ANNALES

DE

L'INSTITUT FOURIER

Nigel P. BYOTT, Lindsay N. CHILDS & G. Griffith ELDER

Scaffolds and generalized integral Galois module structure

Tome 68, nº 3 (2018), p. 965-1010.

<http://aif.cedram.org/item?id=AIF_2018__68_3_965_0>

Ann. Inst. Fourier, Grenoble
68, 3 (2018) 965-1010

SCAFFOLDS AND GENERALIZED INTEGRAL GALOIS MODULE STRUCTURE

by Nigel P. BYOTT, Lindsay N. CHILDS & G. Griffith ELDER

Abstract. — Let L/K be a finite, totally ramified p-extension of complete local fields with residue fields of characteristic $p > 0$, and let A be a K-algebra acting on L. We define the concept of an A-scaffold on L, thereby extending and refining the notion of a Galois scaffold considered in several previous papers, where L/K was Galois and $A = K[G]$ for $G = \mathrm{Gal}(L/K)$. When a suitable A-scaffold exists, we show how to answer questions generalizing those of classical integral Galois module theory. We give a necessary and sufficient condition, involving only numerical parameters, for a given fractional ideal to be free over its associated order in A. We also show how to determine the number of generators required when it is not free, along with the embedding dimension of the associated order. In the Galois case, the numerical parameters are the ramification breaks associated with L/K. We apply these results to biquadratic Galois extensions in characteristic 2, and to totally and weakly ramified Galois p-extensions in characteristic p. We also apply our results to the non-classical situation where L/K is a finite primitive purely inseparable extension of arbitrary exponent that is acted on, via a higher derivation (but in many different ways), by the divided power K-Hopf algebra.

Résumé. — Soit L/K une extension finie et totalement ramifiée, de degré une puissance de p, de corps locaux complets dont le corps résiduel a caractéristique $p > 0$. Soit A une K-algèbre qui opère sur L. Nous définissons le concept d'un A-échafaudage sur L. Ceci étend et raffine la notion d'échafaudage galoisien, que nous avons considérée dans plusieurs articles antérieurs, où L/K était une extension galoisienne et $A = K[G]$ pour $G = \mathrm{Gal}(L/K)$. Dans le cas où il existe un A-échafaudage convenable, nous montrons comment résoudre des questions qui généralisent celles de la théorie classique des modules galoisiens des anneaux des entiers. Nous donnons une condition nécessaire et suffisante, qui contient seulement des paramètres numériques, pour qu'un idéal fractionnaire quelconque soit un module libre sur son ordre associé dans A. Nous montrons aussi comment déterminer le nombre de générateurs dont on a besoin si l'idéal n'est pas libre, et la dimension d'immersion de l'ordre associé. Dans le cas galoisien, les paramètres numériques sont les nombres de ramification de L/K. Nous appliquons ces résultats aux extensions galoisiennes biquadratiques de caractéristique 2, et aux extensions totalement et faiblement ramifiées, de degré une puissance de p et de caractéristique p. Nous appliquons nos résultats aussi à la situation non classique où L/K est une extension finie, purement inséparable, d'exposant quelconque, sur laquelle

Keywords: Ramification, Galois module structure, Hopf–Galois theory.
2010 *Mathematics Subject Classification:* 11S15, 20C11, 16T05, 11R33.

opère la K-algèbre de Hopf des puissances divisées par une dérivation supérieure (mais avec beaucoup d'actions différentes).

1. Introduction

Let K be a local field with residue field of characteristic $p > 0$, and let L be a finite Galois extension of K with Galois group G. We write $\mathfrak{O}_K$, $\mathfrak{O}_L$ for the valuation rings of K, L, respectively, and $\mathfrak{P}_K$, $\mathfrak{P}_L$ for their maximal ideals. Then $\mathfrak{O}_L$ is a module over the integral group ring $\mathfrak{O}_K[G]$. By Noether's criterion [35], it is a free module if and only if the extension L/K is at most tamely ramified. In order to study integral Galois module structure for wildly ramified extensions, H.-W. Leopoldt [30] introduced the associated order

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

of $\mathfrak{O}_L$ in the group algebra $K[G]$. Over the last fifty years, many authors have investigated, in various situations, when $\mathfrak{O}_L$ is free as a module over $\mathfrak{A}_{L/K}$, or, more generally, when a fractional ideal $\mathfrak{P}_L^h$ of $\mathfrak{O}_L$ is free as a module over its associated order in $K[G]$; see for instance [1, 3, 5, 7, 18, 25, 32, 33, 39, 42]. For a comprehensive overview of this area, and a far more extensive bibliography, we refer the reader to the survey [44].

Our goal here is to give a systematic presentation of a new approach to such questions of integral Galois module structure, in a somewhat generalized sense. This approach is restricted to totally ramified extensions of local fields L/K, whose degree is a power p^n of the residue characteristic p, and which admit an action by a K-algebra A of dimension p^n. An *A-scaffold on L* consists of certain special elements in A which act on suitable elements of L in a way which is tightly linked to the valuation on L. The most obvious setting where scaffolds may occur is that described above, where L/K is a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$ and $A = K[G]$. Our approach is not, however, limited to that situation. We will show in §5 how it can be applied to a divided power Hopf algebra A acting in many different ways on an inseparable field extension. Other inseparable examples have been given by Koch [27, 28]. Our approach could also be used for different Hopf Galois structures on a given separable (but not necessarily normal) field extension, as described by Greither and Pareigis [22].

When L/K admits an A-scaffold, L is a free module over A, in analogy to the Normal Basis Theorem of Galois theory. We can then consider any fractional ideal $\mathfrak{P}_L^h$ of $\mathfrak{O}_L$ as a module over its associated order in A,

$$\mathfrak{A}(h, A) = \{\alpha \in A : \alpha \cdot \mathfrak{P}_L^h \subseteq \mathfrak{P}_L^h\},$$

and ask whether it is a free module. It is in this sense that our work is concerned with "generalized" integral Galois module structure. An A-scaffold comes with a "precision" parameter, and the existence of a scaffold of high enough precision will enable us to extract a considerable amount of information about the $\mathfrak{A}(h,A)$-module $\mathfrak{P}_L^h$; not only can we determine if it is free, but (following [39] for extensions of degree p), we can also find the minimal number of generators required when it is not free, and obtain the embedding dimension of $\mathfrak{A}(h,A)$. An important feature of our approach is that all this information depends on purely numerical data, namely certain parameters b_i attached to the scaffold (playing the role of ramification breaks) and the exponent h of the ideal $\mathfrak{P}_L^h$ under consideration. Given the existence of a scaffold with specified parameters b_i, our results are therefore, in some sense, universal: they are independent of the characteristic (0 or p) of the fields involved, and, in the Galois case, independent of the precise structure of the Galois group. In particular, our results make no distinction between abelian and non-abelian extensions. Moreover, we obtain exactly the same results for, say, inseparable extensions as for Galois extensions, provided that the parameters coincide.

The intuition underlying our notion of a scaffold can be explained somewhat informally as follows. Let v_K, v_L denote normalized valuations such that $v_K(K^\times) = v_L(L^\times) = \mathbb{Z}$. Given any positive integers b_i for $1 \leqslant i \leqslant n$ such that $p \nmid b_i$, there are elements $X_i \in L$ such that $v_L(X_i) = -p^{n-i}b_i$. Since the valuations, v_L, of the monomials

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

provide a complete set of residues modulo p^n and, since L/K is totally ramified of degree p^n, these monomials provide a convenient K-basis for L. The action of A on L is clearly determined by its action on the monomials $\mathbb{X}^a$. So if there were $\Psi_i \in A$ for $1 \leqslant i \leqslant n$ such that each Ψ_i acts on the monomial basis element $\mathbb{X}^a$ of L as if it were the differential operator $\partial/\partial X_i$ (with the X_i treated as independent variables), namely

$$\Psi_i \mathbb{X}^a = a_{(n-i)} \mathbb{X}^a / X_i\,, \tag{1.1}$$

then the monomials in the Ψ_i (with exponents at most $p-1$) would furnish a convenient basis for A whose effect on the $\mathbb{X}^a$ would be easy to follow. As a consequence, the determination of the associated order of a particular ideal $\mathfrak{P}_L^h$, and of the structure of this ideal as a module over its associated order, would be reduced to purely numerical considerations. This remains true if (1.1) is loosened to the congruence

$$\Psi_i \mathbb{X}^a \equiv a_{(n-i)} \mathbb{X}^a / X_i \pmod{(\mathbb{X}^a/X_i)\mathfrak{P}_L^{\mathfrak{c}}} \tag{1.2}$$

for a sufficiently large "precision" $\mathfrak{c}$. The Ψ_i, together with the $\mathbb{X}^a$, constitute an A-scaffold on L. Our formal definition of an A-scaffold (Definition 2.3) is a generalization of this situation. When the equality (1.1) holds, our scaffold has precision $\mathfrak{c} = \infty$.

We now explain the background to this work. In the papers [13, 14, 19], the first- and third-named authors began to develop the theory of scaffolds in the setting of Galois extensions. There, the parameters b_i of these Galois scaffolds are just the ramification breaks of the extension L/K. These scaffolds all have precision ∞, apart from those on cyclic extensions of degree p^2 in [13]. The main result of [19] is the existence of a Galois scaffold for a certain class of arbitrarily large elementary abelian extensions in characteristic p (the "near one-dimensional extensions"). The Galois module structure of the valuation ring in such extensions L/K is investigated in [14], where a necessary and sufficient condition (in terms of the b_i) is given for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_{L/K}$. This condition turns out to be equivalent to that given by Miyata [33] (and reformulated in [10]) for a class of cyclic Kummer extensions in characteristic 0. The striking observation that the same numerical condition holds for two apparently unrelated families of extensions, differing both in Galois group and in characteristic, suggests that the methods used in [14] to study Galois module structure for near one-dimensional extensions might be applied more widely. The present paper develops the machinery to substantiate this idea, while [13] indicates the limitations of our approach by demonstrating that most extensions will not admit a scaffold. In any case, our method is necessarily restricted to totally ramified extensions of p-power degree, since if L/K admits an A-scaffold, then it possesses a "valuation criterion": there is an integer b such that any element of L of valuation b is a free generator of L over A (see Proposition 2.12). This property, which can be viewed as a strong version of the Normal Basis Theorem, has been studied in a number of papers [11, 12, 20, 38, 43], and can only hold when L/K is totally ramified and of p-power degree (see [38, Prop. 1.2] for the Galois case).

When the residue field of K is perfect, we know from [19] that Galois scaffolds exist for all totally ramified biquadratic extensions in characteristic 2, and for all totally and weakly ramified p-extensions in characteristic p. To illustrate the sort of explicit information our methods can yield, we examine these two classes of extensions in detail (see Theorems 4.1 and 4.2). However, in this paper we are not primarily concerned with the problem of actually constructing A-scaffolds. In a separate paper [15], we give a criterion for a totally ramified Galois p-extension to have a Galois scaffold of a given precision. This enables us to give an explicit construction for a class of extensions in characteristic 0 which admit Galois scaffolds. These have elementary abelian Galois groups of arbitrarily large rank, and are the analogs in characteristic 0 of the near one-dimensional extensions in characteristic p constructed in [19]. They include the totally ramified biquadratic extensions and the totally and weakly ramified p-extensions satisfying some additional hypotheses. Under these hypotheses, our Galois module results for biquadratic and weakly ramified extensions in characteristic p will also hold in characteristic 0.

Our work is somewhat similar in spirit to that of Bondarko [6, 7, 8], who considers the existence of ideals free over their associated orders in the context of totally ramified extensions of p-power degree. (Unlike us, Bondarko only considers Galois extensions.) Bondarko introduces the class of semistable extensions. Any such extension contains at least one ideal free over its associated order, and all such ideals can be determined from numerical data. Moreover, any abelian extension containing an ideal free over its associated order, and satisfying certain additional assumptions, must be semistable. Abelian semistable extensions can be completely characterized in terms of the Kummer theory of (one-dimensional) formal groups. It would be of interest to understand the precise relationship between Bondarko's approach and our own, and we intend to return to this question in future work.

Finally, regarding the hypotheses needed on the ground field K, we note that our main results on A-scaffolds do not require the residue field of K to be perfect. However, in order to construct scaffolds on particular families of Galois extensions (as we do in [13, 14, 15, 19]), this hypothesis is essential. The hypothesis is also convenient when discussing higher ramification groups, since the standard exposition [37] of higher ramification theory makes use of it at various points. We will therefore not include the condition that K has perfect residue field among the running hypotheses of this paper, but will impose it from time to time when considering examples.

1.1. Outline of the paper

In §2 we define the notion of an A-scaffold on L and obtain some of its properties. A detailed discussion of the relationship between the A-scaffolds considered here and the Galois scaffolds of our earlier papers is relegated to an Appendix at the end of the paper. Our main results, Theorems 3.1

and 3.6, relating A-scaffolds to generalized integral Galois module structure, will be stated and proved in §3. In §4, we give some applications of our approach to Galois extensions, discussing in detail biquadratic extensions and weakly ramified extensions. Finally, in §5, we consider A-scaffolds on inseparable extensions L/K, where A is a divided power Hopf algebra.

2. A-scaffolds

In this section, we consider a totally ramified extension L/K of local fields, together with a K-algebra A which has a K-linear action on L. We assume that the residue field κ of K has characteristic $p > 0$. The characteristic of K may be either 0 or p. We do not require κ to be perfect. We assume that L/K has degree p^n, and that $\dim_K A = p^n$.

Before giving the definition of an A-scaffold on L, we require some notation. We set $\mathbb{S}_{p^n} = \{0, 1, \ldots, p^n - 1\}$ and $\mathbb{S}_p = \{0, 1, \ldots, p - 1\}$, and we identify each $s \in \mathbb{S}_{p^n}$ with its vector of base-p coefficients $(s) = (s_{(n-1)}, \ldots, s_{(0)}) \in \mathbb{S}_p^n$ where

$$s = \sum_{i=1}^{n} s_{(n-i)} p^{n-i}. \tag{2.1}$$

This indexing of the base-p digits as $s_{(n-i)}$, where increasing values of i correspond to decreasing powers of p, is natural in the context of Galois scaffolds, where the b_i are the ramification breaks (in increasing order), and we need to consider expressions of the form $\mathfrak{b}(s)$ defined in (2.2) below. We will almost always write s in this way.

We further endow $\mathbb{S}_{p^n}$ with a partial order that is based upon the usual multi-index partial order on $\mathbb{S}_p^n$, writing $s \preceq t$ (or $t \succeq s$) if and only if $s_{(n-i)} \leqslant t_{(n-i)}$ for $1 \leqslant i \leqslant n$. For the convenience of the reader, we record some facts.

Lemma 2.1. — *Let $s, t \in \mathbb{S}_{p^n}$ and write $s = \sum_{i=1}^{n} s_{(n-i)} p^{n-i}$ and $t = \sum_{i=1}^{n} t_{(n-i)} p^{n-i}$ where $s_{(n-i)}, t_{(n-i)} \in \mathbb{S}_p$. Then $s \preceq t$ if and only if $s \leqslant t$ and there are no carries in the base-p addition of s and $t - s$. Furthermore, the following are equivalent:*

(1) *$s_{(n-i)} + t_{(n-i)} \leqslant p - 1$ for $1 \leqslant i \leqslant n$;*
(2) *$s \preceq p^n - 1 - t$;*
(3) *$t \preceq p^n - 1 - s$;*
(4) *$s + t \in \mathbb{S}_{p^n}$ and $s \preceq s + t$.*

Proof. — Assume $s \preceq t$. Then clearly $s \leqslant t$. Let $m = t - s$, and write $m = \sum_{i=1}^{n} m_{(n-i)} p^{n-i}$ with $m_{(n-i)} \in \mathbb{S}_p$. Since $0 \leqslant t_{(n-i)} - s_{(n-i)} < p$, we have $m_{(n-i)} = t_{(n-i)} - s_{(n-i)}$. When we perform the addition $s_{(n-i)} + m_{(n-i)}$ we get $t_{(n-i)}$ with no carries. On the other hand, assume that $s \leqslant t$ and there are no carries in the base-p addition of s and $m = t - s$. As $m \geqslant 0$ we have $m \in \mathbb{S}_{p^n}$, so that $m = \sum_{i=1}^{n} m_{(n-i)} p^{n-i}$ for some $m_{(n-i)} \in \mathbb{S}_p$. Since there are no carries, $m_{(n-i)} + s_{(n-i)} \leqslant p - 1$ for $1 \leqslant i \leqslant n$. Thus $t_{(n-i)} = m_{(n-i)} + s_{(n-i)}$. Therefore $t_{(n-i)} \geqslant s_{(n-i)}$ for each i, so that $s \preceq t$. The equivalence of (1)–(4) is then clear. □

Associated to an A-scaffold on L will be a sequence $b_1, \ldots, b_n$ of integer *shift parameters*, which are required to be relatively prime to p. Using these integers, we define a function $\mathfrak{b} : \mathbb{S}_{p^n} \longrightarrow \mathbb{Z}$ by

$$\mathfrak{b}(s) = \sum_{i=1}^{n} s_{(n-i)} p^{n-i} b_i \,. \tag{2.2}$$

We write $r : \mathbb{Z} \longrightarrow \mathbb{S}_{p^n}$ for the residue function $r(a) \equiv a \pmod{p^n}$. The coprimality assumption on the b_i ensures that $r \circ \mathfrak{b} : \mathbb{S}_{p^n} \longrightarrow \mathbb{S}_{p^n}$ is bijective. The function $r \circ (-\mathfrak{b}) : \mathbb{S}_{p^n} \longrightarrow \mathbb{S}_{p^n}$, defined by $r \circ (-\mathfrak{b})(s) = r(-\mathfrak{b}(s))$, is therefore also bijective. We denote its inverse by $\mathfrak{a} : \mathbb{S}_{p^n} \longrightarrow \mathbb{S}_{p^n}$. Abusing notation, we will also write $\mathfrak{a}(t)$ for $\mathfrak{a}(r(t))$ where $t \in \mathbb{Z}$, and so regard $\mathfrak{a}$ as a function $\mathbb{Z} \longrightarrow \mathbb{S}_{p^n}$.

Lemma 2.2.

(1) *$r \circ \mathfrak{b}$ is determined by the residues $b_i \bmod p^i$;*
(2) *if $b_i \equiv b_n \pmod{p^i}$ for all i then $\mathfrak{b}(s) \equiv b_n s \pmod{p^n}$ for $s \in \mathbb{S}_{p^n}$;*
(3) *if $s, t \in \mathbb{S}_{p^n}$ and $s \preceq t$ then $\mathfrak{b}(s) + \mathfrak{b}(t-s) = \mathfrak{b}(t)$;*
(4) *$\mathfrak{b}(\mathfrak{a}(t)) \equiv -t \pmod{p^n}$ for all $t \in \mathbb{Z}$;*
(5) *$\mathfrak{a}(-\mathfrak{b}(s)) = s$ for all $s \in \mathbb{S}_{p^n}$.*

Proof. — Clear. □

We are now prepared for the definition.

