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 \( A \) be the order of \( S \) in \( KG \). If \( A \) is a Hopf \( R \)-algebra with operations induced from \( KG \), then \( S \) is locally isomorphic to \( A \) as \( A \)-module. Criteria are found for \( A \) to be a Hopf algebra when \( K = \mathbb{Q} \) 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 \( L \supseteq K \) of number fields with Galois group \( G \) as a \( G \)-module, either absolutely (i.e. over \( \mathbb{Z}G \)) 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. \( K = \mathbb{Q} \), \( L = \mathbb{Q}(\sqrt{m}) \), \( m \equiv 2 \) or \( 3 \) (mod 4), or \( L = \mathbb{Q}(\zeta) \), \( \zeta \) 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 \( A \) of \( S \) in \( KG \).

\[ A = \{ \alpha \in KG \mid \alpha S \subseteq S \}, \]

and consider \( S \) as an \( A \)-module. For \( K = \mathbb{Q} \) this approach was successful: \( S \cong A \) as \( A \)-module when \( G = \text{Gal}(L/\mathbb{Q}) \) is abelian. However, in [2 and 3] it is shown that \( S \cong A \) as \( A \)-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 \( A \) is a Hopf \( R \)-algebra with operations induced from those on the Hopf \( K \)-algebra \( KG \) (abusing language we henceforth call such an \( A \) 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.

©1987 American Mathematical Society

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
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 \( \varepsilon: A \to R \) and \( \Delta: A \to A \otimes A \) which make \( A \) into a bialgebra. In applying this general observation to \( \mathcal{A} \), to require that \( \mathcal{A} \) be a Hopf algebra, not just a bialgebra, is to require that \( \mathcal{A} \) be closed under the inverse map, or antipode, of \( KG \).

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

Perhaps of most interest, however, is that fact that part of Noether's theorem may be recast as: if \( \mathcal{A} = RG \), then locally \( S \cong A \) as \( \mathcal{A} \)-module; and in this formulation the result can be generalized, at least for \( G \) abelian, to the case where \( \mathcal{A} \) 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 \( \mathcal{A} \) of \( S \) in \( KG \), \( G \) abelian, is a Hopf subalgebra of \( KG \), the wild \( RG \)-extension \( S \) becomes a tame \( \mathcal{A} \)-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 \( \mathcal{A} \) is a Hopf subalgebra of \( KG \).

When \( K = Q \), the example of \( L = Q(\sqrt{m}) \), \( m \equiv 1 (\text{mod } 4) \), for which \( \mathcal{A} \equiv (ZG)^* \), the dual of \( ZG \), is almost the only possible example. In general, for \( K = Q \), \( L \) an abelian extension of \( Q \), \( \mathcal{A} \) 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 \( \mathcal{A} \) which correspond to ramification groups of \( L/Q \) of order \( > 2 \) are not sent to \( \mathcal{A} \otimes \mathcal{A} \) by the comultiplication on \( KG \).

For Kummer extensions \( L/K \) of prime order \( l \), we find several equivalent conditions for \( \mathcal{A} \) 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 \( \mathcal{A} \) is Hopf if and only if \( \text{tr}(S) \) is the \((l-1)\)th power of an ideal of \( R \). The analysis of when \( \mathcal{A} \) is a Hopf algebra utilizes Tate and Oort's classification of group schemes of order \( l \) over rings of integers; in particular, if \( \mathcal{A} \) is a Hopf algebra, then \( \mathcal{A} = H_{\mathcal{A}} \), the Hopf algebra corresponding to the ideal \( \mathcal{B} \) with \( \mathcal{B} \cdot \text{tr}(S) = lR \).

The determination of when \( \mathcal{A} \) 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 \( \mathcal{A} \cong (RG)_p^\vee \). Our approach in the prime order Kummer case is...
to find all the Hopf subalgebras of \( \mathcal{A}_p \), using the Tate-Oort theory, and then look for Galois extensions with respect to these Hopf algebras (an \( H \)-Galois extension \( S \) with \( S'' = R \) is an \( H^* \)-Galois object in the sense of Chase and Sweedler [7]). We show that to each Hopf subalgebra of \( \mathcal{A} \) 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 \( \mathcal{A} \). 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 \((\text{tr}(S))^{-1})^{-1} \).

Throughout the paper, \( L \supseteq K \) is a Galois extension of number fields, the Galois group \( \text{Gal}(L/K) = G \), 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 \( \mu, i, \Delta, \epsilon, \) and \( \lambda \), respectively.

If \( H \) is a Hopf \( R \)-algebra, the space of (left) integrals \( I \) of \( H \) is the set
\[
I = \{ x \in H \mid \forall y \in H, yx = \epsilon(y)x \}.
\]

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 \( \alpha: S \to S \otimes H^* \) 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
\[
S'' = \{ s \in S \mid \forall \xi \in H, s = \epsilon(\xi)s \}.
\]
We have \( IS \subseteq S'' \) for \( S \) any \( H \)-module algebra. We call \( S \) an \( H \)-extension of \( R \) if \( S'' = R \) 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, \( \text{rank}_R(S) = \text{rank}_R(H) \) as projective \( R \)-modules, and for \( I = \) the space of integrals of \( H \), \( IS = S'' = R \).

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

\[ \mathcal{A} = \{ \alpha \in KG \mid \alpha O_L \subseteq O_L \}, \]

the order of \( O_L \) in \( KG \), and set \( \mathcal{A}^* = \text{Hom}_{O_K}(\mathcal{A}, O_K) \). In [17], Leopoldt proved that if \( K = Q \), \( O_L \) is always a free \( \mathcal{A} \)-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 \( \mathcal{A} \) for \( L \supset K \) a Kummer extension of prime order.

One reason for interest in knowing if \( \mathcal{A} \) is a Hopf algebra is:

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

**Proof.** Suppose \( \mathcal{A} \) is a Hopf algebra. Let \( R = O_K, S = O_L \). By [9, Theorem 5.4], \( O_L \) is locally isomorphic to \( \mathcal{A}^* \) as \( \mathcal{A} \)-module if and only if \( IS = R \) where \( I \) is the space of integrals of \( \mathcal{A} \). Since \( \mathcal{A}^* \) is locally isomorphic to \( \mathcal{A} \) as \( \mathcal{A} \)-module if \( \mathcal{A} \) 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 \( tr = \Sigma_{\sigma \in G} \sigma \), then if \( tr(S) = aR \) (\( R \), being local, is a discrete valuation ring), \( \theta = tr/a \) maps \( S \) onto \( R \). Thus \( \theta \in \mathcal{A} \). Since \( \mathcal{A} \) is a Hopf subalgebra of \( KG \) and \( tr \) is an integral of \( KG \), \( \theta \) is an integral of \( \mathcal{A} \). 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 $K_v$ be the completion of $K$ at a (finite) prime $v$, $R$ the valuation ring. If $v \cap Z \neq (l)$, then the only Hopf $R$-algebra of interest is the group ring $RG$, which, since $R$ contains $1/l$ and $\xi$, is isomorphic to $\text{Hom}_R(RG, R) = (RG)^*$. The local structure of the Tate-Oort Hopf algebraswhen $v \cap Z = (l)$, involves certain constants $\omega_1, \ldots, \omega_l$, obtained as follows.

