JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Nigel P. BYOTT

A valuation criterion for normal basis generators of Hopf-Galois extensions in characteristic p

Tome 23, n$^{\text{o}}$ 1 (2011), p. 59-70.

<http://jtnb.cedram.org/item?id=JTNB_2011__23_1_59_0>

Journal de Théorie des Nombres
de Bordeaux **23** (2011), 59-70

A valuation criterion for normal basis generators of Hopf-Galois extensions in characteristic p

par Nigel P. BYOTT

Résumé. Soit S/R une extension finie d'anneaux de valuation discrète de caractéristique $p > 0$, et supposons que l'extension correspondante L/K des corps de fractions soit séparable et H-Galoisienne pour une K-algèbre de Hopf H. Soit $\mathcal{D}_{S/R}$ la différente de S/R. Nous montrons que si S/R est totalement ramifiée et que son degré n est une puissance de p alors tout élément ρ de L avec $v_L(\rho) \equiv -v_L(\mathcal{D}_{S/R}) - 1 \pmod{n}$ engendre L comme H-module. Ce critère est le meilleur possible. Ces résultats généralisent à la situation Hopf-Galoisienne un travail récent de G. G. Elder pour les extensions Galoisiennes.

Abstract. Let S/R be a finite extension of discrete valuation rings of characteristic $p > 0$, and suppose that the corresponding extension L/K of fields of fractions is separable and is H-Galois for some K-Hopf algebra H. Let $\mathcal{D}_{S/R}$ be the different of S/R. We show that if S/R is totally ramified and its degree n is a power of p, then any element ρ of L with $v_L(\rho) \equiv -v_L(\mathcal{D}_{S/R}) - 1 \pmod{n}$ generates L as an H-module. This criterion is best possible. These results generalise to the Hopf-Galois situation recent work of G. G. Elder for Galois extensions.

1. Introduction

Let L/K be a finite Galois extension of fields with Galois group $G = \mathrm{Gal}(L/K)$. The Normal Basis Theorem asserts that there is an element ρ of L whose Galois conjugates $\{\sigma(\rho) \mid \sigma \in G\}$ form a basis for the K-vector space L. Equivalently, L is a free module of rank 1 over the group algebra $K[G]$ with generator ρ. Such an element ρ is called a normal basis generator for L/K. The question then arises whether there is a simple condition on elements ρ of L which guarantees that ρ is a normal basis generator. Specifically, suppose that L is equipped with a discrete valuation v_L. (Throughout, whenever we consider a discrete valuation v_F on a field F, we assume it is normalised so that $v_F(F) = \mathbb{Z} \cup \{\infty\}$.) We may then ask whether there exists an integer b such that any $\rho \in L$ with $v_L(\rho) = b$

Mots clefs. Normal basis, Hopf-Galois extensions, local fields.
Classification math.. 11S15.

is automatically a normal basis generator for L/K. We shall refer to any such b as an *integer certificate* for normal basis generators of L/K. In the case that K has characteristic $p > 0$, and is complete with perfect residue field, this question was recently settled by G. Elder [4]. His result can be stated as follows:

Theorem 1 (Elder)**.** *Let K be a field of characteristic $p > 0$, complete with respect to the discrete valuation v_K, and with perfect residue field. Let L be a finite Galois extension of K of degree n with Galois group $G = \mathrm{Gal}(L/K)$, let $w = v_L(\mathcal{D}_{L/K})$, where $\mathcal{D}_{L/K}$ denotes the different of L/K and v_L is the valuation on L, and let $b \in \mathbb{Z}$.*

(a) *If L/K is totally ramified, n is a power of p, and $b \equiv -w - 1 \pmod{n}$, then every $\rho \in L$ with $v_L(\rho) = b$ is a normal basis generator for L/K.*

(b) *The result of (a) is best possible in the sense that, if*
 (i) *n is not a power of p, or*
 (ii) *L/K is not totally ramified, or*
 (iii) *$b \not\equiv -w - 1 \pmod{n}$,*
then there is some $\rho \in L$ with $v_L(\rho) = b$ such that ρ is not *a normal basis generator for L/K*

