CHAPTER 1

Introduction: What is this book about?

1.1. Background: Hopf-Galois theory and Galois module theory

Hopf-Galois theory was first described by Chase and Sweedler in [**CS69**] a half-century ago. To motivate the definition, we begin by recalling classical Galois theory.

Galois theory. Let K be a field, L be a field containing K and having dimension n as a K-vector space: $[L : K] = n$, and suppose L is normal and separable over K: that means, L is the splitting field of some polynomial in $K[x]$ with no repeated roots in an algebraic closure of K. Then the group G of K-algebra automorphisms of L, called the Galois group of L/K, has order n, and the fixed field of L under the action of G,

$$L^G = \{x \in L \mid g(x) = x \text{ for all } g \in G\},$$

is equal to K.

The Fundamental Theorem of Galois Theory states that the function from the set of subgroups G' of G to the set of fields E with $K \subseteq E \subseteq L$, given by $G' \mapsto L^{G'}$, is one-to-one and onto.

Galois theory dates from the 1830s, but it took over a century before E. Artin [**Art42**] described the theory in module-theoretic terms. The idea is that if L/K is a Galois extension with Galois group G, then L becomes a module over the group algebra $K[G]$ where G acts as K-algebra automorphisms of L. Then L/K is a Galois extension if and only if the map $j : L[G] \to \mathrm{End}_K(L)$ given by $j(sg)(x) = sg(x)$ for s, x in L, g in G, is an isomorphism of K-vector spaces. In other words, the elements of G can be viewed as linear transformations on L, and every K-linear transformation of L can be written as an L-linear combination of elements of G.

One example of a purely module-theoretic result in Galois theory is the Normal Basis Theorem, which goes back at least to Hilbert (1897): Let L/K be a Galois extension of fields with Galois group G. Then there is an element s in L so that as a K-vector space, $\{g(s) \mid g \in G\}$ is a K-basis of L. This translates to: L is a free $K[G]$-module of rank one.

Hopf algebras. Hopf algebras arose in topology around 1941 in work of Heinz Hopf, and began to be studied in algebra in the 1960's. To define a Hopf algebra, it is convenient to first recall the linear dual of a module.

Let R be a commutative ring, M, N projective R-modules of finite rank, and let $M^* = \mathrm{Hom}_R(M, R)$, the linear dual of M. If $f : M \to N$ is an R-module homomorphism, then f induces $f^* : N^* \to M^*$ by

$$f^*(\varphi) : M \to R \text{ is } \varphi \circ f : M \to N \to R$$

for φ in N^*.

For a commutative ring R, define an R-bialgebra H to be an R-algebra, finitely generated and projective as an R-module (hence has a multiplication $m : H \otimes_R H \to H$ and a unit map $i : R \to H$ mapping 1_R to 1_H) that is also equipped with a comultiplication $\Delta : H \to H \otimes_R H$ and a counit map $\varepsilon : H \to R$ so that the dual $\varepsilon^* : R \to H^*$ of the counit map ϵ, and the multiplication map $H^* \otimes_R H^* \to H^*$, defined as the composition of the monomorphism from $H^* \otimes_R H^*$ to $(H \otimes_R H)^*$ with the dual map Δ^*, make H^* into an R-algebra. In particular, Δ^* is associative, so

$$(\Delta \otimes 1)\Delta = (1 \otimes \Delta)\Delta : H \to H \otimes_R H \otimes_R H,$$

meaning that $\Delta : H \to H \otimes H$ is coassociative.

An example is a group ring $R[G]$ for G a finite group. The counit is defined by $\varepsilon(g) = 1$ for all g in G, and the comultiplication map Δ is defined by $\Delta(g) = g \otimes g$.

A group ring $R[G]$ also has a "coinverse" map, or "antipode" $S : R[G] \to R[G]$ by $S(g) = g^{-1}$. Recalling that $\Delta(g) = g \otimes g$ for g in G, then $gg^{-1} = 1$ for g in G is the relation: $m(1 \otimes S)\Delta(g) = 1 = i\varepsilon(g)$. Generalizing, an R-Hopf algebra H is an R-bialgebra with an antipode map S, that is, an antihomomorphism: $S : H \to H$ satisfying $m(1 \otimes S)\Delta(h) = 1 = i\varepsilon(h)$ for all h in H.

Hopf-Galois extensions. Back to L/K a Galois extension of fields. If G is the Galois group of L/K, then because G acts as automorphisms of L, $g(st) = g(s)g(t)$ and $g(1) = 1$ for g in G, s, t in L. This idea generalizes to actions by a Hopf algebra: if L is an H-module, then L is an H-module algebra if

$$h(st) = m(\Delta(h)(s \otimes t)), \quad h(1) = \varepsilon(h) \cdot 1.$$

Then L/K is an H-Hopf-Galois extension if L is an H-module algebra and the map

$$j : L \otimes H \to \mathrm{End}_K(L)$$

given by $j(s \otimes h)(x) = sh(x)$ for s, x in L, h in H, is an isomorphism of K-vector spaces.

The H-Hopf Galois extension where $H = K[G]$ will be called the classical Hopf-Galois extension; all others are non-classical.

The Galois correspondence. For L/K Hopf-Galois with Hopf algebra H, Chase and Sweedler obtained a Galois correspondence from K-sub-Hopf algebras J of H to intermediate fields by: J maps to the "fixed field"

$$L^J = \{s \in L \mid h(s) = \varepsilon(h)(s) \text{ for all } h \text{ in } J\}.$$

Then $\dim_K J = \dim_{(L^J)} L$.

The Galois correspondence is one-to one, but in contrast to classical Galois theory, for many non-classical Hopf-Galois structures the Galois correspondence is not onto. See Chapter 7.

Motivation. Chase and Sweedler's motivation for [**CS69**] was "a hope that results of this type should shed some light on inseparable extensions of fields and ramified extensions of rings". The theory does apply to purely inseparable extensions, but Chase, Shatz and others soon realized that a K-algebra of the same K-dimension as L was too small to yield good information about a purely inseparable extension L/K, and went on to study more general automorphism schemes. But Hopf-Galois theory does have interesting potential to study ramified extensions of local fields, as Byott first showed in examples in 1997-2002.

Ramification. Here we give a brief introduction to ramification and Galois module theory. The subject will be studied in much greater depth in later chapters.

A global field of characteristic zero is a finite extension K of the rational numbers $\mathbb{Q}$. The ring of integers $\mathfrak{O}_K$ of K is the set of all elements a of K that are roots of monic polynomials with coefficients in $\mathbb{Z}$. $\mathfrak{O}_K$ is a Dedekind domain: every ideal of $\mathfrak{O}_K$ factors uniquely into a product of prime ideals of $\mathfrak{O}_K$.

Let L be a finite extension of K. If $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}_K$, then the ideal $\mathfrak{p}\mathfrak{O}_L$ factors uniquely into a product of prime ideals of $\mathfrak{O}_L$:

$$\mathfrak{p}\mathfrak{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

The prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ ramifies in L if some $e_i > 1$. Each prime ideal $\mathfrak{p}$ of K contains a unique rational prime p. Then $\mathfrak{p}$ ramifies tamely if all of the exponents e_i are coprime to p, while if p divides some e_i, then $\mathfrak{p}$ ramifies wildly. Thus an extension L/K of global fields is unramified if no prime of $\mathfrak{O}_K$ ramifies in $\mathfrak{O}_L$ (that is, all $e_i = 1$), tamely ramified if no prime of $\mathfrak{O}_K$ ramifies wildly in $\mathfrak{O}_L$, and wildly ramified otherwise.

For each prime number p, one can construct the p-adic integers $\mathbb{Z}_p$ and the p-adic rational numbers $\mathbb{Q}_p$. The ring $\mathbb{Z}_p$ has a unique prime ideal (p), and there is a p-adic valuation on elements of $\mathbb{Z}_p$: $v_p(a)$ is the smallest power of the ideal (p) that contains a.

A finite extension K of $\mathbb{Q}_p$ is a local field, and the p-adic valuation extends to K, so that $\mathfrak{O}_K$ also has a unique prime ideal $\mathfrak{p}_K$.

If L/K is a finite extension of local fields, then $\mathfrak{p}_K\mathfrak{O}_L = \mathfrak{p}_L^{e_p}$ for some exponent e_p. Then L/K is unramified if $e_p = 1$, tamely ramified if e_p and p are coprime, and wildly ramified if p divides e_p. So ideal theory for extensions of local fields is quite a bit less cluttered than for extensions of global fields.

Galois module theory. The paradigm for Galois module theory is the Normal Basis Theorem: If L/K is a Galois extension of fields with Galois group G, then L is a free $K[G]$-module of rank 1.

The first important result in local Galois module theory was by Noether [**Noe32**]: let L/K be a Galois extension of local fields with Galois group G. Then $\mathfrak{O}_L$ is a free rank one $\mathfrak{O}_K[G]$-module if and only if L/K is tamely ramified. If L/K is wildly ramified, one can still try to understand $\mathfrak{O}_L$ as an $\mathfrak{O}_K[G]$-module, but it seems unnatural, because $\mathfrak{O}_K[G]$ is too small.

Instead, define the associated order $\mathfrak{A} = \mathfrak{A}_G$ of $\mathfrak{O}_L$ in $K[G]$:

$$\mathfrak{A}_G = \{a \in K[G] \mid a\mathfrak{O}_L \subseteq \mathfrak{O}_L\},$$

then $\mathfrak{A}_G$ contains $\mathfrak{O}_K[G]$ and $\mathfrak{A}_G = \mathfrak{O}_K[G]$ if and only L/K is tamely ramified.

So for wildly ramified extensions, the idea is to try to understand $\mathfrak{O}_L$ as an $\mathfrak{A}_G$-module. More generally, given an ideal $\mathfrak{J}$ of $\mathfrak{O}_L$, we can define its associated order $\mathfrak{A}_\mathfrak{J}$ and ask if $\mathfrak{J}$ is free as an $\mathfrak{A}_\mathfrak{J}$ -module.

Some old results. The earliest result was a global result by Leopoldt [**Leo59**]: if L is an abelian Galois extension of $K = \mathbb{Q}$, then $\mathfrak{O}_L$ is a free $\mathfrak{A}_G$-module of rank 1. But that result is not valid if one omits "abelian" or "$K = \mathbb{Q}$". [**CH86**] obtained a local result: if L is a Galois extension of the local field K and the associated order $\mathfrak{A}_G$ is a Hopf order in $K[G]$, then $\mathfrak{O}_L$ is a free $\mathfrak{A}_G$-module of rank one. In [**CM94**] this was extended to L/K an H-Hopf-Galois extension of local fields, where $\mathfrak{A}_G$ is replaced by the associated order $\mathfrak{A}_H$ in H.

Byott obtained some highly interesting results that help justify the study of Hopf-Galois structures in local Galois module theory. Suppose L/K is a wildly ramified Galois extension of local fields with Galois group G, and L/K is also a Hopf-Galois extension with K-Hopf algebra H. Byott [**Byo00**], [**Byo02**], obtained examples where the associated order $\mathfrak{A}_H$ is an $\mathfrak{O}_K$-Hopf order, hence $\mathfrak{O}_L$ is $\mathfrak{A}_H$-free of rank one, but the associated order $\mathfrak{A}_G$ is not a Hopf order and $\mathfrak{O}_L$ is not $\mathfrak{A}_G$-free. His examples in [**Byo00**] are described in [**Chi00**] (and were a major inspiration for writing [**Chi00**].)

Byott's examples have motivated research in several directions in local Galois module theory. This book will describe much of this research in the 20 years since the appearance of [**Chi00**].

1.2. Hopf-Galois structures since 2000

Chapters 2-6 are devoted to the study of Hopf-Galois structures on Galois extensions of fields. Prior to [**GP87**], interest in the subject was limited, because Galois extensions of fields have, à priori, a very nice Galois theory. But [**GP87**] and then [**Byo96**] gave group-theoretic methods for studying Hopf-Galois extensions, and then came Byott's examples [**Byo00**]. So there has been a steady stream of research on the question, given a G-Galois extension L/K, what are the possible types of Hopf-Galois structures on L/K, and how many are there of each type?

Greither and Pareigis [**GP87**] showed that Hopf-Galois structures on a G-Galois extension correspond to regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$, the image of G under the left regular representation. If N is such a subgroup then we refer to the isomorphism class of N as the type of the corresponding Hopf-Galois structure But $\mathrm{Perm}(G)$ is a large group with many subgroups, and is difficult to work in. So most of the research on finding Hopf-Galois structures has involved "Byott's translation", namely, the strategy, presented in [**Byo96**], of looking for Hopf-Galois structures of type N on a G-Galois extension by looking for regular subgroups isomorphic to G in $\mathrm{Hol}(N)$, the normalizer of the image $\lambda(N)$ of the left regular representation of N in $\mathrm{Perm}(N)$.

But then something completely unexpected happened.

In 2006, Caranti, Dalla Volta and Sala [**CDVS06**] showed that for N an elementary abelian p-group, hence isomorphic to a finite dimensional vector space over $\mathbb{F}_p$, regular subgroups of the affine group $\mathrm{Aff}_n(\mathbb{F}_p) \cong \mathrm{Hol}(N)$ correspond to radical algebra structures on the additive group $\mathbb{F}_p^n$. An $\mathbb{F}_p$-algebra A with multiplication $\cdot$ is a radical algebra if given the operation $\circ$ defined by $a \circ b = a + b + a \cdot b$, then $(A, \circ)$ is a group, called the circle group of A. The correspondence between regular subgroups of $\mathrm{Hol}(N)$ and circle groups of radical algebras with additive group N was generalized in [**FCC12**] to N an arbitrary finite additive abelian p-group, and was applied to yield a nice result on the existence of Hopf-Galois structures on G-Galois extensions of fields where G is a finite abelian p-group.

In 2007, Rump [**Rum07a**] defined the concept of left brace as a generalization of a radical algebra, and used it to characterize certain set-theoretic solutions of the Yang-Baxter equation in mathematical physics. By 2016 Bachiller recognized that the main result of [**FCC12**] could be generalized from radical algebras to left braces. In 2017 the notion of left brace was generalized to that of a skew left brace, a brace without the requirement that the "additive group" be abelian, and papers of Guarneri and Vendramin[**GV17**] and Smoktunowitz, Vendramin and Byott [**SV18**]

appeared on Arxiv.math giving a precise connection between Hopf-Galois structures and skew braces: every G-Galois extension of fields with a Hopf-Galois structures of type N yields a skew left brace with additive group N and circle group G, and every skew brace with additive group N and circle group G defines Hopf-Galois structures of type N on a G-Galois extension of fields.

Thus questions about Hopf-Galois structures of type N on G-Galois extensions, and techniques used to find them, translate into questions about the existence and number of skew braces with given additive and circle groups, and vice versa.

Chapter 2 of this book describes the connection between the two theories.

Chapter 3 describes a variety of results on the existence of pairs (G, N) for which a G-Galois extension of fields has a Hopf-Galois structure of type N, equivalently, on the existence of skew braces $(B, \circ, \star)$ with additive group $B^\star = (B, \star) \cong N$ and circle, or adjoint group $B^\circ = (B, \circ) \cong G$.

Chapter 4 describes results obtained from assuming that $\lambda(G)$ is contained in the subgroup $\mathrm{InHol}(N) = \lambda(N) \cdot \mathrm{Inn}(N)$ where $\mathrm{Inn}(N)$ is the group of inner automorphisms of N, and discusses bi-skew braces, which are skew braces with either group playing the role of the additive group.

Chapter 5 is concerned with the question of how many Hopf-Galois structures are there of a given type on a G-Galois extension.

Chapter 6 reviews results of Kohl determining the number of Hopf-Galois structures on a G-Galois extension where G and N are groups of order mp where p is a prime, and m satisfies $\gcd(m, p) = 1$ and two other conditions that are always true if $p > m$. Under those conditions, one can avoid Byott's translation, by finding that if $G = \mathcal{P}\mathcal{Q}$ with $\mathcal{P}$ the p-Sylow subgroup of G, then any regular subgroup N of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$ is contained in the normalizer in $\mathrm{Perm}(G)$ of $\mathcal{P}$. Thus the search for regular subgroups of $\mathrm{Perm}(G)$ yielding Hopf-Galois structures can be carried out in a small subgroup $\mathrm{Norm}_{\mathrm{Perm}(G)}(\mathcal{P})$ of $\mathrm{Perm}(G)$.

In contrast to the classical Fundamental Theorem of Galois Theory, for most Hopf-Galois structures on Galois extensions of fields, the Galois correspondence does not map onto all intermediate fields. Chapter 7 provides a proof of a special case of the Galois correspondence theorem of Chase and Sweedler [**CS69**] for Hopf-Galois structures on separable extensions of fields. Then, using skew brace ideas, a variety of results is presented that yield estimates or exact counts of the proportion of intermediate fields that are in the image of the Galois correspondence for a Hopf-Galois structure on a Galois extension of fields. This chapter closes with a brief survey of results, mostly due to Crespo, Rio and Vela, on Hopf-Galois structures on separable but not necessarily normal extensions of fields.

Chapter 8 introduces the concept of normality for a Hopf-Galois extension and provides a skew brace setting for the general Galois correspondence for a Hopf-Galois structure. This chapter includes the concept of normal Hopf-Galois extension, which until recently had been missing from the Galois correspondence for Hopf-Galois structures.

Chapter 9 is on descent theory. Galois descent is a key to Greither and Pareigis' original study of Hopf-Galois structures on separable field extensions, but it is also of use for understanding the algebra structure of the K-Hopf algebras that appear in that Hopf-Galois theory.

The final chapter in the first part of the book is on Hopf-Galois theory applied to purely inseparable extensions of fields. One of the original motivations for Hopf-Galois theory was to generalize Jacobson's Galois theory for purely inseparable extensions of fields. Chapter 10 reviews some of the attempts to develop such a theory, and provides evidence to suggest that a Greither-Pareigis approach towards Hopf-Galois extensions would be unlikely to succeed.

1.3. Galois module theory since 2000

One objective of studying Hopf-Galois structures on an extension L/K of local or global fields is to broaden the array of ways that the ring $\mathfrak{O}_L$ and its ideals may be viewed as Galois modules. The second half of this book is devoted to results related to those applications.

Let L/K be an H-Hopf-Galois extension of local or global fields with valuation rings or rings of integers $\mathfrak{O}_L, \mathfrak{O}_K$, resp. The idea of Hopf-Galois module theory is to try to understand the structure of $\mathfrak{O}_L$ (or more generally, of a (fractional) ideal of $\mathfrak{O}_L$) as a module over its associated order in H. If L/K is an extension of p-adic fields, and the associated order $\mathfrak{A}$ of $\mathfrak{O}_L$ in H is a Hopf order, then $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module of rank 1. Presenting ideas around that fact was the main objective of [**Chi00**]. The most interesting cases are totally ramified p-extensions of p-adic fields.

The result in [**CH86**] that if $\mathfrak{A}$ is a Hopf order in $K[G]$, then $\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module, was applied to Kummer extensions L/K of degree p in [**Chi87**], which had the title, "Taming wild extensions with Hopf algebras". Those results were aided by the fact that $\mathfrak{O}_K$-Hopf algebras of degree p had been classified by Tate and Oort [**TO70**].

Extensions of degree p^2 were subsequently handled by Greither [**Gre92**], who classified Hopf orders over $\mathfrak{O}_K \supseteq \mathbb{Q}_p$ in $K[G]$ for $G = C_{p^2}$ where K contains a primitive p-th root of unity. Let e be the absolute ramification index of K, then $e' = e/(p-1)$ is an integer. Greither described the so-called realizable Hopf orders, those $\mathfrak{O}_K$-Hopf algebras A for which there is a G-Galois extension L/K so that $A = \mathfrak{A}$, the associated order of $\mathfrak{O}_L$ in $K[G]$, and also described the valuation ring $\mathfrak{O}_L$ of the corresponding G-Galois extension on which A acts. The Hopf orders found in [**Gre92**] are known as Greither orders. They involved a condition on parameters that was subsequently relaxed in work of Underwood [**Und94**], who constructed dual Greither orders, and then was extended to the case $G = C_p \times C_p$, involving both Greither orders and dual Greither orders, by Byott in [**Byo02**].

One of the main motivations for [**Chi00**] was to lay the groundwork to present some examples of Byott [**Byo99**] that showed that if L/K is a G-Galois extension of local fields, there can exist a H-Hopf algebra structure on L/K for H a non-classical K-Hopf algebra, so that $\mathfrak{O}_L$ is not free over its associated order in $K[G]$, but is free over its associated order in H. So one question became: Are there many examples of this phenomenon?

Extending a partial result in [**Chi96**], Byott, in [**Byo02**], produced a complete analysis for wildly ramified Galois extensions of local fields of degree p^2.

