Journal de Théorie des Nombres
de Bordeaux **9** *(1997), 201–219*

Galois Structure of Ideals in Wildly Ramified Abelian p-Extensions of a p-adic Field, and Some Applications

par Nigel P. BYOTT

Résumé. Soit K une extension finie de $\mathbb{Q}_p$ d'indice de ramification e, et soit L/K une p-extension abélienne finie de groupe de Galois Γ et d'indice de ramification p^n. Nous donnons un critère en termes des nombres de ramification t_i permettant de décider lorsqu'un idéal fractionnaire $\mathfrak{P}^h$ de l'anneau de valuation S de L peut être libre sur son ordre associé $\mathfrak{A}(K\Gamma;\mathfrak{P}^h)$. En particulier, si $t_n - \lfloor t_n/p \rfloor < p^{n-1}e$, la codifférente ne peut être libre sur son ordre associé que si $t_i \equiv -1 \pmod{p^n}$ pour tout i. Nous déduisons de cela trois conséquences. Premièrement, si $\mathfrak{A}(K\Gamma;S)$ est un ordre de Hopf et si S/R est une $\mathfrak{A}(K\Gamma;S)$-extension galoisienne, où R est l'anneau de valuation de K, alors $t_i \equiv -1 \pmod{p^n}$ pour tout i. Deuxièmement, si $K = k_r$ et $L = k_{m+r}$ sont des corps de points de division d'un groupe de Lubin-Tate, avec $m > r$ et $k \neq \mathbb{Q}_p$, alors S n'est pas libre sur $\mathfrak{A}(K\Gamma;S)$. Troisièmement, ces extensions k_{m+r}/k_r possèdent deux structures galoisiennes de Hopf différentes, mettant en évidence des comportements différents au niveau des entiers.

Abstract. Let K be a finite extension of $\mathbb{Q}_p$ with ramification index e, and let L/K be a finite abelian p-extension with Galois group Γ and ramification index p^n. We give a criterion in terms of the ramification numbers t_i for a fractional ideal $\mathfrak{P}^h$ of the valuation ring S of L not to be free over its associated order $\mathfrak{A}(K\Gamma;\mathfrak{P}^h)$. In particular, if $t_n - \lfloor t_n/p \rfloor < p^{n-1}e$ then the inverse different can be free over its associated order only when $t_i \equiv -1 \pmod{p^n}$ for all i. We give three consequences of this. Firstly, if $\mathfrak{A}(K\Gamma;S)$ is a Hopf order and S is $\mathfrak{A}(K\Gamma;S)$-Galois then $t_i \equiv -1 \pmod{p^n}$ for all i. Secondly, if $K = k_r$, $L = k_{m+r}$ are Lubin-Tate division fields, with $m > r$ and $k \neq \mathbb{Q}_p$, then S is not free over $\mathfrak{A}(K\Gamma;S)$. Thirdly, these extensions k_{m+r}/k_r admit two Hopf Galois structures exhibiting different behaviour at integral level.

1991 *Mathematics Subject Classification.* 11S23, 11R33, 11S31, 16W30.

Key words and phrases. Galois module structure, associated order, Hopf order, Lubin-Tate formal group.

Manuscrit reçu le 12 novembre 1996

This work was started while I was visiting the Institut für Mathematik, Karl-Franzens Universität, Graz, with financial support from the British Council (project number VIE/891/5). I would like to thank the Institut for their hospitality, and Günter Lettl for useful conversations.

1. INTRODUCTION

Let p be a prime number, and let K be a finite extension of the p-adic field $\mathbb{Q}_p$. We write $e = e(K/\mathbb{Q}_p)$ for the absolute ramification index of K. If L is a finite normal extension of K, with Galois group $\Gamma = \mathrm{Gal}(L/K)$ say, it follows from the Normal Basis Theorem that L is a free module of rank 1 over the group algebra $K\Gamma$. Let R (respectively, S) denote the valuation ring of K (respectively, L), and let $\mathfrak{p}$ (respectively, $\mathfrak{P}$) denote its maximal ideal. Then S, or more generally any fractional S-ideal $\mathfrak{P}^h$, is a module over the integral group ring $R\Gamma$. In general, $\mathfrak{P}^h$ is not free over $R\Gamma$. Indeed, it is well-known that S itself is a free $R\Gamma$-module if and only if L/K is at most tamely ramified. In this case every ideal $\mathfrak{P}^h$ is a free $R\Gamma$-module (see [U]). To investigate the $R\Gamma$-structure of $\mathfrak{P}^h$ more generally, one considers the associated order

$$\mathfrak{A}(K\Gamma; \mathfrak{P}^h) = \{\alpha \in K\Gamma \mid \alpha\mathfrak{P}^h \subseteq \mathfrak{P}^h\}.$$

This is indeed an R-order in the group algebra $K\Gamma$, and $\mathfrak{P}^h$ is an $\mathfrak{A}(K\Gamma; \mathfrak{P}^h)$-module.

If $K = \mathbb{Q}_p$ and $L/\mathbb{Q}_p$ is any abelian extension, then S is free over its associated order (see [L]). This is not true for more general K, even if K is unramified (see [Be]), and there are relatively few cases where the associated order is known explicitly (e.g. [B-F], [F], [By1], [T1]). There are however a number of results on the structure of S or $\mathfrak{P}^h$ as a $\mathbb{Z}_p\Gamma$-module, both describing its module structure completely in certain cases (e.g. [RC-VS-M], [E-M], [E]), and giving more general results regarding the associated order in $\mathbb{Q}_p\Gamma$ (e.g. [Bl-Bu], [Bu1], [Bu2]). In a somewhat different direction, the existence of $R\Gamma$-isomorphisms between fractional S-ideals was investigated in [By2].

In this paper, we will be concerned only with associated orders in $K\Gamma$, and will not require any hypothesis on the absolute ramification of K. We take L/K to be an abelian p-extension with ramification index p^n, and we give in Theorem 3.13 a criterion in terms of the ramification numbers t_i for an ideal $\mathfrak{P}^h$ not to be free over its associated order. This takes a somewhat simpler form in the case that $\mathfrak{P}^h$ is the inverse different $\mathfrak{D}_{L/K}^{-1}$ (Theorem 3.10); under a mild restriction on the largest ramification number, $\mathfrak{D}_{L/K}^{-1}$ cannot be free over its associated order unless $t_i \equiv -1 \pmod{p^n}$ for all i. Our method requires only knowledge of the t_i, and does not involve any explicit calculations with associated orders. We do however make essential use of Vostokov's criterion for the $R\Gamma$-indecomposability of S-ideals.

We give three interrelated applications. Firstly if, for the abelian p-extension L/K, the associated order $\mathfrak{A} = \mathfrak{A}(S; K\Gamma)$ is a Hopf order, and if furthermore S is a Galois $\mathfrak{A}$-extension of R, then $t_i \equiv -1 \pmod{p^n}$. This is already known in the special cases where Γ is cyclic of order p^2 (see [G]) or elementary abelian (see [By3]). Secondly, we take $K = k_r$ and $L = k_{m+r}$ to be Lubin-Tate division fields obtained from an extension k of $\mathbb{Q}_p$. When $m \leq r$, these provide one of the few families of extensions where the associated order $\mathfrak{A}$ is known explicitly (see [T1]), and in this case S is free over $\mathfrak{A}$. It is also known that S is free over $\mathfrak{A}$ when $m > r$ and $k = \mathbb{Q}_p$ (see [C-L]). We complete these results with Theorem 5.1, which shows in the remaining case $m > r$, $k \neq \mathbb{Q}_p$ that S is not free over its associated order. Our final application concerns the comparison of different Hopf Galois structures at integral level. The Lubin-Tate extensions k_{m+r}/k_r admit both their classical Hopf Galois structure and another Hopf Galois structure, arising from the Kummer theory of formal groups. In the first Hopf Galois structure, Theorem 5.1 tells us that S is not free over its associated order, while in the second structure, S is automatically Galois, and hence free, over a Hopf order in the underlying Hopf algebra.

