Isomorphic Holomorphs and Bi-Skew Braces

Timothy Kohl

Boston University

May 26, 2021

Hopf-Galois Structures and Isomorphic Holomorphs

Suppose L/K is Galois with group $G = Gal(L/K)$ and that L/K is Hopf-Galois, corresponding to a regular subgroup $N \leq B = Perm(G)$ where $\lambda(G) \leq Norm_B(N)$.

If $Norm_B(N)$ has a regular subgroup N' for which $Norm_B(N') = Norm_B(N)$ then $\lambda(G) \leq Norm_B(N')$ of course, and therefore N' gives rise to a Hopf-Galois structure as well.

The prototype example of this is the case when $N' = N^{opp} = Cent_B(N)$.

And somewhat more generally, this arises naturally in the study of the multiple holomorph,

$$NHol(N) = Norm_B(Norm_B(N))$$

whose size (and action on N by conjugation) determines the set $\mathcal{H}(N)$, of those regular, normal subgroups of $Norm_B(N) \cong Hol(N)$ that are isomorphic to N, where $Norm_B(N) = Norm_B(N')$

More generally however, the condition that $Norm_B(N) = Norm_B(N')$, for N' another regular subgroup of $Norm_B(N)$, does not automatically imply that $N \cong N'$.

Given that $Norm_B(N) \cong Hol(N) \cong N \rtimes Aut(N)$ it stands to reason that the existence of such an N' would imply (by size considerations at the very least) that $|Aut(N)| = |Aut(N')|$, or more possibly that $Aut(N) \cong Aut(N')$.

To see the connection with bi-skew braces, we shall proceed with a bit of formality.

Classes of Regular Subgroups

For X a finite set where $|X| = n$, we consider the totality of all isomorphism classes of groups of order n embedded as regular subgroups of $B = Perm(X)$, namely $\{G_1, \ldots, G_m\}$.

For each such $G \leq B$ one may form the normalizer $Hol(G) = Norm_B(G)$ which is canonically isomorphic to the classic holomorph of G, namely $G \rtimes Aut(G)$.

Note, we are not focusing on regularity defined in terms of the left regular representation of a single group G embedded as $\lambda(G)$ in $Perm(G)$.

The other principal observation is this:

For the regular subgroups $\{G_1, \ldots, G_m\}$ contained in $B = Perm(X)$, chosen from the distinct isomorphism classes, if $N \leq Perm(X)$ is *any* regular subgroup, then obviously $N \cong G_i$ for exactly one G_i, and therefore $N = \beta G_i \beta^{-1}$ for some $\beta \in B$.

Moreover, $N = \tilde{\beta} G_i \tilde{\beta}^{-1}$ if any only if $\tilde{\beta} \in \beta Hol(G_i)$.

For any paring (G_j, G_i) we can define

$$S(G_j, [G_i]) = \{M \leq Hol(G_j) \mid M \text{ is regular and } M \cong G_i\}$$
$$R(G_i, [G_j]) = \{N \leq B \mid N \text{ is regular and } G_i \leq Hol(N) \text{ and } N \cong G_j\}$$

which are two *complementary* sets of regular subgroups of B, where those in S are contained in a fixed subgroup of B, while the other consists of subgroups of B which may be *widely dispersed* within B.

The class $R(G_i, [G_j])$ is of interest as it corresponds exactly to the K-Hopf algebras H which act on a Galois extension L/K where $Gal(L/K) \cong G_i$ and $H = (L[N])^{Gal(L/K)}$ where $N \cong G_j$.

In particular the fundamental relationship between $S(G_j,[G_i])$ and $R(G_i,[G_j])$ has been explored in [2] by Childs, in [1] by Byott, and by the author in [4].

We present the following recapitulation of all these ideas by showing that both sets are enumerated by the union of sets of cosets of $Hol(G_i)$ and of $Hol(G_j)$ which we shall refer to as the reflection principle.

Proposition

If $B = Perm(X)$ for $|X| = n$ and $\{G_1, \ldots, G_m\}$ is a set of regular subgroups of B, one from each isomorphism class of groups of order n, then for any G_i and G_j one has

$$|S(G_j,[G_i])| \cdot |Hol(G_i)| = |R(G_i,[G_j])| \cdot |Hol(G_j)|.$$

Proof.

(Sketch) We can parameterize the elements of $S(G_j, [G_i])$ by a set of distinct cosets

$$\beta_1 Hol(G_i), \ldots, \beta_s Hol(G_i)$$

and $R(G_i, [G_j])$ by distinct cosets

$$\alpha_1 Hol(G_j), \ldots, \alpha_r Hol(G_j)$$

The bijection we seek is as follows:

$$\Phi : \bigcup_{k=1}^{s} \beta_k Hol(G_i) \to \bigcup_{l=1}^{r} \alpha_l Hol(G_j)$$

defined by $\Phi(\beta_k h) = (\beta_k h)^{-1}$. □

The basic principle is that

$$\begin{gathered}\beta G_i \beta^{-1} \leq Hol(G_j) \\ \updownarrow \\ G_i \leq \beta^{-1} Hol(G_j) \beta = Hol(\beta^{-1} G_j \beta)\end{gathered}$$

i.e.

$$M = \beta G_i \beta^{-1} \in S(G_j, [G_i]) \leftrightarrow N = \beta^{-1} G_j \beta \in R(G_i, [G_j])$$

Since $|Hol(G)| = |G| \cdot |Aut(G)|$ (and all G_k have the same size obviously) we have the following.