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

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

Then $\theta_i = \omega_i \theta_{i-1}$, $i = 1, \ldots, l - 1$, and $\theta_l = \omega_l \theta_0$, 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 $\Delta: H \to H \otimes H$ is given by

$$\Delta(\xi^i) = 1 \otimes \xi^i + \xi^i \otimes 1$$

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

the counit $\epsilon: H \to R$ by $\epsilon(\xi^i) = 0$ for $i > 0$, and the antipode $\lambda: H \to H$ 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

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

(c.f. [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 $\xi \mapsto u \xi': (u \xi')^l = u b' \xi' = b(u \xi')$. Whenever $\xi \in R$, $RG \cong (RG)^*$, so $\omega_l$ has an $(l - 1)$st 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 $\tilde{b}^{l-1} . 1 = b$ and (3.2) we obtain inclusions

$$RG = H_{\omega_l} \subseteq H_{\tilde{b}} \subseteq H_{\tilde{a}} = (RG)^*.$$
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 $\nu$ be a prime divisor of $lR$ and $R_\nu$, $K_\nu$ be the completions of $R$, $K$ at $\nu$, respectively. Then $H \otimes_R R_\nu = H_\nu$ for $b$ some divisor of $lR = (1 - \xi)^{l-1} = \nu^{(l-1)e}$. Since $H_\nu \subseteq R_\nu G$, $b$ is an $(l-1)$th power, so $bR = \nu^{(l-1)s}$ for some $0 \leq s \leq e$. If $l \not\in \nu$ then $H \otimes_R R_\nu = R_\nu G \equiv (R_\nu G)^* = H_1$, so $e = 0$. Thus to $H$ corresponds the ideal $\mathfrak{P} = \prod_{\nu \mid l} \nu^{(l-1)s}$. The lattice-preserving property follows from (3.2).

Notation. (3.4). Denote by $H_{\mathfrak{P}}$ the Hopf subalgebra of $KG$ corresponding to the ideal $\mathfrak{P}$ of $O_K$. If $\mathfrak{P} = \mathfrak{p}^{l-1}$, for each prime ideal $\mathfrak{p}$ of $O_K$, $H_{\mathfrak{P}} \otimes_{O_K} O_{K,\mathfrak{p}} = H_\mathfrak{p}$ where $b$ is the $(l-1)$th power of a generator of $\mathfrak{p} \otimes O_{K,\mathfrak{p}}$

(3.5) For $H = H_{\mathfrak{P}} = R[\xi]$, 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 $RG = H_{\omega_i} = R[\theta]$, $\theta = \tilde{a}\xi$, so

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

(from (3.1))

and so

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

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

We will denote $\sum_{\sigma \in G} \sigma = \text{tr}$ since the action of $\text{tr}$ 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 $\text{tr}(S) = aR$, a principal ideal of $R$. Then $S$ is a tame $H_b$ extension, $b = 2/a$, and $H_b = \{ \alpha \in KG | \alpha S \subseteq S \}$.

Proof. First we note that $a$ divides 2, since $\text{tr}(1) = 2$ 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 $S$, $\text{tr}(s) = ar$. 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 $\text{tr}(s) = a$, then $((\sigma + 1)/a)s = 1$. So $IS = R$, and $S$ is a tame $H_b$ module algebra.
Let \( \mathcal{A} = \{ \alpha \in KG \mid \alpha S \subseteq S \} \). Since \( \mathcal{A} S \subseteq S \), \( \mathcal{A} \) is integral over \( R \), so \( \mathcal{A} \subseteq (RG)^* = H_1 = R[y] \), \( y^2 = y \). Further, \( H_b \subseteq H_1 \) by \( \xi = by \). So any \( \alpha \) in \( \mathcal{A} \) has the form \( \alpha = m + n(\xi/b) \), \( m, n \) in \( R \). Let \( s \) be in \( S \), not in \( R \), with \( \text{tr}(s) = a \). If \( \alpha \) is in \( \mathcal{A} \), then

\[
(m + n(\xi/b))(s) = ms + n(\xi s/b)
= ms + n(bs - 1)/b
= ms + ns - n/b
\]
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 \( \mathcal{A} \subseteq H_b \). 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 \( \text{tr}(O_L) \) 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

\[
b = 2 \begin{cases} \quad \text{if } d \equiv 1 \pmod{4}, \\ 1 \quad \text{if } d \equiv 2, 3 \pmod{4}.
\end{cases}
\]

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 \( \leq 2 \), the ring of integers \( O_L \) of \( L \) is not tame for any \( Z \)-Hopf subalgebra of \( QG \), \( G = \text{Gal}(L/Q) \).

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

\[
e_p = \frac{1}{|G_p|} \sum_{\sigma \in G_p} \sigma \quad (|G_p| = \text{order of } G_p)
\]
corresponding to some (possibly trivial) \( p \)-subgroup \( G_p \) of \( G \). Then \( \mathcal{A} \) is a Hopf subalgebra of \( QG \) if and only if \( |G_2| \leq 2 \) 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 \( \mathcal{A} \) is generated over \( Z \) by elements of \( G \) and idempotents \( e_q \) for \( q \) dividing the order of \( G \), \( \Delta e_p \) is in \( \mathcal{A} \otimes \mathcal{A} \) if and only if \( \Delta e_p \) is a \( Z \)-linear combination of the generators \( \sigma \otimes \tau, \sigma \otimes e_q \otimes \tau, \) and \( e_q \otimes e_q \) in \( \mathcal{A} \otimes \mathcal{A} \), 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 $\mathbb{Z}$-linear combination, and (in $QG \otimes QG$) collect the coefficients of $\pi \otimes \pi$, $\rho \otimes \rho$. Since $\pi, \rho \neq 1$ in $G$, the only generators of $\mathcal{A} \otimes \mathcal{A}$ which contribute nonzero coefficients are the generators $\pi \otimes \pi$, $\rho \otimes \rho$ and $\pi \otimes \rho$ 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

$$\Delta e_p = \frac{1}{m} \sum_{\sigma \in G_p} \sigma \otimes \pi = a_{0,0} e_p \otimes e_p + \sum_{\sigma \in G_p} a_{\sigma,0} \sigma \otimes e_p$$

$$+ \sum_{\tau \in G_p} a_{0,\tau} e_p \otimes \tau + \sum_{\sigma, \tau \in G_p} a_{\sigma, \tau} \sigma \otimes \tau$$

$$+ (\text{other terms not containing } \sigma \otimes \tau \text{ for } \sigma, \tau \neq 1 \text{ in } G_p),$$

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

$$1 = \frac{1}{m} a_{0,0} + \frac{1}{m} a_{\pi,0} + \frac{1}{m} a_{0,\pi} + a_{\pi,\pi}$$