2. A non-freeness criterion

In this section, we give a very general criterion for a lattice in a module over a finite-dimensional commutative K-algebra A not to be free over its associated order. This uses only some rather elementary commutative algebra.

Let $v: K \to \mathbb{Z} \cup \{\infty\}$ be the valuation on K, normalised so that v is surjective. We fix once and for all $\mu \in K$ with $v(\mu) = 1$.

Let V be a free left A-module of rank 1. An R-submodule M of V is a *lattice* if it is finitely generated and spans V over K. The associated order $\mathfrak{A}(A; M)$ of a lattice M is defined by

$$\mathfrak{A} = \mathfrak{A}(A; M) = \{\alpha \in A \mid \alpha M \subseteq M\}.$$

Since A acts faithfully on V, it follows that $\mathfrak{A}$ is indeed an R-order in A. Clearly M is an $\mathfrak{A}$-module.

THEOREM 2.1. *With the above notation, suppose that*

(i) *$\mathfrak{A}$ is a local ring;*
(ii) *there exists a generating set $\{m_1, \ldots, m_n\}$ for M as an $\mathfrak{A}$-module, with the property that $\mathfrak{A} m_i \neq M$ for $1 \leq i \leq n$.*

Then M is not free as an $\mathfrak{A}$-module.

Proof. Suppose for a contradiction that M is free over $\mathfrak{A}$. Comparing R-ranks, M must then be free on one generator, m say. For $1 \leq i \leq n$ we have $m_i = \alpha_i m$ for some $\alpha_i \in \mathfrak{A}$. Since $\mathfrak{A}\alpha_i m = \mathfrak{A}m_i \neq M$ but $\mathfrak{A}m = M$, it follows that α_i is not a unit in $\mathfrak{A}$. Thus each α_i lies in the Jacobson radical J of the commutative local ring $\mathfrak{A}$, and we have

$$M = \sum_{i=1}^{n} \mathfrak{A}m_i = \sum_{i=1}^{n} \mathfrak{A}\alpha_i m \subseteq JM.$$

Hence $M = 0$ by Nakayama's Lemma, contradicting the fact that M spans the A-module V of rank 1. $\square$

The next result enables us to verify the condition $\mathfrak{A}m_i \neq M$ in Theorem 2.1 without a complete knowledge of $\mathfrak{A}$.

LEMMA 2.2. *Let $m \in M$, and suppose that there exists $\alpha \in A$ such that*

(i) *$\alpha m \in \mathfrak{p}M$;*

(ii) *$\alpha m' \notin \mathfrak{p}M$ for some $m' \in M$.*

Then $\mathfrak{A}m \neq M$.

Remark. It is *not* assumed that $\alpha \in \mathfrak{A}$.

Proof. We write $\overline{M} = M/\mathfrak{p}M$ and $\overline{\mathfrak{A}} = \mathfrak{A}/\mathfrak{p}\mathfrak{A}$, and use a bar to denote the image of an element of M (respectively, $\mathfrak{A}$) in $\overline{M}$ (respectively, $\overline{\mathfrak{A}}$).

As R is a principal ideal domain, there is a basis $\gamma_1, \ldots, \gamma_d$ of $\mathfrak{A}$ over R. These elements also form a basis of A over K, so $\alpha = \sum_i c_i\gamma_i$ for some $c_i \in K$. Let

$$j = -\min_{1 \leq i \leq d}(v(c_i))$$

and let $\beta = \mu^j\alpha$. Then $\beta \in \mathfrak{A}$ and $\overline{\beta} \neq 0$ in $\overline{\mathfrak{A}}$. Now by (ii) we have $\alpha \notin \mathfrak{p}\mathfrak{A}$, and hence $c_i \notin \mathfrak{p}$ for some i. Thus $j \geq 0$, and it follows from (i) that $\beta m = \mu^j \alpha m \in \mathfrak{p}M$, so that $\overline{\beta}\,\overline{m} = 0$ in $\overline{M}$. Since $\overline{M}$ and $\overline{\mathfrak{A}}$ both have the same dimension d over the residue field $R/\mathfrak{p}$, this implies that $\overline{\mathfrak{A}}\,\overline{m} \neq \overline{M}$, and hence that $\mathfrak{A}m \neq M$. $\square$

Remark. In this section we could have taken K to be the field of fractions of any discrete valuation ring R (not necessarily complete, and with no assumption on the characteristic).

3. Ideals in abelian p-extensions

In this section, we assume that L/K is a finite abelian p-extension, and we apply Theorem 2.1 to the fractional ideals $\mathfrak{P}^h$ of the valuation ring S of L. This gives a condition on the ramification numbers which guarantees that $\mathfrak{P}^h$ is not free over its associated order. The result is strongest, and also easiest to state, when $\mathfrak{P}^h$ is the inverse different. Since this is the case which will be needed for our applications, we will discuss this case separately before considering a general ideal $\mathfrak{P}^h$.

We first recall some ramification theory. For this we take L/K to be any normal p-extension, not necessarily abelian. The ramification subgroups of $\Gamma = \mathrm{Gal}(L/K)$ are defined to be

$$\Gamma_j = \{\gamma \in \Gamma \mid (\gamma - 1)S \subseteq \mathfrak{P}^{j+1}\}, \qquad j \geq -1.$$

Thus $\Gamma_{-1} = \Gamma$, and Γ_0 is the inertia subgroup of Γ. Also, $\Gamma_1 = \Gamma_0$ since L/K is a p-extension. Let $v_L\colon L \to \mathbb{Z} \cup \{\infty\}$ denote the valuation on L, normalised so that v_L is surjective. From [S2, IV §2 Exercise 3(a)] we have

Proposition 3.1. *If $\gamma \in \Gamma_j \backslash \Gamma_{j+1}$ and $x \in L$ then*

$$v_L\big((\gamma - 1)x\big) \geq v_L(x) + j,$$

with equality if and only if $(v_L(x), p) = 1$. $\square$

Let $|\Gamma_1| = p^n$. Thus $p^n = e(L/K)$ is the ramification index of the extension L/K. We assume that L/K is ramified, so $n \geq 1$. The ramification numbers of L/K (in the lower numbering) are the integers $t \geq 1$ such that $\Gamma_t \neq \Gamma_{t+1}$. It is convenient to adopt the following notation for these:

$$t_i = \max\{j \mid |\Gamma_j| > p^{n-i}\} \qquad 1 \leq i \leq n. \tag{3.2}$$

Thus $1 \leq t_1 \leq t_2 \leq \ldots \leq t_n$, and $t_i = t_{i+1}$ for some i if the index of Γ_{j+1} in Γ_j exceeds p for some $j \geq 1$.