Corollary

For G_i and G_j as above one has

$$|S(G_j, [G_i])| \cdot |Aut(G_i)| = |R(G_i, [G_j])| \cdot |Aut(G_j)|.$$

And if $|Aut(G_j)| = |Aut(G_i)|$ then we have the following 'cancellation' formula relating the sizes of the sets S and R.

Corollary

If $|Aut(G_j)| = |Aut(G_i)|$ then

$$|S(G_j, [G_i])| = |R(G_i, [G_j])|$$

Regarding the elements which conjugate G_i to an element of $S(G_j,[G_i])$ or G_j to an element of $R(G_i,[G_j])$ we have the following, which is, more or less, a variant of Hall's marriage theorem.

(Actually it stems from an earlier result due to König [5] on bijections between sets partitioned into equal numbers of subsets.)

Lemma

If $|Aut(G_j)| = |Aut(G_j)|$ then it is possible to choose a set of coset representatives $\pi(S) = \{\beta_1,\dots,\beta_s\}$ for which each $M \in S(G_j,[G_i])$ is of the from $\beta G_i \beta^{-1}$ for exactly one $\beta \in \pi(S)$, so that $\Phi(\pi(S)) = \pi(R) = \{\beta_1^{-1},\dots,\beta_s^{-1}\}$ parameterizes each element of $R(G_i,[G_j])$, namely that each $N \in R(G_i,[G_j])$ is $\beta^{-1}G_j\beta$ for each $\beta \in \pi(S)$.

We'll see the implications of this a bit later.

Skew Braces and Bi-Skew Braces

We will cite a number of results from Guarnieri and Vendramin [3], but will follow the notational conventions set forth in the first section, to frame things within an ambient symmetric group $B = Perm(X)$ for a set X.

In [3], Guarnieri and Vendramin define a skew left brace to be a group $(A, \star)$ (termed the 'additive group') with an additional group structure $(A, \circ)$ (termed the 'multiplicative' structure) satisfying the skew-brace relation.

Note, they use '$\cdot$' instead of $\star$, but I'm using $\star$ as it's become somewhat standard notation.

Definition

A skew left brace is a finite set X together with two operations $\star$ and $\circ$ such that $(X, \star)$ and $(X, \circ)$ are both groups, where the two group operations satisfy the 'brace relation'

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

where 'a^{-1}' is the inverse of a in $(X, \star)$.

To keep with the point of view of $\star$ and $\circ$ having 'equal footing' we note an important equivalence.

For a set X with two group structures $(X, \star)$ and $(X, \circ)$ one may define $\Lambda : X \to B = Perm(X)$ by $\Lambda(a)(b) = a^{-1} \star (a \circ b)$.

This is somewhat notationally different than the definition given in [3] where they define $\lambda_a(b) = a^{-1} \star (a \circ b)$ which is our $\Lambda(a)(b)$.

Our motivation is to distinguish Λ from the left regular representations $\lambda_\star : X \to X$ and $\lambda_\circ : X \to X$ induced by the $\star$ and $\circ$ operations.

We have then the following.

Proposition

[3, Prop. 1.9,Cor. 1.10] The triple $(X, \star, \circ)$ *being a skew left brace is equivalent to*

$$\Lambda(a \circ b)(c) = \Lambda(a)(\Lambda(b)(c))$$

and

$$\Lambda(a)(b \star c) = \Lambda(a)(b) \star \Lambda(a)(c)$$

for all $a, b, c \in X$.

The triple $(X, \star, \circ)$ *being a skew brace therefore implies that* Λ *is a group homomorphism and that* $\Lambda : ((X, \circ)) \to Aut((X, \star))$.

The connection between skew left braces and holomorphs begins with the above mapping which has image in

$$Aut((X,\star)) \leq Norm_B(\lambda_\star(X)) = \lambda_*(X)Aut((X,\star))$$

where $Norm_B(\lambda_\star(X)) = Hol((X,\star))$.

For $(X,\star,\circ)$, the map Λ yields an embedding

$$(X,\circ) \ni a \mapsto (\lambda_\star(a)\Lambda(a))$$

of $(X,\circ)$ as a regular subgroup of $Hol((X,\star))$, which, in a fairly obvious way, recovers $(X,\circ)$ since

$$\begin{aligned} \lambda_\star(a)\Lambda(a)(b) &= a \star a^{-1} \star (a \circ b) \\ &= a \circ b \end{aligned}$$

and similarly,

$$M = \{(\lambda_{\star}(a)f(a)) \in Hol((X,\star)) \mid a \in X\}$$

is a regular subgroup of $Hol((X,\star))$ if and only if

$$\lambda_{\star}(a)f(a) \mapsto \lambda_{\star}(a)$$

is bijective, and if so, then one yields a group $(X,\circ)$ given by

$$(a \circ b) = \lambda_{\star}(a)f(a)(b) = a \star f(b)$$

.

