4.3)

As in the proof of Lemma 4, for $0 \leq h \leq j$ we assign $X_h$ and $Y_h$ the weight $p^h$. This makes the $j$th Witt addition polynomial $S_j$ isobaric of weight $p^j$. Hence $E_{ij}$ is also isobaric of weight $p^j$. It follows from Lemmas 2 and 7 that every term in $E_{ij}$ has a factor $Y_h$ for some $i \leq h \leq j - 1$. Thus if we assign the weight $p^h$ to $x_h$ in (4.3), every term in $\tau_j - x_j$ has weight $< p^j$.

We wish to find a lower bound for the valuations of the terms $x_i^a_1 x_{i+1}^{a_1} \cdots x_{j-1}^{a_{j-1}}$ with $a_h \geq 0$ that satisfy the weight constraint

\[ p^i a_i + p^{i+1} a_{i+1} + \cdots + p^j a_{j-1} < p^j, \]  

(4.4)

and thus may potentially appear in the formula (4.3) for $\tau_j - x_j$. Assume that our choices of $a_h$ for $i \leq h \leq j - 1$ minimize

\[ v_K(x_i^{a_i} x_{i+1}^{a_{i+1}} \cdots x_{j-1}^{a_{j-1}}) = -p^{-1}(a_i u_{i+1} + a_{i+1} u_{i+2} + \cdots + a_{j-1} u_j) \]  

(4.5)

subject to the constraint (4.4). Suppose $a_h \geq p$ for some $i \leq h \leq j - 1$; then $h < j - 1$ by (4.4). Set $a'_h = a_h - p$, $a'_{h+1} = a_{h+1} + 1$, and $a'_t = a_t$ for $i \leq t \leq j - 1, t \neq [h, h + 1]$. Then $a'_i, a'_{i+1}, \ldots, a'_{j-1}$ are nonnegative integers such that

\[ p^i a'_i + p^{i+1} a'_{i+1} + \cdots + p^j a'_{j-1} = p^i a_i + p^{i+1} a_{i+1} + \cdots + p^j a_{j-1} < p^j. \]

Since $h < j < n$ we have $h + 1 \leq n - 1$. Hence by Lemma 4(b) and (3.4) we get

\[ v_K(x_{h+1}) = -p^{-1} u_{h+2} < -u_{h+1} = pv_K(x_h). \]

Therefore

\[ v_K(x_i^{a'_i} x_{i+1}^{a'_{i+1}} \cdots x_{j-1}^{a'_{j-1}}) < v_K(x_i^{a_i} x_{i+1}^{a_{i+1}} \cdots x_{j-1}^{a_{j-1}}). \]

This contradicts the minimality of $v_K(x_i^{a_i} x_{i+1}^{a_{i+1}} \cdots x_{j-1}^{a_{j-1}})$, so we must have $a_h \leq p - 1$ for $i \leq h \leq j - 1$. On the other hand, letting $a_h = p - 1$ for $i \leq h \leq j - 1$ satisfies (4.4), so the minimum is achieved in (4.5) with this choice. Furthermore, this is the unique choice of nonnegative values for $a_h$ satisfying (4.4) which minimizes (4.5). By Lemma 6
the coefficient of $x_i^{p-1}x_{i+1}^{p-1} \cdots x_{j-1}^{p-1}$ in the formula (4.3) for $\tau_j - x_j$ is $(-1)^{j-i}$. Hence by Lemma 4(b) we get

$$v_K((\sigma^{p^{l-1}} - 1)(x_j)) = v_K(x_i^{p-1}x_{i+1}^{p-1} \cdots x_{j-1}^{p-1}) = -(1 - p^{-1})(u_{i+1} + \cdots + u_j).$$

\[\square\]

**Corollary 3** $(\sigma^{p^{n-1}} - 1)(Y) = t_{n-1} \in K^\times$.  

**Proof** Using (4.1) and Proposition 2(a) we get

$$(\sigma^{p^{n-1}} - 1)(Y) = t_{n-1}(\sigma^{p^{n-1}} - 1)(x_{n-1}) = t_{n-1}.$$

Since $L = K(Y)$ we have $t_{n-1} \neq 0$.  \[\square\]

