New York Journal of Mathematics

New York J. Math. **17** (2011) 799–810.

Towards a generalisation of Noether's theorem to nonclassical Hopf–Galois structures

Paul J. Truman

Abstract. We study the nonclassical Hopf–Galois module structure of rings of algebraic integers in some extensions of p-adic fields and number fields which are at most tamely ramified. We show that if L/K is an unramified extension of p-adic fields which is H-Galois for some Hopf algebra H then $\mathfrak{O}_L$ is free over its associated order $\mathfrak{A}_H$ in H. If H is commutative, we show that this conclusion remains valid in ramified extensions of p-adic fields if p does not divide the degree of the extension. By combining these results we prove a generalisation of Noether's theorem to nonclassical Hopf–Galois structures on domestic extensions of number fields.

Contents

1. Introduction

Let L/K be a finite Galois extension of number fields or p-adic fields (for some prime number p) with group G, and let $\mathfrak{O}_L$ and $\mathfrak{O}_K$ be the rings of algebraic integers or valuation rings of L and K respectively. By the normal basis theorem, L is a free module of rank one over the group algebra $K[G]$. The ring of algebraic integers (or valuation ring) $\mathfrak{O}_L$ is likewise a module over the integral group ring $\mathfrak{O}_K[G]$, and Noether's theorem identifies when an analogous result holds at integral level: $\mathfrak{O}_L$ is free over $\mathfrak{O}_K[G]$ (for p-adic fields) or *locally free* over $\mathfrak{O}_K[G]$ (for number fields) if and only if L/K is

Received July 29, 2011.

2010 *Mathematics Subject Classification.* 11R33 (primary), 11S23 (secondary).

Key words and phrases. Noether's theorem, Hopf–Galois structures, domestic extensions.

ISSN 1076-9803/2011

at most tamely ramified [6, Theorem 3]. By locally free we mean that for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ the completed ring of integers $\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{O}_{K,\mathfrak{p}} \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$ is free over the completed integral group ring $\mathfrak{O}_{K,\mathfrak{p}}[G] = \mathfrak{O}_{K,\mathfrak{p}} \otimes_{\mathfrak{O}_K} \mathfrak{O}_K[G]$. An approach to studying wildly ramified extensions is to replace the integral group ring with a larger order in $K[G]$, called the associated order:

$$\mathfrak{A}_{K[G]} = \{\alpha \in K[G] \mid \alpha \cdot x \in \mathfrak{O}_L \text{ for all } x \in \mathfrak{O}_L\}.$$

By construction $\mathfrak{A}_{K[G]}$ is the largest order in $K[G]$ for which $\mathfrak{O}_L$ is a module, and it is possible that $\mathfrak{O}_L$ will be a free (or locally free) $\mathfrak{A}_{K[G]}$-module. In the p-adic case Childs [2] provided a sufficient condition for this to occur by exploiting the fact that $K[G]$ is a Hopf algebra — his theorem is that $\mathfrak{O}_L$ is a free $\mathfrak{A}_{K[G]}$-module if the latter is a Hopf order in $K[G]$. The action of the group algebra $K[G]$ on a Galois extension L/K is a special case of the more general concept of a Hopf–Galois structure on a finite separable extension of fields. A given separable extension L/K may admit a number of Hopf–Galois structures, each consisting of a Hopf algebra H such that L is a H-Galois extension of K (for the definition see the following section). If the extension is Galois then it admits at least one Hopf–Galois structure with Hopf algebra $K[G]$, and we call this the classical structure. We call any other Hopf–Galois structures admitted by the extension nonclassical. A theorem of Greither and Pareigis reduces the enumeration of the Hopf–Galois structures admitted by a given extension to a group theoretic problem, and shows that the Hopf algebras all occur as "twisted" forms of certain group algebras. To study the structure of $\mathfrak{O}_L$ relative to the various Hopf–Galois structures admitted by the extension, we define within each Hopf algebra H an associated order:

$$\mathfrak{A}_H = \{h \in H \mid h \cdot x \in \mathfrak{O}_L \text{ for all } x \in \mathfrak{O}_L\}.$$

As with the group algebra $K[G]$, for each Hopf algebra H which gives a Hopf–Galois structure on the extension, $\mathfrak{A}_H$ is the largest order in H for which $\mathfrak{O}_L$ is a module, and in fact $\mathfrak{A}_H$ is the only order in H over which $\mathfrak{O}_L$ can be free (see [4, Proposition 12.5]). Childs's theorem generalises to this context - if L/K is a finite H-Galois extension of p-adic fields and $\mathfrak{A}_H$ is a Hopf order in H then $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module. [4, Theorem 12.7]