Let L/K be a wildly ramified G-Galois extension of local fields where K is a finite extension of $\mathbb{Q}_p$. Then L/K has (lower) ramification breaks $t_1 = pj - 1, t_2 = p^2 i - 1$ where i and j satisfy $0 \leq i, j \leq e' = e/(p-1)$ where e is the absolute ramification index of p in K. Hence the possible pairs (i, j) lie in an $e' \times e'$ square

in the i, j-plane. Applying Byott's analysis, if $p = 3$ and $e' = 60$ for example, then of the 3600 possible pairs (i, j), there are approximately 180 pairs (i, j) for which the associated order in $K[G]$ is Hopf, and 9 pairs (i, j) where the associated order in $K[G]$ is not Hopf but the associated order in a non-classical Hopf-Galois structure is Hopf. (For more details, see Chapter 11 or [**Byo02**]).

Thus what Byott showed in [**Byo02**] is first, that examples of local fields L/K where the associated order of $\mathfrak{O}_L$ is a Hopf order are relatively rare, and second, that even when the associated order of $\mathfrak{O}_L$ in some H-Hopf-Galois structure on L/K is Hopf, cases where that occurs in a non-classical Hopf-Galois structure and not in the classical structure, as in [**Byo99**], are even more rare. Based on the p^2 case, non-classical Hopf-Galois structures apparently seldom yield better local Galois module results than the classical Hopf-Galois structure does.

Beyond the rarity of examples that motivated the Hopf algebra orientation to local Galois module theory in 2000, there are two other substantial issues.

One was that despite considerable efforts, especially by Underwood and his collaborators, constructing realizable Hopf orders in $K[C_{p^n}]$ for $n > 2$ turned out to be very difficult. A collection of realizable orders in $K[C_{p^3}]$ was found in [**Und08**] but for $n \geq 3$ the description of realizable Hopf orders remains a difficult problem. Chapter 12 describes the present state of the art on constructing Hopf orders of degree p^n, $n > 2$, mostly for K a local field of characteristic zero. Section 12.13 considers the case where K has characteristic p, and even there the algebra structure of the Hopf orders for $n = 3$ is unclear.

Thus even if one knows that $\mathfrak{A}$ is a Hopf order in $K[G]$ so that $\mathfrak{O}_L$ is $\mathfrak{A}$-free, if what $\mathfrak{A}$ looks like as an $\mathfrak{O}_K$-algebra is not understood, then knowing that $\mathfrak{O}_L$ is $\mathfrak{A}$-free is not going to be particularly satisfying.

Scaffold theory may shed some light on this issue. See below.

The other limitation, which is intrinsic, as Byott illustrated in the p^2 case in [**Byo02**] and showed in general in [**Byo97**], is that the fact that the associated order of $\mathfrak{O}_L$ in $K[G]$ is a Hopf order imposes serious constraints on the ramification breaks of L/K. If L/K is a totally ramified Galois extension of local fields of degree p^n, and $\mathfrak{A}$ is a Hopf order in $K[G]$, then the first ramification break b_1 satisfies either $b_1 = -1 + sp^n$ with $1 \leq s \leq e' = e/(p-1)$, or all the ramification breaks b_r satisfy $b_r = p^r e'$. The second case is exceptional and implies that $\mathfrak{A}$ is not a local ring. The first case, which implies that $\mathfrak{O}_L$ is in fact an $\mathfrak{A}$-Hopf-Galois extension of $\mathfrak{O}_K$, also implies that $b_i \equiv -1 \pmod{p^n}$ for all $i = 1, \ldots, n$. Moreover, when $\mathfrak{A}$ is a Hopf order, then the different $\mathfrak{D}_{L/K}$ of $\mathfrak{O}_L/\mathfrak{O}_K$ is the ideal $\mathfrak{D}_{L/K} = \pi_K^c \mathfrak{O}_L$ for some integer c. These results are all in Chapter 8 of [**Chi00**].

In [**Bon00**], Bondarko proved a converse to the first case. Suppose L/K is abelian of degree p^n, totally ramified, the ramification numbers satisfy $b_i \equiv -1 \pmod{p^n}$ and the different $\mathfrak{D}_{L/K} = \pi_K^c \mathfrak{O}_L$ for some integer c. Then $\mathfrak{A}$ is an $\mathfrak{O}_K$-Hopf order in $K[G]$ and $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module of rank 1. The method of proof involves identifying L/K as a Kummer extension for a formal group defined over $\mathfrak{O}_K$.

Finally: for most Galois extensions L/K of local or global fields, the associated order $\mathfrak{A}$ of $\mathfrak{O}_L$ or ideals of L is not Hopf. Chapter 11 also describes some tools for analyzing Hopf-Galois module structure (and making comparisons between different structures) in situations in which the associated order is not necessarily a Hopf order. The chapter includes work on extensions that are tame (in the classical

sense): the evidence to date suggests that for these extensions the ring of integers is (locally) free over its associated order in all of the Hopf-Galois structures admitted by the extension. It also examines some recent work of S. Taylor and Truman on Hopf-Galois module structure of extensions of global fields, including the interesting case where the extension L/K is Hopf-Galois but not normal, hence not classically Galois.

Scaffolds and semi-stable extensions. The ramification restrictions on a Galois extension L/K of p-adic fields with Galois group a finite p-group that would make the associated order $\mathfrak{A}$ of $\mathfrak{O}_L$ a Hopf order make it evident that for most such extensions, the associated order is not Hopf. So other methods have been developed.

One by Bondarko, involves the concept of stable and semi-stable extensions, developed in [**Bon02**] and [**Bon06**]. When L/K is stable, he found necessary and sufficient conditions for any ideal $\mathfrak{P}^h$ of $\mathfrak{O}_L$ to be free over its associated order in $K[G]$. Bondarko's approach is described and generalized in Chapter 14.

The other, first described by Elder and then elaborated in collaboration with Byott, involves the concept of scaffold. For a Galois scaffold, the idea is to take a totally ramified G-Galois extension L/K of p-adic fields of degree p^n, and try to find a K-basis $\{\lambda_t : t \in \mathbb{Z}/p^n\mathbb{Z}\}$, a set $\{\psi_i\}$ of elements of $K[G]$ and a set $b_1, \ldots, b_n$ of shift parameters (which in the Galois case are typically the ramification numbers of L/K) so that

(i) $v_L(\lambda_t) = t$ for all t in $\mathbb{Z}$;

(ii) $\lambda_{t_1}\lambda_{t_2}^{-1}$ is in K whenever $t_1 \equiv t_2 \pmod{p^n}$;

(iii) $\psi_i(1) = 0$ for $1 \leq i \leq n$;

(iv) $\psi_i \cdot \lambda_t = \lambda_{t+p^n b_i}$ or 0 up to a certain level of precision (more precisely, modulo $\lambda_{t+p^n b_i}\mathfrak{c}$ for some fixed ideal $\mathfrak{c}$ which defines the precision). The choice of whether $\psi_i \cdot \lambda_t = \lambda_{t+p^n b_i}$ or 0 depends on the shift parameters b_i.

For details and a slight refinement of the definition, see [**BCE18**, Definition 2.6] or Definition 15.1.

The idea behind this definition is that if one can find p^n elements of $K[G]$ that take on all valuations between 0 and $p^n - 1$, then they will form a basis of $\mathfrak{O}_L$ because L/K is totally ramified. And if the ψ_i all shift the elements λ_t to either zero or K-multiples of other elements in the set $\{\lambda_t\}$, then the elements ψ_i and their powers have a chance of becoming a basis of the associated order $\mathfrak{A}$ of $\mathfrak{O}_L$. When that is the case, then $\mathfrak{O}_L$ will be free over its associated order $\mathfrak{A}$.

The concept of scaffold is studied in more detail in Chapter 15.

Connections with realizable Hopf orders. A striking consequence of scaffold theory has been a potential breakthrough in the problem of describing realizable Hopf orders over $\mathfrak{O}_K$ in $K[G]$ for G a finite abelian p-group.

As noted above, $\mathfrak{O}_K$-Hopf algebras that are realizable, that is, can be the associated orders of valuation rings $\mathfrak{O}_L$ in $K[G]$ for G cyclic of order p^n, are completely understood for $n = 1$ and $n = 2$ but not well-understood for $n \geq 3$.

But scaffold theory as developed in [**BE18**] applies to cyclic p-extensions L/K of p-adic fields under certain conditions on the break numbers b_i.

In case all the $b_i \equiv -1 \pmod{p^n}$ and a certain combinatorial equality holds, then one obtains an explicit basis of the associated order $\mathfrak{A}$, $\mathfrak{O}_L$ is free over $\mathfrak{A}$ and the different is generated by a power of the parameter π of K.

Those are the conditions needed by Bondarko to show that the associated order $\mathfrak{A}$ is obtained from a formal group, hence is a Hopf order, and hence is a realizable Hopf order.

Thus the scaffold theory of [**BE18**] provides a set of generators for realizable Hopf orders for $n \geq 1$, and in particular, for $n \geq 3$.

This connection was used in [**EU17**] to describe realizable Hopf orders in $K[C_{p^3}]$ for K of characteristic p, and shows up in Chapter 15.

Chapters 13-15. Chapters 13-15 are devoted to p-extensions of p-adic fields (local fields) that are semistable, in the sense of Bondarko, or have a Galois scaffold, in the sense of Byott and Elder. A recent paper of Keating [**Kea20**] associates to a semi-stable Galois extension L/K of local fields a certain precision, and shows that if L/K has a scaffold with precision $\mathfrak{c}$, then L/K is semistable with precision $\mathfrak{c}$, while if L/K is semistable, then it has a scaffold of precision 1. Thus scaffold theory applies to Bondarko's semi-stable extensions.

Chapter 13 extends classical ramification theory for Galois extensions of local fields to the case of a separable extension L/K with Galois closure $\widetilde{L}/K$, where L/K is a Hopf-Galois extension.

Chapter 14 describes the concepts of stable and semistable p-extensions of p-adic fields due to Bondarko [**Bon00**], [**Bon02**], [**Bon06**] and extends the theory to the setting of Hopf-Galois extensions.

Chapter 15 introduces the scaffold theory of Elder and Byott ([**BE18**], [**BCE18**]) and, extending [**Kea20**], shows that if a Hopf-Galois extension L/K of local fields has a scaffold of a suitable precision, then it is semistable.

1.4. What's not in this book

There are three areas not well covered in this book. One, global Galois module theory, is discussed only in part of Chapter 11. For the most part, this reflects the (lack of) expertise of the authors. Another, Hopf-Galois structures on non-normal separable extensions, is discussed in the last section of Chapter 7 but, as noted there, does not fit so naturally in the first half of the book because it has not been connected to brace theory. The other is the substantial body of research on braces that has accumulated in the 13 years since [**Rum07a**]. The authors only realized that brace theory might be of interest to Hopf-Galois extensions and Galois module theory with Byott's presentation at the conference "Hopf algebras and Galois module theory" at the University of Nebraska at Omaha in 2017. Several survey papers on braces and skew braces have been written since then, notably [**GV17**], [**Ven19**] and [**SV18**], but there is a large literature on braces that up to this point has not been connected to Hopf-Galois theory.

This book is a snapshot of the state of Hopf-Galois theory and Galois module theory at a particular point in time, namely, the summer of 2020. The idea for this work was to provide a 20 year update of [**Chi00**], and at the same time, present a survey of work in the 50 years since the appearance of the original concept of Hopf-Galois extension in [**CS69**]. While we were writing this, the pace of research in the area has, if anything, accelerated. To authors of recent work that has not been included in this book, we apologize, and hope that your research will become a important part of a 10 year, or 20 year update of this book, one that perhaps you will (co)-author!

Acknowledgments

The authors of this book wish to express their profound gratitude to Griff Elder for his leadership in this area over the past decade, in particular for the organization of a series of week-long conferences/workshops at the University of Nebraska at Omaha in 2012, 2013, 2014, 2016, 2017, 2018 and 2019, and the virtual conference in 2020. The influence of these conferences on this work has been so great that for a long while our working title was "The Omaha Book"! We would like to highlight the extensive influence of Nigel Byott on much of the material presented in this book, and to thank him for organizing the 2015 conference at the University of Exeter. Our thanks also to UNO, the University of Exeter, and the London Mathematical Society for their support of the conferences mentioned above, and to Keele University for hosting the web archive of proceedings of those conferences from 2013 to the present. We are very grateful to Ina Mette of the American Mathematical Society for her patience and support during the development of this project, and we thank the anonymous referees for their insightful comments on the manuscript.

The other authors would like to express here our thanks to Paul Truman for proposing this project at Omaha in 2018 and for taking the lead as corresponding author and as coordinator and chief copy editor for the book.

Part I: Hopf-Galois Extensions

CHAPTER 2

Hopf-Galois structures on Galois extensions of fields, regular subgroups, and skew braces

2.1. Introduction

This chapter describes the connection between Hopf-Galois structures on Galois extensions of fields and skew braces.

We briefly summarize the connection here. The remainder of this chapter will discuss the connection in more detail.

In 1987 the first step was obtained by Greither and Pareigis [**GP87**]. If L/K is a G-Galois extension of fields and is a Hopf-Galois extension by some K-Hopf algebra H, then they showed that $L \otimes_K H = L[N]$ for some regular subgroup N of $\mathrm{Perm}(G)$. That subgroup is normalized by the image $\lambda(G)$ of the left regular representation map $\lambda : G \to \mathrm{Perm}(G)$, so H and its action on L can be recovered by Galois descent. Thus there is a bijection between Hopf-Galois structures on L/K and regular subgroups N of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$. The group N need not be isomorphic to G. By slight abuse of language, if H corresponds to $N \subset \mathrm{Perm}(G)$, we say that the Hopf-Galois structure given by H on L/K has type N (viewed as an abstract group).

In 1996 the next step was obtained by Byott [**Byo96**], building on an observation in [**Chi89**] that if H is a Hopf-Galois structure of type N on a G-Galois extension of fields, then in $\mathrm{Hol}(N)$, the normalizer of $\lambda(N)$ in $\mathrm{Perm}(N)$, there is a subgroup T isomorphic to G that corresponds to H. Byott systematically described the relationship between the set of regular subgroups of $\mathrm{Perm}(G)$ isomorphic to N and normalized by $\lambda(G)$ and the set of regular subgroups of $\mathrm{Hol}(N)$ isomorphic to G. That analysis transformed the problem of finding or counting Hopf-Galois structures on L/K of type N on a G-Galois extension into that of finding or counting regular subgroups isomorphic to G in $\mathrm{Hol}(N)$. This was a highly significant advance, because $\mathrm{Hol}(N) \cong N \rtimes \mathrm{Aut}(N)$ is in general a far smaller and more tractable group than $\mathrm{Perm}(G) \cong \mathrm{Perm}(N)$.

Since 1996 dozens of papers have examined various strategies for constructing or counting or ruling out Hopf-Galois structures of type N on G-Galois extensions of fields. The vast majority of them have worked within the holomorph of N.

In 2006, Caranti, Dalla Volta and Sala [**CDVS06**] observed that regular subgroups of the affine group of an elementary abelian group (identified as $\mathbb{F}_p^n$ for $\mathbb{F}_p$ the field of p elements) give rise to radical algebra structures on the additive group $\mathbb{F}_p^n$. The affine group may be viewed as the holomorph of the elementary abelian group $\mathbb{F}_p^n$. The connection between regular subgroups of a holomorph and radical algebras was generalized in [**FCC12**] to the case where the additive group is any finite abelian p-group N: radical algebra structures on N correspond to regular subgroups of $\mathrm{Hol}(N)$. That paper identified the connection between Hopf-Galois

structures of type N on a G-Galois extension and radical algebras with additive group N and circle (or "adjoint") group G. This connection was further generalized to arbitrary finite abelian groups and commutative radical algebras in Section 5 of [**Byo13**].

Meanwhile, in 2007, Rump [**Rum07a**] introduced the concept of a left brace, generalizing the concept of a radical ring with its adjoint group. His objective was to find solutions of the Yang-Baxter equation arising, e.g. in mathematical physics. Since the appearance of Rump's paper, dozens of papers have studied braces, often from the point of view of ring theory.

In 2016, Bachiller [**Bac16**], extending [**FCC12**], showed that for N any abelian additive group, regular subgroups of $\mathrm{Hol}(N)$ correspond to left brace structures on N, and noted the connection between a left brace $(B, \circ, +)$ and a Hopf-Galois structure of type $(B, +)$ on a Galois extension of fields with Galois group $(B, \circ)$.

In 2017, Guarneri and Vendramin [**GV17**] defined a skew left brace to be a brace with additive group not necessarily abelian and showed that skew braces give solutions to the Yang-Baxter equation.

In 2018, in the appendix to [**SV18**], Byott and Vendramin completed the description of the connection between skew braces and Hopf-Galois structures on Galois extensions of fields. The bottom line is that every Hopf-Galois structure of type N on a G-Galois extension of fields defines a skew brace with additive group isomorphic to N and circle group isomorphic to G, and every skew brace with additive group isomorphic to N and circle group isomorphic to G defines a collection of Hopf-Galois structures of type N on a G-Galois extension of fields.

In the remainder of this chapter we present the details of the connection just described between Hopf-Galois extensions on Galois extensions of fields and skew braces.

2.2. Greither-Pareigis theory

Let L/K be a G-Galois extension of fields. To classify Hopf-Galois structures on L/K, the first step is to associate to a Hopf-Galois structure a regular subgroup of $\mathrm{Perm}(G)$. This was done by Greither and Pareigis [**GP87**], using Galois descent. This is covered fairly thoroughly in [**Chi00**] and is also treated in Chapter 9, so here we will just give a summary of the results.

A subgroup N of $\mathrm{Perm}(G)$ is a regular subgroup if for every g, h in G there is a unique η in N so that $\eta[g] = h$. Thus $|N| = |G|$. To check regularity of N it suffices to check that $|N| = |G|$ and $\{\eta[e] \mid \eta \in N\} = G$ where e is the identity element of G.

Suppose L/K has a Hopf-Galois structure by a K-Hopf algebra H. Then $L \otimes_K H$ is a K-Hopf algebra that acts on $L \otimes_K L$, and since L/K is a Galois extension with Galois group G, $L \otimes_K L \cong \mathrm{Hom}_L(L[G], L)$. (This is an interpretation of the fact that if L/K is a Galois extension with Galois group G, then $L = K[x]/(p(x))$ for some polynomial with distinct roots in any algebraic closure of K, hence $L \otimes_K L = L[x]/(p(x)) \cong L \times L \times \cdots \times L$ as rings.) Then $L \otimes_K L$ is an $L \otimes_K H$-Hopf-Galois extension. But then the L-Hopf algebra $L \otimes_K H$ must be generated by grouplikes (see Section 7.1). So $L \otimes_K H \cong L[N]$, a group algebra, where $N \subset \mathrm{Perm}(G)$ is a regular subgroup: that is, $N[g] = \{\eta[g] \mid \eta \in N\} = G$ for every g in G. And because $L[N] \cong L \otimes_K H$ and N is normalized by the image $\lambda(G)$ of the left regular representation $\lambda : G \to \mathrm{Perm}(G)$ given by $\lambda(g)[x] = gx$, one can recover H

as $L[N]^G$, where G acts on L via action of the Galois group, and acts on N via conjugation by elements of $\lambda(G)$ in $\mathrm{Perm}(G)$.

To summarize:

THEOREM 2.1. *There is a bijection between Hopf-Galois structures on a G-Galois extension L/K of fields and regular subgroups of* $\mathrm{Perm}(G)$ *normalized by $\lambda(G)$, as follows: if $j : H \otimes L \to L$ is an action of a K-Hopf algebra on a G-Galois extension L/K of fields so that L/K is an H-Hopf-Galois extension, then there is a unique subgroup N of* $\mathrm{Perm}(G)$ *so that $L \otimes_K H \cong L[N]$, $1 \otimes j$ is the corresponding action of $L[N]$ on $L \otimes_K L$, and N is normalized by $\lambda(G)$ in* $\mathrm{Perm}(G)$*. Moreover, H and j may be recovered by*

$$H = (L[N])^G = \left\{ \sum s_\eta \eta \;\middle|\; \sum s_\eta \eta = \sum g(s_\eta)\lambda(g)\eta\lambda(g^{-1}) \text{ for all } g \in G, s_\eta \in L, \eta \in N \right\},$$

acting on L/K via the restriction of $1 \otimes j$ on H.

An equivalent description of the action of H on L will be given as Proposition 4.14, based on the Byott translation theory discussed beginning in Section 2.3.

DEFINITION 2.2. If H is a K-Hopf algebra that acts on L and L/K is H-Hopf-Galois, then $L \otimes_K H = L[N]$ and the *type* of H is the isomorphism type of N.

The bijection between Hopf-Galois structures on a G-Galois extension L/K and regular subgroups N of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$ turns the determination of Hopf-Galois structures on L/K into the group-theoretic problem: determine the regular subgroups of $\mathrm{Perm}(G)$ that are normalized by $\lambda(G)$.

In general, this is a hard problem. But it becomes a less hard problem by the following observation, from [**Chi89**].

