HOPF-GALOIS MODULE STRUCTURE OF TAMELY RAMIFIED RADICAL EXTENSIONS OF PRIME DEGREE

PAUL J. TRUMAN

ABSTRACT. Let K be a number field and let L/K be a tamely ramified radical extension of prime degree p. If K contains a primitive p^{th} root of unity then L/K is a cyclic Kummer extension; in this case the group algebra $K[G]$ (with $G = \text{Gal}(L/K)$) gives the unique Hopf-Galois structure on L/K, the ring of algebraic integers $\mathfrak{O}_L$ is locally free over $\mathfrak{O}_K[G]$ by Noether's theorem, and Gómez Ayala has determined a criterion for $\mathfrak{O}_L$ to be a free $\mathfrak{O}_K[G]$-module. If K does not contain a primitive p^{th} root of unity then L/K is a separable, but non-normal, extension, which again admits a unique Hopf-Galois structure. Under the assumption that p is unramified in K, we show that $\mathfrak{O}_L$ is locally free over its associated order in this Hopf-Galois structure and determine a criterion for it to be free. We find that the conditions that appear in this criterion are identical to those appearing in Gómez Ayala's criterion for the normal case.

1. INTRODUCTION

In classical Galois module theory we consider a finite Galois extension L/K of local or global fields with Galois group G and study the structure of each fractional ideal $\mathfrak{B}$ of L as a module over its associated order $\mathfrak{A}_{K[G]}(\mathfrak{B}) \subset K[G]$, with particular emphasis on the case $\mathfrak{B} = \mathfrak{O}_L$, the ring of algebraic integers (or valuation ring) of L. Hopf-Galois module theory generalizes this situation: a *Hopf-Galois structure* on an extension of fields L/K consists of a K-Hopf algebra H together with a certain K-linear action of H on L (see [5, Definition 2.7] for the precise definition). If L/K is an extension of local or global fields and H gives a Hopf-Galois structure on L/K then we can study the structure of each fractional ideal $\mathfrak{B}$ of L as a module over its associated order $\mathfrak{A}_H(\mathfrak{B}) \subset H$. These techniques have applications to Galois extensions L/K: in this case the group algebra $K[G]$ (with $G = \text{Gal}(L/K)$) gives a Hopf-Galois structure on L/K, and any further Hopf-Galois structures admitted by the extension provide alternative contexts in which we can study each fractional ideal (see [3], for example). However, the application of Hopf-Galois theory to extensions which are not Galois is particularly interesting, since it provides descriptions of rings of algebraic integers and/or fractional ideals in situations where classical techniques do not apply. For example, Hopf-Galois theory has recently been used by Koch [15] to study the structure of fractional ideals in a totally ramified purely inseparable extension of local fields of prime power degree, and by Elder [7] to address the same questions for a separable, but non-normal, ramified extension of local fields of prime degree. In this paper we study the Hopf-Galois module structure of the ring of algebraic integers in a tamely ramified non-normal radical extension of number fields of prime degree. These are the first results concerning the Hopf-Galois module structure of rings of algebraic integers in non-normal extensions of global fields.

Let K be a number field, p a prime number, and $\zeta \in \mathbb{C}$ a primitive p^{th} root of unity. Let

1

$L = K(\omega)$ with $\omega^p \in K - K^p$. If $\zeta \in K$ then L/K is a cyclic Kummer extension, and the group algebra $K[G]$ (with $G = \mathrm{Gal}(L/K)$) gives a Hopf-Galois structure on L/K. If L/K is at most tamely ramified (henceforth, "tame") then Noether's theorem [8, Theorem 3] implies that $\mathfrak{A}_{K[G]}(\mathfrak{O}_L) = \mathfrak{O}_K[G]$ and that $\mathfrak{O}_L$ is a locally free $\mathfrak{O}_K[G]$-module (of rank one), and Gómez Ayala [10] has determined a criterion for $\mathfrak{O}_L$ to be a free $\mathfrak{O}_K[G]$-module. By Byott's uniqueness theorem [2, Theorem 1] the Hopf-Galois structure given by $K[G]$ is the only Hopf-Galois structure admitted by the extension, and so we have nothing to add to these results. If $\zeta \notin K$ then L/K is a separable, but non-normal, extension. Results of Childs [4, Section 2] and Kohl [16, Theorem 3.3] imply that L/K also admits a unique Hopf-Galois structure in this case. We show that if L/K is tame and p is unramified in K then $\mathfrak{O}_L$ is a locally free module (of rank one) over its associated order in this Hopf-Galois structure and determine a criterion for $\mathfrak{O}_L$ to be free. Interestingly, we find that the conditions that appear in this criterion are identical to those that appear in Gómez Ayala's criterion for the normal case.

The paper is organized as follows. In section 2 we summarize Gómez Ayala's work on the case in which L/K is normal; thereafter we assume that L/K is non-normal. From section 3 onward we assume that p is unramified in K; under this assumption we establish a criterion for L/K to be tame (proposition 3.3), and determine an integral basis of $\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{O}_{K,\mathfrak{p}} \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$ over $\mathfrak{O}_{K,\mathfrak{p}}$ for each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ in this case (propositions 3.4 and 3.5). In section 4 we study the unique Hopf-Galois structure admitted by L/K; in particular, we show that the Hopf algebra H giving this Hopf-Galois structure is isomorphic to K^p as a K-algebra (proposition 4.3) and give a simple formula for its action on L (proposition 4.4). In section 5 we show that $\mathfrak{O}_L$ is locally free over its associated order $\mathfrak{A} = \mathfrak{A}_H(\mathfrak{O}_L)$ (theorem 5.1), and for each $\mathfrak{p}$ we determine an explicit generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_\mathfrak{p}$. Given that $\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module, a result of Bley and Johnston [1, Proposition 2.1] relates the structure of $\mathfrak{O}_L$ as an $\mathfrak{A}$-module to the structure of $\mathfrak{M}\mathfrak{O}_L$ as an $\mathfrak{M}$-module, where $\mathfrak{M}$ denotes the unique maximal order in H; we use this result, along with an idélic description of the locally free class group $\mathrm{Cl}(\mathfrak{M})$, to derive a criterion for for $\mathfrak{O}_L$ to be a free $\mathfrak{A}$-module (theorem 5.5), and show that the conditions appearing in this criterion are identical to those appearing in Gómez Ayala's criterion for the normal case. Finally, in section 6 we discuss a unified approach to the normal and non-normal cases.