The purpose of this paper is to show that Theorem 1, suitably interpreted, applies not just in the setting of classical Galois theory, but also in the setting of Hopf-Galois theory for separable field extensions, as developed by C. Greither and B. Pareigis [5]. A finite separable field extension L/K is said to be H-Galois, where H is a Hopf algebra over K, if L is an H-module algebra and the map $H \longrightarrow \mathrm{End}_K(L)$ defining the action of H on L extends to an L-linear isomorphism $L \otimes_K H \longrightarrow \mathrm{End}_K(L)$. A Hopf-Galois structure on L/K consists of a K-Hopf algebra H and an action of H on L so that L is H-Galois. This generalises the classical notion of Galois extension: if L/K is a finite Galois extension of fields with Galois group G, we can take H to be the group algebra $K[G]$ with its standard Hopf algebra structure and its natural action on L, and then L/K is H-Galois. A Galois extension may, however, admit many other Hopf-Galois structures in addition to this classical one, and many (but not all) separable extensions which are not Galois nevertheless admit one or more Hopf-Galois structures. Moreover, if L is H-Galois, then L is a free H-module of rank 1 (see the proof of [3, (2.16)]), and, by analogy with the classical case, we will shall refer to any free generator of the H-module L as a normal basis generator for L/K with respect to H. Our main result is that Theorem 1 holds in this more general setting:

Theorem 2. *Let S/R be a finite extension of discrete valuation rings of characteristic $p > 0$, and let L/K be the corresponding extension of fields of fractions. Let $n = [L : K]$, let v_L be the valuation on L associated to S, and let $w = v_L(\mathcal{D}_{S/R})$ where $\mathcal{D}_{S/R}$ denotes the different of S/R. Suppose that L/K is separable, and is H-Galois for some K-Hopf algebra H. Let $b \in \mathbb{Z}$.*

(a) *If L/K is totally ramified, n is a power of p, and $b \equiv -w - 1 \pmod{n}$, then every $\rho \in L$ with $v_L(\rho) = b$ is a normal basis generator for L/K with respect to H.*

(b) *The result of (a) is best possible in the sense that, if*

  (i) *n is not a power of p, or*

  (ii) *L/K is not totally ramified, or*

  (iii) *$b \not\equiv -w - 1 \pmod{n}$,*

  then there is some $\rho \in L$ with $v_L(\rho) = b$ such that ρ is not *a normal basis generator for L/K with respect to H.*

In Theorem 2, we do not require K to be complete with respect to the valuation v_K on K associated to R, and we do not require the residue field of R to be perfect. Thus, even in the case of Galois extensions (in the classical sense), Theorem 2 is slightly stronger than Theorem 1.

We recall that the different $\mathcal{D}_{S/R}$ is defined as the fractional S-ideal such that

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

where $\mathrm{Tr}_{L/K}$ is the trace from L to K. In the case that S/R is totally ramified and L/K is separable, let $p(X) \in R[X]$ be the minimal polynomial over R of a uniformiser Π of S. Then $\mathcal{D}_{S/R}$ is generated by $p'(\Pi)$, where $p'(T)$ denotes the derivative of $p(T)$ [6, III, Cor. 2 to Lemma 2]. (This does not require L/K to be Galois, or the residue field of K to be perfect.) The formulation of Theorem 1(a) in [4] is in terms of $p'(\Pi)$.

If S (and hence L) is complete with respect to v_L, then $\mathcal{D}_{S/R}$ is the same as the different $\mathcal{D}_{L/K}$ of the extension L/K of valued fields occurring in Theorem 1. Theorem 2 also applies, however, if K is a global function field of dimension 1 over an arbitrary field k of characteristic p. In particular, if L is an H-Galois extension of K of p-power degree, and some place $\mathfrak{p}$ of K is totally ramified in L/K, then Theorem 2(a) gives an integer certificate for normal basis generators of L/K with respect to H, in terms of the valuation v_L on L corresponding to the unique place $\mathfrak{P}$ of L above $\mathfrak{p}$ and the $\mathfrak{P}$-part of $\mathcal{D}_{L/K}$. If, on the other hand, there is more than one place $\mathfrak{P}$ of L above $\mathfrak{p}$, then the integral closure of R in L is the intersection S_0 of the corresponding valuation rings S of L [8, III.3.5]. Any one such S strictly contains S_0 and is therefore not integral over R. In particular, S is not finite over R and Theorem 2 does not apply in this case.

