Multiple Holomorphs and Hopf-Galois Structures

Timothy Kohl

Boston University

May 24, 2018

Hopf-Galois Theory

An extension K/k is Hopf-Galois if there is a k-Hopf algebra H and a k-algebra homomorphism $\mu : H \to End_k(K)$ such that

- $\mu(ab) = \sum_{(h)} \mu(h_{(1)}(a)\mu(h_{(2)})(b)$
- $K^H = \{a \in K \mid \mu(h)(a) = \epsilon(h)a \ \forall h \in H\} = k$
- μ induces $I \otimes \mu : K\#H \stackrel{\cong}{\to} End_k(K)$

Although Hopf-Galois theory was developed to address the failure of ordinary Galois theory for non-separable extensions, a prime example is when K/k is Galois with group G, for then $H = k[G]$ acts to make K/k Hopf-Galois.

Greither and Pareigis [4] detailed the requirements for a separable extension K/k (which may or may not be Galois) to be Hopf-Galois.

What was also observed (which are the cases we will examine here), is that an already Galois extension K/k with $G = Gal(K/k)$ can be Hopf-Galois with respect to other k-Hopf algebras, besides $k[G]$.

Normal or not, the Greither-Pareigis theory enumerates the different possible structures.

Let K/k be a finite Galois extension with $G = Gal(K/k)$. G acting on itself by left translation yields an embedding

$$\lambda : G \hookrightarrow B = Perm(G)$$

Definition: $N \leq B$ is *regular* if N acts transitively and fixed point freely on G.

Theorem

[4] The following are equivalent:

- *There is a k-Hopf algebra H such that K/k is H-Galois*
- *There is a regular subgroup $N \leq B$ s.t. $\lambda(G) \leq Norm_B(N)$ where N yields $H = (K[N])^G$.*

We note that N must necessarily have the same order as G, but need not be isomorphic.

To organize the enumeration of the Hopf-Galois structures, one considers

$$R(G) = \{N \leq B \mid N \text{ regular and } \lambda(G) \leq Norm_B(N)\}$$

which are the totality of all N giving rise to H-G structures, which we can subdivide into isomorphism classes given that N need not be isomorphic to G, to wit, let

$$R(G, [M]) = \{N \in R(G) \mid N \cong M\}$$

for each isomorphism class $[M]$ of group of order $|G|$.

Holomorphs and Multiple Holomorphs

From the regular subgroup $\lambda(G) \leq B$ one defines the classical notion of the holomorph $Hol(G)$ as $Norm_B(\lambda(G)) = \rho(G)Aut(G)$ where $\rho(G)$ is the right regular representation and $Aut(G)$ is the set of those elements of the normalizer that fix the identity of G which is, of course, isomorphic to the abstract formulation as $G \rtimes Aut(G)$.

Also, for any other regular subgroup $N \leq B$, the normalizer $Norm_B(N)$ is isomorphic to the holomorph of N as well.

In the formulation of $Norm_B(\lambda(G))$, one has in fact that it equals $\lambda(G)Aut(G)$ as well, and in fact, that $Norm_B(\lambda(G)) = Norm_B(\rho(G))$.

For a non-Abelian group G, $\lambda(G)$ and $\rho(G)$ are distinct but have the same normalizers.

This is the prime example of what one considers when formulating the so-called *multiple holomorph* of G.

For $\lambda(G) \leq B = Perm(G)$, one can ask for what other regular subgroups $N \leq B$ have the same normalizer, (holomorph) as G, namely $Hol(N) = Hol(G)$.

The equality of holomorphs implies that $N \leq Hol(G)$ already. If we restrict our attention to those N which are isomorphic to G then N is a conjugate of $\lambda(G)$ by regularity.

So for such an N, where $\tau \in B$ is such that $\tau\lambda(G)\tau^{-1} = N$ then

$$\begin{aligned}
\tau Norm_B(\lambda(G))\tau^{-1} &= Norm_B(\tau\lambda(G)\tau^{-1}) \\
&= Norm_B(N) \\
&= Norm_B(\lambda(G))
\end{aligned}$$

which means $\tau \in Norm_B(Hol(G))$, and the converse is true as well.