Definition 2.3 (A-scaffold on L). — *Let $b_1, \ldots, b_n$, $\mathfrak{b}$ and $\mathfrak{a}$ be as above, and let $\mathfrak{c} \geqslant 1$. Then an A-scaffold on L of precision $\mathfrak{c}$ with shift parameters $b_1, \ldots, b_n$ consists of*

(1) *elements $\lambda_t \in L$ for $t \in \mathbb{Z}$, such that $v_L(\lambda_t) = t$ and $\lambda_{t_1} \lambda_{t_2}^{-1} \in K$ whenever $t_1 \equiv t_2 \pmod{p^n}$.*
(2) *elements $\Psi_i \in A$ for $1 \leqslant i \leqslant n$, such that $\Psi_i \cdot 1 = 0$, and such that, for each i and for each $t \in \mathbb{Z}$, there exists a unit $u_{i,t} \in \mathfrak{O}_K^{\times}$ making*

the following congruence modulo $\lambda_{t+p^{n-i}b_i}\mathfrak{P}_L^{\mathfrak{c}}$ hold:

$$\Psi_i \cdot \lambda_t \equiv \begin{cases} u_{i,t}\lambda_{t+p^{n-i}b_i}\,, & \text{if } \mathfrak{a}(t)_{(n-i)} \geqslant 1, \\ 0 & \text{if } \mathfrak{a}(t)_{(n-i)} = 0. \end{cases}$$

An A-scaffold of precision ∞ *consists of the above data where the congruence in* (2) *is replaced by equality.*

Remark 2.4. — Condition (2) in Definition 2.3 should be interpreted as saying that the effect of Ψ_i on λ_t is approximated either by a single term or by 0. The precision $\mathfrak{c}$ determines the accuracy of this approximation, with a precision of ∞ meaning that the "approximation" is exact. In more detail, the approximation works as follows. Since Ψ_i is associated with an increase of valuation of $p^{n-i}b_i$, we express the effect of Ψ_i on the basis $\{\lambda_t : 0 \leqslant t \leqslant p^n - 1\}$ in terms of the basis $\{\lambda_{p^{n-i}b_i+s} : 0 \leqslant s \leqslant p^n - 1\}$. Thus we have

$$\Psi_i \cdot \lambda_t = \sum_{s=0}^{p^n-1} a_{ts}\lambda_{p^{n-i}b_i+s}\,, \qquad a_{ts} \in K.$$

Then (2) says that $a_{ts} \in \pi^{\lceil (t-s+\mathfrak{c})/p^n \rceil}\mathfrak{O}_K$ when $t \neq s$, a condition which is independent of i, and each diagonal coefficient a_{tt} is congruent mod $\pi^{\lceil \mathfrak{c}/p^n \rceil}$ to either 0 or a unit of $\mathfrak{O}_K$, according to a criterion involving i as well as t. We observe that the matrix of exponents $(\lceil t-s+\mathfrak{c}/p^n \rceil)_{1 \leqslant t,s \leqslant p^n}$ is constant on each of the $2p^n-1$ diagonals (from top left to bottom right) and the main diagonal $t = s$ resides within a band of p^n diagonals where the exponent is $\lceil \mathfrak{c}/p^n \rceil$. How this band straddles the main diagonal depends on the residue class $\mathfrak{c}$ mod p^n.

Remark 2.5. — In all the examples of A-scaffolds known to date, we can take all the units $u_{i,t}$ in Definition 2.3 (2) to be 1. Moreover, we can assume $\lambda_{t_1} = \pi^{(t_1-t_2)/p^n}\lambda_{t_2}$, for some fixed uniformizing parameter π of K, whenever $t_1 \equiv t_2 \pmod{p^n}$. The extra generality allowed in Definition 2.3 does not significantly add to the complexity of our arguments, and is included since the flexibility it provides may be useful in future applications.

The reader should keep in mind the following situation.

Definition 2.6 (Galois scaffold). — *Suppose that L/K is a Galois extension with Galois group G. We will call a $K[G]$-scaffold on L a* Galois scaffold *if the residue field κ is perfect and the shift parameters b_i of the scaffold are the (lower) ramification breaks $b_1 \leqslant \cdots \leqslant b_n$ of L/K, counted with multiplicity in the following sense: we set $b_i = \max\{j : |G_j| > p^{n-i}\}$ where $G_j = \{\sigma \in G : (\sigma - 1)\mathfrak{O}_L \subseteq \mathfrak{P}_L^{j+1}\}$ is the jth ramification group. In* *particular, the existence of a Galois scaffold means that the ramification breaks b_i are prime to p.*

Remark 2.7. — In the setting of Definition 2.6, L has a subfield F such that F/K is Galois of degree p with ramification break b_1. Moreover, we have $b_i \equiv b_1 \pmod p$ for all i by [37, IV §2 Prop. 11], and $p \nmid b_1$ unless K has characteristic 0 and b_1 attains its maximal value, cf. (2.3) below. Thus the requirement $p \nmid b_i$ in Definition 2.6 is very mild.

As explained in the Appendix, the Galois scaffolds considered in [13, 14, 19] are all Galois scaffolds in the sense of Definition 2.6.

Example 2.8 (Galois extensions of degree p). — We show that a totally ramified Galois extension L/K of degree p admits a Galois scaffold in almost all cases. There is a unique ramification break b_1, which in characteristic p may be any positive integer relatively prime to p. In characteristic 0 we have

$$b_1 \leqslant pv_K(p)/(p-1), \text{ and } p \nmid b_1 \text{ unless } b_1 = pv_K(p)/(p-1); \tag{2.3}$$

see [37, IV,§2, Prop. 11 and Ex. 3].)

If we exclude the exceptional case $b_1 = pv_K(p)/(p-1)$ in characteristic 0 then $p \nmid b_1$, and we can obtain a Galois scaffold as follows. Let $\Psi_1 = \sigma - 1$, where σ is any generator of $\mathrm{Gal}(L/K)$, let π be a uniformizing parameter of K, and let $\rho \in L$ with $v_L(\rho) = b_1$. Then $\mathfrak{b} : \mathbb{S}_p \longrightarrow \mathbb{Z}$ and $\mathfrak{a} : \mathbb{Z} \to \mathbb{S}_p$ are given by $\mathfrak{b}(s) = b_1 s$ and $b_1\mathfrak{a}(t) \equiv -t \pmod p$. In particular, $\mathfrak{a}(b_1) = p-1$. For each $t \in \mathbb{Z}$, put $f_t = (t - b_1 - b_1\mathfrak{a}(b_1 - t))/p \in \mathbb{Z}$. Then the elements $\lambda_t := \pi^{f_t}\Psi_1^{\mathfrak{a}(b_1-t)} \cdot \rho$ satisfy condition (1) of Definition 2.3. Also, $\Psi_1 \cdot 1 = 0$, and $\Psi_1 \cdot \lambda_t = \lambda_{t+b_1}$ unless $\mathfrak{a}(b_1 - t) = p-1$. But $\mathfrak{a}(b_1 - t) = p-1$ precisely when $t \equiv 0 \pmod p$, in which case $t = v_L(\lambda_t) = pf_t + pb_1$, $\mathfrak{a}(t) = 0$, and $\Psi_1 \cdot \lambda_t = \pi^{f_t}\Psi_1^p \cdot \rho$. If K has characteristic p then $\Psi_1^p = (\sigma-1)^p = 0$, so $\Psi_1 \cdot \lambda_t = 0$ and we have a Galois scaffold of precision $\mathfrak{c} = \infty$. Now suppose that K has characteristic 0. Expanding $(\Psi_1 + 1)^p = \sigma^p = 1$, we have $\Psi_1^p = -\sum_{j=1}^{p-1}\binom{p}{j}\Psi_1^j$. Hence

$$\begin{aligned} v_L(\Psi_1 \cdot \lambda_t) &= v_L\left(\pi^{f_t} p \Psi_1 \cdot \rho\right) \\ &= pf_t + pv_K(p) + b_1 + v_L(\rho) \\ &= (t - pb_1) + pv_K(p) + 2b_1 . \end{aligned}$$

Thus $v_L(\Psi_1 \cdot \lambda_t) = t + b_1 + [pv_K(p) - (p-1)b_1]$ when $\mathfrak{a}(t) = 0$, so we have a Galois scaffold of precision $\mathfrak{c} = pv_K(p) - (p-1)b_1$.

Remark 2.9. — If we replace the element Ψ_i in an A-scaffold by $\pi\Psi_i$, where π is some uniformizing parameter of K, then we obtain a new scaffold with the same precision $\mathfrak{c}$, but with the shift parameter b_i replaced by $b_i + p^i$. Suppose that L/K is a Galois extension with ramification breaks $b_1, \ldots, b_n$. If there exists a Galois scaffold on L (whose shift parameters are, by definition, the b_i), we can adjust the Ψ_i by powers of π to obtain a $K[G]$-scaffold whose shift parameters are any integers b_i' with $b_i' \equiv b_i \pmod{p^i}$; this new scaffold will in general not be a Galois scaffold, since its shift parameters will not coincide with the ramification breaks. We do not know whether it is possible to have a $K[G]$-scaffold on a Galois extension L/K with shift parameters $b_1', \ldots, b_n'$ that do not satisfy the congruences $b_i' \equiv b_i \pmod{p^i}$. We do know from [13], however, that if L/K is a $C_3 \times C_3$-extension in characteristic 3, and there exists a $K[G]$-scaffold on L with precision $\mathfrak{c} \geqslant 1$ and some shift parameters b_1', b_2', then there will also exist a Galois scaffold on L (with the ramification breaks b_1, b_2 as its shift parameters) of precision $\mathfrak{c} = \infty$.

Remark 2.10. — In an earlier version of this paper, we called $\mathfrak{c}$ the "tolerance" of the scaffold, and this terminology is used by Koch in [27]. We thank the referee for suggesting the more satisfactory word "precision".

For each $s = \sum_{i=1}^{n} s_{(n-i)} p^{n-i} \in \mathbb{S}_{p^n}$, let $\Upsilon^{(s)}$ be the set of monomials in the (not necessarily commuting) elements Ψ_i such that, for each $1 \leqslant i \leqslant n$, the exponents associated with Ψ_i in the monomial sum to $s_{(n-i)}$. We write $\Psi^{(s)}$ for the distinguished element

$$\Psi^{(s)} = \Psi_n^{s_{(0)}} \Psi_{n-1}^{s_{(1)}} \cdots \Psi_1^{s_{(n-1)}} \in \Upsilon^{(s)}. \tag{2.4}$$

When A is commutative, we have $\Upsilon^{(s)} = \{\Psi^{(s)}\}$.

Suppose that we have an A-scaffold as in Definition 2.3. Then it follows inductively that if $t \in \mathbb{Z}$, $s \in \mathbb{S}_{p^n}$ and $\Psi \in \Upsilon^{(s)}$ then there is a unit $U_{\Psi,t} \in \mathfrak{O}_K^\times$ such that, modulo $\lambda_{t+\mathfrak{b}(s)} \mathfrak{P}_L^{\mathfrak{c}}$, we have

$$\Psi \cdot \lambda_t \equiv \begin{cases} U_{\Psi,t} \lambda_{t+\mathfrak{b}(s)} & \text{if } s \preceq \mathfrak{a}(t), \\ 0 & \text{otherwise,} \end{cases} \tag{2.5}$$

and hence

$$v_L(\Psi \cdot \lambda_t) \begin{cases} = t + \mathfrak{b}(s) & \text{if } s \preceq \mathfrak{a}(t), \\ \geqslant t + \mathfrak{b}(s) + \mathfrak{c} & \text{otherwise.} \end{cases} \tag{2.6}$$

Thus we have

$$\Psi \cdot \mathfrak{P}_L^t \subseteq \mathfrak{P}_L^{t+\mathfrak{b}(s)} \text{ for all } \Psi \in \Upsilon^{(s)},\ s \in \mathbb{S}_{p^n},\ t \in \mathbb{Z}. \tag{2.7}$$

In particular, (2.5), (2.6) and (2.7) hold for $\Psi = \Psi^{(s)}$.

Remark 2.11. — Consider the special case of Definition 2.3 when the precision is infinite, $\mathfrak{c}=\infty$, and the units are trivial, $u_{i,t}=1$ for all i, t. Taking $\Psi=\Psi^{(s)}$ in (2.5), we then have the equality

$$\Psi^{(s)}\cdot\lambda_t=\begin{cases}\lambda_{t+\mathfrak{b}(s)} & \text{if } s\preceq\mathfrak{a}(t),\\ 0 & \text{otherwise.}\end{cases}$$

From this we may check that $\{\Psi^{(s)}:s\in\mathbb{S}_{p^n}\}$ is a K-basis of A and that L is a free A-module of rank 1 (cf. Proposition 2.12 below). Moreover, $\Psi^{(r)}\cdot(\Psi^{(s)}\cdot\lambda_t)=\Psi^{(s)}\cdot(\Psi^{(r)}\cdot\lambda_t)$ for all r, $s\in\mathbb{S}_{p^n}$ and all $t\in\mathbb{Z}$, so that the algebra A is commutative in this case. In general, there are two potential sources of noncommutativity in A, namely the "error terms" which are implied by the congruences of Definition 2.3 (2), and the units $u_{i,t}$.

To help fix ideas, we specialize further, assuming in addition that the shift parameters all satisfy $b_i=1$. (Any totally and weakly ramified p-extension in characteristic p has a scaffold satisfying these conditions; see §4.2 below.) Then $\mathfrak{b}(s)=s$ for all $s\in\mathbb{S}_{p^n}$, and (2.7) states that

$$\Psi^{(s)}\cdot\mathfrak{P}_L^t\subseteq\mathfrak{P}_L^{t+s}\text{ for all } s\in\mathbb{S}_{p^n},\ t\in\mathbb{Z}.$$

The Normal Basis Theorem ensures, in the Galois case, that L is a free $K[G]$-module of rank 1. We now show that a similar assertion holds whenever we have an A-scaffold. Furthermore, L/K satisfies the stronger condition of having a "valuation criterion" for its A-module generator.

Proposition 2.12. — *Let L/K have an A-scaffold of precision $\mathfrak{c}\geqslant 1$. Then $\{\Psi^{(s)}:s\in\mathbb{S}_{p^n}\}$ is a K-basis of A. Moreover, let b be any integer that satisfies $\mathfrak{a}(b)=p^n-1$, and let $\rho\in L$ with $v_L(\rho)=b$. Then L is a free A-module on the generator ρ. Additionally, for each $h\in\mathbb{Z}$, the ring $\mathfrak{A}(h,A)=\{\alpha\in A:\alpha\cdot\mathfrak{P}_L^h\subseteq\mathfrak{P}_L^h\}$ is an $\mathfrak{O}_K$-order in A.*

Proof. — Since $\mathfrak{a}\colon\mathbb{S}_{p^n}\to\mathbb{S}_{p^n}$ is bijective, the condition $\mathfrak{a}(b)=p^n-1$ determines b uniquely mod p^n. We have $\rho=u\lambda_b+\sum_{i>b}a_i\lambda_i$ for $u\in\mathfrak{O}_K^\times$ and $a_i\in\mathfrak{O}_K$. From (2.6), for $i>b$ and for each $s\in\mathbb{S}_{p^n}$ we have $v_L(\Psi^{(s)}\cdot a_i\lambda_i)>v_L(\Psi^{(s)}\cdot u\lambda_b)=b+\mathfrak{b}(s)$. Thus $v_L(\Psi^{(s)}\cdot\rho)=b+\mathfrak{b}(s)$ for each $s\in\mathbb{S}_{p^n}$. Since $\mathfrak{b}:\mathbb{S}_{p^n}\longrightarrow\mathbb{S}_{p^n}$ is surjective, these valuations represent all residue classes mod p^n. As L/K is totally ramified, it follows that $\{\Psi^{(s)}\cdot\rho:s\in\mathbb{S}_{p^n}\}$ is a K-basis for L. Thus $A\cdot\rho=L$, and, comparing dimensions, L is a free A-module on the generator ρ. Moreover, the $\Psi^{(s)}$ must be linearly independent over K. Since $\dim_K A=p^n$, it follows that the $\Psi^{(s)}$ form a K-basis of A. As L is a free A-module and $\mathfrak{P}_L^h$ spans L over K, it is immediate that $\mathfrak{A}(h,A)$ is an $\mathfrak{O}_K$-order in A. $\square$

Remark 2.13. — Suppose we have a Galois scaffold on an abelian extension L/K. By the Hasse–Arf Theorem [37, V, §7], the ramification breaks $u_1, \dots, u_n$ in the upper numbering are integers. Translating to the lower numbering, we obtain the congruences $b_i \equiv b_n \pmod{p^i}$. Thus we have $\mathfrak{b}(s) \equiv b_n s \pmod{p^n}$ and $b_n \mathfrak{a}(t) \equiv -t \pmod{p^n}$. In particular, we can then take b in Proposition 2.12 to be b_n. The same will hold if L/K is a nonabelian Galois extension which satisfies the conclusion of the Hasse–Arf theorem.

If L/K is a Galois extension not necessarily satisfying the conclusion of the Hasse–Arf Theorem, then the u_i need not be integers. In this case, the condition $\mathfrak{a}(b) = p^n - 1$ is equivalent to $b \equiv b_n - p^n u_n \pmod{p^n}$. Thus Proposition 2.12 agrees with the valuation criterion for a normal basis generator in [20].

3. Integral A-module structure

3.1. Statement of the main results

Fix L/K and A as in §2. Assume that there is an A-scaffold on L of precision $\mathfrak{c} \geqslant 1$ as in Definition 2.3. Thus we have shift parameters $b_1, \dots, b_n$ and the associated functions $\mathfrak{b}$ and $\mathfrak{a}$, as well as elements $\lambda_t \in L$ with $v_L(\lambda_t) = t$ for each $t \in \mathbb{Z}$. By Proposition 2.12, we also have a K-basis $\{\Psi^{(s)} : s \in \mathbb{S}_{p^n}\}$ of A. We choose once and for all a uniformizing parameter π of K.

Now let $h \in \mathbb{Z}$, and consider the fractional $\mathfrak{O}_L$-ideal $\mathfrak{P}_L^h$ as a module over its associated order

$$\mathfrak{A} := \mathfrak{A}(h, A) = \{\alpha \in A : \alpha \cdot \mathfrak{P}_L^h \subseteq \mathfrak{P}_L^h\} \tag{3.1}$$

in A. If $h' = h + p^n m$ for some $m \in \mathbb{Z}$ then $\mathfrak{P}_L^{h'} = \pi^m \mathfrak{P}_L^h$. It follows that $\mathfrak{A}(h', A) = \mathfrak{A}(h, A)$, and that $\mathfrak{P}_L^{h'}$ and $\mathfrak{P}_L^h$ are isomorphic as modules over this order. Thus h only matters up to congruence mod p^n.

Let $\mathbb{S}_{p^n}(h) = \{t \in \mathbb{Z} \ : \ h \leqslant t < h + p^n\}$. Note that $\mathbb{S}_{p^n}(0) = \mathbb{S}_{p^n}$, and that $\{\lambda_t \ : \ t \in \mathbb{S}_{p^n}(h)\}$ is an $\mathfrak{O}_K$-basis for $\mathfrak{P}_L^h$. We now fix a specific choice of b in Proposition 2.12 (where b was only determined mod p^n) by stipulating

$$\mathfrak{a}(b) = p^n - 1, \qquad b \in \mathbb{S}_{p^n}(h). \tag{3.2}$$

Thus we have $L = A \cdot \lambda_b$.

For each $s \in \mathbb{S}_{p^n}$ we define

$$d(s) = \left\lfloor \frac{\mathfrak{b}(s) + b - h}{p^n} \right\rfloor. \tag{3.3}$$

In particular, $d(0) = 0$ since $b - h \in \mathbb{S}_{p^n}$. We also define

$$w(s) = \min\{d(u) - d(u - s) \ : \ u \in \mathbb{S}_{p^n},\ u \succeq s\}. \tag{3.4}$$

Using Lemma 2.1, we have

$$w(s) = \min\{d(s + j) - d(j) \ : \ j \in \mathbb{S}_{p^n},\ j \preceq p^n - 1 - s\}.$$

In particular, $d(s) - 1 \leqslant w(s) \leqslant d(s) - d(0) = d(s)$ for all $s \in \mathbb{S}_{p^n}$. Note that whether or not the upper bound $w(s) = d(s)$ is achieved depends only on the residue classes b_i mod p^i, not the integers b_i themselves. In any case, it is important to realize that both $d(s)$ and $w(s)$, as well as b and $b - h$, depend on $b_1, \dots, b_n$ and on h, although we do not indicate this dependence explicitly in our notation.