This is exactly the content of [3, Prop 4.2].

So with the earlier notation in mind, if $(X, \star, \circ)$ is a skew left brace, then for $G_j = \lambda_\star(X)$ and $G_i \cong (X, \circ)$ we have $M = (X, \circ) \in S(G_j, [G_i])$.

That is, the skew left brace structures $(X, \star, \circ)$ where $(X, \star) \cong G_j$ and $(X, \circ) \cong G_i$ are in direct correspondence with $S(G_j, [G_i])$.

But now, as $M \in S(G_j, [G_i])$ then $M = \beta G_i \beta^{-1} \leq Hol(G_j)$ which means, symmetrically, that

$$G_i \leq Hol(\beta^{-1} G_j \beta)$$

namely that $N = \beta^{-1} G_j \beta \in R(G_i, [G_j])$.

The question of isomorphic skew left braces is also readily formulated within $S(G_j, [G_i])$ and $R(G_i, [G_j])$.

In [3] a pair of skew left braces $(A, \cdot, \circ)$ and $(A, \cdot, \times)$ are isomorphic if there is an automorphism $\phi \in Aut(A, \cdot)$ so that $\phi(a \circ b) = \phi(a) \times \phi(b)$.

And in terms of the regular subgroups of $Hol(A)$ one has the following, which we again formulate using the view of $(X, \star)$ and $(X, \circ)$ as regular subgroups of $Perm(X)$.

Proposition

[3, Prop. 4.3] Isomorphic skew brace structures $(X, \star, \circ)$ *and* $(X, \star, \times)$ *correspond to conjugacy classes in* $S(G_j, [G_i])$ *under the action of* $Aut(G_j)$*, where* $G_j = \lambda_\star(X)$ *and* $(X, \circ) \cong (X, \times) \cong G_i$*.*

We can use the reflection principle to further explore this action of $Aut(G_j)$ on $S(G_j, [G_i])$.

If $M_1 = \beta G_i \beta^{-1}$ and for $\mu \in Aut(G_j)$ we define $M_2 = \mu\beta G_i \beta^{-1}\mu^{-1}$ then

$$M_1 = \beta G_i \beta^{-1} \leq Hol(G_j)$$
$$M_2 = \mu\beta G_i \beta^{-1}\mu^{-1} \leq Hol(G_j)$$

and under the passage from S to R, via Φ by passing from β to β^{-1} and $\mu\beta$ to $\beta^{-1}\mu^{-1}$ we have

$$G_i \leq Hol(\beta^{-1} G_j \beta)$$
$$G_i \leq Hol(\beta^{-1}\mu^{-1} G_j \mu\beta) = Hol(\beta^{-1} G_j \beta)$$

namely that $M_1, M_2 \in S(G_j, [G_i])$ correspond to a single

$$N = \beta^{-1}\mu^{-1} G_j \mu\beta = \beta^{-1} G_j \beta$$

in $R(G_i, [G_j])$.

The upshot of this is that elements of $S(G_j,[G_i])$ in the same conjugacy class under the action of $Aut(G_j)$ correspond to the same element of $R(G_i,[G_j])$.

In a symmetric fashion, if $G_i \leq Hol(\alpha G_j \alpha^{-1})$ then for $\nu \in Aut(G_i)$ we have

$$
\begin{aligned}
G_i \leq & Hol(\alpha G_j \alpha^{-1}) \\
& \downarrow \\
G_i = \nu G_i \nu^{-1} \leq & Hol(\nu \alpha G_j \alpha^{-1} \nu^{-1})
\end{aligned}
$$

which means that $Aut(G_i)$ acts on $R(G_i,[G_j])$.

And therefore elements of $R(G_i,[G_j])$ in the same conjugacy class under the action of $Aut(G_i)$ correspond to the same element of $S(G_j,[G_i])$.

We therefore have the following equivalence.

Theorem

If $S(G_j,[G_i])/Aut(G_j)$ is the set of equivalence classes of $S(G_j,[G_i])$ under the action of $Aut(G_j)$ and $R(G_i,[G_j])/Aut(G_i)$ is the set of equivalence classes of the action of $Aut(G_i)$ on $R(G_i,[G_j])$ then

$$|S(G_j,[G_i])/Aut(G_j)| = |R(G_i,[G_j])/Aut(G_i)|$$

via the correspondence given above.

Either of these therefore characterizes the equivalence classes of skew left braces.

Not only do we have the correspondence between the equivalence classes $S(G_j,[G_i])/Aut(G_j)$ and $R(G_i,[G_j])/Aut(G_i)$, there is a correspondence at the level of each orbit.