(5.2)

of $\pi \otimes \rho$:

$$0 = \frac{1}{m} a_{0,0} + \frac{1}{m} a_{\pi,0} + \frac{1}{m} a_{0,\rho} + a_{\pi,\rho}$$

(5.3)

of $\rho \otimes \pi$:

$$0 = \frac{1}{m} a_{0,0} + \frac{1}{m} a_{\rho,0} + \frac{1}{m} a_{0,\pi} + a_{\rho,\pi}$$

(5.4)

of $\rho \otimes \rho$:

$$1 = \frac{1}{m} a_{0,0} + \frac{1}{m} a_{\rho,0} + \frac{1}{m} a_{0,\rho} + a_{\rho,\rho}.$$ 

(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 $\mathcal{A} \otimes \mathcal{A}$ if $|G_p| > 2$. Since $G_p$ is a $p$-group, if $\mathcal{A}$ is a Hopf subalgebra of $QG$ we must have $G_p = (1)$ if $p$ is odd, and $|G_2| < 2$.

Conversely, if $\mathcal{A} = ZG + ZG e_2$ where $G_2 = \langle a \rangle$ has order 2, then $e_2 = (1 + a)/2$, $\mathcal{A}$ contains $e_2 = e_2 - a = (1 - a)/2$, and $\Delta e_2 = e_2 \otimes e_2 + e_2 \otimes e_2$. So $\mathcal{A}$ 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 $\mathcal{A}$ of $O_L$ in $QG$ is a Hopf subalgebra of $QG$ if and only if either $L \supset Q$ is tamely ramified (i.e., $\mathcal{A} = ZG$), 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 $\mathcal{A}$ 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 \( \mathcal{A} \) 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 \( \mathcal{A} \) 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 \( \mathcal{A} \), 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 \( \mathcal{A} \) 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) \( \mathcal{A} = H_\mathcal{B} \) for some ideal \( \mathcal{B} = \mathcal{B}^{l-1} \) dividing \( lO_K \). Using this fact, we obtain a necessary condition for \( \mathcal{A} \) to be a Hopf algebra.

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

Proof. If \( \mathcal{A} \) is a Hopf algebra, then \( O_L \) is locally isomorphic to \( \mathcal{A}^* \) as \( \mathcal{A} \)-module, \( \mathcal{A}^* = \text{Hom}_{O_K}(\mathcal{A}, O_K) \). Now \( \mathcal{A}^* \) is the trivial Galois \( \mathcal{A}^*-\)object, so \( l\mathcal{A}^* = O_K \), \( l \) the space of integrals of \( \mathcal{A} \), by [9, Proposition 2.3]. Since \( O_L \) is locally isomorphic to \( \mathcal{A}^* \) as \( \mathcal{A} \)-module, \( lO_L = O_K \).

Locally at \( p \), \( \mathcal{A} = H_{p^{l-1}e} \) for some \( s, 0 \leq s \leq e \), where \( lO_K, p = p^{l-1}e \) and \( p \) is a uniformizing parameter for \( p \). So \( \mathcal{A} \) corresponds to the ideal \( \mathcal{B} = \prod p^{l-1} \). But if \( \theta \) generates the space of integrals of \( H_{p^{l-1}e} \), then since \( O_K, p G = H_{p^{l-1}e}, \text{tr} = p^{l-1}(e-s)\theta \). Thus
\[
\text{tr} O_L = \prod p^{l-1}(e-s) = (lO_K)(\prod p^{l-1})^{-1} = (lO_K)(\mathcal{B})^{-1}.
\]
Since \( lO_K = (1 - \xi)lO_K \) and \( \mathcal{B} \) is an \((l-1)\)th power by Theorem 3.3, \( \mathcal{W} = \text{tr} O_L \) 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 \( \xi \), \( l \) 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 \( \sigma(z) = \xi z \). 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 \( H_b = R[\xi] \).

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
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 \( H_b \equiv KG \).

**Proof.** Given \( b \), let \( K' = K[\tilde{b}] \), \( L' = L \otimes K' \), \( H_b' = H_b \otimes K' \). We have \( H_{\omega_i} = KG \cong (KG)^* = H_1 \), so by (3.2), \( \omega_i \) has an \((l - 1)\)th root \( \tilde{\omega}_i \) 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 \( H_b' = H_b^{l-1} \cong H_{\omega_i} \), so the action \( \varphi \) yields an action of \( H_{\omega_i} = K'G \) on \( L' \), that is, a map \( G \to \text{Aut}_K(L') \).

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 \( L = K[z] \), \( f(x) = \text{Irr}(z, K) \), the minimal polynomial of \( z \) over \( K \), and \( g(x) = \text{Irr}(z, K') \), 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 \( \text{Irr}(z, K) \) has degree \( \deg[K': K] = l < l \), impossible.

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

Let \( H_{\omega_i} = K'G = K' [\theta] \), \( \theta^l = \omega_i \theta \); \( H_b = K[\xi] \), \( \xi^l = b \xi \); then we have an isomorphism of Hopf algebras \( H_{\omega_i} \to H_b' \) by \( \theta \to \tilde{\alpha} \xi \), \( \tilde{\alpha} = \tilde{\omega}_i / \tilde{b} \). 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 \( G \), \( \sigma(z) = \xi z \), for some root of unity \( \xi \), we have

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

Since \( H_b = K[\xi] \) acts on \( L \) and \( z^i \in L \), then \( \xi z^i \in L \) for all \( i \), that is, for all \( i \), \( - (1/\tilde{a}) \sum_m \chi^{-1}(m) \xi^{im} \in \text{Lie} L \). But since \( \sum_m \chi^{-1}(m) \xi^{im} \in L \), that is the case if and only if \( \tilde{a} \) is in \( L \) or \( \sum \chi^{-1}(m) \xi^{im} = 0 \) 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 \( \tilde{b} = \tilde{\omega}_i / \tilde{\alpha} \) is in \( K \), and \( H_b \equiv H_{\omega_i} \). 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 $L \supseteq K$ 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], $\tilde{S} = \sum_{\sigma \in \hat{G}} S_{\chi}$, where

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

Then $\tilde{S}$ is a tame $(RG)^*$-extension of $S$ 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 $\tilde{S}$,

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

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

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

If $v_p(w) = 0$, 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

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

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

If $v_p(w) > 0$, let $rs - kl = 1$, and let $z = y^s/p^k$. Then $z^l = y^{sl}/p^{kl} = w^s/p^{kl}$ and $v_p(z^l) = rs - kl = 1$. 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 $S_{\chi} = Rz^l$, and $S = \tilde{S}$.