For $s \in \mathbb{S}_{p^n}$, we normalize the $\Psi^{(s)}$ in (2.4), and set

$$\Phi^{(s)} = \pi^{-w(s)} \Psi^{(s)}.$$

The first of our main results explains how the existence of an A-scaffold of high enough precision allows us to give an explicit description of $\mathfrak{A}$, and to determine whether or not $\mathfrak{P}_L^h$ is free over $\mathfrak{A}$, using only the numerical invariants $w(s)$ and $d(s)$.

Theorem 3.1. — *Let L/K admit an A-scaffold of precision $\mathfrak{c}$ with shift parameters $b_1, \dots, b_n$. Fix a fractional ideal $\mathfrak{P}_L^h$, and let $\mathfrak{A}$, b, $d(s)$ and $w(s)$ be defined as in (3.1)–(3.4).*

(1) *Suppose that $\mathfrak{c} \geqslant \max(b - h, 1)$. Then $\{\Phi^{(s)} : s \in \mathbb{S}_{p^n}\}$ is an $\mathfrak{O}_K$-basis of $\mathfrak{A}$. If $w(s) = d(s)$ for all $s \in \mathbb{S}_{p^n}$, then $\mathfrak{P}_L^h$ is free over $\mathfrak{A}$ with $\mathfrak{P}_L^h = \mathfrak{A} \cdot \lambda_b$.*

(2) *Now suppose that the stronger condition $\mathfrak{c} \geqslant p^n + b - h$ holds. Then $\mathfrak{P}_L^h$ is free over $\mathfrak{A}$ if and only if $w(s) = d(s)$ for all $s \in \mathbb{S}_{p^n}$. Moreover, when $\mathfrak{P}_L^h$ is free over $\mathfrak{A}$, we have $\mathfrak{P}_L^h = \mathfrak{A} \cdot \rho$ for any $\rho \in L$ with $v_L(\rho) = b$.*

Remark 3.2. — Since b was chosen so that $b - h \in \mathbb{S}_{p^n}$, the stronger condition $\mathfrak{c} \geqslant p^n + b - h$ holds for all ideals if the A-scaffold has precision $\mathfrak{c} \geqslant 2p^n - 1$.

Example 3.3 (Galois extensions of degree p). — For a totally ramified Galois extension L/K of degree p, the Galois module structure, both of the valuation ring $\mathfrak{O}_L$ and of its fractional ideals $\mathfrak{P}_L^h$, has been studied extensively. We briefly review the existing results and relate them to Theorem 3.1.

For the valuation ring itself, we have $h = 0$, so the number b in Theorem 3.1 is just the least positive residue $r(b_1)$ of b_1 mod p. For K of characteristic 0, Bertrandias and Ferton [5] show that $\mathfrak{O}_L$ is free over its associated order if and only if b divides $p-1$, provided that b_1 is not too close to its maximal value. (See [4] for the excluded cases.) Now $d(s) = \lfloor (b_1 s + b)/p \rfloor$, and one can verify that our condition $w(s) = d(s)$ in this case is equivalent to $b \mid (p-1)$. We therefore recover the result of Bertandias and Ferton whenever we have a Galois scaffold with $\mathfrak{c} \geqslant b + p$; by Example 2.8, this occurs when

$$b_1 < \frac{p v_K(p)}{p-1} - 2\,. \tag{3.5}$$

In characteristic p, Aiba [1] gives a different condition for $\mathfrak{O}_L$ to be free, but his condition can be shown to be equivalent to $b \mid (p-1)$; de Smit and Thomas [39] also obtain $b \mid (p-1)$. Since there is a Galois scaffold with $\mathfrak{c} = \infty$, these results follow from our Theorem 3.1, exactly as in characteristic 0 (but with no upper bound on b_1).

We now consider arbitrary ideals $\mathfrak{P}_L^h$. In characteristic 0, Ferton [21] determines which ideals are free over their associated orders, giving her result in terms of the continued fraction expansion of b_1/p. A corresponding result in characteristic p is given by Huynh [24], who gives a different criterion but proves it is equivalent to Ferton's. Our condition, $w(s) = d(s)$ for all s, must therefore be equivalent to Ferton's continued fraction criterion. This equivalence is verified in [31] (which also contains some partial results relating our Theorem 3.6 below to continued fractions). Given this equivalence, and assuming (3.5) in the characteristic 0 case, the results of Ferton and Huynh follow from our Theorem 3.1.

The following example considers another situation where the technical details associated with Theorem 3.1 are easy to digest.

Example 3.4 ($b_i \equiv -1$). — Suppose that L/K is a totally ramified extension of degree p^n (for arbitrary $n \geqslant 1$) which admits an A-scaffold with precision $\mathfrak{c} \geqslant p^n - 1$ such that $b_i \equiv -1 \pmod{p^i}$ for each i. We consider the valuation ring $\mathfrak{O}_L$ (so $h = 0$). Write $b_i = -1 + m_i p^i$ with $m_i \in \mathbb{Z}$. Using (2.2), we see that $\mathfrak{b}(s) = -s + (\sum_{i=1}^n s_{(n-i)} m_i) p^n \equiv -s \pmod{p^n}$. Thus $b = p^n - 1$ and $d(s) = \sum_{i=1}^n s_{(n-i)} m_i = \sum_{i=1}^n s_{(n-i)} d(p^{n-i})$. In particular, $d(s) + d(j) = d(s+j)$ for all $j \in \mathbb{S}_{p^n}$ with $j \preceq p^n - 1 - s$, so that $w(s) = d(s)$ for all s. Moreover, $w(s) = \sum_{i=0}^{n-1} s_{(i)} w(p^i)$. Thus by

Theorem 3.1 (1), $\mathfrak{O}_L$ is free over $\mathfrak{A}$, and $\mathfrak{A}$ has the particularly simple form:

$$\mathfrak{A} = \mathfrak{O}_K \left[\pi^{-m_1}\Psi_1, \pi^{-m_2}\Psi_2, \ldots, \pi^{-m_n}\Psi_n\right].$$

We make one further remark, concerning the precision in Theorem 3.1.

Remark 3.5. — In some cases it is possible to relax the assumptions on $\mathfrak{c}$ in Theorem 3.1 at the expense of stronger assumptions on the Ψ_i in Definition 2.3. For example, in [13, Thm. 1.1] we give a freeness criterion, which is equivalent to that in Theorem 3.1 (2), for the valuation ring of a cyclic extension of degree p^2 in characteristic p admitting a different sort of "scaffold". From the perspective of Definition 2.3, this is a Galois scaffold of precision $\mathfrak{c} = b_2 - pb_1$, but this value is not used in the proof of the result. In fact, although the residue class $b_1 \equiv b_2 \pmod{p^2}$ satisfied by the ramification breaks could be any class mod p^2 relatively prime to p, the proof of the result requires only that the "scaffold" have precision $\mathfrak{c} \geqslant 1$. In contrast, we would need to assume that $\mathfrak{c} \geqslant 2p^2 - 1$ to guarantee that Theorem 3.1 applies for all possible values of the ramification breaks. The result in [13] depends on the fact that the "scaffold" there satisfies the additional relations $\Psi_1^p = \Psi_2$ and $\Psi_2^p = 0$.

The second of our main results, Theorem 3.6, adapts the techniques of [39] (see in particular Theorem 4) to extract some further information from the numerical data $d(s)$ and $w(s)$. For $s, t \in \mathbb{S}_{p^n}$, we write $s \prec t$ if $s \preceq t$ and $s \neq t$. Let

$$\begin{aligned}\mathcal{D} &= \{u \in \mathbb{S}_{p^n} : d(u) > d(u-s) + w(s) \text{ for all } s \in \mathbb{S}_{p^n} \text{ with } 0 \prec s \preceq u\};\\ \mathcal{E} &= \{u \in \mathbb{S}_{p^n} : w(u) > w(u-s) + w(s) \text{ for all } s \in \mathbb{S}_{p^n} \text{ with } 0 \prec s \prec u\}.\end{aligned}$$

Note that $0 \in \mathcal{D}$ and $0, 1, p, \ldots, p^{n-1} \in \mathcal{E}$ since there are no relevant s in these cases. Thus we always have $|\mathcal{D}| \geqslant 1$ and $|\mathcal{E}| \geqslant n+1$. Again, the dependence on h and on the b_i is suppressed from the notation.

Theorem 3.6. — *Let L/K be as in Theorem 3.1, with the strong condition $\mathfrak{c} \geqslant p^n + b - h$. Then the minimal number of generators of the $\mathfrak{A}$-module $\mathfrak{P}_L^h$ is $|\mathcal{D}|$. Also, $\mathfrak{A}$ is a (not necessarily commutative) local ring with residue field $\kappa = \mathfrak{O}_K/\mathfrak{P}_K$, and, writing $\mathfrak{M}$ for its unique maximal ideal, the embedding dimension $\dim_\kappa(\mathfrak{M}/\mathfrak{M}^2)$ of $\mathfrak{A}$ is $|\mathcal{E}|$.*

Since L is a free A-module by Proposition 2.12, the minimal number of generators of $\mathfrak{P}_L^h$ over $\mathfrak{A}$ is one precisely when $\mathfrak{P}_L^h$ is free over $\mathfrak{A}$.

3.2. Proofs

We keep the notation of the previous subsection. In particular, L/K admits an A-scaffold with precision $\mathfrak{c} \geqslant 1$ and with shift parameters $b_1 \ldots, b_n$, giving rise to the functions $\mathfrak{b} : \mathbb{S}_{p^n} \to \mathbb{Z}$ and $\mathfrak{a} : \mathbb{S}_{p^n} \to \mathbb{S}_{p^n}$. We fix $h \in \mathbb{Z}$ and study the ideal $\mathfrak{P}_L^h$ as a module over its associated order $\mathfrak{A} := \mathfrak{A}(h, a)$. Recall that b is the unique integer satisfying (3.2).

Our goal in this subsection is to prove Theorems 3.1 and 3.6, but we first provide an overview of the strategy of the proofs. The reader might find it helpful initially to consider the special case $\mathfrak{c} = \infty$, $u_{i,t} = 1$ in Remark 2.11 (which forces A to be commutative), and further to suppose that $b_1 = \cdots = b_n = b$, so that $\mathfrak{b}(s) = bs$.

Let $t \in \mathbb{S}_{p^n}(h)$ and $s \in \mathbb{S}_{p^n}$. If $s \preceq \mathfrak{a}(t)$ and $\Psi \in \Upsilon^{(s)}$ then by (2.6) the element $\Psi \cdot \lambda_t$ has valuation $t + \mathfrak{b}(s)$. We wish to relate this element to the $\mathfrak{O}_K$-basis $\{\lambda_m : m \in \mathbb{S}_{p^n}(h)\}$ of $\mathfrak{P}_L^h$, so, for any $t \in \mathbb{S}_{p^n}(h)$ and $s \in \mathbb{S}_{p^n}$, we write

$$t + \mathfrak{b}(s) = H(s,t) + p^n D(s,t) \quad \text{with } H(s,t) \in \mathbb{S}_{p^n}(h). \tag{3.6}$$

Thus we have

$$D(s,t) = \left\lfloor \frac{t + \mathfrak{b}(s) - h}{p^n} \right\rfloor, \qquad H(s,t) = h + r(t + \mathfrak{b}(s) - h). \tag{3.7}$$

In particular, comparing with (3.3), we have

$$D(s,b) = d(s). \tag{3.8}$$

By Proposition 2.12, λ_b has the normal basis property $L = A \cdot \lambda_b$, so we seek to compare $\Psi^{(s)} \cdot \lambda_t$ with $\Psi^{(u)} \cdot \lambda_b$ where $u \in \mathbb{S}_{p^n}$ is chosen to make the valuations of these elements agree mod p^n. Thus we require $H(u,b) = H(s,t)$. There will be a unique u with this property, since $H(u,b)$ realizes each element of $\mathbb{S}_{p^n}(h)$ exactly once as u varies in $\mathbb{S}_{p^n}$.

In order to translate between t and u (for a fixed s), we will need a number of facts which depend on the properties of $\mathfrak{b}$ and $\mathfrak{a}$ given in Lemma 2.2. These facts are recorded in Lemma 3.7. We are interested in the valuations of the elements $\Phi^{(s)} \cdot \lambda_t = \pi^{-w(s)} \Psi^{(s)} \cdot \lambda_t$ or, more generally, $\pi^{-w(s)} \Psi \cdot \lambda_t$ for any $\Psi \in \Upsilon^{(s)}$. In Proposition 3.8 we determine some of these valuations precisely, and bound the rest in terms of $\mathfrak{c}$. To prove Theorem 3.1, we then use this information to obtain an explicit description of the associated order $\mathfrak{A}$ and to determine when $\mathfrak{P}_L^h$ is free over $\mathfrak{A}$.

Before proving Theorem 3.6, we need to deal with the fact that $\mathfrak{A}$ need not in general be commutative. We show in Proposition 3.9 that any two of our basis elements $\Phi^{(r)}$, $\Phi^{(s)}$ of $\mathfrak{A}$ commute mod $\pi\mathfrak{A}$ up to multiplication by a unit in $\mathfrak{O}_K$.

We begin the proof of Theorem 3.6 by showing that the $\mathfrak{O}_K$-lattice $\mathfrak{M}$ in $\mathfrak{A}$, spanned by π and the $\Phi^{(s)}$ for $s \neq 0$, is the unique maximal ideal of $\mathfrak{A}$. Since $\Psi_i \cdot 1 = 0$, it is easy to see that $\mathfrak{M}$ is an ideal of $\mathfrak{A}$, and that $\mathfrak{A}/\mathfrak{M} \cong \kappa$, the residue field of K. To show the uniqueness, we check that $\mathfrak{M}$ is topologically nilpotent. This is easy to see in the special case considered in Remark 2.11, where A is commutative and $\Psi_i^p = 0$ for each i. In general, we use Proposition 3.9 to show that $\mathfrak{M}$ is topologically nilpotent.

Once we have established that $\mathfrak{M}$ is the unique maximal ideal of $\mathfrak{A}$ (so that $\mathfrak{A}$ is a local ring), it follows by Nakayama's Lemma that the minimal number of generators for the $\mathfrak{A}$-module $\mathfrak{P}_L^h$ (resp. $\mathfrak{M}$) is just the dimension of $\mathfrak{P}_L^h/\mathfrak{M}\cdot\mathfrak{P}_L^h$ (resp. $\mathfrak{M}/\mathfrak{M}^2$) as a vector space over κ. To determine these dimensions, we take the obvious $\mathfrak{O}_K$-basis of $\mathfrak{P}_L^h$ (resp. $\mathfrak{M}$), which is indexed by the partially ordered set $\mathbb{S}_{p^n}$. Some of these generators are redundant because they can be obtained by the action of $\mathfrak{A}$ on another generator occurring earlier in the partial order. Removing these redundant generators will leave a basis of the appropriate κ-vector space, since, by hypothesis, the precision of the scaffold is too high to allow any further relations between the surviving generators.

This concludes our overview of the proofs, and we now start the detailed arguments.

Lemma 3.7. — *Fix $s \in \mathbb{S}_{p^n}$, and let $t \in \mathbb{S}_{p^n}(h)$ and $u \in \mathbb{S}_{p^n}$ satisfy $H(u,b) = H(s,t)$. Then we have*

$$s \preceq \mathfrak{a}(t) \Leftrightarrow s \preceq u,$$

Moreover, when $s \preceq \mathfrak{a}(t)$, the following hold:

1. $\mathfrak{a}(H(s,t)) = \mathfrak{a}(t) - s$;
2. $u = p^n - 1 + s - \mathfrak{a}(t)$;
3. $t = H(u-s,b)$;
4. $D(s,t) = d(u) - d(u-s)$.

Proof. — Let $s \preceq \mathfrak{a}(t)$. By Lemma 2.2, we have $\mathfrak{b}(s) + \mathfrak{b}(\mathfrak{a}(t) - s) = \mathfrak{b}(\mathfrak{a}(t)) \equiv -t \pmod{p^n}$. Using (3.7), it follows that $H(s,t) \equiv t + \mathfrak{b}(s) \equiv -\mathfrak{b}(\mathfrak{a}(t)-s) \pmod{p^n}$. Applying $\mathfrak{a}$ gives (1). Similarly, as $u \preceq \mathfrak{a}(b) = p^n - 1$, we have $H(u,b) \equiv b + \mathfrak{b}(u) \equiv \mathfrak{b}(u) - \mathfrak{b}(p^n-1) = -\mathfrak{b}(p^n-1-u)$. Since $H(s,t) = H(u,b)$, we therefore have $\mathfrak{a}(t) - s = p^n - 1 - u$, giving (2), and thus $\mathfrak{a}(t)_{(n-i)} - s_{(n-i)} = (p-1) - u_{(n-i)}$ for $1 \leqslant i \leqslant n$, since $s \preceq \mathfrak{a}(t)$ by hypothesis. Hence $s_{(n-i)} = u_{(n-i)} - (p-1-\mathfrak{a}(t)_{(n-i)})$ for each i, so that $s \preceq u$. This shows the implication $s \preceq \mathfrak{a}(t) \Rightarrow s \preceq u$. The reverse implication follows since the sets $\{t \in \mathbb{S}_{p^n}(h) : s \preceq \mathfrak{a}(t)\}$ and $\{u \in \mathbb{S}_{p^n} : s \preceq u\}$ have the same cardinality.

It remains to prove (3) and (4). Still assuming $s \preceq \mathfrak{a}(t)$, we have from (3.7) that

$$\begin{aligned} H(u-s,b) &\equiv b + \mathfrak{b}(u-s) \\ &\equiv b + \mathfrak{b}(p^n - 1 - \mathfrak{a}(t)) \\ &\equiv b + \mathfrak{b}(p^n-1) + t \\ &\equiv t \pmod{p^n}, \end{aligned}$$

and (3) follows as both sides are in $\mathbb{S}_{p^n}(h)$. Finally, using (3.6) and (3.8), we have

$$\begin{aligned} p^n D(s,t) &= t + \mathfrak{b}(s) - H(s,t) \\ &= H(u-s,b) + \mathfrak{b}(s) - H(u,b) \\ &= [b + \mathfrak{b}(u-s) - p^n D(u-s,b)] + \mathfrak{b}(s) - [b + \mathfrak{b}(u) - p^n D(u,b))] \\ &= p^n d(u) - p^n d(u-s), \end{aligned}$$

since $\mathfrak{b}(u-s) = \mathfrak{b}(u) - \mathfrak{b}(s)$ because $s \preceq u$. Dividing by p^n yields (4). □

It is immediate from Lemma 3.7 that we may rewrite (3.4) as

$$w(s) = \min\{D(s,t) : t \in \mathbb{S}_{p^n}(h),\ \mathfrak{a}(t) \succeq s\}. \tag{3.9}$$

Moreover, it then follows from (3.7) that if $s \preceq \mathfrak{a}(t)$ then either $D(s,t) = w(s)$ or $D(s,t) = w(s)+1$. We define

$$\epsilon(s,t) = D(s,t) - w(s) \in \{0,1\} \text{ for } s \preceq \mathfrak{a}(t). \tag{3.10}$$

Proposition 3.8. — *Suppose that the Ψ_i are as in Definition 2.3. Let $s \in \mathbb{S}_{p^n}$ and $t \in \mathbb{S}_{p^n}(h)$. Let Ψ be any element of $\Upsilon^{(s)}$, and set $\Phi = \pi^{-w(s)}\Psi$.*

(1) *If $s \preceq \mathfrak{a}(t)$ then there is a unit $y_{\Phi,t} \in \mathfrak{O}_K^\times$ such that*

$$\Phi \cdot \lambda_t \equiv \pi^{\epsilon(s,t)} y_{\Phi,t} \lambda_{H(s,t)} \pmod{\pi^{\epsilon(s,t)} \lambda_{H(s,t)} \mathfrak{P}_L^{\mathfrak{c}}}.$$

In particular,

$$v_L(\Phi\cdot\lambda_t) = \begin{cases} H(s,t) & \text{if } s \preceq \mathfrak{a}(t) \text{ and } \epsilon(s,t) = 0, \\ H(s,t) + p^n & \text{if } s \preceq \mathfrak{a}(t) \text{ and } \epsilon(s,t) = 1. \end{cases}$$

(2) *If $s \not\preceq \mathfrak{a}(t)$ then we have the bounds*

$$v_L(\Phi\cdot\lambda_t) \geqslant \begin{cases} H(s,b) + t - b + \mathfrak{c} & \text{if } s \not\preceq \mathfrak{a}(t) \text{ and } w(s) = d(s), \\ H(s,b) + t - b + p^n + \mathfrak{c} & \text{if } s \not\preceq \mathfrak{a}(t) \text{ and } w(s) \neq d(s) \end{cases}$$

Proof. — It follows from (3.6) and Definition 2.3 (1) that there is an $x \in \mathfrak{O}_K^\times$ so that $\lambda_{t+\mathfrak{b}(s)} = x\pi^{D(s,t)}\lambda_{H(s,t)}$.

