LEFT SKEW BRACES AND THE GALOIS CORRESPONDENCE FOR HOPF GALOIS STRUCTURES OMAHA, MAY 2018

LINDSAY N. CHILDS

Introduction. This is the slightly edited text of the two talks I gave at the 2018 Omaha conference on Hopf Algebras and Galois Module Theory. The theory and some of the examples are also found in [Ch18].

The Fundamental Theorem of Galois Theory (FTGT). Let K/k be a Galois extension of fields with Galois group G. Then the Galois correspondence sending subgroups G' of G to subfields $K^{G'}$ of K containing k is, by the Fundamental Theorem of Galois Theory, a bijective correspondence from subgroups of G onto the intermediate fields between k and K.

In 1969 S. Chase and M. Sweedler [CS69] defined the concept of a Hopf Galois extension of fields for a field extension K/k and H a k-Hopf algebra acting on K as an H-module algebra. K/k is an H-Hopf Galois extension iff the map $K \otimes_k H \to End_k(K)$ is surjective.

They proved a weak version of the FTGT, namely, that there is an injective Galois correspondence from k-subHopf algebras H' of H to intermediate fields, given by $H' \mapsto K^{H'}$, the subfield of elements fixed under the action of H'.

But surjectivity could not be proved.

Greither-Pareigis. Greither and Pareigis [GP87] showed that each Hopf Galois structure on K/k with Galois group Γ corresponds to a unique regular subgroup N of $\text{Perm}(\Gamma)$ that is normalized by $\lambda(\Gamma)$, where $\lambda : \Gamma \to \text{Perm}(\Gamma)$ is the left regular representation, $\lambda(\gamma)(\delta) = \gamma\delta$. Then the k-Hopf algebra giving the Hopf Galois structure is $H = K[N]^{\lambda(\Gamma)}$ (Galois descent). As Crespo, et. al. [CRV16] showed in general, the sub-k-Hopf algebras of H are descended from group rings $K[M]$ where $M < N$ is normalized by $\lambda(G)$.

Date: May 29, 2018.

An example of non-surjectivity of the FTGT. Two examples of N are $\rho(\Gamma)$, the image of the right regular representation of Γ, and $\lambda(\Gamma)$ itself. When Γ is non-abelian, $\lambda(\Gamma)$ and $\rho(\Gamma)$ are different subgroups of $\mathrm{Perm}(G)$.

As [GP87] observed, $\rho(\Gamma)$ in $\mathrm{Perm}(\Gamma)$ is centralized by $\lambda(G)$, so $K[\rho(\Gamma)]$ descends to the classical Galois structure on K/k given by Γ. But for Γ non-abelian, the Hopf Galois structure is the canonical non-classical one given by H_λ. In that case the subgroups of $\lambda(\Gamma)$ normalized by $\lambda(G)$ are the normal subgroups of $\lambda(G)$. So for H_λ, the image of the Galois correspondence consists of the normal intermediate subfields of K/k.

Old news. In 2017 in Omaha I talked about a method to estimate the size of the image of the Galois correspondence for Galois extensions K/k when the Galois group Γ is an elementary abelian p-group and K/k has a Hopf Galois structure of type $G \cong \Gamma$.

The idea of [Ch17] is to associate to such a Hopf Galois structure a commutative nilpotent $\mathbb{F}_p$-algebra structure A on the additive group G. This yielded two interesting consequences:

1) If the Hopf Galois structure is not the classical structure, then the Galois correspondence is not surjective;

2) [CG18] For $G = \Gamma \cong (\mathbb{F}_p^n, +)$, $n \geq 3$, we found upper and lower bounds on the proportion of subspaces of the algebra A that are ideals of A. The bounds imply that for most examples, the image of the Galois correspondence contains less than one percent of the intermediate fields between k and K.

What's new this year. In this talk I want to generalize [Ch17] to [almost?] the most general setting possible, by replacing nilpotent $\mathbb{F}_p$-algebras by skew left braces. Skew left braces and their connection with Hopf Galois structures were introduced in [Bac16a] and [GV17] and studied by Nigel Byott in his 2017 Omaha talk and in [BV17]. (See also [Zen18]).

A skew left brace.

Definition. A finite group $(G, \star)$ is a skew left brace with "additive group" $(G, \star)$ if G has an additional group structure $(G, \circ)$ so that for all g, h, k in G,

$$g \circ (h \star k) = (g \circ h) \star g^{-1} \star (g \circ k).$$

Here g^{-1} is the inverse in $(G, \star)$. Let $\overline{g}$ be the inverse in $(G, \circ)$.

Given a skew left brace $(G, \star, \circ)$, the identities of the groups $(G, \star)$ and $(G, \circ)$ coincide.

If the additive group $(G, \star)$ of a skew left brace is abelian, $(G, \star, \circ)$ is a left brace, as defined by Rump [Rum07]

If A is a radical algebra, that is, an associative ring (without unit) $(A, +, \cdot)$ with the property that with the operation $a \circ b = a + b + a \cdot b$, $(A, \circ)$ is a group, then $(A, +, \circ)$ is a left brace. (Just take the two sides of the equation

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

and replace $a \circ x$ by $a + x + a \cdot x$.)

Left regular representations. Associated to a skew left brace $(G, \circ, \star)$ with additive group $(G, \star)$ are the two left regular representation maps:

$$\lambda_\star : G \to \mathrm{Perm}(G), \lambda_\star(g)(h) = g \star h,$$
$$\lambda_\circ : G \to \mathrm{Perm}(G), \lambda_\circ(g)(h) = g \circ h.$$

Hopf Galois structures and skew left braces. To see how Hopf Galois structures correspond to skew left braces, we start with the fact that each Hopf Galois structure on K/k corresponds to a unique regular subgroup N of $\mathrm{Perm}(\Gamma)$, normalized by $\lambda(\Gamma)$.

If G is a group of the same cardinality as Γ and $\alpha : G \to \mathrm{Perm}(\Gamma)$ is a one-to-one homomorphism with image N, we say that the Hopf Galois structure has type G.