Set $(RG)^* = \sum R e_\chi, e_\chi = (\sum_\sigma \chi(\sigma^{-1})\sigma)/l$; the integral $I$ of $(RG)^* = Re_{\chi_0}$. Then $e_\chi S = S_{\chi}$ and in particular, $IS = S_{\chi} = S^G = R$. 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 $v_p(w) = 0$ (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

$$T = (RG)^*T = \sum R e_\chi T = \sum e_\chi T = \sum T_{\chi},$$

and $T_{\chi} \subseteq S_{\chi}$. Thus $T$ is a $G$-graded subalgebra of $\tilde{S}$. Tameness means simply that $T_{\chi_n} = R$ and each $T_{\chi'} \neq 0, (0)$, 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 $\mathcal{S}$ is the unique such Galois $(RG)^*$-module algebra.

Proof. $T$ is a Galois $(RG)^*$-module algebra if and only if $T = \Sigma T_x$ with $T_x = R^{z_x}$ and $T_x T_\psi = T_{x\psi}$ for all $\chi, \psi$ in $\hat{G}$, in particular, $T_x = R$. Thus $T$ is Galois if and only if each $z_x$ is a unit of $S$, in which case $T_x = S_x$, $T = \mathcal{S}$ and $\mathcal{S} = R[z]$ with $z^l$ a unit of $R$.

9. Galois extensions. In contrast to the situation for $H_h = H_x = (RG)^*$, 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 $\wp$ of $R$; let $G$ be cyclic of order $l$. Let $H_h$ be a Tate-Oort Hopf $R$-algebra, $RG \subseteq H_h \subseteq (RG)^*$. Suppose $b \in \wp$. Then any tame $H_h$-extension of $R$ is Galois.

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

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

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

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

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

So, mod $p$, $s, \xi s, \xi^2 s, \ldots, \xi^{l-1} s$ are linearly independent, so are a basis. Thus, $s, \xi s, \ldots, \xi^{l-1} s$ 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 $s, \xi s, \ldots, \xi^{l-1} s$ form a basis of $S$.

Let $h_0, \ldots, h_{l-1}$ be a dual basis in $H_h^*$ for $1, \xi, \xi^2, \ldots, \xi^{l-1}$ in $H_h$. Now $S$ is an $H_h^*$-object via the map $\alpha: S \to S \otimes H_h^*$ 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 $H_h$-extension of $R$ if and only if $\gamma$ is an isomorphism. Since $S \otimes S$ and $S \otimes H_h^*$ 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

$$a_k = \begin{cases} 0 & \text{for } k > i, \\ 1 & \text{for } k = i, \\ -\sum a_m (\xi^k b) & \text{for } k < i. \end{cases}$$
Then
\[ \gamma \left( \sum_{k} a_k \otimes b_k \right) = \sum_{j} \left( \sum_{k} a_k \xi^j b_k \right) \otimes h_j \]
\[ = \sum_{j} \left( \sum_{k} a_k \xi^j \xi^{j-1-k} \right) \otimes h_j \]
\[ = \sum_{j} \left( \sum_{k \geq j} a_k \xi^{j-1-k} \right) \otimes h_j \]
since \( \xi^j = b \xi = 0 \),
\[ = \sum_{j} \left( \sum_{k \geq j} a_k \xi^j \right) \otimes h_j. \]

For \( j > i, k \geq j, a_k = 0 \), so
\[ \sum_{k \geq j} a_k \xi^j b_k = 0. \]

For \( j = i \),
\[ \sum_{k \geq i} a_k \xi^i b_k = a_i \xi^i b_i + \sum_{k > i} a_k \xi^i b_k = a_i \xi^i b_i, \]
since \( a_i = 1 \) and \( \xi^i b_i = \xi^{i-1} s = 1 \), \( \xi^i b_i = 1 \).

For \( j < i \),
\[ \sum_{k \geq j} a_k \xi^j b_k = \sum_{k > j} a_k \xi^j b_k + a_j \xi^j b_j. \]
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 \( \gamma(\sum a_k \otimes b_k) = 1 \otimes h_i \), 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 \( H \),
\[ I = \{ \theta \in H \mid h \theta = \epsilon(h) \theta, \text{for all } h \text{ in } H \} \]
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
\[ j : S^H \rightarrow \text{End}_R(S), \quad j(s^h)(t) = sh(t) \]
is an isomorphism [7, Theorem 9.3]. Denote the image of \( S \) in \( \text{End}_R(S) \) under \( j \) by \( S_j \), 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 \( \varphi: I \otimes S \to S^* (= \text{Hom}_R(S, R)) \), \( \varphi(\theta, s)(t) = \theta(st) \) for \( \theta \) in \( I \), \( s, t \) in \( S \), is an isomorphism.

**Proof.** For \( M \) an \( R \)-submodule of \( \text{End}_R(S) \) denote by \( I \cdot M \) the set \{ \( \theta m \) \mid \( m \) in \( M \), \( \theta \) in \( I \) \}. Then since \( IS \subseteq S^H = R \), \( I \cdot S_i \subseteq S^* \subseteq \text{End}_R(S) \). The image of \( \varphi \) is then \( I \cdot S_i \). 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 \( I \cdot S_i = S^* \). So we shall show that \( S \) is Galois if and only if \( I \cdot S_i = S^* \).

**Lemma 10.2.** \( I \cdot (S^H)_i = I \cdot S_i \).

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

Suppose \( I \cdot S_i = S^* \). Then we have the diagram

\[
\begin{array}{ccc}
S \otimes S^* & \overset{\cong}{\Downarrow} & S \otimes I \cdot S_i \\
\text{End}(S) & \overset{\cong}{\twoheadrightarrow} & j(S^H) \\
\end{array}
\]

where

\[
m(s \otimes \theta(s^H))(t) = \left( \sum s(\theta_{(1)}s')(\theta_{(2)}h) \right)(t) = \sum s(\theta_{(1)}s')(\theta_{(2)}h)(t) = j(\sum s(\theta_{(1)}s')\theta_{(2)}h)(t) = j(s)(t)
\]

and \( \mu(s^f)(t) = sf(t) \).

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

\[
m(s \otimes \theta \cdot s')(t) = \sum s(\theta_{(1)}s')(\theta_{(2)}t) = s\theta(s't) \quad \text{(by measuring)}.
\]

Thus \( j(S^H) = \text{End}_R(S) \), and \( S \) is Galois.