If we define

$$\mathcal{H}(G) = \{N \leq Hol(G) \mid N \text{ regular, } N \cong G \text{ and } Hol(N) = Hol(G)\}$$

then the multiple holmorph is $NHol(G) = Norm_B(Hol(G))$ where $Orb_{NHol(G)}(\lambda(G)) = \mathcal{H}(G)$.

As $Hol(G) \triangleleft NHol(G)$ one can look at $T(G) = NHol(G)/Hol(G)$ which acts *regularly* on $\mathcal{H}(G)$.

We will see soon the application of $NHol(G)$ to the enumeration of $R(G, [M])$.

The size of $T(G)$ has been determined for various classes of groups.

For example, Miller in 1908 determined $T(G)$ for G finite abelian.
We note that if $G = G_1 \times G_2$ where $gcd(|G_1|, |G_2|) = 1$ then, of course, $Aut(G) \cong Aut(G_1) \times Aut(G_2)$ but the same holds for $Hol(G)$ and $NHol(G)$.
If G is abelian of odd order then $T(G)$ is trivial.
Let $|G| = 2^m$ for some m.

- $G \cong C_{2^{2+\epsilon}} \times C_{2^{2+\epsilon-\delta}} \times \overline{G}$ for $\epsilon > \delta > 0$ and $exp(\overline{G}) < 2^{2+\epsilon-\delta}$ implies $T(G) \cong C_2 \times C_2$
- $G \cong C_{2^{2+\epsilon}} \times C_{2^{2+\epsilon-\delta}} \times C_{2^{2+\epsilon-\delta}} \times \overline{G}$ for $\epsilon > \delta > 0$ and $exp(\overline{G}) \leq 2^{2+\epsilon-\delta}$ implies $T(G) \cong C_2$
- $G \cong C_{2^m}$ for $m \geq 3$ implies $T(G) \cong C_2$
- $G \cong C_4 \times C_2$ implies $T(G) \cong C_2$
- $G \cong C_{2^{3+\epsilon}} \times C_{2^{3+\epsilon}} \times \overline{G}$ for $\epsilon \geq 0$ and $exp(\overline{G}) \leq 2^{3+\epsilon}$ implies $T(G) \cong C_2$
- otherwise $|T(G)| = 1$

More recent examples:

- [2] If G is a non-Abelian simple group then $T(G) \cong \mathbb{Z}_2$.
- [5] If $n = 2^e p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$ then

$$T(D_n) \cong \{x \in U_n \mid x^2 = 1\} \cong \begin{cases} (\mathbb{Z}_2)^r & e <= 1 \\ (\mathbb{Z}_2)^{r+1} & e = 2 \\ (\mathbb{Z}_2)^{r+2} & e \geq 3 \end{cases}$$

  where $U_n = (\mathbb{Z}_n)^*$.
- [1] If G is a centerless perfect group then $T(G) \cong (\mathbb{Z}_2)^n$ where n is the number of components in the Remak-Krull-Schmidt decomposition of G as an $Aut(G)$-group.
- [3] There is a class 2 p-group G such that $T(G) \cong Hol(C_p)$.
- [3] There are class 2 p-groups such that $T(G)$ contains a non-Abelian subgroup of order $(p-1) \cdot p^{\binom{n}{2} \cdot \binom{n+1}{2}}$.

$R(G,[M])$ as $Hol(G)$-set

The enumeration of $R(G,[M])$ for different pairings of groups $(G,[M])$ of the same order has been done using a variety of techniques, usually based on structural and order conditions.

We are also going to consider properties of $R(G,[M])$ more broadly, by focusing less on specific classes of groups (mostly) but rather on the condition which defines membership in this set.

The result will be a conjecture (theorem?) which will give a bound on $|R(G,[M])|$ framed in fairly broad terms, not so specifically keyed to particular structural properties.

As the normalizer of a regular subgroup of $N \leq B$ is canonically isomorphic to $Hol(N) \leq Perm(N)$, we shall abuse notation slightly and call $Hol(N) = Norm_B(N)$ for $N \in R(G, [M])$.

As indicated, we will focus on the condition $\lambda(G) \leq Hol(N)$.
If $h \in Hol(G)$ we have

$$\begin{array}{c} h\lambda(G)h^{-1} \leq hHol(N)h^{-1} \\ \downarrow \\ \lambda(G) \leq Hol(hNh^{-1}) \end{array}$$

which means that $hNh^{-1} \in R(G, [M])$ as well.