(1). — If $s \preceq \mathfrak{a}(t)$ then (2.5) gives $\Psi \cdot \lambda_t \equiv U_{\Psi,t}\lambda_{t+\mathfrak{b}(s)} \pmod{\lambda_{t+\mathfrak{b}(s)}\mathfrak{P}_L^{\mathfrak{c}}}$. Multiplying by $\pi^{-w(s)}$ and setting $y_{\Phi,t} = xU_{\Psi,t}$ we obtain the required congruence. The remaining assertions follow immediately.

(2). — If $s \not\preceq \mathfrak{a}(t)$ then (2.5) gives $v_L(\Phi \cdot \lambda_t) \geqslant t + \mathfrak{b}(s) - p^n w(s) + \mathfrak{c}$. From (3.6) we have

$$t + \mathfrak{b}(s) = H(s,t) + p^n D(s,t) = t - b + H(s,b) + p^n D(s,b).$$

Hence, using (3.8),

$$v_L(\Phi \cdot \lambda_t) \geqslant t - b + H(s,b) + p^n(d(s) - w(s)) + \mathfrak{c},$$

and by (3.3) and (3.4) either $w(s) = d(s)$ or $w(s) = d(s) - 1$. The two cases give the stated inequalities. □

We can now prove the first of our main results,

Proof of Theorem 3.1.

(1). — Assume that $\mathfrak{c} \geqslant \max(b-h,1)$. By Proposition 3.8, we have for all $s \in \mathbb{S}_{p^n}$ and all $t \in \mathbb{S}_{p^n}(h)$ that $v_L(\Phi^{(s)} \cdot \lambda_t) \geqslant h$. Since $\{\lambda_t : t \in \mathbb{S}_{p^n}(h)\}$ is an $\mathfrak{O}_K$-basis of $\mathfrak{P}_L^h$, this shows that $\Phi^{(s)} \in \mathfrak{A}$ for all s. Any $\alpha \in A$ may be written $\alpha = \sum_{s \in \mathbb{S}_{p^n}} c_s \Phi^{(s)}$ for some $c_s \in K$. We have just shown that if $c_s \in \mathfrak{O}_K$ for all s then $\alpha \in \mathfrak{A}$. We must show, conversely, that if $\alpha \in \mathfrak{A}$ then each $c_s \in \mathfrak{O}_K$. Applying α to λ_b, we obtain $\alpha \cdot \lambda_b = \sum_s c_s \Phi^{(s)} \cdot \lambda_b$. But $s \preceq \mathfrak{a}(b) = p^n - 1$, so, for each s with $c_s \neq 0$, we have $v_L(c_s\Phi^{(s)} \cdot \lambda_b) \equiv H(s,b) \pmod{p^n}$ by Proposition 3.8 (1). These valuations are distinct mod p^n, so $v_L(c_s\Phi^{(s)} \cdot \lambda_b) \geqslant h$. Thus $c_s \in \mathfrak{O}_K$ if $\epsilon(s,b) = 0$, and $c_s \in \pi^{-1}\mathfrak{O}_K$ otherwise. Now assume for a contradiction that some $c_s \notin \mathfrak{O}_K$. Since $\epsilon(s,b) = 1$, we have $d(s) = D(s,b) = w(s) + 1$. By (3.9), there is some $t \in \mathbb{S}_{p^n}(h)$ with $\mathfrak{a}(t) \succeq s$ and $D(s,t) = w(s)$, so that $\epsilon(s,t) = 0$. Amongst these t, take the one with $H(s,t)$ minimal, and consider $\alpha \cdot \lambda_t = \sum_{j \in \mathbb{S}_{p^n}} c_j \Phi^{(j)} \cdot \lambda_t$. For the term $j = s$ we have

$$v_L(c_j\Phi^{(j)} \cdot \lambda_t) = v_L(c_s) + H(s,t) = -p^n + H(s,t) < h$$

by Proposition 3.8 (1). For the terms with $j \neq s$ but $j \preceq \mathfrak{a}(t)$, we have

$$v_L(c_j\Phi^{(j)} \cdot \lambda_t) > -p^n + H(s,t)$$

by Proposition 3.8 (1) again and the choice of t. For the terms with $j \not\preceq \mathfrak{a}(t)$, since $w(s) \neq d(s)$, we have

$$v_L(c_j\Phi^{(j)} \cdot \lambda_t) \geqslant v_L(c_j) + H(j,b) + t - b + p^n + \mathfrak{c} \geqslant h$$

by Proposition 3.8 (2) and the hypothesis on $\mathfrak{c}$. Hence

$$v_L(\alpha \cdot \lambda_t) = -p^n + H(s,t) < h\,,$$

giving the required contradiction.

(2). — Now assume that the stronger condition $\mathfrak{c} \geqslant p^n + b - h$ holds. Let ρ be an arbitrary element of $\mathfrak{P}_L^h$. We investigate when ρ is a free generator for $\mathfrak{P}_L^h$ over $\mathfrak{A}$. Since $\{\lambda_t : t \in \mathbb{S}_{p^n}(h)\}$ is an $\mathfrak{O}_K$-basis for $\mathfrak{P}_L^h$, we have $\rho = \sum_{t \in \mathbb{S}_{p^n}(h)} x_t \lambda_t$ for some $x_t \in \mathfrak{O}_K$. By Proposition 3.8 and the hypothesis on $\mathfrak{c}$, we therefore have

$$\Phi^{(s)} \cdot \rho \equiv \sum_t x_t y_{s,t} \pi^{\epsilon(s,t)} \lambda_{H(s,t)} \pmod{\pi \mathfrak{P}_L^h}\,,$$

where the sum is over those $t \in \mathbb{S}_{p^n}(h)$ with $s \preceq \mathfrak{a}(t)$. Using Lemma 3.7, we can rewrite this as

$$\Phi^{(s)} \cdot \rho \equiv \sum_{u \succeq s} c_{s,u} \lambda_{H(u,b)} \pmod{\pi \mathfrak{P}_L^h}\,,$$

where the sum is over $u \in \mathbb{S}_{p^n}$ satisfying $u \succeq s$, and where $c_{s,u} = x_t y_{s,t} \pi^{\epsilon(s,t)}$ for $t = H(u-s,b)$. The matrix $(c_{s,u})$ expressing the elements $\Phi^{(s)} \cdot \rho$ (ordered by increasing s) in terms of the basis elements $\lambda_{H(u,b)}$ (ordered by increasing u) is therefore upper triangular mod π. Thus the $\Phi^{(s)} \cdot \rho$ also form an $\mathfrak{O}_K$-basis of $\mathfrak{P}_L^h$ if and only if $c_{s,s} \in \mathfrak{O}_K^\times$ for all s. But when $u = s$, we have $t = H(0,b) = b$ and $D(s,t) = d(s)$. Since $x_b \in \mathfrak{O}_K$, $y_{s,b} \in \mathfrak{O}_K^\times$, and $d(s) \geqslant w(s)$, it follows that $\mathfrak{P}_L^h = \mathfrak{A} \cdot \rho$ if and only if $x_b \in \mathfrak{O}_K^\times$ and $d(s) = w(s)$ for all s. Thus $\mathfrak{P}_L^h$ is a free $\mathfrak{A}$-module on some generator ρ if and only if $d(s) = w(s)$ for all s. Moreover, if $v_L(\rho) = b$ then we must have $v_L(x_t \lambda_t) \geqslant b$ for all t, with equality for $t = b$. In particular, $x_b \in \mathfrak{O}_K^\times$. Hence ρ is a free generator for $\mathfrak{P}_L^h$ over $\mathfrak{A}$, provided that $d(s) = w(s)$ for all s. □

Proposition 3.9. — *Suppose that $\mathfrak{c} \geqslant p^n + b - h$ and let r, $s \in \mathbb{S}_{p^n}$. If $r \not\preceq p^n - 1 - s$ or if $w(r) + w(s) \neq w(r+s)$ then $\Phi^{(r)}\Phi^{(s)} \in \pi\mathfrak{A}$. In the remaining case that $r \preceq p^n - 1 - s$ and $w(r) + w(s) = w(r+s)$, there is some $c \in \mathfrak{O}_K^\times$ such that $\Phi^{(r)}\Phi^{(s)} - c\Phi^{(r+s)} \in \pi\mathfrak{A}$.*

Proof. — By Proposition 3.8 applied successively to $\Psi^{(s)}$ and $\Psi^{(r)}$, together with Lemma 3.7 (1), we have for any $t \in \mathbb{S}_{p^n}(h)$ that $\Phi^{(r)}\Phi^{(s)} \cdot \lambda_t \in \pi\mathfrak{P}_L^h$ unless $s \preceq \mathfrak{a}(t)$ and $r \preceq \mathfrak{a}(H(s,t)) = \mathfrak{a}(t) - s$. In particular, if $r \not\preceq p^n - 1 - s$ then $\Phi^{(r)}\Phi^{(s)} \cdot \lambda_t \in \pi\mathfrak{P}_L^h$ for all $t \in \mathbb{S}_{p^n}(h)$, so that $\Phi^{(r)}\Phi^{(s)} \in \pi\mathfrak{A}$.

Now suppose that $r \preceq p^n - 1 - s$. Applying Proposition 3.8 to $\Psi := \Psi^{(r)}\Psi^{(s)} \in \Upsilon^{(r+s)}$, we find that the element

$$\Phi := \pi^{-w(r+s)}\Psi = \pi^{w(r)+w(s)-w(r+s)}\Phi^{(r)}\Phi^{(s)}$$

satisfies $v_L(\Phi \cdot \lambda_t) \geqslant h$ for all $t \in \mathbb{S}_{p^n}(h)$, so that $\Phi \in \mathfrak{A}$. Now it follows from (3.4) that $w(r+s) \geqslant w(r) + w(s)$. Thus if $w(r) + w(s) \neq w(r+s)$, we have $\Phi^{(r)}\Phi^{(s)} \in \pi^{w(r+s)-w(r)-w(s)}\mathfrak{A} \subseteq \pi\mathfrak{A}$.

It remains to consider the case that $r \preceq p^n - 1 - s$ and $w(r) + w(s) = w(r+s)$, so that $\Phi = \Phi^{(r)}\Phi^{(s)}$. Since the $\Phi^{(u)}$ form an $\mathfrak{O}_K$-basis for the order $\mathfrak{A}$, we have

$$\Phi^{(r)}\Phi^{(s)} = \sum_{u \in \mathbb{S}_{p^n}} c_u \Phi^{(u)} \tag{3.11}$$

for some $c_u \in \mathfrak{O}_K$. We apply Proposition 3.8 on the one hand to $\Psi = \Psi^{(r)}\Psi^{(s)}$, and on the other hand to each $\Psi^{(u)}$. This gives the following congruences mod $\pi\mathfrak{P}_L^h$:

$$\Phi^{(r)}\Phi^{(s)} \cdot \lambda_t \equiv \begin{cases} y_t \lambda_{H(r+s,t)} & \text{if } r+s \preceq \mathfrak{a}(t) \text{ and } \epsilon(r+s,t) = 0, \\ 0 & \text{otherwise,} \end{cases} \tag{3.12}$$

$$\Phi^{(u)} \cdot \lambda_t \equiv \begin{cases} z_{u,t} \lambda_{H(u,t)} & \text{if } u \preceq \mathfrak{a}(t) \text{ and } \epsilon(u,t) = 0, \\ 0 & \text{otherwise,} \end{cases} \tag{3.13}$$

with y_t, $z_{u,t} \in \mathfrak{O}_K^\times$. In view of (3.11), if we multiply (3.13) by c_u and sum over u, we must obtain the same congruence as (3.12) for each t. Thus $c_u\Phi^{(u)} \cdot \lambda_t \in \pi\mathfrak{P}_L^h$ unless $u = r + s \preceq \mathfrak{a}(t)$ and $\epsilon(r+s,t) = 0$, in which case we have $c_{r+s}z_{r+s,t} \equiv y_t \pmod{\pi\mathfrak{O}_K}$. Let $c = c_{r+s}$. Since c is independent of t, it follows that

$$(\Phi^{(r)}\Phi^{(s)} - c\Phi^{(r+s)}) \cdot \lambda_t \in \pi\mathfrak{P}_L^h$$

for all $t \in \mathbb{S}_{p^n}(h)$. Hence $\Phi^{(r)}\Phi^{(s)} - c\Phi^{(r+s)} \in \pi\mathfrak{A}$ as required. □

Proof of Theorem 3.6. — Let $\mathfrak{M}$ be the $\mathfrak{O}_K$-submodule of $\mathfrak{A}$ spanned by $\pi = \pi\Phi^{(0)}$ and the $\Phi^{(s)}$ for $s \in \mathbb{S}_{p^n}\backslash\{0\}$. It is immediate from Proposition 3.9 that $\mathfrak{M}$ is an ideal in $\mathfrak{A}$. Clearly $\mathfrak{A}/\mathfrak{M} \cong \mathfrak{O}_K/\mathfrak{P}_K = \kappa$, so $\mathfrak{M}$ is a maximal ideal and has residue field κ. We claim that $\mathfrak{M}^{n(p-1)+1} \subseteq \pi\mathfrak{A}$, so that $\mathfrak{M}$ is topologically nilpotent. This will show that every maximal ideal is contained in $\mathfrak{M}$, so that $\mathfrak{M}$ is in fact the unique maximal ideal and $\mathfrak{A}$ is a local ring.

To prove the claim, it will suffice to show that if $\Phi^{(s_1)} \dots \Phi^{(s_m)} \notin \pi\mathfrak{A}$ with $s_1, \dots, s_m \in \mathbb{S}_{p^n}\backslash\{0\}$, then $m \leqslant n(p-1)$. For $s = \sum_{i=1}^n s_{(n-i)}p^{n-i} \in \mathbb{S}_{p^n}$, define $|s| = \sum_{i=1}^n s_{(n-i)}$. Thus if $s \in \mathbb{S}_{p^n}\backslash\{0\}$ then $1 \leqslant |s| \leqslant n(p-1)$.

By Proposition 3.9, when $\Phi^{(s_1)}\Phi^{(s_2)} \notin \pi\mathfrak{A}$, we have $\Phi^{(s_1)}\Phi^{(s_2)} \equiv c\Phi^{(s_1+s_2)} \pmod{\pi\mathfrak{A}}$ for some $c \in \mathfrak{O}_K^\times$, and $s_1 \preceq p^n - 1 - s_2$. Since s_1, $s_2 \neq 0$, the latter condition implies that $s_1 + s_2 \in \mathbb{S}_{p^n}$ and $0 \prec s_1 \prec s_1 + s_2$, using Lemma 2.1. Inductively, if $\Phi^{(s_1)} \dots \Phi^{(s_m)} \notin \pi\mathfrak{A}$ then

$$0 \prec s_1 \prec s_1 + s_2 \prec \cdots \prec s_1 + \cdots + s_m\,,$$

so that $0 < |s_1| < |s_1 + s_2| < \cdots < |s_1 + \cdots + s_m|$, which is only possible if $0 < m \leqslant n(p-1)$. This completes the proof that $\mathfrak{A}$ is a local ring.

Consider now the minimal number of generators of $\mathfrak{P}_L^h$ over $\mathfrak{A}$. By Nakayama's Lemma, a subset of $\mathfrak{P}_L^h$ is a generating set if and only if it generates $\mathfrak{P}_L^h/(\mathfrak{M} \cdot \mathfrak{P}_L^h)$ over $\mathfrak{A}/\mathfrak{M} = \kappa$. By Proposition 3.8, $\mathfrak{M} \cdot \mathfrak{P}_L^h$ is spanned over $\mathfrak{O}$ by $\pi\mathfrak{P}_L^h$ and the elements $\Phi^{(s)} \cdot \lambda_t$ where $0 \neq s \preceq \mathfrak{a}(t)$ and $\epsilon(s,t) = 0$. Let u correspond to t as in Lemma 3.7. Then $\Phi^{(s)} \cdot \lambda_t \equiv y\lambda_{H(u,b)} \pmod{\pi\mathfrak{P}_L^h}$ with $y \in \mathfrak{O}_K^\times$, and the condition $\epsilon(s,t) = 0$ is equivalent to $D(s,t) = w(s)$, and hence to $d(u) - d(u-s) = w(s)$. Thus $\mathfrak{M} \cdot \mathfrak{P}_L^h$ is spanned by $\pi\mathfrak{P}_L^h$ and the $\lambda_{H(u,b)}$ for those $u \in \mathbb{S}_{p^n}$ such that $d(u) = d(u-s) + w(s)$ for some s with $0 \neq s \preceq u$. It follows that a κ-basis of $\mathfrak{P}_L^h/(\mathfrak{M} \cdot \mathfrak{P}_L^h)$ is given by the images of the $\lambda_{H(u,b)}$ for $u \in \mathcal{D}$, and the minimal number of generators of $\mathfrak{P}_L^h$ over $\mathfrak{A}$ is $|\mathcal{D}|$.