PROPOSITION 2.3. *If N is a regular subgroup of* $\mathrm{Perm}(G)$ *that is normalized by $\lambda(G)$, then there is a regular subgroup isomorphic to G in* $\mathrm{Perm}(N)$ *that normalizes $\lambda(N)$.*

The normalizer of $\lambda(N)$ in $\mathrm{Perm}(N)$ is the holomorph $\mathrm{Hol}(N) = \lambda(N) \rtimes \mathrm{Aut}(N)$.

This observation, by itself, is useful for restricting the possible types of Hopf-Galois structures on a G-Galois extension L/K. Pick a group N of order n, the order of G. If there is no regular subgroup T isomorphic to G in $\mathrm{Hol}(N)$, then L/K cannot have a Hopf-Galois structure of type N.

Since $\mathrm{Hol}(N)$ is typically a much smaller group than $\mathrm{Perm}(G) \cong \mathrm{Perm}(N)$, the problem of excluding Hopf-Galois structures of type N on a G-Galois extension L/K by working in $\mathrm{Hol}(N)$ becomes feasible in many cases. Here are three notable examples:

• Kohl's result that if G is cyclic of order p^n, p odd, then L/K has no Hopf-Galois structures of non-cyclic type, follows immediately from his proof [**Koh98**, Theorem 4.5], that if N is a non-cyclic group of order p^n, p odd, then $\mathrm{Hol}(N)$ contains no element of order p^n.

• Featherstonhaugh's Theorem ([**Fea03**], [**FCC12**]) partially generalized Kohl's theorem: Let N be an abelian p-group of order p^m where p is sufficiently larger than m. Then every abelian regular subgroup of $\mathrm{Hol}(N)$ is isomorphic to N, so a G-Galois extension has no Hopf-Galois structures of abelian type N for $N \ncong G$.

• Byott's result [**Byo04a**] that if G is a non-abelian simple group, then a G-Galois extension has no Hopf-Galois extensions of type N for $N \ncong G$, was obtained by showing that if N is a group of the same order as G but not isomorphic to G, then there is no regular embedding of G into $\mathrm{Hol}(N)$. The proof depends on consequences of the classification of finite simple groups. (See Section 3.5 for further discussion of this result.)

The observation of Proposition 2.3 concerning regular subgroups of $\mathrm{Hol}(N)$, used to deny the existence of Hopf-Galois structures of given types, has a converse, given in [**Byo96**]:

THEOREM 2.4. *Let G, N be two groups of the same order n. If $\mathrm{Hol}(N)$ has a regular subgroup isomorphic to G, then a G-Galois extension has a Hopf-Galois structure of type N.*

In fact, [**Byo96**] quantified that observation. We'll prove Theorem 2.4 following Theorem 2.8, below.

2.3. Byott translation theory

The next three sections are devoted to a presentation of the connection between Hopf-Galois structures of type N on a G-Galois extension L/K of fields, and regular subgroups of $\mathrm{Hol}(N)$ that are isomorphic to G. The theory, from [**Byo96**] is also described in Section 7 of [**Chi00**]. We present it here because it is essential for understanding the connection between Hopf-Galois structures and skew braces.

Let N, G be two groups of equal order with identities e_G, e_N, respectively. Let

$$\mathcal{E}^G(G,[N]) = \{\text{regular subgroups } M \cong N \text{ of } \mathrm{Perm}(G) \text{ normalized by } \lambda(G)\},$$

and let

$$e(G,[N]) = |\mathcal{E}^G(G,[N])|$$

which

$$= \#\{\text{Hopf-Galois structures of type } N \text{ on a } G\text{-Galois extension}\}$$

by Greither-Pareigis theory. Let

$$\begin{aligned}\mathcal{R}_N(N,[G]) &= \{\text{regular subgroups } T \cong G \text{ of } \mathrm{Hol}(N)\}\\ &= \{\text{regular subgroups } T \cong G \text{ of } \mathrm{Perm}(N) \text{ that normalize } \lambda(N)\ \},\end{aligned}$$

and let $r_N(N,[G]) = |\mathcal{R}_N(N,[G])|$.

To understand the relationship of $e(G,[N])$ and $r_N(N,[G])$, we set

$$\mathrm{Bij}_0(G,N) = \{\text{ bijective maps from } G \text{ to } N \text{ that take } e_G \text{ to } e_N\}.$$

The map $a \mapsto a^{-1}$ gives a bijection between $\mathrm{Bij}_0(G,N)$ and $\mathrm{Bij}_0(N,G)$.

Given a in $\mathrm{Bij}_0(N,G)$, we get a function $\alpha_a : N \to \mathrm{Perm}(G)$ by

$$\alpha_a(m)[g] = a\lambda(m)a^{-1}[g]$$

for g in G, m in N, where $\lambda : N \to \mathrm{Perm}(N)$ is the left regular representation map defined by $\lambda(m)[n] = mn$ for n in N. Then α_a is a homomorphism:

$$\begin{aligned}\alpha_a(mn)[g] &= (a\lambda(mn)a^{-1})[g]\\ &= (a\lambda(m)\lambda(n)a^{-1})[g]\\ &= (a\lambda(m)a^{-1}a\lambda(n)a^{-1})[g]\\ &= \alpha_a(m)\alpha_a(n)[g].\end{aligned}$$

Also, α_a is injective, and regular, because

$$\alpha_a(m)[e_G] = a\lambda(m)a^{-1}[e_G] = a\lambda(m)[e_N] = a(m),$$

and $a : N \to G$ is bijective, so $\{a(m) \mid m \in N\} = G$.

So sending a to α_a gives a map from $\mathrm{Bij}_0(N, G)$ to

$$\mathrm{Reg}(N, \mathrm{Perm}(G)) = \{\alpha : N \to \mathrm{Perm}(G) : \ \alpha \text{ is a regular embedding}\}.$$

The map is 1-1. For if $\alpha_a = \alpha_{a'}$, then $\alpha_a(m)[e_G] = \alpha_{a'}(m)[e_G]$, so $a(m) = a'(m)$ for all m in N, so $a = a'$.

The map from $\mathrm{Bij}_0(N, G)$ to $\mathrm{Reg}(N, \mathrm{Perm}(G))$ is also onto. For we have

PROPOSITION 2.5. *Let $\alpha : N \to \mathrm{Perm}(G)$ be a regular embedding, and let $a : N \to G$ be defined by $a(m) = \alpha(m)[e_G]$. Then a is in $\mathrm{Bij}_0(N, G)$ and $\alpha = \alpha_a$.*

PROOF. To show that $\alpha(m)[g] = a\lambda(m)a^{-1}[g]$ for all g in G, we show that, for m and x in N,

$$a^{-1}\alpha(m)a(x) = \lambda(m)(x),$$

as follows:

$$\begin{aligned} a^{-1}\alpha(m)a(x) &= a^{-1}\alpha(m)\alpha(x)[e_G] \\ &= a^{-1}\alpha(mx)[e_G] \\ &= a^{-1}a(mx) \\ &= mx \\ &= \lambda(m)(x). \end{aligned}$$

□

The bijection between $\mathrm{Bij}_0(N, G)$ and $\mathrm{Bij}_0(G, N)$, defined by mapping $a : N \to G$ to $b = a^{-1} : G \to N$, yields a bijection

$$s : \mathrm{Reg}(N, \mathrm{Perm}(G)) \to \mathrm{Reg}(G, \mathrm{Perm}(N)).$$

If $\alpha : N \to \mathrm{Perm}(G)$ is a regular embedding with induced bijection a, then the corresponding regular embedding $s(\alpha) = \beta : G \to \mathrm{Perm}(N)$ is defined to be the regular embedding induced by the inverse bijection $b = a^{-1}$: if $\alpha(m) = a^{-1}\lambda(m)a$, then $\beta(g) = a\lambda(g)a^{-1} = b^{-1}\lambda(g)b$.

PROPOSITION 2.6. *If $\theta : N' \to N$ is an isomorphism of groups, and α_a is in $\mathrm{Reg}(N, \mathrm{Perm}(G))$, then $\alpha_{a\theta}$ is in $\mathrm{Reg}(N', \mathrm{Perm}(G))$ and $\alpha_{a\theta}(N') = \alpha_a(N)$ in $\mathrm{Perm}(G)$.*

PROOF. Let $\theta : N' \to N$ be an isomorphism and $a : N \to G$ a bijection. Then $a\theta$ is in $\mathrm{Bij}_0(N', G)$. The corresponding map $\alpha_{a\theta} : N' \to \mathrm{Perm}(G)$ is then defined for m' in N', g in G as

$$\begin{aligned} \alpha_{a\theta}(m')(g) &= a\theta\lambda(m')\theta^{-1}a^{-1}(g) \\ &= a\theta(m'(\theta^{-1}a^{-1})(g)) \\ &= a(\theta(m')a^{-1})(g) \\ &= a\lambda(\theta(m'))a^{-1}(g) \\ &= \alpha_a(\theta(m'))(g). \end{aligned}$$

So the image of $\alpha_{a\theta}$ in $\mathrm{Perm}(G)$ is the same as that of α:

$$\alpha_{a\theta}(N') = a\lambda(\theta(N'))a^{-1} = a\lambda(N)a^{-1} = \alpha_a(N).$$

□

As for the map $s(\alpha) = \beta : G \to \mathrm{Perm}(N)$ corresponding to α, we have

PROPOSITION 2.7. *Let $\alpha : N \to \mathrm{Perm}(G)$ be a regular embedding and $\theta : N' \to N$ be an isomorphism. Let $s(\alpha) = \beta : G \to \mathrm{Perm}(N)$. Let α correspond to a in $\mathrm{Bij}(N, G)$, let $b = a^{-1}$ correspond to β in $\mathrm{Bij}(G, N)$, and let*

$$\beta_\theta = s(\alpha_{a\theta}) : G \to \mathrm{Perm}(N').$$

Then in $\mathrm{Perm}(N')$,

$$\beta_\theta(\gamma) = \theta^{-1}\beta(\gamma)\theta.$$

PROOF. The map $\alpha_{a\theta}$ in $\mathrm{Reg}(N', \mathrm{Perm}(G))$ corresponds to $a\theta$ in $\mathrm{Bij}_0(N', G)$, so $s(\alpha_\theta) = \beta_\theta : G \to \mathrm{Perm}(N')$ corresponds to $\theta^{-1}a^{-1} = \theta^{-1}b$. Then for $\beta : G \to \mathrm{Perm}(N)$, defined from $b = a^{-1}$,

$$\beta(g)(m) = b\lambda(g)b^{-1}(m) = a^{-1}\lambda(g)a(m)$$

so in $\mathrm{Perm}(N')$,

$$\begin{aligned}\beta_\theta(g) &= \theta^{-1}b\lambda(g)b^{-1}\theta \\ &= \theta^{-1}\beta(g)\theta.\end{aligned}$$

□

In particular, Propositions 2.6 and 2.7 are valid when $N' = N$ and θ is in $\mathrm{Aut}(N)$.

2.4. Actions by the left regular representations

Given groups G, N of the same order, we will be interested in regular embeddings α in $\mathrm{Reg}(N, \mathrm{Perm}(G))$ whose image is either normalized by $\lambda(G)$ or that normalizes $\lambda(G)$.

Let α correspond to a in $\mathrm{Bij}_0(N, G)$ and β correspond to $b = a^{-1}$ in $\mathrm{Bij}_0(G, N)$. Suppose $\alpha(N) \subset \mathrm{Perm}(G)$ is normalized by $\lambda(G)$: for all m in N, g in G there is some m' in N so that

$$\alpha(m') = \lambda(g)\alpha(m)\lambda(g)^{-1}.$$

Then

$$a\lambda(m')a^{-1} = \lambda(g)a\lambda(m)a^{-1}\lambda(g)^{-1}.$$

So

$$\begin{aligned}\lambda(m') &= a^{-1}\lambda(g)a\lambda(m)a^{-1}\lambda(g)^{-1}a \\ &= b\lambda(g)b^{-1}\lambda(g)b\lambda(m)^{-1}b^{-1} \\ &= \beta(g)\lambda(m)\beta(g)^{-1}.\end{aligned}$$

The argument is reversible. We conclude:

PROPOSITION 2.8. *Let α in $\mathrm{Reg}(N, \mathrm{Perm}(G))$ correspond to β in $\mathrm{Reg}(G, \mathrm{Perm}(N))$. Then $\beta(G)$ normalizes $\lambda(N)$, that is, $\beta(G)$ is in $\mathrm{Hol}(N) \subset \mathrm{Perm}(N)$, if and only if $\alpha(N)$ is normalized by $\lambda(G)$.*

This result implies Theorem 2.4, that if $\mathrm{Hol}(N)$ has a regular subgroup isomorphic to G, then $\mathrm{Perm}(G)$ has a regular subgroup M that is isomorphic to N and normalized by $\lambda(G)$, hence corresponds to a Hopf-Galois structure of type N on any G-Galois extension.

2.5. Counting

By Proposition 2.8, the bijection

$$s : \mathrm{Reg}(N, \mathrm{Perm}(G)) \to \mathrm{Reg}(G, \mathrm{Perm}(N))$$

restricts to a bijection from

$$\begin{aligned}\mathrm{Reg}^G(N, \mathrm{Perm}(G)) &= \{\alpha \in \mathrm{Reg}(N, \mathrm{Perm}(G)) \mid \alpha(N) \in \mathcal{E}^G(G, [N])\} \\ &= \{\alpha \in \mathrm{Reg}(N, \mathrm{Perm}(G)) \mid \alpha(N) \text{ is normalized by } \lambda(G)\}\end{aligned}$$

to

$$\begin{aligned}\mathrm{Reg}_N(G, \mathrm{Perm}(N)) &= \{\beta \in \mathrm{Reg}(G, \mathrm{Perm}(N)) \mid \beta(G) \in \mathrm{Hol}(N)\} \\ &= \mathrm{Reg}(G, \mathrm{Hol}(N)) \\ &= \{\beta \in \mathrm{Reg}(G, \mathrm{Perm}(N)) \mid \beta(G) \text{ normalizes } \lambda(N)\}.\end{aligned}$$

Now for M in $\mathcal{E}^G(G, [N])$, that is, for M a regular subgroup of $\mathrm{Perm}(G)$ isomorphic to N and normalized by $\lambda(G)$, let α in $\mathrm{Reg}^G(N, \mathrm{Perm}(G))$ have image $\alpha(N) = M$. Then for θ in $\mathrm{Aut}(N)$, $\alpha\theta(N) = M$, and if $\alpha, \alpha' : N \to M$, then $\theta = \alpha^{-1}\alpha'$ is in $\mathrm{Aut}(N)$. So the number $e(G, [N])$ of elements of $\mathcal{E}^G(G, [N])$ satisfies

Proposition 2.9.

$$e(G, [N]) = \frac{|\mathrm{Reg}^G(N, \mathrm{Perm}(G))|}{|\mathrm{Aut}(N)|}.$$

Similarly, given T in $\mathcal{R}_N(N, [G])$, that is, given T a regular subgroup of $\mathrm{Perm}(N)$ that normalizes $\lambda(N)$, let β in $\mathrm{Reg}_N(G, \mathrm{Perm}(N))$ have image $\beta(G) = T$. Then, as above, for ψ in $\mathrm{Aut}(G)$, $\beta\psi(G) = T$ and if $\beta(G) = \beta'(G)$, then $\beta^{-1}\beta'$ is in $\mathrm{Aut}(G)$. So the number $r_N(N, [G])$ of elements of $\mathcal{R}_N(N, [G])$ satisfies

$$r_N(N, [G]) = \frac{|\mathrm{Reg}(G, \mathrm{Hol}(N))|}{|\mathrm{Aut}(G)|}.$$

Since

$$|\mathrm{Reg}(G, \mathrm{Hol}(N))| = |\mathrm{Reg}^G(N, \mathrm{Perm}(G))|,$$

we have Byott's counting formula:

Theorem 2.10.

$$r_N(N, [G]) \cdot |\mathrm{Aut}(G)| = e(G, [N]) \cdot |\mathrm{Aut}(N)|.$$

This enables us to count $e(G, [N])$, the number of Hopf-Galois structures of type N on a G-Galois extension of fields, by finding $r_N(N, [G])$, the number of regular subgroups of $\mathrm{Hol}(N)$ that are isomorphic to G.

2.6. Working with regular subgroups of Hol(N)

Now we present an alternative way to count Hopf-Galois structures of type N on a G-Galois extension.

Given a G-Galois extension L/K and a group N of the same order as G, let $\alpha, \alpha' : N \to \mathrm{Perm}(G)$ be regular embeddings such that $\alpha(N)$ and $\alpha'(N)$ are normalized by $\lambda(G)$. Let $\beta, \beta' : G \to \mathrm{Hol}(N)$ be the corresponding regular embeddings. Then $\alpha(N) = \alpha'(N)$ if and only if there is some automorphism θ of N so that $\alpha' = \alpha\theta$, and so $\beta'(\gamma) = \theta^{-1}\beta(\gamma)\theta$ for all γ in G by Proposition 2.7. So define an equivalence relation on regular embeddings from G to $\mathrm{Hol}(N)$:

DEFINITION 2.11. Two regular embeddings $\beta, \beta' : G \to \mathrm{Hol}(N)$ are equivalent, $\beta \sim \beta'$, if and only if there is some θ in $\mathrm{Aut}(N)$ so that $\alpha' = \alpha\theta$, if and only if the corresponding embeddings β, β' satisfy

$$\beta'(g) = C(\theta^{-1})(\beta(g)) = \theta^{-1}\beta(g)\theta$$

for all g in G.

Thus $\beta \sim \beta'$ if and only if they yield the same Hopf-Galois structure of type N on a G-Galois extension L/K, if and only if there is some θ in $\mathrm{Aut}(N)$ so that the corresponding embeddings α and α' satisfy $\alpha' = \alpha\theta$, if and only if

$$\beta'(g) = \theta^{-1}\beta(g)\theta$$

for all g in G.

So to find Hopf-Galois structures on L/K, we can partition the set of regular subgroups of $\mathrm{Hol}(N)$ isomorphic to G into orbits, conjugacy classes under the action of $\mathrm{Aut}(N)$, pick some convenient representative T of each orbit, and determine the regular embeddings of G into T.

EXAMPLE 2.12. (From [**Chi05**, pp. 295-6]) Let G and N be elementary abelian p-groups of rank n, where we can conveniently view N as the $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$. Then $\mathrm{Hol}(N) = \lambda(N) \rtimes \mathrm{Aut}(N) \cong \mathbb{F}_p^n \rtimes \mathrm{GL}_n(\mathbb{F}_p)$, which may be viewed as the affine group

$$\mathrm{Hol}(\mathbb{F}_p^n) = \mathrm{Aff}_n(\mathbb{F}_p) = \left\{ \begin{pmatrix} \mathrm{GL}_n(\mathbb{F}_p) & \mathbb{F}_p^n \\ 0 & 1 \end{pmatrix} \right\} \subset \mathrm{GL}_{n+1}(\mathbb{F}_p).$$

Now regular subgroups of $\mathrm{Hol}(\mathbb{F}_p^n)$ are p-groups, hence are conjugate under action by $\mathrm{Aut}(N) = \mathrm{GL}_n(\mathbb{F}_p)$ to regular subgroups of U_{n+1}, the p-Sylow subgroup of $\mathrm{Aff}_n(\mathbb{F}_p)$ consisting of upper triangular matrices with unit diagonal. So we can focus on regular subgroups T contained in U_{n+1}. (We'll continue this example later in this section.)

In general, let $\beta : G \to \mathrm{Hol}(N)$ with $\beta(G) = T$. Then $\beta' : G \to \mathrm{Hol}(N)$ has $\beta'(G) = T$ if and only if $\beta' = \beta\psi$ for some ψ in $\mathrm{Aut}(G)$. We ask: given T, how many Hopf-Galois structures correspond to T?

The number of Hopf-Galois structures of type N is in bijective correspondence with the number of equivalence classes of regular embeddings $\beta : G \to \mathrm{Hol}(N)$, where $\beta' \sim \beta$ if and only if $\beta' = C(\theta)\beta$ for some θ in $\mathrm{Aut}(N)$. If we restrict this equivalence relation to regular embeddings of G to $\mathrm{Hol}(N)$ with image T, then we are interested in θ in $\mathrm{Aut}(N)$ so that $C(\theta)(T) = T$.