As such $R(G, [M])$ is a $H = Hol(G)$-set.

Since $Hol(G)$ can be quite large, a natural question to ask is whether $R(G,[M])$ is a transitive $Hol(G)$-set?

As it turns out, the answer is No.

Later on, we will consider an 'action' on $R(G,[M])$ which is a bit 'more' transitive.

For a given N for $H = Hol(G)$, we can compute the isotropy subgroup H_N, namely

$$\begin{aligned} H_N &= \{h \in Hol(G) \mid hNh^{-1} = N\} \\ &= Hol(G) \cap Hol(N) \end{aligned}$$

so, by the Orbit-Stabilizer theorem, the orbit $Orb_H(N)$ of a given N has size

$$[H : H_N] = \frac{|Hol(G)|}{|Hol(G) \cap Hol(N)|}.$$

We are especially interested in when $Orb_H(N) = \{N\}$, namely when $N \in R(G,[M])_H$.

This occurs when $Hol(G) \cap Hol(N) = Hol(G)$ which leads to two different cases.

If $Hol(G) \leq Hol(N)$ then clearly $Hol(G) \cap Hol(N) = Hol(G)$.

If $Hol(N) \leq Hol(G)$ then we must have that $Hol(G) \leq Hol(N)$ as well since otherwise the intersection would be properly smaller than $Hol(G)$.

As such, if $N_1, N_2, \ldots, N_r$ are the orbit representatives of the non-trivial orbits of H acting on $R(G,[M])$ then

$$\begin{aligned}|R(G,[M])| &= |R(G,[M])_H| + \sum_{i=1}^{r} |Orb_H(N_i)| \\ &= |R(G,[M])_H| + \sum_{i=1}^{r} [Hol(G) : Hol(G) \cap Hol(N_i)]\end{aligned}$$

which, if we want to come up with a formulation similar to the class equation, makes one wonder if $|R(G,[M])_H|$ is the cardinality of a particular group, analgous to the role that $Z(G)$ plays in the study of conjugacy classes.

[Note: $R(G,[M])_H$ *could* be empty when $G \ncong M$, for example if M has a smaller automorphism group than G.]

If $[M]=[G]$ then there is a natural analog, since then $|Hol(N)|=|Hol(G)|$ obviously, so that $Hol(G)\cap Hol(N)=Hol(G)$ implies that $Hol(G)=Hol(N)$.

As such N is a conjugate of $\lambda(G)$ by an element of $T(G)$.

Moreover, since for regular subgroups of B, two subgroups are isomorphic if and only if they're conjugate, then if $G\cong N$ such N are exactly determined by this quotient, that is $|R(G,[G])_H|=[NHol(G):Hol(G)]=|T(G)|$.

As such, the above equation becomes:

$$|R(G,[G])| = |T(G)| + \sum_{i=1}^{r} [Hol(G) : Hol(G) \cap Hol(N_i)] \qquad (1)$$

where, again, $N_1, \ldots, N_r$ are the orbit representatives for the non-trivial orbits of $R(G,[G])$ under the action of $Hol(G)$.

We'll get back to $R(G,[G])$ in a bit.

Action by Aut(G)

Simplification.

Since $Hol(G) = \rho(G)Aut(G) = \lambda(G)Aut(G) = Aut(G)\lambda(G)$ then if $N \in R(G,[M])$ and $h = \alpha\lambda(g) \in Hol(G)$ then

$$\begin{aligned} hNh^{-1} &= \alpha\lambda(g)N\lambda(g)^{-1}\alpha^{-1} \\ &= \alpha N\alpha^{-1} \end{aligned}$$

so that $Orb_{Hol(G)}(N) = Orb_{Aut(G)}(N)$ and concordantly

$$[Hol(G) : Hol(G) \cap Hol(N)] = [Aut(G) : Aut(G) \cap Hol(N)]$$

for each N.

If we follow the convention that

$$Aut(G) = \{\pi \in Hol(G) \mid \pi(i_G) = i_G\}$$

then if $N \in R(G,[M])$ then $Hol(N) = Norm_B(N) = NAut(N)$ where

$$Aut(N) \cong \{\pi \in Hol(N) \mid \pi(i_G) = i_G\}.$$

and so $Aut(G) \cap Hol(N) = Aut(G) \cap Aut(N)$.

