The Galois correspondence for Hopf Galois structures arising from bi-skew braces

Lindsay N. Childs
University at Albany
Albany, NY 12222

June 6, 2019

Hopf Galois structures

Let L/K be a G-Galois extension of fields: that is, a Galois extension of fields with Galois group $G = (G, \circ)$. Suppose L is also an H-Hopf Galois extension of K. Then H is a cocommutative K-Hopf algebra and from Greither and Pareigis, $L \otimes_K H = LN$ for some regular subgroup N of $\mathrm{Perm}(G)$, where N is normalized by the image $\lambda_\circ(G)$ of the left regular representation $\lambda_\circ : G \to \mathrm{Perm}(G)$. Given N, H can be recovered by Galois descent: $H = LN^G$.

The type of H is the isomorphism type of the group N.

If a G-Galois extension has a Hopf Galois structure of type N, we'll say that the ordered pair (G, N) of abstract groups (of equal order) is realizable.

Two operations on G

Since N is a regular subgroup of $\mathrm{Perm}(G)$, the map $b : N \to G$ given by $n \mapsto n(e)$ is a bijection. Then b defines a new operation $\star$ on G, as follows: with $b(n_1) = g_1, b(n_2) = g_2$, then

$$g_1 \star g_2 = b(n_1 n_2).$$

Then $N = \lambda_\star(G)$. For setting $b(n_1) = g_1, b(n_2) = g_2$, $g_1 \star g_2 = b(n_1 n_2)$, then the action of $N \subset \mathrm{Perm}(G)$ on G is

$$\begin{aligned} n_1(g_2) &= n_1(b(n_2)) = n_1(n_2(e)) = (n_1 n_2)(e) \\ &= b(n_1 n_2) = g_1 \star g_2 = \lambda_\star(g_1)(g_2). \end{aligned}$$

Since $N = \lambda_\star(G)$ in $\mathrm{Perm}(G)$ is normalized by $\lambda_\circ(G)$, then $\lambda_\circ(G)$ is contained in $\mathrm{Hol}(G, \star)$, the normalizer of $\lambda_\star(G)$ in $\mathrm{Perm}(G)$.

Skew left braces

Definition

A skew (left) brace 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, and the 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 $\overline{a}$.

If B has two operations $\star$ and $\circ$ and is a skew brace with $(B, \star)$ the additive group, then we write $B = B(\circ, \star)$ (i. e. the additive group operation is on the right).
A left brace is a skew brace with abelian additive group.

A characterization of skew braces

A set B with two group operations $\circ$ and $\star$ has 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 proved ([GV17], Proposition 1.9):

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

$$\mathrm{Hol}(B, \star) = \lambda_\star(B)\mathrm{Aut}(B, \star) \subset \mathrm{Perm}(B).$$

Relating skew braces and Hopf Galois structures

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 N on L/K. Then N gives $(G, \circ)$ a skew left brace structure with additive group $(G, \star) \cong N$, because $\lambda_\circ(G)$ is contained in $\mathrm{Hol}(G, \star)$.

Conversely, 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 $(G, \star)$. For given the skew brace structure $(G, \circ, \star)$ on the Galois group $(G, \circ)$ of L/K, then $\lambda_\circ(G)$ is contained in $\mathrm{Hol}(G, \star)$, and so the subgroup $N = \lambda_\star(G) \subset \mathrm{Perm}(G)$ is normalized by $\lambda_\circ(G)$. So N corresponds by Galois descent to a Hopf Galois structure on L/K of type $(G, \star)$. Thus, given $(G, \circ, \star)$ a skew brace, the pair $((G, \circ), (G, \star))$ is realizable.

