TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 304, Number 1, November 1987

# TAMING WILD EXTENSIONS WITH HOPF ALGEBRAS

LINDSAY N. CHILDS

ABSTRACT. Let $K \subset L$ be a Galois extension of number fields with abelian Galois group $G$ and rings of integers $R \subset S$, and let $\mathscr{A}$ be the order of $S$ in $KG$. If $\mathscr{A}$ is a Hopf $R$-algebra with operations induced from $KG$, then $S$ is locally isomorphic to $\mathscr{A}$ as $\mathscr{A}$-module. Criteria are found for $\mathscr{A}$ to be a Hopf algebra when $K = \mathbf{Q}$ or when $L/K$ is a Kummer extension of prime degree. In the latter case we also obtain a complete classification of orders over $R$ in $L$ which are tame or Galois $H$-extensions, $H$ a Hopf order in $KG$, using a generalization of the discriminant.

Galois module theory seeks to describe the ring of integers $S$ of a Galois extension $L \supset K$ of number fields with Galois group $G$ as a $G$-module, either absolutely (i.e. over $ZG$) or relatively (i.e. over $RG$, $R$ the ring of integers of $K$). In the relative case, the fundamental result is Noether's theorem: $S$ is locally $RG$-isomorphic to $RG$, that is, $S$ has a normal basis locally at each prime of $R$, if and only if $L/K$ is tame, i.e. tamely ramified.

However, nontame extensions $L/K$ abound (e.g. $K = Q$, $L = Q(\sqrt{m})$, $m \equiv 2$ or $3 \pmod 4$, or $L = Q(\zeta)$, $\zeta$ a primitive $m$th root of unity, $m$ not square-free). In attempting to extend the tame results to nontame extensions, one approach, introduced by H. W. Leopoldt [**17**] and studied by H. Jacobinski [**15**], F. Bertrandias, J.-P. Bertrandias and M. J. Ferton [**2, 3, 4**], A. M. Berge [**1**], and recently, M. Taylor [**24, 28**], is to replace $RG$ by a larger order over $R$ in $KG$, in particular, the order $\mathscr{A}$ of $S$ in $KG$.

$$\mathscr{A} = \{\alpha \in KG \mid \alpha S \subseteq S\},$$

and consider $S$ as an $\mathscr{A}$-module. For $K = Q$ this approach was successful: $S \cong \mathscr{A}$ as $\mathscr{A}$-module when $G = \mathrm{Gal}(L/Q)$ is abelian. However, in [**2** and **3**] it is shown that $S \cong \mathscr{A}$ as $\mathscr{A}$-module may fail, even locally, if $G$ is dihedral or if $L/K$ is a Kummer extension of prime degree.

This paper starts from the premise that it is of interest to know when $\mathscr{A}$ is a Hopf $R$-algebra with operations induced from those on the Hopf $K$-algebra $KG$ (abusing language we henceforth call such an $\mathscr{A}$ a Hopf subalgebra of $KG$). There are several reasons for investigating such a premise.

In general, as Bergman [**29**] has eloquently explained, for an algebra $A$ to act on another algebra $S$ and to respect the algebra structure of $S$, it is natural for $A$ to be

Received by the editors April 11, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R33, 13B05, 16A24; Secondary 11S15.

at least a bialgebra. For to describe how $A$ respects the unit map and the multiplication on $S$, it is necessary for $A$ to act on $R$ and on $S \otimes S$, and a natural way to define such actions is via maps $\varepsilon\colon A \to R$ and $\Delta\colon A \to A \otimes A$ which make $A$ into a bialgebra. In applying this general observation to $\mathscr{A}$, to require that $\mathscr{A}$ be a Hopf algebra, not just a bialgebra, is to require that $\mathscr{A}$ be closed under the inverse map, or antipode, of $KG$.

Asking when $\mathscr{A}$ is a Hopf algebra may be of intrinsic geometric interest. For if so, setting $Y = \mathrm{Spec}(S)$, $X = \mathrm{Spec}(R)$, then $Y$ is acted upon by $\mathbf{A} = \mathrm{Spec}(\mathscr{A}^*)$, the Cartier dual over $X$ of the affine group scheme represented by $\mathscr{A}$, and $\mathbf{A}$ may be a more natural group scheme of operators on $Y$ than is

$$\mathbf{G} = \mathrm{Spec}\big((RG)^*\big).$$

Perhaps of most interest, however, is that fact that part of Noether's theorem may be recast as: if $\mathscr{A} = RG$, then locally $S \cong \mathscr{A}$ as $\mathscr{A}$-module; and in this formulation the result can be generalized, at least for $G$ abelian, to the case where $\mathscr{A}$ is an arbitrary Hopf subalgebra of $KG$. The proof of this, given in §4, is an almost immediate application of one of the main results in **[9]**, which characterizes, for $H$ cocommutative, the condition that there exist local normal bases for an object $S$ of a Hopf $R$-algebra $H$ in terms of a criterion for "tameness" which directly generalizes the criterion for tame ramification that the image of the trace map on $S$ be all of $R$.

Thus in the wild case, when the order $\mathscr{A}$ of $S$ in $KG$, $G$ abelian, is a Hopf subalgebra of $KG$, the wild $RG$-extension $S$ becomes a tame $\mathscr{A}$-extension and has local normal basis at every prime of $R$. This result is a rare example of a general local normal basis criterion for wild extensions of arbitrary number fields $K$.

The main body of the paper is an investigation, for the simplest abelian extensions, cyclotomic extensions of $Q$ and Kummer extensions of prime order, of conditions for which $\mathscr{A}$ is a Hopf subalgebra of $KG$.

When $K = Q$, the example of $L = Q(\sqrt{m})$, $m \not\equiv 1 \pmod 4$, for which $\mathscr{A} \cong (ZG)^*$, the dual of $ZG$, is almost the only possible example. In general, for $K = Q$, $L$ an abelian extension of $Q$, $\mathscr{A}$ is a Hopf subalgebra of $QG$ if and only if every odd prime is tamely ramified, and the first ramification group of $L/Q$ at the prime 2 has order at most 2. The main obstacle is that the idempotents occurring in $\mathscr{A}$ which correspond to ramification groups of $L/Q$ of order $> 2$ are not sent to $\mathscr{A} \otimes \mathscr{A}$ by the comultiplication on $KG$.

For Kummer extensions $L/K$ of prime order $l$, we find several equivalent conditions for $\mathscr{A}$ to be a Hopf subalgebra of $KG$, involving a congruence condition on a Kummer generator of $L$, a condition on the ramification numbers of $L/K$ at primes dividing $l$, and a trace condition. This latter condition is that $\mathscr{A}$ is Hopf if and only if $\mathrm{tr}(S)$ is the $(l-1)$th power of an ideal of $R$. The analysis of when $\mathscr{A}$ is a Hopf algebra utilizes Tate and Oort's classification of group schemes of order $l$ over rings of integers; in particular, if $\mathscr{A}$ is a Hopf algebra, then $\mathscr{A} = H_{\mathscr{B}}$, the Hopf algebra corresponding to the ideal $\mathscr{B}$ with $\mathscr{B} \cdot \mathrm{tr}(S) = lR$.

The determination of when $\mathscr{A}$ is a Hopf algebra is entirely a local question at completions of $K$, and is nontrivial only at primes $p$ dividing $l$ at which $L/K$ is totally ramified and $\not\cong$ $(R_pG)^*$. Our approach in the prime order Kummer case is to find all the Hopf subalgebras of $\mathscr{A}_p$, using the Tate-Oort theory, and then look for Galois extensions with respect to these Hopf algebras (an $H$-Galois extension $S$ with $S^H = R$ is an $H^*$-Galois object in the sense of Chase and Sweedler [7]). We show that to each Hopf subalgebra of $\mathscr{A}$ there corresponds a unique Galois extension which is a suborder of $S \otimes_R R_p$ in $L \otimes K_p$, and then determine when $S \otimes R_p$ itself is such a Galois extension whose Hopf algebra is $\mathscr{A}$. To do this we develop a general codifferent criterion for an $H$-extension, $H$ a Hopf algebra, to be Galois, based on the integral $I$ of $H$, which yields a generalization of the classical discriminant criterion for $H = RG$, and also yields a Galois-theoretic proof of Larson and Sweedler's theorem that if $H$ is a finite, unimodular Hopf algebra, then $H^* \cong H \otimes I$ as $H$-modules [**16**], and a proof of Pareigis' Frobenius criterion for Hopf algebras [**19**]. A by-product of the development is to give a complete local, then global classification of Hopf Galois extensions, and also tame $H$-extensions, which are orders over $R$ in Kummer extensions of $K$ of prime order. In particular, we show that there are orders over $R$ in $L$ which are Galois $H$-extensions for some $H$ if and only if the Kummer order $\tilde{S}$ is a Galois $(RG)^*$-extension, in which case the Galois $H$-extensions are in 1-1 correspondence with ideals of $R$ which are $(l-1)$th powers and contain $(lR)(\mathrm{tr}(S))^{-1}$.

Throughout the paper, $L \supset K$ is a Galois extension of number fields, the Galois group $\mathrm{Gal}(L/K) = G$, and $O_K$, $O_L$ are the rings of integers of $K$, $L$, respectively.

**1. Hopf algebras and their algebras.** Hopf algebras (over a commutative ring $R$) as considered in this paper are in the sense of Sweedler [**22**], that is, $H$ is a Hopf $R$-algebra if it is an $R$-bialgebra with antipode. A Hopf $R$-algebra $H$ is finite if it is a finitely generated projective $R$-module [7, p. 55]. Throughout this paper, all Hopf algebras will be assumed finite. We denote the multiplication, unit, comultiplication, counit and antipode of $H$ by $\mu$, $i$, $\Delta$, $\varepsilon$, and $\lambda$, respectively.

If $H$ is a Hopf $R$-algebra, the space of (left) integrals $I$ of $H$ is the set

$$I = (x \in H \mid yx = \varepsilon(y)x \text{ for all } y \text{ in } H).$$

Let $S$ be an $R$-algebra, finitely generated and projective as $R$-module, and $H$ a Hopf algebra. Then $S$ is an $H$-module algebra [**22**] if $S$ is acted on by $H$ via a measuring. If $S$ is an $H$-module algebra, then the action $H \otimes S \to S$ induces a comodule map $\alpha\colon S \to S \otimes H^*$ which is an $R$-algebra homomorphism [**7**, p. 55]; $S$ is then an $H^*$-object. Conversely, if $S$ is an $H$-object, $S$ is an $H^*$-module algebra.

If $S$ is a $H$-module algebra, the fixed ring is

$$S^H = \{s \in S \mid \xi s = \varepsilon(\xi)s \text{ for all } \xi \text{ in } H\}.$$

We have $IS \subseteq S^H$ for $S$ any $H$-module algebra. We call $S$ an $H$-extension of $R$ if $S^H = R$ and $S$ is an $H$-module algebra.

Let $H$, $J$ be finite Hopf algebras which are dual: $H^* \cong J$, $J^* \cong H$, and $S$ an $R$-algebra, finitely generated and projective as $R$-module, then $S$ is a Galois $H$-extension of $R$ if $S$ is a Galois $J$-object in the sense of [7], and $S$ is a tame $H$-extension of $R$ if $S$ is a tame $J$-object in the sense of [**9**]. We recall these definitions.

DEFINITION 1.1. The $R$-algebra $S$ is a Galois $J$-object if $S$ is a $J$-object via $\alpha$: $S \to S \otimes J$, and the map $\gamma$: $S \otimes S \to S \otimes J$ given by $\gamma(x \otimes y) = (x \otimes 1)\alpha(y)$, is an isomorphism.

$S$ is a tame $J$-object if $S$ is an $H$-module algebra, $H = J^*$, faithful as $H$-module, $\operatorname{rank}_R(S) = \operatorname{rank}_R(H)$ as projective $R$-modules, and for $I =$ the space of integrals of $H$, $IS = S^H = R$.

A Galois $J$-object is a tame $J$-object, by [**9**, (2.3)]. An $H$-extension $S$ of $R$ has normal basis if $S \cong H^*$ as $H$-module, and has local normal basis if for any prime ideal $p$ of $R$, $S_p \cong H_p^*$ as $H_p$-module.

Let $L \supset K$ be a Galois extension of number fields with Galois group $G$, abelian. Let $H$ be a Hopf $O_K$-algebra which is an order over $O_K$ in $KG$. If $O_L$ is an $H$-extension of $O_K$, then the criteria for $O_L$ to be a tame $H$-extension reduce to the single condition $IO_L = O_K$, the analogue for $H$ of the condition, for $H = O_KG$, that the trace map: $O_L \to O_K$ be surjective [**9**]. Thus for abelian extensions of number fields, $O_L$ is a tame $O_KG$-extension if and only if $L/K$ is tamely ramified.

The main theorem of [**9**] is that the $H$-extension $O_L \supset O_K$ has local normal basis if and only if $IO_L = O_K$, $I$ the space of integrals of $H$. Thus determining that $O_L$ is a tame $H$-extension of $O_K$ for some Hopf algebra $H$ yields useful information on the local structure of $O_L$.

**2. The order of $O_L$.** Let $L \supset K$ be an abelian Galois extension of number fields with Galois group $G$. Following Leopoldt [**17**], let

$$\mathscr{A} = \{\alpha \in KG \mid \alpha O_L \subseteq O_L\},$$

the order of $O_L$ in $KG$, and set $\mathscr{A}^* = \operatorname{Hom}_{O_K}(\mathscr{A}, O_K)$. In [**17**], Leopoldt proved that if $K = Q$, $O_L$ is always a free $\mathscr{A}$-module; on the other hand, F. and J. P. Bertrandias and M. Ferton [**3, 4**] have shown that $O_L$ need not be locally free over $\mathscr{A}$ for $L \supset K$ a Kummer extension of prime order.

One reason for interest in knowing if $\mathscr{A}$ is a Hopf algebra is:

THEOREM 2.1. *Let $L \supset K$ be an abelian extension of number fields with Galois group $G$. Suppose $\mathscr{A}$, the order of $O_L$ in $KG$, is a Hopf subalgebra of $KG$. Then $O_L$ is a tame $\mathscr{A}$-extension of $O_K$ and is locally isomorphic to $\mathscr{A}$ as $\mathscr{A}$-module.*

PROOF. Suppose $\mathscr{A}$ is a Hopf algebra. Let $R = O_K$, $S = O_L$. By [**9**, Theorem 5.4], $O_L$ is locally isomorphic to $\mathscr{A}^*$ as $\mathscr{A}$-module if and only if $IS = R$ where $I$ is the space of integrals of $\mathscr{A}$. Since $\mathscr{A}^*$ is locally isomorphic to $\mathscr{A}$ as $\mathscr{A}$-module if $\mathscr{A}$ is a Hopf algebra (see e.g. [**19**] or Corollary 10.4 below), it suffices to show $IS = R$, a local question. So assume $R$ is local. Let $\operatorname{tr} = \sum_{\sigma \in G} \sigma$, then if $\operatorname{tr}(S) = aR$ ($R$, being local, is a discrete valuation ring), $\theta = \operatorname{tr}/a$ maps $S$ onto $R$. Thus $\theta \in \mathscr{A}$. Since $\mathscr{A}$ is a Hopf subalgebra of $KG$ and tr is an integral of $KG$, $\theta$ is an integral of $\mathscr{A}$. Thus $IS = R$.