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

\[
\text{End}_R(S) \cong S \otimes I \cdot (S^H)_i = S \otimes I \cdot S_i
\]

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

\[
\begin{array}{ccc}
S \otimes S^* & \overset{\cong}{\Rightarrow} & S \otimes I \cdot S_i \\
\text{End}(S) & \overset{\cong}{\Rightarrow} & \text{End}_R(S)
\end{array}
\]

commutes, and so the inclusion \( I \cdot S_i \subseteq S^* \) induces an isomorphism \( S \otimes I \cdot S_i \cong S \otimes S^* \). Since \( S \) is \( R \)-faithfully flat, \( I \cdot S_i = S^* \).
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

\[
(\phi(y \# h))(x) = \sum \phi_{(1)}(y) \phi_{(2)} h(x)
\]

\[
= \sum \phi_{(1)}(y) \phi_{(2)} \varepsilon(h_{(1)}) h_{(2)}(x) \quad \text{since } (1 \otimes \varepsilon) \Delta = \text{id},
\]

\[
= \sum \phi_{(1)}(\varepsilon(h_{(1)}))(y) \phi_{(2)} h_{(2)}(x)
\]

\[
= \left( \sum \phi_{(1)}(\varepsilon(h_{(1)})) \otimes \phi_{(2)} h_{(2)}(x) \right) (y \otimes x)
\]

\[
= \Delta(\phi \varepsilon(h_{(1)}))(1 \otimes h_{(2)})(y \otimes x)
\]

\[
= \Delta(\phi h_{(1)})(1 \otimes h_{(2)})(y \otimes x) \quad \text{since } \phi \text{ is a right integral,}
\]

\[
= \left( \sum \phi_{(1)} h_{(1)} \otimes \phi_{(2)} h_{(2)}(x) \right) (y \otimes x)
\]

\[
= \left( \sum \phi_{(1)} h_{(1)} \otimes \phi_{(2)}(y \otimes x) \right)
\]

\[
= \left( \sum \phi_{(1)} h_{(1)} \otimes \phi_{(2)}(y \otimes x) \right)
\]

\[
= \phi(h^\lambda y \cdot x) = \phi(h^\lambda y)_{(1)}(x).
\]

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 \( H = K[f_1, \ldots, f_n] \) with \( f_i^p = 0 \), \( f_i \) commuting and primitive, \( e(f_i) = 0 \) for all \( i \).

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

For \( R = (r_1, r_2, \ldots, r_n) \), 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 \( P = 1 = (p - 1, p - 1, \ldots, p - 1) \), the space of integrals of \( H \) is generated by \( \theta = f_i^{p - 1} \). Then \( \{ y^R | 0 \leq r \leq P \} \) is a \( K \)-basis of \( L \), and if \( \{ \varphi_R \} \) is a dual basis, we have \( \varphi_{P-1} = \theta \). Then \( \varphi_R(y^S) = \theta(y^{P-1} y^S) \), and \( \theta \cdot L = L^* \). 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.** \( H \equiv I \otimes H^* \) 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 \( (xf)(y) = f(yx) \) and \( H^* \) 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 \( \varphi : I \times H^* \to H \) 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
\[
\langle x \varphi(\theta, f), g \rangle = \langle x, g_{(1)} \rangle \langle \varphi(\theta, f), g_{(2)} \rangle = \langle x, g_{(1)} \rangle \langle \theta, fg_{(2)} \rangle = \langle x, g_{(1)} \rangle \langle \theta_{(1)}, f \rangle \langle x \theta_{(2)}, g \rangle
\]
\[
= \langle x^\lambda \theta_{(1)}, f \rangle \langle \theta_{(2)}, g \rangle = \langle x^\lambda f_{(1)}, \theta_{(1)}, f_{(2)} \rangle \langle \theta_{(2)}, g \rangle
\]
\[
= \langle x^\lambda f_{(1)}, \theta, f_{(2)} g \rangle = \langle \theta, f_{(1)} x^\lambda f_{(2)} g \rangle
\]
\[
= \langle \theta, (x \cdot f) g \rangle = \langle \varphi(\theta, x \cdot f), g \rangle.
\]
So \( x \varphi(\theta, f) = \varphi(\theta, x \cdot f) \), completing the proof.

**Corollary 10.5 (Pareigis [19]).** As left \( H \)-modules, \( H^* \equiv H \), 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 \( e(\theta) \neq 0 \), 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 \( \beta : H^* \times H^* \to R \), \( \beta(p, q) = (pq)\theta \), 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 \( C = \{ x \in L \mid \theta x \in R \text{ for all } \theta \text{ in } I \} \supseteq S \). Then \( I \cdot C_I = S^* \). 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, \( I \cdot L_I = L^* \) by Theorem 10.1, and so, viewing \( \theta \) as in \( \text{Hom}_R(S, R) \subseteq \text{Hom}_K(L, K) \), \( S^* \subseteq \theta \cdot L_I \), and \( S^* = \theta \cdot C_I \), where \( C = \{ x \in L \mid \theta x \in S^* \} \). But
\[
S \subseteq C
\]

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
commutes, where $\beta(x)(y) = \theta(xy)$. Since $\beta: C \to S^*$ is an isomorphism, $S = C$ if and only if $\beta|_S$ is an isomorphism, if and only if $I \cdot S_I = S^*$. 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 $\{x_1, \ldots, x_n\}$ be a basis of $S$ as a free $R$-module.

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

Let $\{f_1, \ldots, f_n\}$ be a dual basis in $S^*$ to $\{x_1, \ldots, x_n\}$. Let $\{y_1, \ldots, y_n\}$ 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

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

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

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 $S^* = \theta \cdot S$, 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 $\{x_1, \ldots, x_n\}$ 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 $\{x_1, \ldots, x_n\}$, 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 $\theta = \sum_{\sigma \in G} \sigma = \text{tr}$; $\delta_H(S/R)$ 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 $\delta_H(S/R) = \det(\text{tr}(z^iz^j))$. Since

$$\text{tr}(z^r) = \begin{cases} 0, & r \neq 0 \pmod{n}, \\ nz^r, & n | r, \end{cases}$$

we have

$$\det(\text{tr}(z^iz^j)) = \det \begin{pmatrix} n & 0 & \cdots & 0 \\ 0 & nb & \cdots \\ \vdots & \vdots & \ddots \\ 0 & nb \\ 0 & 0 \end{pmatrix} = \pm n^n b^{n-1}.$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
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 $H = (RG)^* = \sum_{k=0}^{n-1} R e_k$, $e_k(\sigma^j) = \delta_{k,j}$. Then $I = Re_0$.

Define $H$ on $S$ by $e_k(z^j) = \delta_{k,j}z^j$. Then
\[
\delta_H(S/R) = \det(e_0(z^j))
= \det \begin{pmatrix}
1 & 0 & \cdots & 0 \\
0 & 0 & \cdots & b \\
\vdots & \vdots & \ddots & \vdots \\
0 & b & \cdots & 0
\end{pmatrix}
= \pm b^{n-1}.
\]
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 $\mathbb{Z}[\xi]$, $\xi$ a primitive $l$th root of unity, $l$ an odd prime. Let $p$ generate the maximal ideal of $R$, and let $I = (pR)^{e(l-1)}$. Let $H_h$ be the Tate-Oort Hopf algebra $R[\xi]$, with $\xi^p = b\xi$, and comultiplication
\[
\Delta(\xi^i) = (1 \otimes \xi^i) + (\xi^i \otimes 1)
+ \frac{w}{1-l} \left[ \sum_{j=1}^{l-1} \frac{b^j}{\omega_j} \otimes \frac{\xi^{i-j}}{\omega_j} + \sum_{j=i}^{l-1} \frac{a^i}{\omega_j} \otimes \frac{\xi^{i-1+i-j}}{\omega_j} \right]
\]
where $ab = \omega_j$.