α and β. Since $\alpha : G \to \mathrm{Perm}(\Gamma)$ is one-to-one and regular, the map $\alpha_* : G \to \Gamma$ by $\alpha_*(g) = \alpha(g)(e)$ is a bijection. (e is the identity of Γ.) Then α is recoverable from α_*:

$$\alpha(g)(\gamma) = \alpha_* \lambda_\star(g)(\alpha_*)^{-1}(\gamma).$$

Define $\beta : \Gamma \to \mathrm{Perm}(G)$ by

$$\beta(\gamma)(g) = (\alpha_*)^{-1} \lambda_\Gamma(\gamma) \alpha_*(g).$$

Then β is a regular embedding of Γ in $\mathrm{Perm}(G)$, and since $\alpha(G)$ is normalized by $\lambda(\Gamma)$, $\beta(\Gamma)$ normalizes $\lambda(G)$. Hence

$$\beta : \Gamma \to \mathrm{Hol}(G) \subset \mathrm{Perm}(G).$$

Let $\beta_* : \Gamma \to G$ by $\beta_*(\gamma) = \beta(\gamma)(e)$. Then $\beta_* = {\alpha_*}^{-1}$.

The $\circ$ operation on G. Define an operation $\circ$ on G from the operation on Γ via the bijection $\alpha_* : G \to \Gamma$ and its inverse β_*:

$$g \circ h = \beta_*(\alpha_*(g) \cdot \alpha_*(h)).$$

for g, h in G. Then

$$\alpha_*(g \circ h) = \alpha_*(g) \cdot \alpha_*(h),$$

so $\alpha_* : (G, \circ) \to (\Gamma, \cdot)$ is an isomorphism.

Then for γ in Γ, x in G,

$$\begin{aligned}\beta(\gamma)(x) &= (\beta_* \lambda(\gamma)\alpha_*)(x) \\ &= \beta_*(\gamma\alpha_*(x)) \\ &= \beta_*(\alpha_*(\beta_*(\gamma))\alpha_*(x)) \\ &= \beta_*(\gamma) \circ x.\end{aligned}$$

A Hopf Galois structure yields a left skew brace. To recapitulate, we started with K/k with Galois group Γ and a Hopf Galois structure of type G corresponding to the image $\alpha(G)$ of an embedding $\alpha : G \to \mathrm{Perm}(\Gamma)$. From that data we constructed the $\circ$ operation on G to make $(G, \circ)$ isomorphic (via $\beta_* = \alpha_*^{-1}$) to Γ.

We have

Theorem 0.1. *The group $(G, \star)$ with the additional group structure $(G, \circ)$ is a left skew brace with additive group $(G, \star)$.*

Proof that $(G, \circ, \star)$ is a skew left brace. Let $\beta : \Gamma \to \mathrm{Hol}(G) \cong \lambda_*(G) \rtimes \mathrm{Aut}(G, \star)$. Let $\beta(\gamma) = \beta_l(\gamma)\beta_r(\gamma)$ where $\beta_r(\gamma)$ is in $\mathrm{Aut}(G, \star)$ and $\beta_l(\gamma) = \lambda_\star(g)$ for some g in G. Then

$$\beta_*(\gamma) = \beta(\gamma)(e) = \lambda_\star(g)\beta_r(\gamma)(e) = \lambda_\star(g)(e) = g$$

since $\beta_r : \Gamma \to \mathrm{Aut}(G, \star)$. Thus

$$\beta(\gamma)(x) = \beta_*(\gamma) \circ x = g \circ x.$$

Also,

$$\beta_r(\gamma)(x \star y) = \beta_r(\gamma)(x) \star \beta_r(\gamma)(y).$$

Then $\beta_r(\gamma) = \lambda_\star(g)^{-1}\beta(\gamma)$, so replacing $\beta_r(\gamma)$ in the previous equation yields

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

which reduces to the defining equation for a skew left brace:

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

Defining $\circ$-stable subgroups. Given a Galois extension L/K with Galois group Γ, a skew left brace $(G, \star, \circ)$ and an isomorphism $\alpha_* : (G, \circ) \to \Gamma$, there is a H-Hopf Galois structure on L/K of type $(G, \star)$. To study the image of the Galois correspondence for H, we define some subgroups of $(G, \star)$.

Definition. A subgroup $(G', \star)$ of a skew left brace $(G, \star, \circ)$ is $\circ$-stable ("circle-stable") if $\lambda_\star(G')$ is closed under conjugation in $\mathrm{Perm}(G)$ by $\lambda_\circ(g)$ for all g in G.

An easier criterion for $\circ$-stability.

Theorem 0.2. *$\circ$-stability of G' is equivalent to: for all g in G, g' in G', there is an element h' in G' so that*

$$(g \circ g') = h' \star g.$$

For suppose for all g in G and g' in G' there is some h' in G' so that

$$\lambda_\circ(g)\lambda_\star(g') = \lambda_\star(h')\lambda_\circ(g).$$

Then for all x in G, $g \circ (g' \star x)) = h' \star (g \circ x)$. Applying the defining equation for a skew left brace yields

$$(g \circ g') \star g^{-1} \star (g \circ x) = h' \star (g \circ x).$$

Hence $(g \circ g') \star g^{-1} = h'$.

On $\circ$-stable subgroups of $(G, \star)$.

Theorem 0.3. *A $\circ$-stable subgroup of $(G', \star)$ is also a subgroup of $(G, \circ)$*

For if G' is a $\circ$-stable subgroup of $(G, *)$, then, in particular, for all g, g' in G', there is an h' in G' so that $g \circ g' = h' \star g$, and $h' \star g$ is in G'. So G' is closed under the operation $\circ$.

It is routine to check that if a skew left brace is a radical algebra with induced operation $\circ$, then a subgroup $(G', +)$ of G is a $\circ$-stable subgroup of $(G, +)$ if and only if G' is a left ideal of the algebra.

Main result.