2. Gómez Ayala's Criterion

We retain the notation established in the introduction: K is a number field, p a prime number, ζ a primitive p^{th} root of unity, and L/K is an extension of the form $L = K(\omega)$ with $\omega^p \in K - K^p$. In this section we assume that $\zeta \in K$; the extension L/K is then a cyclic Kummer extension and the group algebra $K[G]$ (with $G = \mathrm{Gal}(L/K)$) gives the unique Hopf-Galois structure on L/K. We also suppose that L/K is tame. By Noether's theorem we then have that $\mathfrak{A}_{K[G]}(\mathfrak{O}_L) = \mathfrak{O}_K[G]$ and $\mathfrak{O}_L$ is a locally free $\mathfrak{O}_K[G]$-module. Gómez Ayala [10] has determined a criterion for $\mathfrak{O}_L$ to be a free $\mathfrak{O}_K[G]$-module; we summarize his result using some notation and terminology from [6]. Each ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ has a unique decomposition of the form

$$\mathfrak{a} = \prod_{i \geq 1} \mathfrak{a}_i^i,$$

where the $\mathfrak{a}_i$ are pairwise coprime squarefree ideals of $\mathfrak{O}_F$. (We have $\mathfrak{a}_i = \mathfrak{O}_K$ for i sufficiently large, so the product above is finite.) We call the ideal $\mathfrak{a}_i$ the *i-part of* $\mathfrak{a}$, and note that it is the product of the prime ideals $\mathfrak{p}$ of $\mathfrak{O}_K$ such that $v_\mathfrak{p}(\mathfrak{a}) = i$. Next we define the *ideals associated*

to $\mathfrak{a}$ by

$$\mathfrak{b}_j = \prod_{i \geq 1} \mathfrak{a}_i^{\lfloor ij/p \rfloor} \text{ for } 0 \leq j \leq p-1,$$

where $\lfloor x \rfloor$ denotes the largest integer not exceeding x. We remark that an alternative expression for the $\mathfrak{b}_j$ is

$$\mathfrak{b}_j = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor v_{\mathfrak{p}}(\mathfrak{a}^j)/p \rfloor} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}(\mathfrak{a}^j)} \text{ for } 0 \leq j \leq p-1,$$

where the product is taken over the prime ideals $\mathfrak{p}$ of $\mathfrak{O}_K$, and $r_{\mathfrak{p}}(\mathfrak{a}^j) = \lfloor v_{\mathfrak{p}}(\mathfrak{a}^j)/\mathfrak{p} \rfloor$.

Gómez Ayala's result is that $\mathfrak{O}_L$ is a free $\mathfrak{O}_K[G]$-module if and only if there exists an element $\beta \in \mathfrak{O}_L$ such that

(1) $L = K(\beta)$,
(2) $b = \beta^p \in \mathfrak{O}_K$,
(3) the ideals $\mathfrak{b}_j$ associated to $b\mathfrak{O}_K$ are principal with generators b_j such that

$$\sum_{j=0}^{p-1} \frac{\beta^j}{b_j} \equiv 0 \pmod{p\mathfrak{O}_L}.$$

Furthermore, in this case the element

$$\frac{1}{p} \sum_{j=0}^{p-1} \frac{\beta^j}{b_j}$$

is a free generator of $\mathfrak{O}_L$ as an $\mathfrak{O}_K[G]$-module.

Several authors have studied generalizations or variants of this result. Ichimura [14] proved that if p is unramified in K and L/K is a tamely ramified Galois extension of degree p then L has a normal integral basis if the Kummer extension $L(\zeta)/K(\zeta)$ has a normal integral basis. Ichimura also studied the case in which L/K is a cyclic Kummer extension of arbitrary degree [13], and a criterion for the existence of a normal integral basis in this case was given by Del Corso and Rossi [6].
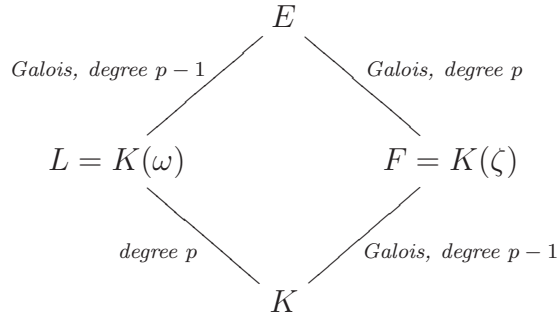
3. TAME RADICAL EXTENSIONS OF PRIME DEGREE

Henceforth we suppose that $\zeta \notin K$, and write $F = K(\zeta)$. The extension L/K is then separable but non-normal. In fact, we impose the stronger hypothesis that p is unramified in K. We record some consequences of this assumption:

Lemma 3.1. *Suppose that p is unramified in K. Then:*

(1) *F/K has degree $p-1$;*
(2) *each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ lying above p is totally ramified in F/K;*
(3) *the set $\{1, \zeta, \dots, \zeta^{p-2}\}$ is an integral basis of $\mathfrak{O}_F$ over $\mathfrak{O}_K$.*

Proof. Let $\mathfrak{p}$ be a prime ideal of K lying above p. Since p in unramified in K the polynomial $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is an Eisenstein polynomial over $K_{\mathfrak{p}}$ and has ζ as a root, so $K_{\mathfrak{p}}(\zeta)/K_{\mathfrak{p}}$ has degree $p-1$ and is totally ramified, by [9, Theorem 24]. Therefore F/K has degree $p-1$ and $\mathfrak{p}$ is totally ramified in F/K. We also have from [9, Theorem 24] that the set $\{1, \zeta, \dots, \zeta^{p-2}\}$ is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{F,\mathfrak{p}}$. Since $\mathfrak{d}(\{1, \zeta, \dots, \zeta^{p-2}\}) = \pm p^{p-2}$, this set is actually an integral basis of $\mathfrak{O}_{F,\mathfrak{p}}$ over $\mathfrak{O}_{K,\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ of $\mathfrak{O}_K$, and therefore an integral basis of $\mathfrak{O}_F$ over $\mathfrak{O}_K$. $\square$

The Galois closure of L/K is $E = K(\zeta, \omega)$, and E/F is a Galois extension of degree p. In this section we use well known results concerning ramification and local integral bases in E/F to establish a criterion for L/K to be tame and to determine local integral bases in this case.

Proposition 3.2. L/K *is tame if and only if* E/F *is tame.*

Proof. The extension F/K is tame since it is Galois of degree $p - 1$ and is ramified only at prime ideal lying above p; similarly E/L is tame. If L/K is tame then since E/L is tame we have that E/K is tame, and so E/F is tame. Conversely, if E/F is tame then since F/K is tame we have that E/K is tame, and so L/K is tame. $\qquad\square$

Proposition 3.3. L/K *is tame if and only if there exists* $\alpha \in \mathfrak{O}_L$ *such that*

(1) $L = K(\alpha)$;
(2) $\alpha^p \equiv 1 \pmod{p^2 \mathfrak{O}_K}$.

Proof. Suppose first that there exists $\alpha \in \mathfrak{O}_L$ with the properties stated in the proposition. Then (since $(\zeta - 1)^{p-1} \mathfrak{O}_F = p \mathfrak{O}_F$) we have $E = F(\alpha)$ with $\alpha^p \equiv 1 \pmod{(\zeta - 1)^p \mathfrak{O}_F}$ and so by [5, Propositions (24.2) and (24.4)] each prime ideal $\mathfrak{q}$ of $\mathfrak{O}_F$ lying above p is unramified in E. Since E/F is a Galois extension of degree p this implies that E/F is tame, and so L/K is tame by proposition 3.2.