Proposition

If $M=\beta G_i\beta^{-1}\in S(G_j,[G_i])$ *and* $N=\beta^{-1}G_j\beta\in R(G_i,[G_j])$ *then*

$$|Orb_{Aut(G_j)}(M)|\cdot|Aut(G_i)|=|Orb_{Aut(G_i)}(N)|\cdot|Aut(G_j)|.$$

So we get a kind of 'miniature' version of the reflection principle

$$|S(G_j,[G_i])|\cdot|Hol(G_i)|=|R(G_i,[G_j])|\cdot|Hol(G_j)|$$
$$\updownarrow$$
$$|S(G_j,[G_i])|\cdot|Aut(G_i)|=|R(G_i,[G_j])|\cdot|Aut(G_j)|$$

These statements about the sizes of the orbits under the actions correspond (basically) to the sizes of the double cosets

$$Aut(G_j)\beta Aut(G_i) \xrightarrow{\Phi} Aut(G_i)\beta^{-1}Aut(G_j)$$

although we could phrase this in terms of holomorphs too (with the reflection principle in mind)

$$Hol(G_j)\beta Hol(G_i) \xrightarrow{\Phi} Hol(G_i)\beta^{-1}Hol(G_j)$$

which would correspond to the statement

$$|Orb_{Hol(G_j)}(M)| \cdot |Hol(G_i)| = |Orb_{Hol(G_i)}(N)| \cdot |Hol(G_j)|.$$

If $|Aut(G_j)| = |Aut(G_i)|$ then we can say more about the orbits, the first observation being that

$$|Orb_{Aut(G_j)}(M)| = |Orb_{Aut(G_i)}(N)|$$

and the passage from $\beta \in \pi(S)$ to $\Phi(\beta) = \beta^{-1} \in \pi(R)$ extends in a natural way to a bijection $\hat{\Phi} : S(G_j, [G_i]) \to R(G_i, [G_j])$ where now $\hat{\Phi}(Orb_{Aut(G_j)}(M)) = Orb_{Aut(G_i)}(N)$.

Bi-Skew Braces

Now, a bi-skew brace is a set X together with two operations $\star$ and $\circ$ such that

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

simultaneously.

So if we start with the skew left brace $(X, \star, \circ)$ which yields a regular subgroup $M \leq Hol((X, \star))$, namely that $M = (X, \circ)$, if we reverse the roles of $\star$ and $\circ$ we have that $\lambda_\star(X)$ becomes a regular subgroup of $Hol((X, \circ)) = Hol(M)$.

As such, if $(X,\star) \cong G_i$ and $(X,\circ) \cong G_j$ then if a skew left brace $(X,\star,\circ)$ is such that $(X,\circ,\star)$ is also a skew left brace, we have the following.

Theorem

For $(X,\star,\circ)$ a bi-skew brace as above with $M \leq Hol((X,\star))$, where $M \cong (X,\circ) \cong G_i$ and $(X,\star) \cong G_j$ we have that

$$M \in S(G_j,[G_i]) \cap R(G_j,[G_i])$$

and if $M = \beta G_i \beta^{-1}$ then for $N = \beta^{-1} G_j \beta$ the reflection principle implies that $N \in S(G_i,[G_j]) \cap R(G_i,[G_j])$.

The existence of a bi-skew brace therefore hinges on

$$S(G_j,[G_i]) \cap R(G_j,[G_i])$$

being *non-empty*, and for this we consider the situation where $Hol(G_j) \cong Hol(G_i)$.

In this case, we can assume G_i and G_j are chosen so that $Hol(G_i) = Hol(G_j)$ as subgroups of $B = Perm(X)$ and an element in $S(G_j, [G_i]) \cap R(G_j, [G_i])$ would be a group N, that is isomorphic to G_i, contained in $Hol(G_j)$, and normalized by G_j.

But if $Hol(G_i) = Hol(G_j)$ and since $G_i \triangleleft Hol(G_i)$ obviously, then $G_i \triangleleft Hol(G_j)$ which guarantees at least one such group in this intersection.

i.e. G_i itself lies in $S(G_j, [G_i]) \cap R(G_j, [G_i])$

Moreover, every element of $\mathcal{H}(G_i)$ lies in $S(G_j, [G_i]) \cap R(G_j, [G_i])$ too.

Isomorphic Holomorphs

For groups D and Q where $|D| = |Q|$ one may have that $Aut(D) \cong Aut(Q)$ and $Hol(D) \cong Hol(Q)$.

The classic example of this is the case of dihedral groups D_{2n} and quaternionic groups Q_n of order $4n$ where $Hol(D_{2n}) \cong Hol(Q_n)$.

This implies, therefore, that $Hol(D)$ contains a regular normal subgroup isomorphic to Q and vice versa.

In general, if $N \triangleleft Hol(G_j)$ is regular, where $N \cong G_i$ then obviously $Hol(G_j) \leq Norm_B(N) \cong G_i \rtimes Aut(G_i)$.

But since $Hol(G_i) = G_i A_z$ (for any $z \in X$) where $A_z \cong Aut(G_i)$ then $G_i \cap A_z = \{1\}$ and similarly $N \cap A_z = \{1\}$ and so

$$NA_z \leq Hol(G_j) \leq Norm_B(N) \cong Hol(G_i)$$

and so if $|Aut(G_i)| = |Aut(G_j)|$ then $|NA_z| = |Hol(G_j)| = |Hol(G_i)|$ which implies that $A_z \cong Aut(G_j) \cong Aut(G_i)$.