The use of nonclassical Hopf–Galois structures has proven to be fruitful in the study of wildly ramified extensions. For example, Byott [1] has exhibited a class of wildly ramified Galois extensions L/K of p-adic fields for which $\mathfrak{O}_L$ is not free over $\mathfrak{A}_{K[G]}$, its associated order in the classical structure with Hopf algebra $K[G]$, but is free over $\mathfrak{A}_H$, its associated order in some Hopf algebra H giving a nonclassical structure on the extension. So from the point of view of describing $\mathfrak{O}_L$, for these extensions the classical structure is not the "correct" structure to use, and a nonclassical structure gives a more satisfactory description of the ring of algebraic integers.

On the other hand, little is known about the nonclassical Hopf–Galois module structure of $\mathfrak{O}_L$ when L/K is a tamely ramified extension. For Galois extensions, Noether's theorem states that in the classical structure with Hopf algebra $K[G]$ we have $\mathfrak{A}_{K[G]} = \mathfrak{O}_K[G]$ and that $\mathfrak{O}_L$ is free (for p-adic fields) or locally free (for number fields) over $\mathfrak{O}_K[G]$, and for number fields results such as the Hilbert–Speiser theorem describe the global structure of $\mathfrak{O}_L$ over $\mathfrak{O}_K[G]$ in certain cases [8]. We might wonder whether analogous results hold for any nonclassical structures admitted by the extension. The purpose of this paper is to address the local question for certain classes of extensions which are at most tamely ramified. In Sections 3 and 4 we prove the following two theorems concerning p-adic fields:

Theorem 1.1. *Let L/K be a finite unramified extension of p-adic fields and let H be a Hopf algebra giving a Hopf–Galois structure on the extension. Then $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.*

Theorem 1.2. *Let L/K be a finite (not necessarily Galois) extension of p-adic fields and let H be a commutative Hopf algebra giving a Hopf–Galois structure on the extension. Suppose that $p \nmid [L : K]$. Then $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.*

In Section 5 we generalise these theorems slightly in order to study completions of extensions of number fields. We call a Galois extension L/K of number fields *domestic* if no prime of $\mathfrak{O}_K$ lying above a prime number dividing $[L : K]$ ramifies in $\mathfrak{O}_L$. By combining these generalized results we obtain the following analogue of Noether's theorem for nonclassical Hopf–Galois structures on domestic extensions:

Theorem 1.3. *Let L/K be a finite domestic extension of number fields and let H be a commutative Hopf algebra giving a Hopf–Galois structure on the extension. Then $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module.*

In all of these cases we find that $\mathfrak{A}_H$ has an explicit description, analogous at integral level to the description of H at field level afforded by the theorem of Greither and Pareigis.

Acknowledgements. This work is based on the author's Ph.D. thesis 'Hopf–Galois Module Structure of Some Tamely Ramified Extensions' (University of Exeter, 2009), written under the supervision of Dr. Nigel Byott.

2. Hopf–Galois structures

The notion of a Hopf–Galois structure is defined for certain extensions of commutative rings. We shall be interested mainly in studying Hopf–Galois structures on finite separable extensions of fields, but we give the definition in this more general context. Let R be a commutative ring with unity, S an R-algebra which is finitely generated and projective as an R-module, and H an R-Hopf algebra which is finitely generated and projective as an R-module.

We shall write $\varepsilon : H \to R$ for the counit of H and $\Delta : H \to H \otimes_R H$ for the comultiplication of H. We shall also make use of Sweedler notation

$$\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}.$$

We say that S is an *H-module algebra* if S is an H-module and for all $h \in H$ and $s, t \in S$ we have

$$\begin{aligned} h \cdot (st) &= \sum_{(h)} (h_{(1)} \cdot s)(h_{(2)} \cdot t) \\ h \cdot 1 &= \varepsilon(h)1. \end{aligned}$$

Definition 2.1. We say that S is an *H-Galois extension of R* (*H-Galois* for short), or that H gives a *Hopf–Galois structure* on the extension, if S is an H-module algebra and the R-linear map

$$j : S \otimes_R H \to \mathrm{End}_R(S)$$

defined by

$$j(s \otimes h)(t) = s(h \cdot t) \quad \text{for} \quad s, t \in S, \quad h \in H$$

is an R-module isomorphism.