Conversely, suppose that L/K is tame. Then by proposition 3.2 E/F is tame, and so by [5, Propositions (24.2) and (24.4)] for each prime ideal $\mathfrak{q}$ of $\mathfrak{O}_F$ lying above p there exists $\beta_{\mathfrak{q}} \in \mathfrak{O}_{E,\mathfrak{q}}$ such that $E_{\mathfrak{q}} = F_{\mathfrak{q}}(\beta_{\mathfrak{q}})$ and $\beta_{\mathfrak{q}}^p \equiv 1 \pmod{(\zeta - 1)^p \mathfrak{O}_{F,\mathfrak{q}}}$. By the Chinese Remainder Theorem there exists $\beta \in \mathfrak{O}_E$ such that $E = F(\beta)$ and $\beta^p \equiv 1 \pmod{(\zeta - 1)^p \mathfrak{O}_F}$. Let $\alpha = N_{E/L}(\beta)$; then $L = K(\alpha)$ and $\alpha^p \equiv 1 \pmod{(\zeta - 1)^p \mathfrak{O}_F}$. But $\alpha^p \in \mathfrak{O}_F \cap \mathfrak{O}_L = \mathfrak{O}_K$, so (again using the fact that $(\zeta - 1)^{p-1} \mathfrak{O}_F = p \mathfrak{O}_F$) we have $\alpha^p \equiv 1 \pmod{p^2 \mathfrak{O}_K}$. $\qquad\square$

Henceforth we shall suppose that L/K is tame and that $L = K(\alpha)$ with $a = \alpha^p \equiv 1 \pmod{p^2 \mathfrak{O}_K}$. We now determine integral bases of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{O}_{K,\mathfrak{p}}$ for each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$.

Proposition 3.4. *Let* $\mathfrak{p}$ *be a prime ideal of* $\mathfrak{O}_K$ *that does not lie above* p, *and let* $\pi_{\mathfrak{p}}$ *be a uniformizer of* $K_{\mathfrak{p}}$. *For* $x \in K$ *let* $r_{\mathfrak{p}}(x) = \left\lfloor \dfrac{v_{\mathfrak{p}}(x)}{p} \right\rfloor$. *Then an integral basis of* $\mathfrak{O}_{L,\mathfrak{p}}$ *over* $\mathfrak{O}_{K,\mathfrak{p}}$ *is given by*

$$\left\{ \frac{\alpha^j}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a^j)}} \,\middle|\, j = 0, 1, \dots, p - 1 \right\}.$$

Proof. The ramification indices of $\mathfrak{p}$ in F/K and E/K depend only on $\mathfrak{p}$, because F/K and E/K are Galois extensions. Let $\mathfrak{q}$ be a prime ideal of $\mathfrak{O}_F$ that lies above $\mathfrak{p}$. Then we have $e_{\mathfrak{p}}(E/K) = e_{\mathfrak{q}}(E/F) e_{\mathfrak{p}}(F/K)$, but $e_{\mathfrak{p}}(F/K) = 1$ since $\mathfrak{p}$ does not lie above p, and $e_{\mathfrak{q}}(E/F) = 1$

or p, since E/F is a Galois extension of degree p. Hence $e_{\mathfrak{p}}(E/K) = 1$ or p. Now let $\mathfrak{P}$ be a prime ideal of $\mathfrak{O}_L$ lying above $\mathfrak{p}$. Then $\mathfrak{P}$ is unramified in E/L, since $E = L(\zeta)$ and $\mathfrak{P}$ does not lie above p. Therefore $\mathfrak{p}$ is either unramified or totally ramified in L/K, according to whether $\mathfrak{q}$ is unramified or totally ramified in E/F. By [12, Theorem 118], $\mathfrak{q}$ is unramified in E/F if $p \mid v_{\mathfrak{q}}(a)$, and totally ramified if $p \nmid v_{\mathfrak{q}}(a)$. Since $\mathfrak{p}$ is unramified in F/K we conclude that $\mathfrak{p}$ is unramified in L/K if $p \mid v_{\mathfrak{p}}(a)$, and totally ramified if $p \nmid v_{\mathfrak{p}}(a)$.

If $p \mid v_{\mathfrak{p}}(a)$ then for each prime ideal $\mathfrak{P}$ of $\mathfrak{O}_L$ lying above $\mathfrak{p}$ and each $j = 0, 1, \ldots, p - 1$ we have $r_{\mathfrak{p}}(a^j) = v_{\mathfrak{P}}(\alpha^j)$, so $v_{\mathfrak{P}}\left(\alpha^j / \pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a^j)}\right) = 0$ (since $v_{\mathfrak{P}}(\pi_{\mathfrak{p}}) = 1$). Therefore the discriminant of the set in the proposition lies in $\mathfrak{O}_{K,\mathfrak{p}}^{\times}$, and so this set is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$.

If $p \nmid v_{\mathfrak{p}}(a)$ then let $\mathfrak{P}$ be the unique prime ideal of $\mathfrak{O}_L$ that lies above $\mathfrak{p}$; we then have $v_{\mathfrak{P}}(\pi_{\mathfrak{p}}) = p$ and $v_{\mathfrak{P}}(\alpha) = v_{\mathfrak{p}}(a)$, so for each $j = 0, 1, \ldots, p - 1$

$$v_{\mathfrak{P}}\left(\frac{\alpha^j}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a^j)}}\right) = v_{\mathfrak{p}}(a^j) - pr_{\mathfrak{p}}(a^j).$$

Therefore for each $j = 0, 1, \ldots, p - 1$ the set in the proposition contains exactly one element whose valuation at $\mathfrak{P}$ is equal to j, and so this set is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{P}} = \mathfrak{O}_{L,\mathfrak{p}}$. $\qquad\square$

Proposition 3.5. *Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$ that lies above p. Then an integral basis of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{O}_{K,\mathfrak{p}}$ is given by*

$$\left\{1, \alpha, \ldots, \alpha^{p-2}, \frac{1}{p}\left(1 + \alpha + \cdots + \alpha^{p-1}\right)\right\}.$$

Proof. Let $\mathfrak{q}$ be the unique prime ideal of $\mathfrak{O}_F$ that lies above $\mathfrak{p}$. By [5, Proposition 24.4] an $\mathfrak{O}_{F,\mathfrak{q}}$-basis of $\mathfrak{O}_{E,\mathfrak{q}}$ is given by

$$\left\{\left(\frac{\alpha - 1}{\zeta - 1}\right)^j \;\middle|\; j = 0, 1, \ldots, p - 1\right\}.$$