DEFINITION 2.13. For a given regular subgroup T of $\mathrm{Hol}(N)$, the stabilizer $\mathrm{Sta}(T)$ of T is

$$\mathrm{Sta}(T) = \{\theta \in \mathrm{Aut}(N) \mid C(\theta)T = T\}.$$

PROPOSITION 2.14. *Given a Galois extension with Galois group G of order n, a group N of order n and a regular embedding $\beta_0 : G \to \mathrm{Hol}(N)$ with image T, then the set of equivalence classes of regular embeddings $\beta : G \to \mathrm{Hol}(N)$ with image T is bijective with the set of right cosets of $\beta_0^{-1}\mathrm{Sta}(T)\beta_0$ in $\mathrm{Aut}(G)$.*

PROOF. Given T and a regular embedding $\beta_0 : G \to T$, then all other regular embeddings of G onto T have the form $\beta_0\psi$ for ψ in $\mathrm{Aut}(G)$. For ψ, ψ' in $\mathrm{Aut}(G)$, we have $\beta_0\psi' \sim \beta_0\psi$ if and only if there is some θ in $\mathrm{Aut}(N)$ so that $C(\theta)\beta_0\psi = \beta_0\psi'$, if

and only if $\beta_0^{-1}C(\theta)\beta_0\psi = \psi'$. So conjugating by β_0^{-1} maps $\mathrm{Sta}(T)$ into $\mathrm{Aut}(G)$, and the number of equivalence classes of embeddings $\beta : G \to \mathrm{Hol}(N)$ with $\beta(G) = T$ is equal to the number

$$\frac{|\operatorname{Aut}(G)|}{|\mathrm{Sta}(T)|}.$$

of right cosets of $\mathrm{Sta}(T)$ in $\mathrm{Aut}(G)$. □

Proposition 2.14 then yields:

THEOREM 2.15. *The number of Hopf-Galois structures of type N on a Galois extension L/K with Galois group G is equal to*

$$\sum_{T\in\mathcal{C}} |\operatorname{Aut}(G)|/|\mathrm{Sta}(T)|$$

where $\mathcal{C}$ is a set of representatives of the orbits (conjugacy classes) of regular subgroups of Hol(N) *isomorphic to G under conjugation by elements of* Aut(N).

PROOF. Consider the set $\mathcal{T}$ of regular subgroups of Hol(N) isomorphic to G. Under conjugation by elements of Aut(N), $\mathcal{T}$ is partitioned into orbits. Let $T_1, \ldots, T_r$ be a set of regular subgroups that represent the orbits under conjugation. Let $\beta_i : G \to T_i$ be regular embeddings for $i = 1, \ldots, r$. Then by Proposition 2.14, for each $i = 1, \ldots, r$, the set of equivalence classes of regular embeddings $\beta : G \to T_i$ is bijective with the set of right cosets of $\mathrm{Sta}(T_i)$ in $\mathrm{Aut}(G)$. So the set of equivalence classes of regular embeddings $\beta : G \to \mathrm{Hol}(N)$ is equal to

$$\sum_{T\in\mathcal{C}} |\operatorname{Aut}(G)|/|\mathrm{Sta}(T)|,$$

which is the number of Hopf-Galois structures of type N on a G-Galois extension. □

EXAMPLE 2.16. Continuing Example 2.12, let $G = N$ be elementary abelian groups of order p^3, $p > 3$. We look at regular subgroups of Hol(C_p^3), which we view as $\mathrm{Aff}_3(\mathbb{F}_p) = \begin{pmatrix} \mathrm{GL}_3(\mathbb{F}_p) & \mathbb{F}_p^3 \\ 0 & 1 \end{pmatrix} \subset \mathrm{GL}_4(\mathbb{F}_p)$. As noted in Example 2.12, we may focus on the regular subgroups of the p-Sylow subgroup U_4, the group of upper triangular matrices of $\mathrm{GL}_4(\mathbb{F}_p)$ with diagonal I. [**Chi05**] found that there are five regular subgroups $J_1, \ldots, J_5$ of U_4, generated by

$$\gamma_i = \begin{pmatrix} I + A_i & \epsilon_i \\ 0 & 1 \end{pmatrix} \text{ for } i = 1, 2, 3$$

where $\{\epsilon_1, \epsilon_2, \epsilon_3\}$ is the standard basis of $\mathbb{F}_p^3$ and

$$A_1 = 0, A_2 = \begin{pmatrix} 0 & d & a \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix},$$

with $cd = 0$ and for each J_i, the values of a, b, c, d are:

$$J_1 : (a, b, c, d) = (0, 0, 0, 0);$$
$$J_2 : (a, b, c, d) = (0, 1, 0, 0);$$
$$J_3 : (a, b, c, d) = (0, 1, 0, 1);$$
$$J_4 : (a, b, c, d) = (1, 0, 1, 0);$$
$$J_5 : (a, b, c, d) = (0, 1, 0, d), d \text{ a non-square of } \mathbb{F}_p.$$

Each group has a different stabilizer, and with $\mathrm{Aut}(G) \cong \mathrm{GL}_3(\mathbb{F}_p)$ [**Chi05**] found that

i	$\lvert \mathrm{Aut}(G)\rvert/\lvert\mathrm{Sta}(J_i)\rvert$
1	1
2	$(p^3-1)(p-1)$
3	$(p^3-1)p(p-1)/2$
4	$(p^3-1)p(p+1)/2$
5	$(p^3-1)(p^3-p)$

which sum to give

$$e(C_p^3, C_p^3) = p^6 + p^5 - p^2$$

the number of Hopf-Galois structures of type C_p^3 on a Galois extension of fields with Galois group C_p^3 for $p > 3$ an odd prime.

For extensions of this result, see Sections 5.3 and 5.4.

2.7. Radical algebras

A ring A (with addition $+$ and multiplication $\cdot$ but without a multiplicative identity) is a radical ring if A is a group under the circle operation $\circ$ on A defined by $a \circ b = a + b + a \cdot b$. The group $(A, \circ)$ is called the circle group or the adjoint group of A.

For N an abelian p-group, a regular abelian subgroup T of $\mathrm{Hol}(N)$ corresponds to a radical commutative algebra structure A on the additive group N, by [**CDVS06**], so that $T = \lambda_\circ(A)$, the left regular representation of $(A, \circ)$ in $\mathrm{Perm}(A)$.

In that setting [**CDVS06**] showed that isomorphism classes of algebras correspond bijectively to conjugacy classes of regular subgroups of $\mathrm{Hol}(N)$. Thus for a given algebra A with circle group G and a G-Galois extension L/K, the number of Hopf-Galois structures of type N on L/K is equal to $\lvert \mathrm{Aut}(G)\rvert/\lvert\mathrm{Sta}(T)\rvert$ where $\mathrm{Sta}(T)$ consists of automorphisms of $(A, +)$ that preserve the image $\lambda(A, \circ) = T$ in $\mathrm{Hol}(N)$ of the circle group of A, hence are automorphisms of the circle group, hence of the multiplicative group of A: that is, $\mathrm{Sta}(T) \cong \mathrm{Aut}_{alg}(A)$.

So the number of Hopf-Galois structures corresponding to a given radical ring A is equal to

$$\mathrm{Aut}(A, \circ)/\mathrm{Aut}_{alg}(A).$$

The results of [**CDVS06**] connecting regular subgroups and radical algebra structures turn out to be a special case of results on skew braces, to which we now turn.

2.8. Skew (left) braces

Here is the definition of a skew brace.

DEFINITION 2.17. A skew brace (always "left") is a finite set B with two operations, $\star$ and $\circ$, so that $(B,\star)$ is a group (the "additive group"), $(B,\circ)$ is a group (the circle group, or adjoint group), and the (left) compatibility condition

$$a\circ(b\star c)=(a\circ b)\star a^{-1}\star(a\circ c)$$

holds for all a,b,c in B. Here a^{-1} is the inverse of a in $(B,\star)$. Denote the inverse of a in $(B,\circ)$ by $\overline{a}$.

It is a fact (easily shown from the compatibility condition) that in a skew brace, the identity elements of the groups $(B,\circ)$ and $(B,\star)$ coincide.

When describing a skew brace $(B,\circ,\star)$ our general convention is that $B^\star=(B,\star)$ is the additive group and $B^\circ=(B,\circ)$ is the adjoint, or circle group. So we write $(B,\text{circle operation, additive operation})$. Under the relationship between skew braces and Hopf-Galois structures on Galois extensions of fields, $G=B^\circ$ becomes the Galois group, and $N=B^\star$ the type of the Hopf-Galois structure.

A (left) brace is a skew brace with abelian additive group. When describing braces, $\star$ will typically be replaced by $+$.

A function $f:B=(B,\circ,\star)\to B'=(B',\circ',\star')$ is a homomorphism of skew braces if f is a group homomorphism from $(B,\circ)$ to $(B',\circ')$ and a group homomorphism from $(B,\star)$ to $(B',\star')$

Braces and skew braces generalize radical rings. A radical ring $(A,+,\cdot)$ with circle operation $\circ$ as in Section 2.7 is a brace $(A,\circ,+)$ with additive group $(A,+)$ and circle group $(A,\circ)$: left distributivity in the ring A translates to the (left) compatibility condition for a skew brace. One can check that a left brace that also satisfies the right compatibility condition

$$(a+b)\circ c=(a\circ c)-c+(a\circ c)$$

is a radical ring with multiplication defined by $a\cdot b=a\circ b-a-b$.

We'll consider radical rings briefly in Section 4.8 and more extensively in chapter 5.

Associated to a set B with two group operations $\circ$ and $\star$ are the two left regular representation maps:

$$\lambda_\star:B\to\mathrm{Perm}(B),\ \lambda_\star(b)(x)=b\star x,$$
$$\lambda_\circ:B\to\mathrm{Perm}(B),\ \lambda_\circ(b)(x)=b\circ x.$$

Then there is a characterization of skew braces, Proposition 1.9 of [**GV17**]:

PROPOSITION 2.18. *$(B,\circ,\star)$ is a skew brace if and only if the group homomorphism $\lambda_\circ:(B,\circ)\to\mathrm{Perm}(B)$ has image in $\mathrm{Hol}(B,\star)=\lambda_\star(B)\mathrm{Aut}(B,\star)\subset\mathrm{Perm}(B)$.*

PROOF. For all b,x,y in B, the left skew brace property:

$$b\circ(x\star y)=(b\circ x)\star b^{-1}\star(b\circ y)$$

holds if and only if

$$b^{-1}\star(b\circ(x\star y))=(b^{-1}\star(b\circ x))\star(b^{-1}\star(b\circ y)),$$

if and only if

$$\lambda_\star(b^{-1})\lambda_\circ(b)(x \star y) = (\lambda_\star(b^{-1})\lambda_\circ(b)(x)) \star (\lambda_\star(b^{-1})\lambda_\circ(b)(y)),$$

if and only if

$$\Theta_b = \lambda_\star(b^{-1})\lambda_\circ(b) \text{ is in } \mathrm{Aut}(B,\star) \text{ for all } b \text{ in } B,$$

if and only if

$$\lambda_\circ(b) = \lambda_\star(b)\Theta_b \text{ is in } \mathrm{Hol}(B,\star).$$

□

Propositions 2.8 and 2.18 imply

COROLLARY 2.19. *$(B,\circ,\star)$ is a skew brace if and only if the group homomorphism $\lambda_\star : (B,\star) \to \mathrm{Perm}(B)$ has image $\lambda_\star(B)$ that is normalized by $\lambda_\circ(B)$.*

PROOF. Given a set $B = (B,\circ,\star)$ with two group operations where $(B,\circ) = G$, $(B,\star) = N$, B is a skew brace if and only if the map $\lambda_\circ : (B,\circ) \to \mathrm{Perm}(B)$ by $\lambda_\circ(g)(x) = g \circ x$ has image in $\mathrm{Hol}(B,\star)$. The corresponding element of $\mathrm{Bij}_0(G,N)$ is the map sending g to $\lambda_\circ(g)(e) = g \circ e = g$, the identity map. Similarly, $\lambda_\star : (B,\star) \to \mathrm{Perm}(B)$, sending n to $\lambda_\star(n)(z) = n \star z$, is in $\mathrm{Reg}(N,\mathrm{Perm}(B))$, and the corresponding element of $\mathrm{Bij}_0(N,G)$ is the map sending n to $\lambda_\star(n)(e) = n \star e = n$, also the identity map. So $\lambda_\star$ corresponds to $\lambda_\circ$ under the canonical bijection $s : \mathrm{Reg}(N,\mathrm{Perm}(G)) \to \mathrm{Reg}(G,\mathrm{Perm}(N))$ given by $s(\lambda_\star) = \lambda_\circ$. The result then follows immediately from Proposition 2.8. □

2.9. Connecting skew braces with Hopf-Galois structures

The next two results show the close connection between Hopf-Galois structures on Galois extensions of fields and skew braces.

PROPOSITION 2.20. *Let $(B,\circ,\star)$ be a skew brace. If L/K is a G-Galois extension with $G \cong (B,\circ)$, then L/K has a Hopf-Galois structure of type $(B,\star)$.*

PROOF. If $(B,\circ,\star)$ is a skew brace, then by Proposition 2.18, the image of the left regular representation map $\alpha = \lambda_\star : (B,\star) \to \mathrm{Perm}(B)$ is normalized by $\lambda_\circ(B)$. So α corresponds to a Hopf-Galois structure of type $(B,\star)$ on L/K. □

Conversely, we have:

PROPOSITION 2.21. *Let L/K be a G-Galois extension. Suppose L/K is a Hopf-Galois extension of type $N = (N,\star)$. There is an operation $\circ$ on N so that $(N,\circ) \cong G$ and $(N,\circ,\star)$ is a skew brace.*

PROOF. Since L/K is a Hopf-Galois extension of type N, there is a regular subgroup M of $\mathrm{Perm}(G)$ and a regular embedding $\alpha : N \to \mathrm{Perm}(G)$ with image M.

Since $M \cong (N,\star)$ is a regular subgroup of $\mathrm{Perm}(G)$, let $\alpha : (N,\star) \to \mathrm{Perm}(G)$ be a regular embedding with image M. The map $a : N \to G$ by $a(n) = \alpha(n)[e]$ is then a bijection. Using a, define a new group operation $\circ$ on N by $m \circ n = a^{-1}(a(m) \cdot a(n))$ where $\cdot$ is the multiplication in G. Then a is an isomorphism from $(N,\circ)$ to $(G,\cdot)$. To show that $(N,\circ,\star)$ is a skew brace, we show that $\lambda_\circ(N)$ is contained in $\mathrm{Hol}(N,\star)$. Now $\alpha(m)(g) = a\lambda_\star(m)a^{-1}(g)$, and (cf. Proposition 2.8) corresponds to $\beta : G \to \mathrm{Hol}(N,\star)$, defined by

$$\beta(g)(x) = a^{-1}\lambda_\cdot(g)a(x)$$

for x in N. The isomorphism $a : N \to G$ then yields the map $\beta a : N \to \mathrm{Hol}(N)$ which for n, x in N is

$$\begin{aligned}\beta(a(n))(x) &= a^{-1}\lambda_{\cdot}(a(n))a(x)\\ &= a^{-1}(a(n)\cdot a(x))\\ &= n \circ x.\end{aligned}$$

So the map βa is the map $\lambda_\circ$, and so $(N, \circ, \star)$ is a skew brace. □

2.10. Isomorphic skew braces

Here is a characterization of when two skew braces with the same additive group are isomorphic.

PROPOSITION 2.22. *Two skew brace structures $(B, \circ, \star)$ and $(B, \circ', \star)$ on the group $(B, \star)$ are isomorphic if and only if $\lambda_{\circ'}(B)$ is conjugate to $\lambda_\circ(B)$ in* $\mathrm{Perm}(B)$ *by some θ in* $\mathrm{Aut}(B, \star)$.

PROOF. Suppose $\theta : (B, \circ, \star) \to (B, \circ', \star)$ is an isomorphism of skew braces. Then for all b, c in B,

$$\theta(b) \circ' \theta(c) = \theta(b \circ c)$$

so

$$\lambda_{\circ'}(\theta(b))(\theta(c)) = \theta(\lambda_\circ(b)(c)) = \theta(\lambda_\circ(b)(\theta^{-1}\theta(c))),$$

so

$$\lambda_{\circ'}(\theta(b)) = \theta\lambda_\circ(b)\theta^{-1}.$$

Hence

$$\lambda_{\circ'}(B) = \theta\lambda_\circ(B)\theta^{-1}.$$

Conversely, let θ be in $\mathrm{Aut}(B, \star)$ and suppose

$$\theta\lambda_\circ(B)\theta^{-1} = \lambda_{\circ'}(B).$$

Then for each b there exists b' so that

$$\lambda_{\circ'}(b')(x) = \theta\lambda_\circ(b)\theta^{-1}(x).$$

Setting $x = e$ shows that $b' = \theta(b)$. Then for all c in B,

$$\begin{aligned}\lambda_{\circ'}(\theta(b))(\theta(c)) &= \theta\lambda_\circ(b)\theta^{-1}(\theta(c)),\\ \theta(b) \circ' \theta(c) &= \theta(b \circ c),\end{aligned}$$

and so $\theta : (B, \circ) \to (B, \circ')$ is an isomorphism, hence a skew brace isomorphism from $(B, \circ, \star)$ to $(B, \circ', \star)$. □

This result was first proved in the case where the skew brace arises from a radical F-algebra, F any field, in [**CDVS06**], and is also found as Proposition 4.3 of [**GV17**].

Switching the roles of $\star$ and $\circ$ in the above proof gives:

COROLLARY 2.23. *Two skew brace structures $(B, \circ, \star)$ and $(B, \circ, \star')$ on the group $(B, \circ)$ are isomorphic if and only if $\lambda_{\star'}(B)$ is conjugate to $\lambda_\star(B)$ in* $\mathrm{Perm}(B)$ *by some θ in* $\mathrm{Aut}(B, \circ)$.

Now we can describe the relationship between the number of Hopf-Galois structures of type N on a G-Galois extension and the number of isomorphism types of skew braces $(B, \circ, \star)$ with $B^\circ \cong G$ and $B^\star \cong N$.

The following result is in [**SV18**] and [**NZ19**].

PROPOSITION 2.24. *Let $B = (B, \circ, \star)$ be a skew brace. The number $e_B(G, N)$ of Hopf-Galois structures of type $N \cong (B, \star)$ on a G-Galois extension L/K with $G \cong (B, \circ)$ corresponding to the given skew brace B is*

$$e_B(G, N) = \frac{|\operatorname{Aut}(G)|}{|\operatorname{Aut}_{sb}(B)|}.$$

Here $\operatorname{Aut}_{sb}(B)$ denotes the group of skew brace automorphisms of the skew brace B, that is, bijective maps $B \to B$ that are group homomorphisms on the additive groups and also on the adjoint groups.

PROOF. Given $(B, \circ, \star)$, a skew brace, we have a Hopf-Galois structure uniquely defined by $\lambda_\star(B) \subset \operatorname{Perm}(B)$ normalized by $\lambda_\circ(B)$. Let $\theta \in \operatorname{Aut}(B, \circ)$. Then θ defines an operation $\star'$ on $(B, \circ)$ by

$$\theta(g \star h) = \theta(g) \star' \theta(h),$$

and $\lambda_{\star'}(B) = \theta\lambda_\star(B)\theta^{-1}$. From the definition of $\star'$, $\theta : (G, \circ, \star) \to (G, \circ, \star')$ is a skew brace isomorphism. Since $(G, \circ, \star')$ is a skew brace, $\lambda_{\star'}(B)$ is normalized by $\lambda_\circ(B)$ in $\operatorname{Perm}(B)$ by Corollary 2.19. So $\lambda_{\star'}(B)$ yields a Hopf-Galois structure on L/K.

Now $\lambda_{\star'}(B) = \lambda_\star(B)$ if and only if $\star' = \star$, if and only if θ is an automorphism of $(B, \star)$. For suppose $\lambda_{\star'}(B) = \lambda_\star(B)$. Then for all b in B there is some c in B so that $\lambda_{\star'}(b) = \lambda_\star(c)$ in $\operatorname{Perm}(B)$. Then

$$\lambda_{\star'}(b)[e] = \lambda_\star(c)[e],$$

so $b = c$ and then $b \star' x = b \star x$ for all b, x in B. Hence $\star' = \star$.

So the number $e_B((B, \circ), (B, \star))$ of Hopf-Galois structures of type $(B, \star)$ on L/K with Galois group $(B, \circ)$ arising from the given skew brace isomorphism type of $(B, \circ, \star)$ is equal to $|\operatorname{Aut}(B, \circ)|/|\operatorname{Aut}_{sb}(B, \circ, \star)|$. □

COROLLARY 2.25. *The number $e(G, [N])$ of Hopf-Galois structures of type N on a G-Galois extension of fields is given by*

$$e(G, [N]) = \sum_B e_B(G, N)$$

where B runs through all isomorphism types of skew braces B with given circle group $(B, \circ) = G$ and $(B, \star) \cong N$.

These results demonstrate the close connection between the classification of Hopf-Galois structures on a given G-Galois extension of fields and the classification of skew braces with given circle group. In particular, any result that finds pairs of groups (G, N) where $e(G, [N])$ is or is not zero is also a result on the existence or non-existence of skew braces with circle group G and additive group N. Such issues have been a persistent theme in both theories since their inception (in [**GP87**] and [**Rum07a**], respectively).