A given finite separable extension of fields L/K may admit a number of Hopf–Galois structures. If the extension is Galois with group G then it admits at least the classical structure with Hopf algebra $K[G]$. A theorem of Greither and Pareigis allows for the enumeration of all Hopf–Galois structures admitted by L/K. Let E/K be the normal closure of L/K. Let $G = \mathrm{Gal}\,(E/K), G' = \mathrm{Gal}\,(E/L)$ and let $X = \{gG' \mid g \in G\}$ be the left coset space of G' in G. We shall write $\overline{x}$ for the coset xG', and $\mathrm{Perm}\, X$ for the group of permutations of the finite set X. Define an embedding $\lambda : G \to \mathrm{Perm}\, X$ by left translation:

$$\lambda(g)(\overline{x}) = \overline{gx} \text{ for } g \in G \text{ and } \overline{x} \in X.$$

Finally, we call a subgroup N of $\mathrm{Perm}\, X$ *regular* if $|N| = |X|$ and N acts transitively on X. We can now state the theorem of Greither and Pareigis:

Theorem 2.2 (Greither and Pareigis)**.** *There is a bijection between regular subgroups N of $\mathrm{Perm}\, X$ normalised by $\lambda(G)$ and Hopf–Galois structures on L/K. If N is such a subgroup, then G acts on the group algebra $E[N]$ by acting simultaneously on the coefficients as the Galois automorphisms and on the group elements by conjugation via the embedding λ. The Hopf algebra giving the Hopf–Galois structure corresponding to the subgroup N is*

$$H = E[N]^G = \{z \in E[N] \mid {}^g z = z \text{ for all } g \in G\}.$$

Such a Hopf algebra acts on the extension L/K as follows: if $\sum_{n\in N} c_n n \in H$ (with $c_n \in E$ a priori), then

$$\left(\sum_{n\in N} c_n n\right)\cdot x = \sum_{n\in N} c_n(n^{-1}(\overline{1_G}))x. \tag{1}$$

Proof. See [4, Theorem 6.8]. □

The Hopf algebras produced by Theorem 2.2 inherit the Hopf algebra structure maps from the group algebra $E[N]$, and are therefore cocommutative. Such a Hopf algebra is commutative precisely when the group N is abelian. Since all the fields we shall study have characteristic zero, all the Hopf algebras we shall study are separable K-algebras (see [10, (11.4)]). The normal basis theorem generalises to H-Galois extensions of fields: if L/K is such an extension then L is a free H-module of rank one (see [4, (2.16)]). For extensions of local or global fields, it is natural to investigate analogous results at integral level. To study the structure of $\mathfrak{O}_L$ relative to the Hopf–Galois structure with corresponding Hopf algebra H we define within H the associated order of $\mathfrak{O}_L$:

$$\mathfrak{A}_H = \{h \in H \mid h\cdot x \in \mathfrak{O}_L \text{ for all } x \in \mathfrak{O}_L\}.$$

As noted in the introduction, $\mathfrak{A}_H$ is the largest order in H for which $\mathfrak{O}_L$ is a module. We are particularly interested in establishing whether $\mathfrak{O}_L$ is a free (or locally free) $\mathfrak{A}_H$-module. In the p-adic case we have already mentioned Childs' theorem. We call an order Λ in a K-Hopf algebra H a *Hopf order* if Λ is an $\mathfrak{O}_K$-Hopf algebra with operations induced from H.

Theorem 2.3 (Childs)**.** *Let L/K be a finite H-Galois extension of p-adic fields. If the associated order $\mathfrak{A}_H$ is a Hopf order in H, then $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.*

Proof. See [4, Theorem 12.7]. □

We also state the following, which comes from integral representation theory. We recall that since we are concerned with fields of characteristic zero, a Hopf algebra H produced by Theorem 2.2 is separable. It follows (see [5, Proposition 26.10]) that if H is commutative then it has a unique maximal order.

Proposition 2.4. *Let L/K be an H-Galois extension of p-adic fields for a commutative Hopf algebra H. If $\mathfrak{A}_H$ is the unique maximal order in H then $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.*

Proof. Since $\mathfrak{A}_H$ is the unique maximal order in H, [5, Theorem 26.12] implies that $\mathfrak{O}_L$ is $\mathfrak{A}_H$-projective. Since K is a p-adic field and L is a free H-module, we may apply [9, Theorem 18.10], and conclude that $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module. □

We end this section by considering a special order inside a Hopf algebra produced by the theorem of Greither and Pareigis (Theorem 2.2). Suppose that L/K is an extension of p-adic fields or number fields with Galois closure E, and that L/K is H-Galois for some Hopf algebra H. Then by Theorem 2.2, we have that $H = E[N]^G$ for N some regular subgroup of $\operatorname{Perm} X$ normalised by $\lambda(G)$. Within this algebra, we shall study the order $\mathfrak{O}_E[N]^G$.