**3. Tate-Oort algebras.** In most of this paper we study extensions of number fields $L \supset K$ which are cyclic of prime order $l$ with Galois group $G$ with generator $\sigma$, where $K$ contains a primitive $l$th root of unity $\zeta$. The Hopf algebras which arise are finitely generated projective $O_K$-modules of rank $l$ which are orders over $O_K$ in $KG$. These have been classified by Tate and Oort [**23**], and are completely determined by their local structure at completions of $O_K$ and at $K$ [**23**, Lemma 4].

Let $K_{\mathfrak{p}}$ be the completion of $K$ at a (finite) prime $\mathfrak{p}$, $R$ the valuation ring. If $\mathfrak{p} \cap Z \neq (l)$, then the only Hopf $R$-algebra of interest is the group ring $RG$, which, since $R$ contains $1/l$ and $\zeta$, is isomorphic to $\operatorname{Hom}_R(RG, R) = (RG)^*$.

The local structure of the Tate-Oort Hopf algebras when $\mathfrak{p} \cap Z = (l)$, involves certain constants $\omega_1, \ldots, \omega_l$, obtained as follows.

Let $\chi\colon F_l \to Z_l \subseteq R$ be the unique multiplicative section of the residue class map $Z_l \to F_l$ [**17**, p. 44]. In $RG$, let

$$\text{(3.1)} \qquad \begin{aligned} \theta_i &= -\sum_{m \in \mathbf{F}_l^*} \chi^i(m)\sigma^m, \qquad i = 1, \ldots, l-2, \\ \theta_{l-1} &= l - \sum_{j=0}^{l-1} \sigma^j \end{aligned}$$

[**23**, p. 9]. Then $\theta_1^i = \omega_i\theta_i$, $i = 1, \ldots, l-1$, and $\theta_1^l = \omega_l\theta_1$, for some elements $\omega_1, \ldots, \omega_l$, of $R$, where $\omega_1 = 1$, $\omega_2, \ldots, \omega_{l-1}$ are units of $R$, and $\omega_l = l\omega_{l-1}$. (See [**23**, formula (17)] for an inductive definition of the $\omega_i$.)

Let $H$ be a Hopf $R$-algebra, free as an $R$-module of rank $l$. Then [**23**, p. 14] there exist $a$, $b$ in $R$, $ab = \omega_l$, such that $H = R[\xi]$ where $\xi^l = b\xi$ as $R$-algebra, and the comultiplication $\Delta\colon H \to H \otimes H$ is given by

$$\Delta(\xi^i) = 1 \otimes \xi^i + \xi^i \otimes 1 + \frac{\omega_i}{1-l}\left[\sum_{j=1}^{i-1} \frac{\xi^j}{\omega_j} \otimes \frac{\xi^{i-j}}{\omega_{i-j}} + \sum_{j=i}^{l-1} a\frac{\xi^j}{\omega_j} \otimes \frac{\xi^{(l-1)+(i-j)}}{\omega_{(l-1)+(i-j)}}\right],$$

the counit $\varepsilon\colon H \to R$ by $\varepsilon(\xi^i) = 0$ for $i > 0$, and the antipode $\lambda\colon H \to H$ by $\lambda(\xi) = -\xi$. The Hopf algebra $H$ is thus defined by the constants $a$ and $b$, which satisfy $ab = \omega_l$. If $p = 2$, $\lambda(\xi) = \xi$.

Denote the Hopf algebra $H = R[\xi]$, $\xi^l = b\xi$, by $H_b$.

With this notation, $RG = H_{\omega_l}$, $(RG)^* = H_1$.

The identification $RG = H_{\omega_l} = R[\theta]$, $\theta^l = \omega_l\theta$, is given by (3.1) and by

$$\text{(3.2)} \qquad \sigma^m = 1 + \frac{1}{1-l}\left(\sum_{i=1}^{l-1} \frac{\chi^i(m)}{\omega_i}\theta^i\right) \quad \text{for } m = 1, \ldots, l-1.$$

(cf. [**23**, p. 15, Remark 5]). There is an inclusion $H_b \subseteq H_{b'}$ if and only if there is an element $u$ of $R$ such that $u^{l-1}b' = b$, in which case the map is given as follows: if $H_b = R[\xi]$, $H_{b'} = R[\xi']$, then $\xi \mapsto u\xi'$: $(u\xi')^l = u^l b'\xi' = b(u\xi')$.

Whenever $\zeta \in R$, $RG \cong (RG)^*$, so $\omega_l$ has an $(l-1)$th root $\tilde{\omega}_l$ in $R$. In general, the Hopf algebra $H_b$, $b \neq 0$ is a subalgebra of $KG$ if and only if $H_b \otimes K \cong KG \cong (KG)^* \cong H_1 \otimes K$, if and only if $b$ has an $(l-1)$th root $\tilde{b}$ in $R$. In case $\tilde{b}$ exists, so does $\tilde{a} = \tilde{\omega}_l/\tilde{b}$, and so from $\tilde{a}^{l-1}b = \omega_l$ and $\tilde{b}^{l-1} \cdot 1 = b$ and (3.2) we obtain inclusions

$$RG = H_{\omega_l} \subseteq H_b \subseteq H_1 = (RG)^*.$$

PROPOSITION 3.3. *Let $K$ be a local or global algebraic field containing a primitive $l$th root of unity $\xi$, and let $R$ be the ring of integers of $k$. Then the set of isomorphism classes of Hopf $R$-algebras contained in $KG$, $G$ cyclic of order $l$, is in* 1-1 *lattice-preserving correspondence with the set of ideals dividing $lR$ which are $(l-1)$th powers.*

PROOF. If $H$ is a Hopf $R$-algebra of rank $l$, then $H$ is uniquely determined by its images at completions of $R$. Let $\mathfrak{p}$ be a prime divisor of $lR$ and $R_{\mathfrak{p}}$, $K_{\mathfrak{p}}$ be the completions of $R$, $K$ at $\mathfrak{p}$, respectively. Then $H \otimes_R R_{\mathfrak{p}} = H_b$ for $b$ some divisor of $lR = (1-\xi)^{l-1}R = \mathfrak{p}^{(l-1)e}$. Since $H_b \subseteq K_{\mathfrak{p}}G$, $b$ is an $(l-1)$th power, so $bR = \mathfrak{p}^{(l-1)s}$ for some $s$, $0 \leqslant s \leqslant e$. If $l \notin \mathfrak{p}$ then $H \otimes_R R_{\mathfrak{p}} = R_{\mathfrak{p}}G \cong (R_{\mathfrak{p}}G)^* = H_1$, so $e = 0$. Thus to $H$ corresponds the ideal $\mathscr{B} = \prod_{\mathfrak{p}|l} \mathfrak{p}^{(l-1)s}$. The lattice-preserving property follows from (3.2).

NOTATION. (3.4). Denote by $H_{\mathscr{B}}$ the Hopf subalgebra of $KG$ corresponding to the ideal $\mathscr{B}$ of $O_K$. If $\mathscr{B} = \ell^{l-1}$, for each prime ideal $\mathfrak{p}$ of $O_K$, $H_{\mathscr{B}} \otimes_{O_K} \hat{O}_{K,\mathfrak{p}} = H_b$ where $b$ is the $(l-1)$th power of a generator of $\ell \otimes_{O_K} \hat{O}_{K,\mathfrak{p}}$

(3.5) For $H = H_b = R[\xi]$, the space of integrals $I$ is the free $R$-module generated by $b - \xi^{l-1}$, as is easily checked. In $KG$, $b - \xi^{l-1}$ has a familiar look: if $RG = H_{\omega_l} = R[\theta]$, $\theta = \tilde{a}\xi$, so

$$\xi^{l-1} = \frac{1}{a}\theta^{l-1} = \frac{1}{a}\omega_{l-1}\theta_{l-1}$$
$$= \frac{1}{a}\omega_{l-1}\left(l - \sum_{j=0}^{l-1}\sigma^j\right) \quad \text{(from (3.1))}$$

and so

$$b - \xi^{l-1} = \frac{\omega_{l-1}}{a}\sum_{j=0}^{l-1}\sigma^j = \frac{b}{l}\sum\sigma^j.$$

Of course $\sum_{j=0}^{l-1}\sigma^j$ generates the space of integrals of $RG$.

We will denote $\sum_{\sigma\in G}\sigma = \mathrm{tr}$ since the action of tr on an $RG$-module gives the trace map.

**4. The quadratic case.** Every quadratic extension is tame. While this will follow as a special case of later results, we give here a short direct argument.

THEOREM 4.1. *Let $R$ be a Dedekind domain with quotient field $K$, let $L$ be a quadratic field extension of $K$ with Galois group $G = \langle\sigma\rangle$ of order 2. Let $S$ be the integral closure of $R$ in $L$. Suppose* $\mathrm{tr}(S) = aR$, *a principal ideal of $R$. Then $S$ is a tame $H_b$ extension, $b = 2/a$, and $H_b = \{\alpha \in KG \mid \alpha S \subseteq S\}$.*

PROOF. First we note that $a$ divides 2, since $\mathrm{tr}(1) = 2$ is in $aR$. So $RG = H_2 \subseteq H_b = R[\xi]$ by $\xi = (1-\sigma)/a$, $\sigma = 1 - a\xi$.

First, $H_b$ acts on $S$. For suppose $s$ is in $S$, $\mathrm{tr}(s) = ar$. Then $(\sigma+1)s = ar$ for some $r$ in $R$, so $\sigma(s) = ar - s$, and $\xi s = ((1-\sigma)/a)s = bs - r$, thus $H_bS \subseteq S$.

The space of integrals $I$ of $H$ is generated by $b - \xi = 2/a - ((1-\sigma)/a) = (\sigma+1)/a$, and if $\mathrm{tr}(s) = a$, then $((\sigma+1)/a)s = 1$. So $IS = R$, and $S$ is a tame $H_b$-module algebra.

Let $\mathscr{A} = \{\alpha \in KG \mid \alpha S \subset S\}$. Since $\mathscr{A}S \subseteq S$, $\mathscr{A}$ is integral over $R$, so $\mathscr{A} \subseteq (RG)^* = H_1 = R[y]$, $y^2 = y$. Further, $H_b \subseteq H_1$ by $\xi = by$. So any $\alpha$ in $\mathscr{A}$ has the form $\alpha = m + n(\xi/b)$, $m$, $n$ in $R$. Let $s$ be in $S$, not in $R$, with $\mathrm{tr}(s) = a$. If $\alpha$ is in $\mathscr{A}$, then

$$\begin{aligned}(m + n(\xi/b))(s) &= ms + n\xi s/b \\ &= ms + n(bs - 1)/b \\ &= ms + ns - n/b \quad \text{is in } S,\end{aligned}$$

and so $n/b$ is in $R$. But then $\alpha = m + n(\xi/b) = m + (n/b)\xi$ is in $R[\xi] = H_b$, and $\mathscr{A} \subseteq H_b$. That completes the proof.

COROLLARY 4.2. *If $L \supset K$ is any quadratic extension of number fields, then there is an $O_K$-Hopf algebra $H$ such that $O_L$ is a tame $H$-module algebra.*

If $\mathrm{tr}(O_L)$ is a principal ideal of $O_K$ this is immediate from (4.1). In general, this follows from the proof of Theorem 4.1, used as a local argument (see §17, below).

EXAMPLES. Let $K = Q$, $L = Q(\sqrt{d})$, $d$ square-free. Then $O_L$ is a tame $H_b$-module algebra, where

$$\begin{cases} b = 2\ (H_b = RG) & \text{if } d \equiv 1 \pmod 4, \\ b = 1\ \big(H_b = (RG)^*\big) & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

For $K \neq Q$, numerous examples of quadratic extensions $L \supset K$ for which $O_L$ is a Galois, hence tame $H_b$-module algebra, for $H_b \neq O_K G$ or its dual, are described in **[8]**.

**5. Absolutely abelian extensions.** In this section we show that unless the abelian extension $L \supset Q$ is tamely ramified except possibly at the prime 2, and then only with ramification group cyclic of order $\leqslant 2$, the ring of integers $O_L$ of $L$ is not tame for any $Z$-Hopf subalgebra of $QG$, $G = \mathrm{Gal}(L/Q)$.

THEOREM 5.1. *Let $G$ be a finite abelian group, and let $\mathscr{A}$ be an order over $Z$ in $QG$ generated by $ZG$ and, for each prime $p$ dividing the order of $G$, an idempotent*

$$e_p = \frac{1}{|G_p|} \sum_{\sigma \in G_p} \sigma \qquad \big(|G_p| = \textit{order of } G_p\big)$$

*corresponding to some (possibly trivial) $p$-subgroup $G_p$ of $G$. Then $\mathscr{A}$ is a Hopf subalgebra of $QG$ if and only if $|G_2| \leqslant 2$ and $G_p$ is trivial for all odd $p$.*

PROOF. Suppose $m = |G_p| > 2$ for some $p$, and fix $\pi, \rho \neq 1$ in $G_p$. Now in $QG$,

$$\Delta e_p = \frac{1}{m} \sum_{\sigma \in G_p} \sigma \otimes \sigma.$$

Since $\mathscr{A}$ is generated over $Z$ by elements of $G$ and idempotents $e_q$ for $q$ dividing the order of $G$, $\Delta e_p$ is in $\mathscr{A} \otimes \mathscr{A}$ if and only if $\Delta e_p$ is a $Z$-linear combination of the generators $\sigma \otimes \tau$, $\sigma \otimes e_{q'} e_q \otimes \tau$, and $e_q \otimes e_{q'}$ in $\mathscr{A} \otimes \mathscr{A}$, for $\sigma$, $\tau$ in $G$ and $q$, $q'$ running through prime divisors of the order of $G$.

We suppose we can write $\Delta e_p$ as such a $Z$-linear combination, and (in $QG \otimes QG$) collect the coefficients of $\pi \otimes \pi$, $\pi \otimes \rho$, $\rho \otimes \pi$, $\rho \otimes \rho$. Since $\pi, \rho \neq 1$ in $G$, the only generators of $\mathscr{A} \otimes \mathscr{A}$ which contribute nonzero coefficients are the generators $\pi \otimes \pi$, $\pi \otimes \rho$, $\rho \otimes \pi$ and $\rho \otimes \rho$ themselves, together with $e_p \otimes \pi$, $e_p \otimes \rho$, $\pi \otimes e_p$, $\rho \otimes e_p$, and $e_p \otimes e_p$. (The nonidentity terms in $e_q$, $q \neq p$, lie in $G_q$, and $G_q \cap G_p = (1)$.)