Let $K$ be the quotient field of $R$, and $L = K[z]$, $z^l = w$, $w$ in $R$. For $0 \leq s \leq e$, let $S = R[x]$, $x = (z-1)/ps$. Then $x$ satisfies $(1 + p^s z)^l = w$; or
\[
x^l + \left( \frac{l}{l-1} \right) x^{l-1} + \cdots + \left( \frac{l}{r} \right) x^r \frac{x^r}{p^{(l-r)s}} + \cdots + \left( \frac{l}{1} \right) \frac{x}{p^{(l-1)s}} = \frac{w-l}{p^{sl}}.
\]
Since $s \leq e$, all coefficients of $x^r$, $r > 0$, are in $R$, and $x$ is integral over $R$ if and only if $w \equiv 1 \pmod{p^u}$.

Suppose $w = 1 + p^u c$, $c$ in $R$.

Let $H_h$, $b = p^{ul-1}$ act on $S$ by $\xi x = 1 + p^s x = z$, $\xi z = p^s z$. Then $H_h$ sends $Rx$ into $S$. But then, using the measuring property:
\[
\xi^i(x^r x^s) = x^r(\xi^i x^s) + (\xi^i x^r)x^s
+ \frac{w_i}{1-l} \left[ \sum_{j=1}^{l-1} \left( \frac{\xi^i x^s}{\omega_j} \right) \left( \frac{\xi^i x^r}{\omega_j} \right) + \sum_{j=i}^{l-1} \left( \frac{\xi^i x^r}{\omega_j} \right) \left( \frac{\xi^{i-1+i-j} x^s}{\omega_j} \right) \right].
\]
one sees easily by induction on $k$ that $H$ sends $Rz^k$ into $S$ for all $k > 0$. Thus $H_h$ acts on $S$.

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

Thus

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

and so

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

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

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

So

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

where

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

Thus $(\det A)^2 = p^{s(l-1)s}$ 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 $H_{p^{r(l-1)}}$-extension of $R$.

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

Summarizing, we have shown

\textbf{Theorem 12.2.} Let $K$ be a local field with valuation ring $R$, maximal ideal $\wp = pR$ and $l \in \wp$. Let $L \supseteq K$ 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 $0 \leq r < l$ 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 $R$, $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_q$, all contained in $S$, where $S_k$ is a Galois $H_{p^{r(l-1)}}$-extension of $R$, $0 \leq k \leq h$, and $h = \min\{ql+r\}$.
13. Some lemmas on Kummer extensions of prime order. Throughout this section, let $K$ be a local field, a finite extension of $\mathbb{Q}_l$, 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 $z' = 1 + up^{lq+r}$, $u$ a unit of $R$, where $q < e$ and $0 < r < l$. Set $x = (z - 1)/pq$. Then $v_L(x) = r$.

**Proof.** Since $z' = 1 + up^{lq+r}$, $x$ satisfies

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

or

$$(13.2) \quad 0 = x^l + \frac{lp^{q(l-1)}}{p^{ql}} x^{l-1} + \cdots + \left(\begin{array}{c} l \\ k \end{array}\right) \frac{p^{qk} x^k}{p^{ql}} + \cdots + \frac{lp^q}{p^{ql}} - up^r.$$ 

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 $1 \leq k \leq l - 1$, 

$$v_L\left(\left(\begin{array}{c} l \\ k \end{array}\right) \frac{x^k}{p^{q(l-k)}}\right) = el(l-1) + kv_L(x) - lq(l-k)$$

$$\geq el(l-1) - l(e-1)(l-1) + kv_L(x)$$

$$\geq l(l-1) + kv_L(x).$$

Thus

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

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 $z' = 1 + up^{lq+r}$, $u$ a unit, $q < e$, $2 \leq r \leq l - 1$. Let $T = R[x]$ where $x = (z - 1)/p^q$. Then $T$ is not integrally closed.

**Proof.** We have

$$z^l - 1 = \left(\prod_{k \neq 0} \frac{kz - 1}{p^q} \frac{z - 1}{p^q}\right) = up^r.$$
Let
\[ y = \frac{1}{p^{r-1}} \left( \prod_{\xi \neq 1} \xi^z - 1 \right) p^q = \frac{1}{p^{r-1}} \left( \prod_{i=1}^{l-1} \sigma^i(x) \right). \]

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

However,
\[ p^{r-1} y = \frac{z^l - 1}{p^q} \left/ \frac{z - 1}{p^q} \right. = \frac{1}{p^q(l-1)} \sum_{k=0}^{l-1} \left( 1 + p^q x \right)^k = \frac{1}{p^q(l-1)} \sum_{k=m=0}^{l-1} \sum_{m=0}^{k} \left( \begin{array}{c} k \\ m \end{array} \right) p^{mq} x^m \]
\[ = \frac{1}{p^q(l-1)} \sum_{m=0}^{l-1} \left( \frac{l-1}{m+1} \right) p^{mq} x^m. \]

So
\[ y = \frac{1}{p^q(l-1)+(r-1)} \sum_{m=0}^{l-1} \left( \frac{l}{m+1} \right) p^{mq} x^m. \]

Let \( c_m \) be the coefficient of \( x^m \), \( m = 0, \ldots, l - 1 \). Since \( q(l-1) + r - 1 < e(l-1) = v_K(l) \), \( c_m \) is in \( R \) for all \( m = 0, 1, 2, \ldots, l - 2 \). 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 \( IR = p^{v(e(l-1))} \).

**Proposition 13.4.** Let \( L \supseteq K \) 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 \( \wp \), or
(ii) \( w = 1 + up^k \), \( u \) a unit of \( R \), \( k = lq + r \geq 1, 0 \leq r < l, \) and
   (a) \( r \neq 0 \) or
   (b) \( q \geq e. \)

If \( w = 1 + up^k \) with \( k = lq + r \geq 1, k < le \) 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 \( vR = \wp^t \) and \( l + t \), find \( s, m \) with \( ts = 1 + lm \), then \((yp^{-m})^s = z\) satisfies
\[ z^l = w = (yp^{-m})^s = v^s p^{1-ts} = (p'u')^s p^{1-ts} = up \] for some
\[ \text{units} \ u, u' \text{ of } R. \]
If \( l \mid t, t = lq \), then \((y/p^q)^t\) is a unit of \( R \), so we can assume \( y^t = v \not\equiv v \). Suppose \( v = 1 + up^k \), \( u \) a unit of \( R \), for some \( k > 0 \). If \( l \mid k, k = lq \), let \( -u \equiv v^t \) (mod \( v \)) (possible since \( R/v \) is a finite field of characteristic \( l \)) and set \( c = 1 + v_1p^q \), and \( z = cy \), then

\[
\begin{align*}
z^t &= (yc)^t = (1 + up^k)(1 + v_1p^q)^t, \\
&= 1 + up^k + v_1^tp^{ql} + v_1p^{k+ql} + lv_2,
\end{align*}
\]

some \( v_2 \in v^q \).

\[
\equiv \begin{cases} 1 \pmod{v^{k+1}} & \text{if } k < le, \\ 1 \pmod{v^{e}} & \text{if } k \geq le. \end{cases}
\]

Repeating this construction as needed, we may eventually find \( z \) with \( z^t = w = 1 + up^k \) with \( l \mid k \) or \( k \geq le \). If \( k = 0 \) the argument is similar.