CHAPTER 11

Hopf-Galois module theory

This chapter surveys some of the applications of Hopf-Galois theory to questions of integral module structure in extensions of local or global fields, with particular emphasis on developments since the publication of [**Chi00**].

We begin by expanding a little on the summary of classical Galois module theory given in Chapter 1. If L/K is a G-Galois extension of fields then by the Normal Basis Theorem L is a free module of rank one over the group algebra $K[G]$. In the case that L/K is an extension of local or global fields we can investigate integral analogues of this result, with the most natural approach being to study the structure of the ring of integers (or valuation ring) $\mathfrak{O}_L$ as a module over the integral group ring $\mathfrak{O}_K[G]$. Noether's Theorem [**Noe32**] (see also [**Frö83**, Theorem 3]) states that $\mathfrak{O}_L$ is a locally free $\mathfrak{O}_K[G]$-module if and only if L/K is at most tamely ramified. In the local case this is the desired analogue of the Normal Basis Theorem; in the global case it is a necessary condition for $\mathfrak{O}_L$ to be a free $\mathfrak{O}_K[G]$-module.

The integral group ring $\mathfrak{O}_K[G]$ is an example of an $\mathfrak{O}_K$*-order* in $K[G]$: it is a finitely generated projective $\mathfrak{O}_K$-submodule of $K[G]$ that is closed under multiplication, and we have $K \otimes_{\mathfrak{O}_K} \mathfrak{O}_K[G] = K[G]$. One approach to studying wildly ramified extensions is to replace the integral group ring with a larger order in $K[G]$ called the *associated order* of $\mathfrak{O}_L$ in $K[G]$:

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

By construction, this is the largest subring of $K[G]$ for which $\mathfrak{O}_L$ is a module. If $\mathfrak{O}_L$ is a free $\mathfrak{A}_{K[G]}$-module then it must have rank one, and $\mathfrak{A}_{K[G]}$ is the only $\mathfrak{O}_K$-order in $K[G]$ over which $\mathfrak{O}_L$ can possibly be free [**Chi00**, Proposition 12.5]. In general, we have $\mathfrak{O}_K[G] \subseteq \mathfrak{A}_{K[G]}$, and Noether's Theorem implies that we have equality if and only if L/K is at most tamely ramified. The use of associated orders was pioneered by Leopoldt [**Leo59**], who proved that if $L/\mathbb{Q}$ is an abelian extension then $\mathfrak{O}_L$ is a free $\mathfrak{A}_{\mathbb{Q}[G]}$-module. This theorem implies the corresponding result for abelian extensions of $\mathbb{Q}_p$, but it does not generalize easily to other base fields, or to nonabelian Galois groups.

Hopf-Galois theory broadens the scope of these investigations considerably. If L/K is an H-Galois extension of local or global fields then L is a free H-module of rank one [**Chi00**, Theorem 2.16], and we may study $\mathfrak{O}_L$ as a module over its associated order in H:

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

If L/K admits a number of Hopf-Galois structures then we can compare the structure of $\mathfrak{O}_L$ as a module over its various associated orders. Some of the most striking results in this direction arise in the case in which L/K is already Galois in the classical sense. As mentioned in Chapter 1, the publication of [**Chi00**] was largely motivated by results of Byott [**Byo00**], who exhibited a family of G-Galois

extensions of p-adic fields L/K for which $\mathfrak{O}_L$ is not a free $\mathfrak{A}_{K[G]}$-module but is a free $\mathfrak{A}_H$-module for some other Hopf algebra H giving a Hopf-Galois structure on the extension. Hopf-Galois theory can also provide contexts in which we can ask module-theoretic questions about the structure of rings of integers in extensions of local or global fields that are not Galois in the classical sense.

More generally, if L/K is an H-Galois extension then we can study the structure of each fractional ideal $\mathfrak{B}$ of L as a module over its associated order in H:

$$\mathfrak{A}_H(\mathfrak{B}) = \{z \in H \mid z \cdot x \in \mathfrak{B} \text{ for all } x \in \mathfrak{B}\}.$$

In order to streamline the exposition of the results in this chapter, we have chosen to focus on the study of the ring of integers $\mathfrak{O}_L$. A number of the results we present can be generalized to more general fractional ideals: we highlight where this is the case and refer the reader to the original papers for details of these generalizations.

In Section 11.1 we study generalized normal basis generators in Hopf-Galois extensions. We then turn to the study of associated orders in Hopf-Galois extensions. Section 11.2 concerns Childs' theorem, which is the flagship result in this area: if L/K is a finite H-Galois extension of p-adic fields and $\mathfrak{A}_H$ is a Hopf order in H then $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module. We summarize results concerning the application of this result to questions of integral Hopf-Galois module structure in Galois extensions of p-adic fields of degree p or p^2. We then present some tools for studying associated orders that are not Hopf, including subextension techniques based upon the results of Section 8.1. In Section 11.5 we focus on extensions of p-adic fields that are at most tamely ramified: the evidence to date leads us to conjecture that for these extensions each fractional ideal is free over its associated order in every Hopf-Galois structure admitted by the extension. Finally, in Section 11.6 we survey the application of Hopf-Galois theory to questions of integral module structure in extensions of global fields, including some non-normal extensions.

We will always assume that L/K denotes a finite separable extension of fields with Galois closure $\widetilde{L}$, and write $G = \mathrm{Gal}(\widetilde{L}/K)$, $G_L = \mathrm{Gal}(\widetilde{L}/L)$, and $X = G/G_L$. In particular: if L/K is a Galois extension then $G = \mathrm{Gal}(L/K)$, $G_L = \{1\}$, and $X = G$.

11.1. The Normal Basis Theorem for Hopf-Galois structures

The Hopf-Galois analogue of the Normal Basis Theorem is that if L/K is H-Galois then L is a free H-module of rank one [**Chi00**, Theorem 2.16]. An element $x \in L$ with the property that $L = H \cdot x$ is necessarily a free generator of L as an H-module: we shall call such an element a *normal basis generator for L with respect to H*.

11.1.1. Normal basis generators for separable Hopf-Galois extensions. By Greither-Pareigis theory each Hopf algebra giving a Hopf-Galois structure on L/K has the form $H = \widetilde{L}[N]^G$ for N some regular subgroup of $\mathrm{Perm}(X)$ normalized by the image of G under the left translation map $\lambda : G \to \mathrm{Perm}(G)$. In this subsection we give a concrete criterion, in terms of G and N, for an element $x \in L$ to be a normal basis generator for L with respect to H. These results are an amalgamation of results in [**Tru16a**] and [**Tru18b**].

Recall from [**GP87**] that the action of $\widetilde{L}[N]^G$ on L is obtained via descent from the action of $\widetilde{L}[N]$ on $M = \mathrm{Map}(X, \widetilde{L})$. The $\widetilde{L}$-algebra M has a basis of mutually orthogonal idempotents $\{u_{\overline{g}} \mid \overline{g} \in X\}$, where $\overline{g}$ denotes the left coset $gG_L \in X$ and

$$u_{\overline{g}}(\overline{h}) = \delta_{\overline{g},\overline{h}} \text{ for all } \overline{g}, \overline{h} \in X.$$

The group N permutes these idempotents by acting on the subscripts:

$$\eta \cdot u_{\overline{g}} = u_{\eta(\overline{g})} \text{ for all } \eta \in N \text{ and } \overline{g} \in X,$$

and extending this action to $\widetilde{L}[N]$ makes M into an $\widetilde{L}[N]$-Galois extension of $\widetilde{L}$. By Galois descent we obtain that $\widetilde{L}[N]^G$ is a K-Hopf algebra and that M^G is an $\widetilde{L}[N]^G$-Galois extension of K. Finally, we may identify L with the fixed ring M^G via the K-algebra isomorphism $L \xrightarrow{\sim} M^G$ defined by

$$x \mapsto f_x = \sum_{\overline{g} \in X} \overline{g}(x) u_{\overline{g}} \text{ for all } x \in L.$$

LEMMA 11.1. *An element $f \in M^G$ is a free $\widetilde{L}[N]^G$-generator of M^G if and only if it is a free $\widetilde{L}[N]$-generator of M.*

PROOF. If $M^G = \widetilde{L}[N]^G \cdot f$ for some $f \in M^G$ then $\widetilde{L} \otimes_K M^G = \widetilde{L} \otimes_K (\widetilde{L}[N]^G \cdot f)$. By Galois descent, we have $\widetilde{L} \otimes_K M^G = M$ and $\widetilde{L} \otimes_K \widetilde{L}[N]^G = \widetilde{L}[N]$, so we obtain $M = \widetilde{L}[N] \cdot f$. Conversely, if $M = \widetilde{L}[N] \cdot f$ for some $f \in M^G$ then we have $M^G = (\widetilde{L}[N] \cdot f)^G = \widetilde{L}[N]^G \cdot f$. □

LEMMA 11.2. *For $x \in L$, the element f_x is an $\widetilde{L}[N]$-generator of M if and only if the matrix*

$$T_N(x) = (\eta(\overline{g})[x]) \text{ (where } \eta \in N \text{ and } \overline{g} \in X)$$

is nonsingular.

Strictly speaking, the definition of $T_N(x)$ depends upon orderings of the group N and the set X. However, the question of whether it is nonsingular does not.

PROOF. The set $\{u_{\overline{g}} \mid \overline{g} \in X\}$ is an $\widetilde{L}$-basis of M. For $x \in L$ and $\eta \in N$, we have

$$\begin{aligned} \eta \cdot f_x &= \eta \cdot \left(\sum_{\overline{g} \in X} \overline{g}(x) u_{\overline{g}} \right) \\ &= \sum_{\overline{g} \in X} \overline{g}(x) u_{\eta(\overline{g})} \\ &= \sum_{\overline{g} \in X} \eta^{-1}(\overline{g})[x] u_{\overline{g}}. \end{aligned}$$

Therefore the transition matrix from the set $\{u_{\overline{g}} \mid \overline{g} \in X\}$ to the set $\{\eta \cdot f_x \mid \eta \in N\}$ is row equivalent to the matrix $T_N(x)$ defined above, and so f_x is an $\widetilde{L}[N]$-generator of M if and only if this matrix is nonsingular. □

Combining Lemmas 11.1 and 11.2 we obtain:

PROPOSITION 11.3. *An element $x \in L$ is a normal basis generator of L with respect to H if and only if the matrix*

$$T_N(x) = (\eta(\overline{g})[x]) \text{ (where } \eta \in N \text{ and } \overline{g} \in X)$$

is nonsingular.

This result is useful for relating normal basis generators with respect to different Hopf-Galois structures on a given extension: see for example Proposition 11.15.

11.1.2. Valuation criteria for normal basis generators. For extensions of local fields L/K it is sometimes possible to detect normal basis generators in terms of the normalized valuation $v_L : L \to \mathbb{Z} \cup \{\infty\}$. We say that an H-Galois extension of local fields L/K has a *valuation criterion with respect to H* if there is an integer b such that every element $x \in L$ satisfying $v_L(x) = b$ is a normal basis generator of L with respect to H. If such an integer b exists, then all integers that are congruent to b modulo the ramification index of L/K satisfy the same property. Valuation criteria for normal basis generators are an essential component in the development of *scaffolds*: see Chapter 15

The first results on valuation criteria for normal basis generators in Galois extensions of local fields were due to Byott and Elder [**BE07**], who studied elementary abelian totally ramified p-extensions of p-adic fields. In [**Tho08**] Thomas proved an analogous result for arbitrary totally ramified abelian p-extensions of local fields in characteristic p. In both of these cases, the valuation criterion was described in terms of the largest ramification break associated with L/K (see [**Ser62**] or [**Chi00**, §23]). In [**Eld10**] Elder reformulated the existing results on the valuation criterion in terms of the valuation of the relative different $\mathcal{D}_{L/K}$ and resolved the question for local fields of characteristic p:

THEOREM 11.4. *Let L/K be a Galois extension of complete local fields of characteristic p with perfect residue fields. If L/K is a totally ramified p-extension then L/K has a valuation criterion with respect to $K[G]$, with $b \equiv -\mathcal{D}_{L/K} - 1 \pmod{[L : K]}$, and given $i \not\equiv b \pmod{[L : K]}$ there exists $x_i \in L$ that satisfies $v_L(x_i) = i$ but is not a normal basis generator for L with respect to $K[G]$.*

If L/K is not a totally ramified p-extension then given any $i \in \mathbb{Z}$ there exists $x_i \in L$ that satisfies $v_L(x_i) = i$ but is not a normal basis generator for L with respect to $K[G]$.

The most comprehensive results on the Galois case are due to de Smit, Florence, and Thomas [**dSFT12**]. They note that a necessary condition for an element $x \in L$ to be a normal basis generator for L with respect to $K[G]$ is that $\mathrm{Tr}_{L/K}(x) \neq 0$, and that every element of L of valuation b satisfies $\mathrm{Tr}_{L/K}(x) \neq 0$ if and only if L/K is totally ramified and $b \equiv -\mathcal{D}_{L/K} - 1$ [**dSFT12**, Proposition 1.1]. Using this, they prove [**dSFT12**, Proposition 1.2]:

PROPOSITION 11.5. *A Galois extension of local fields L/K with residue characteristic p has a valuation criterion for normal basis generators with respect to $K[G]$ if and only if*

(1) *L/K is a totally ramified p-extension;*
(2) *Every non-zero $K[G]$-submodule of L contains an element of valuation 0.*

In the case that K has characteristic p condition (1) of Proposition 11.5 implies condition (2), and so Proposition 11.5 implies Theorem 11.4 above. In the case that

K has characteristic 0, de Smit, Florence, and Thomas identify precisely the abelian extensions of K that have a valuation criterion for normal basis generators with respect to $K[G]$. If L/K is a totally ramified Kummer p-extension whose Galois group G has exponent $m = p^s$ then this occurs if and only if L is obtained by adjoining m-th roots of units of $\mathfrak{O}_K$; in this case we say that L is a *unit root Kummer extension* of K. More generally [**dSFT12**, Theorem 1.4]:

THEOREM 11.6. *Let L/K be a totally ramified abelian extension of local fields whose degree is a power of the residue characteristic p, let $m = p^s$ be the exponent of G, and let $r \mid m$ be the number of m-th roots of unity inside K. If $p = 2$ and $8 \mid m$, assume that $r \neq 2$. Then L/K has a valuation criterion for normal basis generators with respect to $K[G]$ if and only if every cyclic subextension F/K of L/K of degree r is a unit root Kummer extension.*

In [**Byo11**] Byott generalized the results of [**Eld10**] to give a Hopf-Galois valuation criterion in characteristic p.

THEOREM 11.7. *Let L/K be a separable H-Galois extension of local fields of characteristic p. If L/K is a totally ramified p-extension then L/K has a valuation criterion with respect to H, with $b \equiv -\mathcal{D}_{L/K} - 1 \pmod{[L:K]}$, and given $i \not\equiv b \pmod{[L:K]}$ there exists $x_i \in L$ that satisfies $v_L(x_i) = i$ but is not a normal basis generator for L/K with respect to H.*

If L/K is not a totally ramified p-extension then given any $i \in \mathbb{Z}$ there exists $x_i \in L$ that satisfies $v_L(x_i) = i$ but is not a normal basis generator for L/K with respect to H.

In the case that L/K is a totally ramified p-extension the strategy of the proof is to show that an element $t \in L$ is a normal basis generator for L with respect to H if and only if $\mathrm{Tr}_{L/K}(x) \neq 0$ [**Byo11**, Lemma 2.3]; a consequence this is that in this case the set of normal basis generators is the same for all Hopf-Galois structures on L/K.

At the time of writing there is no known analogue of Theorem 11.7 for Hopf-Galois extensions of p-adic fields.

11.2. Hopf orders and Childs' theorem

A *Hopf order* in a K-Hopf algebra H is an $\mathfrak{O}_K$-order in H which is also an $\mathfrak{O}_K$-Hopf algebra with operations inherited from those on H [**Chi00**, Definition 5.1]. The question of determining all Hopf orders in a given Hopf algebra (in particular, in a given group algebra) is a topic of long-standing interest: Chapter 12 of this book surveys some of the extensive work in this area.

The importance of Hopf orders in Hopf-Galois module theory is due to Childs' Theorem:

THEOREM 11.8 (Childs). *Let L/K be an H-Galois extension of p-adic fields and suppose that $\mathfrak{A}_H$ is a Hopf order in H. Then $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.*

Childs' Theorem is proved in detail in [**Chi00**, Chapter 3]; we summarize the proof below.

To help illuminate this summary, we consider first a Galois extension of p-adic fields L/K that is at most tamely ramified, and reinterpret one half of the standard modern proof of Noether's Theorem [**Frö83**, Theorem 3] using the fact that $\mathfrak{O}_K[G]$ is a Hopf order in $K[G]$ [**Chi00**, §5]. Since L/K is at most tamely ramified there

CHAPTER 12

Hopf orders in group rings

12.1. Hopf orders and Galois module theory

Let K be a field that is complete with respect to a discrete valuation $\nu : K \to \mathbb{Z} \cup \{\infty\}$. Let $\mathfrak{O}_K = \{x \in K \mid \nu(x) \geq 0\}$ denote its valuation ring, with group of units $\mathfrak{O}_K^\times = \{x \in \mathfrak{O}_K \mid \nu(x) = 0\}$ and unique maximal ideal $\mathfrak{p} = \{x \in \mathfrak{O}_K \mid \nu(x) \geq 1\}$, and let π denote a uniformizing parameter of K (so that $\nu(\pi) = 1$). Assume that the residue field $k = \mathfrak{O}_K/\mathfrak{p}$ is finite, with characteristic p. Then K is either a finite extension of the p-adic rationals $\mathbb{Q}_p$ (a p-adic field) or the field of formal Laurent series $\mathbb{F}_q((T))$ over a finite field $\mathbb{F}_q$, where q is a power of p.

Now let L be a G-Galois extension of K, with valuation ring $\mathfrak{O}_L$. Then, as discussed in the overview of Galois module theory in Chapter 11, $\mathfrak{O}_L$ is a module over its associated order $\mathfrak{A}$ in the Hopf algebra $K[G]$, and we seek criteria for $\mathfrak{O}_L$ to be a free $\mathfrak{A}$-module. If $\mathrm{char}(K) = 0$ then, by Childs' generalization of Noether's theorem (Theorem 11.8), a sufficient condition for this to occur is that $\mathfrak{A}$ is a *Hopf order* in $K[G]$:

Definition 12.1. An $\mathfrak{O}_K$-order in $K[G]$ that is also an $\mathfrak{O}_K$-Hopf algebra with operations inherited from those on $K[G]$ is called an $\mathfrak{O}_K$*-Hopf order* in $K[G]$.

To show that an $\mathfrak{O}_K$-order H in $K[G]$ is an $\mathfrak{O}_K$-Hopf order, it suffices to show that the comultiplication on $K[G]$ restricts to H: see [**Und15**, Proposition 3.4.5].

It is not hard to show that the integral group ring $\mathfrak{O}_K[G]$ is a Hopf order in $K[G]$, and the proof of the "if" part of Noether's theorem can be interpreted in this Hopf-theoretic framework: see Section 11.2. Childs' theorem generalizes this approach to the case of wild extensions: the strategy is to determine $\mathfrak{A}$ and check to see whether it is an $\mathfrak{O}_K$-Hopf order in $K[G]$. This requires, of course, good knowledge of the structure of $\mathfrak{O}_K$-Hopf orders in $K[G]$ for G a finite group.

Childs also generalizes the "only if" part of Noether's theorem, again assuming that $\mathfrak{A}$ is a Hopf order. In this case $\mathfrak{O}_L$ is an $\mathfrak{A}$-*extension of* $\mathfrak{O}_K$: that is, $\mathfrak{O}_L$ is an $\mathfrak{A}$-module algebra and the fixed ring

$$\{x \in \mathfrak{O}_L \mid a \cdot x = \varepsilon(a)x \ \forall a \in \mathfrak{A}\}$$

is equal to $\mathfrak{O}_K$. Childs shows that there is a left integral θ of $\mathfrak{A}$ such that $\theta \cdot \mathfrak{O}_L = \mathfrak{O}_K$ [**Chi00**, Theorem 13.3]. That is, $\mathfrak{O}_L$ is a *tame* $\mathfrak{A}$*-extension of* $\mathfrak{O}_K$ (see Section 11.2). In this language, a G-Galois extension L/K is at most tamely ramified if and only if $\mathfrak{O}_L$ is a tame $\mathfrak{O}_K[G]$-extension of $\mathfrak{O}_K$.

Example 12.2. Let $K = \mathbb{Q}_p(\zeta_p)$ and let π be the uniformizing parameter for K. Then the polynomial $x^p - \pi$ is irreducible over K by Eisenstein's criterion. Let $L = K(z)$, where z is a root of $x^p - \pi$. Then L/K is Galois with group $C_p = \langle g \rangle$; the Galois action is given as $g^i(z) = \zeta_p^i z$. Since $\pi = z^p$, L/K is wild.