If $A = Aut(G)$ then the orbit formula becomes:

$$
\begin{aligned}
|R(G,[M])| &= |R(G,[M])_A| + \sum_{i=1}^{r} |Orb_A(N_i)| \\
&= |R(G,[M])_A| + \sum_{i=1}^{r} [Aut(G) : Aut(G) \cap Aut(N_i)]
\end{aligned}
$$

for $N_1, \ldots, N_r$ the non-trivial orbit representatives, and, again, for $R(G,[G])$ we get

$$
|R(G,[G])| = |T(G)| + \sum_{i=1}^{r} [Aut(G) : Aut(G) \cap Aut(N_i)]
$$

with $T(G)$ is the multiple holomorph as discussed earlier.

The multiple holomorph does not appear only in the $(G, [G])$ case, but more generally.

Recall a frequently quoted fact used in the enumeration of $R(G, [M])$, namely that

$$N \in R(G, [M]) \text{ implies } N^{opp} = Cent_B(N) \in R(G, [M])$$

since $Hol(N) = Hol(N^{opp})$ which, if $[M]$ is non-Abelian, means that $N \neq N^{opp}$ and so that $2 \big| |R(G, [M])|$.

However, since $N \cong N^{opp}$ then $N^{opp} = \tau N \tau^{-1}$ for some $\tau \in B$.

And since $Hol(N) = Hol(N^{opp})$ then $\tau \in T(N)$, the multiple holomorph of N.

Indeed, for a non-Abelian group N, one has that $|T(N)| \geq 2$ since it at least contains the element which conjugates N to its opposite.

More generally, for any regular $N \leq B$ one may write $T(N)$ to be the group of those $\tau \in B$ such that $Hol(N) = Hol(\tau N \tau^{-1})$ and that for each N in a given isomorphism class, all $T(N)$ are isomorphic.

This yields:

Theorem

For each isomorphism class $[M]$ of groups where $|M| = |G|$, one has that $|T(M)|$ divides $|R(G,[M])|$.

This is quite interesting since for a given $N \in R(G,[M])$ where $\alpha \in Aut(G)$ and $\tau \in T(N)$ one has

$$\begin{tikzcd} N \arrow[r, "\alpha"] \arrow[d, "\tau"'] & \alpha(N) \\ \tau(N) & \end{tikzcd}$$

where both $\alpha(N)$ and $\tau(N)$ lie in $R(G,[M])$ where $|Orb_{T(N)}(N)| = |T(M)|$.

The idea we will explore is this simultaneous action of $Aut(G)$ and $T(M)$, where all $T(N)$ are isomorphic to $T(M)$ since each $N \in R(G,[M])$.

This is how the action of $T(M)$ must be understood since, for those N in $R(G,[M])$ which have the same holomorph, there is the group $T(N)$ whose orbit is this subset. As such, $R(G,[M])$ is divided into equivalence classes, each of size $|T(M)|$.

What we look to obtain is a bound on $|R(G,[M])|$ arising from these actions by $Aut(G)$ and $T(M)$.

As observed earlier, the action of $Aut(G)$ is neither transitive, nor fixed point free, and the action by $T(M)$ is fixed point free, but not transitive.

Conjecture: Is it possible (or when is it the case) that

$$|R(G,[M])| \leq |T(M)| \cdot |Aut(G)|$$

for groups $(G,[M])$ of some order n?

In the enumeration of $R(G,[M])$ we have that $|T(M)|$ divides

$$|R(G,[M])_A| + \sum_{i=1}^{r}[Aut(G) : Aut(G)\cap Aut(N_i)]$$

but it's a slightly delicate question as to *how* it divides the terms.

And applied to $R(G,[G])$ where

$$|R(G,[G])| = |T(G)| + \sum_{i=1}^{r}[Aut(G) : Aut(G)\cap Aut(N_i)]$$

then $|T(G)|$ divides the first term on the right and must therefore divide $\sum_{i=1}^{r}[Aut(G) : Aut(G)\cap Aut(N_i)]$ as well.

Let's first establish this for some well understood classes of examples.