The inverse different $\mathfrak{D}^{-1}_{L/K}$ is the fractional S-ideal defined by

$$\mathfrak{D}^{-1}_{L/K} = \{x \in L \mid \mathrm{Tr}_{L/K}(xS) \subseteq R\}, \tag{3.3}$$

where $\mathrm{Tr}_{L/K}$ denotes the trace from L to K. It can be expressed in terms of the ramification numbers by means of Hilbert's formula [S2, IV §2 Proposition 4]:

$$\begin{aligned} &\mathfrak{D}^{-1}_{L/K} = \mathfrak{P}^{-w} \qquad \text{where} \\ &w = \sum_{j=0}^{\infty}(|\Gamma_j| - 1) = (t_1 + 1)(p^n - 1) + \sum_{i=1}^{n-1}(t_{i+1} - t_i)(p^{n-i} - 1). \end{aligned} \tag{3.4}$$

Let $a \in \{0, \dots, p-1\}$ be the least non-negative residue of t_1 modulo p. Then from [S2, IV §2 Proposition 11 and Exercise 3(f)] we have

PROPOSITION 3.5. *$t_i \equiv a \pmod p$ for $1 \le i \le n$, and if $a = 0$ then $t_i = \dfrac{p^i e}{p-1}$ for $1 \le i \le n$.* □

We now recall a result of Vostokov. For any real number x, we write $\lfloor x \rfloor$ for the unique integer satisfying $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$.

THEOREM 3.6. *([V1, Theorem 3], [V2, Theorem 4]) Let L/K be an abelian p-extension with ramification index p^n. If the largest ramification number t_n satisfies the condition*

$$t_n - \left\lfloor \frac{t_n}{p} \right\rfloor < p^{n-1} e$$

then every fractional S-ideal is indecomposable as an $R\Gamma$-module. □

The hypothesis on t_n is rather mild, as the next result shows.

PROPOSITION 3.7. *For any normal p-extension L/K with ramification index p^n, we have*

$$t_n - \left\lfloor \frac{t_n}{p} \right\rfloor \le p^{n-1} e, \tag{3.8}$$

with equality if and only if

$$t_n = \frac{p^n e - a}{p-1}.$$

If equality occurs in (3.8) then $a \equiv e \pmod{p-1}$ and one of the following holds:

(i) *Γ_1 is cyclic, $\mathrm{Tr}_{L/K}(S) = p^n R$ and $t_i = \dfrac{p^i e - a}{p-1}$ for $1 \le i \le n$;*

(ii) *$p = 2$, and for some $k \in \{1, \dots, n-1\}$ we have*

$$t_i = 1 \quad \text{for } 1 \le i \le k \qquad \text{and} \qquad t_i = \frac{p^i e - a}{p-1} = 2^i e - 1 \quad \text{for } k+1 \le i \le n.$$

Moreover $\Gamma_{t_{k+1}}$ is cyclic and $\Gamma_1/\Gamma_{t_{k+1}}$ is elementary abelian.

Proof. By [S2, IV §2 Exercise 3(c)], $\Gamma_i = \{1\}$ if $i > \dfrac{p^n e}{p-1}$, so $t_n \leq \dfrac{p^n e}{p-1}$. As $(p-1)t_n \equiv -a \pmod{p}$, it follows that

$$t_n \leq \frac{p^n e - a}{p-1}. \tag{3.9}$$

Writing $t_n = pt' + a$, we therefore have $t' \leq \dfrac{p^{n-1}e - a}{p-1}$, with equality if and only if equality holds in (3.9). Thus

$$t_n - \left\lfloor \frac{t_n}{p} \right\rfloor = (p-1)t' + a \leq p^{n-1}e,$$

with equality if and only if equality holds in (3.9). This proves the first sentence of the Proposition. If equality holds in (3.9) then $p^n e \equiv a \pmod{p-1}$ since t_n is an integer, and hence $a \equiv e \pmod{p-1}$. Moreover, since $t_i \equiv a \pmod{p}$ for $1 \leq i \leq n$ by Proposition 3.5, the above argument, applied to suitable subextensions L_i/K of L/K, shows that, for each i,

$$t_i - \left\lfloor \frac{t_i}{p} \right\rfloor \leq p^{i-1}e \quad \text{with equality if and only if } t_i = \frac{p^i e - a}{p-1}.$$

If equality holds in (3.8), it now follows from [V1, Proposition 1] that (i) occurs, except in the case $p = 2$, $t_1 = 1$. In this case, if $t_n = 1$ then equality in (3.8) implies that $n = 1$, $e = 1$, and again (i) holds. We may therefore assume that $p = 2$, and that for some $k \in \{1, \ldots, n-1\}$ we have $t_k = 1$, $t_{k+1} > 1$. Let F be the fixed subfield of L under $\Gamma_{t_{k+1}}$. Applying [V1, Proposition 1] to L/F, we find that $\Gamma_{t_{k+1}}$ is cyclic and the t_i for $i > k$ are as stated in (ii). (Note that our t_2 does not necessarily coincide with Vostokov's h_2, because of our convention (3.2).) Finally, $\Gamma_1/\Gamma_{t_{k+1}} = \Gamma_{t_k}/\Gamma_{1+t_k}$, and this is elementary abelian by [S2, IV §2 Corollary 3 to Proposition 7]. $\square$

We are now ready to apply Theorem 2.1 to the inverse different $\mathfrak{D}_{L/K}^{-1} = \mathfrak{P}^{-w}$.

THEOREM 3.10. *Let L/K be an abelian p-extension with ramification index p^n and ramification numbers $t_1, \ldots, t_n$. Suppose that*

$$t_n - \left\lfloor \frac{t_n}{p} \right\rfloor < p^{n-1}e. \tag{3.11}$$

If $\mathfrak{D}_{L/K}^{-1}$ is free over its associated order then $t_i \equiv -1 \pmod{p^n}$ *for* $1 \le i \le n$.

Proof. We assume that some ramification number $t = t_i$ satisfies $t \not\equiv -1 \pmod{p^n}$, and apply Theorem 2.1 with $M = \mathfrak{D}_{L/K}^{-1}$, $A = K\Gamma$, $V = L$ to show that $\mathfrak{D}_{L/K}^{-1}$ is not free over its associated order $\mathfrak{A}$. (Note that L is indeed a free $K\Gamma$-module of rank 1 by the Normal Basis Theorem.) Thus we must verify conditions (i) and (ii) of Theorem 2.1.

As $\mathfrak{D}_{L/K}^{-1}$ spans L over K, the ring of $R\Gamma$-endomorphisms of $\mathfrak{D}_{L/K}^{-1}$ is precisely $\mathfrak{A}$. But $\mathfrak{D}_{L/K}^{-1}$ is indecomposable by Theorem 3.6, so $\mathfrak{A}$ contains no idempotents except 0 and 1. As R is complete, this implies that $\mathfrak{A}$ is a local ring, and condition (i) of Theorem 2.1 is satisfied.

We now turn to condition (ii) of Theorem 2.1. From the definition (3.3) of $\mathfrak{D}_{L/K}^{-1}$, we have

$$\mathrm{Tr}_{L/K}(\mathfrak{D}_{L/K}^{-1}) \subseteq R \quad \text{but} \quad \mathrm{Tr}_{L/K}(\mathfrak{P}^{-1}\mathfrak{D}_{L/K}^{-1}) \not\subseteq R,$$

and hence

$$\mathrm{Tr}_{L/K}(\mathfrak{p}\mathfrak{D}_{L/K}^{-1}) \subseteq \mathfrak{p} \quad \text{but} \quad \mathrm{Tr}_{L/K}(\mathfrak{p}\mathfrak{P}^{-1}\mathfrak{D}_{L/K}^{-1}) \not\subseteq \mathfrak{p}.$$

Thus $\mathrm{Tr}_{L/K}(x)$ is a unit in R for some $x \in \mathfrak{p}\mathfrak{P}^{-1}\mathfrak{D}_{L/K}^{-1} \backslash \mathfrak{p}\mathfrak{D}_{L/K}^{-1}$. Since $x \notin \mathfrak{p}\mathfrak{D}_{L/K}^{-1}$, we may extend x to an R-basis $x_1 = x, x_2, \ldots, x_d$ of $\mathfrak{D}_{L/K}^{-1}$. Let $z = \mathrm{Tr}_{L/K}(x)$, and define $y_1 = x_1$ and $y_j = x_j - z^{-1}T_{L/K}(x_j)x_1$ for $2 \le j \le d$. Then $y_1 \ldots, y_d$ is again an R-basis of $\mathfrak{D}_{L/K}^{-1}$, so $\{y_1, \ldots, y_d\}$ is certainly a generating set for $\mathfrak{D}_{L/K}^{-1}$ as an $\mathfrak{A}$-module. We must show, for each i, that $\mathfrak{A}y_i \ne \mathfrak{D}_{L/K}^{-1}$.

