Hopf Galois extensions after 50 years

Lindsay N. Childs
University at Albany

Introduction

This is a biased survey of some results related to Hopf Galois structures on Galois extensions of fields.
They were first defined by Steve Chase and Moss Sweedler and published in 1969, 50 years ago.

Galois theory

Let K be a field, L be field containing K and has 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 G,

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

the fixed field of L under the action of G.

The Fundamental Theorem of Galois Theory is 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 and module theory

Galois theory dates from the 1830s, but it took over a century before E. Artin [Ar42] 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 ring $K[G]$.

Here is a condition for L/K to be a G-Galois extension:

- 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: the elements of G can be viewed as linear transformations on L, and every K-linear transformation on L can be written as a K-linear combination of elements of G.

One example of a purely module-theoretic result in Galois theory is the Normal Basis Theorem [Ar42, Theorem 28]: 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, $\{g(s)|g \in G\}$ is a K-basis of L.

This translates to: L is a free KG-module of rank one.

Linear duals

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

Let R be a commutative ring, M, N projective R-module of finite rank, and let $M^* = Hom_R(M, R)$, the linear dual of M.

If $f : M \to N$ is a R-module homomorphism, then f induces $f^* : N^* \to M^*$ by

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

for ϕ in N^*.

Bialgebras

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). We also assume that H has a comultiplication $\Delta : H \to H \otimes_R H$ and a counit map $\epsilon : H \to R$ so that the induced maps $\Delta^* : H^* \otimes_R H^* \to H^*$ and $\epsilon^* : R \to H^*$ make H^* into an R-algebra. In particular, Δ^* is associative, hence $\Delta : H \to H \otimes H$ is "coassociative".

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

Hopf algebras

A group ring RG also has a "coinverse" map, or "antipode" $s : RG \to RG$ 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: $m(1 \otimes s)\Delta(g) = 1 = i\epsilon(g)$.
Generalizing, a R-Hopf algebra H is a bialgebra with an antipode map s, that is, an antihomomorphism: $s : H \to H$ satisfying $m(1 \otimes s)\Delta(h) = 1 = i\epsilon(h)$ for all h in H.

Hopf Galois extensions

Back to L/K a field extension. 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, a, b in L. This idea generalizes to the concept that if L is an H-module, then L is an H-module algebra if

$$h(ab) = m(\Delta(h)(a \otimes b)), \quad h(1) = \epsilon(h) \cdot 1.$$

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

- 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, g in G, is an isomorphism of K-vector spaces.

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"

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

Then $dim_K J = dim_{(L^J)} L$.
The Galois correspondence is one-to one, but, in contrast to classical Galois theory, C-S could not show onto (because it is usually not true).

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". It seems to have more potential in the latter than the former, as we'll see. But the theory does apply to purely inseparable extensions: see [Koc14].

Ramification

A global field 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 $\mathfrak{O}$, 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.

Local fields

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 called 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 Normal Basis Theorem is the paradigm for Galois module theory. If L/K is a Galois extension of fields with Galois group G, then L is a free KG-module of rank 1. It goes back at least to Hilbert (1897). The first important result in local Galois module theory was by Emmy Noether [No31]: 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 is very difficult, as Elder can attest, and the results are not so elegant.

Associated orders

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

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

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 the idea is to try to understand $\mathfrak{O}_L$ as an $\mathfrak{A}_G$-module.

Some results

The earliest result was a global result by Leopoldt [Le59]: if L is an abelian Galois extension of $K = \mathbb{Q}$, then $\mathfrak{O}_L$ is a free module of rank one as an $\mathfrak{A}_G$-module. But that result is not valid if one omits "abelian" or "$K = \mathbb{Q}$".

In [CH86] Hurley and I 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 KG, 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 $\mathfrak{A}_G$ replaced by the associated order $\mathfrak{A}_H$ in H.

Byott's examples

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. Nigel Byott [By00], [By02], obtained examples where the associated order $\mathfrak{A}_H$ is an $\mathfrak{O}_K$-Hopf order and $\mathfrak{O}_L$ 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. I suspect he may describe some of this work in his talk. (His 20th century examples were a major motivation for writing [Ch00].)