We have $\mathfrak{O}_L = \mathfrak{O}_K[z]$. The associated order $\mathfrak{A}$ contains the elements $\{e_i\}$, $0 \leq i \leq p-1$, where

$$e_i = \frac{1}{p}\sum_{j=0}^{p-1} \zeta_p^{-ij} g^j.$$

Thus $\mathfrak{A}$ is the maximal integral order in $K[C_p]$. Arguing via duality (see Section 12.2 below) we can show that $\mathfrak{A}$ is an $\mathfrak{O}_K$-Hopf order in $K[C_p]$. By the results of Childs cited above, $\mathfrak{O}_L$ is a free rank one $\mathfrak{A}$-module and a tame $\mathfrak{A}$-extension of $\mathfrak{O}_K$.

We might also ask: given a Hopf order H in a group algebra $K[G]$ (for some finite group G) does there exist a G-Galois extension L/K such that $\mathfrak{A} = H$?

Definition 12.3. An $\mathfrak{O}_K$-Hopf order H in $K[G]$ is *realizable* if there exists a G-Galois extension L/K whose associated order $\mathfrak{A}$ in $K[G]$ is H.

Realizability is of central importance in Galois module theory. For if H is realizable, then there exists a G-Galois extension L/K for which $H = \mathfrak{A}$. Thus $\mathfrak{A}$ is a Hopf order and so by Childs' Theorem (Theorem 11.8) $\mathfrak{O}_L$ is a free rank one $\mathfrak{A}$-module; we have characterized $\mathfrak{O}_L$ as a Galois module. Moreover, $\mathfrak{O}_L$ is a tame $\mathfrak{A}$-extension of $\mathfrak{O}_K$.

There is also a narrower definition of realizability:

Definition 12.4. An $\mathfrak{O}_K$-Hopf order H in $K[G]$ is *realizable as a Galois group* if there exists a G-Galois extension L/K for which the valuation ring $\mathfrak{O}_L$ of L is an H-Galois extension of $\mathfrak{O}_K$.

If H is realizable as a Galois group then it is realizable in the sense of Definition 12.3. For if L/K is a G-Galois extension for which $\mathfrak{O}_L$ is an H-Galois extension of $\mathfrak{O}_K$ then $\mathfrak{O}_L$ is a free H-module of rank one, so $H = \mathfrak{A}$ (by [**Chi00**, Proposition 12.5]) and $\mathfrak{O}_L$ is a tame $\mathfrak{A}$-extension of $\mathfrak{O}_K$. However, it is possible for $\mathfrak{A}$ to be a Hopf order in $K[G]$ (so that that $\mathfrak{O}_L$ is a free rank one $\mathfrak{A}$-module and a tame $\mathfrak{A}$-extension of $\mathfrak{O}_K$) without $\mathfrak{O}_L$ being an $\mathfrak{A}$-Galois extension of $\mathfrak{O}_K$. To explain this, we first need to generalize the notion of the discriminant of $\mathfrak{O}_L$.

Recall that a *(left) integral* of H is an element $\theta \in H$ that satisfies

$$h\theta = \varepsilon(h)\theta,$$

for all $h \in H$. The set of integrals of H forms an ideal of H, denoted by I_H (see [**Chi00**, §3]), and by [**Und11**, Proposition 4.3.3], there exists a generating integral Λ for I_H. Suppose that $\mathfrak{O}_L$ is an H-extension of $\mathfrak{O}_K$, and let $\{x_1, x_2, \ldots, x_n\}$ denote a basis for $\mathfrak{O}_L$ over $\mathfrak{O}_K$. Let M denote the $n \times n$ matrix whose i,jth entry is

$$m_{i,j} = \Lambda \cdot (x_i x_j).$$

The *discriminant* of $\mathfrak{O}_L$ over $\mathfrak{O}_K$ with respect to H is the ideal of $\mathfrak{O}_K$ defined by

$$\det(M)\mathfrak{O}_K.$$

The discriminant is independent of the choice of $\mathfrak{O}_K$-basis for $\mathfrak{O}_L$. We denote the discriminant with respect to H by $\mathrm{disc}_H(\mathfrak{O}_L/\mathfrak{O}_K)$.

Proposition 12.5. *Let K be a p-adic field and let L/K be a G-Galois extension. Let H be an $\mathfrak{O}_K$-Hopf order in $K[G]$, and suppose that $\mathfrak{O}_L$ is an H-extension of $\mathfrak{O}_K$. Then $\mathfrak{O}_L$ is an H-Galois extension of $\mathfrak{O}_K$ if and only if* $\mathrm{disc}_H(\mathfrak{O}_L/\mathfrak{O}_K) = \mathfrak{O}_K$.

Proof. See [**Und11**, Proposition 10.3.8]. □

Now we give an example of an extension L/K for which $\mathfrak{A}$ is a Hopf order in $K[G]$ (so $\mathfrak{O}_L$ is a free rank one $\mathfrak{A}$-module and a tame $\mathfrak{A}$-extension of $\mathfrak{O}_K$) but $\mathfrak{O}_L$ is not an $\mathfrak{A}$-Galois extension of $\mathfrak{O}_K$.

EXAMPLE 12.6. Let $K = \mathbb{Q}_p(\zeta_p)$, where ζ_p is a primitive pth root of unity, let π be a uniformizing parameter for $\mathfrak{O}_K$. Then the polynomial $x^p - \pi$ is irreducible over K by Eisenstein's criterion. Let $L = K(z)$, where z is a root of $x^p - \pi$. Then L/K is Galois with group $C_p = \langle g \rangle$; the Galois action is given as $g^i(z) = \zeta_p^i z$. Since $\pi = z^p$, L/K is wild. We have $\mathfrak{O}_L = \mathfrak{O}_K[z]$.

As stated in Example 12.2, the associated order $\mathfrak{A}$ is an $\mathfrak{O}_K$-Hopf order in $K[C_p]$. By results of Childs discussed above, $\mathfrak{O}_L$ is isomorphic to $\mathfrak{A}$ as $\mathfrak{A}$-modules and $\mathfrak{O}_L$ is a tame $\mathfrak{A}$-extension of $\mathfrak{O}_K$.

Note that

$$\Lambda = \frac{1}{p} \sum_{g \in C_p} g$$

is a generating integral for $\mathfrak{A}$. We compute $\mathrm{disc}_{\mathfrak{A}}(\mathfrak{O}_K[z]/\mathfrak{O}_K)$. We first compute $\mathrm{disc}(\mathfrak{O}_K[z]/\mathfrak{O}_K)$. With respect to the basis $\{1, z, z^2, \ldots, z^{p-1}\}$, we have by [**Lan65**, p. 348],

$$\mathrm{disc}(\mathfrak{O}_K[z]/\mathfrak{O}_K) = (-1)^{p(p-1)/2} \mathrm{N}_{L/K}(pz^{p-1})\mathfrak{O}_K = p^p \pi^{p-1} \mathfrak{O}_K.$$

Thus

$$\begin{aligned} p^p \pi^{p-1} \mathfrak{O}_K &= \det(\mathrm{Tr}_{L/K}(z^a z^b))\mathfrak{O}_K \\ &= p^p \det(\mathrm{Tr}_{L/K}(z^a z^b)/p)\mathfrak{O}_K \\ &= p^p \det(\Lambda(z^a z^b))\mathfrak{O}_K. \end{aligned}$$

Thus,

$$\mathrm{disc}_{\mathfrak{A}}(\mathfrak{O}_L/\mathfrak{O}_K) = \pi^{p-1}\mathfrak{O}_K \neq \mathfrak{O}_K.$$

Thus by Proposition 12.5, $\mathfrak{O}_L$ is not a $\mathfrak{A}$-Galois extension of $\mathfrak{O}_K$.

In this chapter we shall construct and classify classes of Hopf orders in group algebras over K and decide which of those are realizable or not (in the sense of Definition 12.4).

12.2. Dual Hopf orders

If H is an $\mathfrak{O}_K$-Hopf algebra, free of finite rank over $\mathfrak{O}_K$, then the linear dual $H^* = \mathrm{Hom}_{\mathfrak{O}_K}(H, \mathfrak{O}_K)$ is an $\mathfrak{O}_K$-Hopf algebra with structure maps induced from those on H by duality (see [**Und11**, Proposition 4.1.7] or [**Und15**, Proposition 3.1.12]).

If K is a field and G is a finite group then the group algebra $K[G]$ is a K-Hopf algebra with comultiplication $\Delta : K[G] \to K[G] \otimes_K K[G]$ defined as $g \mapsto g \otimes g$, counit $\varepsilon : K[G] \to K$ given as $g \mapsto 1$, and antipode $S : K[G] \to K[G]$ defined as $g \mapsto g^{-1}$, for $g \in G$.

Let $\{e_g\}_{g \in G}$ be the basis for $K[G]^*$ that is dual to the basis $\{g\}_{g \in G}$ for $K[G]$, i.e., $\langle e_g, h \rangle = \delta_{g,h}$ where

$$\langle -, - \rangle : K[G]^* \times K[G] \to K$$

is the duality pairing.

By [**Und11**, Proposition 4.1.7] (or [**Und15**, Proposition 3.1.12]), $K[G]^*$ is a K-Hopf algebra. Multiplication on $K[G]^*$ is defined through duality:

$$\begin{aligned}(e_g e_h)(s) &= m_{K[G]}(e_g \otimes e_h)\Delta_{K[G]}(s)\\ &= m_{K[G]}(e_g \otimes e_h)(s \otimes s)\\ &= e_g(s)e_h(s)\\ &= \delta_{g,s}\delta_{h,s}\\ &= \delta_{g,h}e_g(s)\end{aligned}$$

for $g, h, s \in G$. Thus $\{e_g\}_{g\in G}$ is a set of mutually orthogonal idempotents and as a K-algebra $K[G]^*$ decomposes as

$$K[G]^* = \bigoplus_{g\in G} Ke_g.$$

The unit map $i_{K[G]^*} : K \to K[G]^*$ is defined through duality:

$$i_{K[G]^*}(r)(g) = r(\varepsilon_{K[G]}(g)) = r,$$

for $r \in K$, $g \in G$.

The Hopf algebra structure on $K[G]^*$ is also defined through duality. Comultiplication is given as

$$\begin{aligned}\Delta_{K[G]^*}(e_g)(s \otimes t) &= e_g(m_{K[G]}(s \otimes t))\\ &= e_g(st)\\ &= \Big(\sum_{\substack{a,b\in G,\\ g=ab}} e_a \otimes e_b\Big)(s \otimes t)\end{aligned}$$

for $g, s, t \in G$. Thus

$$\Delta_{K[G]^*}(e_g) = \sum_{\substack{a,b\in G,\\ g=ab}} e_a \otimes e_b.$$

The counit map is given as

$$\begin{aligned}\varepsilon_{K[G]^*}(e_g)(r) &= e_g(i_{K[G]}(r))\\ &= e_g(1)r\end{aligned}$$

for $g, r \in G$, thus

$$\varepsilon_{K[G]^*}(e_g) = e_g(1).$$

Finally, the antipode is given by

$$\begin{aligned}S_{K[G]^*}(e_g)(t) &= e_g(S_{K[G]}(t))\\ &= e_g(t^{-1})\\ &= e_{g^{-1}}(t)\end{aligned}$$

for $g, t \in G$, thus

$$S_{K[G]^*}(e_g) = e_{g^{-1}}.$$

PROPOSITION 12.7. *Let $G = C_{p^n}$ denote the cyclic group of order p^n, $n \geq 1$, and suppose that K contains a primitive p^nth root of unity, ζ_{p^n}. Then $K[C_{p^n}]^* \cong K[C_{p^n}]$ as K-Hopf algebras.*

PROOF. Let $\{e_i\}_{i=0}^{p^n-1}$ be the basis for $K[C_{p^n}]^*$ dual to the basis $\{g^i\}_{i=0}^{p^n-1}$ for $K[C_{p^n}]$. There is a K-Hopf algebra isomorphism $\psi : K[C_{p^n}]^* \to K[C_{p^n}]$ defined as

$$\psi(e_i) = \frac{1}{p^n} \sum_{j-0}^{p^n-1} \zeta_{p^n}^{-ij} g^j$$

for $0 \leq i \leq p^n - 1$. □

REMARK 12.8. Suppose K contains a primitive p^nth root of unity, ζ_{p^n}. Let $\widehat{C}_{p^n}$ denote the group of characters of C_{p^n}. Then $\widehat{C}_{p^n}$ is cyclic of order p^n, generated by the character $\gamma : C_{p^n} \to K$; we have $C_{p^n} = \langle \gamma \rangle = \{\gamma^i\}$, $0 \leq i \leq p^n - 1$, where $\gamma^i(g^j) = \zeta_{p^n}^{ij}$, $0 \leq j \leq p^n - 1$; $\widehat{C}_{p^n} \cong C_{p^n}$, the isomorphism being given as $\gamma \mapsto g$. $K[\widehat{C}_{p^n}] \cong K[C_{p^n}]$ as K-Hopf algebras through the map $\gamma \mapsto g$.

We make the identification

$$K[C_{p^n}]^* := K[\widehat{C}_{p^n}],$$

where e_i, $0 \leq i \leq p^n - 1$, is identified with the element $\frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_{p^n}^{-ij} \gamma^j$ in $K[\widehat{C}_{p^n}]$.

The linear dual $H^* = \mathrm{Hom}_{\mathfrak{O}_K}(H, \mathfrak{O}_K)$ can be defined as

$$H^* = \{x \in K[G]^* \mid \langle x, H \rangle \subseteq \mathfrak{O}_K\}.$$

PROPOSITION 12.9. *Let H be an $\mathfrak{O}_K$-Hopf order in $K[G]$, G a finite group. Then H^* is an $\mathfrak{O}_K$-Hopf order in $K[G]^*$.*

PROOF. By [**Und15**, Proposition 3.1.12], $K[G]^*$ is a finite dimensional Hopf algebra over K. We check that H^* is an $\mathfrak{O}_K$-order in $K[G]^*$. By [**Und11**, Proposition 4.1.7], H^* is an $\mathfrak{O}_K$-Hopf algebra with multiplication induced from that of $K[G]^*$ since $\Delta_{K[G]}(H) \subseteq H \otimes_{\mathfrak{O}_K} H$. Thus H^* is an $\mathfrak{O}_K$-subalgebra of $K[G]^*$.

In addition, H^* is an $\mathfrak{O}_K$-submodule $K[G]^*$, free of rank $|G|$ over $\mathfrak{O}_K$, and

$$K \otimes_{\mathfrak{O}_K} H^* \cong (K \otimes_{\mathfrak{O}_K} H)^* \cong K[G]^*$$

as K-algebras. Thus H^* is an $\mathfrak{O}_K$-order in $K[G]^*$.

Finally, the maps $\Delta_{K[G]^*}$, $\varepsilon_{K[G]^*}$ and $S_{K[G]^*}$ induce on H^* its structure as an $\mathfrak{O}_K$-Hopf algebra. Thus H^* is an $\mathfrak{O}_K$-Hopf order in $K[G]^*$. □

We stated earlier that the integral group ring $\mathfrak{O}_K[G]$ is an example of an $\mathfrak{O}_K$-Hopf order in $K[G]$. In fact:

PROPOSITION 12.10. *Let H be an $\mathfrak{O}_K$-Hopf order in $K[G]$. Then $\mathfrak{O}_K[G] \subseteq H$.*

PROOF. The group ring $\mathfrak{O}_K[G]$ is an $\mathfrak{O}_K$-Hopf order in $K[G]$. Thus by Proposition 12.9, $\mathfrak{O}_K[G]^*$ is an $\mathfrak{O}_K$-Hopf order in $K[G]^*$. We have

$$\mathfrak{O}_K[G]^* = \bigoplus_{g \in G} \mathfrak{O}_K e_g,$$

where $\{e_g\}_{g \in G}$ is the basis for $\mathfrak{O}_K[G]^*$ dual to the basis $\{g\}_{g \in G}$ for $\mathfrak{O}_K[G]$.

We claim that $\mathfrak{O}_K[G]^*$ is the maximal $\mathfrak{O}_K$-Hopf order in $K[G]^*$. To see this, let $\alpha = \sum_{g \in G} r_g e_g \in K[G]^*$ with $r_g \in K \setminus \mathfrak{O}_K$ for some $g \in G$. Then α cannot be integral over $\mathfrak{O}_K$. Thus $\mathfrak{O}_K[G]^*$ is maximal. Consequently, $H^* \subseteq \mathfrak{O}_K[G]^*$ and so $\mathfrak{O}_K[G] \subseteq H$. □

Proposition 12.10 is also proved in [**Lar67**, Theorem], [**Und11**, Proposition 4.4.3] without using duality.

12.2.1. Galois H^*-objects and realizability. We have seen that if H is an $\mathfrak{O}_K$-Hopf algebra, free of finite rank over $\mathfrak{O}_K$, then the linear dual $H^* = \mathrm{Hom}_{\mathfrak{O}_K}(H, \mathfrak{O}_K)$ is an $\mathfrak{O}_K$-Hopf algebra. Let $\Delta = \Delta_{H^*}$ and $\varepsilon = \varepsilon_{H^*}$ denote the comultiplication and counit map of H^*. An $\mathfrak{O}_K$-module A is called a *right H^*-comodule* if there exists an $\mathfrak{O}_K$-linear map $\alpha : A \to A \otimes_{\mathfrak{O}_K} H^*$ for which

(i) $(\alpha \otimes Id)\alpha = (Id \otimes \Delta)\alpha$,
(ii) $(Id \otimes \varepsilon)\alpha(b) = b \otimes 1,\ \forall b \in A$.

We adapt the Sweedler notation to write

$$\alpha(b) = \sum_{(b)} b_{(1)} \otimes b_{(2)},$$

for $b, b_{(1)} \in A$, $b_{(2)} \in H^*$.

Now suppose that A is an $\mathfrak{O}_K$-algebra with multiplication $m_A : A \otimes_{\mathfrak{O}_K} A \to A$ and unit map $i_A : \mathfrak{O}_K \to A$ that is also a (right) H^*-comodule. Then $A \otimes_{\mathfrak{O}_K} A$ is an H^*-comodule via

$$\alpha : A \otimes A \to A \otimes A \otimes H^*$$

defined as $b \otimes c \mapsto \sum_{(b),(c)} b_{(1)} \otimes c_{(1)} \otimes b_{(2)}c_{(2)}$ and $\mathfrak{O}_K$ is an H^*-comodule via $\alpha(r) = r \otimes 1_{H^*}$. We say that A is an *H^*-comodule algebra* if m_A, i_A are H^*-comodule homomorphisms, and that A is a *Galois H^*-object* if in addition the map

$$\gamma : A \otimes A \to A \otimes H^*$$

defined by $\gamma(b \otimes c) = (b \otimes 1)\alpha(c)$ is an isomorphism. (See Chapter 10.)

These concepts appeared in Section 10.1. Similarly to Proposition 10.9 and Corollary 10.10, we have

PROPOSITION 12.11. *Let H be an $\mathfrak{O}_K$-Hopf algebra that is free of finite rank over $\mathfrak{O}_K$. Then A is an H-Galois extension of $\mathfrak{O}_K$ if and only if A is a Galois H^*-object.*

PROOF. See [**Chi00**, (2.10) Corollary]. □

We can infer the realizability (in the sense of Definition 12.4) of $\mathfrak{O}_K$-Hopf orders though the use of short exact sequences.

Let G be a finite abelian group with $G' \leq G$. The short exact sequence of groups

$$1 \to G' \to G \to G'' \to 1,$$

$G'' \cong G/G'$, induces a short exact sequence of K-Hopf algebras

$$K \to K[G'] \to K[G] \to K[G''] \to K$$

[**Chi00**, §4].

Let H be an $\mathfrak{O}_K$-Hopf order in $K[G]$. Then there is a short exact sequence of $\mathfrak{O}_K$-Hopf orders

$$\mathfrak{O}_K \to H' \to H \to H'' \to \mathfrak{O}_K,$$

dualizing as

$$\mathfrak{O}_K \to J' \to J \to J'' \to \mathfrak{O}_K,$$

where $J' = (H'')^*$, $J = H^*$ and $J'' = (H')^*$.

PROPOSITION 12.12. *Suppose A is a Galois J-object with J-comodule algebra map $\alpha : A \to A \otimes J$. Then*

$$A_{J'} = \{x \in A \mid \alpha(x) \in A \otimes_{\mathfrak{O}_K} J' \subseteq A \otimes_{\mathfrak{O}_K} J\}$$

is a Galois J'-object and A is a Galois $(A_{J'} \otimes_{\mathfrak{O}_K} J'')$-object.