Comparing R-ranks, it is clear that if $\mathfrak{D}_{L/K}^{-1} = \mathfrak{A}y_i$ then $\mathfrak{D}_{L/K}^{-1}$ must be free over $\mathfrak{A}$ on the generator y_i. If this occurs then y_i also generates L as a free $K\Gamma$-module, and this is not the case for $i \ge 2$ since $\left(\sum_{\gamma\in\Gamma}\gamma\right) y_i = \mathrm{Tr}_{L/K}(y_i) = 0$. To show that $\mathfrak{A}y_1 \ne \mathfrak{D}_{L/K}^{-1}$, we use Lemma 2.2. Let $t = p^n b + \bar{t}$ with $0 \le \bar{t} \le p^n - 1$. If $\bar{t} = 0$ then $a = 0$, so

$$t_n = \frac{p^n e}{p-1} = \frac{p^n e - a}{p-1}$$

by Proposition 3.5, and hence we have equality in (3.8), contradicting (3.11).

Since $t \not\equiv -1 \pmod{p^n}$ by assumption, we therefore have $1 \le \bar{t} \le p^n - 2$. Let $\alpha = \mu^{-b}(\gamma - 1) \in K\Gamma$, where $\gamma \in \Gamma_t \backslash \Gamma_{t+1}$. Then, since $v_L(y_1) = v_L(x) = p^n - 1 - w$, it follows from Proposition 3.1 that

$$v_L(\alpha y_1) \ge p^n - 1 - w + \bar{t} \ge -w + p^n,$$

so condition (i) of Lemma 2.2 holds for y_1. To show condition (ii) of Lemma 2.2, choose $y' \in \mathfrak{D}_{L/K}^{-1}$ with valuation $1 - w$ if w is divisible by p and valuation $-w$ otherwise. In either case, $(v_L(y'), p) = 1$, so by Proposition 3.1,

$$v_L(\alpha y') = v_L(y') + \bar{t} \le (1 - w) + (p^n - 2) < -w + p^n.$$

Thus $\alpha y' \notin \mathfrak{p}\mathfrak{D}_{L/K}^{-1}$ and by Lemma 2.2, $\mathfrak{A} y_1 \ne \mathfrak{D}_{L/K}^{-1}$. Hence $\mathfrak{D}_{L/K}^{-1}$ is not free over $\mathfrak{A}$. □

Corollary 3.12. *Let L/K be an abelian p-extension with ramification index p^n and ramification numbers $t_1, \ldots, t_n$. Suppose that (3.11) holds and that $w \equiv 0 \pmod{p^n}$. If S is free over its associated order then $t_i \equiv -1 \pmod{p^n}$ for $1 \le i \le n$.*

Proof. We have $w = p^n c$ for some integer c, so $\mathfrak{D}_{L/K}^{-1} = \mu^{-c} S$. Thus $\mathfrak{D}_{L/K}^{-1}$ and S are isomorphic as $R\Gamma$-modules. These modules therefore have the same associated order $\mathfrak{A}$, and if S is free over $\mathfrak{A}$ then so is $\mathfrak{D}_{L/K}^{-1}$. The result is now immediate from Theorem 3.10. □

We now apply Theorem 2.1 to a general ideal $\mathfrak{P}^h$. In the case $h = -w$, Theorem 3.13 below reduces to Theorem 3.10. For any integer h, we write $\overline{h}$ for the least non-negative residue of h modulo p^n.

Theorem 3.13. *Let L/K be an abelian p-extension with ramification index p^n and ramification numbers $t_1, \ldots, t_n$, and suppose that (3.11) holds. Let $\mathfrak{P}^h$ be an arbitrary fractional S-ideal. Suppose that for some ramification number t we have $\bar{t} > \overline{h + w}$. If p divides h, suppose further that $\bar{t} \ne p^n - 1$. Then $\mathfrak{P}^h$ is not free over its associated order.*

Proof. For any integer c, we have $\mathfrak{P}^{h + p^n c} = \mu^c \mathfrak{P}^h \cong \mathfrak{P}^h$ as $R\Gamma$-modules. We may therefore assume that $-w \le h \le p^n - 1 - w$. Then $\overline{h + w} = h + w$, and $\mathrm{Tr}_{L/K}(\mathfrak{P}^h) = R$.

We now proceed much as in the proof of Theorem 3.10. Again, the associated order $\mathfrak{A}$ of $\mathfrak{P}^h$ is a local ring, and there is an element x in $\mathfrak{P}^h$ of valuation $p^n - 1 - w$ whose trace is a unit in R. As before, this enables us to construct an R-basis $y_1 = x, y_2, \ldots, y_d$ of $\mathfrak{P}^h$ with $v_L(y_1) = p^n - 1 - w$

and with $\mathrm{Tr}_{L/K}(y_i) = 0$ for $2 \leq i \leq d$. Then $\mathfrak{A}y_i \neq \mathfrak{P}^h$ for $2 \leq i \leq d$. The result will follow from Theorem 2.1 once we verify that $\mathfrak{A}y_1 \neq \mathfrak{P}^h$. We shall again do this using Lemma 2.2.

Let $t = p^n b + \bar{t}$ and let $\alpha = \mu^{-b}(\gamma - 1) \in K\Gamma$ where $\gamma \in \Gamma_t \backslash \Gamma_{t+1}$. Then by Proposition 3.1 we have

$$v_L(\alpha y_1) \geq (p^n - 1 - w) + \bar{t} > h + p^n - 1$$

since $\bar{t} > h + w$. Thus $\alpha y_1 \in \mathfrak{p}\mathfrak{P}^h$, and condition (i) of Lemma 2.2 is satisfied for y_1. To check condition (ii), take $y' \in \mathfrak{P}^h$ with valuation h if $(h, p) = 1$ and with valuation $h+1$ otherwise. In either case $(v_L(y'), p) = 1$, so

$$v_L(\alpha y') = v_L(y') + \bar{t} \leq h + p^n - 1$$

by Proposition 3.1, since by hypothesis $\bar{t} \leq p^n - 2$ if p divides h. Thus $\alpha y' \notin \mathfrak{p}\mathfrak{P}^h$, as required. $\square$

We illustrate Theorem 3.13 with some special cases.