Proposition 2.5. *We have* $\mathfrak{O}_E[N]^G \subseteq \mathfrak{A}_H$.

Proof. Let $z \in \mathfrak{O}_E[N]^G$. Then $z \in \mathfrak{O}_E[N]$, so we may write

$$z = \sum_{n \in N} c_n n$$

with $c_n \in \mathfrak{O}_E$. Since $z \in H$, the action of z on an element $x \in L$ is given by equation (1). Now for each $n \in N$, any group element representing $n^{-1}(\overline{1_G})$ is a Galois automorphism of E, so if $x \in \mathfrak{O}_L$ then $n^{-1}(\overline{1_G})x \in \mathfrak{O}_E$. Therefore for $x \in \mathfrak{O}_L$ we have

$$z \cdot x = \sum_{n \in N} c_n n^{-1}(\overline{1_G})x \in \mathfrak{O}_E.$$

Since also $z \cdot x \in L$, we have that $z \cdot x \in \mathfrak{O}_E \cap L = \mathfrak{O}_L$, whence $z \in \mathfrak{A}_H$. □

The proofs in this paper involve showing that under appropriate conditions we have locally the reverse inclusion.

3. Unramified extensions

Throughout this section, we let L/K be a finite unramified extension of p-adic fields. Then L/K is automatically Galois, with cyclic Galois group, say G. By the theorem of Greither and Pareigis (Theorem 2.2), a Hopf algebra H giving a Hopf–Galois structure on L/K is of the form $L[N]^G$ for N some regular subgroup of $\operatorname{Perm} G$ normalised by $\lambda(G)$. We shall show that $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$, and that this is a Hopf order in H, which by Theorem 2.3 implies that $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module. We begin with a technical result:

Proposition 3.1. *We have*

$$\mathfrak{O}_L[N]^G \otimes_{\mathfrak{O}_K} \mathfrak{O}_L = \mathfrak{O}_L[N].$$

Proof. Since L/K is unramified, the extension $\mathfrak{O}_L/\mathfrak{O}_K$ of commutative rings is a Galois extension with group G in the sense of [3], and so we may apply Galois descent. By Morita theory (see [5, Section 3D]) there is an equivalence of categories between the category of left $\mathfrak{O}_K$-modules and the category of left $\operatorname{End}_{\mathfrak{O}_K}(\mathfrak{O}_L)$-modules given by the base change functor $X \to \mathfrak{O}_L \otimes_{\mathfrak{O}_K} X$. Since $\mathfrak{O}_L/\mathfrak{O}_K$ is a Galois extension with group G, the inverse to this functor is the fixed module functor $M \to M^G$ (see [4, Section 2.12]). Applying this to the $\operatorname{End}_{\mathfrak{O}_K}(\mathfrak{O}_L)$-module $\mathfrak{O}_L[N]$ yields the result. □

We now use this result to show that if L/K is an unramified extension of p-adic fields and $H = L[N]^G$ is a Hopf algebra giving a Hopf–Galois structure on the extension then we have the reverse inclusion to Proposition 2.5.

Proposition 3.2. *We have* $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$.

Proof. By Proposition 2.5, $\mathfrak{O}_L[N]^G \subseteq \mathfrak{A}_H$. On the other hand, since L/K is unramified, we have that $\mathfrak{O}_L \otimes_{\mathfrak{O}_K} \mathfrak{O}_L \cong \mathfrak{O}_L^{[L:K]}$, and this is the ring of integers of $L \otimes_K L \cong L^{[L:K]}$. The group N acts on $L^{[L:K]}$ by permuting the components, and so the L-algebra $H \otimes_K L \cong L[N]$ acts on $L \otimes_K L$. The associated order of $\mathfrak{O}_L \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$ in $L[N]$ is $\mathfrak{O}_L[N]$. Since $\mathfrak{A}_H \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$ also acts on $\mathfrak{O}_L \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$, we conclude that

$$\mathfrak{A}_H \otimes_{\mathfrak{O}_K} \mathfrak{O}_L \subseteq \mathfrak{O}_L[N].$$

So by Proposition 3.1 we have

$$\mathfrak{A}_H \otimes_{\mathfrak{O}_K} \mathfrak{O}_L \subseteq \mathfrak{O}_L[N]^G \otimes_{\mathfrak{O}_K} \mathfrak{O}_L,$$

and therefore

$$\mathfrak{A}_H \subseteq \mathfrak{O}_L[N]^G.$$

Hence $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$. □

We now use this explicit description of $\mathfrak{A}_H$ to show that $\mathfrak{A}_H$ is in fact a Hopf order. Again we employ Galois descent:

Proposition 3.3. *The associated order* $\mathfrak{A}_H$ *is a Hopf order in* H.