**Proposition 3** Let $L/K$ be a $C_{p^{n}}$-extension which satisfies assumptions (3.1), (3.2), and (3.3). Then for $1 \leq i \leq n-1$ we have

$$(\sigma^{p^{i-1}} - 1)(Y) \equiv t_{i-1} \pmod{t_{i-1}M_L^{(u_{i+1} - u_i) - p^{n}u_i + p^{n-1}u_i}}.$$

**Proof** It follows from (4.1) and Proposition 2(a) that

$$v_K(\sigma^{p^{i-1}}(Y) - Y - t_{i-1}) \geq \min\{v_K(t_j(\sigma^{p^{j-1}} - 1)(x_j)) : i \leq j \leq n-1\}. \quad (4.6)$$

Using Proposition 2(b), Lemma 5(c), and assumption (3.2) we get

$$v_K(t_j(\sigma^{p^{j-1}} - 1)(x_j)) - v_K(t_{j-1}(\sigma^{p^{j-1}} - 1)(x_{j-1})) = v_K(t_j) - v_K(t_{j-1}) - (1 - p^{-1})u_j$$

$$= p^{-n}(b_{j+1} - b_j) - (1 - p^{-1})u_j$$

$$> u_j - p^{-n}b_j - (1 - p^{-1})u_j$$

$$= -p^{-n}b_j + p^{-1}u_j$$

$$= p^{-n}(p^{n-1}u_j - b_j)$$

for $i + 1 \leq j \leq n-1$. This last quantity is positive by Lemma 1. Hence by (4.6), Proposition 2(b), Lemma 5(c), and (2.1) we have

$$v_K(\sigma^{p^{i-1}}(Y) - Y - t_{i-1}) \geq v_K(t_i(\sigma^{p^{i-1}} - 1)(x_i))$$

$$= v_K(t_i) - (1 - p^{-1})u_i$$

$$= v_K(t_{i-1}) + p^{-n}(b_{i+1} - b_i) - (1 - p^{-1})u_i$$

$$= v_K(t_{i-1}) + p^{-n}(u_{i+1} - u_i) - (1 - p^{-1})u_i.$$  

It follows that $\sigma^{p^{i-1}}(Y) - Y - t_{i-1} \in t_{i-1}M_L^{(u_{i+1} - u_i) - p^{n}u_i + p^{n-1}u_i}$.  \[\square\]

**Remark 2** Let $L/K$ be a be a $C_{p^{n}}$-extension satisfying the conditions of Proposition 3. Using (3.2) and Lemma 1 we get

$$p^{i}(u_{i+1} - u_i) - p^{n}u_i + p^{n-1}u_i = b_{i+1} - b_i - p^{n}u_i + p^{n-1}u_i > p^{n-1}u_i - b_i > 0.$$

Therefore the congruence given in the proposition does not reduce to $0 \equiv 0$. 

---

**Note:** The text appears to be a continuation from a previous page, as indicated by the page number and section references. The content seems to be a proof involving formal mathematical notations and propositions, typical of a number theory or algebraic number theory context. The references to previous lemmas and propositions (e.g., Lemma 1, Lemma 4(b), Proposition 2(a)) suggest a structured and rigorous approach to proving mathematical statements. The notation and symbols used (e.g., $\sigma$, $v_K$, $M_L$, $Y$, $t_i$) are consistent with advanced mathematical literature, particularly in the field of algebraic number theory. The document appears to be a continuation of a larger work, possibly a research paper or a textbook chapter. The sections (3.1), (3.2), (3.3), and (4.1) indicate that the text is part of a structured proof or discussion, likely building on prior results to reach a conclusion or a new proposition. The proof method involves analyzing congruences and using properties of $C_{p^{n}}$-extensions to derive inequalities and congruences, which are then used to establish the final statement or proposition.
Corollary 4 Let \( L/K \) be a \( C_{p^n} \)-extension which satisfies assumptions (3.1), (3.2), and (3.3). Let \( X = \tau_{n-1}^{-1} Y \), and for \( 1 \leq i \leq n \) set \( \mu_i = \tau_{n-1}^{-1} t_i - 1 \) and \( \epsilon_i = (\sigma^{p^{i-1}} - 1)(X) - \mu_i \). Then \( \epsilon_n = 0 \), and for \( 1 \leq i \leq n - 1 \) we have
\[
v_L(\epsilon_i) - v_L(\mu_i) \geq p^i (u_{i+1} - u_i) - (p^n - p^{i-1}) u_i.
\]

Proof The first claim follows from Corollary 3, and the second follows from Proposition 3.