Finally, consider the embedding dimension $\dim_\kappa(\mathfrak{M}/\mathfrak{M}^2)$. Write A^+ for the augmentation ideal $\{a \in A : a \cdot 1 = 0\}$ of A. This is spanned over K by the $\Phi^{(s)}$ for $s \in \mathbb{S}_{p^n} \backslash \{0\}$. Then $\pi\mathfrak{A} \cap A^+ = \pi\mathfrak{M} \cap A^+$, since both are spanned over $\mathfrak{O}_K$ by the $\pi\Phi^{(u)}$ for $u \in \mathbb{S}_{p^n} \backslash \{0\}$. Now $\mathfrak{M}^2$ is spanned over $\mathfrak{O}_K$ by $\pi\mathfrak{M}$ and the products $\Phi^{(r)}\Phi^{(s)}$ for r, $s \in \mathbb{S}_{p^n} \backslash \{0\}$. By Proposition 3.9 we have $\Phi^{(r)}\Phi^{(s)} \in \pi\mathfrak{A} \cap A^+ \subset \pi\mathfrak{M}$ unless $s \preceq p^n - 1 - r$ and $w(r) + w(s) = w(r+s)$. Conversely, when $s \preceq p^n - 1 - r$ and $w(r) + w(s) = w(r+s)$, we have $\Phi^{(r)}\Phi^{(s)} \equiv c\Phi^{(r+s)} \pmod{\pi\mathfrak{M}}$ for some $c \in \mathfrak{O}_K^\times$. Now we may write $u \in \mathbb{S}_{p^n}$ as $u = r + s$, where r, $s \in \mathbb{S}_{p^n} \backslash \{0\}$ with $s \preceq p^n - 1 - r$ and $w(r) + w(s) = w(r+s)$, precisely when $u \notin \mathcal{E}$. Thus the images in $\mathfrak{M}/\mathfrak{M}^2$ of π and the $\Phi^{(u)}$ with $u \in \mathcal{E} \backslash \{0\}$ form a κ-basis of $\mathfrak{M}/\mathfrak{M}^2$. Since $0 \in \mathcal{E}$, we have $\dim_\kappa(\mathfrak{M}/\mathfrak{M}^2) = |\mathcal{E}|$. □

4. Applications to Galois Extensions

In this section, we give some explicit applications of Theorems 3.1 and 3.6, and relate our approach to various results already in the literature. Except where otherwise stated, we consider only the classical setting, where L/K is a Galois extension and A is the group algebra $K[G]$ for $G = \mathrm{Gal}(L/K)$, with its usual action on L. The scaffolds will then be Galois scaffolds in the sense of Definition 2.6. In particular the residue field κ of K will be assumed to be perfect of characteristic p, and the shift parameters will be the (lower) ramification breaks. Also, the units $u_{i,t}$ in Definition 2.3 (2) will always be 1.

Our basic examples are the near one-dimensional extensions constructed in [19]. These are certain elementary abelian extensions in characteristic p. In the terminology of this paper, the main result of [19] is that any near one-dimensional extension admits a Galois scaffold of precision ∞. A necessary and sufficient condition for the valuation ring $\mathfrak{O}_L$ of a near one-dimensional extension to be free over $\mathfrak{A}_{L/K}$ is given in [14, Thm. 1.1] (see §4.3 below). Theorem 3.1 of this paper, applied to near one-dimensional extensions, improves on this result by giving an analogous result for any fractional ideal of the valuation ring.

The near one-dimensional extensions include all totally ramified biquadratic extensions in characteristic 2, and all totally and weakly ramified extensions in characteristic p. In the next two subsections, we study these two cases in detail. In a separate paper [15], we construct a family of elementary abelian extensions in characteristic 0 which possess Galois scaffolds and are the analog of the near one-dimensional extensions. These include all biquadratic extensions and weakly ramified p-extensions satisfying some mild additional hypotheses. The results of the next two subsections hold also in characteristic 0 under these hypotheses.

4.1. Biquadratic extensions

Let L/K be a totally ramified biquadratic extension of local fields of residue characteristic 2. When K has characteristic 0, the structure of $\mathfrak{O}_L$ over its associated order in $K[G]$ was studied by Martel [32]. When K has characteristic 2 and has perfect residue field, $\mathfrak{O}_L$ is always free over its associated order [14, Cor. 1.4]. These results trivially extend to fractional ideals $\mathfrak{P}_L^h$ when $h \equiv 0 \pmod 4$, but we are not aware of any results for $h \not\equiv 0 \pmod 4$. In this subsection, we give analogous results for arbitrary h. We also provide supplementary information about the number of generators for the ideals which are not free and the embedding dimensions of the associated orders.

Theorem 4.1. — *Let K be a local field of characteristic $p = 2$ with perfect residue field. Let L be a totally ramified biquadratic extension of K with lower ramification breaks b_1, b_2, let $h \in \mathbb{Z}$, and let $\mathfrak{A}$ be the associated*

Table 4.1. The biquadratic case: $d(s)$, $w(s)$, $\mathcal{D}$ and $\mathcal{E}$.

		$d(s)$				$w(s)$					
		$s=$				$s=$					
b	h	0	1	2	3	0	1	2	3	$\mathcal{D}$	$\mathcal{E}$
1	1	0	0	0	0	0	0	0	0	$\{0\}$	$\{0,1,2\}$
1	0	0	0	0	1	0	0	0	1	$\{0\}$	$\{0,1,2,3\}$
1	-1	0	0	1	1	0	0	1	1	$\{0\}$	$\{0,1,2\}$
1	-2	0	1	1	1	0	0	0	1	$\{0,1,2\}$	$\{0,1,2,3\}$
3	3	0	0	1	2	0	0	1	2	$\{0\}$	$\{0,1,2,3\}$
3	2	0	1	1	2	0	1	1	2	$\{0\}$	$\{0,1,2\}$
3	1	0	1	2	2	0	0	1	2	$\{0,1,2\}$	$\{0,1,2,3\}$
3	0	0	1	2	3	0	1	2	3	$\{0\}$	$\{0,1,2\}$

order of $\mathfrak{P}_L^h$. Then $\mathfrak{P}_L^h$ is free over $\mathfrak{A}$ if and only if $b_1 \equiv 1 \pmod 4$, $h \not\equiv 2 \pmod 4$ *or* $b_1 \equiv 3 \pmod 4$, $h \not\equiv 1 \pmod 4$. *In the cases where $\mathfrak{P}_L^h$ is not free, it requires 3 generators over $\mathfrak{A}$. The embedding dimension of $\mathfrak{A}$ is 3 if* $b_1 \equiv 1 \pmod 4$, $h \equiv 1 \pmod 2$ *or* $b_1 \equiv 3 \pmod 4$, $h \equiv 0 \pmod 2$, *and is 4 otherwise.*

Proof. — By [19, Lem. 5.1], L/K has a Galois scaffold of precision ∞, so we may apply Theorems 3.1 and 3.6. Recall that b in Theorem 3.1 satisfies $b \equiv b_2 \pmod 4$ and $0 \leqslant b - h < 4$. As the ramification breaks b_1 and $\frac{1}{2}(b_1 + b_2)$ of the quadratic subextensions F/K of L/K must be odd, we have $b_1 \equiv b_2 \equiv 1$ or $3 \pmod 4$. Since the condition $w(s) = d(s)$, together with the sets $\mathcal{D}$ and $\mathcal{E}$, only depends on the residue classes of h, b_1 and b_2 mod 4, there is no loss of generality in assuming that $b_1 = b_2 = b = 1$ or 3 and $b - 3 \leqslant h \leqslant b$. Then $\mathfrak{b}(s) = bs$ and the values of $d(s)$ and $w(s)$ are as shown in Table 4.1, which also shows the sets $\mathcal{D}$ and $\mathcal{E}$ occurring in Theorem 3.6. To obtain the $w(s)$, note that $w(0) = d(0) = 0$, $w(1) = \min(d(1) - d(0), d(3) - d(2))$, $w(2) = \min(d(2) - d(0), d(3) - d(1))$, $w(3) = d(3) - d(0)$.

From Table 4.1, we have $w(s) = d(s)$ for all s except in the cases $b = 1$, $h = -2$ and $b = 3$, $h = 1$. The criterion for $\mathfrak{P}_2^h$ to be free then follows from Theorem 3.1. In the cases where $\mathfrak{P}_2^h$ is not free, $|\mathcal{D}| = 3$, so that $\mathfrak{P}_2^h$ requires 3 generators over $\mathfrak{A}$ by Theorem 3.6. The cardinalities of the sets $\mathcal{E}$ in Table 4.1 show that the embedding dimension is as stated. $\square$

4.2. Weakly ramified p-extensions

A Galois extension L/K of local fields with Galois group G is said to be weakly ramified if its second ramification group G_2 is trivial. Then $\mathfrak{P}_L$ is free over the group ring $\mathfrak{O}_K[G]$, and $\mathfrak{O}_L$ is free over the order $\mathfrak{O}_K[G][\pi^{-1}\sum_{g\in G_0} g]$, where π is a uniformizing parameter of K and G_0 is the inertia subgroup of G (see for instance [26]). Moreover, a fractional ideal $\mathfrak{P}_L^h$ is free over $\mathfrak{O}_K[G]$ if and only if $h \equiv 1 \pmod{|G_1|}$ [29, Thm. 1.1]. Thus if L/K is totally and weakly ramified of degree p^n then the ideals $\mathfrak{P}_L^h$ are free over their associated orders when $h \equiv 0$ or $1 \pmod{p^n}$. For other values of h, nothing seems to be known when $n > 1$ beyond the fact that $\mathfrak{P}_L^h$ cannot be free over $\mathfrak{O}_K[G]$. The case $n = 1$ is covered by Ferton's result [21] mentioned in Remark 3.3.

In this subsection, we will give detailed information on $\mathfrak{P}_L^h$ for all h (and arbitrary n), assuming that K has characteristic p and has perfect residue field. We will determine precisely when $\mathfrak{P}_L^h$ is free over its associated order $\mathfrak{A}$, and will obtain supplementary information about the minimal number of generators of $\mathfrak{P}_L^h$ over $\mathfrak{A}$ and the embedding dimension of $\mathfrak{A}$. Our results will be expressed in terms of combinatorial properties of the base-p digits of numbers closely related to h.

Let K be as just described, and let L/K be a totally and weakly ramified extension of degree p^n. Thus L/K has ramification breaks $b_1 = \cdots = b_n = 1$, and its Galois group must be elementary abelian. Moreover, L/K admits a Galois scaffold of precision ∞. For $n = 1$, we have already seen this in Example 2.8, and for $n \geqslant 2$ it follows from [19, Lem. 5.3]. We can therefore apply Theorems 3.1 and 3.6.

We first define some notation. For $s = \sum_{i=1}^{n} s_{(n-i)}p^{n-i} = \sum_{j=0}^{n-1} s_{(j)}p^j \in \mathbb{S}_{p^n}$, set

$$\alpha(s) = |\{j : 1 \leqslant j \leqslant n-1, j > v_p(s), s_{(j)} \neq p-1\}|,$$
$$\beta(s) = \max\{c : 0 \leqslant c < n - v_p(s),\ s_{(n-1)} = \cdots = s_{(n-c)} = \tfrac{1}{2}(p-1)\},$$

where the maximum is to be interpreted as 0 if no such c exists, and

$$\gamma(s) = \begin{cases} 1 & \text{if } p = 2 \text{ and } s = 2^{n-1}, \\ 0 & \text{otherwise.} \end{cases}$$

Thus $\alpha(s)$ is the number of base-p digits of s which are not equal to $p-1$, including any leading 0's $s_{(n-1)} = \cdots = s_{(m)} = 0$, but excluding the last nonzero digit $s_{(v)} \neq 0$ for $v = v_p(s)$ and any trailing 0's $s_{(v-1)} = \cdots = s_{(0)} = 0$. Also, $\beta(s)$ is the number of leading base-p digits (including leading

0's but excluding the last nonzero digit) which are equal to $\frac{1}{2}(p-1)$. In particular, $\beta(s)=0$ if $s<\frac{1}{2}p^{n-1}(p-1)$ or if $p=2$.

For $0\leqslant j\leqslant n-1$, we define

$$\lfloor s\rfloor_j = p^j\left\lfloor\frac{s}{p^j}\right\rfloor = \sum_{i=j}^{n-1} s_{(i)}p^i,$$

and

$$\lceil s\rceil_j = p^j\left\lceil\frac{s}{p^j}\right\rceil = \begin{cases}\lfloor s\rfloor_j = s & \text{if } s\equiv 0 \pmod{p^j}\\ \lfloor s\rfloor_j + p^j & \text{otherwise.}\end{cases}$$

Theorem 4.2. — *Let L/K be a totally and weakly ramified extension of degree p^n in characteristic p. Let $h\in\mathbb{Z}$.*

(1) *If $h\equiv 1 \pmod{p^n}$ then $\mathfrak{P}_L^h$ is free over its associated order, and this order has embedding dimension $n+1$.*

(2) *If $h\not\equiv 1 \pmod{p^n}$, let $h'\equiv h \pmod{p^n}$ with $2\leqslant h'\leqslant p^n$, and write $m=h'-1$ and $k=\max(m,p^n-m)$. Then*

  (a) *$\mathfrak{P}_L^h$ is free over its associated order $\mathfrak{A}$ if and only if $h'\geqslant 1+\frac{1}{2}p^n$;*

  (b) *if $\mathfrak{P}_L^n$ is not free, the minimal number of generators of $\mathfrak{P}_L^h$ as a module over $\mathfrak{A}$ is $2+\alpha(m)-\beta(m)$;*

  (c) *the embedding dimension of $\mathfrak{A}$ is $n+2+\alpha(k)-\gamma(k)$.*

(Note that when $h=0$ we have $h'=p^n$ so that, in particular, $\mathfrak{O}_L$ is free over its associated order; cf. Remark 4.4 below.)

Proof. — As $b_i=1$ for each i, we have $\mathfrak{b}(s)=s$. Without loss of generality, we suppose that $2\leqslant h\leqslant p^n+1$. Thus $b=p^n+1$, and $h'=h$ in (2). We then have

$$d(s)=\left\lfloor\frac{1+p^n+s-h}{p^n}\right\rfloor = \begin{cases}1 & \text{if } s\geqslant m;\\ 0 & \text{if } s<m.\end{cases} \tag{4.1}$$

(1). — If $h=p^n+1$ we have $d(s)=0$ for all s, and hence $w(s)=0$ for all s as well. Thus $\mathfrak{P}_L^h$ is free over its associated order $\mathfrak{A}$ by Theorem 3.1. In Theorem 3.6, we have $\mathcal{D}=\{0\}$, $\mathcal{E}=\{0,1,p,\dots,p^{n-1}\}$, so that $\mathfrak{A}$ has embedding dimension $n+1$.

(2). — Now let $2\leqslant h\leqslant p^n$. We first determine the $w(s)$; for any $s\in\mathbb{S}_{p^n}$ we have

$$\begin{aligned} w(s)=1 &\Leftrightarrow d(u)=1 \text{ and } d(u-s)=0 \text{ for all } u\succeq s\\ &\Leftrightarrow u\geqslant m \text{ and } u-s<m \text{ for all } u\succeq s\\ &\Leftrightarrow s\geqslant m \text{ and } (p^n-1)-s<m\\ &\Leftrightarrow s\geqslant \max(m,p^n-m),\end{aligned}$$

so that

$$w(s) = \begin{cases} 1 & \text{if } s \geqslant k; \\ 0 & \text{if } s < k. \end{cases} \tag{4.2}$$

Note that $\frac{1}{2}p^n \leqslant k \leqslant p^n - 1$.

(2a). — From (4.1) and (4.2) we have

$$d(s) = w(s) \text{ for all } s \in \mathbb{S}_{p^n} \Leftrightarrow k = m \Leftrightarrow h \geqslant 1 + \tfrac{1}{2}p^n.$$

(2b). — Let $2 \leqslant h < 1+\frac{1}{2}p^n$. Then $0 < m < k$. It is immediate from (4.1) and (4.2) that $\mathcal{D}$ contains 0 and m. Moreover, if $0 < u < m$ or $u \geqslant k$ then $u \notin \mathcal{D}$ since $d(u) = d(0) + w(u)$.

We need to show that there are $\alpha(m) - \beta(m)$ elements $u \in \mathcal{D}$ with $m < u < k$. Let $j = v_p(u)$. Then $0 \leqslant j \leqslant n-1$ and $u_{(j)} \neq 0$. If $u - p^j \geqslant m$ then, taking $s = p^j$, we have $d(u-s) = 1$ and $0 \prec s \preceq u$, so that $u \notin \mathcal{D}$. Conversely, if $u \notin \mathcal{D}$, then there is some s with $d(u-s) = 1$ and $0 \prec s \preceq u$. Since $v_p(u) = j$, we must have $s \geqslant p^j$ and hence $m \leqslant u - s \leqslant u - p^j$. It follows that $u \in \mathcal{D}$ if and only if $u - p^j < m$. But as $j = v_p(u)$, we have $u - p^j < m < u$ if and only if $u = \lceil m \rceil_j$ and $v_p(m) < j$. We conclude that, for each $j > v_p(m)$, there is at most one $u \in \mathcal{D}$ with $v_p(u) = j$ and $u > m$, namely $u = \lceil m \rceil_j$; such a u exists if and only if $\lceil m \rceil_j < k$ and $v_p(\lceil m \rceil_j) = j$. Since $j > v_p(m)$, the latter condition is equivalent to $m_{(j)} \neq p-1$, and the number of j for which this occurs is $\alpha(m)$. We claim that, amongst these, there are $\beta(m)$ values of j for which $\lceil m \rceil_j \geqslant k$.

We count the $j \leqslant n-1$ such that

$$m_{(j)} \neq p-1 \text{ and } \lceil m \rceil_j \geqslant k. \tag{4.3}$$

Any such j automatically satisfies $j > v_p(m)$ since if $j \leqslant v_p(m)$ then $\lceil m \rceil_j = m < k$. We distinguish two cases. Firstly, we consider the special case where the base-p digits of m are all $\frac{1}{2}(p-1)$, possibly followed by a block of 0's. Thus $m = \frac{1}{2}(p-1)(p^{n-1} + \cdots + p^v)$ where $v = v_p(m) \geqslant 0$. In this case, $\beta(m) = n - v - 1$ and $k = m + p^v$. If $j \geqslant n - \beta(m) = v+1$ then $\lceil m \rceil_j = \lceil k \rceil_j > k$, and of course $m_{(j)} = \frac{1}{2}(p-1) \neq p-1$, while if $j \leqslant v$ then $\lceil m \rceil_j = m < k$. Thus there are $\beta(m)$ values of j satisfying (4.3) in this case. Secondly, suppose we are not in this special case, and let $c = \beta(m)$. Then $0 \leqslant c \leqslant n-1$ and $v_p(m) < n-c$. Moreover, since $m < \frac{1}{2}p^n$ (because $m < k$) and we are not in the first case, we have $m_{(n-c-1)} < \frac{1}{2}(p-1)$. If $p \neq 2$ then $m_{(n-c-1)} \leqslant \frac{1}{2}(p-3)$ and we may write $m = \frac{1}{2}(p-1)(p^{n-1} + \cdots + p^{n-c}) + r$ with $0 < r < \frac{1}{2}(p-3)p^{n-c-1} + p^{n-c-1} = \frac{1}{2}(p-1)p^{n-c-1}$. Then $\lceil m \rceil_j = \lceil k \rceil_j > k$ if $j \geqslant n-c$, and $\lceil m \rceil_j \leqslant \lfloor k \rfloor_j \leqslant k$ if $j < n-c$. Thus there are again $\beta(m)$ values of j satisfying (4.3). Finally, if $p = 2$ then $\beta(m) = 0$

and, since $m < 2^{n-1} < k$, we have $\lceil m \rceil_j < k$ for all $j < n$, yet again giving the required conclusion.

(2c). — By Theorem 3.6, the embedding dimension of $\mathfrak{A}$ is $|\mathcal{E}|$ where

$$\mathcal{E} = \{u \in \mathbb{S}_{p^n} \,:\, w(u) > w(u-s) + w(s) \text{ for all } s \in \mathbb{S}_{p^n} \text{ with } 0 \prec s \prec u\}.$$

This set will be unchanged on replacing h by p^n+2-h, since both give the same value for k and hence the same sequence $w(s)$. Certainly $\mathcal{E}$ contains the $n+1$ elements $0, 1, p, \ldots, p^{n-1}$, and no other elements $u < k$. It also contains k since $w(k) = 1$ and $w(s) = 0$ for $s < k$. Note that $k > p^{n-1}$ except in the case $p = 2$, $k = 2^{n-1}$ (corresponding to $h = 2^{n-1}+1$). Thus the number of elements $u \in \mathcal{E}$ with $u \leqslant k$ is $n + 2 - \gamma(k)$. The proof will be complete if we show that there are precisely $\alpha(k)$ elements $u \in \mathcal{E}$ with $u > k$. But if $u > k$ and $v_p(u) = j$ then, arguing as in (2b) above, $u \in \mathcal{E}$ if and only if $u - p^j < k$, and the number u satisfying this condition is $\alpha(k)$. □

Remark 4.3. — When $h \equiv 1 \pmod{p^n}$, the associated order $\mathfrak{A}$ is just the group ring $\mathfrak{O}_K[G]$, and its maximal ideal is $\mathfrak{M} = \mathfrak{P}_K + I$ where I is the augmentation ideal of $\mathfrak{O}_K[G]$. Thus $\mathfrak{M}/\mathfrak{M}^2$ is generated as a κ-vector space by the $n+1$ elements π, $\sigma_1 - 1, \ldots, \sigma_n - 1$, where $\pi \in K$ with $v_K(\pi) = 1$ and $\sigma_1, \ldots, \sigma_n$ is any set of generators of G.