Theorem 0.4. *Let $(G, \star, \circ)$ be a skew left brace. Let $\beta_* : \Gamma \to (G, \circ)$ be an isomorphism of groups and K/k be a Galois extension with Galois group Γ. Then for the unique H-Hopf Galois structure on K/k of type $(G, \star)$ corresponding to the isomorphism β_*, there is a bijection between the k-subHopf algebras of H and the $\circ$-stable subgroups G' of $(G, \star)$.*

Why is the main result true? Given a $\circ$-stable subgroup G' and the $\circ$-stable equation for all g, x in G, g', h' in G',

$$g \circ (g' \star x) = h' \star (g \circ x),$$

let $\alpha_*(g) = \gamma$. Then for all x in G

$$\beta_*(\gamma) \circ \lambda_\star(g')(x) = \lambda_\star(h')(\beta_*(\gamma) \circ x),$$

so

$$\beta(\gamma)\lambda_\star(g') = \lambda_\star(h')\beta(\gamma)$$

Conjugating each term in this last equation by α_* gives

$$\lambda_\star(\gamma)\alpha(g') = \alpha(h')\lambda_\star(\gamma).$$

Thus the condition for G' to be $\circ$-stable translates into the condition that $\alpha(G')$ is a $\lambda_\star(\Gamma)$-stable subgroup of $\alpha(G)$.

So it's entirely a formal consequence of the relationships among α, β and the circle operation.

As good as Galois? To find the image of the Galois correspondence for H directly, we would need to find the $\lambda(\Gamma)$-invariant subgroups of the subgroup N of Perm(G) corresponding to H. Our result says we just need to understand the left skew brace structure on the group G itself, and G is usually much smaller than Perm(G).

It's somewhat analogous to Galois' original result:

- Galois: to determine the intermediate fields between k and K, just work inside the Galois group G of the field extension to find the subgroups of G .
- This result: to determine the intermediate fields between k and K in the image of the Galois correspondence for the Hopf Galois structure associated to a skew left brace structure on the Galois group G, just work inside G and find the $\circ$-stable subgroups of G, a collection of subsets that are subgroups of both $(G, \star)$ and $(G, \circ)$.

Specializing to the classical case. I'd like to say that the left skew brace with $\circ = \star$ corresponds to the classical Hopf Galois case $H = k\Gamma$. That would suggest that our result is a perfect generalization of Galois' result.

But it's not quite true. If we specialize to $\Gamma = G$ and $H = kG$, then $\alpha = \rho$ and $\alpha_*(g) = g^{-1} = \beta_*(g)$. To determine $\circ$ on G, for g, h in $G = \Gamma$, we have

$$g \circ h = \beta_*(\alpha_*(g) \star \alpha_*(h)) = \beta_*(g^{-1} \star h^{-1}) = \beta_*((h \star g)^{-1}) = h \star g.$$

So a subgroup G' is $\circ$-stable if for all g in G, g' in G', there is h' in G' so that $g \circ g' = h' \star g$, or $g' \star g = h' \star g$, which is true with $g' = h'$ for all g in G. So every subgroup of G is $\circ$-stable, as should be the case.

Should $(G, \star, \circ)$ where $g \circ h = h \star g$ be viewed as the trivial left skew brace, instead of the one where $g \circ h = g \star h$??

Examples. The rest of these notes are devoted to examples.

First we look at two examples where we begin with special cases of skew left braces: one involving a non-commutative radical algebra, one involving an example of a left brace of Rump.

A nilpotent non-commutative degree 3 $\mathbb{F}_p$-algebra. Let K/k be a Galois extension of fields with Galois group $\Gamma = H_3(\mathbb{F}_p)$, the Heisenberg group of order p^3, isomorphic to the group of 3×3 upper triangular matrices in $\mathrm{M}_3(\mathbb{F}_p)$ with diagonal entries all equal to 1. There is a radical algebra $A = A_{3,5} = \langle x, y\rangle$ with $(A, +) \cong (\mathbb{F}_p^3, +)$, generated as an $\mathbb{F}_p$-module by elements x, y, z where $xy = z, yx = -z$ and all other products among the basis elements are zero. (The notation $A_{3,5}$ is from De Graaf [DeG17].) Then A is a group under the operation $\circ$, defined by $u \circ v = u + v + uv$, and the group $(A, \circ)$ is isomorphic to Γ. This yields a left skew brace structure on $G = (A, +)$. In this case the $\circ$-stable subgroups of $(A, +)$ are the left ideals of the algebra A.

Some tedious but routine computations (in [Ch18]) yield:

Theorem 0.5. *The Heisenberg group $H_3(\mathbb{F}_p)$ has $2p^2+2p+4$ subgroups. The algebra $A = A_{3,5}$ has $p + 4$ left ideals.*

The same result holds for the De Graaf algebras $A_{3,4}$–the circle group of these is also isomorphic to the Heisenberg group.

A left brace of Rump. Example 2 of [Rum07] is a left brace $A = (A, +, \circ)$ with additive group $(A, +)$ isomorphic to $(\mathbb{F}_2^3, +) \cong C_2^3$ and circle group $(A, \circ)$ isomorphic to the dihedral group D_4. Thus if L/K is a Galois extension with Galois group Γ isomorphic to D_4, then corresponding to the brace A is a H-Hopf Galois structure on L/K where the K-Hopf algebra H is of elementary abelian type: that is, $L\otimes_K H = LN$ where $N \cong C_2^3 \cong (\mathbb{F}_2^3.+)$. The brace A is not a ring, as Rump notes. For this example, more routine but somewhat fussy computations, found in [Ch18], yield:

Theorem 0.6. *The group $(A, \circ) \cong D_4$ has ten subgroups, of which three are $\circ$-stable subgroups of A.*

Starting with a Hopf Galois structure. Hopf Galois structures have most often been found in practice by finding regular embeddings β of the Galois group Γ of L/K into $\mathrm{Hol}(G)$ for G a group of the same order as Γ. Each such $\beta : \Gamma \to \mathrm{Hol}(G)$ yields a unique Hopf Galois structure on L/K of type G.

To understand the Galois correspondence for such Hopf Galois structures involves two steps:

I. Determine the circle operation corresponding to β that makes G into a skew left brace.

II. Find the $\circ$-stable subgroups of the additive group $(G, \star)$ of the skew left brace G. They are among the subgroups of $(G, \circ)$.

To decide whether the Galois correspondence is surjective for the Hopf Galois structure, we then compare the number of $\circ$-stable subgroups of $(G, \circ)$ to the total number of subgroups of $(G, \circ)$. (Of course, the number of subgroups of $(G, \circ)$ may itself be a non-trivial problem.)

0.1. **Fixed point free pairs.** We focus on Galois extensions L/K with Galois group Γ where the Hopf Galois extension arises from a fixed point free pair of homomorphisms from Γ to G. ($|\Gamma| = |G|$.)