The correspondence is not bijective

Theorem (Byott, Nejabati Zenouz)

Given an isomorphism type $(B, \circ, \star)$ of skew left brace, the number of Hopf Galois structures on a Galois extension L/K with Galois group isomorphic to $(B, \circ)$ and skew brace isomorphic to $(B, \circ, \star)$ is

$$\mathrm{Aut}(B, \circ)/\mathrm{Aut}_{sb}(B, \circ, \star).$$

Here $\mathrm{Aut}_{sb}(B, \circ, \star)$ is the group of skew brace automorphisms of $(B, \circ, \star)$, that is, maps from B to B that are simultaneously group automorphisms of $(B, \star)$ and of $(B, \circ)$.

Bi-skew braces

Definition

A bi-skew brace is a finite set B with two operations, $\star$ and $\circ$ so that $(B, \star)$ is a group, $(B, \circ)$ is a group, and B is a skew brace with either group acting as the additive group. Thus the two compatibility conditions

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

and

$$a \star (b \circ c) = (a \star b) \circ \overline{a} \circ (a \star c)$$

hold for all a, b, c in B.

If $(G, \circ, \star)$ is a bi-skew brace, then the ordered pair of groups $((G, \circ), (G, \star))$ is realizable, and the ordered pair of groups $((G, \star), (G, \circ))$ is also realizable.

Examples of bi-skew braces

From [Ch19]:
• Radical algebras A with $A^3 = 0$ yield bi-skew braces.
• Semidirect products of groups yield bi-skew braces.

We note a consequence of the latter:
Let $(G, \cdot) = H \rtimes J$ be a semidirect product of finite groups. By the method of fixed point free homomorphisms, we know that if $(G, \circ) = H \times J$, then $(H \times J, H \rtimes J)$ is realizable, so $(G, \circ, \cdot)$ is a skew brace, hence a bi-skew brace. But then $(H \rtimes J, H \times J)$ is also realizable–a skew brace proof of a theorem of Crespo, Rio and Vela [CRV16]. A class of examples: if G is any group of square-free order n, then G is a semidirect product of cyclic groups. So (C_n, G) is realizable (Alebdali and Byott [AB18]), and also (G, C_n) is realizable: every Galois extension of squarefree order has a cyclic Hopf Galois structure.

Galois correspondence

Let L/K be Galois with group $(G, \circ)$ and Hopf Galois of type $(G, \star)$, so $(G, \circ, \star)$ is a skew brace. We're interested in

$$\frac{|\{E \text{ in the image of the Galois correspondence for } H\}|}{|\{E : K \subset E \subset L\}|}.$$

The numerator counts the $\lambda_\circ(G)$-invariant subgroups of $\lambda_\star(G)$. Looking at them in the skew brace setting, we have

Definition

Let $(G, \circ, \star)$ be a skew left brace. A subgroup $(G', \star)$ of $(G, \star)$ is $\circ$-stable if $\lambda_\star(G')$ is closed under conjugation in $\mathrm{Perm}(G)$ by $\lambda_\circ(G)$.

$\circ$-stable subgroups

The $\circ$-stable condition is equivalent to

$$\text{For all } g \in G, g' \in G', \text{ there is some } h' \in G' \text{ so that } g \circ g' = h' \star g.$$

A $\circ$-stable subgroup of $(G, \circ, \star)$ is a subgroup of both $(G, \circ)$ and $(G, \star)$.

For the rest of this talk, we'll consider some examples.

Bi-skew braces from radical algebras

A finite ring $(A, +, \cdot)$ is a radical ring if with the operation $\circ$ defined by $a \circ b = a + b + a \cdot b$, $(A, \circ)$ is a group. Then $(A, \circ, +)$ is a skew brace with additive group $(A, +)$. $(A, +, \circ)$ is also a skew brace (and hence is a bi-skew brace) if and only if $A^3 = 0$ (i. e. for every a, b, c in A, $a \cdot b \cdot c = 0$).