We write

$$\Delta e_p = \frac{1}{m} \sum_{\sigma \in G_p} \sigma \otimes \sigma = a_{0,0} e_p \otimes e_p + \sum_{\sigma \in G_p} a_{\sigma,0} \sigma \otimes e_p$$
$$+ \sum_{\tau \in G_p} a_{0,\tau} e_p \otimes \tau + \sum_{\sigma, \tau \in G_p} a_{\sigma,\tau} \sigma \otimes \tau$$
$$+ \left(\text{other terms not containing } \sigma \otimes \tau \text{ for } \sigma, \tau \neq 1 \text{ in } G_p\right),$$

with all coefficients in $Z$. Then, collecting coefficients of $\pi \otimes \pi$:

$$\frac{1}{m} = \frac{1}{m^2} a_{0,0} + \frac{1}{m} a_{\pi,0} + \frac{1}{m} a_{0,\pi} + a_{\pi,\pi} \tag{5.2}$$

of $\pi \otimes \rho$:

$$0 = \frac{1}{m^2} a_{0,0} + \frac{1}{m} a_{\pi,0} + \frac{1}{m} a_{0,\rho} + a_{\pi,\rho} \tag{5.3}$$

of $\rho \otimes \pi$:

$$0 = \frac{1}{m^2} a_{0,0} + \frac{1}{m} a_{\rho,0} + \frac{1}{m} a_{0,\pi} + a_{\rho,\pi} \tag{5.4}$$

of $\rho \otimes \rho$:

$$\frac{1}{m} = \frac{1}{m^2} a_{0,0} + \frac{1}{m} a_{\rho,0} + \frac{1}{m} a_{0,\rho} + a_{\rho,\rho}. \tag{5.5}$$

Multiplying the four equations by $m$ and taking the differences (5.2)–(5.3) and (5.4)–(5.5), yields

$$1 = (a_{0,\pi} - a_{0,\rho}) + m(a_{\pi,\pi} - a_{\pi,\rho}),$$
$$-1 = (a_{0,\pi} - a_{0,\rho}) + m(a_{\rho,\pi} - a_{\rho,\rho}),$$

impossible if $m > 2$. Thus $\Delta e_p$ is not in $\mathscr{A} \otimes \mathscr{A}$ if $|G_p| > 2$. Since $G_p$ is a $p$-group, if $\mathscr{A}$ is a Hopf subalgebra of $QG$ we must have $G_p = (1)$ if $p$ is odd, and $|G_2| \leqslant 2$.

Conversely, if $\mathscr{A} = ZG + ZGe_2$ where $G_2 = \langle \sigma \rangle$ has order 2, then $e_2 = (1 + \sigma)/2$, $\mathscr{A}$ contains $\bar{e}_2 = e_2 - \sigma = (1 - \sigma)/2$, and $\Delta e_2 = e_2 \otimes e_2 + \bar{e}_2 \otimes \bar{e}_2$. So $\mathscr{A}$ is a $Z$-Hopf subalgebra of $QG$.

NOTE. For $G$ of odd order, Theorem 5.1 follows from a theorem of R. Larson [**30**].

COROLLARY 5.6. *If $L \supset Q$ is an abelian extension with Galois group $G$, then the order $\mathscr{A}$ of $O_L$ in $QG$ is a Hopf subalgebra of $QG$ if and only if either $L \supset Q$ is tamely ramified* (*i.e.* $\mathscr{A} = \mathbf{Z}G$), *or the only prime which ramifies wildly in $L$ is* 2 *and the first ramification group of $G$ corresponding to* 2 *has order* 2.

This follows from the description of the order $\mathscr{A}$ given in [**17**], cf. [**1**].

PROPOSITION 5.7. *Let $L \supset Q$ be an abelian extension with Galois group $G$. Then $O_L$ is tame with respect to some Hopf subalgebra of $KG$ if and only if $L$ is tamely ramified except possibly at 2, and the first ramification group of $G$ for the prime 2 has order dividing 2.*

PROOF. If $L$ satisfies the ramification conditions, then the order $\mathscr{A}$ of $O_L$ in $KG$ is a Hopf algebra by Corollary 5.6. That $O_L$ is tame then follows from Theorem 2.1.

Conversely, if $O_L$ does not satisfy the ramification hypothesis, then the order $\mathscr{A}$ of $O_L$ in $QG$ is not a Hopf algebra. But then, as Bergé notes [**1**, p. 17], $O_L$ cannot be locally free for any order in $KG$ other than $\mathscr{A}$, so, in particular, $O_L$ cannot be a tame $J$-module for any order $J$ which is a Hopf subalgebra of $KG$. This completes the proof of Proposition 5.7.

**6. Orders of Kummer extensions.** We now proceed to the case of Kummer extensions of prime order.

Let $L \supset K$ be a Kummer extension of number fields of prime order $l$. If the order $\mathscr{A}$ of $O_L$ in $KG$ is a Hopf algebra, it is a Hopf algebra of the kind described by Tate and Oort [**23**], so by (3.3) $\mathscr{A} = H_{\mathscr{B}}$ for some ideal $\mathscr{B} = \ell^{l-1}$ dividing $lO_K$. Using this fact, we obtain a necessary condition for $\mathscr{A}$ to be a Hopf algebra.

THEOREM 6.1. *Let $L \supset K$ be a Kummer extension of prime order $l$. If $\mathscr{A}$, the order of $O_L$ in $KG$, is a Hopf algebra isomorphic to $H_{\mathscr{B}}$ and $\mathscr{B}\mathscr{W} = lO_K$, then* $\operatorname{tr}(O_L) = \mathscr{W}$. *Hence* $\operatorname{tr}(O_L)$ *is the $(l-1)$th power of an ideal of $O_K$.*

PROOF. If $\mathscr{A}$ is a Hopf algebra, then $O_L$ is locally isomorphic to $\mathscr{A}^*$ as $\mathscr{A}$-module, $\mathscr{A}^* = \operatorname{Hom}_{O_K}(\mathscr{A}, O_K)$. Now $\mathscr{A}^*$ is the trivial Galois $\mathscr{A}^*$-object, so $I\mathscr{A}^* = O_K$, $I$ the space of integrals of $\mathscr{A}$, by [**9**, Proposition 2.3]. Since $O_L$ is locally isomorphic to $\mathscr{A}^*$ as $\mathscr{A}$-module, $IO_L = O_K$.

Locally at $\mathfrak{p}$, $\mathscr{A} = H_{p^{(l-1)s}}$ for some $s$, $0 \leqslant s \leqslant e$, where $lO_{K,\mathfrak{p}} = \mathfrak{p}^{(l-1)e}$ and $p$ is a uniformizing parameter for $\mathfrak{p}$. So $\mathscr{A}$ corresponds to the ideal $\mathscr{B} = \prod \mathfrak{p}^{(l-1)s}$. But if $\theta$ generates the space of integrals of $H_{p^{(l-1)s}}$, then since $O_{K,p}G = H_{p^{(l-1)e}}$, $\operatorname{tr} = p^{(l-1)(e-s)}\theta$. Thus

$$\operatorname{tr} O_L = \prod p^{(l-1)(e-s)} = (lO_K)\left(\prod \mathfrak{p}^{(l-1)s}\right)^{-1} = (lO_K)(\mathscr{B})^{-1}.$$

Since $lO_K = (1-\zeta)^{l-1}O_K$ and $\mathscr{B}$ is an $(l-1)$th power by Theorem 3.3, $\mathscr{W} = \operatorname{tr} O_L$ is an $(l-1)$th power of an ideal of $O_K$.

One objective of the remainder of this paper is to prove the converse of this result, Theorem 17.3 below.

**7. The local case. I: Which Hopf algebra can occur?** In the following sections we will focus on the situation where $K$ is a local field containing a primitive $l$th root of unity $\zeta$, $l$ prime, and $L \supset K$ is a Kummer extension, $L = K[z]$, $z^l = w \in K$, with Galois group $G = \langle \sigma \rangle$ acting on $L$ by $\sigma(z) = \zeta z$. Let $R$ be the valuation ring of $K$. We shall determine the tame and the Galois $H_b$-extensions of $R$ contained in $S$, the integral closure of $R$ in $L$, and, in particular, find criteria for $S$ itself to be a tame $H_b$-extension of $R$ for some $b$, where $H_b$ is the Tate-Oort Hopf algebra $H_b = R[\xi]$, $\xi^l = b\xi$.

In this section we show that if $T$ is an order over $R$ in $L$ which is a faithful $J$-extension of $R$ for some Hopf algebra $J$ of rank $l$, then $J$ must be a sub-Hopf algebra of $KG$, hence, since $J$ must be of the form $H_b$ for some $b$ in $R$, $b$ must have an $(l-1)$th root in $R$. We first look at $L$ itself.

PROPOSITION 7.1. *Let $K$ be a local or global number field containing $1/l$ and a primitive $l$th root of unity, $l$ prime. Let $L$ be a Galois field extension of $K$ with Galois group $G = \langle \sigma \rangle$, cyclic of order $l$. For $b \neq 0$ in $K$, $H_b$ acts faithfully on $L$ if and only if $b$ has a $(l-1)$th root $\tilde{b}$ in $K$, if and only if $H_b \cong KG$.*

PROOF. Given $b$, let $K' = K[\tilde{b}]$, $L' = L \otimes K'$, $H'_b = H_b \otimes K'$. We have $H_{\omega_l} = KG \cong (KG)^* = H_1$, so by (3.2), $\omega_l$ has an $(l-1)$th root $\tilde{\omega}_l$ in $K$.

Let $\varphi$: $H_b \otimes L \to L$ be a measuring. Then $\varphi$ induces $\varphi'$: $H'_b \otimes L' \to L'$, a measuring. But $H'_b = H'_{\tilde{b}^{l-1}} \cong H_{\omega_l}$, so the action $\varphi$ yields an action of $H_{\omega_l} = K'G$ on $L'$, that is, a map $G \to \mathrm{Aut}_{K'}(L')$.

Now since $L/K$ is a Galois field extension of prime degree $l$ and $[K' : K]$ divides $l-1$, $L'$ is a field. For if $L = K[z]$, $f(x) = \mathrm{Irr}(z, K)$, the minimal polynomial of $z$ over $K$, and $g(x) = \mathrm{Irr}(z, K')$, then, since $L/K$ is Galois, $f(x) = \prod \sigma(g(x))$ where $\sigma$ runs through a transversal of the stabilizer of $g(x)$ in $G$. Since $\deg(f(x)) = l$, prime, $\deg(g(x)) = 1$ or $l$. If $\deg(g(x)) = l$, $L'$ is a field; if $\deg(g(x)) = 1$, then $z$ is in $K'$, so $\mathrm{Irr}(z, K)$ has degree $\leqslant \deg[K' : K] < l$, impossible.

Thus if $L = K[z]$, $z^l = w$, then $L' = K'[z]$ is a field, and the only actions of $G$ on $L'$ are those given by $\sigma(z) = \zeta z$ for $\zeta$ some primitive $l$th root of unity.

Let $H'_{\omega_l} = K'G = K'[\theta]$, $\theta^l = \omega_l \theta$; $H_b = K[\xi]$, $\xi^l = b\xi$; then we have an isomorphism of Hopf algebras $H'_{\omega_l} \to H'_b$ by $\theta \mapsto \tilde{a}\xi$, $\tilde{a} = \tilde{\omega}_l/\tilde{b}$. Here

$$\theta = -\sum_{m=1}^{l-1} \chi^{-1}(m)\sigma^m.$$

Thus any action of $G$ on $L'$ extends uniquely to an action of $H'_b$ on $L'$, and so given the action of $G$, $\sigma(z) = \zeta z$, for some root of unity $\zeta$, we have

$$\xi z^i = \left(-\frac{1}{\tilde{a}}\sum_m \chi^{-1}(m)\zeta^{im}\right) z^i.$$

Since $H_b = K[\xi]$ acts on $L$ and $z^i \in L$, then $\xi z^i$ is in $L$ for all $i$, that is, for all $i$, $-(1/\tilde{a})\Sigma_m \chi^{-1}(m)\zeta^{im}$ is in $L$. But since $\Sigma_m \chi^{-1}(m)\zeta^{im} \in L$, that is the case if and only if $\tilde{a}$ is in $L$ or $\Sigma\chi^{-1}(m)\zeta^{im} = 0$ for all $i$; and the latter possibility cannot occur, since otherwise $\xi$ would act trivially on $L$ and the action of $H_b$ on $L$ would be unfaithful.

Thus if $H_b$ acts on $L$, then $\tilde{b} = \tilde{\omega}_l/\tilde{a}$ is in $K$, and $H_b \cong H_{\omega_l}$. That completes the proof of Proposition 7.1.

COROLLARY 7.2. *Let $L \supset K$ be a Galois extension of local fields, cyclic of order $l$, prime, where $K$ contains $1/l$ and a primitive $l$th root of unity. Let $R$ be the valuation ring of $K$, $T$ an integral $R$-subalgebra of $L$ with $TK = L$, which is an $H_b$-extension of $R$ for $b$ in $R$. Then $H_b$ is an order over $R$ in $KG$ containing $RG$, and $b$ is an $(l-1)$th power in $R$.*

PROOF. If $H_b$ acts on $S$, $H_b \otimes K$ acts on $L$, so since $R$ is integrally closed, Proposition 7.1 implies that $\tilde{b}$, an $(l-1)$th root of $b$, is in $R$, and the inclusion $H_b \subseteq KG$ then follows from (3.2). Since $b$ divides $l$ by definition of $H_b$, we have $RG \subseteq H_b$.

The uniqueness in Theorem 7.1 may also be obtained as a special case of Theorem 3.1 of [**27**].

**8. Kummer orders.** Now we begin the classification of $H_b$-extensions $S$ as in (7.2) which are tame. First we consider the case $b = 1$, $H_b = (RG)^*$.

PROPOSITION 8.1. *Let $L \supset K$ be a Galois extension of local fields with Galois group $G$, cyclic of order $l$, and suppose $K$ contains a primitive $l$th root of unity. Let $R$ be the valuation ring of $K$, and let $S$ be the integral closure of $R$ in $L$. Let $\tilde{S}$ be the Kummer order of $S$* [**12**], *$\tilde{S} = \sum_{\chi \in \hat{G}} S_\chi$, where*

$$S_\chi = \{s \in S \mid \sigma(s) = \chi(\sigma)s \text{ for all } \sigma \text{ in } G\}.$$

*Then $\tilde{S}$ is a tame $(RG)^*$-extension of $R$ contained in $S$, $\tilde{S} = R[z]$, $z^l$ in $R$, and the tame $(RG)^*$-extensions of $R$ contained in $S$ are the $G$-graded subalgebras $T$ of $\tilde{S}$,*

$$T = \sum_{i=0}^{l-1} Rc_i z^i, \quad c_i \text{ in } R,\ c_i \neq 0, \text{ with } c_0 = 1.$$

PROOF. Let $p$ be a uniformizing parameter for the maximal ideal $\mathfrak{p}$ of $R$.

First we identify $\tilde{S}$. Let $L = K[y]$, $y^l$ in $K$. By altering $y$ by an $l$th power, we can choose $y^l = w$ in $R$ with $v_\mathfrak{p}(w)$, the $\mathfrak{p}$-adic valuation of $w$, satisfying $0 \leqslant v_\mathfrak{p}(w) < l$, so $y$ is in $S$.

If $v_\mathfrak{p}(w) = 0$, i.e. $w$ is a unit, then $\tilde{S} = R[y]$. For since $y^l$ is in $R$, the map $\chi$: $G \to K$ by $\chi(\sigma) = \sigma(y)/y$ is a character of $G$ which generates the character group $\hat{G}$, and

$$S_{\chi^i} = S \cap L_{\chi^i} = S \cap Ky^i \supseteq Ry^i;$$

since $y^i$ is a unit of $S$, $S_{\chi^i} = Ry^i$.

If $v_\mathfrak{p}(w) = r > 0$, let $rs - kl = 1$, and let $z = y^s/p^k$. Then $z^l = y^{sl}/p^{kl} = w^s/p^{kl}$ and $v_\mathfrak{p}(z^l) = rs - kl = 1$. In that case, $z$ is the root of the Eisenstein polynomial $Z^l - z^l$, so $L/K$ is totally ramified and $S = R[z]$. In that case, if $\chi(\sigma) = \sigma(z)/z$, then $S_{\chi^i} = Rz^i$, and $S = \tilde{S}$.