Two homomorphisms $f, g : \Gamma \to G$ form a fixed point free pair (f, g) iff for all γ in Γ, $f(\gamma) = g(\gamma)$ only for $\gamma = e$, the identity of Γ. So if we set

$$\beta : \Gamma \to \mathrm{Hol}(G)$$

by $\beta(\gamma) = \lambda(f(\gamma))\rho(g(\gamma))$, then $\beta_*(\gamma) = f(\gamma)g(\gamma)^{-1}$ is a bijection from Γ onto G, and β is a regular embedding of Γ into $\mathrm{Hol}(G)$.

Fixed point free pairs and $\mathrm{InHol}(G)$**.** We have:

Proposition 0.7. *For groups Γ, G of the same cardinality, $\beta : \Gamma \to \mathrm{Hol}(G)$ arises from a fixed point free pair of homomorphisms $\Gamma \to G$ if and only if β maps into $\mathrm{InHol}(G) \cong G \rtimes \mathrm{Inn}(G)$, where $\mathrm{Inn}(G)$ is the group of inner automorphisms of G.*

Proof. Suppose $\beta(\gamma) = \lambda(f_1(\gamma))\rho(f_2(\gamma)$ for $f_1, f_2 : \Gamma \to G$ a pair of fixed point free homomorphisms. Then

$$\begin{aligned}\beta(\gamma) &= \lambda(f_1(\gamma)f_2(\gamma)^{-1})\lambda(f_2(\gamma))\rho(f_2(\gamma) \\ &= \lambda(f_1(\gamma)f_2(\gamma^{-1})C(g(\gamma))\end{aligned}$$

has image in $\mathrm{InHol}(G)$, and

$$\beta_*(\gamma) = f_1(\gamma)f_2(\gamma^{-1})$$

is a bijective map from Γ to G. The converse is similar. ☐

Some past results. Hopf Galois extensions of this kind have been studied in at least six papers since 1999, yielding results such as:

• If L/K is Galois with non-abelian simple group Γ, then there are exactly two Hopf Galois structures on L/K of type $G \cong \Gamma$. [CaC99]

• If Γ is an abelian non-cyclic Galois group Γ of odd order p^n, p prime, $n \geq 3$, then every Galois extension L/K with Galois group Γ admits a Hopf Galois structure whose type G is a non-abelian group. [BC12]

• There exists a Galois extension with Galois group Γ admitting a Hopf Galois structure of type G where Γ and G do not have the same composition factors. [By15]

Examples involving complementary subgroups. We look at a class of examples of Hopf Galois structures arising from a group with complementary subgroups.

Let G be a finite group with two subgroups G_l and G_r so that $|G_l||G_r| = |G|$ and $G_l \cap G_r = e$. The subgroups G_l and G_r are called complementary in G in Section 7 of [By15]. Then the two obvious projection-inclusion maps from $\Gamma = G_l \times G_r$ to G form a fixed point free pair of maps from Γ to G.

Theorem 0.8. *Let G be a group with complementary subgroups G_l and G_r. Let $\Gamma = G_l \times G_r$, and define $\beta : \Gamma \to \mathrm{Hol}(G)$ by*

$$\beta((g_l, g_r)(\gamma) = \lambda(g_l)\rho(g_r)(\gamma) = g_l\gamma g_r^{-1}$$

in $\mathrm{Hol}(G)$. Then the $\circ$-stable subgroups of G are the subgroups of G that are normalized by G_l.

The proof: finding the left skew brace structure on G. First note that $\beta_*(g_l, g_r) = g_l g_r^{-1}$, so $\alpha_*(g_l g_r) = (g_l, g_r^{-1})$. So for g, h in G,

$$\begin{aligned} g \circ h &= \beta_*(\alpha_*(g)\alpha_*(h)) = \beta_*((g_l, g_r^{-1})(h_l, h_r)^{-1}) \\ &= \beta_*((g_l h_l, g_r^{-1} h_r^{-1}) = \beta_*((g_l h_l, (h_r g_r)^{-1}) \\ &= g_l h_l h_r g_r = g_l h g_r. \end{aligned}$$

This defines a skew left brace structure on G (where the additive group $(G, \star)$ is G with the given operation).

Finding the $\circ$-stable subgroups. Let G' be a subgroup of $G = G_l G_r$. Then G' is $\circ$-stable if for all x in G' and all $g = g_l g_r$ in G, there exists y in G' so that $g \circ x = yg$. This is true if and only if $g_l x g_r = y g_l g_r$, if and only if

$$y = g_l x g_l^{-1} = C(g_l)x.$$

So the $\circ$-stable subgroups G' are the subgroups closed under conjugation by elements of G_l.

That completes the proof.

"exact factorization". In [SV17], the paper that contains the appendix [BV17] that Byott spoke about in Omaha-17, the left skew brace just described is called the skew brace on G arising from the exact factorization of G into H and K.

Simple examples. Here is a class of examples.

Theorem 0.9. *Let $\Gamma = A \times \Delta$ and $G = A \rtimes \Delta$ where A is simple. Let G' be a $\circ$-stable subgroup of G and suppose there exists some x in G' and a in A so that $a^{-1}xa \neq x$. Then $A \subseteq G'$.*

Proof: We find the G' normalized by A. Suppose x is in G' and a is in A with $a^{-1}xa \neq x$. Then $a' = a^{-1}xax^{-1} \neq 1$ and is in A because A is normal in G. So $G' \cap A$ is a non-trivial subgroup of A and is normalized by A. Since A is simple, $G' \cap A = A$.

Regarding the hypothesis $a^{-1}xa \neq x$. The hypothesis that conjugation by elements of A is non-trivial on G' is necessary. Let

$$\Gamma = A \times \mathrm{Inn}(A), \quad G = A \rtimes \mathrm{Inn}(A) = \{[a, C(s)] : a, s \in A\}.$$

Then $G' = \{[a, C(a^{-1})] : a \in A\}$ is a $\circ$-stable subgroup of G.

An application of the last theorem. Let $G = Z_p \rtimes \Delta$ where Δ is a non-trivial subgroup of $Z_p^\times$. Then the $\circ$-stable subgroups of G are (1) and the subgroups of G containing Z_p.