Corollary 3.14. *With the notation of Theorem 3.13, suppose that (3.11) holds. Let $\mathfrak{P}^h$ be an arbitrary fractional S-ideal.*

(i) *If $t_i \equiv -2 \pmod{p^n}$ for some i, then $\mathfrak{P}^h$ cannot be free over $\mathfrak{A}(K\Gamma; \mathfrak{P}^h)$ unless $h \equiv -1 - w$ or $-2 - w \pmod{p^n}$.*

(ii) *If $t_i \equiv -1 \pmod{p^n}$ for some i, then $\mathfrak{P}^h$ cannot be free over $\mathfrak{A}(K\Gamma; \mathfrak{P}^h)$ unless either $h \equiv -1 - w \pmod{p^n}$ or $h \equiv 0 \pmod{p}$.*

(iii) *If $t_i \equiv -1 \pmod{p^n}$ for all i, then $\mathfrak{P}^h$ cannot be free over $\mathfrak{A}(K\Gamma; \mathfrak{P}^h)$ unless either $h \equiv -1 \pmod{p^n}$ or $h \equiv 0 \pmod{p}$.*

Proof. (i) and (ii) are immediate from Theorem 3.13. (iii) is a special case of (ii), since if $t_i \equiv -1 \pmod{p^n}$ for all i then $w \equiv 0 \pmod{p^n}$ by (3.4). $\square$

Remarks. (i) Our method gives no information on the excluded ideals in Theorem 3.13. For a ramified cyclic extension of degree p, Ferton [F] has determined the structure of all ideals over their associated orders. Assuming that $t_1 < \dfrac{pe}{p-1} - 2$, it follows from her results that when $t_1 \equiv -1 \pmod{p}$ the ideal $\mathfrak{P}^h$ is free if and only if $h \equiv 0$ or $p - 1 \pmod{p}$, and when $t_1 \equiv -2 \pmod{p}$, the ideal $\mathfrak{P}^h$ is free if and only if $h \equiv p - 3$ or $p - 2 \pmod{p}$. In these cases, Corollary 3.14 therefore gives all the ideals which are not free over their associated orders. In the case $p = 7$, $e = 3$, $t_1 = 1$, however, $\mathfrak{P}^h$ is free if and only if $h \equiv 0, 1, 5$ or $6 \pmod{7}$, but Theorem 3.13 only tells us that $\mathfrak{P}^h$ is not free if $h \equiv 2 \pmod{7}$.

(ii) Burns [Bu2] has recently obtained necessary and sufficient conditions for the existence of an ideal $\mathfrak{P}^h$ which is free over its associated order $\mathfrak{A}(\mathbb{Q}_p\Gamma; \mathfrak{P}^h)$ in $\mathbb{Q}_p\Gamma$. For a totally ramified abelian p-extension ($p \neq 2$) satisfying (3.11), this occurs if and only if either $t_i = 1$ for all i, or Γ is cyclic and $e = 1$.

(iii) If we relax the restriction that L/K be a p-extension then the associated order will no longer be local, as it will contain the trace idempotent of the maximal subgroup of Γ of order prime to p. We can therefore no longer apply Theorem 2.1 directly. We can however still show that certain ideals are not free over their associated orders. To do so, let F/K be the maximal p-subextension of L/K, and let $\Pi = \mathrm{Gal}(F/K)$. If $\mathfrak{P}^h$ is free over $\mathfrak{A}(K\Gamma; \mathfrak{P}^h)$, then $\mathrm{Tr}_{L/F}(\mathfrak{P}^h)$ is free over its associated order in $K\Pi$, since L/F is at most tamely ramified (cf. [By-L, Lemma 6]). We can then apply Theorem 3.13 to $\mathrm{Tr}_{L/F}(\mathfrak{P}^h)$, noting that if L/F has degree m then $t_i(L/K) = mt_i(F/K)$ for $1 \leq i \leq n$ by [S2, IV Proposition 14]. This could be used to obtain a general criterion that guarantees $\mathfrak{P}^h$ is not free over its associated order, although such a result would be rather cumbersome to formulate.

4. Occurrence of Hopf orders as associated orders

In this section, we investigate the ramification numbers of abelian p-extensions L/K for which the associated order $\mathfrak{A}(K\Gamma; S)$ is a Hopf order in $K\Gamma$.

We endow the group algebra $K\Gamma$ with its usual structure as a Hopf algebra over K. Thus the comultiplication $\Delta\colon K\Gamma \to K\Gamma \otimes_K K\Gamma$, the augmentation $\varepsilon\colon K\Gamma \to K$ and the antipode $\sigma\colon K\Gamma \to K\Gamma$ are the K-linear maps determined by

$$\Delta(\gamma) = \gamma \otimes \gamma, \quad \varepsilon(\gamma) = 1, \quad \sigma(\gamma) = \gamma^{-1} \qquad \text{for } \gamma \in \Gamma.$$

An order $\mathfrak{A}$ in $K\Gamma$ is called a *Hopf order* if these operations make $\mathfrak{A}$ into a Hopf algebra over R. For this, it is sufficient that $\Delta(\mathfrak{A}) \subseteq \mathfrak{A} \otimes_R \mathfrak{A}$, where $\mathfrak{A} \otimes_R \mathfrak{A}$ is identified with a lattice in $K\Gamma \otimes_K K\Gamma$ in the obvious manner,

Let $\mathfrak{A}$ be any Hopf order in $K\Gamma$. Then S is a tame $\mathfrak{A}$-extension of R in the sense of [C] if and only if $\mathfrak{A}$ coincides with the associated order $\mathfrak{A}(K\Gamma; S)$ of S. When this occurs, S is automatically free over $\mathfrak{A}$ (see [C, Theorem 2.1], or, for non-abelian Γ, [C-M, Corollary 1.2]). If moreover the map

$$\xi\colon S \otimes_R S \to \mathrm{Hom}_R(\mathfrak{A}, S), \qquad (\xi(s \otimes t))(\alpha) = s(\alpha t) \quad \text{for } s, t \in S,\ \alpha \in \mathfrak{A}$$

is bijective, then we say that S is a Galois $\mathfrak{A}$-extension of R. If the Hopf order $\mathfrak{A}$ is a local ring then any tame $\mathfrak{A}$-extension is automatically Galois (see [W]; cf. also Theorem 4.4 below).

If S is a Galois $\mathfrak{A}$-extension of R then by [By3, Proposition 2.11], $\mathfrak{D}_{L/K}^{-1} = \mathfrak{g}^{-1}S$ for a certain R-ideal $\mathfrak{g}$, and hence

$$w(L/K) \equiv 0 \pmod{e(L/K)}. \tag{4.1}$$

Furthermore, it is known that the ramification numbers must satisfy certain congruence conditions:

Proposition 4.2. *Let L/K be a totally ramified p-extension with ramification index p^n, and let $\Gamma = \mathrm{Gal}(L/K)$. If S is a Galois extension of R over some Hopf order $\mathfrak{A}$ then*

(i) *$t_i \equiv -1 \pmod{p^i}$ for $1 \leq i \leq n$. In particular, with the notation of Proposition 3.5, $a = p-1$.*

(ii) *If Γ is elementary abelian of order p^n then $t_i \equiv -1 \pmod{p^n}$ for $1 \leq i \leq n$.*

(iii) *If Γ is cyclic of order p^2 then $t_1 \equiv t_2 \equiv -1 \pmod{p^2}$.*

Proof. (i) and (ii) are [By3, Theorem 3 and Corollary 6.3]. For (iii), see [G, remarks after Theorem II.3.2]. □

As noted in [By3], these congruences suggest that, more generally, if S is a Galois extension over a Hopf order then $t_i \equiv -1 \pmod{p^n}$. We shall prove this in Theorem 4.4 below, as a consequence of Corollary 3.12. First, we consider certain Hopf orders which are not local rings.