Set $(RG)^* = \sum Re_\chi$, $e_\chi = (\sum_\sigma \chi(\sigma^{-1})\sigma)/l$; the integral $I$ of $(RG)^* = Re_{\chi_0}$. Then $e_\chi S = S_\chi$ and in particular, $IS = S_{\chi_0} = S^G = R$. Since $\tilde{S}$ is a faithful $(RG)^*$-module of rank $l$, $\tilde{S}$ is a tame $(RG)^*$-extension of $R$. $\tilde{S}$ is a Galois $(RG)^*$-extension of $R$ if and only if $\tilde{S} = R[z]$ with $z$ a unit of $R$, if and only if $v_\mathfrak{p}(w) = 0$ (cf. Example 11.6 below).

Write $\tilde{S} = R[z]$ with $\sigma(z) = \chi(\sigma)z$.

Let $T$ be an $(RG)^*$-module subalgebra of $S$. Then

$$T = (RG)^*T = \sum Re_{\chi^i}T = \sum e_{\chi^i}T = \sum T_{\chi^i}$$

and $T_{\chi^i} \subseteq S_{\chi^i}$. Thus $T$ is a $G$-graded subalgebra of $\tilde{S}$. Tameness means simply that $T_{\chi_0} = R$ and each $T_{\chi^i} \neq (0)$, from which the description of $T$ given in the statement of the theorem is clear.

COROLLARY 8.2. *With $L$, $K$, $S$, $R$, $G$ as in Proposition* 8.1, *there exists a Galois $(RG)^*$-module subalgebra of $S$ if and only if $S = R[z]$ with $z^l$ a unit of $R$, in which case $\tilde{S}$ is the unique such Galois $(RG)^*$-module algebra.*

PROOF. $T$ is a Galois $(RG)^*$-module algebra if and only if $T = \sum T_\chi$ with $T_\chi = Rz_\chi$ and $T_\chi T_\psi = T_{\chi\psi}$ for all $\chi$, $\psi$ in $\hat{G}$, in particular, $T_\chi^l = R$. Thus $T$ is Galois if and only if each $z_\chi$ is a unit of $S$, in which case $T_\chi = S_\chi$, $T = \tilde{S}$ and $\tilde{S} = R[z]$ with $z^l$ a unit of $R$.

**9. Galois extensions.** In contrast to the situation for $H_b = H_1 = (RG)^*$, we have

THEOREM 9.1. *Let $R$ be a local ring containing a primitive $l$th root of unity, $l$ prime, with $l$ contained in the maximal ideal $\mathfrak{p}$ of $R$; let $G$ be cyclic of order $l$. Let $H_b$ be a Tate-Oort Hopf $R$-algebra, $RG \subseteq H_b \subseteq (RG)^*$. Suppose $b \in \mathfrak{p}$. Then any tame $H_b$-extension of $R$ is Galois.*

PROOF (from [**13**, Theorem 4.4]). Let $H_b = R[\xi]$, $\xi^l = b\xi$; then $\phi = \xi^{l-1} - b$ generates the space of integrals of $H_b$. If $S$ is tame, then $\phi s = 1$ for some $s$ in $S$.

We claim that $s, \xi s, \xi^2 s, \dots, \xi^{l-1}s$ is an $R$-basis of $S$. To see this, it suffices to show it mod $p$. But mod $p$, $\xi^{l-1}s \equiv 1$ and $\xi^l s \equiv 0$. Suppose

$$\sum_{i=0}^{l-1} r_i \xi^i s \equiv 0 \pmod{p}.$$

If $k$ is the least index with $r_k \neq 0$, then since $\xi^l s \equiv 0 \pmod{p}$,

$$0 \equiv \xi^{l-1-k}\left(\sum_{i=1}^{l-1} r_i \xi^i s\right) \equiv r_k \xi^{l-1}s \equiv r_k.$$

So, mod $p$, $s, \xi s, \xi^2 s, \dots, \xi^{l-1}s$ are linearly independent, so are a basis. Thus, $s, \xi s, \dots, \xi^{l-1}s$ span $S$ over $R$ [**5**, II, §3, No. 2, Corollaire 2]. But since $S$ is tame $S$ is free over $R$ of rank $l$. Hence $s, \xi s, \dots, \xi^{l-1}s$ form a basis of $S$.

Let $h_0, \dots, h_{l-1}$ be a dual basis in $H_b^*$ for $1, \xi, \xi^2, \dots, \xi^{l-1}$ in $H_b$. Now $S$ is an $H_b^*$-object via the map $\alpha$: $S \to S \otimes H_b^*$ given by

$$\alpha(s) = \sum_i \xi^i s \otimes h_i.$$

Define $\gamma$: $S \otimes S \to S \otimes H$ by

$$\gamma(s \otimes t) = \sum_i s\xi^i t \otimes h_i.$$

Then $S$ is a Galois $H_b$-extension of $R$ if and only if $\gamma$ is an isomorphism. Since $S \otimes S$ and $S \otimes H_b^*$ are of equal ranks as free $R$-modules, it suffices to show that $\gamma$ is surjective modulo $p$ [**5**, II, §3, No. 2, Corollaire 1]. So for the rest of the proof, assume $R$ is a field with $b = l = 0$.

We show that $\gamma$ is surjective by finding, for each $i$, elements $a_k$ and $b_k$ in $S$ such that $\gamma(\sum a_k \otimes b_k) = 1 \otimes h_i$, as follows: we set $b_k = \xi^{l-1-k}s$ for all $k$, and

$$a_k = \begin{cases} 0 & \text{for } k > i, \\ 1 & \text{for } k = i, \\ -\sum_{m>k} a_m(\xi^k b) & \text{for } k < i. \end{cases}$$

Then

$$\gamma\left(\sum_k a_k \otimes b_k\right) = \sum_j \left(\sum_k a_k \xi^j b_k\right) \otimes h_j$$

$$= \sum_j \left(\sum_k a_k \xi^j \xi^{l-1-k} s\right) \otimes h_j$$

$$= \sum_j \left(\sum_{k \geqslant j} a_k \xi^{l-1+j-k} s\right) \otimes h_j$$

since $\xi^l = b\xi = 0$,

$$= \sum_j \left(\sum_{k \geqslant j} a_k \xi^j b_k\right) \otimes h_j.$$

For $j > i$, $k \geqslant j$, $a_k = 0$, so

$$\sum_{k \geqslant j} a_k \xi^j b_k = 0.$$

For $j = i$,

$$\sum_{k \geqslant i} a_k \xi^j b_k = a_i \xi^i b_i + \sum_{k > i} a_k \xi^i b_k = a_i \xi^i b_i;$$

since $a_i = 1$ and $\xi^i b_i = \xi^{l-1} s = 1$, $\xi^i b_i = 1$.

For $j < i$,

$$\sum_{k \geqslant j} a_k \xi^j b_k = \sum_{k > j} a_k \xi^j b_k + a_j \xi^j b_j.$$

Now $\xi^j b_j = 1$, and, substituting for $a_j$, we get

$$= \sum_{k > j} a_k \xi^j b_k - \sum_{m > j} a_m \xi^j b_m = 0.$$

Thus $\gamma(\Sigma a_k \otimes b_k) = 1 \otimes h_i$, completing the proof.

**10. Frobenius conditions on Galois $H$-extensions.** We develop some general theory for $H$-extensions which may be of independent interest.

Let $R$ be a commutative ring with unity, and $H$ a finite (i.e. finitely generated and projective as $R$-module) $R$-Hopf algebra. Finiteness implies that the space of left integrals of $H$,

$$I = \{\theta \in H \mid h\theta = \varepsilon(h)\theta, \text{ for all } h \text{ in } H\}$$

is a rank one projective $R$-module, as is the space of right integrals. Following Larson and Sweedler [**16**], $H$ is called unimodular if the space of left integrals equals the space of right integrals.

Let $S$ be an $R$-algebra, finitely generated and projective as $R$-module ("finite"), and an $H$-extension.

If $S^H = R$, then $S$ is a Galois $H$-extension of $R$ if and only if the map

$$j\colon S\# H \to \operatorname{End}_R(S), \quad j(s\# h)(t) = sh(t)$$

is an isomorphism [7, Theorem 9.3]. Denote the image of $S$ in $\mathrm{End}_R(S)$ under $j$ by $S_l$, the set of left multiplications by elements of $S$.

THEOREM 10.1. *Let $H$ be a finite unimodular Hopf algebra with space of integrals $I$, and $S$ a finite $R$-algebra and an $H$-module algebra with $S^H = R$. Then $S$ is a Galois $H$-extension of $R$ if and only if the map $\varphi$: $I \otimes S \to S^*$ $(= \mathrm{Hom}_R(S, R))$, $\varphi(\theta, s)(t) = \theta(st)$ for $\theta$ in $I$, $s$, $t$ in $S$, is an isomorphism.*

PROOF. For $M$ an $R$-submodule of $\mathrm{End}_R(S)$ denote by $I \cdot M$ the set $\{\theta m \mid m$ in $M$, $\theta$ in $I\}$. Then since $IS \subseteq S^H = R$, $I \cdot S_l \subseteq S^* \subseteq \mathrm{End}_R(S)$. The image of $\varphi$ is then $I \cdot S_l$. Since $I \otimes S$ and $S^*$ are both finitely generated projective $R$-modules of equal ranks, $\varphi$ is an isomorphism if and only if $\varphi$ is an epimorphism, if and only if $I \cdot S_l = S^*$. So we shall show that $S$ is Galois if and only if $I \cdot S_l = S^*$.

LEMMA 10.2. $I \cdot (S\sharp H)_l = I \cdot S_l$.

Assuming the lemma, the proof of the theorem proceeds as follows.

Suppose $I \cdot S_l = S^*$. Then we have the diagram

$$\begin{array}{ccccc} S \otimes S^* & = & S \otimes I \cdot S_l & = & S \otimes I \cdot (S\sharp H)_l \\ \wr\!\!\parallel\ \mu & & & & \downarrow m \\ \mathrm{End}(S) & & \supseteq & & j(S\sharp H) \end{array}$$

where

$$\begin{aligned} m\big(s \otimes \theta(s'\sharp h)\big)(t) &= \left(\textstyle\sum s\left(\theta_{(1)}s'\right)\sharp\theta_{(2)}h\right)(t) \\ &= \textstyle\sum s\left(\theta_{(1)}s'\right)\left(\theta_{(2)}h\right)(t) \\ &= j\left(\textstyle\sum s\left(\theta_{(1)}s'\right)\sharp\theta_{(2)}h\right)(t) \end{aligned}$$

and $\mu(s\sharp f)(t) = sf(t)$.

The diagram commutes: for given $s$, $s'$ in $S$, $\theta$ in $I$, we have $\mu(s \otimes \theta \cdot s')(t) = s\theta(s't)$, while

$$m(s \otimes \theta \cdot s')(t) = \textstyle\sum s\left(\theta_{(1)}s'\right)\left(\theta_{(2)}t\right) = s\theta(s't) \quad \text{(by measuring)}.$$

Thus $j(S\sharp H) = \mathrm{End}_R(S)$, and $S$ is Galois.

Conversely, suppose $S$ is a Galois $H^*$-object. Then $\mathrm{End}_R(S) \cong S\sharp H$, and by Morita theory

$$\mathrm{End}_R(S) \cong S \otimes I \cdot (S\sharp H)_l = S \otimes I \cdot S_l$$

by Lemma 10.2, where the map $S \otimes I \cdot S_l$ to $\mathrm{End}_R(s)$ is $\mu$. Thus the diagram

$$\begin{array}{ccc} S \otimes S^* & \leftarrow & S \otimes I \cdot S_l \\ \searrow\!\!\wr & & \wr\!\!\swarrow \\ & \mathrm{End}_R(S) & \end{array}$$

commutes, and so the inclusion $I \cdot S_l \subset S^*$ induces an isomorphism $S \otimes I \cdot S_l \cong S \otimes S^*$. Since $S$ is $R$-faithfully flat, $I \cdot S_l = S^*$.

We are left only with proving the lemma: $I \cdot S_l = I \cdot (S\#H)_l$.

PROOF OF LEMMA 10.2. For $x, y \in S$, $h \in H$, $\phi \in I$, we have

$$\begin{aligned}
(\phi(y\#h))(x) &= \sum \phi_{(1)}(y)\phi_{(2)}h(x) \\
&= \sum \phi_{(1)}(y)\phi_{(2)}\varepsilon(h_{(1)})h_{(2)}(x) \quad \text{since } (1 \otimes \varepsilon)\Delta = \text{id}, \\
&= \sum \phi_{(1)}\big(\varepsilon(h^\lambda_{(1)})\big)(y)\phi_{(2)}h_{(2)}(x) \\
&= \Big(\sum \phi_{(1)}\varepsilon(h^\lambda_{(1)}) \otimes \phi_{(2)}h_{(2)}\Big)(y \otimes x) \\
&= \Delta\big(\phi\varepsilon(h^\lambda_{(1)})\big)(1 \otimes h_{(2)})(y \otimes x) \\
&= \Delta(\phi h^\lambda_{(1)})(1 \otimes h_{(2)})(y \otimes x) \quad \text{since } \phi \text{ is a right integral,} \\
&= \Big(\sum \phi_{(1)}h^\lambda_{(1)} \otimes \phi_{(2)}h^\lambda_{(2)}h_{(3)}\Big)(y \otimes x) \\
&= \Big(\sum \phi_{(1)}h^\lambda_{(1)} \otimes \phi_{(2)}\varepsilon(h^\lambda_{(2)})\Big)(y \otimes x) \\
&= \Big(\sum \phi_{(1)}h^\lambda_{(1)}\varepsilon(h^\lambda_{(2)}) \otimes \phi_{(2)}\Big)(y \otimes x) \\
&= \Big(\sum \phi_{(1)}h^\lambda \otimes \phi_{(2)}\Big)(y \otimes x) = \sum \phi_{(1)}h^\lambda(y)\phi_{(2)}(x) \\
&= \phi(h^\lambda y \cdot x) = \phi(h^\lambda y)_l(x).
\end{aligned}$$

So $I \cdot (S\#H)_l \subseteq I \cdot S_l$. The opposite inclusion is clear.

EXAMPLE 10.3. Let $K$ be a domain of characteristic $p$. Let $H = K[f_1, \dots, f_n]$ with $f_i^p = 0$, $f_i$ commuting and primitive, $\varepsilon(f_i) = 0$ for all $i$.

Let $L = K[x_1, \dots, x_n]$ with $x_i^p = a_i$ in $K$, acted on by $H$ with $f_i$ acting by $\partial/\partial x_i$.

For $R = (r_1, r_2, \dots, r_n)$, set

$$x^R = x_1^{r_1} \cdots x_n^{r_n}, \quad f^R = f_1^{r_1} \cdots f_n^{r_n},$$

and

$$y^R = x^R/(r_1)! \cdots (r_n)!.$$

Setting $P - 1 = (p-1, p-1, \dots, p-1)$, the space of integrals of $H$ is generated by $\theta = f^{P-1}$. Then $\{y^R \mid 0 \leqslant r \leqslant p-1\}$ is a $K$-basis of $L$, and if $\{\varphi_R\}$ is a dual basis, we have $\varphi_{P-1} = \theta$. Then $\varphi_R(y^S) = \theta(y^{P-1-R}y^S)$, and $\theta \cdot L_l = L^*$. By Theorem 10.1 $L$ is a Galois $H$-extension of $K$.