To see this, let $Z_p = \langle a \rangle$ (written multiplicatively) and let $G = \langle a, \delta : a^p = \delta^k = 1, \delta a = a^b\delta \rangle$ where the order of δ in the group U_p of units modulo p is $k > 1$. If $g = a^r\delta^s$ is in G' with $\delta^s \neq 1$ (so $1 \leq s < k$), then one sees easily that g is not fixed under conjugation by a^{-1}, and so $C(a^{-1})(g)g^{-1}$ is a non-trivial element of $G' \cap Z_p$. Thus G' contains Z_p. Conversely, if G' is a subgroup of G containing Z_p, then clearly G' is closed under conjugation by elements of Z_p, so is $\circ$-stable.

An example of Byott. Let $G = S_n = A_n \rtimes Z_2$ and $\Gamma = A_n \times Z_2$, where A_n, S_n is the alternating, resp. symmetric group and $n \geq 5$. Then the only $\circ$-stable subgroups of G are $(1), A_n$ and S_n.

To see this, let G' be a non-trivial $\circ$-stable subgroup of G. It suffices to show that $G' \cap A_n$ is non-trivial. Let $\tau \neq 1 \in G'$.

If τ is even, then $G' \cap A_n$ is non-trivial.

If $a\tau a^{-1} \neq \tau$ for some a in A_n, then $a\tau a^{-1}\tau^{-1} \neq 1$ and is even, so $G' \cap A_n$ is non-trivial.

So suppose τ is odd, and $a\tau a^{-1} = \tau$ for all a in A_n. Since τ is odd, every odd b in S_n has the form $b = a\tau$ for some a in A_n. Then $b\tau b^{-1} = \tau$ for all b in S_n, so τ is in the center of S_n, impossible. So G' must contain A_n.

Another Heisenberg example. Let $\Gamma = \mathbb{F}_p^3$ and let

$$G = (\mathbb{F}_p^3, \star) \cong \mathrm{Heis}_3(\mathbb{F}_p) = \{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \subset \mathrm{GL}_3(\mathbb{F}_p)\} \cong \{ \begin{pmatrix} a \\ b \\ c \end{pmatrix} \in \mathbb{F}_p^3\}.$$

The multiplication on vectors in $\mathbb{F}_p^3$ corresponding to that in $\mathrm{Heis}_3(\mathbb{F}_p)$ is

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \star \begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} = \begin{pmatrix} a + a' \\ b + b' \\ c + c' + ab' \end{pmatrix}.$$

Define $f_l, f_r : \mathbb{F}_p^2 \times \mathbb{F}_p \to \mathrm{Heis}_3(\mathbb{F}_p)$ by

$$f_l((a, b, c)) = \lambda(\begin{pmatrix} 0 \\ b \\ c \end{pmatrix}),$$

$$f_r((a, b, c) = \rho(\begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix})].$$

Then (f_l, f_r) is a fixed point free pair of homomorphisms, hence makes $A = \mathbb{F}_p^3$ into a skew left brace $(A, \star, \circ)$ with $(A, \star) \cong \mathrm{Heis}_3(\mathbb{F}_p)$ (the additive group), and $(A, \circ) \cong (\mathbb{F}_p^3, +)$.

Theorem 0.10. *There are $2p + 4$ $\circ$-stable subgroups of $(A, \star, \circ)$.*

Proof: Given a subgroup G' of $G = (A, \star)$ we see if for all $h = (r, s, t)^T$ in G', $g = g_l \star g_r$ in G, it is true that $g_l \star h \star g_l^{-1}$ is in G'.

For $g = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$, $g_l = \begin{pmatrix} 0 \\ b \\ c \end{pmatrix}$, so

$$g_l \star h \star g_l^{-1} = \begin{pmatrix} 0 \\ b \\ c \end{pmatrix} \star \begin{pmatrix} r \\ s \\ t \end{pmatrix} \star \begin{pmatrix} 0 \\ -b \\ -c \end{pmatrix} = \begin{pmatrix} r \\ s \\ t - rb \end{pmatrix}.$$

So a subgroup G' of $(G, \star)$ is $\circ$-stable if and only if for all b in $\mathbb{F}_p$,

$$\text{if } \begin{pmatrix} r \\ s \\ t \end{pmatrix} \text{ is in } G', \text{ then } \begin{pmatrix} r \\ s \\ t - rb \end{pmatrix} \text{ is in } G'.$$

The subgroups of the Heisenberg group. Since G' is a subgroup of $(G, \circ) = (\mathbb{F}_p^3, +)$, if $r \neq 0$, then G' must contain $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.

The subgroups of $\mathrm{Heis}_3(\mathbb{F}_p) = (\mathbb{F}_p^3, \star)$ are $\langle 0 \rangle$, $\mathrm{Heis}_3(\mathbb{F}_p)$ and

$$\langle\begin{pmatrix}1\\b\\c\end{pmatrix}\rangle,\langle\begin{pmatrix}1\\0\\c\end{pmatrix},\begin{pmatrix}0\\1\\c'\end{pmatrix}\rangle,\langle\begin{pmatrix}0\\1\\c\end{pmatrix}\rangle;\ \langle\begin{pmatrix}0\\0\\1\end{pmatrix}\rangle,\langle\begin{pmatrix}1\\c\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\end{pmatrix}\rangle,\langle\begin{pmatrix}0\\1\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\end{pmatrix}\rangle.$$

The $\circ$-stable subgroups. Of these, the $2p+4$ $\circ$-stable subgroups of $(G,\star) = \mathrm{Heis}_3(\mathbb{F}_p)$ are $\langle 0\rangle$, $\mathrm{Heis}_3(\mathbb{F}_p)$ and the last four listed subgroups.

This implies that if the left skew brace $(\mathbb{F}_p^3,\star,\circ)$ corresponds to a H-Hopf Galois structure of type $\mathrm{Heis}_3(\mathbb{F}_p)$ on a Galois extension L/K with Galois group $\Gamma \cong \mathbb{F}_p^3$, then the number of intermediate fields = number of subgroups of $\mathbb{F}_p^3 = 2p^2+2p+4$, while the number of fields in the image of the Galois correspondence for H is $2p+4$.