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

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

\[
(cz^s)^t = (1 + vp^d)^t(1 + up^k)^t, \\
= (1 + v^1p^{dl} + vp^d)(1 + u_1p^k), \quad u_0, u_1 \text{ units}.
\]

If \( k < le \) then

\[
(cz^s)^t = 1 + u_2p^n, \quad u_2 \text{ a unit},
\]

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 \( L = K[z], \ z^t = w \in R, \) be a Kummer extension of local fields, with \( l = p = pR \), 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 \( l \mid r_n(w) \) 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 \( w = 1 + p^ku, u \) a unit of \( R \), where \( k = ql + r, \) and \( 1 \leq r \leq l \) or \( q \geq e \).

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 \( m \leq h \).

**Proof.** The results of §7 imply that if \( S \) is a Galois extension of \( R \) such that \( SK = L \), then \( S \) is a Galois \( H_p\) extension for some \( m, 0 \leq m \leq e \), with induced action from that of \( KG \) on \( L \). By the results of [14], \( S = R[t] \) with \( 1 + p^mt = y \) satisfying \( y^t = v \) in \( R, \ v \equiv 1 \pmod{p^m} \) a unit of \( R \). Now \( S_m = R[x] \) where \( 1 + p^nx = z, \ z^t = w \in R \). Since \( K[y] = K[z], \ z = cy^t \) 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

\[
(14.2) \quad 1 + p^nx = c(1 + p^n)^s \quad \text{and} \quad 1 + p^nt = d(1 + p^m)^t,
\]
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 \( S \subsetneq S_m \).

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

**Theorem 14.3.** Let \( L = K[z], z^l = w = 1 + p^k u, k = ql + r, l \). Let \( S \) be the integral closure of \( R \) in \( L \). If \( q \geq e \) 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 \( H^{p^{e+1}} \)-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 \( v_i(x) = r \) 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

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

which is in \( R[X] \) since \( lR = p^{e(l-1)} \) and \( q \leq e \). 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 \( H^h \)-extension of \( R \), where \( b, \) an \((l - 1)\)th root of \( b, \) is in \( R \). Then the description of Galois \( H_h \)-extensions of \( R \) with normal basis given by Hurley [14] applies. Namely, let \( H_h = R[\xi], \xi^l = b \xi, \) then \( T = R[y] \) with \( \xi y = 1 + \bar{b} y = z, \xi z = b z, z^l = w \) is a unit of \( R \) congruent to 1 modulo \( b^l \), 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 \( x^2 + (2/b) x = 2 u, u \) 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 \( \wp \), the maximal ideal of \( R \), and \( S \) is the integral closure of \( R \) in \( L \). Suppose \( T \) is a tame \( H^h \)-extension contained in \( S \). If \( \mathscr{A} = \{ \alpha \in KG | \alpha T \subset T \} \), the order of \( T \) in \( KG \), then \( H_b = \mathscr{A} \).

**Proof.** Since \( H_b \subset KG, H_b \subset \mathscr{A} \).

First assume \( b \) is in \( \wp, \) the maximal ideal of \( R \). Suppose \( \alpha \) is in \( \mathscr{A}, \alpha T \subset T \). Since \( T \) is a tame \( H \)-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 $\alpha = \sum_{i=0}^{l-1} d_i \xi^i$ 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, $\mathcal{A} = H_b$.

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

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 $L = K[z]$, $z^l = w = 1 + p^k u$, $k \geq 1$ maximal, $k = q l + r$, $u$ a unit of $R$. If $r = 1$ or $q \geq e$ then the order $\mathcal{A}$ of $S$ is a Hopf algebra.

16. **The local case. V: Trace, ramification number.** Again assume $L \supseteq K$ is a Kummer extension of local fields of prime order $l$, let $R$ be the valuation ring of $K$ with maximal ideal $p = p R$, $S$ 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 $R$, $q \geq e$ or $1 \leq r < l$. If $q \geq e$ then $S$ is a Galois extension of $R$ with group $G$, $\text{tr}(S) = R$ and $p$ is unramified in $S$.

Suppose $q < e$, then $p$ is totally ramified in $S$. Let $\mathfrak{p}$ be the maximal ideal of $S$.

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 $H_{p^{(e-1)}}$-extension,

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

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

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

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

$$\nu_p(\text{tr}(S)) = \left[ (t + 1)(l - 1) / l \right]$$

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

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

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

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

We have

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

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

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
(iv) $\Rightarrow$ (i). Suppose $v_k(\text{tr}(S)) = q(l - 1)$, some $q$. Let $t$ be the ramification number, $h = t + 1$. Then $q(l - 1) = [h(l - 1)/l]$. Write $h = cl + r$, $0 \leq r < l$. Then

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

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

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

**Proof of Claim.** Let $\pi$ be a uniformizing parameter for $\mathcal{O}$, 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 $i$,

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

Recall that $RG = R[\theta]$, $\theta^i = \omega_i\theta$ where

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

Thus

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

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

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

For any $x$ in $S$,

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

and $\pi^h/p^q = u_1\pi'$, 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 $H_{p^{q(l-1)-1}}$ is generated by

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

So $IS = \phi S = \text{tr}(S)/p^{q(l-1)} = R$. It follows that $S$ is a tame, hence Galois $H_{p^{q(l-1)-1}}$-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 $H_k$-extension for some $H_k$, by Theorem 16.1. So assume $S$ is not Galois. In that case, $v_k(\text{tr}(S))$ is not a multiple of $l - 1$. So if $h = t + 1 = cl + r$, $0 \leq r < l$, again by [22, p. 91],

$$v_k(\text{tr}(S)) = [(cl + r)(l - 1)/l] = c(l - 1) + [r(l - 1)/l]$$
is not a multiple of \(l - 1\). So \(r \geq 2\), and \(t \neq -1\) 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 \(v\) of \(K\), let \(\hat{R}_v\), \(\hat{K}_v\) be the completions at \(v\), and let \(\hat{S}_v = S \otimes_K \hat{R}_v\), \(\hat{L}_v = L \otimes_K \hat{K}_v\). Then \(\hat{L}_v \supset \hat{K}_v\) is a Kummer extension. \(\hat{L}_v = \hat{K}_v[z], \; z^l \in \hat{K}_v\) (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 \(v\) of \(R\), we are given a Tate-Oort Hopf algebra \(\hat{H}_v \subseteq \hat{K}_v G\) and a tame \(\hat{H}_v\)-extension \(\hat{T}_v\) of \(\hat{K}_v\) contained in \(\hat{S}_v\) such that at all but a finite number of primes \(v\), \(\hat{T}_v = \hat{S}_v\). Then there exists a unique Hopf algebra \(H\) contained in \(KG\) and a tame \(H\)-extension \(T\) of \(R\) contained in \(S\) such that \(T \otimes_R \hat{R}_v = \hat{T}_v\) and \(H \otimes_R \hat{R}_v = \hat{H}_v\).