Using Theorem 10.1 we may give a Galois-theoretic proof of a well-known result of Larson and Sweedler **[16]**. The usual proof (cf. **[16, 18, 19, 22]**, uses a Hopf module approach, which we avoid.

COROLLARY 10.4. *$H \cong I \otimes H^*$ as left $H$-modules, where $I$ is the space of integrals of $H$ and $I \otimes H^*$ is a left $H$-module via the action of $H$ on $H^*$ given by $(x \cdot f)(y) = f(yx)$.*

PROOF. We can assume that the $H$-action on $H^*$ is given by $(x \cdot f)(y) = f(x^\lambda \cdot y)$, for the antipode $\lambda$: $H^* \to H^*$ induces an isomorphism between $H_1^* = H^*$ with action $(xf)(y) = f(x^\lambda \cdot y)$ and $H_2^* = H^*$ with action $(xf)(y) = f(yx)$.

If $\theta$ is an integral of $H$, then

$$\sum_{(\theta)} x^{\lambda}\theta_{(1)} \otimes \theta_{(2)} = \sum_{(\theta)} \theta_{(1)} \otimes x\theta_{(2)}$$

(cf. [**22**, p. 104]).

Define $\varphi\colon I \times H^* \to H$ by

$$\langle \varphi(\theta, f), g \rangle = \langle \theta, fg \rangle$$

for $f$, $g$ in $H^*$, $\theta$ in $I$. Since $H^*$ is a Galois $H^*$-object, $\varphi$ is an isomorphism by Theorem 10.1. Then $\varphi$ is an $H$-module isomorphism. For

$$\begin{aligned}\langle x\varphi(\theta, f), g \rangle &= \langle x, g_{(1)} \rangle \langle \varphi(\theta, f), g_{(2)} \rangle = \langle x, g_{(1)} \rangle \langle \theta, fg_{(2)} \rangle \\ &= \langle x, g_{(1)} \rangle \langle \theta_{(1)}, f \rangle \langle \theta_{(2)}, g_{(2)} \rangle = \langle \theta_{(1)}, f \rangle \langle x\theta_{(2)}, g \rangle \\ &= \langle x^{\lambda}\theta_{(1)}, f \rangle \langle \theta_{(2)} g \rangle = \langle x^{\lambda}, f_{(1)} \rangle \langle \theta_{(1)}, f_{(2)} \rangle \langle \theta_{(2)}, g \rangle \\ &= \langle x^{\lambda}, f_{(1)} \rangle \langle \theta, f_{(2)} g \rangle = \langle \theta, \langle f_{(1)}, x^{\lambda} \rangle f_{(2)} g \rangle \\ &= \langle \theta, (x \cdot f) g \rangle = \langle \varphi(\theta, x \cdot f), g \rangle.\end{aligned}$$

So $x\varphi(\theta, f) = \varphi(\theta, x \cdot f)$, completing the proof.

COROLLARY 10.5 (PAREIGIS [**19**]). *As left $H$-modules, $H^* \cong H$, i.e. $H$ is a Frobenius $R$-algebra, if and only if $I$ is $R$-free.*

REMARK 10.6. The condition that $H$ is unimodular, i.e. that the spaces of left integrals and right integrals are equal, is obvious if $H$ is commutative. Unimodularity has been studied by Larson and Sweedler [**16**], who showed that a finite Hopf algebra over a field is unimodular if $H$ has a left integral $\theta$ with $\varepsilon(\theta) \neq 0$, which is equivalent to $H$ being semisimple; or if $H$ has an antipode of order 2 and $H^*$ is separable. They give an example of a finite cocommutative Hopf algebra $H$ with $H^*$ connected over a field of characteristic 2 which is not unimodular.

The trivial Galois $H^*$-object is $H^*$ itself, which is acted upon by $H$. Theorem 10.1 then specializes, for unimodular $H$, to the result of Larson and Sweedler [**16**] that for a finite bialgebra with antipode, the bilinear form $\beta\colon H^* \times H^* \to R$, $\beta(p, q) = (pq)\theta$, associated to a generator $\theta$ of the space of integrals of $H$, is nonsingular.

**11. Discriminants.** We may define a codifferent using the integrals of $H$.

PROPOSITION 11.1. *Let $R$ be a domain with quotient field $K$, $H$ a finite unimodular Hopf $R$-algebra with space of integrals $I$. Let $S$ be a finite $R$-algebra and an $H$-extension of $R$ such that $L = S \otimes_R K$ is a Galois $H \otimes_R K$-extension of $K$. Let $C = \{x \in L \mid \theta x \in R$ for all $\theta$ in $I\} \supseteq S$. Then $I \cdot C_l = S^*$. Hence $S$ is a Galois $H$-extension of $S^*$ if and only if $C = S$.*

PROOF. Both conditions are true if and only if they are true locally, so we may assume $R$ is a local ring and $I = R\theta$ for some $\theta$. Since $L$ is Galois, $I \cdot L_l = L^*$ by Theorem 10.1, and so, viewing $\theta$ as in $\mathrm{Hom}_R(S, R) \subseteq \mathrm{Hom}_K(L, K)$, $S^* \subseteq \theta \cdot L_l$, and $S^* = \theta \cdot C_l$, where $C = \{x$ in $L \mid \theta x \in S^*\}$. But

$$\begin{array}{ccc} S & \subseteq & C \\ & {\scriptstyle \beta|_S} \searrow \ \swarrow {\scriptstyle \beta} & \\ & S^* & \end{array}$$

commutes, where $\beta(x)(y) = \theta(xy)$. Since $\beta\colon C \to S^*$ is an isomorphism, $S = C$ if and only if $\beta|_S$ is an isomorphism, if and only if $I \cdot S_l = S^*$. Theorem 10.1 applies to complete the proof.

To define a discriminant of an $H$-extension $S$ of $R$, first assume $R$ is local, so that $I = R\theta$ and $S$ is a free $R$-module. Let $\{x_1, \dots, x_n\}$ be a basis of $S$ as a free $R$-module.

Define $\delta_H(x_1, \dots, x_n) = \det(\theta(x_i x_j))$.

Let $\{f_1, \dots, f_n\}$ be a dual basis in $S^*$ to $\{x_1, \dots; x_n\}$. Let $\{y_1, \dots, y_n\}$ in $C$ be such that $f_i = \theta \cdot y_i$. Write $y_i = \sum_j a_{ij} x_j$, $a_{ij}$ in $K$. Then

$$\delta_{ij} = f_i(x_j) = \theta(y_i x_j) = \theta\Big(\sum_k a_{ik} x_k x_j\Big) = \sum_k a_{ik}\theta(x_k x_j)$$

so $(a_{ik})(\theta(x_k x_j))$ = the $n \times n$ identity matrix.

Thus $(\theta(x_k x_j))$ is invertible if and only if all $a_{ik}$ are in $R$, if and only if all $y_i$ are in $S$, if and only if $S^* = \theta \cdot S_l$, if and only if $S$ is a Galois $H$-object.

Globalizing, we get the following:

DEFINITION 11.2. $\delta_H(S/R)$, the discriminant of $S$ with respect to $H$, is the ideal of $R$ generated by $\{\det \theta(x_i x_j)\}$ for $\theta$ in $I$ and $\{x_1, \dots, x_n\}$ running through $K$-bases of $L$ contained in $S$.

PROPOSITION 11.3. *Under the same assumptions as in Proposition* 11.1, $\delta_H(S/R) = R$ *if and only if $S$ is a Galois $H^*$-object.*

PROOF. Both conditions are true if and only if they are true locally. So we can assume $S$ is a free $R$-module with basis $\{x_1, \dots, x_n\}$, and $I = R\theta$, in which case the above argument applies.

REMARKS. 11.4. When $H = RG$, $S$ is a Galois $H$-extension of $R$ if and only if $S$ is a Galois extension of $R$ with group $G$, in the sense of Chase, Harrison, Rosenberg [**6**]. In that case, $H = RG$, which is unimodular with space of integrals generated by $\theta = \sum_{\sigma \in G} \sigma = \mathrm{tr}$; $\delta_H(S/R)$ is the classical discriminant. The above results then specialize to the results on pages 92–93 of DeMeyer and Ingraham [**10**].

EXAMPLE 11.5 (CLASSICAL). Suppose $R$ is a domain with quotient field $K$, and $R$ contains a primitive $n$th root of unity $\zeta$; let $S = R[z]$ with $z^n = b$, and $H = RG$, $G$ cyclic of order $n$ with generator $\sigma$ acting on $S$ by $\sigma(z) = \zeta z$. Then $\delta_H(S/R) = \det(\mathrm{tr}(z^i z^j))$. Since

$$\mathrm{tr}(z^r) = \begin{cases} 0, & r \not\equiv 0 \pmod n, \\ n z^r, & n \mid r, \end{cases}$$

we have

$$\det\big(\mathrm{tr}(z^i z^j)\big) = \det\begin{pmatrix} n & 0 & \cdots & 0 \\ 0 & & & nb \\ \vdots & & \cdot^{\cdot^{\cdot}} & \\ 0 & nb & & 0 \end{pmatrix} = \pm n^n b^{n-1}.$$

Hence $S$ is a Galois $H$-extension of $R$, $H = RG$ if and only if $n$ and $b$ are units of $R$. Of course, $\delta_H(S/R)$ is the classical discriminant.

Note here that if $n$ is a unit of $R$, then $RG = (RG)^*$. Consider, then,

EXAMPLE 11.6. Same $S$, but do not assume $R$ contains a primitive $n$th root of unity. Let $H = (RG)^* = \sum_{k=0}^{n-1} Re_k$, $e_k(\sigma^j) = \delta_{k,j}$. Then $I = Re_0$.

Define $H$ on $S$ by $e_k(z^j) = \delta_{k,j} z^j$. Then

$$\begin{aligned} \delta_H(S/R) &= \det\big(e_0(z^i z^j)\big) \\ &= \det\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & b \\ \vdots & & \cdot^{\cdot^{\cdot}} & \\ 0 & b & & 0 \end{pmatrix} \\ &= \pm b^{n-1}. \end{aligned}$$

Hence $S$ is a Galois $H$-extension of $R$ for $H = (RG)^*$ if and only if $b$ is a unit of $R$. See also Chase and Sweedler [7, Example 4.16].

**12. The local case. II: A chain of Galois module algebras.** The discriminant permits us to construct a chain of Galois module algebras inside the ring of integers of a Kummer extensions of local fields.

EXAMPLE 12.1. Let $R$ be the completion at some prime lying over $l$ of a finite extension of $Z[\zeta]$, $\zeta$ a primitive $l$th root of unity, $l$ an odd prime. Let $p$ generate the maximal ideal of $R$, and let $lR = (pR)^{e(l-1)}$. Let $H_b$ be the Tate-Oort Hopf algebra $R[\xi]$, with $\xi^p = b\xi$, and comultiplication

$$\begin{aligned} \Delta(\xi^i) &= (1 \otimes \xi^i) + (\xi^i \otimes 1) \\ &\quad + \frac{w_i}{1-l}\left[\sum_{j=1}^{i-1} \frac{\xi^j}{\omega_j} \otimes \frac{\xi^{i-j}}{\omega_{i-j}} + \sum_{j=i}^{l-1} \frac{a^{\xi^j}}{\omega_j} \otimes \frac{\xi^{l-1+i-j}}{\omega_{l-1+i-j}}\right] \end{aligned}$$

where $ab = \omega_l$.

Let $K$ be the quotient field of $R$, and $L = K[z]$, $z^l = w$, $w$ in $R$. For $0 \leqslant s \leqslant e$, let $S = R[x]$, $x = (z-1)/p^s$. Then $x$ satisfies $(1 + p^s z)^l = w$, or

$$x^l + \binom{l}{l-1}\frac{x^{l-1}}{p^s} + \cdots + \binom{l}{r}\frac{x^r}{p^{(l-r)s}} + \cdots + \binom{l}{1}\frac{x}{p^{(l-1)s}} = \frac{w-1}{p^{sl}}.$$

Since $s \leqslant e$, all coefficients of $x^r$, $r > 0$, are in $R$, and $x$ is integral over $R$ if and only if $w \equiv 1 \pmod{p^{sl}}$.

Suppose $w = 1 + p^{sl}c$, $c$ in $R$.

Let $H_b$, $b = p^{s(l-1)}$ act on $S$ by $\xi x = 1 + p^s x = z$, $\xi z = p^s z$. Then $H_b$ sends $Rx$ into $S$. But then, using the measuring property:

$$\begin{aligned} \xi^i(x^r x^s) &= x^r(\xi^i x^s) + (\xi^i x^r)x^s \\ &\quad + \frac{\omega_i}{1-l}\left[\sum_{j=1}^{i-l}\left(\frac{\xi^j x^r}{\omega_j}\right)\left(\frac{\xi^{i-j} x^s}{\omega_{ij}}\right) + \sum_{j=i}^{l-1} a\left(\frac{\xi^j x^r}{\omega_j}\right)\left(\frac{\xi^{l-1+i-j} x^s}{\omega_{l-1+i-j}}\right)\right], \end{aligned}$$

one sees easily by induction on $k$ that $H$ sends $Rx^k$ into $S$ for all $k > 0$. Thus $H_b$ acts on $S$.

Now $RG = H_{p^{e(l-1)}} \subseteq H_b = H_{p^{s(l-1)}} \subseteq H_1 = (RG)^*$; if $l = up^{e(l-1)}$ for some unit $u$ of $R$, then $\theta = (\sum\sigma)/p^{(e-s)(l-1)}u$ generates the space of integrals of $H$.

Thus

$$\theta(z^r) = \begin{cases} 0, & l \nmid r, \\ z^r p^{s(l-1)}, & l \mid r. \end{cases}$$

and so

$$\begin{aligned} \delta_H(1, z, z^2, \ldots, z^{l-1}) &= \det\left(\theta(z^{i+j})\right) \\ &= \det\begin{pmatrix} p^{s(l-1)} & 0 & \cdots & 0 \\ 0 & & & p^{s(l-1)}w \\ \vdots & & \cdot^{\cdot^{\cdot}} & \\ 0 & p^{s(l-1)}w & & 0 \end{pmatrix} \\ &= w^{l-1}p^{sl(l-1)}. \end{aligned}$$

Now $z = 1 + p^s x$, so

$$z^r = \sum_{k=0}^{r} p^{sk}\binom{r}{k}x^k.$$

So

$$\delta_H(1, x, x^2, \ldots, x^{l-1}) \det(A)^2 = p^{sl(l-1)}w^{l-1},$$

where

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & p^s & & \cdot \\ 1 & \binom{2}{1}p^s \; p^{2s} & & \vdots \\ & \cdots & & 0 \\ \cdot & \cdot & \cdots & p^{(l-1)s} \end{pmatrix}.$$

Thus $(\det A)^2 = p^{l(l-1)s}$ and $\delta_H(1, x, x^2, \ldots, x^{l-1}) = w^{l-1}$, a unit of $R$. Thus $S = R[x]$, $x = (z-1)/p^s$, is a Galois $H_{p^{s(l-1)}}$-extension of $R$.

If $L = K[z]$, $z^l = w$, $w = 1 + p^{ql+r}u$, $0 \leqslant r < 1$, $0 \leqslant q \leqslant e$, $ql + r \geqslant 1$, $u$ a unit of $R$, then we get a chain of Galois extensions of $R$ contained in the integral closure $S$ of $R$ in $L$: $S_0 \subsetneqq S_1 \subsetneqq S_2 \subsetneqq \cdots \subsetneqq S_q$ where $S_s = R[(z-1)/p^s]$ is a Galois $(H_{p^{s(l-1)}})$-extension of $R$. In particular, $S_0$ is as in Example 11.6, and is the Kummer order $\tilde{S}$ of $S$ arising in Theorem 8.1.