We briefly recall the background to the above results. In the (characteristic 0) situation where K is a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers, the author and Elder [2] showed the existence of integer certificates for normal basis generators in totally ramified elementary abelian extensions L/K, under the assumption that L/K contains no maximally ramified subfield. This assumption is necessary, since there can be no integer certificate in the case $L = K(\sqrt[p]{\pi})$ with $v_K(\pi) = 1$: indeed, for any $b \in \mathbb{Z}$, the element $\pi^{b/p}$ has valuation b but is not a normal basis generator. (Here K must contain a primitive pth root of unity for L/K to be Galois.) We also raised the question of whether the corresponding result held in characteristic $p > 0$, where the exceptional situation of maximal ramification cannot arise. Our question was answered by L. Thomas [9], who observed that general properties of group algebras of p-groups in characteristic p allow an elegant derivation of integer certificates for arbitrary finite abelian p-groups G. Her result was expressed in terms of the last break in the sequence of ramification groups of L/K, but is equivalent to Theorem 1 for totally ramified abelian p-extensions G. Finally, Elder [4] removed the hypothesis that G is abelian by expressing the result in terms of the valuation of the different, and also gave the converse result that no integer certificate exists if L/K is not totally ramified or is not a p-extension.

We end this introduction by outlining the structure of the paper. In §2, we review the facts we shall need from Hopf-Galois theory, and prove several preliminary results in the case of p-extensions. These show, in effect, that the relevant Hopf algebras behave similarly to the group algebras considered in [9]. In §3 we develop some machinery to handle extensions whose degrees are not powers of p. In [4], such extensions were treated by reducing to a totally and tamely ramified extension. For Hopf-Galois extensions, it is not clear whether such a reduction is always possible. (Indeed, while a totally ramified Galois extension of local fields is always soluble, the author does not know of any reason why such an extension could not admit a Hopf-Galois structure in which the associated group N, as in §2 below, is insoluble.) We therefore adopt a different approach, using a small part of the theory of modular representations. We complete the proof of Theorem 2 in §4. The ramification groups, which play an essential role in the arguments of [4] and [9], are not available in the Hopf-Galois setting, but their use can be avoided by working directly with the inverse different. Finally, in §5, we give an example of a family of extensions which are not Galois, but to which Theorem 2 applies.

2. Hopf-Galois theory for p-extensions in characteristic p

In this section, we briefly recall the description of Hopf-Galois structures on a finite separable field extension L/K, and note some properties of the

Hopf algebras H which arise when $[L : K]$ is a power of $p = \mathrm{char}(K)$. We do not make any use of valuations on K and L in this section.

Let E be a (finite or infinite) Galois extension of K containing L. Set $G = \mathrm{Gal}(E/K)$ and $G' = \mathrm{Gal}(E/L)$, and let $X = G/G'$ be the set of left cosets gG' of G' in G. Then G acts by left multiplication on X, giving a homomorphism $G \longrightarrow \mathrm{Perm}(X)$ into the group of permutations of X. The main result of [5] can be stated as follows: the Hopf-Galois structures on L/K (up to the appropriate notion of isomorphism) correspond bijectively to the regular subgroups N of $\mathrm{Perm}(X)$ which are normalised by G. In the Hopf-Galois structure corresponding to N, the Hopf algebra acting on L is $H = E[N]^G$, the fixed point algebra of the group algebra $E[N]$ under the action of G simultaneously on E (as field automorphisms) and on N (by conjugation inside $\mathrm{Perm}(X)$). The Hopf algebra operations on H are the restrictions of the standard operations on $E[N]$. We write 1_X for the trivial coset G' in X. Then there is a bijection between elements η of N and K-embeddings $\sigma \colon L \longrightarrow E$, given by $\eta \mapsto \sigma_\eta$ where $\sigma_\eta(\rho) = g(\rho)$ with $\eta^{-1}(1_X) = gG'$. The action of H on L can be described explicitly as follows (see e.g. [1, p. 338]):

$$\left(\sum_{\eta \in N} \lambda_\eta \eta\right)(\rho) = \sum_{\eta \in N} \lambda_\eta \sigma_\eta(\rho) \text{ for } \sum_{\eta \in N} \lambda_\eta \eta \in H \text{ and } \rho \in L. \tag{2.1}$$

Remark. In [5], E is taken to be the the Galois closure E_0 of L over K. In this case, the action of G on X is faithful. However, it is clear that one may take a larger field E as above: all that changes is that G need no longer act faithfully on X. (Indeed, the action of G on both X and L factors through $\mathrm{Gal}(E/E_0)$.) In the proof of Lemma 3.1 below, it will be convenient to take E to be a finite extension of E_0.