Remark 4.4. — In the case $h = 0$, we have $h' = p^n$, so that $k = m = p^n - 1$ and $\alpha(k) = \gamma(k) = 0$ (unless $p^n = 2$, when $\gamma(k) = 1$). Hence $\mathfrak{O}_L$ is free over its associated order $\mathfrak{A}_{L/K}$, as we already know from [19, Lem. 5.3] and [14, Thm. 1.1]. Moreover, $\mathfrak{A}_{L/K}$ has embedding dimension $n+2$ (or $n+1$ when $p^n = 2$). One can check directly that

$$d(s) = w(s) = \begin{cases} 1 & \text{if } s = p^n - 1; \\ 0 & \text{if } 0 \leqslant s < p^n - 1, \end{cases}$$

so that $\mathcal{E} = \{0, 1, p, p^2, \ldots, p^{n-1}, p^n - 1\}$. In fact,

$$\mathfrak{A} = \mathfrak{O}_K[G][\pi^{-1}\Sigma],$$

where $v_K(\pi) = 1$ and $\Sigma = \sum_{\sigma \in G} \sigma$ is the trace element of $K[G]$. Thus, with the notation of Remark 4.3, $\mathfrak{M}/\mathfrak{M}^2$ is generated by π, $\sigma_1 - 1, \ldots, \sigma_n - 1, \pi^{-1}\Sigma$.

To give some idea of the range of complexity occurring in the Galois module structure of ideals for wildly ramified extensions, we record the maxima and minima of the number of generators and the embedding dimension. We are not aware of any similar results in the Galois module literature beyond the discussion of the degree p case in [39].

Corollary 4.5. — *Let L/K be as in Theorem 4.2, and let $\mathfrak{A}$ be the associated order of $\mathfrak{P}_L^h$.*

(1) (a) *When $p > 2$, the maximal number of generators required for $\mathfrak{P}_L^h$ over $\mathfrak{A}$ is $n+1$. The minimal number of generators in cases where $\mathfrak{P}_L^h$ is not free is 2. This occurs, for example, when $h = \frac{1}{2}(p^n+1)$.*

(b) *When $p = 2$ and $n > 1$, the maximal number of generators for $\mathfrak{P}_L^h$ over $\mathfrak{A}$ is again $n+1$. There are no $\mathfrak{P}_L^h$ requiring precisely 2 generators. Precisely 3 generators are required, for example, if $h = 2^{n-1}$.*

(2) (a) *When $p > 2$, the embedding dimension of $\mathfrak{A}$ can take any value between $n+1$ and $2n+1$. The minimum $n+1$ occurs only for $h \equiv 1 \pmod{p^n}$. The value $n+2$ occurs, for example, if $h = 2$ or $h = p^n$. The maximal value $2n+1$ occurs, for example, if $h = \frac{1}{2}(p^n+1)$.*

(b) *When $p = 2$, the minimum embedding dimension $n+1$ is attained only for $h \equiv 1$ and $2^{n-1}+1 \pmod{2^n}$. The maximum is $2n$, attained only for $h \equiv 2^{n-1}$ and $2^{n-1}+2 \pmod{2^n}$.*

Remark 4.6. — If L/K is any extension of local fields (not necessarily Galois) with an action of an algebra A admitting a scaffold of $\mathfrak{c} \geqslant 2p^n - 1$ whose shift parameters satisfy $b_i \equiv 1 \pmod{p^i}$, then we can reduce to the case $b_i = 1$ for all i by Remark 2.9. We will then obtain the same sequences $d(s)$ and $w(s)$ as in the proof of Theorem 4.2, so the conclusions of Theorem 4.2 will still hold. In particular, this gives an alternative approach to Theorem 4.1 in the case that $b_1 \equiv 1 \pmod 4$.

Remark 4.7. — There is an arithmetic interpretation of the fact that the sequence $w(s)$ is unchanged on replacing h by $p^n + 2 - h$. Let L/K be a totally and weakly ramified extension of degree p^n. Then its inverse different is $\mathfrak{P}_L^{2(1-p^n)}$. For any $m \in \mathbb{Z}$, the ideals $\mathfrak{P}_L^{1-p^n+m}$ and $\mathfrak{P}_L^{1-p^n-m}$ are therefore mutually dual under the trace pairing. Thus, for any $h \in \mathbb{Z}$, the ideals $\mathfrak{P}_L^h$ and $\mathfrak{P}_L^{2-2p^n-h} \cong \mathfrak{P}_L^{p^n+2-h}$ are mutually dual. When $h \equiv 1 \pmod p$, the ideal $\mathfrak{P}_L^h$ is isomorphic to its dual, and is free over the group ring $\mathfrak{O}_K[G]$. If $p = 2$ and $h \equiv 1 + 2^{n-1} \bmod 2^n$, the ideal $\mathfrak{P}_L^h$ is again isomorphic to its dual, and is free over its associated order $\mathfrak{A}$; in this case $\mathfrak{A} \neq \mathfrak{O}_K[G]$, although $\mathfrak{A}$ attains the minimal embedding dimension $n+1$. In the remaining case $2h \not\equiv 2 \bmod p^n$, the mutually dual ideals $\mathfrak{P}_L^h$ and $\mathfrak{P}_L^{2-2p^n-h}$ are not isomorphic; they have the same associated order, since both give rise to the same sequence $w(s)$, but one ideal is free over this order while the other is not.

4.3. More on the valuation ring

In this subsection, we discuss how Theorem 3.1 is related to a result of Miyata [33] and to our previous work in [10] and [14]. This will lead to a strengthening of [14, Cor. 1.2].

We first recall Miyata's result. Let K be a finite extension of $\mathbb{Q}_p$ containing a primitive p^nth root of unity, and let $L = K(\sqrt[p^n]{a})$ be an extension of degree p^n, where $a \in K$ and $p \nmid v_K(a-1)$. Recall that $r(x)$ denotes the least non-negative residue mod p^n of an integer x. We set $t_0 = r(v_K(a-1))$. Miyata [33, Thm. 5] shows that $\mathfrak{O}_L$ is free over its associated order $\mathfrak{A}_{L/K}$ if and only if the following condition holds: $t_0 + r(it_0) - r(ht_0) > 0$ for all integers h, i, j such that $0 \leqslant h \leqslant i \leqslant j < p^n$, $i + j = p^n - 1 + h$ and $p \nmid \binom{i}{h}$. This can be interpreted as a condition on the ramification breaks $b_1, \ldots, b_n$ of L/K, since, writing $b = r(-v_K(a-1)) = p^n - t_0$, we have $b_i \equiv b \pmod{p^i}$ for $1 \leqslant i \leqslant n$.

Miyata's condition was reformulated in [10], where it was used to deduce a more transparent (but less complete) criterion: $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$ if b divides $p^m - 1$ for some $m \in \{1, \ldots, n\}$. The converse is not always true when $n \geqslant 3$, but for $n = 2$ the converse does hold. Thus, for $n = 2$, we have that $\mathfrak{O}_L$ is free if and only if b divides $p^2 - 1$. This is closely analogous to the result [5] for $n = 1$ (cf. Example 3.3): $\mathfrak{O}_L$ is free if and only if $b \mid (p-1)$.

In [14], we considered near one-dimensional extensions E/F, and gave a criterion [14, Thm. 2.3] for $\mathfrak{O}_E$ to be free over its associated order. In the notation of the present paper, this criterion is just the condition that $w(s) = d(s)$ for all s, and the result is a special case of Theorem 3.1 (with $h = 0$). We also showed [14, Lem. 2.4] that this criterion was equivalent to Miyata's, as reformulated in [10]. (This is despite the fact that Miyata's extensions are cyclic in characteristic 0 and the near one-dimensional extensions are elementary abelian in characteristic p).

Now, given that $b_i \equiv b \pmod{p^i}$ for $1 \leqslant i \leqslant n$, the equivalence of Miyata's condition and our condition $w(s) = d(s)$ is a purely numerical statement, depending only on the parameter b. We may therefore combine it with Theorem 3.1 (in the case $h = 0$) whenever we have an extension L/K admitting a scaffold with high enough precision and suitable shift parameters. We therefore obtain the following result:

Theorem 4.8. — *Let L/K be a totally ramified extension of local fields of degree p^n. Let there be an A-scaffold on L with shift parameters $b_1, \ldots, b_n$ that satisfy $b_i \equiv b_n \pmod{p^i}$ for all i and with precision $\mathfrak{c} \geqslant r(b_n)$. Then $\mathfrak{O}_L$ is free over its associated order in A if $r(b_n) \mid (p^m - 1)$*

for some $m \in \{1, 2, \ldots, n\}$. Conversely, if $n \leqslant 2$ and $\mathfrak{c} \geqslant p^n + r(b_n)$ then $\mathfrak{O}_L$ is free only if $r(b_n) \mid (p^n - 1)$.

Remark 4.9. — We reiterate that, in the case of near one dimensional extensions, Theorem 4.8 is [14, Cor. 1.2]. The new feature here is that the same statement holds for any extension (not necessarily Galois, and not necessarily in characteristic p), provided that it admits a scaffold of high enough precision whose shift parameters satisfy the stated congruences. These congruences automatically hold for Galois scaffolds on abelian extensions, cf. Remark 2.13, but also for the inseparable examples in §5 below, where there is a single shift parameter b.

One question which remains unanswered is whether (or under what conditions) Miyata's cyclic extensions admit a Galois scaffold of sufficiently high precision for Theorem 3.1 (2) to be applicable. If this were the case, then Miyata's result could be viewed as particular instance of ours. We hope to return to this question in future work.

4.4. A result on the inverse different

Let L/K be a totally ramified Galois extension of degree p^n, with abelian Galois group. In [9, Thm. 3.10], it was shown that, under a rather mild technical hypothesis, the inverse different $\mathfrak{D}_{L/K}^{-1}$ of L/K cannot be free over its associated order unless the ramification breaks satisfy the congruence $b_i \equiv -1 \pmod{p^n}$. (Note that the modulus here is p^n, and not p^i.) Only the characteristic 0 case was considered in [9], but the same argument works in characteristic p. We will now show that, if L/K admits a suitable Galois scaffold, this necessary condition for freeness is also sufficient, and we note an interesting consequence for the order $\mathfrak{A}$.

Theorem 4.10. — *Let L/K be an abelian extension of degree p^n which admits a Galois scaffold of precision $\mathfrak{c} \geqslant 2p^n - 1$. Then $\mathfrak{D}_{L/K}^{-1}$ is free over its associated order $\mathfrak{A}$ if and only the ramification breaks satisfy $b_i \equiv -1 \pmod{p^n}$ for $1 \leqslant i \leqslant n$. If this occurs, then $\mathfrak{A}$ is also the associated order of the valuation ring $\mathfrak{O}_L$, and $\mathfrak{A}$ is a Hopf order in the Hopf algebra $K[G]$, where $G = \mathrm{Gal}(L/K)$.*

Proof. — The condition (3.11) in [9, Thm. 3.10] is only required to ensure that $\mathfrak{A}$ is a local ring (or, equivalently, that $\mathfrak{D}_{L/K}^{-1}$ is indecomposable as an $\mathfrak{O}_K[G]$-module). However, this is guaranteed by Theorem 3.6 under our hypothesis on $\mathfrak{c}$. It follows that $\mathfrak{D}_{L/K}^{-1}$ cannot be free over $\mathfrak{A}$ unless $b_i \equiv -1 \pmod{p^n}$ for all i.

Conversely, suppose that $b_i \equiv -1 \pmod{p^n}$ for all i. Then Hilbert's formula for the different [37, IV§2 Prop. 4] gives $\mathfrak{D}_{L/K}^{-1} = \mathfrak{P}_L^{-w}$ with $w \equiv 0 \pmod{p^n}$, so that $\mathfrak{D}_{L/K}^{-1} = \delta\mathfrak{O}_L$ for some $\delta \in K$. It follows that $\mathfrak{D}_{L/K}^{-1}$ is isomorphic to $\mathfrak{O}_L$ as an $\mathfrak{O}_K[G]$-module. Thus both $\mathfrak{O}_L$ and $\mathfrak{D}_{L/K}^{-1}$ have the same associated order $\mathfrak{A}$, and if either of them is free over $\mathfrak{A}$ then so is the other. Now since the assumption on the b_i implies the weaker congruences $b_i \equiv -1 \pmod{p^i}$, it follows from Example 3.4 that $\mathfrak{O}_L$, and hence also $\mathfrak{D}_{L/K}^{-1}$, is indeed free over $\mathfrak{A}$. Finally, as $\mathfrak{D}_{L/K}^{-1} = \delta\mathfrak{O}_L$ with $\delta \in K$, and $\mathfrak{A}$ is a local ring, $\mathfrak{A}$ must be a Hopf order in $K[G]$ by work of Bondarko [6, Thm. A and Prop. 3.4.1]. □

Corollary 4.11. — *Let L/K be an abelian extension of degree p^n which admits a Galois scaffold of precision $\mathfrak{c} \geqslant 2p^n - 1$. If the largest ramification break b_n satisfies the congruence $b_n \equiv -1 \pmod{p^n}$, then we have $b_i \equiv -1 \pmod{p^n}$ for all i.*

Proof. — By the Hasse–Arf Theorem (see Remark 2.13), the hypothesis $b_n \equiv -1 \pmod{p^n}$ ensures that $b_i \equiv -1 \pmod{p^i}$ for all i (which is weaker than the desired conclusion). But then, on the one hand, it follows from Example 3.4 that $\mathfrak{O}_L$ is free over its associated order $\mathfrak{A}$. On the other hand, from Hilbert's formula for the different, we again have $\mathfrak{D}_{L/K}^{-1} = \delta\mathfrak{O}_L$ for some $\delta \in K$. Thus $\mathfrak{D}_{L/K}^{-1}$ also has associated order $\mathfrak{A}$, and is free over $\mathfrak{A}$. Hence, by Theorem 4.10, we have the stronger congruence $b_i \equiv -1 \pmod{p^n}$ for all i. □

One can easily construct elementary abelian extensions whose ramification breaks satisfy $b_i \equiv -1 \pmod{p^i}$ for all i, but do not satisfy $b_i \equiv -1 \pmod{p^n}$ for all i. Corollary 4.11 therefore shows that certain realizable sequences of ramification breaks preclude the existence of a Galois scaffold of high precision.

5. Purely inseparable extensions

The purpose of this section is to provide an example of a particularly natural scaffold (with precision $\mathfrak{c} = \infty$) in the setting of purely inseparable extensions, and since the results of §3 are therefore applicable, submit the topic of generalized Galois module structure in purely inseparable extensions for further study.

The divided power Hopf algebra $\mathcal{A}(n)$ of dimension p^n (see Definition 5.2 below) is a standard example of a Hopf algebra over a field K of characteristic $p > 0$. We will prove the following result:

Theorem 5.1. — *Let K be a local field of characteristic $p > 0$, and let L be any totally ramified and purely inseparable extension of K of degree p^n. Let b satisfy $0 < b < p^n$ and $\gcd(b, p) = 1$. Then there is an action of $\mathcal{A}(n)$ on L which makes L into an $\mathcal{A}(n)$-Hopf Galois extension of K, and which admits an $\mathcal{A}(n)$-scaffold with unique shift parameter b and with precision $\mathfrak{c} = \infty$.*

This means that we can study generalized Galois module structure questions for each of these actions of $\mathcal{A}(n)$: the valuation ring $\mathfrak{O}_L$ of L, or more generally any fractional ideal $\mathfrak{P}_L^h$, is a module over its associated order in $\mathcal{A}(n)$ under each action, and, as before, we can ask if it is free, how many generators are required if it is not, and what the embedding dimension of the associated order is. The answers to these questions are given in terms of b by Theorems 3.1 and 3.6, and so will be identical to those for any Galois extension of degree p^n admitting a Galois scaffold of high enough precision and having lower ramification breaks $b_i \equiv b \pmod{p^i}$ for $1 \leqslant i \leqslant n$. In particular, it follows from Theorem 4.8 that $\mathfrak{O}_L$ will be free over its associated order if b divides $p^m - 1$ for any $m \leqslant n$ (and conversely for $n = 1, 2$).

The material in this section is partly based on discussions with Alan Koch.

5.1. Hopf Galois structures

Let L/K be a finite extension of fields, and let H be a cocommutative K-Hopf algebra with comultiplication $\Delta : H \to H \otimes H$, augmentation (or counit) $\epsilon : H \to K$ and antipode $\sigma : H \to H$. We say that L is an H-module algebra if there is a K-linear action of H on L such that the following hold: for all $h \in H$ and s, $t \in L$,

$$\mu(\Delta(h)(s \otimes t)) = h(st)$$

where μ is the multiplication map $L \otimes L \to L$; and

$$h \cdot 1 = \epsilon(h)1 \text{ for all } h \text{ in } H.$$

Then L/K is an H-Hopf Galois extension if L is an H-module algebra and the map

$$L \otimes_K H \to \mathrm{End}_K(L),$$

given by $(s \otimes h)(t) \mapsto sh(t)$ for $h \in H$ and $s,\, t \in L$, is a bijection.

This notion, defined (in dual form) in [16], extends the classical concept of a finite Galois extension of fields: if L/K is Galois with group G, then the map

$$L \otimes_K K[G] \to \mathrm{End}_K(L)$$

is bijective.

An early example of a class of Hopf Galois extensions was furnished by finite primitive purely inseparable field extensions. Let K be a field of characteristic $p > 0$ and let $L = K(x)$ with $x^{p^n} = a$, where $a \in K$ but $a^{1/p} \notin K$. Note that $x^{p^n} - a$ is irreducible. Then L is called a primitive extension of K of exponent n. Associated with a primitive extension L/K of exponent n are higher derivations, or unital Hasse–Schmidt derivations, of length p^n. A higher derivation on L/K is a sequence

$$\mathcal{D} = (D_0 = 1, D_1, \ldots, D_{p^n-1})$$

of K-homomorphisms from L to L such that for all m and for all a, b in L,

$$D_m(ab) = \sum_{i=0}^{m} D_i(a) D_{m-i}(b)$$

and $D_i(a) = \delta_{i,0} a$ for all $a \in K$. (Unital means $D_0 = 1$: see [23].) In particular, D_1 is a derivation of L. The set of all $a \in L$ so that $D_i(a) = 0$ for all $i > 0$ is the field of constants of $\mathcal{D}$ (which contains K).

The significance of higher derivations in inseparable field theory stems in part from characterizations of finite modular purely inseparable field extensions L/K. A finite purely inseparable field extension L of K is modular if L is isomorphic to a tensor product $K(x_1) \otimes \cdots \otimes K(x_r)$ of primitive extensions. Sweedler [40] characterized a finite modular extension as one for which K is the field of constants of all higher derivations on L/K.

Higher derivations of purely inseparable field extensions can arise from actions of divided power Hopf algebras, defined as follows.