Proof. By Proposition 3.2, $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$. Note that the action of G on the $\mathfrak{O}_L$-Hopf algebra $\mathfrak{O}_L[N]$ is via Hopf algebra homomorphisms; this follows from the proof of the theorem of Greither and Pareigis (see [4, Theorem 6.8]). Since $\mathfrak{O}_L/\mathfrak{O}_K$ is a Galois extension of commutative rings with group G the $\mathfrak{O}_L$-module homomorphisms giving the Hopf algebra structure on $\mathfrak{O}_L[N]$ induce structure maps on $\mathfrak{O}_L[N]^G$ with the same properties (see [4, Section 2.12]). This implies that $\mathfrak{O}_L[N]^G$ is an $\mathfrak{O}_K$-Hopf algebra. □

In fact, in this case $\mathfrak{O}_L[N]^G$ is the minimal Hopf order in $H = L[N]^G$, since $\mathfrak{O}_L[N]$ is the minimal Hopf order in $L[N]$. We now restate and prove Theorem 1.1:

Theorem 3.4. *Let* L/K *be a finite unramified extension of* p*-adic fields and let* $H = L[N]^G$ *be a Hopf algebra giving a Hopf–Galois structure on the extension. Then* $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$ *and* $\mathfrak{O}_L$ *is a free* $\mathfrak{A}_H$*-module.*

Proof. By Proposition 3.2 we have $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$, and by Proposition 3.3 this is a Hopf order in H. Now apply Theorem 2.3. □

4. Maximal associated orders

Throughout this section we let L/K be a finite (not necessarily Galois) extension of p-adic fields with Galois closure E, and suppose that $p \nmid [L : K]$. We shall consider Hopf–Galois structures admitted by L/K for which the corresponding Hopf algebra H is commutative. We recall that since K has characteristic zero, H is a separable K-algebra, and so this implies that H has a unique maximal order. In the notation established prior to Theorem 2.2, we have that $H = E[N]^G$ for some abelian regular subgroup N of $\operatorname{Perm} X$ normalised by $\lambda(G)$. In particular we note that $|N| = [L : K]$. We show that in this case $\mathfrak{A}_H$ coincides with the unique maximal order in H. When this occurs, it follows by Proposition 2.4 that $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.

Proposition 4.1. *The integral group ring $\mathfrak{O}_E[N]$ is the unique maximal order in $E[N]$.*

Proof. This follows easily from [5, Proposition 27.1]. In fact $\mathfrak{O}_E[N]$ is the only order in $E[N]$. □

We now show that taking the fixed points of $E[N]$ under the action by G preserves this maximality, so that $\mathfrak{O}_E[N]^G$ is the unique maximal order in $H = E[N]^G$.

Proposition 4.2. *Let G act on the group algebra $E[N]$ by acting on E as Galois automorphisms and on N by conjugation via the embedding λ. Then $\mathfrak{O}_E[N]^G$ is the unique maximal order in the K-algebra $E[N]^G$.*

Proof. Since E has characteristic zero and N is abelian, $E[N]^G$ has a unique maximal order. Since $p \nmid |N|$, the maximal $\mathfrak{O}_E$ order in $E[N]$ is $\mathfrak{O}_E[N]$ by Proposition 4.1. Denote by $\mathfrak{M}$ the maximal order in $E[N]^G$, and let $x \in \mathfrak{M}$. Then x is integral over $\mathfrak{O}_K$ in $E[N]^G$, so x is integral over $\mathfrak{O}_E$ in $E[N]$, whence $x \in \mathfrak{O}_E[N]$. So $x \in E[N]^G \cap \mathfrak{O}_E[N] = \mathfrak{O}_E[N]^G$, and so $\mathfrak{O}_E[N]^G = \mathfrak{M}$. □

Proposition 4.3. *The associated order $\mathfrak{A}_H$ is the unique maximal order in H.*