Since $v_{\mathfrak{q}}(p) = p - 1$, it follows that an $\mathfrak{O}_{F,\mathfrak{q}}$-basis of $\mathfrak{O}_{E,\mathfrak{q}}$ is given by

$$\left\{\frac{(\alpha - 1)^j}{p}(\zeta - 1)^{p-1-j} \;\middle|\; j = 0, 1, \ldots, p - 1\right\}$$

and (using lemma 3.1) that an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{E,\mathfrak{p}}$ is given by

$$\left\{\frac{(\alpha - 1)^j}{p}\zeta^i(\zeta - 1)^{p-1-j} \;\middle|\; \begin{array}{l} i = 0, 1, \ldots, p - 2 \\ j = 0, 1, \ldots, p - 1 \end{array}\right\}.$$

Since E/L is tamely ramified, we have $\mathfrak{O}_L = \mathrm{Tr}_{E/L}(\mathfrak{O}_E)$, and so $\mathfrak{O}_{L,\mathfrak{p}}$ is spanned over $\mathfrak{O}_{K,\mathfrak{p}}$ by the images of the elements of this set under the map $\mathrm{Tr} = \mathrm{Tr}_{E/L}$. Since $[F : K] = p - 1$ by lemma 3.1, we have

$$\mathrm{Tr}(\zeta^r) = \begin{cases} p - 1 & \text{if } r \equiv 0 \pmod{p} \\ -1 & \text{otherwise.} \end{cases}$$

Now for $i, j = 0, 1, \ldots p - 2$ we have

$$
\begin{aligned}
\mathrm{Tr}\left(\frac{(\alpha - 1)^j}{p}\zeta^i(1 - \zeta)^{p-1-j}\right) &= \frac{(\alpha - 1)^j}{p}\sum_{k=0}^{p-1-j}\binom{p - 1 - j}{k}\mathrm{Tr}\left(\zeta^i(-\zeta)^k\right) \\
&= \frac{(\alpha - 1)^j}{p}\left((-1)^{p-i}\binom{p - 1 - j}{p - i}p - \sum_{k=0}^{p-1-j}\binom{p - 1 - j}{k}(-1)^k\right) \\
&= (-1)^{p-i}\binom{p - 1 - j}{p - i}(\alpha - 1)^j,
\end{aligned}
$$

where we interpret the binomial coefficient $\binom{p-1-j}{p-i}$ as zero if $p - i > p - 1 - j$. The $\mathfrak{O}_{K,\mathfrak{p}}$-span of these elements is equal to the $\mathfrak{O}_{K,\mathfrak{p}}$-span of $1, \alpha, \ldots, \alpha^{p-2}$. For $i = 0, 1, \ldots, p - 2$ and $j = p - 1$ we have

$$
\mathrm{Tr}\left(\frac{(\alpha - 1)^{p-1}}{p}\zeta^i\right) = \begin{cases} (\alpha - 1)^{p-1} - \frac{(\alpha-1)^{p-1}}{p} & \text{if } i = 0 \\ -\frac{(\alpha-1)^{p-1}}{p} & \text{otherwise.} \end{cases}
$$

Therefore $\frac{(\alpha-1)^{p-1}}{p} \in \mathfrak{O}_{L,\mathfrak{p}}$ and, using the fact that $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$, we have $\frac{1}{p}(1 + \alpha + \cdots + \alpha^{p-1}) \in \mathfrak{O}_{L,\mathfrak{p}}$. Therefore the set in the proposition spans $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{O}_{K,\mathfrak{p}}$. Since this set is clearly linearly independent over $\mathfrak{O}_{K,\mathfrak{p}}$, it forms an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$. $\qquad\square$

4. THE HOPF-GALOIS STRUCTURE ON A RADICAL EXTENSION OF PRIME DEGREE

As discussed in the introduction, the extension L/K admits a unique Hopf-Galois structure. This fact is established in, for example, [4, Section 2] or [16, Theorem 3.3], but we give a self contained proof in our case for the convenience of the reader. We also establish some properties of this Hopf-Galois structure, which will be useful in what follows.

We rewrite the Galois closure of L/K as $E = K(\alpha, \zeta)$; we then have $\mathrm{Gal}(E/K) = \langle\sigma, \tau\rangle$, where $\sigma(\alpha) = \zeta\alpha$, $\sigma(\zeta) = \zeta$, $\tau(\alpha) = \alpha$, and $\tau(\zeta) = \zeta^d$ for some primitive root d modulo p. We have $\sigma^p = \tau^{p-1} = 1$ and $\tau\sigma\tau^{-1} = \sigma^d$. Let $G = \mathrm{Gal}(E/K)$, $G' = \langle\tau\rangle$, and let X denote the left coset space G/G'. By a theorem of Greither and Pareigis ([11, Theorem 2.1] or [5, Theorem 6.8]), the Hopf-Galois structures on L/K are in bijective correspondence with regular subgroups of $\mathrm{Perm}(X)$ that are normalized by the image of G under the left translation map $\lambda : G \to \mathrm{Perm}(X)$. Since $|X| = p$, any such subgroup must be cyclic of order p. We shall reformulate the problem via Byott's translation theorem ([2, Proposition 1] or [5, Theorem 7.3]): let $M = \langle\mu\rangle$ be an abstract group of order p, and recall that the *holomorph* of M is the group $\mathrm{Hol}(M) \cong M \rtimes \mathrm{Aut}(M)$; the appropriate subgroups of $\mathrm{Perm}(X)$ are then in bijective correspondence with equivalence classes of embeddings $\beta : G \hookrightarrow \mathrm{Hol}(M)$ such that $\beta(G') = \mathrm{Stab}(1_M)$, modulo conjugation by elements of $\mathrm{Aut}(M)$.

Proposition 4.1. *The extension L/K admits exactly one Hopf-Galois structure.*

Proof. Let $\theta \in \mathrm{Aut}(M)$ be defined by $\theta(\mu) = \mu^d$; it is then easy to see that $\beta : G \to \mathrm{Hol}(M)$ defined by

$$\beta(\sigma) = (\mu, 1) \text{ and } \beta(\tau) = (1, \theta)$$

is an embedding $\beta : G \hookrightarrow \mathrm{Hol}(M)$ such that $\beta(G') = \mathrm{Stab}(1_M)$. If β' is another such embedding then since $(M, 1)$ is the unique Sylow p-subgroup of $\mathrm{Hol}(M)$ we have $\beta'(\sigma) = \mu^i$ for some integer i. Similarly, since $\beta'(\tau)[1_M] = 1_M$ and τ has order $p - 1$ we have $\beta'(\tau) = (1, \theta^j)$ for some integer

j coprime to $p-1$. Now we have

$$\beta'(\tau\sigma\tau^{-1}) = \beta'(\sigma^d) = (\mu^{id}, 1),$$

but also

$$\beta'(\tau\sigma\tau^{-1}) = (1, \theta^j)(\mu^i, 1)(1, \theta^{-j}) = (\mu^{ijd}, 1).$$

Hence $j = 1$. Now let $\varphi \in \mathrm{Aut}(M)$ be defined by $\varphi(\mu) = \mu^i$. Then

$$\beta'(\sigma) = (\mu^i, 1) = \varphi(\mu, 1)\varphi^{-1} = \varphi\beta(\sigma)\varphi^{-1},$$

and (since $\mathrm{Aut}(M)$ is abelian)

$$\beta'(\tau) = (1, \theta) = \varphi(1, \theta)\varphi^{-1} = \varphi\beta(\tau)\varphi^{-1}.$$