Let L/K be H-Galois, where the Hopf algebra H corresponds to N as above. We define

$$t_H = \sum_{\eta \in N} \eta \in E[N].$$

We now show that t_H behaves like the trace element in a group algebra:

Proposition 2.1. *We have $t_H \in H$ and, for any $h \in H$,*

$$h t_H = t_H h = \epsilon(h) t_H,$$

where $\epsilon \colon H \to K$ is the augmentation. In particular, writing I_H for the augmentation ideal $\ker \epsilon$ *of H, we have*

$$I_H t_H = t_H I_H = 0.$$

Also, $t_H(\rho) = \mathrm{Tr}_{L/K}(\rho)$ for any $\rho \in L$.

Proof. Since N is normalised by G, each $g \in G$ permutes the elements of N. Hence $t_H \in E[N]^G = H$. For any $h = \sum_{\nu \in N} \lambda_\nu \nu \in H$, we have

$$ht_H = \sum_{\nu,\eta} \lambda_\nu \nu \eta = \left(\sum_\nu \lambda_\nu \right) \left(\sum_\eta \eta \right) = \epsilon(h) t_H.$$

In particular, if $h \in I_H$ then $ht_H = \epsilon(h)t_H = 0$, so $I_H t_H = 0$. Similarly $t_H h = \epsilon(h) t_H$ and $t_H I_H = 0$. Finally, for $\rho \in L$ we have

$$t_H(\rho) = \sum_{\eta \in N} \sigma_\eta(\rho) = \mathrm{Tr}_{L/K}(\rho).$$

□

Remark. Proposition 2.1 shows that $K \cdot t_H$ is the ideal of (left or right) integrals of H.

Corollary 2.2. *If* $\mathrm{Tr}_{L/K}(\rho) = 0$ *then* ρ *cannot be a normal basis generator for* L/K *with respect to* H.

Proof. If ρ is a free generator for L over H, then the annihilator of ρ in H must be trivial. But if $\mathrm{Tr}_{L/K}(\rho) = 0$ then ρ is annihilated by $t_H \neq 0$. □

We next show that [9, Proposition 7] still holds in our setting:

Lemma 2.3. *If* $[L : K] = p^m$ *for some integer* m, *then any* $\rho \in L$ *with* $\mathrm{Tr}_{L/K}(\rho) \neq 0$ *is a normal basis generator for* L/K *with respect to* H.

Proof. We first observe that the augmentation ideal I_H is a nilpotent ideal of H, since $I_H = I_{E[N]} \cap H$ and the augmentation ideal $I_{E[N]}$ of $E[N]$ is a nilpotent ideal of $E[N]$ because $|N| = [L : K] = p^m$. Thus I_H is contained in (and in fact equals) the Jacobson radical J_H of H.

Now consider the H-submodule $M = H \cdot \rho + I_H \cdot L$ of L. Since L is a free H-module of rank 1, and $H/I_H \cong K$, the K-subspace $I_H L$ of L has codimension 1. But $\rho \notin I_H L$ since $\mathrm{Tr}_{L/K}(I_H L) = (t_H I_H) L = 0$ by Proposition 2.1, so $M = L$. Since $I_H \subseteq J_H$, Nakayama's Lemma shows that $H \cdot \rho = L$, and, comparing dimensions over K, we see that ρ is a free generator for the H-module L. □

The next result is immediate from Corollary 2.2 and Lemma 2.3

Corollary 2.4. *If* $[L : K] = p^m$ *then* $\rho \in L$ *is a normal basis generator for* L/K *with respect to* H *if and only if* $\mathrm{Tr}_{L/K}(\rho) \neq 0$. *In particular, the set of normal basis generators is the same for all Hopf-Galois structures on* L/K.