Definition 5.2 ([34, 5.6.8]). — *Let K be a field of characteristic p. The divided power K-Hopf algebra of dimension p^n is the K-vector space $\mathcal{A}(n)$ of dimension p^n with basis $t_0, t_1, \ldots, t_{p^n-1}$. Multiplication is defined by*

$$t_i t_j = \begin{cases} \binom{i+j}{j} t_{i+j} & \text{if } i + j < p^n, \\ 0 & \text{otherwise} \end{cases}$$

and t_0 is the identity. The coalgebra structure is given by

$$\Delta(t_r) = \sum_{j=0}^{r} t_j \otimes t_{r-j} \text{ and } \epsilon(t_r) = \delta_{0,r}\,.$$

The antipode is given by $s(t_r) = (-1)^r t_r$.

Remark 5.3. — As Alan Koch has pointed out to us, the divided power Hopf algebra $\mathcal{A}(n)$ represents the group scheme given by the kernel of the Frobenius homomorphism on the additive group of Witt vectors of length n over K.

Let $L = K(x)$ be a primitive purely inseparable field extension of exponent n. Let $\mathcal{A}(n)$ act on L by

$$t_r(x^s) = \binom{s}{r} x^{s-r} \tag{5.1}$$

(where $\binom{s}{r} = 0$ if $r > s$). Then, as Sweedler observes [41, p. 215], L is an $\mathcal{A}(n)$-module algebra, K is the field of constants

$$L^{\mathcal{A}(n)} = \{y \in L : h(y) = \epsilon(h)y \text{ for all } h \in \mathcal{A}(n)\}$$

and $[\mathcal{A}(n) : K] = [L : K] = p^n$. By a theorem of Sweedler ([41, Thm. 10.1.1]), these conditions imply that the map from $L \otimes_K \mathcal{A}(n)$ to $\mathrm{End}_K(L)$ is bijective, and hence L is an $\mathcal{A}(n)$-Hopf Galois extension of K.

This example also shows up in [2, Lem. 1.2,3] and in dual form (that is, L is an $\mathcal{A}(n)^*$-Galois object) in [16, Ex. 4.11].

Evidently if $\mathcal{A}(n)$ acts on L/K, then the basis $\{t_0, t_1, \ldots, t_{p^n-1}\}$ of $\mathcal{A}(n)$ defines a higher derivation of L/K. So henceforth we denote t_i by D_i. As a K-vector space,

$$\mathcal{A}(n) = K[D_0, D_1, \ldots D_{p^n-1}]\,,$$

and we turn our attention now to the structure of $\mathcal{A}(n)$ as an algebra.

Proposition 5.4. — *As a K-algebra,*

$$\mathcal{A}(n) = K[D_1, D_p, \ldots D_{p^{n-1}}] \cong K[T_0, T_1, \ldots T_{n-1}]/(T_0^p, T_1^p, \ldots, T_{n-1}^p]$$

is an exponent p truncated polynomial algebra over K.

To show this, it is convenient to invoke

Theorem 5.5 (Lucas's Theorem, 1878). — *Let p be prime, and let the integers $a, b \geqslant 0$ be written p-adically:*

$$a = a_0 + a_1 p + \cdots + a_r p^r$$
$$b = b_0 + b_1 p + \cdots + b_r p^r$$

where we may assume $b \leqslant a$ (so that b_r may be 0) and $0 \leqslant a_i, b_i < p$ for all i. Then

$$\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\dots\binom{a_r}{b_r} \pmod{p}.$$

Here $\binom{0}{0} = 1$ and $\binom{a}{b} = 0$ if $a < b$. For a nice proof of Lucas's Theorem using the Binomial Theorem modulo p, see [36].

Proof of Proposition 5.4. — This is a matter of showing by induction (using Lucas's Theorem) that modulo p: first,

$$k!D_{kp^r} = D_{p^r}^k$$

for $1 \leqslant k \leqslant p$, and hence $D_{p^r}^p = 0$ for all r; and second,

$$D_{a_0+a_1p+\dots a_rp^r} = D_{a_0}D_{a_1p}\dots D_{a_rp^r}.$$

Hence

$$D_{a_0+a_1p+\dots a_rp^r} = \frac{D_1^{a_0}}{a_0!}\cdot\frac{D_p^{a_1}}{a_1!}\dots\frac{D_{p^r}^{a_r}}{a_r!}.$$

Since all the factorials are units modulo p, the result follows. □

5.2. $\mathcal{A}(n)$-scaffolds on purely inseparable extensions

Let K be a local field with normalized valuation v_K and uniformizing parameter π. Let L be a purely inseparable field extension of exponent n which is totally ramified. To see that L/K is primitive, let ν be a uniformizing parameter for L. As L/K is purely inseparable, we have $\nu^{p^n} \in K$. As L/K is totally ramified, it follows that $v_K(\nu^{p^n}) = 1$, so that $\nu^{p^{n-1}} \notin K$ and $L = K(\nu)$. Now that L/K is primitive, $\mathcal{A}(n) = K[D_1, D_p, \dots, D_{p^{n-1}}]$, the divided power Hopf algebra of dimension p^n, acts on L/K. Indeed, it can act on L/K in many ways.

Let $0 < b < p^n$ with $\gcd(b,p) = 1$, and set $x = \nu^{-b}$. Then $L = K(x)$ and $v_L(x) = -b$. We specify that $\mathcal{A}(n)$ acts on L as in (5.1), that is,

$$D_{p^r}(x^a) = \binom{a}{p^r}x^{a-p^r}. \tag{5.2}$$

By Lucas's Theorem,

$$\binom{a}{p^r} = a_{(r)}$$

where $a_{(r)}$ is the rth digit of the p-adic expansion of a. Note that this action depends on the choice of the generator x for L/K, and therefore depends on b.

Remark 5.6. — At this point, we make explicit the connection with the intuition of a scaffold, presented in §1. Let $X_i = x^{p^{n-i}}$, and $\Psi_i = D_{p^{n-i}}$. Then (5.2) and (1.1) agree where $0 \leqslant a < p^n$ is expressed p-adically as both $a = a_0 + a_1 p + \cdots + a_{n-1}p^{n-1}$ to be consistent with Theorem 5.5 and $a = a_{(0)} + a_{(1)}p + \cdots + a_{(n-1)}p^{n-1}$ to be consistent with (2.1).

Remark 5.7. — In the present purely inseparable situation, the convention adopted by (2.1) where integers $0 \leqslant a < p^n$ are expressed p-adically as $a = \sum_{i=1}^{n} a_{(n-i)}p^{n-i}$ (and thus necessarily $X_i = x^{p^{n-i}}$ and $\Psi_i = D_{p^{n-i}}$) may seem awkward. So it is worth reiterating that we adopted this convention because scaffolds arose first in the setting of Galois extensions and in that setting it is natural to label the ith ramification break with the subscript i.

To complete the proof of Theorem 5.1 we now define an $\mathcal{A}(n)$-scaffold on L/K with b as its sole shift parameter. This means, following Definition 2.3, that we need two sets of elements: elements $\lambda_t \in L$ for all integers t with $v_L(\lambda_t) = t$, and elements $\Psi_k \in \mathcal{A}(n)$ for $1 \leqslant k \leqslant n$. But since the shift parameters are all the same, we can simplify notation. From (2.2), we see that $\mathfrak{b}(s) = bs$. Let a be an integer with $ab \equiv -1 \pmod{p^n}$. Thus for $t \in \mathbb{Z}$, $\mathfrak{a}(t)$ can be more easily understood as the least non-negative residue of at modulo p^n. For each t in $\mathbb{Z}$, define f_t by

$$t = -b\mathfrak{a}(t) + p^n f_t\,.$$

Hence $f_t > 0$ for all $t > 0$. Expand $\mathfrak{a}(t)$ p-adically as $\mathfrak{a}(t) = \mathfrak{a}(t)_{(0)} + \mathfrak{a}(t)_{(1)}p + \cdots + \mathfrak{a}(t)_{(n-1)}p^{n-1}$. For the λ_t with $t \in \mathbb{Z}$, set

$$\lambda_t = \frac{\pi^{f_t} x^{\mathfrak{a}(t)}}{\mathfrak{a}(t)_{(0)}!\mathfrak{a}(t)_{(1)}!\ldots\mathfrak{a}(t)_{(n-1)}!} = \pi^{f_t}\prod_{i=1}^{n}\frac{X_i^{\mathfrak{a}(t)_{(n-i)}}}{\mathfrak{a}(t)_{(n-i)}!}\,,$$

where X_i is as in Remark 5.6. Observe that f_t was defined so that $v_L(\lambda_t) = -b\mathfrak{a}(t)+p^n f_t = t$, and if $t_1 \equiv t_2 \pmod{p^n}$, then $\mathfrak{a}(t_1) = \mathfrak{a}(t_2)$ and $\lambda_{t_1}\lambda_{t_2}^{-1} = \pi^{f_{t_1}-f_{t_2}} \in K$. As in Remark 5.6, for $1 \leqslant r \leqslant n$, set

$$\Psi_r = D_{p^{n-r}}\,.$$

Now observe that (5.2) together with Lucas's Theorem imply

$$\Psi_r\lambda_t = \begin{cases} \lambda_{t+p^{n-r}b} & \text{if } \mathfrak{a}(t)_{(n-r)} > 0\,,\\ 0 & \text{if } \mathfrak{a}(t)_{(n-r)} = 0\,.\end{cases}$$

Based upon Definition 2.3 this justifies our assertion that the intuition of a scaffold yields a scaffold. It also proves the following result.

Proposition 5.8. — *The elements* $\{\lambda_t\}_{t\in\mathbb{Z}}, \{\Psi_r\}_{0\leqslant r\leqslant n}$ *form an* $\mathcal{A}(n)$-*scaffold on* L *of precision* ∞.

Appendix A. Comparison of definitions of scaffold

A.1. An alternative characterization of A-scaffolds

Let K be a local field with residue characteristic p, let L/K be a totally ramified field extension of degree p^n, and let A be a K-algebra of dimension p^n with a K-linear action on L. We assume that we are given a family of elements $\Psi_1, \dots, \Psi_n$ of A. For $s \in \mathbb{S}_{p^n}$, we then have the set $\Upsilon^{(s)}$ of monomials in the Ψ_i, as defined before (2.4). We also suppose we are given functions $\mathfrak{b}$, $\mathfrak{a}$ corresponding to a family of shift parameters $b_1, \dots, b_n$, all relatively prime to p. We consider the following conditions on the Ψ_i:

$$\Psi_i \cdot 1 = 0 \text{ for each } i\,; \tag{A.1}$$

$$v_L(\Psi \cdot \rho) = v_L(\rho) + \mathfrak{b}(s) \text{ for all } \Psi \in \Upsilon^{(s)} \text{ and } s \in \mathbb{S}_{p^n}\,, \tag{A.2}$$

for some given $\rho \in L\backslash\{0\}$;

$$v_L(\Psi_i^p \cdot \alpha) > v_L(\alpha) + b_i p^{n-i+1} \text{ for all } i \text{ and all } \alpha \in L\backslash\{0\}\,; \tag{A.3}$$

and the stronger form of (A.3),

$$\Psi_i^p = 0 \text{ for all } i\,. \tag{A.4}$$

Let $\{\lambda_t\}_{t\in\mathbb{Z}}$ be any family of elements of L satisfying the conditions of Definition 2.3 (1): $v_L(\lambda_t) = t$ for all t, and $\lambda_{t_1}\lambda_{t_2}^{-1} \in K$ whenever $t_1 \equiv t_2 \pmod{p^n}$.

Theorem A.1.

(1) *Suppose that the* Ψ_i *satisfy* (A.1) *and* (A.3), *and there is some* ρ *for which* (A.2) *holds. Then the* λ_t *and the* Ψ_i *form an* A-*scaffold of precision* $\mathfrak{c} = 1$ *on* L *in the sense of Definition 2.3, and its shift parameters are* $b_1, \dots, b_n$. *Moreover* $\mathfrak{a}(v_L(\rho)) = p^n - 1$.

(2) *If, furthermore,* (A.4) *holds and* A *is commutative, then the* λ_t *may be chosen so that the* A-*scaffold has precision* ∞.

(3) *Conversely, if the* λ_t *and the* Ψ_i *form an* A-*scaffold of some precision* $\mathfrak{c} \geqslant 1$ *in the sense of Definition 2.3, then* (A.1) *and* (A.3) *hold, and* (A.2) *holds for any* $\rho \in L$ *with* $\mathfrak{a}(v_L(\rho)) = p^n - 1$.

Proof.

(1). — Since (A.1) holds by hypothesis, we will have an A-scaffold of precision 1 provided that the congruence in Definition 2.3 (2) holds with $\mathfrak{c} = 1$ and some choice of the units $u_{i,t}$. This will be the case if, for each $t \in \mathbb{Z}$ and each i, we have

$$v_L(\Psi_i \cdot \lambda_t) \begin{cases} = t + p^{n-i} b_i & \text{if } \mathfrak{a}(t)_{(n-i)} \geqslant 1, \\ > t + p^{n-i} b_i & \text{if } \mathfrak{a}(t)_{(n-i)} = 0. \end{cases} \tag{A.5}$$

Fix i, and, for each $s \in \mathbb{S}_{p^n}$, define $\Psi_*^{(s)} \in \Upsilon^{(s)}$ by

$$\Psi_*^{(s)} = \Psi_i^{s_{(n-i)}} \Psi_n^{s_{(0)}} \dots \Psi_{i-1}^{s_{(n-i-1)}} \Psi_{i+1}^{s_{(n-i+1)}} \dots \Psi_1^{s_{(n-1)}}.$$

Thus $\Psi_*^{(s)}$ is obtained from $\Psi^{(s)}$ by bringing all the factors Ψ_i to the left (so in particular $\Psi_*^{(s)} = \Psi^{(s)}$ if $i = n$). From (A.2) we have $v_L(\Psi_*^{(s)} \cdot \rho) = v_L(\rho) + \mathfrak{b}(s)$. Thus $\{v_L(\Psi_*^{(s)} \cdot \rho) : s \in \mathbb{S}_{p^n}\}$ is a complete set of residues mod p^n, and hence $\{\Psi_*^{(s)} \cdot \rho : s \in \mathbb{S}_{p^n}\}$ is a K-basis for L.

Now fix s as well. If $s_{(n-i)} < p-1$ then $\Psi_i \Psi_*^{(s)} \in \Upsilon^{(s')}$ where $s' = s + p^{n-i}$, so that $s'_{(n-i)} = s_{(n-i)} + 1$ and $s'_{(n-j)} = s_{(n-j)}$ for $j \neq i$. Thus, from (A.2),

$$v_L(\Psi_i \Psi_*^{(s)} \cdot \rho) = v_P(\rho) + \mathfrak{b}(s') = v_L(\Psi_*^{(s)} \cdot \rho) + b_i p^{n-i} \text{ if } s_{(n-i)} < p-1. \tag{A.6}$$

On the other hand, if $s_{(n-i)} = p-1$ then $\Psi_i \Psi_*^{(s)} = \Psi_i^p \Psi_*^{(s'')}$ where $s'' = s - (p-1)p^{n-i}$, so that $s''_{(n-i)} = 0$ and $s''_{(n-j)} = s_{(n-j)}$ for $j \neq i$. Then $v_L(\Psi_i \Psi_*^{(s)} \cdot \rho) = v_L(\Psi_i^p \Psi_*^{(s'')} \cdot \rho) > v_L(\Psi_*^{(s'')} \cdot \rho) + b_i p^{n-i+1}$ by (A.3). But $v_L(\Psi_*^{(s'')} \cdot \rho) = v_L(\rho) + \mathfrak{b}(s'') = v_L(\rho) + \mathfrak{b}(s) - b_i(p-1)p^{n-i}$ by (A.2). Hence

$$v_L(\Psi_i \Psi_*^{(s)} \cdot \rho) > v_L(\Psi_*^{(s)} \rho) + b_i p^{n-i} \text{ if } s_{(n-i)} = p-1. \tag{A.7}$$

Now let $\alpha \neq 0$ be an arbitrary element of L with $v_L(\alpha) = t$. Then we may write $\alpha = \sum_{s \in \mathbb{S}_{p^n}} x_s \Psi_*^{(s)} \cdot \rho$ with the $x_s \in K$. The sum contains a unique term of minimal valuation; let this occur at $s = s'$. Then $t = p^n v_K(x_{s'}) + v_L(\rho) + \mathfrak{b}(s')$. Applying (A.6) or (A.7) to each term in the sum separately, we obtain

$$v_L(\Psi_i \cdot \alpha) \begin{cases} = t + p^{n-i} b_i & \text{if } s'_{(n-i)} < p-1, \\ > t + p^{n-i} b_i & \text{if } s'_{(n-i)} = p-1. \end{cases} \tag{A.8}$$

Before completing the proof of (A.5), we consider $v_L(\rho)$. There is some $s \in \mathbb{S}_{p^n}$ for which $v_L(\Psi_*^{(s)} \cdot \rho) \equiv 0 \pmod{p^n}$. By (A.2), s is independent of i. We may write $\Psi_*^{(s)} \cdot \rho = x + \beta$ where $x \in K$ and $v_L(\beta) > v_L(\Psi_*^{(s)} \rho)$. Using (A.1) and (A.8), we therefore have

$$v_L(\Psi_i \Psi_*^{(s)} \cdot \rho) = v_L(\Psi_i \cdot \beta) > v_L(\Psi_*^{(s)} \cdot \rho) + p^{n-i} b_i\,.$$

Comparing with (A.8), we see that we must have $s_{(n-i)} = p-1$. This holds for each i, so $s = p^n-1$. Thus, by the choice of s, we have $v_L(\rho) \equiv -\mathfrak{b}(p^n-1) \pmod{p^n}$, or equivalently, $\mathfrak{a}(v_L(\rho)) = p^n - 1$.

Recall that in (A.8) we have $t = v_L(\alpha) \equiv v_L(\rho) + \mathfrak{b}(s') \pmod{p^n}$. Thus $t \equiv -\mathfrak{b}(p^n - 1) + \mathfrak{b}(s') = -\mathfrak{b}(p^n - 1 - s')$. Hence $\mathfrak{a}(t) = p^n - 1 - s'$, so the condition $s'_{(n-i)} < p-1$ in (A.8) is equivalent to $\mathfrak{a}(t)_{(n-i)} \geqslant 1$. Now (A.5) follows on applying (A.8) to $\alpha = \lambda_t$.

(2). — Fix a uniformizing element π of K. Given $t \in \mathbb{Z}$, we choose $\lambda_t = \pi^f \Psi^{(s)} \cdot \rho$ where $p^n f + v_L(\rho) + \mathfrak{b}(s) = t$. Then $v_L(\lambda_t) = t$, and $\lambda_{t_1}\lambda_{t_2}^{-1} = \pi^{(t_1-t_2)/p^n} \in K$ when $t_1 \equiv t_2 \pmod{p^n}$. Also, as we have shown above, $\mathfrak{a}(t) = p^n - 1 - s$, so that $\mathfrak{a}(t)_{(n-i)} \geqslant 1$ if and only if $s_{n-i)} < p-1$. As A is commutative and $\Psi_i^p = 0$, we have $\Psi_i \Psi^{(s)} \cdot \rho = 0$ if $s_{(n-i)} = p-1$, so that $\Psi_i \cdot \lambda_t = 0$. On the other hand, if $s_{(n-i)} \neq p-1$ then $\Psi_i \cdot \lambda_t = \lambda_{t+b_i p^{n-i}}$. Thus the congruence in Definition 2.3 (2) becomes an equality (with $u_{i,t} = 1$ for all i and t).