As such, it is necessary that the respective automorphism groups *must* be isomorphic, but it is not sufficient.

For example

$$Aut(Q_3) \cong Aut(D_6) \cong Aut(C_6 \times C_2) \cong D_6$$

but

$$Hol(Q_3) \cong Hol(D_6) \cong (C_3 \times C_3) \rtimes (C_2 \times D_4)$$

whereas $Hol(C_6 \times C_2) \cong D_3 \times S_4$.

Dihedral and Quaternionic Groups

We have the presentation for the Quaternion group of order $4n$ for $n \geq 3$:

$$Q_n = \langle x, t | x^{2n} = 1, t^2 = x^n, txt^{-1} = x^{-1} \rangle$$

where a typical element is of the form $t^i x^j$ for $i \in \mathbb{Z}_2$ and $j \in \mathbb{Z}_{2n}$ where

$$\begin{aligned}
x^{j_1} x^{j_2} &= x^{j_1+j_2} \\
x^{j_1} t x^{j_2} &= t x^{j_2-j_1} \\
t x^{j_1} x^{j_2} &= t x^{j_1+j_2} \\
t x^{j_1} t x^{j_2} &= x^{j_2-j_1+n} \\
(t^i x^j)^{-1} &= t^i x^{(-1)^{(i+1)} j + in} \\
t^{i_1} x^{j_1} t^{i_1} x^{j_2} &= t^{i_1+i_2} x^{j_2+(-1)^{i_2} j_1 + (i_1 i_2) n}
\end{aligned}$$

The presentation of the Dihedral group D_{2n} of order $4n$ for $n \geq 3$ is

$$D_{2n} = \langle x, t | x^{2n} = 1, t^2 = 1, t^{-1}xt = x^{-1} \rangle$$

where a typical element is of the form $t^i x^j$ for $i \in \mathbb{Z}_2$ and $j \in \mathbb{Z}_{2n}$ where

$$\begin{aligned}
x^{j_1} x^{j_2} &= x^{j_1+j_2} \\
x^{j_1} t x^{j_2} &= t x^{j_2-j_1} \\
t x^{j_1} x^{j_2} &= t x^{j_1+j_2} \\
t x^{j_1} t x^{j_2} &= x^{j_2-j_1} \\
(t^i x^j)^{-1} &= t^i x^{(-1)^{(i+1)} j} \\
t^{i_1} x^{j_1} t^{i_1} x^{j_2} &= t^{i_1+i_2} x^{j_2+(-1)^{i_2} j_1}
\end{aligned}$$

Beyond these two examples, there are others.

Consider the following two groups of order $8p^n$ for p an odd prime.

$$G_1 = \langle t, x, z \mid t^2, x^{p^n}, z^4, txt^{-1}x, [t,z], [x,z] \rangle$$
$$G_2 = \langle t, x, z \mid t^2, x^{p^n}, z^4, txt^{-1}x, tzt^{-1}z, zxz^{-1}x \rangle$$

These are somewhat obscure looking, except that they are reasonably familiar groups.

Specifically $G_1 \cong D_{p^n} \times C_4$ and $G_2 \cong C_{p^n} \rtimes D_4$ where in G_1 the subgroup $\langle t, x \rangle \cong D_{p^n}$ with $\langle z \rangle$ being central, and in G_2, the subgroup $\langle t, z \rangle \cong D_4$ and $\langle x \rangle \cong C_{p^n}$ where t inverts x and z, and z inverts x.

Isomorphic vs. Equal Holomorphs

As we saw above, the groups D_{2n} and Q_n can be given as different group operations on the common set of symbols $X = \{t^a x^b \mid a \in \mathbb{Z}_2; b \in \mathbb{Z}_{2n}\}$.

As such, both $\rho(D_{2n})$ and $\rho(Q_n)$ are permutations on this set. Moreover, the isomorphism group of both can be viewed as permutations of this set, namely

$$Aut(D_{2n}) = Aut(Q_n) = \{\phi_{i,j} \mid i \in \mathbb{Z}_{2n}, j \in U_{2n}\}$$
$$\text{where } \phi_{i,j}(t^a x^b) = t^a x^{ia+jb}$$

where, $Aut(D_{2n}) = Aut(Q_n) \cong Hol(C_{2n})$.

Moreover, if we denote by ρ_d the right regular action of D_{2n} (as permutations of X), and ρ_q the right regular action of Q_n then we have the following *equalities*

$$\rho_q(x^b)\phi_{i,j} = \rho_d(x^b)\phi_{i,j}$$
$$\rho_q(tx^b)\phi_{i,j} = \rho_d(tx^{b+n})\phi_{i+n,j}$$

yielding the fact that, as subgroups of $Perm(\{t^a x^b\})$ we have $Hol(D_{2n}) = Hol(Q_n)$.

In a similar way, the groups G_1 and G_2 are 'built' on the same underlying set $X = \{t^a x^b z^c\}$ and the automorphism group of G_1 and G_2 are isomorphic, but here too can be viewed as identical when viewed as permutations of this set.