Twisted versions of semidirect products. Now let $\Gamma = H\times K$ and $G = H \rtimes_\psi K = \{[h,k]\}$, where $\psi : K \to \mathrm{Aut}(H)$ is a homomorphism and

$$[h_1,k_1][h_2,k_2] = [h_1\psi(k_1)(h_2), k_1k_2].$$

Consider the fixed point free pair (f_2,f_1) where $f_1(h,k) = [h,1]$, $f_2(h,k) = [1,k]$.

Theorem 0.11. *Let $G = H \rtimes_\psi K$ be a semi-direct product of groups where K is abelian, and a skew left brace corresponding to the fixed point free pair of homomorphisms (f_2,f_1) from $H\times K$ to G as above. A subgroup G' of G is $\circ$-stable if for all $[t,w]$ in G' and all k in K, $[\psi(k)(t),w]$ is in G'.*

Proof. For $\gamma = (h,k)$,

$$\beta(\gamma) = \lambda(f_2(\gamma))\rho(f_1(\gamma)).$$

So

$$\beta_*(h,k) = [1,k][h^{-1},1] = [\psi(k)(h^{-1}),k],$$

from which it follows that

$$\alpha_*([h,k]) = (\psi(k^{-1})(h^{-1}),k).$$

Then the operation $\circ$ on $G = H\rtimes_\phi K$ is given by

$$\begin{aligned}[h_1,k_1]\circ[h_2,k_2] &= \beta_*(\alpha_*([h_1,k_1])(\alpha_*([h_2,k_2]))\\ &= \beta_*((\psi(k_1^{-1})(h_1^{-1}),k_1)((\psi(k_2^{-1})(h_2^{-1}),k_2))\\ &= \beta_*((\psi(k_1^{-1})(h_1^{-1})\cdot(\psi(k_2^{-1})(h_2^{-1}),k_1k_2))\\ &= [\psi(k_1)(h_2)\cdot(\psi(k_1k_2k_1^{-1})(h_1),k_1k_2].\end{aligned}$$

Since K is abelian, this reduces to

$$[h_1, k_1] \circ [h_2, k_2] = [\psi(k_1)(h_2) \cdot (\psi(k_2)(h_1), k_1k_2].$$

Now $G' \subseteq H \rtimes_\psi K$ is $\circ$-stable iff for every x in G' and every g in G, there exists y in G' so that $g \circ x = yg$.

Let $x = [t, w], y = [v, z], g = [h, k]$. The equation $g \circ x = yg$ becomes

$$[h, k] \circ [t, w] = [v, z][h, k],$$

or

$$[(\psi(k)(t))(\psi(w)(h)), kw] = [v\psi(z)(h), zk],$$

which implies that $w = z$ and for all $[h, k]$ in G,

$$\psi(k)(t)\psi(w)(h) = v\psi(w)(h),$$

so

$$\psi(k)(t) = v.$$

Recap.

Theorem 0.12. *Let $\Gamma = H \times K$, $G = H \rtimes_\psi K$ with K abelian. The natural fixed point free pair (f_1, f_2), $f_1(h, k) = [h, 1], f_2(h, k) = [1, k]$ yields*

$$\beta(h, k) = \lambda(h)\rho(k),$$

and a subgroup G' of G is $\circ$-stable iff for every $[t, w]$ in G' and every h in H, $[ht\psi(w)(h^{-1}), w]$ is in G'.

For the twisted natural fixed point free pair (f_2, f_1), yielding

$$\beta(hk) = \lambda(k)\rho(h),$$

a subgroup G' of G is $\circ$-stable iff for every $[t, w]$ in G' and every k in K, $[\psi(k)(t), w]$ is in G'.

... so... Let $G = H \rtimes_\psi K$. For the natural fixed point free pair, setting $w = 1$ shows that the $\circ$-stable subgroups of H are the normal subgroups of G, while for the twisted fixed point free pair, setting $t = 1$ shows that every subgroup of K is $\circ$-stable.

A special case of the twisted fpf pair. For A any finite group, let $\Gamma = A, \epsilon(g) = 1, \iota(g) = g$, let $G = A \times (1)$. Let $\beta : \Gamma \to \mathrm{Hol}(G)$ by

$$\beta(g) = \lambda(\epsilon(g))\rho(\iota(g)).$$

Then $\beta_*(g) = g^{-1}$, so the corresponding map $\alpha_* : G \to \mathrm{Perm}(\Gamma)$ is given by

$$\alpha_*(g)(x) = (\beta_*)^{-1}(\lambda(g)(\beta_*(x)) = xg^{-1} = \rho(g)(x).$$

The last theorem implies that every subgroup G' of G is $\circ$-stable, because the $\circ$-stability equation $g \circ g' = h'g$ in this case reduces to $g' = h'$. This is what we should get, because $\alpha(G) = \rho(G)$, which yields the classical Hopf Galois structure on a Galois extension L/K with Galois group Γ.

Holomorphs of $\mathbb{Z}_q$. Let $G = Z_q \rtimes Z_{\phi(q)}$ where $q = p^e$, p an odd prime, both groups written additively. Let b be a primitive root modulo q.

Let $\Gamma = Z_q \times Z_{\phi(q)}$ with operation

$$[h_1, k_1][h_2, k_2] = [h_1 + b^{k_1} h_2, k_1 + k_2]$$

and let f_1, f_2 be the projection maps from Γ to G mapping onto the left, resp. right factors. Let $\beta : \Gamma \to \mathrm{Hol}(G)$ be the twisted regular embedding arising from the fixed point free pair (f_1, f_2). Then a subgroup G' of G is $\circ$-stable in the skew left brace defined by β if and only if for all $[h, k]$ in G', $[b^k h, k]$ is in G'.

The subgroups of G all have the form

$$G' = \langle [a, 0], [c, d] \rangle.$$

Let v_p be the p-adic valuation with $v_p(p) = 1$. Then

Theorem 0.13. *$G' = \langle [a, 0], [c, d]$ is $\circ$-stable if and only if $v_p(a) \leq v_p(b^d - 1) + v_p(c)$*

Fixed point free endomorphisms. In [Ch13] we took a Galois extension K/k with Galois group G, a semidirect product of abelian groups, and considered Hopf Galois structures on L/K of type G arising from a fixed point free endomorphism. We look at that situation.