Proposition 4.3. *Let Γ be a cyclic group of order p^n and let $\mathfrak{A}$ be a Hopf order in $K\Gamma$ containing the trace idempotent*

$$\mathcal{E}_\Gamma = \frac{1}{p^n} \sum_{\gamma \in \Gamma} \gamma.$$

Then $\mathfrak{A}$ is the unique maximal order in $K\Gamma$, and is unramified as an R-algebra. Moreover, the absolute ramification index e of K is divisible by $(p-1)p^{n-1}$.

Proof. Since $\mathcal{E}_\Gamma$ lies in the ideal of integrals of $\mathfrak{A}$, and $\varepsilon(\mathcal{E}_\Gamma) = 1$, it follows as in the proof of [By3, Corollary 1.7] that $\mathfrak{A}$ is an unramified R-algebra. Hence $\mathfrak{A}$ is the unique maximal order in $K\Gamma$. As K-algebras,

$$K\Gamma = \prod_{i=0}^{n} K \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(\zeta_{p^i})$$

where ζ_{p^i} is a primitive p^ith root of unity. Since the maximal order in this algebra is unramified, the maximal order in each component must be unramified. In particular, $K \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(\zeta_{p^n})$ contains an unramified order, so $K(\zeta_{p^n})/K$ must be unramified. Thus $e = e(K/\mathbb{Q}_p)$ is divisible by $e(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) = (p-1)p^{n-1}$. $\square$

Theorem 4.4. *Let L/K be an abelian p-extension with ramification index p^n and Galois group Γ. If $\mathfrak{A} = \mathfrak{A}(K\Gamma; S)$ is a Hopf order then one of the following holds:*

(i) *S is a Galois $\mathfrak{A}$-extension of R, and $t_i \equiv -1 \pmod{p^n}$ for $1 \le i \le n$;*

(ii) *S is not a Galois $\mathfrak{A}$-extension of R, $t_i = \dfrac{p^i e}{p-1} \equiv 0 \pmod{p^n}$ for $1 \le i \le n$, and Γ_1 is cyclic.*

Proof. If S is a Galois $\mathfrak{A}$-extension of R and $t_n - \lfloor t_n/p \rfloor < p^{n-1}e$ then (i) holds by (4.1) and Corollary 3.12.

Before dealing with the remaining cases, we show that L/K may be taken to be totally ramified. Let $L_1 = L^{\Gamma_1}$ be the inertia field in L/K, and let S_1 be its valuation ring. Then L/L_1 is totally ramified of degree p^n, with Galois group Γ_1, and L/L_1 has the same ramification numbers $t_1, \ldots, t_n$ as L/K. Let $\mathfrak{A}_1 = S_1 \otimes_R (\mathfrak{A} \cap K\Gamma_1)$. Then $\mathfrak{A}_1$ is a Hopf order in $L_1\Gamma_1$. Our assumption is that S is a tame $\mathfrak{A}$-extension of R, and this implies that S is also a tame $\mathfrak{A}_1$-extension of S_1 (see [By3, Remark 5.4]). Moreover, by [By3, Theorem 2], S is a Galois $\mathfrak{A}$-extension of R if and only if it is a Galois $\mathfrak{A}_1$-extension of S_1. Thus K may be replaced by L_1, so there is no loss of generality in assuming that L/K is totally ramified.

We next show that (i) again holds when S is a Galois $\mathfrak{A}$-extension of R but $t_n - \lfloor t_n/p \rfloor = p^{n-1}e$. Here $a = p - 1$ by Proposition 4.2(i), so

$$t_n = \frac{p^n e - a}{p-1} = \frac{p^n e}{p-1} - 1$$

by Proposition 3.7. Moreover, one of (3.7)(i), (3.7)(ii) holds.

We claim that (3.7)(ii) cannot hold. This is clear if $n = 1$. If $n > 1$ then, since L/K is totally ramified, it has a normal subextension L'/K of degree p^2 with ramification numbers t_1, t_2. Let $\Gamma' = \mathrm{Gal}(L'/K)$. The valuation ring S' of L' is a Galois $\mathfrak{A}'$-extension of R, where the Hopf order $\mathfrak{A}'$ is the image of $\mathfrak{A}$ in $K\Gamma'$ (see [By3, Lemma 4.5]). As Γ' has order p^2, it is either elementary abelian or cyclic of order p^2. Thus $t_1 \equiv -1 \pmod{p^2}$ by Proposition 4.2(ii) or (iii). Hence $t_1 \ne 1$, and 3.7(ii) does not hold, as claimed.

We are therefore in the case 3.7(i). Since $\mathrm{Tr}_{L/K}(S) = p^n R$, it follows that $\mathcal{E}_\Gamma$ is in $\mathfrak{A}$, so $e \equiv 0 \pmod{(p-1)p^{n-1}}$ by Proposition 4.3. Thus for $1 \leq i \leq n$ we have

$$t_i = \frac{p^i e}{p-1} - 1 \equiv -1 \pmod{p^n}$$

and (i) holds.

Finally, we consider the case where S is not Galois. Since L/K is totally ramified, [By3, Theorem 5] gives all the assertions of (ii) except for $t_i \equiv 0 \pmod{p^n}$. The same result shows that $\mathfrak{A}$ is the maximal order in $K\Gamma$. This implies that the trace idempotent $\mathcal{E}_\Gamma$ again lies in $\mathfrak{A}$, so by Proposition 4.3 we have $e \equiv 0 \pmod{(p-1)p^{n-1}}$, and hence $t_i \equiv 0 \pmod{p^n}$. $\square$

Now (3.11) fails in case (ii) of Theorem 4.4, so Theorem 4.4 and Corollary 3.14(iii) together give

COROLLARY 4.5. *Let L/K be an abelian p-extension for which (3.11) holds, and suppose that $\mathfrak{A} = \mathfrak{A}(K\Gamma; S)$ is a Hopf order. Then a fractional S-ideal $\mathfrak{P}^h$ cannot be free over $\mathfrak{A}(K\Gamma; \mathfrak{P}^h)$ unless either $h \equiv 0 \pmod{p}$ or $h \equiv -1 \pmod{p^n}$.* $\square$

5. LUBIN-TATE EXTENSIONS

Let k be a finite extension of $\mathbb{Q}_p$, and let $\mathfrak{o}$ be its valuation ring. Let π be a fixed generator of the maximal ideal in $\mathfrak{o}$, and let $q = p^f$ be the cardinality of the residue field $\mathfrak{o}/\pi\mathfrak{o}$. A formal power series $f(X) \in \mathfrak{o}[[X]]$ is a *Lubin-Tate series* associated to k and π if it satisfies the two conditions

$$f(X) \equiv \pi X \pmod{X^2 \mathfrak{o}[[X]]}, \qquad f(X) \equiv X^q \pmod{\pi \mathfrak{o}[[X]]}.$$

By standard theory, as given for example in [S1], there is then a unique 1-dimensional formal group F over $\mathfrak{o}$ with $f(X)$ as an endomorphism. The endomorphism ring $\mathrm{End}(F)$ of F is canonically isomorphic to $\mathfrak{o}$, and, writing $[a](X) \in \mathfrak{o}[[X]]$ for the endomorphism corresponding to $a \in \mathfrak{o}$, we have $[\pi](X) = f(X)$.

Let k^c be a fixed algebraic closure of k, and let $\mathfrak{p}^c$ be the maximal ideal of its valuation ring. For $n \geq 0$, let $G_n = \ker[\pi^n] = \{x \in \mathfrak{p}^c \mid [\pi^n](x) = 0\}$. Then G_n is an $\mathfrak{o}$-module, where addition is via the formal group F, and where $a \in \mathfrak{o}$ acts via $[a](X)$. For $n \geq 1$, let k_n be the field obtained by adjoining all elements of G_n to k, and let $\mathfrak{o}_n$ be the valuation ring of k_n.