Therefore β' and β are conjugate by an element of $\mathrm{Aut}(M)$, so there is exactly one equivalence class of suitable embeddings $\beta : G \hookrightarrow \mathrm{Hol}(M)$, and so exactly one Hopf-Galois structure on L/K. $\qquad\square$

By using elements of the proof of Byott's translation theorem, we can determine the regular subgroup of $\mathrm{Perm}(X)$ that corresponds to the unique Hopf-Galois structure on L/K:

Proposition 4.2. *Let $\eta \in Perm(X)$ be defined by $\eta(\overline{\sigma}^i) = \overline{\sigma}^{i-1}$. Then $N = \langle\eta\rangle$ is the regular subgroup of $Perm(X)$ that corresponds to the unique Hopf-Galois structure on L/K.*

Proof. Let $\beta : G \to \mathrm{Hol}(M)$ be defined by

$$\beta(\sigma) = (\mu, 1) \text{ and } \beta(\tau) = (1, \theta),$$

as in proposition 4.1. From β we obtain a bijection $b : X \to M$ defined by $b(\overline{\sigma}^i) = \beta(\sigma^i)[1_M] = \mu^i$, where $\overline{\sigma}^i = \sigma^i G'$. The map $\widehat{\beta} : M \to \mathrm{Perm}(X)$ defined by $\widehat{\beta}(\mu) = b^{-1}\lambda_M(\mu)b$ (where λ_M denotes the left regular representation of M) is then an embedding of M into $\mathrm{Perm}(X)$ whose image is regular and normalized by $\lambda(G)$, and $\widehat{\beta}(M)$ is the regular subgroup of $\mathrm{Perm}(X)$ that corresponds to β. We have:

$$\begin{aligned}
\widehat{\beta}(\mu)[\overline{\sigma}^i] &= b^{-1}[\lambda_M(\mu)b[\overline{\sigma}^i]] \\
&= b^{-1}[\lambda_M(\mu)\mu^i] \\
&= b^{-1}[\mu^{i+1}] \\
&= \overline{\sigma}^{i+1} \\
&= \eta^{-1}(\overline{\sigma}^i),
\end{aligned}$$

and so $\widehat{\beta}(M) = N$. $\qquad\square$

The theorem of Greither and Pareigis also asserts that the Hopf algebra giving the Hopf-Galois structure corresponding to N is $H = E[N]^G$, where G acts on E as Galois automorphisms and on N by conjugation via λ, viz. ${}^g\eta = \lambda(g)\eta\lambda(g)^{-1}$ for all $g \in G$.

Proposition 4.3. *We have $H \cong K^p$ as K-algebras.*

Proof. Since $\zeta \in E$ the group algebra $E[N]$ has an E-basis of mutually orthogonal idempotents

$$e_i = \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{-ik}\eta^k \text{ for } i = 0, 1, \ldots, p-1,$$

and so $E[N] \cong E^p$ as E-algebras. It is easy to verify that ${}^\sigma\eta = \eta$ and ${}^\tau\eta = \eta^d$; it follows that each idempotent e_i is fixed by each element of G, and so lies in $E[N]^G = H$. Therefore H has a K-basis of mutually orthogonal idempotents, and so $H \cong K^p$ as K-algebras. $\qquad\square$

Finally, the theorem of Greither and Pareigis implies that the action of H on L is given by

$$\left(\sum_{k=0}^{p-1} c_k \eta^k \right) \cdot x = \sum_{k=0}^{p-1} c_k \eta^{-k} [\overline{1_G}](x) = \sum_{k=0}^{p-1} c_k \overline{\sigma}^k(x) \text{ for all } x \in L.$$

Proposition 4.4. *For $i, j = 0, 1, \ldots, p-1$ we have $e_i \cdot \omega^j = \delta_{i,j} \omega^j$.*

Proof. For $i, j = 0, 1, \ldots, p-1$ we have

$$
\begin{aligned}
e_i \cdot \omega^j &= \left(\frac{1}{p} \sum_{k=0}^{p-1} \zeta^{-ik} \eta^k \right) \cdot \omega^j \\
&= \frac{1}{p} \sum_{k=0}^{p-1} \zeta^{-ik} \overline{\sigma}^k \omega^j \\
&= \frac{1}{p} \sum_{k=0}^{p-1} \zeta^{-ik} \zeta^{jk} \omega^j \\
&= \frac{1}{p} \sum_{k=0}^{p-1} \zeta^{k(j-i)} \omega^j \\
&= \delta_{i,j} \omega^j.
\end{aligned}
$$

$\square$

5. Hopf-Galois module structure

In this section we show that $\mathfrak{O}_L$ is locally free over its associated order $\mathfrak{A}$ in H, and determine a criterion for it to be free. We have previously studied the Hopf-Galois module structure of fractional ideals in tame extensions of local or global fields (see [17], [18], or [19], for example), and some of our results could be applied here: for example [17, Proposition 5.6] implies that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_\mathfrak{p}$-module for each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ that does not lie above p. However, our existing results do not apply to the prime ideals lying above p in our current situation, or construct explicit generators, which we shall require in what follows. Therefore the following proposition is necessary:

Theorem 5.1. *We have $\mathfrak{A} = \mathfrak{O}_E[N]^G$, and $\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module. For each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$, a free generator of $\mathfrak{O}_{L,\mathfrak{p}}$ as an $\mathfrak{A}_\mathfrak{p}$-module is given by*

$$
x_\mathfrak{p} = \begin{cases}
\dfrac{1}{p} \displaystyle\sum_{j=0}^{p-1} \alpha^j & \text{if } \mathfrak{p} \mid p\mathfrak{O}_K \\[2ex]
\dfrac{1}{p} \displaystyle\sum_{j=0}^{p-1} \dfrac{\alpha^j}{\pi_\mathfrak{p}^{r_\mathfrak{p}(a^j)}} & \text{otherwise.}
\end{cases}
$$

Proof. By [17, Proposition 2.5] we have $\mathfrak{O}_E[N]^G \subseteq \mathfrak{A}$. On the other hand, note that for $i = 0, 1, \ldots, p-1$ we have $pe_i \in \mathfrak{O}_E[N]^G$. We shall show that for each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ the set $\{x_\mathfrak{p}, pe_1 \cdot x_\mathfrak{p}, \ldots, pe_{p-1} \cdot x_\mathfrak{p}\}$ (with $x_\mathfrak{p}$ as defined in the proposition) is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$. This will imply that $\mathfrak{O}_L$ is a locally free $\mathfrak{O}_E[N]^G$-module, and hence that $\mathfrak{A} = \mathfrak{O}_E[N]^G$. Recall from proposition 4.4 that for $i, j = 0, 1, \ldots, p-1$ we have $e_i \cdot \alpha^j = \delta_{i,j} \alpha^j$. If $\mathfrak{p}$ lies above p then we have

$$
\begin{aligned}
1 \cdot x_\mathfrak{p} &= x_\mathfrak{p} \\
pe_i \cdot x_\mathfrak{p} &= \alpha^i \text{ for } i = 1, 2, \ldots, p-1 .
\end{aligned}
$$