PROOF. See [**Gre92**, Part II, Lemma 1.6]. □

COROLLARY 12.13. *Suppose that A is an H-Galois extension of $\mathfrak{O}_K$. Then $A_{J'}$ is an H''-Galois extension of $\mathfrak{O}_K$ and A is an H'-Galois extension of $A_{J'}$.*

PROOF. This follows from Proposition 12.11. □

Corollary 12.13 generalizes the classical Fundamental Theorem of Galois Theory in the following sense. Suppose H is realizable as a Galois group via the Galois extension L/K with group G. Then $\mathfrak{O}_L$ is an H-Galois extension of $\mathfrak{O}_K$. Thus $(\mathfrak{O}_L)_{J'}$ is a Galois H''-extension of $\mathfrak{O}_K$. In fact, $(\mathfrak{O}_L)_{J'}$ is the ring of integers of the fixed field L' of $G' \subseteq G$. In other words, the Hopf quotient

$$H/(H')^+H \cong H''$$

is realizable as a Galois group via the extension L'/K with group $G/G' \cong G''$.

Moreover, $\mathfrak{O}_L$ is a Galois H'-extension of $(\mathfrak{O}_L)_{J'}$ and the Hopf kernel H' is realizable as a Galois group via the Galois extension L/L' with group G'.

Thus:

COROLLARY 12.14. *If H is realizable as a Galois group, then H'' and H' are realizable as Galois groups.*

12.3. Byott's theorem on realizability

In [**Byo04c**, Theorem 6.1] Byott provided a convenient criterion for realizability.

Byott's result requires that certain Hopf algebras are local rings. So we review a general method for showing that a commutative $\mathfrak{O}_K$-Hopf algebra is local.

Let A be a commutative ring. The *nilradical* of A, denoted as $\mathrm{nil}(A)$, is the ideal consisting of all of the nilpotent elements of A.

PROPOSITION 12.15. *Let*

$$\mathfrak{O}_K \to H' \to H \xrightarrow{s} H'' \to \mathfrak{O}_K$$

be a short exact sequence of finite (finitely generated, projective as $\mathfrak{O}_K$-modules) commutative $\mathfrak{O}_K$-Hopf algebras. Then H is local if and only if H' and H'' are local.

PROOF. We may consider the situation over $k = \mathfrak{O}_K/\mathfrak{p}$.

Suppose that $kH' = k \otimes_{\mathfrak{O}_K} H'$ and $kH'' = k \otimes_{\mathfrak{O}_K} H''$ are local. We show that $kH = k \otimes_{\mathfrak{O}_K} H$ is local. Then $\ker(\varepsilon_{kH'})$ is the unique maximal ideal of kH' and $\ker(\varepsilon_{kH''})$ is the unique maximal ideal of kH''. By [**Und11**, Proposition 1.3.2], $\mathrm{nil}(kH')$ is the intersection of all prime ideals of kH'. But each prime ideal of kH' is maximal, hence $\mathrm{nil}(kH') = \ker(\varepsilon_{kH'})$. Likewise $\mathrm{nil}(kH'') = \ker(\varepsilon_{kH''})$.

We always have $\mathrm{nil}(kH) \subseteq \ker(\varepsilon_{kH})$. Let $x \in \ker(\varepsilon_{kH})$. Then $s(x) \in \mathrm{nil}(kH'')$ and so, $(s(x))^n = s(x^n) = 0$ for some $n > 0$. Thus $x^n \in \ker(\varepsilon_{kH'})kH = \mathrm{nil}(kH')kH$. Thus $x^n \in \mathrm{nil}(kH)$. And so, $\mathrm{nil}(kH) \subseteq \ker(\varepsilon_{kH})$, which implies that kH is local. It follows that H is local.

Conversely, suppose that kH is local, so that $\ker(\varepsilon_{kH}) = \mathrm{nil}(kH)$. Then $\ker(\varepsilon_{kH'}) = \mathrm{nil}(kH')$ and $\ker(\varepsilon_{kH''}) = \mathrm{nil}(kH'')$ and so, KH' and kH'' are local. Thus H' and H'' are local. □

THEOREM 12.16 (Byott). *Let K be a p-adic field, let G be an abelian group of order p^n, $n \geq 1$. Let H be an $\mathfrak{O}_K$-Hopf order in $K[G]$ and suppose that H^* is a local ring. Then H is realizable as a Galois group if and only if H^* is a monogenic $\mathfrak{O}_K$-algebra.*

PROOF. Suppose H^* is monogenic of rank $q = p^n$ over $\mathfrak{O}_K$. Set $m = q - 1$. Let $\overline{x} = (x_1, x_2, \cdots, x_m)$, x_i indeterminate. Set $q_1 = q$, $q_i = 1$, $2 \leq i \leq m$. Let $\mathrm{wt} : \mathfrak{O}_K[[\overline{x}]] \to \mathbb{Z} \cup \{\infty\}$ denote the weight function determined by the integers $q_1, q_2, \ldots, q_m$ [**Byo04c**, Definition 4.5].

By Byott's Embedding Theorem ([**Byo04c**, Theorem 5.4]) there exists an isogeny

$$\varphi : F \to G$$

of m-dimensional formal groups with

$$H^* \cong \mathfrak{O}_K[[\overline{x}]]_F/(\varphi(\overline{x}))$$

where the isogeny is defined as

$$\varphi(\overline{x}) = (\varphi_1(\overline{x}), \varphi_2(\overline{x}), \ldots, \varphi_m(\overline{x}))$$

with

$$\varphi_1(\overline{x}) \equiv x_1^q \bmod \mathrm{wt}\ q+1,$$

$$\varphi_i(\overline{x}) = x_i, \quad 2 \leq i \leq m.$$

Here the equivalence is defined as follows: $\varphi_1(\overline{x}) \equiv x_1^q \bmod \mathrm{wt}\ q+1$ if $\varphi_1 - x_1^q = \sum_\alpha c_\alpha \overline{x}^\alpha$ where $c_\alpha = 0$ for all α with $\mathrm{wt}(\overline{x}^\alpha) < q+1$.

Let $c \in \mathfrak{p} \backslash \mathfrak{p}^2$, and let $A = \mathfrak{O}_K[[\overline{x}]]/J$, where J is the ideal

$$(\varphi_1(\overline{x}) - c, \varphi_2(\overline{x}), \ldots, \varphi_m(\overline{x})).$$

By [**Byo04c**, Lemma 3.7], A is a Galois H^*-object. Thus by Proposition 12.11, A is an H-Galois extension of $\mathfrak{O}_K$. We have

$$A \cong \mathfrak{O}_K[[x_1]]/(\psi(x_1) - c),$$

with $\psi(x_1) = \varphi_1(x_1, 0, 0, \ldots, 0)$.

The power series $\psi(x_1)$ satisfies $\psi(x_1) \equiv x_1^q \bmod \deg\ q+1$. By the Weierstrass Preparation Theorem,

$$\psi(x_1) - c = f(x_1)u(x_1)$$

where $f(x_1)$ is an irreducible polynomial of degree q and $u(x_1)$ is an invertible power series. Consequently,

$$A \cong \mathfrak{O}_K[[x_1]]/(f(x_1)) \cong \mathfrak{O}_K[x_1]/(f(x_1)).$$

Let α be a zero of $f(x_1)$ in some algebraic closure K^{alg}. Then $A \cong \mathfrak{O}_K[\alpha]$ is the ring of integers of $L = K(\alpha)$.

We know that $\mathfrak{O}_K[\alpha]$ is an H-Galois extension of $\mathfrak{O}_K$. Thus (see discussion following Definition 7.1)

$$j : \mathfrak{O}_K[\alpha] \# H \to \mathrm{End}(\mathfrak{O}_K[\alpha])$$

is an isomorphism of algebras. Since $\mathfrak{O}_K[G] \subseteq H$, this says that L/K is Galois with group G and so H is realizable as a Galois group.

For the converse suppose there exists a Galois extension L/K with group G, $|G| = p^n$, for which $\mathfrak{O}_L$ is H-Galois. Let $k = \mathfrak{O}_K/\mathfrak{p}$ denote the residue class field of $\mathfrak{O}_K$. Since k is finite, $\mathfrak{O}_L$ is monogenic over $\mathfrak{O}_K$ [**CF67**, Proposition 1, p. 33]. Thus $\mathfrak{O}_L/\mathfrak{p}\mathfrak{O}_L$ is a monogenic k-algebra.

Now $k \otimes_{\mathfrak{O}_K} \mathfrak{O}_L = \mathfrak{O}_L/\mathfrak{p}\mathfrak{O}_L$ is a Galois $(k \otimes_{\mathfrak{O}_K} H)$-extension of k and so $k \otimes_{\mathfrak{O}_K} H^*$ is monogenic over k by [**Byo04c**, Corollary 4.4]. By Nakayama's lemma, H^* is then monogenic over $\mathfrak{O}_K$. □

REMARK 12.17. In the proof of Theorem 12.16 it is important that H^* is local. For then $k \otimes_{\mathfrak{O}_K} H^*$ is local with unique maximal ideal its augmentation ideal $(k \otimes_{\mathfrak{O}_K} H^*)^+$.

Now, the nilradical $\mathrm{nil}(k \otimes_{\mathfrak{O}_K} H^*)$ is the intersection of all prime ideals of $k \otimes_{\mathfrak{O}_K} H^*$. But every non-zero prime ideal of $k \otimes_{\mathfrak{O}_K} H^*$ is maximal. Thus, $\mathrm{nil}(k \otimes_{\mathfrak{O}_K} H^*) = (k \otimes_{\mathfrak{O}_K} H^*)^+$.

By [**Wat79**, 6.8, Lemma], the largest separable algebra of $k \otimes_{\mathfrak{O}_K} H^*$ is k and so by [**Wat79**, 6.6, Theorem], $k \otimes_{\mathfrak{O}_K} H^*$ represents a connected k-group scheme. We can then use [**Wat79**, 14.4, Theorem] to write

$$k \otimes_{\mathfrak{O}_K} H^* \cong k[x_1]/(x_1^q)$$

(since $k \otimes_{\mathfrak{O}_K} H^*$ is also monogenic). This is a key step in Byott's proof of his Embedding theorem.

Byott tells us precisely when a Hopf order is realizable in the sense of Definition 12.3.

THEOREM 12.18 (Byott). *Let K be a p-adic field, let G be an abelian group G of order p^n, $n \geq 1$. Let H be an $\mathfrak{O}_K$-Hopf order in $K[G]$ and suppose that both H and H^* are local rings. Then H is realizable if and only if H^* is a monogenic $\mathfrak{O}_K$-algebra. That is, there exists a Galois extension L/K with group G and $\mathfrak{A} = H$, if and only if H^* is monogenic.*

PROOF. If H^* is monogenic, then by Theorem 12.16, there exists a Galois extension L/K with group G for which $\mathfrak{O}_L$ is an H-Galois extension of $\mathfrak{O}_K$. Thus $H = \mathfrak{A}_{L/K}$, and so H is realizable.

Conversely, suppose H is realizable, i.e., there exists a Galois extension L/K with group G and $\mathfrak{A}_{L/K} = H$. Then by Childs' Theorem $\mathfrak{O}_L$ is is free rank one H-module and so $\mathfrak{O}_L$ is a tame H-extension.

Since H is local, [**Chi00**, (14.7) Theorem, (2) $\rightarrow$ (3)] applies to show that $\mathfrak{O}_L$ is an H-Galois extension of $\mathfrak{O}_K$. Thus by Theorem 12.16, H^* is monogenic. □

12.4. Group valuations and Larson orders

Let K be a p-adic field. For G arbitrary, the only general construction of Hopf orders in $K[G]$ is due to Larson [**Lar76**]. Larson's construction involves the notion of a group valuation. We follow the treatment given in [**Und11**, §5.2, §5.3].

12.4.1. Group valuations.

DEFINITION 12.19. Let G be a finite group. A *group valuation* is a function $\xi : G \rightarrow \mathbb{Z} \cup \{\infty\}$ which satisfies, for all $g, h \in G$,

(i) $\xi(g) \geq 0$;

(ii) $\xi(g) = \infty$ if and only if $g = 1$;

(iii) $\xi(gh) \geq \min\{\xi(g), \xi(h)\}$;

(iv) $\xi(ghg^{-1}h^{-1}) \geq \xi(g) + \xi(h)$.

We review some properties of the group valuation ξ on G.

PROPOSITION 12.20. *For all $g, h \in G$,*

(i) $\xi(g) = \xi(g^{-1})$;

(ii) $\xi(ghg^{-1}) = \xi(h)$.

PROOF. For (i), let $g \in G$ and let $n = |\langle g \rangle|$, thus $g^{n-1} = g^{-1}$. Since $g = (g^{n-1})^{n-1}$,

$$\xi(g) = \xi((g^{n-1})^{n-1}) \geq \xi(g^{n-1}) = \xi(g^{-1})$$

by Definition 12.19(iii). On the other hand, $\xi(g^{-1}) = \xi(g^{n-1}) \geq \xi(g)$.

For (ii), let $g, h \in G$. Then

$$\begin{aligned} \xi(ghg^{-1}) &= \xi(ghg^{-1}h^{-1}h) \\ &\geq \min\{\xi(ghg^{-1}h^{-1}), \xi(h)\} \quad \text{by Definition 12.19(iii)} \\ &\geq \min\{\xi(g) + \xi(h), \xi(h)\} \quad \text{by Definition 12.19(iv)} \\ &\geq \xi(h). \end{aligned}$$

Now,

$$\xi(h) = \xi(g^{-1}(ghg^{-1})g) \geq \xi(ghg^{-1}) \geq \xi(h),$$

thus $\xi(h) = \xi(ghg^{-1})$. □

Let $\mathbb{Z}_{\geq 0} = \{r \in \mathbb{Z} | r \geq 0\}$ and let ξ be a group valuation on G. For each $r \in \mathbb{Z}_{\geq 0}$, put

$$G_r = \{g \in G \mid \xi(g) \geq r\}.$$

PROPOSITION 12.21. *For each $r \in \mathbb{Z}_{\geq 0}$, G_r is a normal subgroup of G.*

PROOF. By Definition 12.19(iii), G_r is closed under the binary operation of G. We have $1 \in G_r$ since $\xi(1) = \infty$ and $g^{-1} \in G_r$ whenever $g \in G_r$ by Proposition 12.20(i). Thus $G_r \leq G$.

Now let $gh \in gG_r$. Then $\xi(ghg^{-1}) = \xi(h) \geq r$ by Proposition 12.20(ii) and so, $ghg^{-1} \in G_r$. Thus $gG_r \subseteq G_r g$. Next, let $hg \in G_r g$. Then $\xi(g^{-1}hg) = \xi(h) \geq r$, and so $g^{-1}hg \in G_r$, thus, $G_r g \subseteq gG_r$. □

PROPOSITION 12.22. *Let ξ be a group valuation on G, where G is a p-group of order p^n. Then ξ has at most n distinct finite values.*

PROOF. Let $m = \max\{\xi(g) \mid g \in G, g \neq 1\}$. We have $G_0 = G$, $1 = G_{m+1}$, and $1 \subset G_m$ since there exists at least one $g \in G$ with $\infty > \xi(g) \geq m$. Now by Proposition 12.21, $G_j \triangleleft G$ for $0 \leq j \leq m$ and so there is a normal series

$$1 \subset G_m \subseteq G_{m-1} \subseteq \cdots \subseteq G_1 \subseteq G_0 = G$$

which can be refined to a composition series

$$1 \subset N_s \subset N_{s-1} \subset \cdots \subset N_1 \subset N_0 = G$$

with $N_i/N_{i+1} \cong C_p$, for $i = 0, 1, \ldots, s$ (here, $N_{s+1} = 1$). Note that $s = n - 1$.

For each i, $0 \leq i \leq s$, there is a subseries

$$G_{r+1} \subseteq N_{i+1} \subset N_i \subseteq G_r.$$

Let $g \in N_i \backslash N_{i+1}$. Since $g \in G_r$, $\xi(g) \geq r$. But since $g \notin N_{i+1}$, $g \notin G_{r+1}$ and thus, $\xi(g) \ngeq r + 1$. Thus $\xi(g) = r$. Let $r_i = r$ and let $\{r_i\}$ denote the collection of the r_i as i ranges from 0 to s.

Note that each non-trivial $g \in G$ is in $N_i \backslash N_{i+1}$ for exactly one i and so the collection $\{r_i\}_{i=0}^s$ determines the values of ξ. At most n of the values in $\{r_i\}_{i=0}^s$ are distinct since $s + 1 = n$. □

DEFINITION 12.23. Let G be a finite group. The group valuation $\xi : G \to \mathbb{Z} \cup \{\infty\}$ is *order bounded* with respect to the discrete valuation ν if

(i) $\xi(g) = 0$ for $|\langle g\rangle|$ not a power of p,

(ii) $\xi(g) \leq e/(p^a - p^{a-1})$ for $|\langle g\rangle| = p^a$, $a \geq 1$ (where $e = \nu(p)$).

An order bounded group valuation (obgv) ξ on G is *p-adic* if $\xi(g^p) \geq p\xi(g)$ for all $g \in G$.

12.4.2. Hopf orders from group valuations (Larson orders). Let G be a finite group. Larson [**Lar76**, Proposition 3.2] has shown that order bounded group valuations on G give rise to Hopf orders in $K[G]$. We sketch Larson's proof, for complete details see [**Chi00**, (18.1)].

THEOREM 12.24 (Larson). *Let K be a p-adic field and let G be a finite group. Let ξ be a group valuation on G which is order bounded with respect to ν. Let $A(\xi)$ be the $\mathfrak{O}_K$-subalgebra of $K[G]$ generated by $\pi^{-\xi(g)}(g-1)$ for $g \neq 1$. Then $A(\xi)$ is an $\mathfrak{O}_K$-Hopf order in $K[G]$.*

PROOF. We consider first the case where $\xi(g) > 0$ for all $g \in G$. The elements of $G\backslash\{1\}$ can be ordered by the rule: $g \leq h$ if and only if $\xi(g) \leq \xi(h)$. We have the list of elements of $G\backslash\{1\}$:

$$g_1 \leq g_2 \leq g_3 \leq \cdots \leq g_l.$$

For each i, $1 \leq i \leq l$, let A_{g_i} be the $\mathfrak{O}_K$-subalgebra of $K\langle g_i\rangle$ of the form

$$A_{g_i} = \mathfrak{O}_K[\pi^{-\xi(g_i)}(g_i - 1)].$$

Since ξ is order bounded, each A_{g_i} is a finitely generated $\mathfrak{O}_K$-module and thus the tensor product

$$A_{g_1} \otimes A_{g_2} \otimes \cdots \otimes A_{g_l}$$

is finitely generated.

Larson next shows that there is a surjective map of $\mathfrak{O}_K$-modules

$$s : A_{g_1} \otimes A_{g_2} \otimes \cdots \otimes A_{g_l} \to A(\xi),$$

defined by $s(a_{g_1} \otimes a_{g_2} \otimes \cdots \otimes a_{g_l}) = a_{g_1} a_{g_2} \cdots a_{g_l}$. Thus $A(\xi)$ is finitely generated.

Now, let ξ be an arbitrary obgv on G and let $G_+ = \{g \in G \mid \xi(g) > 0\}$. By Proposition 12.21, G_+ is a normal subgroup of G. Now, $\xi|_{G_+}$ is an obgv on G_+ and as we have seen above, $A(\xi|_{G_+})$ is a finitely generated $\mathfrak{O}_K$-submodule of $K[G_+]$. It follows that

$$A(\xi) = A(\xi|_{G_+})\mathfrak{O}_K[G]$$

is finitely generated.

Since $K \otimes_{\mathfrak{O}_K} A(\xi) \cong K[G]$, $A(\xi)$ is an $\mathfrak{O}_K$-order in $K[G]$.

We have $\varepsilon_{K[G]}(A(\xi)) \subseteq \mathfrak{O}_K$. Also, since $\Delta_{K[G]}(g) = g \otimes g$ for all $g \in G$,

$$\Delta_{K[G]}\left(\frac{g-1}{\pi^{\xi(g)}}\right) = \frac{g-1}{\pi^{\xi(g)}} \otimes 1 + 1 \otimes \frac{g-1}{\pi^{\xi(g)}} + (g-1) \otimes \frac{g-1}{\pi^{\xi(g)}},$$

and so,

$$\Delta_{K[G]}(A(\xi)) \subseteq A(\xi) \otimes_{\mathfrak{O}_K} A(\xi).$$

Now, $S_{K[G]}(A(\xi)) \subseteq A(\xi)$ follows from Proposition 12.20(i), and so $A(\xi)$ is an $\mathfrak{O}_K$-Hopf algebra with structure induced from $K[G]$. Thus $A(\xi)$ is an $\mathfrak{O}_K$-Hopf order in $K[G]$. □

An $\mathfrak{O}_K$-Hopf order H in $K[G]$ is a *Larson order* in $K[G]$ if H is of the form $A(\xi)$ where ξ is a p-adic obgv on G. Note that the group ring $\mathfrak{O}_K[G]$ is a Larson order given by the trivial p-adic obgv: $\xi(g) = 0$, $\forall g \in G$.