Summarizing, we have shown

THEOREM 12.2. *Let $K$ be a local field with valuation ring $R$, maximal ideal $\mathfrak{p} = pR$ and $l \in \mathfrak{p}$. Let $L \supset K$ be a Kummer extension of degree $l$, $L = K[z]$, $z^l = w = 1 + up^k$, $u$ a unit of $R$, $k$ maximal, $k > 0$, $k = ql + r$, where $0 \leqslant r < l$ and $0 < r$ if $q < e$. Let $S$ be the integral closure of $R$ in $L$. Then there is a chain of Galois extensions of $R$, $S_0 \subsetneqq S_1 \subsetneqq \cdots \subsetneqq S_h$, all contained in $S$, where $S_k$ is a Galois $H_{p^{k(l-1)}}$-extension of $R$, $0 \leqslant k \leqslant h$, and $h = \min\{q, e\}$.*

**13. Some lemmas on Kummer extensions of prime order.** Throughout this section, let $K$ be a local field, a finite extension of $Q_l$, with valuation ring $R$, maximal ideal $\mathfrak{p} = pR$, $lR = \mathfrak{p}^{e(l-1)}$, and $L$ a Kummer extension of $K$ of prime order $l$.

We wish to show that the chain of Galois extensions described in Theorem 12.2 contains all the Galois extensions of $R$ contained in $L$. We need a preliminary lemma.

LEMMA 13.1. *Let $z^l = 1 + up^{lq+r}$, $u$ a unit of $R$, where $q < e$ and $0 < r < l$. Set $x = (z-1)/p^q$. Then $v_L(x) = r$.*

PROOF. Since $z^l = 1 + up^{lq+r}$, $x$ satisfies

$$0 = \left((1 + p^q x)^l - 1 - up^{lq+r}\right)/p^{ql}$$

or

$$0 = x^l + \frac{lp^{q(l-1)}}{p^{ql}}x^{l-1} + \cdots + \binom{l}{k}\frac{p^{qk}x^k}{p^{ql}} + \cdots + \frac{lp^q}{p^{ql}} - up^r. \tag{13.2}$$

Since $q < e$, $L \supset K$ is totally ramified, and $v_L(p) = l$. In order that equation (13.2) hold, (13.2) must contain two terms whose valuations are equal and minimal. Now

$$v_L(x^l) = lv_L(x), \quad v_L(up^r) = lr$$

and for $1 \leqslant k \leqslant l-1$,

$$\begin{aligned} v_L\left(\binom{l}{k}\frac{x^k}{p^{q(l-k)}}\right) &= el(l-1) + kv_L(x) - lq(l-k) \\ &\geqslant el(l-1) - l(e-1)(l-1) + kv_L(x) \\ &\geqslant l(l-1) + kv_L(x). \end{aligned}$$

Thus

$$v_L(up^r) < v_L\left(\binom{l}{k}\frac{x^k}{p^{q(l-k)}}\right)$$

unless $r = l-1$ and $v_L(x) = 0$. But then $0 = v_L(x^l)$ and $x^l$ is the unique term in minimal valuation, impossible. So we must have $lv_L(x) = lr$, and $v_L(x) = r$, as claimed.

The following result will help to identify when the ring of integers of $L$ is a Galois extension.

PROPOSITION 13.3. *Suppose $L = K[z]$ is totally ramified. Suppose $z^l = 1 + up^{lq+r}$, $u$ a unit, $q < e$, $2 \leqslant r \leqslant l-1$. Let $T = R[x]$ where $x = (z-1)/p^q$. Then $T$ is not integrally closed.*

PROOF. We have

$$\frac{z^l - 1}{p^{ql}} = \left(\prod_{\zeta \neq 1}\frac{\zeta z - 1}{p^q}\right)\frac{z-1}{p^q} = up^r.$$

Let

$$y = \frac{1}{p^{r-1}} \prod_{\zeta \neq 1} \frac{\zeta z - 1}{p^q} = \frac{1}{p^{r-1}} \prod_{i=1}^{l-1} \sigma^i(x).$$

Then $yx = up$, and, using Lemma 13.1, $v_L(y) = l - r \geqslant 0$, and $y$ is in $S$, the integral closure of $R$ in $L$.

However,

$$\begin{aligned} p^{r-1}y &= \frac{z^l - 1}{p^{ql}} \Big/ \frac{z-1}{p^q} = \frac{1 + z + z^2 + \cdots + z^{l-1}}{p^{q(l-1)}} \\ &= \frac{1}{p^{q(l-1)}} \sum_{k=0}^{l-1} (1 + p^q x)^k = \frac{1}{p^{q(l-1)}} \sum_{k=0}^{l-1} \sum_{m=0}^{k} \binom{k}{m} p^{qm} x^m \\ &= \frac{1}{p^{q(l-1)}} \sum_{m=0}^{l-1} \left( \sum_{k=m}^{l-1} \binom{k}{m} \right) p^{mq} x^m \\ &= \frac{1}{p^{q(l-1)}} \sum_{m=0}^{l-1} \binom{l}{m+1} p^{mq} x^m. \end{aligned}$$

So

$$y = \frac{1}{p^{q(l-1)+(r-1)}} \sum_{m=0}^{l-1} \binom{l}{m+1} p^{mq} x^m.$$

Let $c_m$ be the coefficient of $x^m$, $m = 0, \dots, l-1$. Since $q(l-1) + r - 1 < e(l-1) = v_K(l)$, $c_m$ is in $R$ for all $m = 0, 1, 2, \dots, l-2$. But

$$c_{l-1} = \frac{p^{(l-1)q}}{p^{(l-1)q+(r-1)}}$$

is not in $R$ if $r > 1$. So $y$ is not in $T = R[x]$, and $T$ is not integrally closed.

Finally we need to know how we can adjust a generator $z$ of a Kummer extension $L = K[z]$. We retain the hypothesis of this section.

Recall that $lR = \mathfrak{p}^{e(l-1)}$.

**PROPOSITION 13.4.** *Let $L \supset K$ be a Kummer extension, then $z \in L$ may be chosen so that $L = K[z]$, $z^l = w \in R$ and*

(i) *$w$ generates $\mathfrak{p}$, or*

(ii) *$w = 1 + up^k$, $u$ a unit of $R$, $k = lq + r \geqslant 1$, $0 \leqslant r < l$, and*

  (a) *$r \neq 0$ or*

  (b) *$q \geqslant e$.*

*If $w = 1 + up^k$ with $k = lq + r \geqslant 1$, $k < le$ and $r \neq 0$, then $k$ is maximal for all possible $z$ with $L = K[z]$, $z^l \in R$.*

**PROOF.** Let $L = K[y]$, $y^l = v$. If $vR = \mathfrak{p}^t$ and $l \nmid t$, find $s$, $m$ with $ts = 1 + lm$, then $(yp^{-m})^s = z$ satisfies

$$z^l = w = (yp^{-m})^{sl} = v^s p^{1-ts} = (p^t u')^s p p^{-ts} = up \quad \text{for some}$$

units $u$, $u'$ of $R$.

If $l \mid t$, $t = lq$, then $(y/p^q)^l$ is a unit of $R$, so we can assume $y^l = v \notin \mathfrak{p}$. Suppose $v = 1 + up^k$, $u$ a unit of $R$, for some $k > 0$. If $l \mid k$, $k = lq$, let $-u \equiv v_1^l \pmod{\mathfrak{p}}$ (possible since $R/\mathfrak{p}$ is a finite field of characteristic $l$) and set $c = 1 + v_1 p^q$, and $z = cy$, then

$$z^l = (yc)^l = (1 + up^k)(1 + v_1 p^q)^l$$
$$= 1 + up^k + v_1^l p^{ql} + v_1 p^{k+ql} + lv_2,$$

some $v_2 \in \mathfrak{p}^q$,

$$\equiv \begin{cases} 1 \pmod{\mathfrak{p}^{k+1}} & \text{if } k < le, \\ 1 \pmod{\mathfrak{p}^{el}} & \text{if } k \geqslant le. \end{cases}$$

Repeating this construction as needed, we may eventually find $z$ with $z^l = w = 1 + up^k$ with $l \nmid k$ or $k \geqslant le$. If $k = 0$ the argument is similar.

To show maximality, first note that given $z$ with $L = K[z]$, $z^l \in R$, all other elements of $L$ with $y^l \in R$ have the form $y = cz^s$, $c \in R$, $1 \leqslant s \leqslant l - 1$.

Suppose $z^l = w = 1 + up^k$, $k \not\equiv 0 \pmod{l}$, $u$ a unit of $R$, $k < le$. For any $c = 1 + vp^d$, $v$ a unit of $R$, and any $s$, $1 \leqslant s \leqslant l - 1$, we have

$$(cz^s)^l = (1 + vp^d)^l (1 + up^k)^s$$
$$= (1 + v^l p^{dl} + lp^d u_0)(1 + u_1 p^k), \qquad u_0, u_1 \text{ units.}$$

If $k < le$ then

$$(cz^s)^l = 1 + u_2 p^n, \qquad u_2 \text{ a unit,}$$

where $n = \min\{k, dl\}$. Hence if $k < le$, $k \not\equiv 0 \pmod{l}$, then $k$ is maximal.

**14. The local case. III: Galois orders in** $L$. Let $L = K[z]$, $z^l = w \in R$, be a Kummer extension of local fields, with $l \in \mathfrak{p} = pR$, the maximal ideal of $R$. In this section we will classify the Galois and tame extensions of $R$ which are orders over $R$ in $L$.

The case where $l \nmid \nu_{\mathfrak{p}}(w)$ was done in Proposition 8.1. So throughout this section assume $w$ is a unit of $R$. In view of Proposition 13.4 we may assume $w = 1 + p^k u$, $u$ a unit of $R$, where $k = ql + r$, and $1 \leqslant r < l$ or $q \geqslant e$.

Recall that inside $S$, the integral closure of $R$ in $L$, is the chain $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_h$ of Galois extensions of $R$, where $h = \min\{q, e\}$ (Proposition 12.2).

THEOREM 14.1. *Let $S$ be a Galois extension of $R$ which is an order over $R$ in $L$. Then $S = S_m$ for some $m \leqslant h$.*

PROOF. The results of §7 imply that if $S$ is a Galois extension of $R$ such that $SK = L$, then $S$ is a Galois $H_{p^{m(l-1)}}$-extension for some $m$, $0 \leqslant m \leqslant e$, with induced action from that of $KG$ on $L$. By the results of [**14**], $S = R[t]$ with $1 + p^m t = y$ satisfying $y^l = v$ in $R$, $v \equiv 1 \pmod{p^{ml}}$ a unit of $R$. Now $S_m = R[x]$ where $1 + p^m x = z$, $z^l = w \in R$. Since $K[y] = K[z]$, $z = cy^r$ some $c \in K$, and $y = dz^s$, some $d$ in $K$. Since $z$, $y$ are both units of $S$, $c$, $d$ are units of $R$. Substituting, we have

$$(14.2) \qquad 1 + p^m x = c(1 + p^m t)^r \quad \text{and} \quad 1 + p^m t = d(1 + p^m x)^s;$$

thus $c$, $d \equiv 1 \pmod{p^m}$. Writing $c = 1 + p^m e$, $d = 1 + p^m f$, $e, f \in R$, and substituting into (14.2) yields easily that $x \in R[t]$, $t \in R[x]$, so $S = S_m$.

Now we ask when the integral closure of $R$ in $L$ is a Galois extension. Again assume $l \mid v_k(w)$.

THEOREM 14.3. *Let $L = K[z]$, $z^l = w = 1 + p^k u$, $k = ql + r$, is a unit of $R$, and $q \geqslant e$ or $1 \leqslant r < l$. Let $S$ be the integral closure of $R$ in $L$. If $q \geqslant e$ then $S = S_e$ is a Galois extension. If $q < e$, then $S$ is a Galois extension if and only if $r = 1$, in which case $S = S_q$, a Galois $H_{p^{q(l-1)}}$-extension.*

PROOF. Since $S_h \subset S$ where $h = \min\{e, q\}$, and $S_h$ is the largest Galois extension contained in $S$, $S$ is a Galois extension if and only if $S = S_h$.

If $h = e$, $S_e$ is a Galois $RG$-extension so is integrally closed, and $S_e = S$.

If $h = q < e$, set $S_q = R[x]$, $1 + p^q x = z$, then $v_L(x) = r$ by Lemma 13.1. If $r > 1$ then $S_q$ is not integrally closed, hence $S_q \neq S$, by Proposition 13.3. If $r = 1$, then $x$ satisfies the Eisenstein equation

$$\frac{(1 + p^q X)^l - (1 + p^{ql+1} u)}{p^{ql}} = 0$$

which is in $R[X]$ since $lR = \mathfrak{p}^{e(l-1)}$ and $q \leqslant e$. Thus [**21**, Chapitre I, Corollaire to Proposition 17], $S_q = R[x] = S$.

**15. The local case. IV: The order of $S$ in $KG$.** Assume $R$ is a local ring. Let $T$ be a Galois $H_b$-extension of $R$, where $\tilde{b}$, an $(l-1)$th root of $b$, is in $R$. Then the description of Galois $H_b$-extensions of $R$ with normal basis given by Hurley [**14**] applies. Namely, let $H_b = R[\xi]$, $\xi^l = b\xi$, then $T = R[y]$ with $\xi y = 1 + \tilde{b} y = z$, $\xi z = \tilde{b} z$, $z^l = w$ is a unit of $R$ congruent to 1 modulo $\tilde{b}^l$, and

$$v = \frac{1}{b}\left(1 - \sum_{i=1}^{l-1} z^i\right)$$

generates a normal basis for $T$ over $R$, in the sense that $\{v, \xi v, \xi^2 v, \ldots, \xi^{l-1} v\}$ is a basis for $T$ as a free $R$-module.

EXAMPLE 15.1. Let $l = 2$, $H = H_{p^q}$, $T$ a Galois $H$-extension of $R$. Then $T = R[x]$ where $x = (z - 1)/p^q$ satisfies $x^2 + (2/b)x = 2u$, $u$ in $R$ and $v = x = (1 - z)/p^q$ generates a normal basis $\{x, \xi x = z\}$.

Using the existence of the normal basis, we have

PROPOSITION 15.2. *Suppose $L \supset K$ is a Kummer extension of local fields of order $l$ with Galois group $G$, $R$ is the valuation ring of $K$, $l$ is in $\mathfrak{p}$, the maximal ideal of $R$, and $S$ is the integral closure of $R$ in $L$. Suppose $T$ is a tame $H_b$-extension contained in $S$. If $\mathscr{A} = \{\alpha \in KG \mid \alpha T \subseteq T\}$, the order of $T$ in $KG$, then $H_b = \mathscr{A}$.*

PROOF. Since $H_b \subseteq KG$, $H_b \subseteq \mathscr{A}$.

First assume $b$ is in $\mathfrak{p}$, the maximal ideal of $R$. Suppose $\alpha$ is in $\mathscr{A}$, $\alpha T \subseteq T$. Since $T$ is a tame $H_b$-module algebra, where $H_b = R[\xi]$, $T$ is Galois, so $T$ has a basis over

$R$ consisting of $v, \xi v, \xi^2 v, \ldots, \xi^{l-1} v$ for some $v$ in $T$. Let $\alpha = \sum_{i=0}^{l-i} d_i \xi^i$ in $H_b \otimes K = KG$, $d_i \in K$. Then

$$\alpha v = \sum_{i=0}^{l-1} d_i \xi^i v.$$

If $\alpha v$ is in $T$, then $d_i$ must be in $R$ for all $i$, and so $\alpha$ is in $R[\xi] = H_b$. Thus in this case, $\mathscr{A} = H_b$.