Definition. A fixed point free endomorphism of G is an endomorphism ψ of G such that $g = \psi(g)$ if and only if g is the identity element e of G. An endomorphism ψ of G is abelian if the image of ψ is abelian, that is, for all g_1, g_2 in G, $\psi(g_1 g_2) = \psi(g_2 g_1)$.

If ψ is a fixed point free endomorphism of G, then (id, ψ) is a fixed point free pair of homomorphisms from G to G.

Suppose ψ is an abelian fixed point free endomorphism. Then by Caranti [Ca13], ψ has a quasi-inverse abelian fixed point free endomorphism θ, so that

$$\theta(\psi(g)) = \psi(g)\theta(g) \text{ and } \psi(\theta(g) = \theta(g)\psi(g).$$

Getting β. Given a fixed point free endomorphism on the Galois group G of a Galois extension K/k, define

$$\beta : G \to \mathrm{Hol}(G)$$

by

$$\beta(g) = \lambda(g)\rho(\psi(g)).$$

Then β_*, defined by $\beta_*(g) = g\psi(g^{-1})$, is a bijection from G to G. If θ is the quasi-inverse of ψ, then

$$\alpha_* : G \to G$$

defined by

$$\alpha_*(g) = g\theta(g^{-1})$$

is the inverse of the map β_*.

The left skew brace structure. Given the regular embedding $\beta : G \to \mathrm{Hol}(G)$, we define $\circ$ on G by

$$\begin{aligned} g \circ h &= \beta_*(\alpha_*(g)\alpha_*(h)) \\ &= \beta_*(g\theta(g)^{-1}h\theta(h)^{-1}) \\ &= g\theta(g)^{-1}h\theta(h)^{-1}\psi(g\theta(g)^{-1})h\theta(h)^{-1})^{-1} \\ &= g\theta(g)^{-1}h\theta(h)^{-1}\psi\theta(h)\psi(h^{-1})\psi\theta(g)\psi(g^{-1}) \\ &= g\theta(g)^{-1}h\theta(h)^{-1}\theta(h)\psi(h)\psi(h^{-1})\theta(g)\psi(g)\psi(g^{-1}) \\ &= g\theta(g)^{-1}h\theta(g) \\ &= gC(\theta(g)^{-1})(h). \end{aligned}$$

$\circ$-stable subgroups.

Theorem 0.14. *Let ψ, θ be a quasi-inverse pair of abelian fixed point free endomorphisms of G. Let $\beta(g) = \lambda(g)\rho(\psi(g))$ as above, yielding the skew left brace structure as just shown. Then G' is a $\circ$-stable subgroup of G if and only if G' is a normal subgroup of G.*

Proof. A subgroup G' of G is $\circ$-stable if for all x in G', g in G, there exists y in G' so that $yg = g \circ x$. That is,

$$yg = gC(\theta(g)^{-1})(x) = g\theta(g)^{-1}x\theta(g)$$

So $y = (g\theta(g)^{-1})x(\theta(g)g^{-1}) = C(g\theta(g)^{-1})(x)$. In words, G' is $\circ$-stable iff G' is closed under conjugation by $\{g\theta(g)^{-1} : g \in G\} = G$, iff G' is a normal subgroup of G. ∎

A special case. One example of a fixed point free endomorphism of G is the trivial endomorphism, in which case $\beta = \lambda$. So this set of examples generalizes the case of the canonical non-classical Hopf Galois extension by H_λ.

This result could presumably be proved directly, as a consequence of a theorem of Koch, Kohl, Truman and Underwood that if L/K is a Galois extension with Galois group G and has a H-Hopf Galois structure by H_ψ where ψ is an abelian fixed point free endomorphism of G as above, then H_ψ is isomorphic to H_λ as Hopf algebras, hence by descent from a G-equivariant isomorphism between the subgroups $\lambda(G)$ and M_ψ of $\mathrm{Perm}(G)$ that descend to H_λ and H_ψ. A G-equivariant isomorphism should map G-equivariant subgroups of $\lambda(G)$ onto those of M_ψ, hence yield a bijection of K-sub-Hopf algebras of the two Hopf algebras.

Some examples of fixed point free endomorphisms. Let $G = \mathbb{Z}/p^e\mathbb{Z} \rtimes W$ where $W = \langle \omega \rangle$ for ω in $\mathbb{Z}/p^e\mathbb{Z}^\times$ of order q, where q divides $p-1$. The operation in G is:

$$[a, s][a', s'] = [a + \omega^s a', s + s'].$$

Define the abelian fixed point free endomorphisms ψ and θ by

$$\psi[a, 0] = [0, 0], \quad \psi[0, 1] = [h, s];$$
$$\theta[a, 0] = [0, 0], \quad \theta[0, 1] = [k, t]$$

where $(s-1, q) = (t-1, q) = 1$, $s, t \not\equiv 0 \pmod q$, and

$$(\omega^s - 1)k = (\omega^t - 1)h.$$

Then ψ and ω are quasi-inverses of each other. There are $\phi(q) - 1$ choices for s, and p^e choices for h, hence $(\phi(q) - 1)p^e$ different Hopf Galois structures on a Galois extension K/k with Galois group G arising from the different ψ.

The $\circ$-stable subgroups G' of G are the normal subgroups of G. These consist of the subgroups of $\mathbb{Z}/p^e\mathbb{Z}$ and the subgroups $\mathbb{Z}/p^e\mathbb{Z} \rtimes B$ for B a non-trivial subgroup of W. For if G' contains $[c, d]$, then

$$[-1, 0][c, d][1, 0] = [-1 + c + \omega^d, d] = [\omega^d - 1, 0][c, d]$$

is in G', hence $[\omega^d - 1, 0]$. But $\omega^d - 1 \not\equiv 0 \pmod p$ for $1 \leq d < q \leq p-1$, and hence G' contains $\langle [\omega^d - 1, 0] \rangle = \mathbb{Z}/p^e\mathbb{Z} \rtimes 0$. (The subgroup $\langle [p^r, 0], [0, s] \rangle$ is not a normal subgroups of G for every r, $0 \leq r < e$ and every divisor of q.)

There are $(e+1)d(q)$ subgroups of G, including $e + d(q)$ normal subgroups, where $d(q)$ = number of divisors of q. For example, for

$p^e = 121, a = 10$, there are $3 \cdot 4 = 12$ subgroups of G, of which 6 are normal.