(3). — Since we have an A-scaffold in the sense of Definition 2.3, (A.1) holds. Also, from (2.6), for any $s \in \mathbb{S}_{p^n}$ and any $\Psi \in \Upsilon^{(s)}$ we have

$$v_L(\Psi \cdot \lambda_t) \begin{cases} = t + \mathfrak{b}(s) & \text{if } s \preceq \mathfrak{a}(t), \\ > t + \mathfrak{b}(s) & \text{otherwise.} \end{cases} \tag{A.9}$$

For an arbitrary $\alpha \in L$ with $v_L(\alpha) = t$, we may write $\alpha = u\lambda_t + \sum_{j=1}^{p^n-1} y_j \lambda_{t+j}$ for some $u \in \mathfrak{O}_K^\times$ and $y_j \in \mathfrak{O}_K$. Applying (A.9) to each term, we find that (A.9) still holds if we replace λ_t by α. In particular, taking $\Psi = \Psi_i$, we have

$$v_L(\Psi_i \cdot \alpha) \begin{cases} = t + b_i p^{n-i} & \text{if } \mathfrak{a}(t)_{(n-i)} > 0, \\ > t + p^{n-i} b_i & \text{otherwise.} \end{cases} \tag{A.10}$$

Moreover, writing $t' = v_L(\Psi_i \cdot \alpha)$, we have $\mathfrak{a}(t')_{(n-i)} = \mathfrak{a}(t)_{(n-i)} - 1$ if $\mathfrak{a}(t)_{(n-i)} > 0$. Repeating this argument p times, we obtain (A.3). Finally, for any ρ with $\mathfrak{a}(v_L(\rho)) = p^n - 1$, (A.2) follows inductively from (A.10). $\square$

A.2. Galois scaffolds in previous papers

We now use Theorem A.1 to explain how the A-scaffolds of this paper are related to the Galois scaffolds of the earlier papers [19, 13, 14]. There we considered only abelian extensions L/K in characteristic p; the extensions in [19, 14] were elementary abelian of arbitrary rank, and those in [13] were elementary abelian or cyclic of degree p^2. The algebra A acting on L was

Table A.1. Properties of Galois scaffolds.

Paper	Explicit in definition	Used for Galois module structure
[19]	(A.11)	
[13]	(A.1), (A.11), (A.12)	(A.1), (A.2), (A.3)
[14]	(A.1), (A.11), (A.12),	(A.1), (A.2), (A.4)

always the group algebra $A = K[G]$ with $G = \mathrm{Gal}(L/K)$; in this setting, (A.1) simply says that the Ψ_i lie in the augmentation ideal of $K[G]$.

The definition of Galois scaffold varies slightly between these papers, and the conditions explicitly required are a little less restrictive than those of this paper. The Galois scaffolds constructed turn out to satisfy supplementary conditions which were used in obtaining results on Galois module structure. For the reader's convenience, the role of the different conditions in the various papers is summarized in Table A.1. (The conditions not already mentioned are introduced below.)

A.2.1. The paper [19]

Galois scaffolds first appeared in [19], where they were presented as a strengthening of the valuation criterion. Let K be a local field of residue characteristic $p > 0$, and let L/K be a totally ramified Galois extension of degree p^n with Galois group $G = \mathrm{Gal}(L/K)$. We say that L/K satisfies the valuation criterion if there exists $c \in \mathbb{Z}$ such that $L = K[G] \cdot \rho$ for every $\rho \in L$ with $v_L(\rho) = c$. In [19], L/K was said to have a Galois scaffold if there exist $c \in \mathbb{Z}$ and elements $\Psi_1, \ldots, \Psi_n \in K[G]$ such that, for every $\rho \in L$ with $v_L(\rho) = c$, the following condition holds:

$$\left\{v_L\left(\Psi^{(s)} \cdot \rho\right) : s \in \mathbb{S}_{p^n}\right\} \text{ is a complete set of residues } p^n. \tag{A.11}$$

Since L/K is totally ramified, (A.11) implies the valuation criterion for L/K.

For the Galois scaffolds actually constructed in [19], the conditions (A.1) and (A.2) hold, where the shift parameters b_i used to define $\mathfrak{b}$ are the (lower) ramification breaks of L/K, and ρ is any element of L with $v_L(\rho) \equiv b_n \pmod{p^n}$. (Indeed, for the near one-dimensional extensions considered in [19], the b_i are all congruent mod p^n, so $\mathfrak{b}(s) \equiv b_n s \pmod{p^n}$.) Moreover, (A.4) holds, and Theorem A.1 (1)(2) shows that the Galois scaffolds in [19] are $K[G]$-scaffolds of precision ∞ in the sense of this paper.

A.2.2. The paper [14]

In [14] (which was in fact written before [13]), the definition of Galois scaffold was refined to require (A.1) explicitly, and also to require the uniformity condition

$$v_L(\Psi_i^j \cdot \rho) - v_L(\rho) = j \cdot (v_L(\Psi_i \cdot \rho') - v_L(\rho')) \tag{A.12}$$

whenever $0 \leqslant j \leqslant p-1$ and $v_L(\rho)$, $v_L(\rho') \equiv c \pmod{p^n}$. Here, as above, c is the integer occurring in the valuation criterion. Note that (A.12) makes no explicit mention of the ramification breaks b_i. If we set

$$a_i = v_L(\Psi_i \cdot \rho) - v_L(\rho),$$

then (A.12) means that a_i is independent of the choice of ρ with $v_L(\rho) \equiv c \pmod{p^n}$, and that

$$v_L(\Psi_i^j \cdot \rho) = v_L(\rho) + j a_i \text{ if } 0 \leqslant j \leqslant p-1 \text{ and } v_L(\rho) \equiv c \pmod{p^n}. \tag{A.13}$$

Moreover, if (A.2) holds for the function $\mathfrak{b}$ given by some shift parameters $b_1, \ldots, b_n$, then (A.13) holds for $a_i = p^{n-i} b_i$ and any $c \equiv -\mathfrak{b}(p^n - 1) \pmod{p^n}$.

In view of (A.2), it is reasonable to replace (A.12) by

$$v_L\left(\Psi^{(s)} \cdot \rho\right) = v_L(\rho) + \sum_{i=1}^{n} s_{(n-i)} a_i \text{ for all } s \in \mathbb{S}_{p^n}, \tag{A.14}$$

where again ρ is any element of L with $v_L(\rho) \equiv c \pmod{p^n}$. Now if (A.14) holds for some integers a_i, then, by Proposition A.2 below, (A.11) is equivalent to the condition that (possibly after renumbering the Ψ_i and the a_i) there are integers $b_1, \ldots, b_n$, all relatively prime to p, such that $a_i = p^{n-i} b_i$. If we use these to define the function $\mathfrak{b}$, then, in the case of an abelian extension, (A.14) is equivalent to (A.2). We may therefore regard (A.2) as a natural strengthening of (A.14), and hence of (A.12).

The extensions considered in [14] are the near one-dimensional extensions constructed in [19], and the Galois scaffolds used are those of that paper. As explained above, they satisfy (A.1), (A.2) and (A.4). These properties were used in [14] to investigate the Galois module structure of the valuation rings.

A.2.3. The paper [13]

So that we focus on those results in [13] which are in neither [19] nor [14], we restrict our discussion here to cyclic extensions of degree p^2. In any case,

[13] used the same definition of Galois scaffold as [14]. The Galois scaffolds considered in [13] satisfy (A.1) and (A.2). The cyclic Galois scaffolds satisfy $\Psi_1^p = \Psi_2$, $\Psi_2^p = 0$, and (A.3) holds since $b_2 > p^2 b_1$. Thus again they are $K[G]$-scaffolds of some precision $\mathfrak{c} \geqslant 1$. (In fact $\mathfrak{c} = b_2 - pb_1$.) These properties are used in [13] to investigate the Galois module structure of the valuation ring in cyclic extensions of degree p^2 admitting a Galois scaffold.

A.3. An alternative form of the function $\mathfrak{b}$

In the above discussion, we needed the following result:

Proposition A.2. — *Given $a_i \in \mathbb{Z}$, let $\mathfrak{b}' : \mathbb{S}_p^n \longrightarrow \mathbb{Z}$ be defined by*

$$\mathfrak{b}'(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i \,.$$

Let $r : \mathbb{Z} \longrightarrow \mathbb{S}_{p^n}$ be given by $r(a) \equiv a \pmod{p^n}$, and let v denote the normalized valuation on the p-adic rationals. Then the function $r \circ \mathfrak{b}' : \mathbb{S}_{p^n} \to \mathbb{S}_{p^n}$ is bijective if and only if, after relabelling if necessary, $v(a_i) = n - i$ for $1 \leqslant i \leqslant n$.

Proof. — Note that $r \circ \mathfrak{b}'$ is surjective if and only if it is bijective. If $v(a_i) = n - i$ for $1 \leqslant i \leqslant n$, then clearly the image of $r \circ \mathfrak{b}'$ is $\mathbb{S}_{p^n}$. So consider the converse: Let $\mathfrak{b}'_n(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i$ and induct on n. For $n = 1$ the statement holds, since $r \circ \mathfrak{b}'_1 : \mathbb{S}_p \longrightarrow \mathbb{S}_p$ is bijective if and only if $\gcd(a_1, p) = 1$. Assume the statement holds for $n - 1$, and consider it for n. If $v(a_i) \geqslant 1$ for all i, then each $\mathfrak{b}'_n(x_1, \ldots, x_n)$ is a multiple of p. So we may assume there is an a_i that is relatively prime to p. Relabel so that $v(a_n) = 0$.

We prove now that, for $0 \leqslant k \leqslant p^{n-1} - 1$, there exist $x_{i,k} \in \mathbb{S}_p$ with

$$kpa_n = \mathfrak{b}'_n(x_{1,k}, \ldots, x_{n-1,k}, 0) = x_{1,k} a_1 + \cdots + x_{n-1,k} a_{n-1}. \tag{A.15}$$

The case $k = 0$ is clear. Assume the statement holds for $k - 1$, and consider it for k. Since $r(kpa_n) \in \mathbb{S}_{p^n}$ and $r \circ \mathfrak{b}'_n$ is surjective, there are $x_{i,k} \in \mathbb{S}_p$ such that $kpa_n = x_{1,k} a_1 + x_{2,k} a_2 + \cdots + x_{n,k} a_n$. If $x_{n,k} \neq 0$ then, on subtracting $(k-1)pa_n = x_{1,k-1} a_1 + \cdots + x_{n-1,k-1} a_{n-1}$, we find that

$$(p - x_{n,k}) a_n = (x_{1,k} - x_{1,k-1}) a_1 + \cdots + (x_{n-1,k} - x_{n-1,k-1}) a_{n-1} \,. \tag{A.16}$$

Let $y_n = p - x_{n,k}$, and, for $1 \leqslant i \leqslant n - 1$, let

$$y_i = \begin{cases} x_{i,k-1} - x_{i,k} & \text{if } x_{i,k-1} \geqslant x_{i,k} \,, \\ 0 & \text{if } x_{i,k-1} < x_{i,k} \,. \end{cases}$$

Let $z_n = 0$, and for $1 \leqslant i \leqslant n-1$ let

$$z_i = \begin{cases} 0 & \text{if } x_{i,k-1} \geqslant x_{i,k}\,, \\ x_{i,k} - x_{i,k-1} & \text{if } x_{i,k-1} < x_{i,k}\,. \end{cases}$$

Then (A.16) means that $\mathfrak{b}'_n(y_1, \ldots, y_n) = \mathfrak{b}'_n(z_1, \ldots, z_n)$. As $y_n \neq z_n$, this contradicts the injectivity of $r \circ \mathfrak{b}'_n$. Thus $x_{n,k} = 0$, and the statement holds for k.

Since $r \circ \mathfrak{b}_n$ is injective, (A.15) establishes a bijection between $\mathbb{S}_p^{n-1}$ and the multiples of p in $\mathbb{S}_{p^n}$. In particular, $a_i = \mathfrak{b}'_n(0, \ldots, 0, 1, 0 \ldots 0)$ is a multiple of p for each $i \leqslant n-1$. Thus the image of $\mathbb{S}_p^{n-1}$ under $\mathfrak{b}'_{n-1}(x_1, \ldots, x_{n-1}) = \sum_{i=1}^{n-1} x_i(a_i/p)$ maps modulo p^{n-1} onto $\mathbb{S}_{p^{n-1}}$. Using induction, we may relabel so that $v(a_i/p) = n-1-i$ for $1 \leqslant i \leqslant n-1$. We conclude that $v(a_i) = n-i$ for $1 \leqslant i \leqslant n$. □

BIBLIOGRAPHY

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

[2] H. P. Allen & M. E. Sweedler, "A theory of linear descent based on Hopf algebraic techniques", *J. Algebra* **12** (1969), p. 242-294.

[3] A.-M. Bergé, "Sur l'arithmétique d'une extension diédrale", *Ann. Inst. Fourier* **22** (1972), no. 2, p. 31-59.

[4] F. Bertrandias, J.-P. Bertrandias & M.-J. Ferton, "Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local", *C. R. Acad. Sci. Paris Sér. A* **274** (1972), p. 1388-1391.

[5] F. Bertrandias & M.-J. Ferton, "Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local", *C. R. Acad. Sci. Paris Sér. A* **274** (1972), p. 1330-1333.

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

[7] ———, "Local Leopoldt's problem for ideals in totally ramified p-extensions of complete discrete valuation fields", in *Algebraic number theory and algebraic geometry*, Contemporary Mathematics, vol. 300, American Mathematical Society, Providence, RI, 2002, p. 27-57.

[8] ———, "Leopoldt's problem for abelian totally ramified extensions of complete discrete valuation fields", *Algebra Anal.* **18** (2006), no. 5, p. 99-129, English transl. in *St. Petersbg. Math. J.* **18** (2007) no. 5, 757–778.

[9] N. P. Byott, "Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications", *J. Théor. Nombres Bordx* **9** (1997), no. 1, p. 201-219.

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

[11] ———, "A valuation criterion for normal basis generators of Hopf-Galois extensions on characteristic p", *J. Théor. Nombres Bordx* **23** (2011), no. 1, p. 59-70.

[12] N. P. Byott & G. G. Elder, "A valuation criterion for normal bases in elementary abelian extensions", *Bull. Lond. Math. Soc.* **39** (2007), no. 5, p. 705-708.

[13] ———, "Galois scaffolds and Galois module structure in extensions of characteristic p local fields of degree p^2", *J. Number Theory* **133** (2013), no. 11, p. 3598-3610.

[14] ———, "Integral Galois module structure for elementary abelian extensions with a Galois scaffold", *Proc. Am. Math. Soc.* **142** (2014), no. 11, p. 3705-3712.

[15] ———, "Sufficient conditions for large Galois scaffolds", *J. Number Theory* **182** (2018), p. 95-130.

[16] S. U. Chase & M. E. Sweedler, *Hopf algebras and Galois theory*, Lecture Notes in Math., vol. 97, Springer, Berlin, 1969.

[17] M. Chellali, "Erratum on: "Structure of inseparable extensions" by M. E. Sweedler", *Int. Math. Forum* **2** (2007), no. 65-68, p. 3269-3272.

[18] L. Childs & D. J. Moss, "Hopf algebras and local Galois module theory", in *Advances in Hopf algebras (Chicago, IL, 1992)*, Lecture Notes in Pure and Appl. Math., vol. 158, Dekker, New York, 1994, p. 1-24.

[19] G. G. Elder, "Galois scaffolding in one-dimensional elementary abelian extensions", *Proc. Am. Math. Soc.* **137** (2009), no. 4, p. 1193-1203.

[20] ———, "A valuation criterion for normal basis generators in local fields of characteristic p", *Arch. Math.* **94** (2010), no. 1, p. 43-47.

[21] M.-J. Ferton, "Sur les idéaux d'une extension cyclique de degré premier d'un corps local", *C. R. Acad. Sci. Paris Sér. A* **276** (1973), p. 1483-1486.

[22] C. Greither & B. Pareigis, "Hopf Galois theory for separable field extensions", *J. Algebra* **106** (1987), no. 1, p. 239-258.

[23] F. Heiderich, "On Hasse-Schmidt rings and module algebras", *J. Pure Appl. Algebra* **217** (2013), no. 7, p. 1303-1315.

[24] D. V. Huynh, "Artin–Schreier extensions and generalized associated orders", *J. Number Theory* **136** (2014), p. 28-45.

[25] H. Jacobinski, "Über die Hauptordnung eines Körpers als Gruppenmodul", *J. Reine Angew. Math.* **213** (1963/1964), p. 151-164.

[26] H. Johnston, "Explicit integral Galois module structure of weakly ramified extensions of local fields", *Proc. Am. Math. Soc.* **143** (2015), no. 12, p. 5059-5071.

[27] A. Koch, "Hopf Galois structures on primitive purely inseparable extensions", *New York J. Math.* **20** (2014), p. 779-797.

[28] ———, "Scaffolds and integral Hopf Galois module structure on purely inseparable extensions", *New York J. Math.* **21** (2015), p. 73-91.

[29] B. Köck, "Galois structure of Zariski cohomology for weakly ramified covers of curves", *Am. J. Math.* **126** (2004), no. 5, p. 1085-1107.

[30] H.-W. Leopoldt, "Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers", *J. Reine Angew. Math.* **201** (1959), p. 119-149.

[31] M. L. Marklove, "Local Galois Module Structure in Characteristic p", PhD Thesis, University of Exeter (U.K.), 2014, `https://ore.exeter.ac.uk/repository/handle/10871/14743`.

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

[33] Y. Miyata, "On the module structure of rings of integers in $\mathfrak{p}$-adic number fields over associated orders", *Math. Proc. Camb. Philos. Soc.* **123** (1998), no. 2, p. 199-212.

[34] S. Montgomery, *Hopf algebras and their actions on rings*, CBMS Regional Conference Series in Mathematics, vol. 82, American Mathematical Society, 1993.

[35] E. Noether, "Normalbasis bei Körpern ohne höhere Verzweigung", *J. Reine Angew. Math.* **167** (1932), p. 147-152.

[36] L. Riddle, "Proof of Lucas's Theorem", 2013, `http://ecademy.agnesscott.edu/~lriddle/ifs/siertri/LucasProof.htm`.

[37] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[38] B. de Smit, M. Florence & L. Thomas, "The valuation criterion for normal basis generators", *Bull. Lond. Math. Soc.* **44** (2012), no. 4, p. 729-737.

[39] B. de Smit & L. Thomas, "Local Galois module structure in positive characteristic and continued fractions", *Arch. Math.* **88** (2007), no. 3, p. 207-219.

[40] M. E. Sweedler, "Structure of inseparable extensions", *Ann. Math.* **87** (1968), p. 401-410, corrigendum in *ibid.* **89** (1969), 206–207; cf. also [17].

[41] ———, *Hopf algebras*, Mathematics Lecture Note Series, W. A. Benjamin, Inc., New York, 1969.

[42] M. J. Taylor, "Formal groups and the Galois module structure of local rings of integers", *J. Reine Angew. Math.* **358** (1985), p. 97-103.

[43] L. Thomas, "A valuation criterion for normal basis generators in equal positive characteristic", *J. Algebra* **320** (2008), no. 10, p. 3811-3820.

[44] ———, "On the Galois module structure of extensions of local fields", in *Actes de la Conférence "Fonctions L et Arithmétique"*, Publications Mathématiques de Besançon. Algèbre et Théorie des Nombres, Laboratoire de Mathématique de Besançon, 2010, p. 157-194.

Manuscrit reçu le 15 décembre 2014,
révisé le 18 juin 2016,
accepté le 13 juillet 2017.

Nigel P. BYOTT
Department of Mathematics
University of Exeter
Exeter, EX4 4QF (UK)
n.p.byott@exeter.ac.uk

Lindsay N. CHILDS
Department of Mathematics and Statistics
University at Albany
Albany, NY 12222 (USA)
lchilds@albany.edu

G. Griffith ELDER
Department of Mathematics
University of Nebraska at Omaha
Omaha NE 68182-0243 (USA)
elder@unomaha.edu