3. The non-p-power case

As in Theorem 2, let S/R be a finite extension of discrete valuation rings, such that the corresponding extension L/K of their fields of fractions is H-Galois for some Hopf algebra H. We do not require S and R to be complete. Let v_L, v_K be the corresponding valuations on L, K.

Lemma 3.1. *Suppose that $[L : K]$ is not a power of p. Then H contains nonzero orthogonal idempotents e_1, e_2 with $e_1 + e_2 = 1$, such that*

$$v_L(e_j\rho) \geq v_L(\rho) \text{ for all } \rho \in L \text{ and } j = 1, 2.$$

Proof. Let $[L : K] = p^m r$ where $m \geq 0$ and where $r \geq 2$ is prime to p. We have $H = E[N]^G$ where $G = \mathrm{Gal}(E/K)$ and, in view of the remark before Proposition 2.1, we may take E to be a finite Galois extension of K, containing L and also containing a primitive rth root of unity ζ_r. Let k' be the algebraic closure in E of the prime subfield $\mathbb{F}_p$. Thus $\zeta_r \in k'$.

Now let t be the number of conjugacy classes in N consisting of elements whose order is prime to p. As $|N| = [L : K]$ is not a power of p, we have $t \geq 2$. For any field F of characteristic p containing ζ_r, the group algebra $A = F[N]$ has exactly t nonisomorphic simple modules [7, §18.2, Corollary 3]. Let J_A denote the Jacobson radical of A. Then the semisimple algebra A/J_A has exactly t Wedderburn components, and therefore has exactly t primitive central idempotents. Since A is a finite-dimensional F-algebra, we may lift these idempotents from A/J_A to A. Thus A has exactly t primitive central idempotents, $\phi_1, \ldots, \phi_t$ say, and hence has t maximal 2-sided ideals. One of these, say the ideal $(1 - \phi_1)A$ associated to ϕ_1, is the augmentation ideal I_A.

Taking $F = k'$ in the previous paragraph, we obtain orthogonal idempotents $\phi_1, \ldots, \phi_t \in k'[N]$. But $k' \subset E$, and taking $F = E$, we find that $\phi_1, \ldots, \phi_t$ are again the primitive central idempotents in $E[N]$. The action of G on $E[N]$ permutes these idempotents, and fixes ϕ_1 since it fixes the augmentation ideal of $E[N]$. Hence $\phi_1 \in H$. Let $e_1 = \phi_1$ and $e_2 = 1 - \phi_1$. Then e_1, e_2 are orthogonal idempotents in $H \cap k'[N]$ with $e_1 + e_2 = 1$. Moreover $e_1 \neq 0$ by definition and $e_2 \neq 0$ since $t \geq 2$.

We now show that $v_L(e_j\rho) \geq v_L(\rho)$ for $j = 1$, 2 and for any $\rho \in L$. Since S/R is finite, S is the unique valuation ring of L containing R. Thus each valuation ring T of E containing R must also contain S. (There may be several such T if R is not complete.) Fix one of these valuation rings T of E, and let v_E be the corresponding valuation on E. Then any valuation v' on E with $v'(\mu) = v_E(\mu)$ for all $\mu \in K$ necessarily satisfies $v'(\rho) = v_E(\rho)$ for all $\rho \in L$. In particular, for each $g \in G$, the valuation $v_E \circ g$ on E must have the same restriction to L as v_E. Thus, for each $\eta \in N$, we have $v_E(\sigma_\eta(\rho)) = v_E(\rho)$ for all $\rho \in L$.

For $j = 1$ or 2, let

$$e_j = \sum_{\eta \in N} \lambda_\eta \eta \quad \text{with } \lambda_\eta \in k'.$$

Then, as $e_j \in H$, we have

$$e_j(\rho) = \sum_{\eta \in N} \lambda_\eta \sigma_\eta(\rho)$$

by (2.1). But λ_η is algebraic over $\mathbb{F}_p$, so either $\lambda_\eta = 0$ or $v_E(\lambda_\eta) = 0$. We then have

$$v_E(e_j \rho) \geq \min_{\eta \in N}(v_E(\lambda_\eta) + v_E(\sigma_\eta(\rho))) \geq 0 + v_E(\rho).$$

As ρ, $e_j\rho \in L$, it follows that $v_L(e_j\rho) \geq v_L(\rho)$ as required. □

We can now prove case (i) of Theorem 2(b).