Radical algebras and the Galois correspondence

Last year I showed that if A is a radical algebra, so that $(A, \circ, +)$ is a skew brace, then the $\circ$-stable subgroups of $(A, +)$ are the left ideals of the algebra A.
Suppose A is a radical algebra with $A^3 = 0$, so that $(A, +, \circ)$ is also a skew left brace. Then we're interested in the set of $+$-stable subgroups of $(A, \circ)$.
We have:

Theorem

Let $(A, +, \circ)$ be the skew brace arising from the radical ring $(A, +, \cdot)$ with $A^3 = 0$. Then the $+$-stable subgroups of $(A, \circ)$ are the right ideals of the ring A.

A four-dimensional example

Let $A^0_{4,21}$ [De Graaf's notation ([DeG18])] with $\mathbb{F}_p$-basis (a, b, c, d) with multiplication given by $a^2 = c$, $ab = d$ and all other products of basis elements $= 0$. Then $A^3 = 0$, so $(A, +, \cdot)$ is a bi-skew brace. Let L/K be G-Galois with an H-Hopf Galois structure of type N where $G = (A, +), N = (A, \circ)$. Then

$$\frac{|\text{ image of g. c. for } H|}{|\{E : K \subset E \subset L\}|} = \frac{|\{\text{ right ideals of } A\}|}{|\{\text{ subgroups of } (A, +)\}|} = \frac{2p^2 + 3p + 5}{p^4 + 3p^3 + 4p^2 + 3p + 5}.$$

For L/K $(A, \circ)$-Galois with a HG structure of type $(A, +)$, the corresponding ratio is

$$\frac{|\{\text{ left ideals of } A\}|}{|\{\text{ subgroups of } (A, \circ)\}|} = \frac{p^2 + 3p + 5}{2p^3 + 4p^2 + 3p + 5}.$$

Semidirect products and the Galois correspondence

Let $G = G_L \rtimes G_R$ be a semidirect product of two finite groups G_L and G_R, where G_L is normal in G. Denote the group operation in G by $\cdot$, which we will often omit. Thus for x, y in G, $xy = x \cdot y$.
An element of G has a unique decomposition as $x = x_L x_R^{-1}$ for x_L in G_L, x_R in G_R. An element y_R of G_R acts on x_L in G_L by conjugation:

$$y_R^{-1} x_L = (y_R^{-1} x_L y_R) y_R.$$

The direct product operation

Along with the given group operation on G we also define the direct product operation $\circ$, as follows:

$$\begin{aligned} x \circ y &= x_L x_R^{-1} \circ y_L y_R^{-1} \\ &= x_L y_L y_R^{-1} x_R^{-1} \\ &= x_L y x_R^{-1} = (xy)_L (xy)_R^{-1}. \end{aligned}$$

So the map $G_L \times G_R \to (G, \circ)$ by

$$(x_L, x_R) \mapsto x_L x_R^{-1}$$

is an isomorphism. Then $(G, \circ, \cdot)$ is a bi-skew brace.

For $(G, \circ, \cdot)$ the bi-skew brace where $(G, \cdot) = G_L \rtimes G_R$ and $(G, \circ) = G_L \times G_R$, we have
(i) A subgroup G' of $(G, \cdot)$ is $\circ$-stable if and only if G' is normalized by G_L.
(ii) A subgroup G' of $(G, \circ)$ is $\cdot$-stable if and only if G' is closed under conjugation of left components by elements of G: for every $x = x_L x_R^{-1}$ in G' and all g in G, $(g x_L g^{-1}) x_R^{-1}$ is in G'.

Some examples:

A group of order 54

Let $(G, +) = G_L \times G_R = \mathbb{Z}_9 \times \mathbb{Z}_6$, the direct product with the usual operation, $(r, s) + (r', s') = (r + r', s + s')$, and define a semidirect product operation $\cdot$ on G by identifying (r, s) with $r \cdot 2^s$ in $(G, \cdot) = \mathbb{Z}_9 \rtimes U_9 \cong \mathrm{Hol}(C_9)$. So $(r, s) \cdot (r', s') = (r + 2^s r', s + s')$. (Here, $\circ = +$).)