Referring to proposition 3.5 we see that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{O}_{E,\mathfrak{p}}[N]^G$-module with generator $x_\mathfrak{p}$. If $\mathfrak{p}$ does not lie above p then we have

$$
\begin{aligned}
1 \cdot x_\mathfrak{p} &= x_\mathfrak{p} \\
pe_i \cdot x_\mathfrak{p} &= \frac{\alpha^i}{\pi_\mathfrak{p}^{r_\mathfrak{p}(a^i)}} \text{ for } i = 1, 2, \ldots, p-1 .
\end{aligned}
$$

Referring to proposition 3.4 and recalling that $p \in \mathfrak{O}_{K,\mathfrak{p}}^\times$ in this case, we see as above that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{O}_{E,\mathfrak{p}}[N]^G$-module with generator $x_\mathfrak{p}$. Therefore $\mathfrak{O}_L$ is a locally free $\mathfrak{O}_E[N]^G$-module, so $\mathfrak{A} = \mathfrak{O}_E[N]^G$. $\qquad\square$

To establish a criterion for $\mathfrak{O}_L$ to be a free $\mathfrak{A}$-module, we use a result of Bley and Johnston [1, Proposition 2.1]. The K-algebra H contains a unique maximal $\mathfrak{O}_K$-order $\mathfrak{M}$, which is the preimage of $\mathfrak{O}_K^p$ under the isomorphism $H \cong K^p$ constructed in proposition 4.3. Let $\mathfrak{M}\mathfrak{O}_L$ denote the smallest $\mathfrak{M}$-submodule of L that contains $\mathfrak{O}_L$. Then the result of Bley and Johnston implies that $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module if and only if

- $\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module;
- $\mathfrak{M}\mathfrak{O}_L$ is a free $\mathfrak{M}$-module, and $\mathfrak{M}\mathfrak{O}_L = \mathfrak{M} \cdot x$ for some $x \in \mathfrak{O}_L$.

Furthermore, in this case the element $x \in \mathfrak{O}_L$ is a free generator of $\mathfrak{O}_L$ as an $\mathfrak{A}$-module. We have shown in theorem 5.1 that $\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module, and so we now focus our attention on the $\mathfrak{M}$-module $\mathfrak{M}\mathfrak{O}_L$. We shall first establish a criterion for $\mathfrak{M}\mathfrak{O}_L$ to be a free $\mathfrak{M}$-module, and then turn to the question of when it has a free generator lying in $\mathfrak{O}_L$. Certainly $\mathfrak{M}\mathfrak{O}_L$ is a locally free $\mathfrak{M}$-module, and $(\mathfrak{M}\mathfrak{O}_L)_\mathfrak{p} = \mathfrak{M}_\mathfrak{p} \cdot x_\mathfrak{p}$ (with $x_\mathfrak{p}$ as defined in theorem 5.1) for each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$. The $\mathfrak{M}$-module $\mathfrak{M}\mathfrak{O}_L$ therefore defines a class in the locally free class group $\mathrm{Cl}(\mathfrak{M})$. Since H is commutative it satisfies the Eichler condition, and so $\mathfrak{M}\mathfrak{O}_L$ is a free $\mathfrak{M}$-module if and only if its class in $\mathrm{Cl}(\mathfrak{M})$ is trivial. The fact that H is commutative also implies that there is an isomorphism

$$
\mathrm{Cl}(\mathfrak{M}) \cong \frac{\mathbb{J}(H)}{H^\times \mathbb{U}(\mathfrak{M})},
$$

where $\mathbb{J}(H)$ denotes the idèle group of H, $H^\times$ denotes the subgroup of principal idèles, and $\mathbb{U}(\mathfrak{M})$ is the subgroup of unit idèles of $\mathfrak{M}$. Using the explicit generators determined in theorem 5.1, we can identify the idèle whose coset corresponds to the class of $\mathfrak{M}\mathfrak{O}_L$ in $\mathrm{Cl}(\mathfrak{M})$:

Proposition 5.2. *The class of $\mathfrak{M}\mathfrak{O}_L$ in $Cl(\mathfrak{M})$ corresponds to the coset of the idèle $(h_\mathfrak{p})_\mathfrak{p}$, where*

$$
h_\mathfrak{p} = \begin{cases} 1 & \text{if } \mathfrak{p} \mid p\mathfrak{O}_K \\ \displaystyle\sum_{j=0}^{p-1} \frac{e_j}{\pi_\mathfrak{p}^{r_\mathfrak{p}(a^j)}} & \text{otherwise} \end{cases}
$$

Proof. Let $x = \dfrac{1}{p}\displaystyle\sum_{j=0}^{p-1} \alpha^j$. Then x is a free generator of L as an H-module since by proposition 4.4 we have $e_i \cdot x = (1/p)\alpha^i$ for each i, and $\{1, \alpha, \ldots, \alpha^{p-1}\}$ is a K-basis of L. Therefore the class of $\mathfrak{O}_L$ in $\mathrm{Cl}(\mathfrak{M})$ corresponds to the idele $(h_\mathfrak{p})_\mathfrak{p}$, where for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ the element $h_\mathfrak{p} \in H_\mathfrak{p}$ is defined by $h_\mathfrak{p} \cdot x = x_\mathfrak{p}$ and $x_\mathfrak{p}$ is defined as in theorem 5.1. The result follows immediately. $\qquad\square$

Since $H \cong K^p$ and $\mathfrak{M} \cong \mathfrak{O}_K^p$, we have isomorphisms

$$\frac{\mathbb{J}(H)}{H^\times \mathbb{U}(\mathfrak{M})} \cong \left(\frac{\mathbb{J}(K)}{K^\times \mathbb{U}(\mathfrak{O}_K)} \right)^p \cong \mathrm{Cl}(\mathfrak{O}_K)^p,$$

where $\mathrm{Cl}(\mathfrak{O}_K)$ is the ideal class group of $\mathfrak{O}_K$. Explicitly, if $(h_\mathfrak{p})_\mathfrak{p} \in \mathbb{J}(H)$ then, writing $h_\mathfrak{p} = \sum_{j=0}^{p-1} z_{j,\mathfrak{p}} e_j$ with $z_{j,\mathfrak{p}} \in K_\mathfrak{p}$ for each $\mathfrak{p}$, the idéle $(h_\mathfrak{p})_\mathfrak{p}$ is then mapped to the tuple of classes of ideals

$$\left(\prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(z_{0,\mathfrak{p}})}, \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(z_{1,\mathfrak{p}})}, \ldots, \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(z_{p-1,\mathfrak{p}})} \right).$$

Using this, we obtain a criterion for $\mathfrak{M}\mathfrak{O}_L$ to be a free $\mathfrak{M}$-module in terms of certain ideals of $\mathfrak{O}_K$ being principal. Recall from section 2 that the *ideals associated* to $a\mathfrak{O}_K$ are

$$\mathfrak{b}_j = \prod_\mathfrak{p} \mathfrak{p}^{r_\mathfrak{p}(a^j)} \text{ for } 0 \le j \le p-1,$$

where $r_\mathfrak{p}(a^j) = \lfloor v_\mathfrak{p}(a^j)/p \rfloor$.