Corollary 3.2. *Let S/R be as in Theorem 2, and suppose that $[L : K]$ is not a power of p. Then, for any $b \in \mathbb{Z}$, there exists some $\rho \in L$ with $v_L(\rho) = b$ such that ρ is not a normal basis generator for L/K with respect to H.*

Proof. Take any $\rho' \in L$ with $v_L(\rho') = b$. With e_1, $e_2 \in H$ as in Lemma 3.1, we have

$$\rho' = e_1\rho' + e_2\rho', \qquad v_L(e_1\rho') \geq b, \quad v_L(e_2\rho') \geq b.$$

Both inequalities cannot be strict since $v_L(\rho') = b$, so without loss of generality we have $v_L(e_1\rho') = b$. Set $\rho = e_1\rho'$. Then $v_L(\rho) = b$ but ρ cannot be a normal basis generator with respect to H, since $e_2\rho = (e_2e_1)\rho' = 0$. □

4. Proof of Theorem 2

For this section, the hypotheses of Theorem 2 are in force. In particular, S/R is a finite extension of discrete valuation rings of characteristic $p > 0$, and the corresponding extension of fields of fractions L/K is separable of degree n. Also, L/K is H-Galois for some K-Hopf algebra H.

By Corollary 3.2, we may assume that $n = [L : K]$ is a power of p. Let e be the ramification index of S/R, let $w = v_L(\mathcal{D}_{S/R})$, and let π and Π be uniformisers for R and S respectively. By definition of the different, we have

$$\mathrm{Tr}_{L/K}(\Pi^{-w}S) \subseteq R, \qquad \mathrm{Tr}_{L/K}(\Pi^{-w-1}S) \not\subseteq R,$$

and therefore

$$\mathrm{Tr}_{L/K}(\Pi^{e-w}S) \subseteq \pi R, \qquad \mathrm{Tr}_{L/K}(\Pi^{e-w-1}S) = R.$$

Hence there is some $x_1 \in L$ with $v_L(x_1) = e-w-1$ and $\mathrm{Tr}_{L/K}(x_1) = 1$. For $2 \le i \le e$, pick $x'_i \in L$ with $v_L(x'_i) = e-w-i$, and set $x_i = x'_i - \mathrm{Tr}_{L/K}(x'_i)x_1$. Since $\mathrm{Tr}_{L/K}(x'_i) \in R$ and $v_L(x'_i) < v_L(x_1)$, we have

$$(4.1) \qquad v_L(x_i) = e - w - i \text{ for } 1 \le i \le e,$$

and clearly

$$(4.2) \qquad \mathrm{Tr}_{L/K}(x_i) = \begin{cases} 1 & \text{if } i = 1; \\ 0 & \text{otherwise.} \end{cases}$$

We first consider the totally ramified case $e = n$. Then $x_1, \ldots, x_n$ is a K-basis for L, since the $v_L(x_i)$ represent all residue classes modulo n.

Let $\rho \in L$ with $v_L(\rho) \equiv -w-1 \pmod{n}$. We may write

$$\rho = \sum_{i=1}^{n} a_i x_i$$

with the $a_i \in K$. Then $v_L(\rho) = \min_i\{nv_K(a_i) + (n-w-i)\}$. The hypothesis on ρ means that the minimum must occur at $i = 1$. In particular, $a_1 \neq 0$. Then, by (4.2), we have

$$\mathrm{Tr}_{L/K}(\rho) = \sum_{i=1}^{n} a_i \mathrm{Tr}_{L/K}(x_i) = a_1 \neq 0,$$

and by Lemma 2.3, ρ is a normal basis generator for L/K with respect to H. This completes the proof of Theorem 2(a).

Next let $b \in \mathbb{Z}$ with $b \not\equiv -1-w \pmod{n}$. Then $b = n(s+1) - w - i$ with $2 \le i \le n$ and $s \in \mathbb{Z}$. Set $\rho = \pi^s x_i$, so $v_L(\rho) = b$ by (4.1). But $\mathrm{Tr}_{L/K}(\rho) = 0$ by (4.2), so that ρ cannot be a normal basis generator by Corollary 2.2. This completes the proof of Theorem 2 for totally ramified extensions.