Then k_n is a totally ramified abelian extension of k of degree $(q-1)q^{n-1}$, and any element of $G_n \backslash G_{n-1}$ generates the maximal ideal of $\mathfrak{o}_n$. The isomorphism between $\mathfrak{o}$ and $\mathrm{End}(F)$ induces an isomorphism between $(\mathfrak{o}/(1+\pi^n\mathfrak{o}))^\times$ and $\mathrm{Gal}(k_n/k)$.

In this section, we consider extensions L/K obtained by taking $K = k_r$ and $L = k_{m+r}$ for integers $r, m \geq 1$. Here we have $\Gamma = \mathrm{Gal}(L/K) \cong U_k^r/U_k^{m+r}$, where U_k^n denotes the subgroup $1+\pi^n\mathfrak{o}$ of the units of k. In the case $m \leq r$, Taylor [T1] determined the associated order $\mathfrak{A} = \mathfrak{A}(K\Gamma, S)$ of the valuation ring S of L, and showed that S is free over $\mathfrak{A}$. In fact, $\mathfrak{A}$ is a Hopf order (see [T2]). In the case $m > r$, Chan and Lim [C-L] showed that S is again free over its associated order when $k = \mathbb{Q}_p$. We now show that these are the only cases where S is free:

Theorem 5.1. *Let $K = k_r$, $L = k_{m+r}$ and $\Gamma = \mathrm{Gal}(L/K)$ be as above. If $m > r$ and $k \neq \mathbb{Q}_p$ then the valuation ring S of L is not free over its associated order in $K\Gamma$.*

Proof. The extension L/K is totally ramified of degree $q^m = p^{fm}$. We first determine its ramification numbers. It follows from [S1, p. 156] that, in the isomorphism between Γ and U_k^r/U_k^{m+r}, the ramification subgroup Γ_j corresponds to $(U_k^r \cap U_k^s)U_k^{m+r}/U_k^{m+r}$ if $q^{s-1}-1 < j \leq q^s - 1$. Hence the ramification numbers t_i of L/K are given by

$$\begin{array}{ccccc} t_1 & = \ldots = & t_f & = & q^r - 1, \\ t_{f+1} & = \ldots = & t_{2f} & = & q^{r+1}-1, \\ \vdots & & \vdots & & \vdots \\ t_{(m-1)f+1} & = \ldots = & t_{mf} & = & q^{r+m-1}-1. \end{array}$$

By (3.4) we have $\mathfrak{D}_{L/K}^{-1} = \mathfrak{P}^{-w}$ where

$$\begin{aligned} w &= (t_1+1)(q^m-1) + \sum_{i=1}^{m-1}(t_{if+1}-t_{if})(q^{m-i}-1) \\ &= q^r(q^m-1) + \sum_{i=1}^{m-1}(q-1)q^{r+i-1}(q^{m-i}-1) \\ &= (q-1)mq^{m+r-1}. \end{aligned}$$

As $r \geq 1$, we conclude that $w \equiv 0 \pmod{q^m}$. Also $t_1 = q^r - 1 \not\equiv -1 \pmod{q^m}$ since $m > r$ by hypothesis. Corollary 3.12 then shows that S is not free over its associated order, provided that (3.11) holds, i.e. that

$$t_{mf} - \left\lfloor \frac{t_{mf}}{p} \right\rfloor < p^{f-1} q^{m-1} e. \tag{5.2}$$

It remains to verify that (5.2) holds whenever $k \neq \mathbb{Q}_p$. Since $t_{mf} = q^{r+m-1} - 1$ and $e = e(K/\mathbb{Q}_p) = (q-1)q^{r-1}e(k/\mathbb{Q}_p)$, we may rewrite (5.2) as

$$(p-1)p^{f-1}q^{r+m-2} < p^{f-1}q^{m+r-2}(q-1)e(k/\mathbb{Q}_p),$$

which simplifies to $p - 1 < (q-1)e(k/\mathbb{Q}_p)$. Clearly this inequality holds unless $q = p$ and $e(k/\mathbb{Q}_p) = 1$, and these last two conditions together imply that $k = \mathbb{Q}_p$. $\square$

Remarks. (i) As $t_1 \not\equiv 0, -1 \pmod{q^m}$ for $m > r$, it follows from Theorem 4.4 that the associated order is not a Hopf order, even in the case $k = \mathbb{Q}_p$.

(ii) The proof of Theorem 5.1 gives very little information about the associated order. In [By5] we determine the associated order explicitly in the case $r = 1$, $m = 2$, under the hypothesis $e > q^2$.

6. Comparing Hopf Galois structures

In this final section, we consider the implications of Theorem 5.1 for the integral module structure in field extensions admitting more than one Hopf Galois structure. If L/K is any finite extension of fields which is normal and separable, then of course L is a Hopf Galois extension of K over the group algebra $K\Gamma$ of $\Gamma = \mathrm{Gal}(L/K)$. Greither and Pareigis [G-P] investigated when, given a finite separable field extension L/K, there exists a Hopf algebra H making L into a Hopf Galois extension of K. If this occurs, then L is necessarily a free H-module of rank 1. Some, but not all, non-normal extensions admit a Hopf Galois structure. It is common for a given extension to have more than one Hopf Galois structure, corresponding to different Hopf algebras H. Indeed, it is shown in [By4] that if L/K is normal of degree n, and if $(n, \phi(n)) > 1$ (where ϕ is the Euler totient function), then there are always non-classical Hopf Galois structures admitted by L/K, in addition to the classical one corresponding to $H = K\Gamma$.

Now let K again be a finite extension of $\mathbb{Q}_p$. If L/K admits more than one Hopf Galois structure, we may consider the integral module structure for each of the corresponding Hopf algebras. The valuation ring S of L has an associated order in each of these Hopf algebras. Just as in the classical case, this might or might not turn out to be a Hopf order. The question then arises as to how the integral module structures for the different Hopf algebras are related.

This was briefly considered by Childs and Moss [C-M], who investigated the non-normal extension $\mathbb{Q}_2(\sqrt[4]{2})/\mathbb{Q}_2$. Here there are precisely two Hopf Galois structures. Both Hopf algebras are commutative and cocommutative. In the first Hopf Galois structure, the associated order of the valuation ring $S = \mathbb{Z}_2[\sqrt[4]{2}]$ is a Hopf order, while in the second it is not. Both associated orders are, however, maximal orders, and S is free over its associated order in both structures.

The extensions k_{m+r}/k_r of the previous section provide a large family of examples where we can compare Hopf Galois structures at integral level. One Hopf Galois structure on k_{m+r}/k_r is the classical one, and for $m > r$ the behaviour of S in this structure is given by Theorem 5.1. The same extension k_{m+r}/k_r can also be endowed with a Hopf Galois structure by means of the Kummer theory of formal groups, as developed in [C-M, §3].