Some directions in local Galois module theory

These results have motivated research in several directions in local Galois module theory:

I. Hopf orders

One is to try to understand the structure of Hopf orders $\mathfrak{A}_H$, especially when $H = KG$. This subject began with work of Tate and Oort in 1970 when G has order p and Raynaud in 1974 for elementary abelian p-groups. The case where G has order p^2 was completed by Greither [Gr92], Byott [By93] and Underwood [Un94]. But the case for G of order p^n, $n > 2$ has remained wide open despite a lot of effort, especially by Underwood, with contributions by Sauerberg, Zimmermann, Greither, Smith, Koch, Elder, Byott, Tossici and me. Underwood, Elder, and Tossici and his collaborators continue to work on this problem. Underwood's talk on Friday will discuss this problem for $n = 3$, and Truman's talk will relate to this topic.

II. Structure of associated orders

Another is to try to determine a general structure of associated orders $\mathfrak{A}_H$ in H (where $\mathfrak{A}$ is not necessarily a Hopf order) that would permit a determination of whether or not $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$, especially but not exclusively when $H = KG$. This effort has led to the scaffold theory of Elder and Byott, (see [BCE18]) and to "semi-stable" extensions of Bondarko. The relationship between these theories has been illuminated in recent work of Keating, who will give talks on this subject today and Thursday.

III, Non-classical Hopf Galois structures

A third is to try to determine the possible non-classical Hopf Galois structures on a Galois extension L/K of fields. This is the direction I know best. It has few algebraic number-theoretic prerequisites, but rather ends up involving some deep group theory and some other surprising ideas. So for the rest of this talk I will focus on this topic. Byott's talk on Wednesday will be in this area.

The Galois case

For the rest of this talk I'll assume that any field extension L/K is Galois with Galois group G. The theory extends to not necessarily normal sub-extensions of Galois extensions, and there are a number of interesting results on this subject, starting with [GP87]–see also [Ch89], [By96], [Ko98] six papers within the past four years by Crespo and her Barcelona collaborators, and recent work of Truman. But in the interest of time, I'll omit that generalization.

Greither-Pareigis 1987

For L/K a G-Galois extension, [GP87] transformed the problem of finding Hopf Galois structures into a problem in finite permutation groups, namely: find regular subgroups N of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$, the image in $\mathrm{Perm}(G)$ of the left regular representation map, $\lambda(g)(g') = gg'$.
A subgroup N of $\mathrm{Perm}(S)$ is a regular subgroup if for every s, t in S there is a unique n in N so that $n(s) = t$. Thus $|N| = |S|$.

If N is also normalized by $\lambda(G)$, then for s_η in L, η in N,

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

is a K-Hopf algebra that acts on L and L/K is H-Hopf Galois. The type of H is the isomorphism type of the abstract group N.

First examples

For G a non-abelian group, there are always at least two regular subgroups of $\mathrm{Perm}(G)$, namely $\lambda(G)$ and $\rho(G)$, where $\rho : G \to \mathrm{Perm}(G)$ is the right regular representation: $\rho(g)(h) = hg^{-1}$. Then $\rho(G)$ is centralized by $\lambda(G)$, so corresponds to the classical Hopf Galois structure given by the Galois group. Not so for $\lambda(G)$.

The Galois correspondence

If L/K is a G-Galois extension and has an H-Hopf Galois structure, then the FTGT for the H-action sends K-subHopf algebras of H to intermediate fields of L/K. The K-subHopf algebras of H correspond to the subgroups N' of N that are normalized by $\lambda(G)$ [CRV16]. For example, for G non-abelian, $\lambda(G)$ is a regular subgroup of $\mathrm{Perm}(G)$, and the subgroups of $\lambda(G)$ that are normalized by $\lambda(G)$ are the subgroups $\lambda(N)$ where N is a normal subgroup of G. Thus the image of the Galois correspondence consists of subfields E so that E/K is a normal extension.

Translation to the holomorph

For a group G of fairly large order n, finding regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$ is not easy, because $\mathrm{Perm}(G) \cong S_n$ is large and has many subgroups. But [Ch89] observed that $\lambda(G)$ normalizes a regular subgroup N of $\mathrm{Perm}(G)$ if and only G is (isomorphic to) a subgroup of the holomorph $\mathrm{Hol}(N) = \lambda(N) \rtimes \mathrm{Aut}(N)$, the normalizer in $\mathrm{Perm}(N)$ of $\lambda(N)$. Byott, in [By96], took that observation and turned it into a systematic way of counting Hopf Galois structures of type N on a G-Galois extension L/K by counting equivalence classes of regular homomorphisms from G into $\mathrm{Hol}(N)$. Since Byott's work, nearly all of the results on the existence or non-existence of Hopf Galois structures have used the holomorph.