Now suppose $b$ is not in $p$. Then $H_b = H_1$ is the integral closure of $RG$ in $KG$. Since $\mathscr{A}$ is an order over $R$ in $KG$, $\mathscr{A} \subseteq H_1$.

That completes the proof.

COROLLARY 15.3. *Suppose $K$, $R$, $L$ are as in* (15.2) *and $S$ is the integral closure of $R$ in $L$. Suppose $L = K[z]$, $z^l = w = 1 + p^k u$, $k \geqslant 1$ maximal, $k = ql + r$, $u$ a unit of $R$. If $r = 1$ or $q \geqslant e$ then the order $\mathscr{A}$ of $S$ is a Hopf algebra.*

**16. The local case. V: Trace, ramification number.** Again assume $L \supset K$ is a Kummer extension of local fields of prime order $l$, let $R$ be the valuation ring of $K$ with maxinmal ideal $\mathfrak{p} = pR$, $S$ the integral closure of $R$ in $L$. Assume $L = K[z]$, $z^l = w$ a unit of $R$, $w = 1 + p^k u = 1 + p^{ql+r} u$, $u$ a unit of $R$, $q \geqslant e$ or $1 \leqslant r < l$. If $q \geqslant e$ then $S$ is a Galois extension of $R$ with group $G$, $\mathrm{tr}(S) = R$ and $\mathfrak{p}$ is unramified in $S$.

Suppose $q < e$, then $\mathfrak{p}$ is totally ramified in $S$. Let $\mathscr{P}$ be the maximal ideal of $S$. Set $G_i = \{\sigma \in G \mid \sigma x \equiv x \pmod{\mathscr{P}^{i+1}}$ for all $x$ in $S\}$, the $i$th ramification group. The ramification number $t$ of $L/K$ is the number $t$ so that $G_t = G$, $G_{t+1} = (1)$.

THEOREM 16.1. *With the above notation, suppose $L = K[z]$, $z^l$ a unit of $R$, and suppose $L/K$ is totally ramified. Then the following are equivalent*:

(i) *$S$ is a Galois $H_{p^{q(l-1)}}$-extension*,

(ii) *$z$ may be chosen with $z^l = 1 + up^{ql+1}$, $u$ a unit of $R$*,

(iii) $t = (e - q)l - 1$,

(iv) $\mathrm{tr}(S) = p^{(e-q)(l-1)} R$.

Note that (i), (iii), (iv) all hold when $L/K$ is unramified (in which case $q = e$).

PROOF. (iii) $\Rightarrow$ (iv). Let $t$ be the ramification number, then

$$v_p(\mathrm{tr}(S)) = [(t + 1)(l - 1)/l]$$

by [**22**, Lemma 4, p. 91]. Then (iii) $\Rightarrow$ (iv) is obvious.

(i) $\Leftrightarrow$ (ii) is Theorem 14.3.

(i) $\Rightarrow$ (iii). If $S$ is a Galois $H_{p^{q(l-1)}}$-extension then

$$S = S_q = R[x], \quad x = (z - 1)/p^q.$$

We have

$$\sigma(x) = \sigma\left(\frac{z-1}{p^q}\right) = \frac{\zeta z - 1}{p^q} = \frac{z-1}{p^q} + \frac{\zeta z - z}{p^q} = x + \frac{x(\zeta - 1)}{p^q}$$

so $\sigma(x) - x$ is in $\mathfrak{p}^{e-q} = \mathscr{P}^{l(e-q)}$, and is not in $\mathscr{P}^{l(e-q)+1}$. So $t = (e - q)l - 1$.

(iv) $\Rightarrow$ (i). Suppose $v_k(\mathrm{tr}(S)) = q(l-1)$, some $q$. Let $t$ be the ramification number, $h = t+1$. Then $q(l-1) = [h(l-1)/l]$. Write $h = cl + r$, $0 \leqslant r < l$. Then

$$q(l-1) = [(cl+r)(l-1)/l] \quad [\mathbf{22}, \text{p. } 91]$$
$$= c(l-1) + [r(l-1)/l], \quad \text{so } c = q \text{ and } r = 0 \text{ or } 1.$$

CLAIM. $S$ is an $H_{p^{(e-q)(l-1)}}$-module algebra.

PROOF OF CLAIM. Let $\pi$ be a uniformizing parameter for $\mathscr{P}$, the maximal ideal of $S$.

If $G = \langle \sigma \rangle$, for any $x$ in $S$, $\sigma(x) \equiv x \pmod{\pi^h}$, so for each $i$,

$$\sigma^i(x) = x + u_i \pi^h \quad \text{for some } u \text{ in } S.$$

Recall that $RG = R[\theta]$, $\theta^l = \omega_l \theta$ where

$$\theta = -\sum_{m \in \mathbf{F}_l^*} \chi^{-1}(m) \sigma^m.$$

Thus

$$\theta(x) = -\sum_{m=1}^{l-1} \chi^{-1}(m) \sigma^m(x)$$
$$= -\sum_{m=1}^{l-1} \chi^{-1}(m) x - \sum_{m=1}^{l-1} \chi^{-1}(m) u_m \pi^h$$
$$= \left( -\sum_{m=1}^{l-1} \chi^{-1}(m) u_m \right) \pi^h.$$

If $h = lq + r$, $0 \leqslant r < l$, let $\xi = \theta / p^q$ in $KG$; then $R[\xi] = H_b$ for $b = \omega_l / p^{q(l-1)}$. For any $x$ in $S$,

$$\xi(x) = \left( -\sum_{m=1}^{l-1} \chi^{-1}(m) u_m \right) \pi^h / p^q,$$

and $\pi^h / p^q = u_1 \pi^r$, an element of $S$ (where $u_1$ is a unit of $S$). Thus $H_b = R[\xi]$ maps $S$ to $S$. Since $H_b = R[\xi] \subseteq KG$ and the action of $H_b$ on $S$ is the restriction of that of $KG$ on $L$, $S$ is an $H_b$-module algebra, completing the proof of the claim.

Now the space of integrals of $H_{p^{(e-q)(l-1)}}$ is generated by

$$\phi = b - \xi^{l-1} = \left( \sum_{i=0}^{l-1} \sigma^i \right) \Big/ p^{q(l-1)}.$$

So $IS = \phi S = \mathrm{tr}(S)/p^{q(l-1)} = R$. It follows that $S$ is a tame, hence Galois $H_{p^{(e-q)(l-1)}}$-extension. Thus (iv) $\Rightarrow$ (i), completing the proof of Theorem 16.1.

COROLLARY 16.2 (cf. [**3**]). *Let $L \supset K$ be a Kummer extension of local fields of prime order $l$. Then $l$ does not divide the ramification number $t$ of $L/K$.*

PROOF. The conclusion is true if $S$ is a Galois $H_b$-extension for some $H_b$, by Theorem 16.1. So assume $S$ is not Galois. In that case, $v_k(\mathrm{tr}(S))$ is not a multiple of $l-1$. So if $h = t + 1 = cl + r$, $0 \leqslant r < l$, again by [**22**, p. 91],

$$v_k(\mathrm{tr}(S)) = [(cl+r)(l-1)/l] = c(l-1) + [r(l-1)/l]$$

is not a multiple of $l-1$. So $r \geqslant 2$, and $t \not\equiv -1$ or $0 \pmod{l}$. That completes the proof.

**17. Globalization.** In this section we obtain global versions of the local results of the previous sections.

Let $L \supset K$ be a Kummer extension of number fields of prime order $l$ with Galois group $G$ and with rings of integers $R = O_K$, $S = O_L$. For each (finite) prime $\mathfrak{p}$ of $K$, let $\hat{R}_\mathfrak{p}$, $\hat{K}_\mathfrak{p}$ be the completions at $\mathfrak{p}$, and let $\hat{S}_\mathfrak{p} = S \otimes_R \hat{R}_\mathfrak{p}$, $L_\mathfrak{p} = L \otimes_K \hat{K}_\mathfrak{p}$. Then $\hat{L}_\mathfrak{p} \supset \hat{K}_\mathfrak{p}$ is a Kummer extension, $\hat{L}_\mathfrak{p} = \hat{K}_\mathfrak{p}[z]$, $z^l \in \hat{K}_\mathfrak{p}$ (even though if $p$ splits completely in $S$, $\hat{L}_p$ will be a direct sum of fields, rather than a field).

PROPOSITION 17.1. *Suppose $L \supset K$ are as above, and at each prime $\mathfrak{p}$ of $R$, we are given a Tate-Oort Hopf algebra $\hat{H}_\mathfrak{p} \subseteq \hat{K}_\mathfrak{p}G$ and a tame $\hat{H}_\mathfrak{p}$-extension $\hat{T}_\mathfrak{p}$ of $\hat{R}_\mathfrak{p}$ contained in $\hat{S}_\mathfrak{p}$ such that at all but a finite number of primes $\mathfrak{p}$, $\hat{T}_\mathfrak{p} = \hat{S}_\mathfrak{p}$. Then there exists a unique Hopf algebra $H$ contained in $KG$ and a tame $H$-extension $T$ of $R$ contained in $S$ such that $T \otimes_R \hat{R}_\mathfrak{p} = \hat{T}_\mathfrak{p}$ and $H \otimes \hat{R}_\mathfrak{p} = \hat{H}_\mathfrak{p}$.*

If we can find unique $H_\mathfrak{p}$ and $T_\mathfrak{p}$ over $R_\mathfrak{p}$, the localization of $R$ at $\mathfrak{p}$, so that $T_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p} = \hat{T}_\mathfrak{p}$, $H_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p} = \hat{H}_\mathfrak{p}$, such that $T_\mathfrak{p} = S_\mathfrak{p}$ for all but a finite number of primes, then, since $H_\mathfrak{p} = R_\mathfrak{p}G$ for all $\mathfrak{p} \nmid l$, $H = \bigcap H_\mathfrak{p}$, and $T = \bigcap T_\mathfrak{p}$ by standard module theory over Dedekind domains. So (17.1) follows from

PROPOSITION 17.2. *Let $R$ be a discrete valuation ring with quotient field $K$, $L$ a finite extension of $K$, $S$ the integral closure of $R$ in $L$. Let $\hat{K}$ be the completion of $K$ with respect to the valuation on $R$, $\hat{R}$ = valuation ring, $\hat{L} = L \otimes_K \hat{K}$, $\hat{S} = S \otimes_R \hat{R}$. Let $T_1$ be an order over $\hat{R}$ in $\hat{L}$. Then there exists a unique order $T$ over $R$ in $L$ with $\hat{T} = T \otimes_R \hat{R} = T_1$.*

PROOF. Since $T_1$ is an order over $\hat{R}$ in $\hat{L}$, there exists some $m$ so that $p^m\hat{S} \subseteq T_1 \subseteq \hat{S}$. Let $i$: $L \to \hat{L}$ be the canonical inclusion. Let $T = \{x \in S \mid i(s) \in T_1\}$. Then $p^m S \subseteq T$. We claim $T_1 = \hat{T}$. We have the following diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \to & T & \to & S & \to & S/T & & \\ & & \downarrow i & & \downarrow i & & \downarrow & & \\ 0 & \to & T_1 & \to & \hat{S} & \to & \hat{S}/T_1 & \to & 0 \end{array}$$

Since $\hat{R}$ is $R$-faithfully flat, $\hat{R} \otimes S/T = \hat{S}/\hat{T}$. But then

$$\begin{aligned} \hat{S}/\hat{T} &= \hat{R} \otimes_R (S/T) = (\hat{R}/p^m\hat{R}) \otimes_R (S/T) = (R/p^mR) \otimes_R (S/T) \\ &= R \otimes_R (S/T) = S/T. \end{aligned}$$

Now $\hat{T} \subseteq T_1$, so $S/T = \hat{S}/\hat{T} \to \hat{S}/T_1$ is surjective, but by definition of $T_1$ $S/T \to \hat{S}/T_1$ is injective. Thus $\hat{S}/T_1 \cong S/T \cong \hat{S}/\hat{T}$, and $T_1 = \hat{T}$.

To show $T$ is unique with $\hat{T} = T_1$, suppose $T'$ has $\hat{T}' = T_1$. Then $T' \subseteq T$, and $\hat{R} \otimes_R T' = \hat{T}' = T_1 = \hat{T} = \hat{R} \otimes T$. By faithful flatness of $\hat{R}$, $T' = T$.

Using 17.1, the globalizations of the local results for Kummer extensions of the previous three sections are immediate. The globalization of the trace criterion of Theorem 16.1 for $\mathcal{O}_L$ is the converse of Theorem 6.1:

THEOREM 17.3. *Let $L \supset K$ be a Kummer extension of prime order $l$ of number fields. Let $\mathscr{W} = \mathrm{Tr}(O_L)$. Then the order $\mathscr{A}$ of $O_L$ is a Hopf algebra and $O_L$ is a tame $\mathscr{A}$-extension if and only if $\mathscr{W}$ is the $(l-1)$th power of an ideal of $O_K$. If so, $\mathscr{A} = H_{\mathscr{B}}$ where $\mathscr{B}\mathscr{W} = lO_K$.*

Here is the global version of the congruence criterion 14.2:

THEOREM 17.4. *Let $L = K[z]$, $z^l = w \in K$ be a Kummer extension of prime order of number fields, with Galois group $G$. Then the order $\mathscr{A}$ of $O_L$ in $KG$ is a Hopf algebra and $O_L$ is a tame $\mathscr{A}$-extension if and only if for each prime $p$ of $O_K$ dividing $lO_K$,*

(a) *$l$ does not divide $v_{\mathfrak{p}}(w)$, or*

(b) *$l$ divides $v_p(w)$ and there is some $c$ in $K$ so that $v_{\mathfrak{p}}(c^l w - 1) \geqslant lv_{\mathfrak{p}}(l)$ or $v_{\mathfrak{p}}(c^l w - 1) \equiv 1 \pmod{l}$.*

If (a) holds for all primes $\mathfrak{p}$ of $O_K$ dividing $lO_K$, then $\mathscr{A} = (O_K G)^*$. If (b) holds for some $\mathfrak{p}$ dividing $lO_K$, then $\mathscr{A} = H_{\mathscr{B}}$ where for each prime $\mathfrak{p}$ of $O_K$ dividing $lO_K$, choosing $c \in K$ so that $v_{\mathfrak{p}}(c^l w - 1) \geqslant le$ or $\equiv 1 \pmod{l}$, we have

If $v_{\mathfrak{p}}(c^l w - 1) \geqslant le$, then $v_{\mathfrak{p}}(\mathscr{B}) = 0$,

If $v_{\mathfrak{p}}(c^l w - 1) = k, 0 < k < le$, then $v_{\mathfrak{p}}(\mathscr{B}) = (k-1)(l-1)/l$.