If we can find unique \(H_v\) and \(T_v\) over \(R_v\), the localization of \(R\) at \(v\), so that \(T_v \otimes_{R_v} \hat{R}_v = \hat{T}_v\), \(H_v \otimes_{R_v} \hat{R}_v = \hat{H}_v\), such that \(T_v = S_v\) for all but a finite number of primes, then, since \(H_v = R_v G\) for all \(v \neq l\), \(H = \bigcap H_v\), and \(T = \bigcap T_v\) 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 \(\hat{R}\) be the completion of \(K\) with respect to the valuation on \(R\), \(\hat{R} = \text{valuation ring, } \hat{L} = L \otimes_K \hat{K}\), \(\hat{S} = S \otimes_R \hat{R}\). Let \(T_1\) be an order over \(\hat{R}\) in \(\hat{L}\). Then there exists a unique order \(T\) over \(R\) in \(L\) with \(T = T \otimes_R \hat{R} = T_1\).

**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 \(T = \{x \in S | i(s) \in T_1\}\). Then \(p^m S \subseteq T\). We claim \(T_1 = \hat{T}\). We have the following diagram with exact rows:

\[
\begin{array}{ccc}
0 & \rightarrow & T & \rightarrow & S & \rightarrow & S/T \\
\downarrow i & & \downarrow i & & \downarrow & & \\
0 & \rightarrow & T_1 & \rightarrow & \hat{S} & \rightarrow & \hat{S}/T_1 & \rightarrow & 0
\end{array}
\]

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

\[
\hat{S}/\hat{T} = \hat{R} \otimes_R (S/T) = (\hat{R}/p^m \hat{R}) \otimes_R (S/T) = (R/p^m R) \otimes_R (S/T)
\]

\[
= R \otimes_R (S/T) = S/T.
\]

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 \(S/T \cong \hat{S}/\hat{T}\), 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 \(G\) is the converse of Theorem 6.1.
Theorem 17.3. Let $L \supseteq K$ be a Kummer extension of prime order $l$ of number fields. Let $\mathcal{W} = \text{Tr}(O_L)$. Then the order $\mathcal{A}$ of $O_L$ is a Hopf algebra and $O_L$ is a tame $\mathcal{A}$-extension if and only if $\mathcal{W}$ is the $(l - 1)$th power of an ideal of $O_K$. If so, $\mathcal{A} = H_{\mathcal{B}}$ where $\mathcal{B}^\mathcal{W} = lO_K$.

Here is the global version of the congruence criterion 14.2:

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

(a) $l$ does not divide $v_p(w)$, or

(b) $l$ divides $v_p(w)$ and there is some $c$ in $K$ so that $v_p(c^lw - 1) \geq \nu_p(l)$ or $v_p(c^lw - 1) \equiv 1 \pmod{l}$.

If (a) holds for all primes $p$ of $O_K$ dividing $lO_K$, then $\mathcal{A} = (O_KG)^*$. If (b) holds for some $p$ dividing $lO_K$, then $\mathcal{A} = H_{\mathcal{B}}$ where for each prime $p$ of $O_K$ dividing $lO_K$, choosing $c \in K$ so that $v_p(c^lw - 1) \geq \nu_p(l)$ or $\equiv 1 \pmod{l}$, we have

If $v_p(c^lw - 1) \geq \nu_p(l)$, then $v_p(\mathcal{B}) = 0$.

If $v_p(c^lw - 1) = k, 0 < k < \nu_p(l)$, then $v_p(\mathcal{B}) = (k - 1)(l - 1)/l$.

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

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

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

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

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

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

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

$$\text{tr}(S_p) = p^{(e-h)(l-1)}\phi(S_h) \subseteq \text{tr}(O_{L,v})$$
and so
\[(lO_K)(\text{tr}(O_{L,v}))^{-1} \subseteq v^{h(l-1)} \subseteq v^{k(l-1)}\]
for all \(k, 0 \leq k \leq h\). 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 \(lO_K = (v_1^{p_1} \cdots v_g^{p_g})^{l-1}\) 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
\[\prod_{i=1}^{g} (e_i + 1).\]

**Proof.** The first two factors represent the number of Galois \(H_1\)-extensions of \(O_K\). This follows from the exact sequence
\[1 \to \text{NB}(O_K, H_1) \to \text{Gal}(O_K, H_1) \to \text{Prim Pic}(H_1) \to 1\]
given by the Picard invariant map [26], where \(\text{Gal}(O_K, H_1)\) is the group of Galois \(H_1\)-extensions, \(\text{NB}(O_K, H_1)\) is the subgroup of Galois \(H_1\)-extensions with normal basis, and \(\text{Prim Pic}(H_1)\) is the subgroup of primitive elements of \(\text{Pic}(H_1)\), the group of rank one projective \(H_1\)-modules. Now \(\text{NB}(O_K, H_1) \cong U(O_K)/U(O_K)^l\) by [14], and \(\text{Prim Pic}(H_1) \cong \text{Cl}_l(O_K)\) 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 \(U(O_K)/U(O_K)^2\) has order 4, \(\text{Pic}(O_K)\) 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, \(\text{Gal}(O_K, H_2) = \text{Gal}(O_K, O_K G)\) 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 \( O_L \):
\[
\mathcal{T}(O_L/O_K) = \prod' \mathcal{T}(O_{L,p}/O_{K,p})
\]
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 \( \mathcal{T}(O_{L,p}/O_{K,p}) \) 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 \( K = \mathbb{Q}(\zeta), \zeta = (-1 + \sqrt{-3})/2 \), 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 \( \text{tr}(O_L) = 3O_K \), since the only prime ideal \( \mathfrak{p} \) of \( O_K \) containing \( l = 3 \) is \( \mathfrak{p} = \sqrt{-3} O_K, v_0(\text{tr}(O_L)) = 2 \). So \( O_L \) is a tame \( (O_KG)^* \)-extension of \( O_K \).

(ii) If \( s \equiv t \pmod{3} \), then \( s, t \) 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 \( ((s + z + z^2)/t)/\sqrt{-3} \). Then \( \text{tr}(O_L) \) is generated by \( 3, -3/\sqrt{-3} = \sqrt{-3} \) and \( s \), so \( \text{tr}(O_L) = O_K \). 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 \( \text{tr}(O_L) = -3/\sqrt{-3} = \sqrt{-3} \) and \( s \), so \( \text{tr}(O_L) = O_K \). Thus \( O_L \) is a tame \( O_KG \)-extension of \( O_K \) (that is, tame in the classical sense [11]).

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
\[
\alpha = \frac{1}{\sqrt{-3}} \text{tr} = \frac{1}{\sqrt{-3}} (1 + \sigma + \sigma^2)
\]
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


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