Working in $\mathrm{Perm}(G)$

The main exceptions to using the holomorph method are some results of Crespo, Rio and Vela and their students, and work of Kohl.
Kohl [Ko98] completely classified the Hopf Galois structures on a separable extension of odd prime power degree p^n. In particular, he showed that if L/K is Galois with Galois group G cyclic of order p^n, then every Hopf Galois structure on L/K has type G. He originally did this within the Greither-Pareigis framework, but it is more routinely done using the holomorph method: Byott proved [By96] that if N is a non-cyclic group of order p^n, then $\mathrm{Hol}(N)$ has no element of order p^n, so there can be no regular embedding of a cyclic group G of order p^n in $\mathrm{Hol}(N)$ for N non-cyclic of order p^n.

A converse to Kohl's result

In [CS16], Crespo and Salguero proved a converse. Suppose L/K is Galois with Galois group G of order p^n, and has a Hopf Galois structure of type N where $N \cong C_{p^n}$ is cyclic. Then G must be cyclic.

The heart of their proof is to show that every regular subgroup of $\mathrm{Hol}(C_{p^n})$ must contain an element of order p^n. Having done so, the proof proceeds as follows. Suppose G is any group of order p^n. If L/K has a Hopf Galois structure of type C_{p^n}, then there must be a regular embedding β of G into $\mathrm{Hol}(C_{p^n})$. Hence $\beta(G) \cong G$ of order p^n is a regular subgroup of $\mathrm{Hol}(C_{p^n})$, and so must have an element of order p^n. Hence G must be cyclic.

recent work of Kohl

Before leaving the $\mathrm{Perm}(G)$ setting, I want to talk about a neat result of Kohl from last year [Ko18].

Theorem

Suppose L/K is Galois with Galois group G of order n. Suppose G has no subgroup of order m. Let N be a group of order n, and suppose N has a characteristic subgroup of order m. Then L/K cannot have a Hopf Galois structure of type N.

Why?

Here is the idea. Suppose L/K has a Hopf Galois structure corresponding to a subgroup M of $\mathrm{Perm}(G)$ of type N. Then the FTGT for the Hopf Galois structure gives a one-to-one correspondence from subgroups M_1 of M that are normalized by $\lambda(G)$ in $\mathrm{Perm}(G)$ to intermediate fields E with $K \subseteq E \subseteq L$, by sending M_1 to the corresponding K-subHopf algebra $H_1 = LM_1^G$, then to the corresponding fixed field $E = L^{H_1}$. Furthermore, $|M_1| = [L : E]$.
If N has a characteristic subgroup of order m, then $M \cong N$ has a characteristic subgroup M_1 of order m, and so any automorphism of M restricts to an automorphism of M_1. In particular, M_1 is normalized by $\lambda(G)$. So by the FTGT for Hopf Galois structures, there is an intermediate subfield E with $[L : E] = m$.

But if L/K is G-Galois and G has no subgroups of order m, then by the classical FTGT, there are no subfields E with $[L : E] = m$. So L/K can't have a Hopf Galois structure of type M.

Examples?

A class of examples:

Theorem

Suppose G is a group of order n and for some m dividing n, G has no subgroup of order m. Then a G-Galois extension cannot have a Hopf Galois structure of cyclic type.

This is because every subgroup of a cyclic group is a characteristic subgroup.
There are examples! Let $G = A_n$ for $n \geq 4$. Then G has no subgroups of index 2.

The result generalizes easily: if for some m dividing $|G| = |N|$, the number of characteristic subgroups of N of order m is larger than the number of subgroups of G of order m, then a Galois extension with Galois group G can have no Hopf Galois structures of type N.

Using the holomorph

As noted, many of the deepest results on the existence or non-existence of Hopf Galois structures on Galois extensions of fields use the holomorph.
Here are some examples.

Byott's simple groups theorem

[By04] showed that if L/K is Galois with Galois group G a non-abelian simple group, then any Hopf Galois structure must have type G. Combining that with an earlier result [CC99], his result shows that there are exactly two Hopf Galois structures on L/K.