Since the $+$-stable subgroups of G and the $\cdot$-stable subgroups of G are subgroups of both $(G, +)$, and $(G, \cdot)$, we began by finding the subgroups of the direct product $(G, +)$ that are also subgroups of $(G, \cdot)$, and then asked which are $+$-stable and which are $\cdot$-stable.

Results

We found that there are 20 subgroups of $\mathbb{Z}_9 \times \mathbb{Z}_6$: sixteen are cyclic groups.
Six of the 16 cyclic groups of the direct product are not subgroups of the semidirect product $(G, \cdot)$. So that leaves 14 possibilities for subgroups that are $+$-stable or $\cdot$-stable, namely, the four non-cyclic groups, along with the cyclic groups with generators

$$(0,0),(1,0),(3,0),(0,2),(1,2),(3,2),(1,4),(3,4),(0,3) \text{ and } (0,1).$$

Stable subgroups

It turns out that a subgroup G' of $(G, \cdot)$ is $\cdot$-stable iff for all (r, s) in G', $(r, 0)$ is in G'.
Using that criterion, there are ten $\cdot$-stable subgroups of $(G, +)$.
There are 31 subgroups of $(G, \cdot)$. So

$$\frac{|\cdot\text{-stable subgroups of } (G, +)|}{|\text{ subgroups of } (G, \cdot)|} = \frac{10}{31}.$$

A subgroup G' of G is $+$-stable if G' is normalized by G_L in $(G, \cdot)$, iff for all (r, s) in G', $(2^s - 1, 0)$ is in G'.
Using this criterion, there are seven $+$-stable subgroups of $(G, \cdot)$.
There are 20 subgroups of $(G, +)$. So the ratio

$$\frac{|\cdot\text{-stable subgroups of } (G, \cdot)|}{|\text{ subgroups of } (G, \cdot)|} = \frac{7}{20}.$$

Groups of squarefree order

Hopf Galois structures on groups of squarefree order were studied by Alebdali and Byott [AB18]. Their results implied that if the field extension L/K has a Galois group G cyclic of squarefree order mn, then L/K has a Hopf Galois structure of type N for every group N of order mn: each such group N must be a semidirect product of cyclic groups.

Some examples

Let $(G, +) = \mathbb{Z}_m \times \mathbb{Z}_n$ under componentwise addition, where m and n are coprime and squarefree and n divides $\phi(m)$. Then $(G, +)$ is cyclic of order mn, and every element of G may be written as $(r, s) = (r, 0) + (0, s)$ for r modulo m, s modulo n.
Let b have order n in U_m, the group of units modulo m. Form the semidirect product $(G, \cdot)$ with the operation

$$(r, s) \cdot (r', s') = (r + b^s r', s + s').$$

Then $(G, +, \cdot)$ is a bi-skew brace.
The subgroups of $(G, +)$ are generated by (r, s) where r divides m and s divides n, so there are $d(m)d(n)$ subgroups of $(G, +)$, where $d(m)$ is the number of divisors of m. If m is a product of g distinct primes, and n is a product of h distinct primes, then $d(m) = 2^g$, $d(n) = 2^h$. Hence the number of subgroups of $(G, +)$ is 2^{g+h}.

A preliminary observation

With $(G, +, \cdot)$ the bi-skew brace with $(G, +) = Z_m \times Z_n$,$(G, \cdot) = Z_m \rtimes Z_n$, we found that every subgroup of $(G, +)$ is also a subgroup of $(G, \cdot)$. Since the $+$-stable subgroups and the $\cdot$-stable subgroups of $(G, +, \cdot)$ are subgroups of both $(G, +)$ and $(G, \cdot)$, we could search for each from among the subgroups $\langle (r, s) \rangle$ of the cyclic group $(G, +)$, where r divides m and s divides n.