We may also give a complete classification of Galois extensions inside $O_L$, globalizing Theorem 14.1:

THEOREM 17.5. *Let $L = K[z]$, $z^l = w \in K$ be a Kummer extension of prime order $l$ of number fields. The set $\mathrm{Gal}(L/K)$ of Galois extensions of $O_K$ contained in $O_L$ is as follows:*

(a) *if for some prime $\mathfrak{p}$ of $O_K$, $l \nmid v_{\mathfrak{p}}(w)$, then $\mathrm{Gal}(L/K)$ is empty.*

(b) *if for all primes $\mathfrak{p}$ of $O_K$, $l \mid v_{\mathfrak{p}}(w)$, then the set $\mathrm{Gal}(L/K)$ is in 1-1 lattice-inverting correspondence with the ideals of $O_K$ which are $(l-1)$th powers and which contain $(lO_K)(\mathrm{tr}(O_L))^{-1}$.*

PROOF. An order $S \subseteq O_L$ over $O_K$ in $L$ is a Galois $H_{\mathscr{B}}$-extension if and only if $S_{\mathfrak{p}}$ is a Galois $H_{\mathscr{B}_{\mathfrak{p}}}$-extension for each prime $\mathfrak{p}$ of $O_K$. If $l$ does not divide $v_{\mathfrak{p}}(w)$ for some prime $\mathfrak{p}$, then there are no Galois extension of $O_{K,\mathfrak{p}}$ contained in $L$ by Corollary 8.2, hence (a) holds.

Suppose that $l$ divides $v_p(w)$ for all primes $\mathfrak{p}$ of $O_K$. If $\mathfrak{p}$ is a prime which does not divide $lO_K$, then $O_{L,\mathfrak{p}}$ itself is a Galois $H_{1,\mathfrak{p}}$-extension of $O_{k,\mathfrak{p}}$ and is unique. If $\mathfrak{p}$ divides $lO_K$ we have a chain $S_0 \subset S_1 \subset \cdots \subset S_h \subseteq O_{L,\mathfrak{p}}$ where $S_k$ is a Galois $H_{p^{k(l-1)}}$-extension of $O_{K,\mathfrak{p}}$. Set $L = K[z]$, $z^l = 1 + up^k$ where $k \geqslant le$ or $u$ is a unit in $O_{K,\mathfrak{p}}$ and $l$ does not divide $k$. If $k \geqslant le$ then $h = e$ and $\mathrm{tr}(O_{L,\mathfrak{p}}) = O_{K,\mathfrak{p}}$. If $k < le$, $k = ql + r, 0 < r < l$, then $h = q$.

Thus the set of Galois extensions of $O_K$ contained in $L$ is in 1-1 correspondence with ideals $\mathscr{E}$ so that at $\mathfrak{p}$ not dividing $lO_K$, $\mathscr{E}_{\mathfrak{p}} = (1)$ and at $\mathfrak{p}$ dividing $lO_K$, $\mathscr{E}_p = \mathfrak{p}^{k(l-1)}$ for $0 \leqslant k \leqslant h$. Since $S_h \subseteq O_{L,\mathfrak{p}}$, $\mathrm{tr}(S_k) \subseteq \mathrm{tr}(O_{L,\mathfrak{p}})$ for all $k \leqslant h$. But $\mathrm{tr}(S_h) = \mathfrak{p}^{(e-h)(l-1)}\phi(S_h)$ where $\phi$ generates the space of integrals of $H_{p^{h(l-1)}}$; since $S_h$ is a Galois $H_{p^{h(l-1)}}$-extension, $\phi(S_h) = O_{K,\mathfrak{p}}$. Thus

$$\mathrm{tr}(S_h) = p^{(e-h)(l-1)} \subseteq \mathrm{tr}(O_{L,\mathfrak{p}})$$

and so

$$(lO_K)\left(\operatorname{tr}(O_{L,\mathfrak{p}})\right)^{-1} \subseteq \mathfrak{p}^{h(l-1)} \subseteq \mathfrak{p}^{k(l-1)}$$

for all $k$, $0 \leqslant k \leqslant h$. That completes the proof.

Note that (b) holds if and only if the Kummer order $\tilde{O}_L$ of $O_L$ is a Galois $H_1$-extension of $O_K$. Then $\tilde{O}_L$ corresponds to the unit ideal, and is contained in all other Galois extensions inside $O_L$. This observation allows determination of an upper bound on the number of Galois extensions of rank $l$ of $O_K$:

COROLLARY 17.6. *Let $K$ be a number field containing $\zeta$, a primitive $l$th root of unity, $l$ prime, and suppose $lO_K = (\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g})^{l-1}$ is the factorization of $lO_K = (1-\zeta)^{l-1}O_K$ into a product of prime ideals. Then the number of Galois extensions $S$ of $O_K$ of rank $l$ such that $S \otimes_{O_K} K$ is a Galois extension of $K$ with group $G$, cyclic of order $l$, is at most*

$$\left|U(O_K)/U(O_K)^l\right| \cdot \left|\mathrm{Cl}_l(O_K)\right| \cdot \prod_{i=1}^{g}(e_i+1).$$

PROOF. The first two factors represent the number of Galois $H_1$-extensions of $O_K$. This follows from the exact sequence

$$1 \to \mathrm{NB}(O_K, H_1) \to \mathrm{Gal}(O_K, H_1) \to \mathrm{Prim\,Pic}(H_1) \to 1$$

given by the Picard invariant map [**26**], where $\mathrm{Gal}(O_K, H_1)$ is the group of Galois $H_1$-extensions, $\mathrm{NB}(O_K, H_1)$ is the subgroup of Galois $H_1$-extensions with normal basis, and $\mathrm{Prim\,Pic}(H_1)$ is the subgroup of primitive elements of $\mathrm{Pic}(H_1)$, the group of rank one projective $H_1$-modules. Now $\mathrm{NB}(O_K, H_1) \cong U(O_K)/U(O_K)^l$ by [**14**], and $\mathrm{Prim\,Pic}(H_1) \cong \mathrm{Cl}_l(O_K)$ the $l$-torsion subgroup of the class group of $O_K$, essentially by [**7**, Example 4.16]. The third factor is the number of ideals containing $lO_K$ which are $(l-1)$th powers: this factor is an upper bound for the number of Galois extensions of $O_K$ contained in any Galois extension of $K$ with group $G$ of order $l$, by Theorem 17.5.

COROLLARY 17.7. *Let $K = Q(\sqrt{p})$, $p$ a prime* $\equiv 3 \pmod 4$. *Then $K$ has at most* 12 *Galois extensions of rank* 2.

For $U(O_R)/U(O_K)^2$ has order 4, $\mathrm{Pic}(O_K)$ has odd order, $2O_K$ is the square of a prime ideal, and for any Galois extension $S$ of rank 2, $S \otimes K$ is a Galois extension of $K$ with group $G$ of order 2.

In fact, by genus theory, $\mathrm{Gal}(O_K, H_2) = \mathrm{Gal}(O_K, O_KG)$ has order 2, so the bound of 12 is not best possible: we suspect the correct number is 8.

Corollary 17.7 may be used to show the existence of many Azumaya $O_K$-algebras which are not crossed products for large $p$: see [**31**].

In Corollary 17.6 the hypothesis that $S \otimes K$ be a $KG$-Galois extension of $K$ is necessary. For example, if $l = 3$, there exist nonnormal cubic field extensions of $K$ and any such is a Galois $H$-extension for some rank 3 Hopf $K$-algebra $H \neq KG$: see Theorem 4.6 of [**27**].

REMARK 17.8. It is a straightforward matter to classify the set $\mathcal{T}(O_L/O_K)$ of tame extensions of $O_K$ contained in $O_L$:

$$\mathcal{T}(O_L/O_K) = \prod_{\mathfrak{p}}{}' \mathcal{T}(O_{L,\mathfrak{p}}/O_{K,\mathfrak{p}})$$

where $\prod'$ mean the elements of the direct product over all primes $p$ of $O_K$ such that at all but a finite number of primes $p$, $S_p = O_{L,p}$. Here $\mathcal{T}(O_{L,\mathfrak{p}}/O_{K,\mathfrak{p}})$ is the union of the Galois extensions of $O_{K,p}$ contained in $O_{L,p}$, described in Theorem 14.1, and the non-Galois, tame $H_1$-extensions, which are described in Theorem 8.1.

**18. A cubic example.** By way of illustrating the trace condition of Theorem 17.3, we consider $K = Q(\zeta)$, $\zeta = (-1+\sqrt{-3})/2$, a cube root of unity. H. Wada [**25**] has determined relative integral bases for the rings of integers $O_L$ of $L = K[z]$, $z^3 = w$.

Write $w = st^2$, where $s$, $t$ are cube-free elements of $O_K$, with $s$, $t$ both $\not\equiv -1 \pmod{\sqrt{-3}}$. Then Wada considers three cases.

(i) If $s \not\equiv t \pmod 3$, then $1$, $z$, $z^2/t$ is an $O_K$-basis of $O_L$.

In this case $\mathrm{tr}(O_L) = 3O_K$; since the only prime ideal $\mathfrak{p}$ of $O_K$ containing $l = 3$ is $\mathfrak{p} = \sqrt{-3}\,O_K$, $v_{\mathfrak{p}}(\mathrm{tr}(O_L)) = 2$. So $O_L$ is a tame $(O_KG)^*$-extension of $O_K$.

(ii) If $s \equiv t \pmod{3\sqrt{-3}}$, then $s$ and $t$ are relatively prime to 3, for otherwise $\sqrt{-3}$ divides $t$ or $s$, hence both, and $3\sqrt{-3} = \sqrt{-3}^{\,3}$ would divide $w$, contrary to the assumption that $w$ is cube-free. In this case, $O_L$ has an $O_K$-basis consisting of $1$, $(1-z)/\sqrt{-3}$, and $((s+z+z^2)/t)/3$. Then $\mathrm{tr}(O_L)$ is generated by $3$, $-3/\sqrt{-3} = \sqrt{-3}$ and $s$, so $\mathrm{tr}(O_L) = O_K$. Thus $O_L$ is a tame $O_KG$-extension of $O_K$ (that is, tame in the classical sense [**11**]).

(iii) If $s \equiv t \pmod 3$, $s \not\equiv t \pmod{3\sqrt{-3}}$, then Wada shows that $O_L$ has an $O_K$-basis $1$, $z$, $((1+z+z^2)/t)/\sqrt{-3}$ and $\mathrm{tr}(O_L) = \sqrt{-3}\,O_K$. Thus $v_{\mathfrak{p}}(\mathrm{tr}(O_L)) = 1$ is not divisible by $3-1=2$, so by Theorem 6.1 the order $\mathcal{A}$ of $O_L$ in $KG$ is not a Hopf algebra.

This last fact can be seen directly:

Locally at (3), hence globally, the only Hopf algebras of order 3 contained in $KG$ are $H_{-3}$ and $H_1$ by Corollary 7.2. Since

$$\alpha = \frac{1}{\sqrt{-3}}\,\mathrm{tr} = \frac{1}{\sqrt{-3}}(1+\sigma+\sigma^2)$$

has $\alpha O_L = O_L$, the order $\mathcal{A}$ of $O_L$ in $KG$ contains $\alpha$ but not

$$-\alpha/\sqrt{-3} = (1+\sigma+\sigma^2)/3.$$

Thus $\mathcal{A}$ lies properly between $H_{-3} = O_KG$ and $H_1 = (O_KG)^*$, and so is not a Hopf algebra.

## REFERENCES

1. A.-M. Bergé, *Arithmétique d'une extension Galoisienne a groupe d'inertie cyclique*, Ann. Inst. Fourier (Grenoble) **28** (1978), 17–44.

2. F. Bertrandias, *Decomposition du Galois-module des entiers d'une extension cyclique de degre premier d'un corps de nombres ou d'un corps local*, Ann. Inst. Fourier (Grenoble) **29** (1979), 33–48.

3. F. Bertrandias and M. J. Ferton, *Sur l'anneau des entiers d'une extension cyclique de degre premier d'un corps local*, C. R. Acad. Sci. Paris A **274** (1972), 1330–1333.

4. F. Bertrandias, J.-P. Bertrandias and M. J. Ferton, *Sur l'anneau des entiers d'une extension cyclique de degre premier d'un corps local*, C. R. Acad. Sci. Paris A **274** (1972), 1388–1391.

5. N. Bourbaki, *Algèbre commutative*, Chapitre II, Hermann, Paris, 1961.

6. S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52, 1965, pp. 15–33.

7. S. U. Chase and M. E. Sweedler, *Hopf algebras and Galois theory*, Lecture Notes in Math., vol. 97 Springer, 1969.

8. L. N. Childs, *Representing classes in the Brauer group of quadratic number rings as smash products*, Pacific J. Math. (to appear).

9. L. N. Childs and S. Hurley, *Tameness and local normal bases for objects of finite Hopf algebras*, Trans. Amer. Math. Soc. **298** (1986), 763–778.

10. F. DeMeyer and E. Ingraham, *Separable Algebras Over Commutative Rings*, Lecture Notes in Math., vol. 181, Springer, 1971.

11. A. Frohlich, *Local fields*, Algebraic Number Theory, (J. W. S. Cassels and A. Frohlich, eds.), Thompson, Washington, D. C., 1967.

12. ______, *The module structure of Kummer extensions over Dedekind domains*, J. Reine Angew. Math. **209** (1962), 39–53.

13. S. Hurley, *Tame and Galois Hopf algebras with normal bases*, Thesis, SUNY at Albany, 1984.

14. ______, *Galois objects with normal bases for free Hopf algebras of prime degree*, J. Algebra (to appear).

15. H. Jacobinski, *Über die Hauptordnung eines Korpers als Gruppenmodul*, J. Reine Angew. Math. **213** (1964), 151–164.

16. R. Larson and M. Sweedler, *An associative orthogonal bilinear form for Hopf algebra*, Amer. J. Math. **91** (1969), 75–94.

17. H. W. Leopoldt, *Über die Hauptordnung der ganzen Elementen eines abelschen Zahlkorpers*, J. Reine Angew. Math. **201** (1959), 119–149.

18. T. Ligon, *Galois-Theorie in monoidalen Kategorien*, Algebra Ber. **35** (1978).

19. B. Pareigis, *When Hopf algebras are Frobenius algebras*, J. Algebra **18** (1971), 588–596.

20. P. Ribenboim, *Algebraic numbers*, Wiley-Interscience, New York, 1972.

21. J.-P. Serre, *Corps locaux*, Hermann, Paris, 1962.

22. M. E. Sweedler, *Hopf algebras*, Benjamin, New York, 1969.

23. J. Tate and F. Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21.

24. M. Taylor, *Relative Galois module structure of rings of integers and elliptic functions*. II, Ann. of Math. **121** (1985), 519–535.

25. H. Wada, *On cubic Galois extensions of* $Q(\sqrt{-3})$, Proc. Japan Acad. **46** (1970), 397–400.

26. L. Childs and A. Magid, *The Picard invariant of a principal homogeneous space*, J. Pure Appl. Algebra **4** (1974), 273–286.

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

28. M. Taylor, *Hopf structure and the Kummer theory of formal groups*, J. Reine Angew. Math. **375 / 376** (1987), 1–11.

29. G. Bergman, *Everybody knows what a Hopf algebra is*, Contemp. Math., vol. 43, Amer. Math. Soc., Providence, R. I., 1985, pp. 25–48.

30. R. G. Larson, *Group rings over Dedekind domains*, J. Algebra **5** (1967), 358–361.

31. L. N. Childs, *Azumaya algebras which are not smash products*, Rocky Mountain J. Math. (to appear).

DEPARTMENT OF MATHEMATICS AND STATISTICS, STATE UNIVERSITY OF NEW YORK AT ALBANY, ALBANY, NEW YORK 12222