This common automorphism group is $A = \langle \phi_{(1,1)}, \phi_{(0,w)}, \psi, \tau \rangle$ where $\langle w \rangle = U_{p^n}$ where

$\phi_{(1,1)}(t) = tx$	$\phi_{(0,w)}(t) = t$	$\psi(t) = t$	$\tau(t) = tz^2$
$\phi_{(1,1)}(x) = x$	$\phi_{(0,w)}(x) = x^w$	$\psi(x) = x$	$\tau(x) = x$
$\phi_{(1,1)}(z) = z$	$\phi_{(0,w)}(z) = z$	$\psi(z) = z^{-1}$	$\tau(z) = z$

where $|\phi_{(1,1)}| = p^n$, $|\phi_{(0,w)}| = \phi(p^n)$, $|\psi| = 2$, and $|\tau| = 2$.

So now, if we denote by ρ_1 and ρ_2 the corresponding right regular representations then

$$Hol(G_1) = \langle \rho_1(t), \rho_1(x), \rho_1(z), \phi_{(1,1)}, \phi_{(0,w)}, \psi, \tau \rangle$$
$$Hol(G_2) = \langle \rho_2(t), \rho_2(x), \rho_2(z), \phi_{(1,1)}, \phi_{(0,w)}, \psi, \tau \rangle$$

where one can show that the bridge between these is what '$\rho_1(z)$' is in $Hol(G_2)$, (or equivalently what $\rho_2(z)$ equals in $Hol(G_1)$)

$$\rho_1(z) = \rho_2(t)\rho_2(z)\psi\tau \in Hol(G_2)$$
$$\rho_2(z) = \rho_1(t)\rho_1(z)\psi\tau \in Hol(G_1)$$

so that $Hol(G_1)$ may be regarded as equal to $Hol(G_2)$.

Beyond just pairs with isomorphic holomorphs

We've just seen how having $Hol(G_i) \cong Hol(G_j)$ implies the existence of a bi-skew brace, but are there larger collections of groups (of the same order) with isomorphic/equal holomorphs?

Yes, although these results are (at the moment) computational:

In degree 48 there are 4 groups with isomorphic holomorphs:

$$(C_3 \times D_4) \rtimes C_2$$
$$(C_3 \rtimes Q_2) \rtimes C_2$$
$$(C_3 \times Q_2) \rtimes C_2$$
$$C_3 \rtimes Q_4$$

where Q_2 is the usual 8 element quaternion group, Q_4 is the order 16 quaternion group, and D_4 is the fourth dihedral group.

Going still further, in degree 96 we have 8 groups with isomorphic holomorphs:

$$C_3 \rtimes (C_4 \rtimes Q_2)$$
$$C_3 \rtimes ((C_2 \times C_2).(C_2 \times C_2 \times C_2))$$
$$(C_4 \rtimes C_4) \times D_3$$
$$C_3 \rtimes ((C_4 \times C_4) \rtimes C_2)$$
$$C_3 \rtimes ((C_4 \times C_2 \times C_2) \rtimes C_2)$$
$$C_3 \rtimes ((C_2 \times Q_2) \rtimes C_2)$$
$$C_3 \rtimes ((C_4 \times C_2 \times C_2) \rtimes C_2)$$
$$C_3 \rtimes ((C_2 \times Q_2) \rtimes C_2)$$

and these, like the degree 48 cases in the previous slide, and the order $8p^n$ groups G_1 and G_2, have certain structural similarities.

Even more recently discovered (i.e. yesterday) it seems that there are **many** groups of order 192 with isomorphic holomorphs.

The largest 'cluster' of these is a family of 52 different groups.

One final observation to make is that for those $\{G_k\}$ with isomorphic holomorphs, the fact they have isomorphic holomorphs implies that they mutually normalize each other.

Thank you!

Appendix - Proving the (Bi-)Skew Brace Relations Explicitly

What we wish to demonstrate is that the set $X = \{t^i x^j \mid i \in \mathbb{Z}_2, j \in \mathbb{Z}_{2n}\}$ together with $(X, \star) \cong Q_n$ and $(X, \circ) \cong D_{2n}$ satisfy the skew-brace relations

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

which we shall denote

$$D(a, Q(b, c)) = Q(Q(D(a, b), Q^{-1}(a)), D(a, c))$$

and similarly if $(X, \star) \cong D_{2n}$ and $(X, \circ) \cong Q_n$ which we shall denote

$$Q(a, D(b, c)) = D(D(Q(a, b), D^{-1}(a)), Q(a, c))$$

so that the two group operations on X yield a bi-skew brace.