$\cdot$-stable subgroups of $(G, +)$

We found that every subgroup of $(G, +) = Z_m \times Z_n$ is $\cdot$-stable:

$$(q, t)^{-1}(r, 0)(q, t)(0, s) = (-b^{-t}r, 0)(0, s) \text{ is in } \langle (r, s) \rangle.$$

Thus, if L/K is $Z_m \rtimes Z_n$-Galois with a HG structure by H of cyclic type $Z_m \times Z_n$, the ratio

$$\frac{|\text{ image of the G. c. for } H|}{|\{E : K \subset E \subset L\}|}$$

is

$$\frac{|\{\text{ subgroups of } Z_m \times Z_n\}|}{|\{\text{subgroups of } Z_m \rtimes Z_n\}|}$$

A special case: $(G, +) = Z_p \rtimes Z_q$

Consider $(G, +) = \mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$ where p is prime and q is a prime divisor of $p - 1$. Let b have order q modulo $p - 1$ and let $(G, \cdot) = \mathbb{Z}_p \rtimes \mathbb{Z}_q$ with operation

$$(r_1, s_1)(r_2, s_2) = (r_1 + b^{s_1} r_2, s_1 + s_2).$$

Then $(G, +)$ has four subgroups, generated by $(1, 0), (0, 1), (1, 1)$ and $(0, 0)$, of orders p, q, pq and 1, respectively. A subgroup G' of G is $+$-stable iff for all (r, s) in G', $(2^s - 1, 0)$ is in G'. The only subgroup of $(G, +)$ that is not $+$-stable is $(0, 1)$, because $b - 1$ is not in $\langle 0 \rangle \subset \mathbb{Z}_p$. So for the biskew brace $(G, \cdot, +)$ with $(G, +) = Z_p \times Z_q$ $(G, \cdot) = Z_p \rtimes Z_q$, the ratio,

$$\frac{|\{+\text{-stable subgroups of } (G, \cdot)\}|}{|\{\text{subgroups of } (G, +)\}|} = \frac{3}{4}.$$

$(G, \cdot) = Z_p \rtimes Z_q$

For the other ratio: All four subgroups of $(G, +)$ are $\cdot$-stable. There are $p + 3$ subgroups of $(G, \cdot)$. So

$$\frac{\{\cdot\text{-stable subgroups of } (G, +)\}}{|\{\text{subgroups of } (G, \cdot)\}|} = \frac{4}{p+3}.$$

Generalize

Now let $(G,+) = \mathbb{Z}_{mn}$ where $m = p_1 \cdots p_g$, and $n = q_1 \cdots q_g$, all pairwise distinct primes, where for $i = 1, \ldots g$, q_i divides $p_i - 1$. Let b have order q_i modulo p_i for all i, so b has order n modulo m. Then

$$(G,+) \cong \mathbb{Z}_{p_1 q_1} \times \cdots \times \mathbb{Z}_{p_g q_g}$$
$$(G,\cdot) \cong (\mathbb{Z}_{p_1} \rtimes \mathbb{Z}_{q_1}) \times \cdots \times (\mathbb{Z}_{p_g} \rtimes \mathbb{Z}_{q_g}),$$

and the subgroups decompose as direct products by an application of Goursat's Lemma. So the ratios are

$$\frac{|\{\cdot\text{-stable subgroups of } (G,+)\}|}{|\{\text{subgroups of } (G,\cdot)\}|} = \frac{4^g}{(p_1+3)(p_2+3)\cdots(p_g+3)}$$

and

$$\frac{|\{+\text{-stable subgroups of } (G,\cdot)\}|}{|\{\text{subgroups of } (G,+)\}|} = (\frac{3}{4})^g.$$

Both ratios go to zero for large g.