Proof. By Proposition 4.2, $\mathfrak{O}_E[N]^G$ is the unique maximal order in H. On the other hand, by Proposition 2.5 $\mathfrak{O}_E[N]^G \subseteq \mathfrak{A}_H$. So $\mathfrak{O}_E[N]^G = \mathfrak{A}_H$ is the unique maximal order in H. □

We now restate and prove Theorem 1.2

Theorem 4.4. *Let L/K be a finite (not necessarily Galois) extension of p-adic fields and let H be a commutative Hopf algebra giving a Hopf–Galois structure on the extension. Suppose that $p \nmid [L : K]$. Then $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$ and $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.*

Proof. By Proposition 4.3 we have that $\mathfrak{A}_H = \mathfrak{O}_E[N]^G$ and that this is the unique maximal order in H. Now apply Proposition 2.4. □

5. Consequences for number fields

In this section we consider a finite extension of number fields L/K. We shall prove results analogous to those in Sections 3 and 4 which will give us information about the local structure of $\mathfrak{O}_L$ as a module over its associated order $\mathfrak{A}_H$ in a Hopf algebra H giving a nonclassical Hopf–Galois structure on the extension.

If $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ and A is a K-algebra then we shall write $A_\mathfrak{p}$ for the $K_\mathfrak{p}$-algebra $A \otimes_K K_\mathfrak{p}$, and similarly for orders in A. We then have that $L_\mathfrak{p}$ is an $H_\mathfrak{p}$-Galois extension of $K_\mathfrak{p}$, and we seek to study the completed ring of integers $\mathfrak{O}_{L,\mathfrak{p}}$ over the completed associated order $\mathfrak{A}_{H,\mathfrak{p}}$. In general $L_\mathfrak{p}$ is not a local field but a finite product of local fields - we have the isomorphism

$$L_\mathfrak{p} \cong \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P},$$

where the product is taken over the prime ideals $\mathfrak{P}$ of $\mathfrak{O}_L$ which lie above $\mathfrak{p}$ and each $L_\mathfrak{P}$ is a p-adic field. We have an analogous decomposition at integral level. (see [7, (2.16)].)

Since the results quoted in Theorem 2.3 and Proposition 2.4 are applicable only to extensions of local fields, we require generalisations of these results in order to proceed. The appropriate generalisation of Proposition 2.4 is straightforward:

Proposition 5.1. *Let L/K be an extension of number fields which is H-Galois for a commutative Hopf algebra H, and let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$. If $\mathfrak{A}_{H,\mathfrak{p}}$ is the unique maximal order in $H_\mathfrak{p}$ then $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.*

Proof. This is essentially the same as the proof of Proposition 2.4. □

To state the appropriate generalisation of Childs' theorem (Theorem 2.3) we need a generalisation of the notion of tameness, due to Childs ([4, (13.1)]). Let H be a Hopf algebra (over an arbitrary commutative ring R) and S an R-algebra which is finitely generated and projective as an R-module, and which is an H-module algebra. We call an element $\theta \in H$ a *left integral* if for all $h \in H$ we have $h\theta = \varepsilon(h)\theta$, where $\varepsilon : H \to R$ is the counit map. We say that S is an *H-tame extension of R* if the following conditions are satisfied:

(1) $\{s \in S \mid hs = \varepsilon(h)s \text{ for all } h \in H\} = R$.
(2) $\mathrm{rank}_R(S) = \mathrm{rank}_R(H)$.
(3) S is a faithful H-module.
(4) There exists a left integral θ of H satisfying $\theta S = R$.

Then we have:

Proposition 5.2. *If $\mathfrak{A}_{H,\mathfrak{p}}$ is a Hopf order in $H_\mathfrak{p}$ and $\mathfrak{O}_{L,\mathfrak{p}}$ is an $\mathfrak{A}_{H,\mathfrak{p}}$-tame extension of $\mathfrak{O}_{K,\mathfrak{p}}$ then $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.*

Proof. See [4, Theorem 13.4]. □

We can now prove analogues of the results in Sections 3 and 4 for completions of extensions of number fields. We begin with completions at an unramified prime $\mathfrak{p}$. Motivated by Proposition 3.2 we consider the $\mathfrak{O}_{K,\mathfrak{p}}$-order $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ in the completed Hopf algebra $H_{\mathfrak{p}}$. Note that in this proposition we do not require that H be commutative.