His proof used the classification of finite simple groups to show that there is no regular embedding of a simple group G into the holomorph of a group of order $|G|$ that is not isomorphic to G.

Fixed point free pairs of homomorphisms

In [BC12] we introduced the idea of constructing Hopf Galois structures by the method of fixed point free pairs of homomorphisms. In its most general setting, let $G = G_L G_R$ be a group with complementary subgroups: this means, every element g of G has a unique decomposition as $g = g_L g_R$ with g_L in G_L, g_R in G_R. (G is a "Zappa-Szep product".) Then there is a regular embedding

$$G_L \times G_R \to \mathrm{Hol}(G) = \lambda(G) \rtimes \mathrm{Aut}(G)$$

by $g \mapsto \lambda(g_L)\rho(g_R)$ where $\lambda(g_L)\rho(g_R)(x) = g_L x g_R^{-1}$.
Thus fixed point free pairs of homomorphisms yield Hopf Galois structures of type G on a Galois extension with Galois group $G_L \times G_R$. In particular, it shows that given a semi-direct product $H \rtimes J$ of groups, then a Galois extension with Galois group $H \times J$ has a Hopf Galois structure of type $H \rtimes J$.

Application to non-abelian Hopf Galois structures

As an example, [BC12] applied that idea to show that if G is any non-cyclic abelian group of order p^n, $n \geq 3$, $p \geq 3$, then a G-Galois extension of fields has a Hopf Galois structure of non-abelian type.

The idea also lies behind [AB18]'s complete description of Hopf Galois structures on a Galois extension L/K with Galois group cyclic of square-free order n. If N is any group of order n, then N is a semidirect product of cyclic groups. Thus:

Theorem

If L/K is Galois with Galois group G cyclic of square-free order n, then every group of order n can be the type of a Hopf Galois structure on L/K.

This is in sharp contrast to the cyclic of prime power order case.

Composition factors

In [By15] Byott used the method of fixed point free pairs of homomorphisms to find examples of G-Galois extensions L/K that have Hopf Galois structures of type N where G and N have different composition factors.
An example is to let $N = S_n$ for $n = 5$, let $H = S_{n-1}$, the stabilizer of a point, and let J be the cyclic group generated by any n-cycle in S_n. Then H and J are complementary subgroups in S_n. Thus any Galois extension with group $G = S_{n-1} \times C_n$ admits a Hopf Galois structure of type S_n. Since $n = 5$, S_n has the simple group A_n as a composition factor, while G does not.

Abelian Galois extensions have only Hopf Galois structures of solvable type

Among the most sophisticated applications of the holomorph approach thus far are in [By15]: Let L/K be a G-Galois extension of fields where G is abelian. Then any Hopf Galois structure on L/K is of type N where N is solvable.
One of his two proofs used the classification of finite simple groups.
The other applies a result of Li used in the solution of a 100 year old problem of Burnside in permutation groups.
Byott's talk on Wednesday may set a new standard of sophistication?

Extending Kohl's result for cyclic of order p^n

Finally, we note a theorem of Featherstonhaugh [FCC12], namely: let G be a finite abelian group of p-rank m. If L/K is Galois with Galois group G and $m+1 < p$, then any abelian Hopf Galois structure must have type G. This generalizes the abelian part of Kohl's result for cyclic p-groups.
The inequality on m and p is necessary: see [Ch07].
The proof in [FCC12] used a result of Caranti [CVDS06] that if N is a finite abelian p-group, written additively, then every regular subgroup of $Hol(N)$ is isomorphic to the group $(N, \circ)$ induced from a structure $(N, +, \cdot)$ of a commutative, associative nilpotent ring on the additive group $(N, +)$, where $a \circ b = a + b + a \cdot b$.
That result was prescient.

Meanwhile ...

Braces

In 2007, W. Rump [Ru07] defined a left brace to be a set G with two group operations, $(G, +)$ and $(G, \circ)$ where $(G, +)$ is abelian, that satisfy the single compatibility condition

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

for all a, b, c in G. Given a left brace, one gets a solution of the Yang-Baxter equation. See Nejabati Zenouz's talk on Tuesday for more on this connection?

Radical rings

A radical ring is a finite ring $A(+,\cdot)$ with the property that if the operation $\circ$ is defined on A by $a \circ b = a + b + a \cdot b$, then $(A, \circ)$ is a group. Then the two groups $(A, +)$ and $(A, \circ)$ have a common identity, 0, and the set $A(\circ, +)$ is a left brace.