$D(a, Q(b, c)) = Q(Q(D(a, b), Q^{-1}(a)), D(a, c))$

Let $a = t^{i_1}x^{j_1}$, $b = t^{i_2}x^{j_2}$, $c = t^{i_3}x^{j_3}$ then

$$D(a, Q(b, c)) = t^{I_L}x^{J_L}$$
$$Q(Q(D(a, b), Q^{-1}(a)), D(a, c)) = t^{I_R}x^{J_R}$$

where

$$\begin{aligned}
I_L &= i_1 + i_2 + i_3 \\
I_R &= i_1 + i_2 + i_3 \\
J_L &= j_3 + (-1)^{i_3} j_2 + i_2\, i_3\, n + (-1)^{i_2+i_3} j_1 \\
J_R &= j_3 + (-1)^{i_3} j_1 + (-1)^{i_1+i_3} \left((-1)^{i_1+1} j_1 + i_1\, n + (-1)^{i_1} \left(j_2 + (-1)^{i_2} j_1\right) + (i_1 + i_2)\, i_1\, n\right) \\
&\quad + i_2\, (i_1 + i_3)\, n
\end{aligned}$$

That $I_L = I_R$ is obvious, and for the difference:

$$J_L - J_R = (-1)^{i_3} j_2 + i_2\, i_3\, n + (-1)^{i_2+i_3} j_1 - (-1)^{i_3} j_1 - \\ (-1)^{i_1+i_3} \left((-1)^{i_1+1} j_1 + i_1\, n + (-1)^{i_1} \left(j_2 + (-1)^{i_2} j_1 \right) + (i_1 + i_2)\, i_1\, n \right)$$

it's basically a case by case analysis to show that this is always 0

$Q(a, D(b, c)) = D(D(Q(a, b), D^{-1}(a)), Q(a, c))$

Similarly, $Q(a, D(b, c)) = t^{I_L} x^{J_L}$ and
$D(D(Q(a, b), D^{-1}(a)), Q(a, c)) = t^{I_R} x^{J_R}$ where

$$
\begin{aligned}
I_L &= i_1 + i_2 + i_3 \\
I_R &= i_1 + i_2 + i_3 \\
J_L &= j_3 + (-1)^{i_3} j_2 + (-1)^{i_2+i_3} j_1 + i_1\, (i_2 + i_3)\, n \\
J_R &= j_3 + (-1)^{i_3} j_1 + i_1\, i_3\, n \\
&\quad + (-1)^{i_1+i_3} \left((-1)^{i_1+1} j_1 + (-1)^{i_1} \left(j_2 + (-1)^{i_2} j_1 + i_1\, i_2\, n\right)\right)
\end{aligned}
$$

and here too, we can show that $I_L = I_R$ and $J_L = J_R$.

For the groups

$$G_1 = \langle t, x, z \mid t^2, x^{p^n}, z^4, txt^{-1}x, [t, z], [x, z] \rangle$$
$$G_2 = \langle t, x, z \mid t^2, x^{p^n}, z^4, txt^{-1}x, tzt^{-1}z, zxz^{-1}x \rangle$$

we can also demonstrate that the (bi-)skew brace relations hold.

In both cases, each group consists of expressions of the form

$$X = \{t^i x^j z^k \mid i \in \mathbb{Z}_2; j \in \mathbb{Z}_{p^n}; k \in \mathbb{Z}_4\}$$

and so any potential bi-skew brace structure is defined on this single set X.

We now need to determine the multiplication formulae, which arise from the presentations above.

In G_1 the following holds:

$$(t^{i_1}x^{j_1}z^{k_1})(t^{i_2}x^{j_2}z^{k_2}) = t^{i_1+i_2}x^{j_2+(-1)^{i_1}j_1}z^{k_1+k_2}$$

which is quite similar to that for D_{p^n} obviously since $\langle z \rangle$ is central in G_1. We easily deduce from this that

$$(t^i x^j z^k)^{-1} = t^i x^{(-1)^{i+1}j} z^{-k}$$

which we shall need later.

In G_2 the following holds:

$$
\begin{aligned}
(t^{i_1}x^{j_1}z^{k_1})(t^{i_2}x^{j_2}z^{k_2}) &= t^{i_1}x^{j_1}t^{i_2}z^{(-1)^{i_2}k_2}x^{j_2}z^{k_2} \\
&= t^{i_1+i_2}x^{(-1)^{i_2}j_1}z^{(-1)^{i_2}k_1}x^{j_1}z^{k_2} \\
&= t^{i_1+i_2}x^{(-1)^{i_2}j_1}x^{(-1)^{(-1)^{i_2}k_1}j_2}z^{(-1)^{i_2}k_1}z^{k_2} \\
&= t^{i_1+i_2}x^{(-1)^{i_2}j_1+(-1)^{(-1)^{i_2}k_1}j_2}z^{(-1)^{i_2}k_1}z^{k_2} \\
&\downarrow \text{ since } k_1 = -k_1 \ (mod\ 2) \\
&= t^{i_1+i_2}x^{(-1)^{i_2}j_1+(-1)^{k_1}j_2}z^{(-1)^{i_2}k_1+k_2}
\end{aligned}
$$

which is more complicated due to z being non-central in G_2.

And we also deduce that

$$(t^i x^j z^k)^{-1} = t^i x^{(-1)^{i+k+1} j_1} z^{(-1)^{i+1} k}$$

which is the inverse for G_2.

So for the set X, if we define (for some notational consistency with the above examples) $D = (X, \circ) \cong G_1$ and $Q = (X, \star) \cong G_2$ then the skew brace relation

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

again translates to the 'function' formulation

$$D(a, Q(b, c)) = Q(Q(D(a, b), Q^{-1}(a)), D(a, c))$$

as we used above.