5 Main results

Recall that for \( 0 \leq j \leq n \), \( K_j \) is the fixed field of the subgroup \( \langle \sigma^j \rangle \) of \( \text{Gal}(L/K) = \langle \sigma \rangle \). Furthermore, since \( \langle \sigma^j \rangle \) is a ramification subgroup of \( \text{Gal}(L/K) \), the upper ramification breaks of \( K_j/K \) are \( u_1, u_2, \ldots, u_j \), and the lower ramification breaks are \( b_1, b_2, \ldots, b_j \). We can describe the extension \( K_j/K \) by truncating the Witt vector equations in Sect. 3. Thus \( K_j = K(x_0, x_1, \ldots, x_{j-1}) \) with \( \phi(x) = x \oplus \beta, d = (x \oplus \beta) - x - \beta \), and
\[
x = \begin{bmatrix}
x_0 \\
x_1 \\
\vdots \\
x_{j-1}
\end{bmatrix},
d = \begin{bmatrix} 0 \\ d_1 \\ \vdots \\ d_{j-1} \end{bmatrix},
\omega = \begin{bmatrix} 1 \\ \omega_1 \\ \vdots \\ \omega_{j-1} \end{bmatrix},
\beta = \begin{bmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{j-1} \end{bmatrix}.
\]

Assumptions (3.1), (3.2), and (3.3) continue to be valid for \( K_j/K \). As a result, we may use the methods of Sect. 3 to construct a generator \( Y_j \) for the extension \( K_j/K \), as in (3.9). In doing so, we add a subscript \( j \). Let \( t_{ij} \) denote the \( (i, 0) \) cofactor of the matrix that defines \( Y_j \). (Thus \( t_i \) from Sect. 3 will now be expressed as \( t_{i,0} \).) By Corollary 1 we have \( v_{K_j}(Y_i) = v_{K_j}(t_{j-1, i}) - b_j \). Corollary 3 yields
\[
(\sigma^{p^{j-1}} - 1)(Y_j) = t_{j-1, i} \in K^X.
\]

Thus \( X_j = t_{j-1, i}^{-1} Y_j \) is defined, \( v_{K_j}(X_j) = -b_j, (\sigma^{p^{j-1}} - 1)(X_j) = 1 \), and \( K_j = K(Y_j) = K(X_j) \).

We are now prepared to state and prove our main result.

Theorem 2 Let \( K \) be a local field of characteristic \( p \) with perfect residue field and let \( L/K \) be a totally ramified \( C_{p^n} \)-extension. Let \( \beta \in W_n(K) \) be a reduced Witt vector which corresponds to \( L/K \) and let \( \beta_0, \beta_1, \ldots, \beta_{n-1} \) be the coordinates of \( \beta \). Set \( \beta = \beta_0 \) and assume there are \( \omega_i, \delta_i \in K \) such that \( \beta_i = \beta \omega_i^{p^{i-1}} + \delta_i \) and \( v_K(\delta_i) > v_K(\beta_i) \) for \( 1 \leq i \leq n - 1 \). Assume further that assumptions (3.1), (3.2) and (3.3) hold. Then there is a Galois scaffold \( ((\lambda_w), \{\Psi_i\}) \) for \( L/K \) with precision
\[
\xi = \min\{b_{i+1} - p^n u_i : 1 \leq i \leq n - 1\} \geq 1,
\]
where \( b_1 < b_2 < \cdots < b_n \) and \( u_1 < u_2 < \cdots < u_n \) are the lower and upper ramification breaks of \( L/K \).