Finally, suppose that S/R is not totally ramified. Given $b \in \mathbb{Z}$, write $b = e(s+1) - w - i$ with $1 \le i \le e$ and $s \in \mathbb{Z}$. If $i \neq 1$ then $\rho = \pi^s x_i$ satisfies $v_L(\rho) = b$ and $\mathrm{Tr}_{L/K}(\rho) = 0$, so as before ρ cannot be a normal basis generator. It remains to consider the case $i = 1$. Let l, k be the residue fields of S, R respectively. Then l/k has degree $f > 1$ with $ef = n$. (Note, however, that l/k need not be separable.) Pick $\omega \in l$ with $\omega \notin k$, let $\Omega \in S$ be any element whose image in l is ω, and set

$$\rho = \pi^s(\Omega - \mathrm{Tr}_{L/K}(x_1\Omega))x_1.$$

Then $\mathrm{Tr}_{L/K}(x_1\Omega) \in \mathrm{Tr}_{L/K}(\mathcal{D}_{S/R}^{-1}) \subseteq R$. Since ω and 1 are elements of l which are linearly independent over k, it follows that $v_L(\Omega - \mathrm{Tr}_{L/K}(x_1\Omega)) = v_L(\Omega) = 0$, and hence $v_L(\rho) = es + v_L(x_1) = b$. But once more we have $\mathrm{Tr}_{L/K}(\rho) = 0$, so that ρ cannot be a normal basis generator for L/K with respect to H. This concludes the proof of Theorem 2.

5. An example

We end with an example of a family of extensions L/K which are H-Galois for a suitable Hopf algebra H, but which are not Galois. Theorem 2 will give an integer certificate for normal basis generators in L/K, although Theorem 1 is not applicable.

Fix a prime number p, and let $K = \mathbb{F}_p((T))$ be the field of formal Laurent series over the finite field $\mathbb{F}_p$ of p elements. Then K is complete with respect to the discrete valuation v_K such that $v_K(T) = 1$, and the valuation ring is $R = \mathbb{F}_p[[T]]$. Take any integer $f \geq 2$, and set $q = p^f$. Let $b > 0$ be an integer which is not divisible by p, and let $\alpha \in K$ be any element with $v_K(\alpha) = -b$. The field we consider is $L = K(\theta)$, where θ is a root of the polynomial $g(X) = X^q - X - \alpha \in K[X]$.

To see that L is not Galois over K, consider the unramified extension $F = \mathbb{F}_q K$ of K (where $\mathbb{F}_q$ is the field of q elements), and let $E = LF$. Then E is the splitting field of g over K, and the roots of g in E are $\{\theta+\omega \mid \omega \in \mathbb{F}_q\}$. Thus E is the Galois closure of L/K, and it follows in particular that L/K is not Galois. We are therefore in the situation of §2, with $G = \mathrm{Gal}(E/K)$ of order fq, and with $G' = \mathrm{Gal}(E/L) \cong \mathrm{Gal}(F/K) \cong \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ cyclic of order f. Moreover, G' has a normal complement $N = \mathrm{Gal}(E/F) \cong \mathbb{F}_q$ in G. Thus $G \cong N \rtimes G'$ (and, since $\mathbb{F}_q/\mathbb{F}_p$ has a normal basis, it is easy to see that any generator of G' acts on N with minimal polynomial $X^f - 1$). In the terminology of [5, §4], L/K is an almost classically Galois extension. It therefore admits at least one Hopf-Galois structure, namely that corresponding to the group N.

Now E/F is totally ramified of degree q, and the ramification filtration of $\mathrm{Gal}(E/F)$ has only one break, occurring at b. Hence, by Hilbert's formula [6, IV, Prop. 4], $v_E(\mathcal{D}_{E/F}) = (b+1)(q-1)$. As E/L and F/K are unramified, it follows that L/K is totally ramified, and, using the transitivity of the different [6, III, Prop. 8], that $v_L(\mathcal{D}_{L/K}) = (b+1)(q-1)$. Thus Theorem 2(a) applies with $w \equiv -1-b \pmod{q}$. Hence any $\rho \in L$ with $v_L(\rho) \equiv b \pmod{q}$ is a normal basis generator with respect to *any* Hopf-Galois structure on L/K.