A final example

Let $m = p_1 \cdots p_g$, a product of primes, and let $n = q_1 \cdots q_h$ where $q_1, \ldots, q_h$ are primes that divide every $p_i - 1$ for $i = 1, \ldots, g$. Let b have order n modulo p_i for every i. Then $(G, \cdot) = \mathbb{Z}_m \rtimes \mathbb{Z}_n$ and

$$\frac{|\{\ +\text{-stable subgroups of } G, \cdot)\}|}{|\{\text{ subgroups of } (G, +)|\}} = \frac{2^h + 2^g - 1}{2^{h+g}}.$$

If $h = 1$ (for example if $n = q = 2$ and $p_1, \ldots, p_g$ are any g distinct primes), then $G, \cdot) = D_m$, the dihedral group, and the ratio is

$$\frac{2^g + 1}{2^{g+1}} \sim \frac{1}{2}$$

for g large. So for L/K cyclic of order $2m$, m odd, squarefree, with a Hopf Galois structure of type $(G, \cdot)$, a lower bound for the Galois correspondence ratio is 1/2.

The other ratio

Suppose L/K has Galois group $(G, \cdot) \cong D_m$, $m = p_1 \cdots p_g$ a product of g distinct odd primes, and has a Hopf Galois structure of type $(G, +) \cong C_{2m}$. Then the Galois correspondence ratio is

$$\frac{2^{g+1}}{m + 2^g + 2^g} = \frac{1}{\frac{1}{2}(\frac{p_1}{2} \cdot \frac{p_2}{2} \cdots \frac{p_g}{2}) + 1}.$$

For g large this is close to 0.

Summary

For a Galois extension L/K with Galois group G and a Hopf Galois structure of type N, determining the proportion of intermediate subfields of L/K in the image of the Galois correspondence for H involves finding subgroups of N normalized by $\lambda(G)$. We have translated the problem to one involving a ratio of the sizes of certain sets of subgroups of the skew brace associated to the Galois extension and the Hopf Galois structure. One question I had was: Is there any clear relationship between the pair of ratios corresponding to a bi-skew brace.

As the last example illustrates, the answer appears to be, “no”.

In conclusion

Many thanks to Griff for everything he does to make these conferences possible, and something to look forward to each year.

bibliography

[AB18] A. A. Alebdali, N. P. Byott, Counting Hopf-Galois structures on cyclic field extensions of squarefree degree, J. Algebra 493 (2018), 1-19.
[CS69] S. U. Chase, M. E. Sweedler, Hopf Algebras and Galois Theory, Springer LNM 97 (1969).
[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 structures, J. Algebra 511 (2018), 270–291.
[Ch19] L. N. Childs, Bi-skew braces and Hopf Galois structures, New York J. Math. (to appear).

[CG18] L. N. Childs, C. Greither, Bounds on the number of ideals in finite commutative nilpotent $\mathbb{F}_p$-algebras, Publ. Math. Debrecen 92 (2018), 495–516.
[CRV16] T. Crespo, A. Rio, M. Vela, On the Galois correspondence theorem in separable Hopf Galois theory, Publ. Math. (Barcelona) 60 (2016), 221–234.
[CRV16] T. Crespo, A. Rio, M. Vela, Induced Hopf Galois structures, J. Algebra 457 (2016), 312–322.
[DeG18] W. A. De Graaf, Classification of nilpotent associative algebras of small dimension, International Journal of Algebra and Computation 28 (2018), 133–161.
[GP87] C. Greither, B. Pareigis, Hopf Galois theory for separable field extensions, J. Algebra 106 (1987), 239–258.

[GV17] L. Guarneri, L. Vendramin, Skew braces and the Yang-Baxter equation, Math. Comp. 86 (2017), no. 307, 2519–2534.
[NZ19] K. Nejabati Zenouz, Skew braces and Hopf-Galois structures of Heisenberg type, J. Algebra 524 (2019), 187–225.
[Rum07] W. Rump, Braces, radical rings, and the quantum Yang-Baxter equation, J. Algebra 307 (2007), 153–170.
[SV18] A. Smoktunowicz, L. Vendramin, On skew braces (with an appendix by N. Byott and L. Vendramin), J. Comb. Algebra 2 (2018), no.1, 47–86.
[Ven18] L. Vendramin, Problems on skew left braces, Advances in Group Theory and Applications, to appear.