Proposition 5.3. *The $\mathfrak{M}$-module $\mathfrak{M}\mathfrak{O}_L$ is free if and only if $\mathfrak{b}_j$ is principal for all $j = 0, 1, \ldots, p-1$.*

Proof. As discussed above, $\mathfrak{M}\mathfrak{O}_L$ is a free $\mathfrak{M}$ module if and only if it has trivial class in $\mathrm{Cl}(\mathfrak{M})$, the class of $\mathfrak{M}\mathfrak{O}_L$ in $\mathrm{Cl}(\mathfrak{M})$ corresponds to the class of the idéle $(h_\mathfrak{p})_\mathfrak{p}$ defined in proposition 5.2, and this idéle corresponds to the tuple of classes of ideals

$$\left(\prod_{\mathfrak{p}|a} \mathfrak{p}^{-r_\mathfrak{p}(a^0)}, \prod_{\mathfrak{p}|a} \mathfrak{p}^{-r_\mathfrak{p}(a^1)}, \ldots, \prod_{\mathfrak{p}|a} \mathfrak{p}^{-r_\mathfrak{p}(a^{p-1})} \right) = \left(\mathfrak{b}_0^{-1}, \mathfrak{b}_1^{-1}, \ldots, \mathfrak{b}_{p-1}^{-1} \right).$$

Therefore $\mathfrak{M}\mathfrak{O}_L$ is a free $\mathfrak{M}$-module if and only if $\mathfrak{b}_j$ is principal for all $j = 0, 1, \ldots, p-1$. $\square$

Next we turn to the question of when $\mathfrak{M}\mathfrak{O}_L$ has a free generator lying in $\mathfrak{O}_L$:

Proposition 5.4. *The $\mathfrak{M}$-module $\mathfrak{M}\mathfrak{O}_L$ has a free generator lying in $\mathfrak{O}_L$ if and only if the ideals $\mathfrak{b}_j$ associated to $a\mathfrak{O}_K$ are principal, with generators $a_0, a_1, \ldots, a_{p-1} \in \mathfrak{O}_K$ such that*

$$\frac{1}{p} \sum_{j=0}^{p-1} \frac{\alpha^j}{a_j} \in \mathfrak{O}_L.$$

Proof. By proposition 5.3 $\mathfrak{M}\mathfrak{O}_L$ is a free $\mathfrak{M}$ module if and only if $\mathfrak{b}_j$ is principal for all $j = 0, 1, \ldots, p-1$. Suppose that each ideal $\mathfrak{b}_j$ is principal, say $\mathfrak{b}_j = b_j \mathfrak{O}_K$ for each $j = 0, 1, \ldots, p-1$. Then a free generator of $\mathfrak{M}\mathfrak{O}_L$ over $\mathfrak{M}$ is given by

$$x = \frac{1}{p} \sum_{j=0}^{p-1} \frac{\alpha^j}{b_j},$$

and the set of free generators for $\mathfrak{M}\mathfrak{O}_L$ as an $\mathfrak{M}$-module is precisely the set $\{z \cdot x \mid z \in \mathfrak{M}^\times\}$. Recalling that we have $\mathfrak{M} \cong \mathfrak{O}_K^p$ and $e_i \alpha^j = \delta_{i,j} \alpha^j$ for $i, j = 0, 1, \ldots, p-1$, we see that an element $y' \in L$ is a free generator for $\mathfrak{M}\mathfrak{O}_L$ as an $\mathfrak{M}$-module if and only if it has the form

$$x' = \frac{1}{p} \sum_{j=0}^{p-1} \frac{u_j \alpha^j}{b_j}$$

with $u_j \in \mathfrak{O}_K^\times$ for $j = 0, 1, \ldots, p-1$. Therefore $\mathfrak{M}\mathfrak{O}_L$ has a free generator lying in $\mathfrak{O}_L$ if and only if there are elements $u_0, u_1, \ldots, u_{p-1} \in \mathfrak{O}_K^\times$ such that the corresponding element x' lies in $\mathfrak{O}_L$. Writing $a_j = u_j^{-1} b_j$ for each j, this is equivalent to the existence of elements a_j as in the proposition. □

By combining the results of this section we obtain a criterion for $\mathfrak{O}_L$ to be a free $\mathfrak{A}$-module:

Theorem 5.5. *The ring of algebraic integers $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module if and only if there exists $\beta \in \mathfrak{O}_L$ such that*

(1) $L = K(\beta)$;
(2) $b = \beta^p \in \mathfrak{O}_K$;
(3) *the ideals associated to $b\mathfrak{O}_K$ are principal with generators b_j such that*

$$\sum_{j=0}^{p-1} \frac{\beta^j}{b_j} \equiv 0 \pmod{p\mathfrak{O}_L}.$$

Furthermore, in this case the element

$$\frac{1}{p} \sum_{j=0}^{p-1} \frac{\beta^j}{b_j}$$

is a free generator of $\mathfrak{O}_L$ as an $\mathfrak{A}$-module.

Proof. If $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module then by the result of Bley and Johnston $\mathfrak{M}\mathfrak{O}_L = \mathfrak{M} \cdot x$ for some $x \in \mathfrak{O}_L$. Therefore by proposition 5.4 the ideals associated to $a\mathfrak{O}_K$ are principal, with generators $a_0, a_1, \ldots, a_{p-1} \in \mathfrak{O}_K$ such that

$$\frac{1}{p} \sum_{j=0}^{p-1} \frac{\alpha^j}{a_j} \in \mathfrak{O}_L,$$

and so the element $\beta = \alpha \in \mathfrak{O}_L$ satisfies (1),(2), and (3). Conversely, suppose that $\beta \in \mathfrak{O}_L$ satisfies (1),(2), and (3). We follow the argument of [6, Remark 1]. Since $L = K(\beta)$, we have $\beta = \alpha^\ell c$ for some $\ell = 1, 2, \ldots, p-1$ and $c \in K$. Let t be the inverse of ℓ modulo p, and for each $j = 0, 1, \ldots, p-1$ let

$$a_j = b_{\overline{jt}} c^{-jt} a^{-\lfloor \ell jt/p \rfloor} \in \mathfrak{O}_L,$$

where $\overline{jt}$ denotes the principal remainder of jt modulo p. Then the elements a_j generate that ideals associated to $a\mathfrak{O}_K$, and there is an equality of sets

$$\{1, \beta/b_1, \ldots, \beta^{p-1}/b_{p-1}\} = \{1, \alpha/a_1, \ldots, \alpha^{p-1}/a_{p-1}\}.$$

Therefore

$$\sum_{j=0}^{p-1} \frac{\alpha^j}{a_j} = \sum_{j=0}^{p-1} \frac{\beta^j}{b_j} \equiv 0 \pmod{p\mathfrak{O}_L},$$

so by proposition 5.4 we have $\mathfrak{M}\mathfrak{O}_L = \mathfrak{M} \cdot x$ for some $x \in \mathfrak{O}_L$, and so by the result of Bley and Johnston $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module. □

Finally, we observe that the conditions appearing in this criterion are identical to those appearing in Gómez Ayala's criterion, as summarized in section 2.