Proposition 5.3. *Let L/K be a finite Galois extension of number fields with group G, and suppose L/K is H-Galois for the Hopf algebra $H = L[N]^G$. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which is unramified in $\mathfrak{O}_L$. Then the order $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a Hopf order in $H_{\mathfrak{p}}$.*

Proof. Since $\mathfrak{p}$ is unramified in $\mathfrak{O}_L$, the completed ring of integers $\mathfrak{O}_{L,\mathfrak{p}}$ is a Galois extension of $\mathfrak{O}_{K,\mathfrak{p}}$. The proof now follows that of Proposition 3.3. □

Theorem 5.4. *Let L/K be a finite Galois extension of number fields with group G, and suppose L/K is H-Galois for the Hopf algebra $H = L[N]^G$. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which is unramified in $\mathfrak{O}_L$. Then $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.*

Proof. By Proposition 5.3, $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a Hopf order in $H_{\mathfrak{p}}$. We note that the trace element

$$\theta = \sum_{n \in N} n$$

is a left integral of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$, and since $\mathfrak{p}$ is unramified in $\mathfrak{O}_L$ there exists an element $t \in \mathfrak{O}_{L,\mathfrak{p}}$ such that $\theta \cdot t = 1$. Thus $\mathfrak{O}_{L,\mathfrak{p}}$ is an $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$-tame extension of $\mathfrak{O}_{K,\mathfrak{p}}$, and so $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$-module. Thus $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$. □

Corollary 5.5. *Under the same assumptions as Theorem 5.4, $\mathfrak{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{H,\mathfrak{p}}$ for all primes $\mathfrak{p}$ of $\mathfrak{O}_K$ which are unramified in $\mathfrak{O}_L$. Thus in order to determine whether $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module, it is sufficient to consider the structure of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$ for each of the (finitely many) primes $\mathfrak{p}$ which are ramified in $\mathfrak{O}_L$.*

Now we consider the situation analogous to that considered in Section 4.

Proposition 5.6. *Let L/K be a finite (not necessarily Galois) extension of number fields with Galois closure E. Suppose L/K is H-Galois for some commutative Hopf algebra $H = E[N]^G$. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which lies above a prime number $p \nmid [L : K]$. Then $\mathfrak{O}_{E,\mathfrak{p}}[N]^G$ is the unique maximal order in $H_{\mathfrak{p}}$.*

Proof. Let $\mathfrak{M}$ denote the unique maximal order in H, so that $\mathfrak{M}_{\mathfrak{p}}$ is the unique maximal order in $H_{\mathfrak{p}}$, and let $x \in \mathfrak{M}_{\mathfrak{p}}$. Then $x \in E_{\mathfrak{p}}[N]^G$, so $x \in E_{\mathfrak{p}}[N]$. We have an isomorphism

$$E_{\mathfrak{p}}[N] \cong \prod_{\mathfrak{P}|\mathfrak{p}} E_{\mathfrak{P}}[N],$$

where the product is taken over the prime ideals $\mathfrak{P}$ of $\mathfrak{O}_L$ lying abve $\mathfrak{p}$, and each factor on the right is a group algebra over a p-adic field whose residue characteristic is coprime to $|N|$. Applying Proposition 4.1 to each factor on the right, we see that the image of x under the isomorphism above lies in the product

$$\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}_{E,\mathfrak{P}}[N] \cong \mathfrak{O}_{E,\mathfrak{p}}[N],$$

and so $x \in \mathfrak{O}_{E,\mathfrak{p}}[N] \cap E_{\mathfrak{p}}[N]^G = \mathfrak{O}_{E,\mathfrak{p}}[N]^G$. Therefore $\mathfrak{M}_{\mathfrak{p}} = \mathfrak{O}_{E,\mathfrak{p}}[N]^G$. □

Proposition 5.7. *Retain the assumptions of Proposition 5.6. Then the completed associated order $\mathfrak{A}_{H,\mathfrak{p}}$ is the unique maximal order in $H_{\mathfrak{p}}$.*

Proof. By Proposition 5.6, $\mathfrak{O}_{E,\mathfrak{p}}[N]^G$ is the unique maximal order in $H_{\mathfrak{p}}$. On the other hand, by Proposition 2.5 $\mathfrak{O}_{E,\mathfrak{p}}[N]^G \subseteq \mathfrak{A}_{H,\mathfrak{p}}$. So $\mathfrak{O}_{E,\mathfrak{p}}[N]^G = \mathfrak{A}_{H,\mathfrak{p}}$ and this is the maximal order in $H_{\mathfrak{p}}$. □