And in reverse, if we let $D = (X, \star) \cong G_1$ and $Q = (X, \circ) \cong G_2$ which we express in function form as

$$Q(a, D(b, c)) = D(D(Q(a, b), D^{-1}(a)), Q(a, c))$$

and we wish to verify both to confirm that we have a bi-skew brace structure on X arising from these two groups.

$D(a, Q(b, c)) = Q(Q(D(a, b), Q^{-1}(a)), D(a, c))$

We explore the first of the two brace relations.
Let $a = t^{i_1}x^{j_1}z^{k_1}$, $b = t^{i_2}x^{j_2}z^{k_2}$, $c = t^{i_3}x^{j_3}z^{k_3}$ then

$$D(a, Q(b, c)) = t^{I_L}x^{J_L}z^{K_L}$$
$$Q(Q(D(a, b), Q^{-1}(a)), D(a, c)) = t^{I_R}x^{J_R}z^{K_R}$$

where

$$
\begin{aligned}
I_L &= i_1 + i_2 + i_3 \\
I_R &= i_1 + i_2 + i_3 \\
&\downarrow \\
I_L - I_R &= 0 \\
J_L - J_R &= (-1)^{i_3} j_2 + (-1)^{i_2+i_3} j_1 - (-1)^{2\,i_1+i_3} j_2 - (-1)^{2\,i_1+i_3+i_2} j_1 + \\
&(-1)^{2\,i_1+i_3+2\,k_1+k_2} j_1 - (-1)^{k_2+i_3} j_1 \\
&= (-1)^{i_3} j_2 + (-1)^{i_2+i_3} j_1 - (-1)^{i_3} j_2 - (-1)^{i_3+i_2} j_1 + \\
&(-1)^{i_3+k_2} j_1 - (-1)^{k_2+i_3} j_1 \\
&= (-1)^{i_3+k_2} j_1 - (-1)^{k_2+i_3} j_1 \\
&= 0 \\
K_L - K_R &= (-1)^{i_3} k_2 - (-1)^{i_3} k_2 \\
&= 0
\end{aligned}
$$

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

For the reversed case, we consider, for a, b and c as above, the expressions:

$$\begin{aligned} Q(a, D(b,c)) &= t^{I_L} x^{J_L} z^{K_L} \\ D(D(Q(a,b), D^{-1}(a)), Q(a,c)) &= t^{I_R} x^{J_R} z^{K_R} \end{aligned}$$

to see if $I_L = I_R$, $J_L = J_R$, and $K_L = K_R$ but these verifications aren't too difficult.

We have

$$
\begin{aligned}
I_L &= i_1 + i_2 + i_3 \\
I_R &= i_1 + i_2 + i_3 \\
&\downarrow \\
I_L - I_R &= 0 \\
J_L - J_R &= (-1)^{i_2+i_3} j_1 + (-1)^{k_1+i_3} j_2 - (-1)^{i_3} j_1 + \\
&(-1)^{2\,i_1+i_3} j_1 - (-1)^{2\,i_1+i_3+i_2} j_1 - (-1)^{2\,i_1+i_3+k_1} j_2 \\
&= (-1)^{i_2+i_3} j_1 + (-1)^{k_1+i_3} j_2 - (-1)^{i_3} j_1 + \\
&(-1)^{i_3} j_1 - (-1)^{i_3+i_2} j_1 - (-1)^{i_3+k_1} j_2 \\
&= 0
\end{aligned}
$$

$$
\begin{aligned}
K_L - K_R &= (-1)^{i_2+i_3}k_1 - (-1)^{i_2}k_1 + k_1 - (-1)^{i_3}k_1 \\
&= (-1)^{i_2+i_3}k_1 + (-1)^{i_2+1}k_1 + k_1 + (-1)^{i_3+1}k_1 \\
&= \begin{cases} (-1)^{i_3}k_1 - k_1 + k_1 + (-1)^{i_3+1}k_1 & i_2 = 0 \\ (-1)^{1+i_3}k_1 + k_1 + k_1 + (-1)^{i_3+1}k_1 & i_2 = 1 \end{cases} \\
&= \begin{cases} k_1 - k_1 + k_1 - k_1 & i_2 = 0, i_3 = 0 \\ k_1 + k_1 + k_1 + k_1 & i_2 = 1, i_3 = 1 \end{cases} \\
&= 0 \text{ (recall that } k_1 \in \mathbb{Z}_4)
\end{aligned}
$$

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

N.P. Byott.
Uniqueness of Hopf Galois structure of separable field extensions.
Comm. Algebra, 24:3217–3228, 1996.

L. Childs.
On the Hopf-Galois theory for separable field extensions.
Comm. Algebra, 17(4):809–825, 1989.

L. Guarnieri and L. Vendramin.
Skew braces and the yang baxter equation.
Math. Comp., 86:2519–2534, 2017.

T. Kohl.
Classification of the Hopf Galois structures on prime power radical extensions.
J. Algebra, 207:525–546, 1998.

D. König.
Über graphen und ihre anwendung auf determinantentheorie und mengenlehre.
Math. Ann., 77:453–465, 1916.