Following a suggestion of the referee, we specialise this example further. Let us take $b = q - 1$ and $\alpha = T^{1-q}$. Then $v_L(\theta) = 1 - q$. We obtain a uniformising parameter for S by seting $\eta = T\theta$. Then η is a root of the Eisenstein polynomial $X^q - T^{q-1}X - T$, so $\mathcal{D}_{L/K}$ is generated by T^{q-1} and $w \equiv 0 \pmod{q}$. Hence any element ρ of L with $v_L(\rho) \equiv -1 \pmod{q}$ is a normal basis generator with respect to any Hopf-Galois structure on L/K. This can easily be verified directly for $\rho = \eta^{q-1}$ and the Hopf-Galois structure corresponding to N as above. Indeed, let σ_ω be the element of $N = \mathrm{Gal}(E/F)$ corresponding to $\omega \in \mathbb{F}_q$, so $\sigma_\omega(\eta) = \eta + \omega T$. We first claim that η^{q-1} is a normal basis generator for the Galois extension E/F, or equivalently, that $F[N] \cdot \eta^{q-1} = E$. We have

$$\sigma_\omega(\eta^{q-1}) = (\eta + \omega T)^{q-1} = \sum_{i=0}^{q-1} \eta^{q-1-i}(-\omega T)^i,$$

so the claim follows from the non-vanishing of the Vandermonde matrix $\left((-\omega)^i\right)_{\omega \in \mathbb{F}_q, 0 \leq i < q}$. Since the $F[N]$-module E is free on the generator η^{q-1}, and $H = F[N]^G$ is a K-subalgebra of $F[N]$, it follows that $H \cdot \eta^{q-1}$ has dimension $\dim_K(H) = q = [L : K]$ over K. But $\eta \in L$ and $H \cdot L = L$, so we must have $H \cdot \eta^{q-1} = L$. Thus η^{q-1} is a normal basis generator for L/K over H, as required.

Remark (Galois extensions)**.** If we apply the preceding construction starting with $\mathbb{F}_q((T))$ rather than $\mathbb{F}_p((T))$ (that is, we just consider the extension E/F above) then we obtain a *Galois* (indeed, abelian) extension of degree q for which we have given a direct verification that η^{q-1} is a normal basis generator. This provides an explict example of the situation considered in [9]

Remark (Global examples)**.** We can easily adapt the above arguments to the case where K is not complete. Let K be a function field of dimension 1 with field of constants $\mathbb{F}_p$, and choose any valuation v_K on K which corresponds to a place of K with residue field $\mathbb{F}_p$. With q, b and α as above, let $L = K(\theta)$ where $\theta^q - \theta = \alpha$. Then the extension L/K has degree q and is a totally ramified at v_K. As before, L/K is not Galois but does admit at least one Hopf-Galois structure, and Theorem 2(a) shows that any $\rho \in L$ with $v_L(\rho) \equiv b \pmod{q}$ is a normal basis generator for L/K with respect to any Hopf-Galois structure on L/K.

References

[1] N. P. Byott, *Integral Hopf-Galois structures on degree p^2 extensions of p-adic fields.* J. Algebra **248** (2002), 334–365.

[2] N. P. Byott and G. G. Elder, *A valuation criterion for normal bases in elementary abelian extensions.* Bull. London Math. Soc. **39** (2007), 705–708.

[3] L. N. Childs, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory.* Mathematical Surveys and Monographs **80**, American Mathematical Society, 2000.

[4] G. G. Elder, *A valuation criterion for normal basis generators in local fields of characteristic p.* Arch. Math. **94** (2010), 43–47.

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

[6] J.-P. Serre, *Local Fields.* Graduate Texts in Mathematics **67**, Springer, 1979.

[7] J.-P. Serre, *Linear Representations of Finite Groups.* Graduate Texts in Mathematics **42**, Springer, 1977.

[8] H. Stichtenoth, *Algebraic Function Fields and Codes.* Springer, 1993.

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

Nigel P. Byott
Mathematics Research Institute
University of Exeter
Harrison Building
North Park Road
Exeter EX4 4QF, UK
E-mail: N.P.Byott@ex.ac.uk