We resume the notation of the previous section, so in particular $K = k_m$ and $L = k_{m+r}$. Let $\omega_r \in G_r \backslash G_{r-1}$, and let ω_{m+r} be any zero of $[\pi^m](X) - \omega_r$. Then $\omega_{m+r} \in G_{m+r} \backslash G_{m+r-1}$, and ω_r (respectively, ω_{m+r}) generates the maximal ideal of $R = \mathfrak{o}_r$ (respectively, of $S = \mathfrak{o}_{m+r}$). Now G_m is the kernel of the formal group homomorphism $[\pi^m] : F \to F$ defined over R (in fact, defined over $\mathfrak{o}$). It follows by [C-M, Theorems 3.5 and 3.1] that S is free, and indeed is a Galois extension, over some Hopf order $\mathfrak{A}$. The dual Hopf order to $\mathfrak{A}$ is $\mathfrak{o}[[X]]/([\pi^n](X))$, which may be viewed as a Hopf order in the Hopf algebra $\mathrm{Map}_{\Omega_K}(G_m, k^c)$ of functions from G_m to k^c respecting the action of the absolute Galois group $\Omega_K = \mathrm{Gal}(k^c/K)$ of K. Thus $\mathfrak{A}$ itself is a Hopf order in a form of the group algebra kG_m, namely in the Hopf algebra $(k^c G_m)^{\Omega_K}$ of fixed points in $k^c G_m$ under Ω_K (acting simultaneously on k^c and G_m).

If $m \le r$ we may identify Γ with G_m via the Kummer isomorphism

$$\gamma \mapsto \omega_{m+r}^{\gamma} -_F \omega_{m+r} \in G_m \qquad \text{for } \gamma \in \Gamma.$$

where $-_F$ denotes subtraction in the formal group F. In this case we also have $G_m \subset K$, so $\mathfrak{A}$ can be viewed as a Hopf order in $K\Gamma$. Thus for $m \le r$, the Kummer theory approach specialises to the classical situation, and we recover the freeness assertion of Taylor's result [T1].

If $m > r$, however, then $G_m \not\subset K$ and we obtain a new Hopf Galois structure in which the integral module structure exhibits better behaviour than in the classical case. We summarise the above discussion, along with Theorem 5.1, in our final result:

Theorem 6.1. *Let k be a finite extension of $\mathbb{Q}_p$, let $m > r \geq 1$, let $K = k_r$ and $L = k_{m+r}$ be the corresponding division fields for a Lubin-Tate series for k, and let $\Gamma = \mathrm{Gal}(L/K)$. In the classical Hopf Galois structure for L/K, corresponding to the Hopf algebra $H_1 = K\Gamma$, the associated order $\mathfrak{A}_1$ of the valuation ring S of L is not a Hopf order, and if $k \neq \mathbb{Q}_p$ then S is not free over $\mathfrak{A}_1$. The extension L/K also admits another Hopf Galois structure, corresponding to the Hopf algebra $H_2 = (k^c G_m)^{\Omega_K}$, in which the associated order $\mathfrak{A}_2$ of S is a Hopf order. In this structure, S is a Galois $\mathfrak{A}_2$-extension of the valuation ring R of K, and S is a free $\mathfrak{A}_2$-module of rank 1.* $\square$

References

[Be] A.-M. Bergé, *Arithmétique d'une extension galoisienne à groupe d'inertie cyclique*, Ann. Inst. Fourier, Grenoble **28** (1978), 17–44.

[B-F] F. Bertrandias and M.-J. Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sc. Paris **274** (1972), A1330–A1333.

[Bl-Bu] W. Bley and D. Burns, *Über arithmetische assoziierte Ordnungen*, J. Number Theory **58** (1996), 361–387.

[Bu1] D. Burns, *Factorisability and wildly ramified Galois extensions*, Ann. Inst. Fourier, Grenoble **41** (1991), 393–430.

[Bu2] D. Burns, *On the equivariant structure of ideals in Galois extensions of fields*, Preprint, King's College London (1996).

[By1] N. P. Byott, *Some self-dual rings of integers not free over their associated orders*, Math. Proc. Camb. Phil. Soc. **110** (1991), 5–10; *Corrigendum* **116** (1994), 569.

[By2] N. Byott, *On Galois isomorphisms between ideals in extensions of local fields*, Manuscripta Math. **73** (1991), 289–311.

[By3] N. P. Byott, *Tame and Galois extensions with respect to Hopf orders*, Math. Z. **220** (1995), 495–522.

[By4] N. P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Alg. **24** (1996), 3217–3228; *Corrigendum* **24** (1996), 3705.

[By5] N. P. Byott, *Associated orders of certain extensions arising from Lubin-Tate formal groups*, to appear in J. de Théorie des Nombres de Bordeaux.

[By-L] N. P. Byott and G. Lettl, *Relative Galois module structure of integers in abelian fields*, J. de Théorie des Nombres de Bordeaux **8** (1996), 125–141.

[C-L] S.-P. Chan and C.-H. Lim, *The associated orders of rings of integers in Lubin-Tate division fields over the p-adic number field*, Ill. J. Math. **39** (1995), 30–38.

[C] L. N. Childs, *Taming wild extensions with Hopf algebras*, Trans. Am. Math. Soc. **304** (1987), 111–140.

[C-M] L. N. Childs and D. J. Moss, *Hopf algebras and local Galois module theory*, in Advances in Hopf Algebras, Lect. Notes Pure and Appl. Math. Series, Vol. 158 (J. Bergen and S. Montgomery, eds.), Dekker, 1994, pp. 1–14.

[E] G. G. Elder, *Galois module structure of ideals in wildly ramified cyclic extensions of degree p^2*, Ann. Inst. Fourier, Grenoble **45** (1995), 625–647.

[E-M] G. G. Elder and M. L. Madan, *Galois module structure of the integers in wildly ramified cyclic extensions*, J. Number Theory **47** (1994), 138–174.

[F] M.-J. Ferton, *Sur les idéaux d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Paris **276** (1973), A1483–A1486.

[G] C. Greither, *Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring*, Math. Z. **210** (1992), 37–67.

[G-P] C. Greither and B. Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), 239–258.

[L] H.-W. Leopoldt, *Uber die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. reine u. angew. Math. **201** (1959), 119–149.

[RC-VS-M] M. Rzedowski Calderón, G. D. Villa Salvador and M. L. Madan, *Galois module structure of rings of integers*, Math. Z. **204** (1990), 401–424.

[S1] J.-P. Serre, *Local Class Field Theory*, in Algebraic Number Theory (J.W.S. Cassels and A. Fröhlich, eds.), Academic Press, 1967.

[S2] J.-P. Serre, *Local fields* (Graduate Texts in Mathematics, Vol. 67), Springer, 1979.

[T1] M. J. Taylor, *Formal groups and the Galois module structure of local rings of integers*, J. reine angew. Math. **358** (1985), 97–103.

[T2] M. J. Taylor, *Hopf structure and the Kummer theory of formal groups*, J. reine angew. Math. **375/376** (1987), 1–11.

[U] S. Ullom, *Integral normal bases in Galois extensions of local fields*, Nagoya Math. J. **39** (1970), 141–148.

[V1] S. V. Vostokov, *Ideals of an abelian p-extension of an irregular local field as Galois modules*, Zap. Nauchn. Sem. Lening. Otdel. Math. Inst. Steklov. (LOMI) **46** (1974), 14–35; English transl. in J. Soviet Math. **9** (1978), 299–317.

[V2] S. V. Vostokov, *Ideals of an abelian p-extension of a local field as Galois module*, Zap. Nauchn. Sem. Lening. Otdel. Math. Inst. Steklov. (LOMI) **57** (1976), 64–84; English transl. in J. Soviet Math. **11** (1979), 567–584.

[W] W. C. Waterhouse, *Normal basis implies Galois for coconnected Hopf algebras*, Preprint, Pennsylvania State University (1992).

Nigel P. Byott
Department of Mathematics
University of Exeter, North Park Road
Exeter EX4 4QE, UK
email: NPByott@maths.exeter.ac.uk