6. A UNIFORM APPROACH TO THE NORMAL AND NON-NORMAL CASES

We have seen that a radical extension of number fields L/K of degree p admits a unique Hopf-Galois structure: that given by $H = K[G]$ (with $G = \mathrm{Gal}(L/K)$) if L/K is normal, and

that given by $H = E[N]^G$ (with E the Galois closure of L/K, $G = \mathrm{Gal}(E/K)$, and N as in proposition 4.2) if L/K is non-normal. In either case we have $H \cong K^p$ as K-algebras: in the normal case because K contains a primitive p^{th} root of unity; in the non-normal case by proposition 4.3. Writing $L = K(\alpha)$ for some $\alpha \in L$ such that $\alpha^p \in K$ and renumbering if necessary, the orthogonal idempotents in H then act by $e_i \cdot \alpha^j = \delta_{i,j}\alpha^j$ for $i,j = 0, 1, \ldots, p-1$. This uniformity in the K-algebra structure of H and its action on L has implications for questions of integral module structure.

Suppose that L/K is tame. Assuming that p is unramified in K in the non-normal case, we can then choose α such that $\alpha^p \equiv 1 \pmod{(\zeta - 1)^p \mathfrak{O}_K}$ if L/K is normal and $\alpha^p \equiv 1 \pmod{p^2 \mathfrak{O}_K}$ if L/K is non-normal (proposition 3.3). In either case, the ring of algebraic integers $\mathfrak{O}_L$ is locally free over its associated order in H: in the normal case by Noether's theorem and in the non-normal case by theorem 5.1. Moreover, the local generators of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_\mathfrak{p}$ are the same in both cases: for a prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ not lying above p the orthogonal idempotents in $H_\mathfrak{p}$ form an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{A}_\mathfrak{p}$ in both cases, so the appropriate parts of the proof of theorem 5.1 apply equally well to the normal and non-normal case. For $\mathfrak{p}$ lying above p a small modification to the argument of theorem 5.1 shows that the element $x_\mathfrak{p}$ defined there is also a free generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_\mathfrak{p}$ in the normal case. (Alternatively, since in the normal case $\mathfrak{A}_\mathfrak{p}$ is a local Hopf order for such $\mathfrak{p}$, we could deduce this from the Childs-Hurley criterion: see [5, Theorem 14.7].)

Given that $\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module in both case, the result of Bley and Johnston [1, Proposition 2.1] implies that it is a free $\mathfrak{A}$-module if and only if $\mathfrak{M}\mathfrak{O}_L$ is a free $\mathfrak{M}$-module with a generator lying in $\mathfrak{O}_L$ (where $\mathfrak{M}$ denotes the unique maximal order in H). But we have $\mathfrak{M} \cong \mathfrak{O}_K^p$ via orthogonal idempotents in both cases, and for each $\mathfrak{p}$ the element $x_\mathfrak{p}$ defined in theorem 5.1 is a free generator of $(\mathfrak{M}\mathfrak{O}_L)_\mathfrak{p}$ as an $\mathfrak{M}_\mathfrak{p}$-module. Therefore all of the arguments in section 5 involving the idélic description of $\mathrm{Cl}(\mathfrak{M})$ and the idéle corresponding to the class of $\mathfrak{M}\mathfrak{O}_L$ apply equally well in both cases, which explains why the criterion we obtained in theorem 5.5 is identical to that obtained by Gómez Ayala.

References

[1] Bley W, Johnston H. *Computing generators of free modules over orders in group algebras.* Journal of Algebra. 2008; 320(2):836-52.

[2] Byott NP. *Uniqueness of Hopf Galois structure for separable field extensions.* Communications in Algebra. 1996; 24(10):3217-28.

[3] Byott NP. *Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications.* Journal de Théorie des Nombres de Bordeaux.1997; 9(1):201-19.

[4] Childs LN. *On the Hopf Galois theory for separable field extensions.* Communications in Algebra. 1989; 17(4):809-25.

[5] Childs L. *Taming wild extensions: Hopf algebras and local Galois module theory.* American Mathematical Soc. 2000.

[6] Del Corso I, Rossi LP. *Normal integral bases for cyclic Kummer extensions.* Journal of Pure and Applied Algebra. 2010; 214(4):385-91.

[7] Elder GG. *Ramified extensions of degree p and their HopfGalois module structure.* Journal de Théorie des Nombres de Bordeaux. 2018; 30(1):19-40.

[8] Fröhlich A. *Galois module structure of algebraic integers.* Springer: New York. 1983.

[9] Fröhlich A, Taylor MJ. *Algebraic number theory.* Cambridge University Press. 1993

[10] Gómez Ayala EJ. *Bases normales d'entiers dans les extensions de Kummer de degré premier.* Journal de Théorie des Nombres de Bordeaux. 1994; 6:95-116.

[11] Pareigis B, Greither C. *Hopf Galois theory for separable field extensions.* Journal of Algebra. 1987; 1:239-58.

[12] Hecke E, Goldman JR, Kotzen R. *Lectures on the theory of algebraic numbers.* Springer: New York. 1981.

[13] Ichimura, H. *On the ring of integers of a tame Kummer extension over a number field.* Journal of Pure and Applied Algebra. 2004; 187:169-182.

[14] Ichimura, H. *Note on Galois descent of a normal integral basis of a cyclic extension of degree p.* Proc. Japan Acad. 2009; 85 Ser. A: 160-162.

[15] Koch A. *Scaffolds and integral Hopf Galois module structure on purely inseparable extensions.* New York J. Math. 2015; (21):73-91.

[16] Kohl T. *Classification of the Hopf Galois structures on prime power radical extensions.* Journal of Algebra. 1998; 207(2):525-46.

[17] Truman PJ. *Towards a generalisation of Noethers theorem to nonclassical HopfGalois structures.* New York J. Math. 2011; 17:799-810.

[18] Truman PJ. *Integral HopfGalois structures for tame extensions.* New York J. Math. 2013; 19:647-55.

[19] Truman PJ. *Commutative HopfGalois module structure of tame extensions.* Journal of Algebra. 2018; 503:389-408.

School of Computing and Mathematics, Keele University, Staffordshire, ST5 5BG, UK
E-mail address: P.J.Truman@Keele.ac.uk