Proof Let \( 1 \leq i \leq j \leq n \). The congruence hypothesis \( b_i \equiv b_j \pmod{p^n} \) in Theorem 1 is satisfied as a consequence of Lemma 5(c). Corollary 4 yields
\[
(\sigma^{p^{j-1}} - 1)(X_j) = \mu_{ij} + \epsilon_{ij}
\]
for \( 1 \leq i \leq j \leq n \), where \( \mu_{ij} = t_{j-1, i}^{-1} t_{i-1, j}, \mu_{jj} = 1, \epsilon_{jj} = 0 \), and
\[
v_{K_j}(\epsilon_{ij}) - v_{K_j}(\mu_{ij}) \geq p^i(u_{i+1} - u_i) - (p^n - p^{i-1})u_i.
\]
Using (2.1) we get
\[
v_L(\epsilon_{ij}) - v_L(\mu_{ij}) \geq p^{n-1}(u_{i+1} - u_i) - p^n u_i + p^{n-1} u_i
\]
\[
= p^{n-1}(b_{i+1} - b_i) - p^nu_i + p^{n-1}u_i
\]
\[
= p^{n-1}u_i - p^n - b_i + p^{n-1}(b_{i+1} - b_i)
\]
for $1 \leq i < j \leq n$. Therefore by Theorem 1 the extension $L/K$ has a scaffold of precision $c$, with
\[
c = \min \{p^{n-1}(b_{i+1} - b'_i) : 1 \leq i < j \leq n\}
\]
\[
= \min \{b_{i+1} - p^n u_i : 1 \leq i < n\}.
\]
Finally, we have $c \geq 1$ by (3.2).

\(\square\)

**Remark 3** Theorem 2 for $n = 2$ is in complete agreement with Theorem 2.1 in [3]. First, the hypotheses are the same: Assumptions (3.2), (3.3), which are required here for Theorem 2, reduce to (7), (8) in [3], which are required there for Theorem 2.1. However, because the definition of a scaffold and the notion of a scaffold’s precision had not been fully formulated when [3] was written, a comparison of the resulting scaffolds, including their precisions, is not so immediate. One has to interpret the content of Theorem 2.1 in [3] appropriately. There one sees that $\Psi_2$ increases valuations by $b_2$, while $\Psi_1$ increases valuations by $pb_1$. As a result, one would expect $\Psi_p^2$ to increase valuations by $p^2b_1$, but since $\Psi_p^2 = \Psi_1$, it actually increases valuations by more, namely $b_2$. This difference $c = b_2 - p^2b_1$ is the precision of the Galois scaffold given in [3], and it is the same as the precision given in Theorem 2. (Beware that both Remark 3.5 and Appendix A.2.3 in [2] erroneously state that $c = b_2 - pb_1$ is the precision of the scaffold in [3].)

Recall that the associated order $\mathfrak{A}$ of $\mathcal{O}_L$ in $K[C_p]$ is defined in (1.1). In [3] sufficient conditions are given for $\mathcal{O}_L$ to be free over its associated order in the case $n = 2$. Using the scaffolds provided by Theorem 2 we can extend this criterion to $C_{p^m}$-extensions with $n \geq 3$.

**Corollary 5** Let $L/K$ be a $C_{p^m}$-extension which satisfies the hypotheses of Theorem 2. Let $r(u_i)$ denote the least nonnegative residue modulo $p^m$ of the upper ramification break $u_i$. Strengthen assumption (3.2) by requiring that $b_{i+1} - p^n u_i \geq r(u_i)$ for $1 \leq i \leq n - 1$. Assume further that $r(u_i) \mid p^m - 1$ for some $1 \leq m \leq n$. Then $\mathcal{O}_L$ is free over its associated order $\mathfrak{A}$.

**Proof** Since $b_n \equiv b_1 \pmod{p^n}$ and $b_1 = u_1$ we have $r(b_n) = r(u_1)$. Theorem 2 gives us a scaffold with precision $c \geq r(b_n)$, so the corollary follows from Theorem 4.8 of [2].

\(\square\)

Let $K$ be a local field, let $G$ be a finite group, and let $H$ be an $\mathcal{O}_K$-order in $K[G]$. Say that $H$ is a Hopf order if $H$ is a Hopf algebra over $\mathcal{O}_K$ with respect to the operations inherited from the $K$-Hopf algebra $K[C_p]$. Say that the Hopf order $H \subset K[C_{p^m}]$ is realizable if there is a $G$-extension $L/K$ such that $H$ is isomorphic to the associated order $\mathfrak{A}$ of $\mathcal{O}_L$ in $K[G]$. As described in Chap. 12 of [5], a great deal of effort has gone into constructing and classifying Hopf orders in $K[C_p]$ and $K[C_{p^m}]$ in the case where $K$ is a local field of characteristic 0. For instance, a large family of Hopf orders in $K[C_{p^m}]$ can be produced.
from the results of [10] using duality. This family is conjectured to include all Hopf orders in $K[C_{p^n}]$; this has been proved in the cases with $n \leq 2$ [14]. In the case char($K$) = $p$, the duals of Hopf orders in $K[C_{p^2}]$ were characterized in [14], and the duals of Hopf orders in $K[C_p^n]$ were characterized in [8]. However, little seems to be known about Hopf orders in $K[C_{p^n}]$ when char($K$) = $p$ and $n \geq 3$. Therefore it is significant that the scaffolds from Theorem 2 can be used to construct realizable Hopf orders in $K[C_{p^n}]$:

**Corollary 6** Let $L/K$ be a $C_{p^n}$-extension which satisfies the hypotheses of Corollary 5. Assume further that $u_1 \equiv -1 \pmod{p^n}$. Then the associated order $\mathfrak{A}$ of $\mathcal{O}_L$ in $K[C_{p^n}]$ is a Hopf order.

**Proof** It follows from the preceding corollary that $\mathcal{O}_L$ is free over $\mathfrak{A}$. Since $b_i \equiv b_1 \equiv -1 \pmod{p^n}$ for $1 \leq i \leq n$, the different ideal of $L/K$ is generated by an element of $K$. Hence by Theorem A and Proposition 3.4.1 of [1] we deduce that $\mathfrak{A}$ is a Hopf order in $K[C_{p^n}]$. $\square$

**Data Availability Statement** Data sharing is not applicable to this article as no datasets were generated or analyzed in this research.

**Author details**

1Department of Mathematics, University of Nebraska Omaha, Omaha, NE 68182, USA e-mail: elder@unomaha.edu,

2Department of Mathematics, University of Florida, Gainesville, FL 32611, USA e-mail: keating@ufl.edu.

Received: 29 January 2022 Accepted: 9 September 2022 Published online: 30 September 2022

**References**

1. Bondarko, M.V.: Local Leopoldt’s problem for rings of integers in abelian $p$-extensions of complete discrete valuation fields. Documenta Math. 5, 657–693 (2000)

2. Byott, N.P., Childs, L.N., Elder, G.G.: Scaffolds and generalized integral Galois module structure. Ann. Inst. Fourier 68, 965–1010 (2018)

3. Byott, N.P, Elder, G.G.: Galois scaffolds and Galois module structure in extensions of characteristic $p$ local fields of degree $p^2$. J. Number Theory 133, 3598–3610 (2013)

4. Byott, N.P., Elder, G.G.: Sufficient conditions for large Galois scaffolds. J. Number Theory 182, 95–130 (2018)

5. Childs, L., Greither, C., Keating, K., Koch, A., Kohl, T., Truman, P., Underwood, R.: Hopf Algebras and Galois Module Theory. American Mathematical Society, Providence (2022)

6. Demazure, M.: Lectures on p-Divisible Groups, Lecture Notes in Mathematics 302

7. Elder, G.G., Keating, K.P.: Refined ramification breaks in characteristic $p$. Acta Arith. 192, 371–395 (2020)

8. Koch, A.: Primitively generated Hopf orders in characteristic $p$. Commun. Algebra 45, 2673–2689 (2017)

9. Martinet, J.: Anneau des entiers d’une extension galoisienne considéré comme module sur l’algèbre du groupe de Galois, Colloque de Théorie des Nombres (Univ. Bordeaux, Bordeaux, 1969), 123–126. Bull. Soc. Math. France, Mém. 25, Soc. Math. France, Paris (1971)

10. Mézard, A., Romagny, M., Tossici, D.: Models of group schemes of roots of unity. Ann. Inst. Fourier 63, 1055–1135 (2013)

11. Serre, J.-P.: Corps Locaux, Hermann, Paris, 1962; translated as Local Fields. Springer, New York (1979)

12. Thomas, L.: Ramification groups in Artin-Schreier-Witt extensions. J. Theor. Nombres Bordeaux 17, 689–720 (2005)

13. Thomas, L.: A valuation criterion for normal basis generators in equal positive characteristic. J. Algebra 320, 3811–3820 (2008)

14. Tossici, D.: Models of $\mu_{p^n}$ over a discrete valuation ring. With an appendix by Xavier Caruso. J. Algebra 323, 1908–1957 (2010)

15. Witt, E.: Zyklische Körper und Algebren der Charakteristik vom Grad $p^n$. J. Reine Angew. Math. 174, 126–140 (1936)

**Publisher’s Note**

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.