Examples are easy to find: for example, let x, y, z, u, v, w be a basis for A as a vector space over $\mathbb{F}_p$, define $xy = u, yz = v, zx = w$ and all other products of the generators $= 0$. Then $A^3 = 0$ and defining $a \circ b = a + b + ab$, the $\circ$-inverse $\overline{a}$ of a is $-a + a^2$.

But there are left braces that do not arise from radical rings.

skew braces

Skew braces were introduced in [GV17] as a non-commutative generalization of the left braces of [Rum07]. Skew braces also yield set-theoretic solutions of the Yang-Baxter equation.
But there is also a close connection between skew braces and Hopf Galois structures on Galois extensions of fields.

- [CDVS06] found a relationship between abelian radical $\mathbb{F}_p$-algebras and regular subgroups of the affine group = the holomorph of $(\mathbb{F}_p^n, +)$.
- This was generalized to abelian radical rings and used in [FCC12].
- Bachiller in [Bac16] extended the connection in [FCC12] to a connection between abelian Hopf Galois structures on Galois extensions of fields and left braces.
- That relationship was further extended to skew braces and arbitrary Hopf Galois structures by Byott and Vendramin in [SV18].

Skew braces have already been used to study Hopf Galois structures, for example in [Ze18], [Ch18] and [Ch19].

Regular representation maps

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 Guarneri and Vendramin [GV17, Proposition 1.9] showed:

Theorem

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

Connecting skew braces with Hopf Galois structures

Let L/K be a Galois extension with Galois group $G = (G, \circ)$. Hopf Galois structures on L/K of a given type $(G, \star)$ correspond by Galois descent [GP87] to regular subgroups N of $\mathrm{Perm}(G)$ isomorphic to $(G, \star)$ and normalized by $\lambda_\circ G$.

Theorem

Let L/K be a Galois extension with group $G = (G, \circ)$. Let H be a K-Hopf algebra giving a Hopf Galois structure of type M on L/K. Then $(G, \circ)$ has a skew left brace structure with additive group $(G, \star) \cong M$.

The idea is that H corresponds to a regular subgroup N of $\mathrm{Perm}(G)$. So there is a bijection $b : N \to G$ by $n \mapsto n(e)$. This can be used to define a new group operation on G by $g \star h = b(b^{-1}(g)b^{-1}h))$. Then $(G, \circ, \star)$ is a skew brace by the G-V Theorem.

Conversely

Theorem

Let $(G, \circ, \star)$ be a skew brace. Let L/K be a Galois extension with Galois group $(G, \circ)$. Then L/K has a Hopf Galois structure of type $(G, \star)$.

Proof.

Given the skew brace structure $(G, \circ, \star)$ on the Galois group $(G, \circ)$ of L/K, we have by the G-V Theorem that $\lambda_\circ(G)$ is contained in $\mathrm{Hol}(G, \star)$, and so the subgroup $N = \lambda_\star(G) \subset \mathrm{Perm}(G)$ is normalized by $\lambda_\circ(G)$. Thus N corresponds by Greither-Pareigis theory to a Hopf Galois structure on L/K of type $(G, \star)$. □

Bachiller

Work on skew braces yields results on Hopf Galois structures.

For a notable example, [Bac16] found a group of order p^{10} and exponent p for $p > 12$ that is not the circle group of a brace with additive group an elementary abelian group of order p^{10}. That is equivalent to saying that there is a Galois extension with a Galois group of order p^{10} and exponent p that has no Hopf Galois structure of elementary abelian type.

One of Bachiller's tools was to extend [FCC12] to show that if $(B, \circ, +)$ is a left brace of order p^n where $n + 2 \leq p$, and $(B, +)$ is elementary abelian, then $(B, \circ)$ must be a group of exponent p.

Today

So this is an exciting time to be working on Hopf Galois structures. Vendramin posted a paper [Ven18] on arxiv.math in the summer of 2018 entitled “Problems on skew left braces” with a list of 50 problems. A dozen or so relate to the existence or classification of skew braces with additive and circle groups with various properties or sizes. And he hardly mentioned Hopf Galois structures. The paper has a list of 69 references.
So suddenly we find our research on Hopf Galois structures to be of interest to a much larger collection of mathematicians than we ever imagined two years ago.

Thank you!