We describe Larson orders in $K[G]$ where $G = C_{p^n}$ is the cyclic group of order p^n generated by g.

First, we consider the case $n = 1$. To characterize a Larson order in $K[C_p]$, we need only describe the possible p-adic obgvs on C_p. By Proposition 12.22, an obgv ξ on C_p has exactly one finite value: we have $\xi(g) = i$ for $g \neq 1$. Since ξ is order bounded, $0 \leq i \leq e'$, where $e' = e/(p-1)$. Since $\xi(g^p) = \xi(1) = \infty \geq \xi(g)$, ξ is p-adic. The Larson order $H = A(\xi)$ is written as

$$H = A(\xi) = \mathfrak{O}_K\left[\frac{g-1}{\pi^i}, \frac{g^2-1}{\pi^i}, \ldots, \frac{g^{p-1}-1}{\pi^i}\right].$$

PROPOSITION 12.25. $H = \mathfrak{O}_K\left[\dfrac{g-1}{\pi^i}\right]$.

PROOF. Clearly, $\mathfrak{O}_K\left[\frac{g-1}{\pi^i}\right] \subseteq A(\xi)$. So we prove the reverse containment. For $a = 2, 3, \ldots, p-1$, one has

$$\frac{g^a-1}{\pi^i} = \sum_{m=0}^{a-1} \binom{a}{m} \pi^{i(a-m-1)} \left(\frac{g-1}{\pi^i}\right)^{a-m}$$

Thus $\frac{g^a-1}{\pi^i} \in \mathfrak{O}_K\left[\frac{g-1}{\pi^i}\right]$ which proves the proposition. □

We shall denote the Larson order of Proposition 12.25 by $H(i)$ since it depends on only one valuation parameter i, $0 \leq i \leq e'$.

We next consider Larson orders in $K[G]$ where $G = C_{p^2}$. By Proposition 12.22, a group valuation ξ on C_{p^2} has at most two finite values: $\xi(g^a) = i$, for $1 \leq a \leq p^2-1$, $a \equiv 0 \pmod p$, and $\xi(g^b) = j$, for $1 \leq b \leq p^2-1$, $b \not\equiv 0 \pmod p$. Since ξ is order bounded, $0 \leq i \leq e'$ and $0 \leq j \leq e'/p$, and since ξ is p-adic, $pj \leq i$. The Larson order $H = A(\xi)$ can be written as

$$H = A(\xi) = \mathfrak{O}_K\left[\left\{\frac{g^a-1}{\pi^i}, \frac{g^b-1}{\pi^j}\right\}_{a,b}\right],$$

where $1 \leq a \leq p^2-1$, $a \equiv 0 \pmod p$, $1 \leq b \leq p^2-1$, $b \not\equiv 0 \pmod p$.

PROPOSITION 12.26. $H = A(\xi) = \mathfrak{O}_K\left[\frac{g^p-1}{\pi^i}, \frac{g-1}{\pi^j}\right]$.

PROOF. The proof of Proposition 12.25 shows that

$$A(\xi) = \mathfrak{O}_K\left[\frac{g^p-1}{\pi^i}\right]\left[\left\{\frac{g^b-1}{\pi^j}\right\}_b\right],$$

$1 \leq b \leq p^2-1$, $b \not\equiv 0 \pmod p$. Certainly, $\mathfrak{O}_K\left[\frac{g^p-1}{\pi^i}, \frac{g-1}{\pi^j}\right] \subseteq A(\xi)$, so it remains to show that $A(\xi) \subseteq \mathfrak{O}_K\left[\frac{g^p-1}{\pi^i}, \frac{g-1}{\pi^j}\right]$. For $b = 2, 3, \ldots, p^2-1$, $b \not\equiv 0 \pmod p$, one has

$$\frac{g^b-1}{\pi^j} = \sum_{m=0}^{b-1} \binom{b}{m} \pi^{j(b-m-1)} \left(\frac{g-1}{\pi^j}\right)^{b-m}.$$

Thus $\frac{g^b-1}{\pi^i} \in \mathfrak{O}_K\left[\frac{g^p-1}{\pi^i}, \frac{g-1}{\pi^j}\right]$ which proves the proposition. □

We denote the Larson order $H = A(\xi)$ in $K[C_{p^2}]$ by $H(i,j)$ since it depends on only two values of the group valuation ξ, namely, $\xi(g^p) = i$ and $\xi(g) = j$.

For the general case, Larson orders in $K[C_{p^n}]$ can be described as follows.

PROPOSITION 12.27. *Let $n \geq 1$, and let ξ be a p-adic obgv on C_{p^n}. Then the Larson order $A(\xi)$ in $K[C_{p^n}]$ has the form*

$$A(\xi) = \mathfrak{O}_K \left[\frac{g^{p^{n-1}} - 1}{\pi^{i_1}}, \frac{g^{p^{n-2}} - 1}{\pi^{i_2}}, \ldots, \frac{g^p - 1}{\pi^{i_{n-1}}}, \frac{g-1}{\pi^{i_n}} \right]$$

where i_r, $1 \leq r \leq n$, are integers satisfying $0 \leq pi_r \leq i_{r-1}$ for $2 \leq r \leq n$.

PROOF. By Proposition 12.22, a p-adic obgv on C_{p^n} has n distinct finite values $\xi(g^{p^{n-r}}) = i_r$, for $r = 1, \ldots, n$, which satisfy $0 \leq pi_r \leq i_{r-1}$ for $2 \leq r \leq n$. We use induction on n. As we have shown, the proposition is true for the cases $n = 1, 2$, thus we assume that the $(n-1)$st case holds.

Let

$$B = \mathfrak{O}_K \left[\left\{ \frac{g^a - 1}{\pi^{\xi(g^a)}} \;\middle|\; 1 \leq a \leq p^n - 1, a \equiv 0 \pmod{p} \right\} \right].$$

Then

$$A(\xi) = B \left[\left\{ \frac{g^b - 1}{\pi^{i_n}} \;\middle|\; 1 \leq b \leq p^n - 1, b \not\equiv 0 \pmod{p} \right\} \right].$$

By the induction hypothesis, $B = C$ with

$$C = \mathfrak{O}_K \left[\frac{g^{p^{n-1}} - 1}{\pi^{i_1}}, \frac{g^{p^{n-2}} - 1}{\pi^{i_2}}, \ldots, \frac{g^p - 1}{\pi^{i_{n-1}}} \right],$$

and so,

$$A(\xi) = C \left[\left\{ \frac{g^b - 1}{\pi^{i_n}} \middle| 1 \leq b \leq p^n - 1, b \not\equiv 0 \pmod{p} \right\} \right].$$

Now,

$$\frac{g^b - 1}{\pi^{i_n}} = \sum_{m=0}^{b-1} \binom{b}{m} \pi^{i_n(b-m-1)} \left(\frac{g-1}{\pi^{i_n}} \right)^{b-m}$$

and so,

$$A(\xi) = \mathfrak{O}_K \left[\frac{g^{p^{n-1}} - 1}{\pi^{i_1}}, \frac{g^{p^{n-2}} - 1}{\pi^{i_2}}, \ldots, \frac{g^p - 1}{\pi^{i_{n-1}}} \right] \left[\frac{g-1}{\pi^{i_n}} \right]. \qquad \square$$

Larson orders in $K[C_{p^n}]$ will be denoted as $H(i_1, i_2, \ldots, i_n)$.

For c with $0 \leq c \leq e'/p^{n-1}$, $\xi(g) = c$ defines a p-adic order bounded group valuation on C_{p^n}; the corresponding Hopf order is the *one-parameter Larson order* in $K[C_{p^n}]$:

$$H(p^{n-1}c, \ldots, pc, c) = \mathfrak{O}_K \left[\frac{g^{p^{n-1}} - 1}{\pi^{p^{n-1}c}}, \ldots, \frac{g^p - 1}{\pi^{pc}}, \frac{g-1}{\pi^c} \right].$$

By construction one-parameter Larson orders are monogenic as $\mathfrak{O}_K$-algebras; we have

$$H(p^{n-1}c, \ldots, pc, c) = \mathfrak{O}_K \left[\frac{g-1}{\pi^c} \right].$$

One-parameter Larson orders will be used to construct a class of Hopf orders in Section 12.8.

12.4.3. Group valuations from Hopf orders. Let G be a finite group. Then Larson shows that an $\mathfrak{O}_K$-Hopf order in $K[G]$ determines a p-adic obgv on G [**Lar76**, Section 3].

PROPOSITION 12.28. *Let G be a finite group and let H be an $\mathfrak{O}_K$-Hopf order in $K[G]$. Then H determines a p-adic obgv on G.*

PROOF. Define $\xi(g) = \infty$ if $g = 1$. For each $g \in G$, $g \neq 1$, let $|\langle g \rangle| = l$. If l is not a power of p, set $\xi(g) = 0$. If $|\langle g \rangle|$ is a power of p, then define

$$I_g = \{x \in K \mid x(g-1) \in H\}$$

and

$$I_g^{-1} = \{x \in K \mid xI_g \subseteq \mathfrak{O}_K\}.$$

By Proposition 12.10, $\mathfrak{O}_K[G] \subseteq H$ and so $\mathfrak{O}_K \subseteq I_g$. Thus I_g^{-1} is an ideal of $\mathfrak{O}_K$; I_g is a principal fractional ideal in K and we have $I_g^{-1} I_g = \mathfrak{O}_K$. Put $\xi(g) = \nu(I_g^{-1})$.

Thus $\xi(g) \geq 0$ for all $g \in G$ and so, the function $\xi : G \to \mathbb{Z} \cup \{\infty\}$ satisfies Definition 12.19(i),(ii).

For $g, h \in G$, we have

$$gh - 1 = (g-1)h + h - 1,$$

and so, $I_g \cap I_h \subseteq I_{gh}$. Thus, $I_{gh}^{-1} \subseteq (I_g \cap I_h)^{-1}$.

We can assume without loss of generality that $I_g = I_g \cap I_h$ and so, there exists $x \in I_g \cap I_h$ so that $xI_g^{-1} = \mathfrak{O}_K$. Now $x(I_g^{-1} + I_h^{-1}) = \mathfrak{O}_K + xI_h^{-1} = \mathfrak{O}_K$, hence $(I_g \cap I_h)(I_g^{-1} + I_h^{-1}) = \mathfrak{O}_K$. Thus

$$(I_g \cap I_h)^{-1} = I_g^{-1} + I_h^{-1}$$

and consequently, $I_{gh}^{-1} \subseteq I_g^{-1} + I_h^{-1}$. It follows that

$$\xi(gh) \geq \min\{\xi(g), \xi(h)\}.$$

By [**Chi00**, Theorem (17.1)(ii)], $\xi(ghg^{-1}h^{-1}) \geq \xi(g) + \xi(h)$, hence ξ is a group valuation.

To show that ξ is order bounded and p-adic, see [**Chi00**, Theorem (17.1)(iv), (v)]. □

Thus each $\mathfrak{O}_K$-Hopf order H in $K[G]$ gives rise to a p-adic obgv on G which we denote as $\Xi(H)$.

Given an $\mathfrak{O}_K$-Hopf order H in $K[G]$, $\Xi(H)$, in turn, yields a Larson order $A(\Xi(H))$ which is contained in H. For a given H, $A(\Xi(H))$ is the *largest Larson order contained in H* [**Und94**, §1.4], [**Und96**, §2.1], [**Chi00**, §19].

For valuations ξ and ξ' on G, define $\xi \leq \xi'$ if $\xi(g) \leq \xi'(g)$ for all $g \in G$. The relationship between A and Ξ is given as follows.

PROPOSITION 12.29. *Let H be an $\mathfrak{O}_K$-Hopf order in $K[G]$. Let ξ be an obgv on G. Then*

(i) $A(\Xi(H)) \subseteq H$, with equality holding if H is a Larson order.

(ii) $\xi \leq \Xi(A(\xi))$, with equality holding if ξ is p-adic.

PROOF. See [**Chi00**, §19]. □

Let G be any finite group and let H be an $\mathfrak{O}_K$-Hopf order in $K[G]$. Let $\Xi(H)$ be the p-adic obgv determined by H and let

$$G_+ = \{g \in G \mid \Xi(H)(g) > 0\}.$$

Then G_+ is a p-group, and by Proposition 12.21, G_+ is a normal subgroup of G.

Let $k = \mathfrak{O}_K/\mathfrak{p}$ denote the residue field of K. Following [**Chi00**, (20.1)], there is a homomorphism of k-Hopf algebras

$$j : k[G] \to k \otimes_{\mathfrak{O}_K} H,$$

which yields the group homomorphism

$$j : \Gamma(k[G]) \to \Gamma(k \otimes_{\mathfrak{O}_K} H),$$

where $\Gamma(-)$ denotes the set of grouplike elements. Now, $\Gamma(k[G]) = G$.

LEMMA 12.30. $\ker(j) = G_+$.

PROOF. Let $b_1, b_2, \ldots, b_n$ be an $\mathfrak{O}_K$-basis for H. Then their images form a k-basis for $k \otimes_{\mathfrak{O}_K} H$. Now if $j(g) = 1$, then $j(g-1) = 0$ in $k \otimes_{\mathfrak{O}_K} H$. Thus $g - 1 = \sum_{m=1}^{n} r_m b_m$, with $\nu(r_m) > 0$ for all m. Thus $g - 1 \in \pi H$, so that $\Xi(H)(g) > 0$, i.e., $g \in G_+$. Conversely, if $g \in G_+$, then $j(g-1) = 0$ in $k \otimes_{\mathfrak{O}_K} H$, hence $g \in \ker(j)$. □

PROPOSITION 12.31. *Suppose G is a group with no non-trivial normal subgroup which is a p-group. Then $\mathfrak{O}_K[G]$ is the only Hopf order in $K[G]$.*

PROOF. Let H be an $\mathfrak{O}_K$-Hopf order in $K[G]$ and let

$$j : \Gamma(k[G]) \to \Gamma(k \otimes_{\mathfrak{O}_K} H),$$

be the group homomorphism. By Lemma 12.30, $\ker(j) = G_+$.

Now, $\ker(j)$ is trivial since G admits no non-trivial normal subgroups that are p-groups. Consequently j is an injection, which yields $k[G] \cong k \otimes_{\mathfrak{O}_K} H$. By Nakayama's lemma, we conclude that $\mathfrak{O}_K[G] \cong H$. □

Here is another consequence of Lemma 12.30. Let G be a finite group with $|G| > 2$. Then $\mathbb{Z}_p[G]$ is the only $\mathbb{Z}_p$-Hopf order in $\mathbb{Q}_p[G]$. To see this, suppose that H is a $\mathbb{Z}_p$-Hopf order and let $\Xi(H)$ be the associated p-adic obgv. In this case, $\nu(p) = 1$, $k = \mathbb{Z}_p/\mathfrak{p} = \mathbb{F}_p$, and so by Definition 12.23(ii), G_+ is trivial. Thus

$$j : \Gamma(\mathbb{F}_p[G]) \to \Gamma(\mathbb{F}_p \otimes_{\mathfrak{O}_K} H)$$

is an injection. It follows that $H = \mathbb{Z}_p[G]$.

If the order of G is relatively prime to p then the only Hopf order in $K[G]$ is $\mathfrak{O}_K[G]$. So we look for Hopf orders in the cases where G is an abelian p-group, for instance $G = C_{p^n}$, where C_{p^n} is the cyclic group of order p^n or $G = C_p^n$, where C_p^n is the elementary abelian group of order p^n.

To give a complete accounting of Hopf orders in $K[C_{p^n}]$ or $K[C_p^n]$, we need to look beyond the Larson orders in $K[C_{p^n}]$ or $K[C_p^n]$; not every Hopf order in $K[C_{p^n}]$ is Larson. For an example, suppose $K = \mathbb{Q}_p(\zeta_{p^2})$, where ζ_{p^2} is a primitive p^2nd root of unity, and let $\widehat{C}_{p^2}$ denote the character group of C_{p^2}.

By Proposition 12.9, the dual $\mathfrak{O}_K[C_{p^2}]^*$ is an $\mathfrak{O}_K$-Hopf order in $K[C_{p^2}]^*$. But in view of Remark 12.8, $\mathfrak{O}_K[C_{p^2}]^*$ is an $\mathfrak{O}_K$-Hopf order in $K[\widehat{C}_{p^2}]$ and has the form

$$\mathfrak{O}_K[C_{p^2}]^* = \bigoplus_{i=0}^{p^2-1} \mathfrak{O}_K e_i,$$

where

$$e_i = \frac{1}{p^2}\sum_{j=0}^{p^2-1} \zeta_{p^2}^{-ij}\gamma^j.$$

We can take this one step further and identify e_i with

$$\frac{1}{p^2}\sum_{j=0}^{p^2-1} \zeta_{p^2}^{-ij} g^j,$$

and thus view $\mathfrak{O}_K[C_{p^2}]^*$ as an $\mathfrak{O}_K$-Hopf order in $K[C_{p^2}]$.

PROPOSITION 12.32. *The $\mathfrak{O}_K$-Hopf order $\mathfrak{O}_K[C_{p^2}]^*$ in $K[C_{p^2}]$ is not Larson, i.e. $\mathfrak{O}_K[C_{p^2}]^*$ is not of the form $A(\xi)$ for some p-adic obgv ξ on C_{p^2}.*

PROOF. By way of contradiction, we assume that $\mathfrak{O}_K[C_{p^2}]^* = A(\xi)$ for some p-adic obgv ξ on C_{p^2}. By Proposition 12.22, an obgv on C_{p^2} has at most two finite values: $\xi(g^{pa}) = i$ for $a = 1, 2, \ldots, p-1$, and $\xi(g^b) = j$ for $\gcd(b,p) = 1$. Since ξ is order bounded, $0 \le i \le e/(p-1) = p(p-1)/(p-1) = p$, and $0 \le j \le e/p(p-1) = 1$.

Let $I_{\mathfrak{O}_K[C_{p^2}]}$, $I_{\mathfrak{O}_K[C_{p^2}]^*}$ denote the ideal of left integrals of $\mathfrak{O}_K[C_{p^2}]$, $\mathfrak{O}_K[C_{p^2}]^*$, respectively. By [**Und11**, Proposition 4.4.11],

$$\nu(\varepsilon_{\mathfrak{O}_K[C_{p^2}]}(I_{\mathfrak{O}_K[C_{p^2}]})) + \nu(\varepsilon_{\mathfrak{O}_K[C_{p^2}]^*}(I_{\mathfrak{O}_K[C_{p^2}]^*})) = 2e = 2p(p-1),$$

and so, since $\nu(\varepsilon_{\mathfrak{O}_K[C_{p^2}]}(I_{\mathfrak{O}_K[C_{p^2}]})) = 2p(p-1)$, $\nu(\varepsilon_{\mathfrak{O}_K[C_{p^2}]^*}(I_{\mathfrak{O}_K[C_{p^2}]^*})) = 0$. Now, by [**Und11**, Proposition 5.3.6], $\nu(\varepsilon_{A(\xi)}(I_{A(\xi)})) = 2p(p-1) - (p-1)(i+j)$, and so, $2p(p-1) = (p-1)(i+j)$. Thus, $2p = i + j$. However, by the bounds on i, j, we have $1 + p \ge 2p$, which is impossible. Thus $A(\xi) \ne \mathfrak{O}_K[C_{p^2}]^*$. □

REMARK 12.33. As we will see in Section 12.6, the non-Larson Hopf order $\mathfrak{O}_K[C_{p^2}]^*$ in $K[C_{p^2}]$ is the dual of the Greither order $A(0,0,1) = H(0,0)$ and has the form $\mathfrak{O}_K[C_{p^2}]^* = A(e', e', \zeta_{p^2}^{-1})$. Thus $\mathfrak{O}_K[C_{p^2}]^*$ is given by two valuation parameters e', e', and one unit parameter $v = \zeta_{p^2}^{-1}$. We have

$$\mathfrak{O}_K[C_{p^2}]^* = \mathfrak{O}_K\left[\frac{g^p - 1}{\pi^{e'}}, \frac{g a_v - 1}{\pi^{e'}}\right],$$

where a_v is an element of $K[\langle g^p\rangle]$ of the form

$$a_v = \sum_{m=0}^{p-1} v^m f_m, \quad v = \zeta_{p^2}^{-1},$$

with $f_m = \frac{1}{p}\sum_{i=0}^{p-1} \zeta_p^{-mi} g^{pi}$.

12.5. Hopf orders in $K[G]$, $G = C_p$

In this section, and until Section 12.13, we assume that K is a p-adic field.

Let g be a generator for C_p. Then a Larson order in $K[C_p]$ can be written as

$$H(i) = \mathfrak{O}_K\left[\frac{g-1}{\pi^i}\right],$$

where i is an integer $0 \le i \le e'$ (Proposition 12.25).

In this section we show that every Hopf order in $K[C_p]$ is of the form $H(i)$ for some integer i, $0 \le i \le e'$.