Theorem 5.8. *Let L/K be a finite (not necessarily Galois) extension of number fields with Galois closure E, and let $G = \mathrm{Gal}\,(E/K)$. Suppose that L/K is H-Galois for some commutative Hopf algebra $H = E[N]^G$. Suppose that $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ lying above a prime number $p \nmid [L : K]$. Then $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{E,\mathfrak{p}}[N]^G$ and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.*

Proof. By Proposition 5.6 and Proposition 5.7 we have that

$$\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$$

and that this is the unique maximal order in $H_{\mathfrak{p}}$. Now apply Proposition 5.1. □

We obtain Theorem 1.3 by combining these results. Recall that a Galois extension L/K of number fields is called *domestic* if no prime of $\mathfrak{O}_K$ lying above a prime number dividing $[L : K]$ ramifies in $\mathfrak{O}_L$.

Theorem 5.9. *Let L/K be a finite domestic extension of number fields. Suppose that L/K is H-Galois for some commutative Hopf algebra H. Then $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$ and $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module.*

Proof. By Theorem 5.4, we have that if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which is unramified in $\mathfrak{O}_L$ then $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module. Suppose $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which is ramified in $\mathfrak{O}_L$. Then $\mathfrak{p}$ lies above a prime number p, and since L/K is domestic, we have $p \nmid [L : K]$. We may therefore apply Theorem 5.8, and conclude that $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ and that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module. □

As a particular example, we have:

Corollary 5.10. *Let L/K be a finite Galois extension of number fields of prime power degree which is at most tamely ramified. Suppose that L/K is H-Galois for some commutative Hopf algebra H. Then $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module.*

Proof. By Corollary 5.9, it is sufficient to observe that since L/K has prime power degree, the assumption that it is tamely ramified is equivalent to the assumption that it is domestic. □

References

[1] Byott, Nigel P. Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications. *Journal de Theorie des Nombres de Bordeaux* **9** (1997), 201–219. MR1469668 (98h:11152), Zbl 0889.11040.

[2] Childs, Lindsay N. Taming wild extensions with Hopf algebras. *Trans. Amer. Math. Soc.* **304** (1987), 111–140. MR0906809 (89a:11119), Zbl 0632.12013.

[3] Chase, S. U.; Harrison, D. K.; Rosenberg, Alex. Galois theory and cohomology of commutative rings. *Memoirs of the American Mathematical Society*, No. 52, 1965, 15–33. MR0195922 (33 #4118), Zbl 0143.05902.

[4] Childs, Lindsay N. Taming wild extensions: Hopf algebras and local Galois module theory. Mathematical Surveys and Monographs, 80. *American Mathematical Society, Providence, RI*, 2000. viii+215 pp. ISBN: 0-8218-2131-8. MR1767499 (2001e:11116), Zbl 0944.11038.

[5] Curtis, Charles W.; Reiner, Irving. Methods of representation theory. Vol. I. With applications to finite groups and orders. Pure and Applied Mathematics. A Wiley-Interscience Publication. *John Wiley & Sons, Inc., New York*, 1981. xxi+819 pp. ISBN: 0-471-18994-4. MR0632548 (82i:20001), Zbl 0469.20001.

[6] Fröhlich, Albrecht. Galois module structure of algebraic integers. Ergebnisse der Mathematik und ihrer Grenzgebiete, 1. *Springer-Verlag, Berlin, 1983.* x+262 pp. ISBN: 3-540-11920-5. MR0717033 (85h:11067), Zbl 0501.12012.

[7] Fröhlich, A. ; Taylor, M. J. Algebraic number theory. Cambridge Studies in Advanced Mathematics, 27. *Cambridge University Press, Cambridge*, 1993. xiv+355 pp. ISBN: 0-521-43834-9. MR1215934 (94d:11078), Zbl 0744.11001.

[8] Hilbert, D. Die theorie der algebraischen zahlen. *Gesammelte Abhandlungen*, **1** (1965), 63–363.

[9] Reiner, Irving. Maximal orders. London Mathematical Society Monographs, No. 5. *Academic Press, London-New York*, 1975. xii+395 pp. MR0393100 (52 #13910), Zbl 0305.16001.

[10] Waterhouse, William C. Introduction to affine group schemes. Graduate Texts in Mathematics, 66. *Springer-Verlag, New York-Berlin*, 1979. xi+164 pp. ISBN: 0-387-90421-2. MR0547117 (82e:14003), Zbl 0442.14017.

School of Computing and Mathematics, Keele University, UK
P.J.Truman@Keele.ac.uk

This paper is available via http://nyjm.albany.edu/j/2011/17-34.html.