A twisted version? The twisted version of this last example doesn't work–the quasi-inverse formula becomes different and forces the fixed point free endomorphisms to be trivial.

An example of Stuart Taylor. Let $G = D_4 = \langle r, f\rangle$ be the dihedral group, where $r^4 = 1$ (r = rotation 90°), $f^2 = 1$ (reflection) and $rf = fr^3$. Let $\Gamma = Q_8 = \langle k, i\rangle$ be the quaternion group, where $ki = -ik = j, i^2 = j^2 = k^2 = -1$. Define

$$\alpha : D_4 \to \mathrm{Perm}(Q_8)$$

by $\alpha(r) = \lambda(k), \alpha(f) = \lambda(i)\rho(k)$. Then the map α_* is as in the following table, and β_* is the inverse of α_*:

D_4	α_*	Q_8
1	$\to$	1
r	$\to$	k
r^2	$\to$	k^2
r^3	$\to$	k^3
f	$\to$	ik^3
fr	$\to$	i
fr^2	$\to$	ik
fr^3	$\to$	ik^2

Then one sees that

$$r \circ x = \beta_*(\alpha_*(r)\alpha_*(x)) = rx$$

for all x in D_4, while

$$f \circ r^t = fr^t,$$

$$f \circ fr^t = r^{t+2}.$$

A subgroup G' of D_4 is $\circ$-stable iff for all g' in G' and all g in G, $(g \circ g')g^{-1}$ is in G'. Some computations show that G' is $\circ$-stable iff:

- r is in G' iff r^3 is in G';
- f is in G' iff fr^2 is in G';
- fr is in G' iff fr^3 is in G';

It follows that among the ten subgroups of D_4, the $\circ$-stable subgroups of $G = D_4$ are precisely the six normal subgroups of G.

References

[Bac16] D. Bachiller, Counterexample to a conjecture about braces, J. Algebra 453 (2016), 160–176.

[Bac16a] D. Bachiller, Solutions of the Yang-Baxter equation associated to skew left braces, with applications to racks, arXiv: 1611.08138v1, 24 Nov. 2016.

[By96] N. P. Byott, Uniqueness of Hopf Galois structure of separable field extensions, Comm. Algebra 24 (1996), 3217–3228, 3705.

[By15] N. P. Byott, Solubility criteria for Hopf-Galois structures, New York J. Math 21 (2015), 883–903.

[BC12] N. P. Byott, L. N. Childs, Fixed point free pairs of homomorphisms and Hopf Galois structures, New York J. Math. 18 (2012), 707–731.

[BV17] N. P. Byott, L. Vendramin, Hopf-Galois extensions, Appendix A of [SV17].

[Ca13] A. Caranti, Quasi-inverse endomorphisms, J. Group Theory 16 (2013), 779–792.

[CDVS06] A. Caranti, F. Dalla Volta, M. Sala, Abelian regular subgroups of the affine group and radical rings, Publ. Math. Debrecen 69 (2006), 297–308.

[CaC99] S. Carnahan, L. N. Childs, Counting Hopf Galois structures on non-abelian Galois extensions, J. Algebra 218 (1999), 81–92.

[CS69] S. U. Chase, M. E. Sweedler, Hopf Algebras and Galois Theory, Springer LNM 97 (1969).

[Ch89] L. N. Childs, On the Hopf Galois theory for separable field extensions, Comm. Algebra 17 (1989), 809-825.

[Ch03] L. N. Childs, Hopf Galois structures and complete groups, New York J. Math. 9 (2003), 99-115.

[Ch13] L. N. Childs, Fixed-point free endomorphisms and Hopf Galois structures, Proc. Amer Math. Soc. 141 (2013), 1255-1265.

[Ch15] L. N. Childs, On abelian Hopf Galois structures and finite commutative nilpotent rings, New York J. Math. 21 (2015), 205–229.

[Ch16] L. N. Childs, Obtaining abelian Hopf Galois structures from finite commutative nilpotent rings, arxiv: 1604.05269

[Ch17] L. N. Childs, On the Galois correspondence for Hopf Galois structures, New York J. Math. (2017), 1–10.

[Ch18] L. N. Childs, Left skew braces and the Galois Correspondence for Hopf Galois extensions, arxiv:1802l03448.

[CCo07] L. N. Childs, J. Corradino, Cayley's Theorem and Hopf Galois structures arising from semidirect products of cyclic groups, J. Algebra 308 (2007), 236–251.

[CG17] L. N. Childs, C. Greither, Bounds on the number of ideals in finite commutative nilpotent $\mathbb{F}_p$-algebras, arXiv:1706.02518, Publ. Math. Debrecen 92 (2018), 495–516.

[Con] Keith Conrad, Groups of order p^3, 5 pages, retrieved from www.math.uconn.edu/ kconrad/blurbs/grouptheory/groupsp3.pdf

[CRV16] T. Crespo, A. Rio, M. Vela, On the Galois correspondence theorem in separable Hopf Galois theory, Publ. Math. (Barcelona) 60 (2016), 221–234.

[DeG17] W. A. De Graaf, Classification of nilpotent associative algebras of small dimension, arXiv:1009.5339v2 (22 May 2017).

[FCC12] S. C. Featherstonhaugh, A. Caranti, L. N. Childs, Abelian Hopf Galois structures on prime-power Galois field extensions, Trans. Amer. Math. Soc. 364 (2012), 3675–3684.

[GP87] C. Greither, B. Pareigis, Hopf Galois theory for separable field extensions, J. Algebra 106 (1987), 239–258.

[GV17] L. Guarnieri, L. Ventramin, Skew braces and the Yang-Baxter equation, Math. Comp.86 (2017), 2519–2534.

[Rum07] W. Rump, Braces, radical rings, and the quantum Yang-Baxter equation, J. Algebra 307 (2007), 153–170.

[SV17] A. Smoktunowicz, L. Vendramin, On skew braces (with an appendix by N. Byott and L. Vendramin), arXiv:1705.06958v2 (13 June 2017).

[Zen18] K. Zenouz, Skew braces and Hopf-Galois structures of Heisenberg type, arXiv:1804.03160v4 (17 May 2018).

Department of Mathematics and Statistics, University at Albany, Albany, NY 12222

E-mail address: lchilds@albany.edu