If p, q are prime, where $p > q$ then there are one $[p \not\equiv 1 \ (mod q)]$ or two $[p \equiv 1 \ (mod q)]$ groups of order pq and $R(G,[M])$ was computed by Byott.

$G \setminus M$	C_{pq}	$C_p \rtimes C_q$
C_{pq}	1	$2(q-2)$
$C_p \rtimes C_q$	p	$2(p(q-2)+1)$

Now, $|Aut(C_{pq})| = \phi(p)\phi(q)$, $|Aut(C_p \rtimes C_q)| = p(p-1)$, and also $|T(C_{pq})| = 1$, $|T(C_p \rtimes C_q)| = 2$ which yields the following parallel table for $|Aut(G)| \cdot |T(M)|$

$G \setminus M$	C_{pq}	$C_p \rtimes C_q$
C_{pq}	$(p-1)(q-1)$	$2(p-1)(q-1)$
$C_p \rtimes C_q$	$p(p-1)$	$2(p(p-1))$

and it's clear that $|R(G,[M])| \leq |Aut(G)| \cdot |T(M)|$ for each pairing.

Let's look at some empirical evidence, first in degree 6 which we already know works.

```
gap> Read("../RLIB/R6.g");
gap> Read("conjecture.g");
gap> conjecture(6);
[ true, true ]              <- |R(G,[M])| <= |Aut(G)|
[ true, true ]

[ true, true ]              <- |R(G,[M])| <= |Aut(G)| x |T(M)|
[ true, true ]
gap> List([1..Size(G[6])],t->Size(AutG[6][t]));
[ 6, 2 ]
gap> List([1..Size(G[6])],t->Index(NHolG[6][t],HolG[6][t]));
[ 2, 1 ]
gap> aprint(List([1..Size(G[6])],i->List([1..Size(G[6])],j->Size(R[6][i][j]))));
[ 2, 3 ]
[ 2, 1 ]
gap> aprint(List([1..Size(G[6])],i->List([1..Size(G[6])],j->Size(AutG[6][i])*Index(NHolG
[ 12, 6 ]
[ 4, 2 ]
gap>
```

```
gap> Read("../RLIB/R8.g");
gap> Read("conjecture.g");
gap> conjecture(8);
[ true, true, true, true, true ]          <- |R(G,[M])| <= |Aut(G)|
[ true, false, true, true, true ]
[ true, false, true, true, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]

[ true, true, true, true, true ]          <- |R(G,[M])| <= |Aut(G)| x |T(M)|
[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]
gap> List([1..Size(G[8])],t->Size(AutG[8][t]));
[ 4, 8, 8, 24, 168 ]
gap> List([1..Size(G[8])],t->Index(NHolG[8][t],HolG[8][t]));
[ 2, 2, 2, 2, 1 ]
gap> aprint(List([1..Size(G[8])],i->List([1..Size(G[8])],j->Size(R[8][i][j]))));
[ 2, 0, 2, 2, 0 ]
[ 4, 10, 6, 2, 4 ]
[ 2, 14, 6, 2, 6 ]
[ 6, 6, 6, 2, 2 ]
[ 0, 42, 42, 14, 8 ]
gap> aprint(List([1..Size(G[8])],i->List([1..Size(G[8])],j->Size(AutG[8][i])*Index(NHolG[8][j],HolG[8][j]
[ 8, 8, 8, 8, 4 ]
[ 16, 16, 16, 16, 8 ]
[ 16, 16, 16, 16, 8 ]
[ 48, 48, 48, 48, 24 ]
[ 336, 336, 336, 336, 168 ]
```

Looking at the orbits with respect to the actions of $Aut(G)$ and $T(M)$, some interesting patterns can be seen.

```
gap> orbitlist(6);
R(S3,[S3]) i=1 j=1
[ [ 1 ], [ 2 ] ]   <- orbits with respect to Aut(G) {\lambda(G) \rho(G)}
[ [ 1, 2 ] ]       <- orbits with respect to T(M)

R(S3,[C6]) i=1 j=2
[ [ 1, 3, 2 ] ]
[ [ 1 ], [ 2 ], [ 3 ] ]         <- note T(C6) is trivial


R(C6,[S3]) i=2 j=1
[ [ 1 ], [ 2 ] ]                <- Hol(G) is contained in Hol(N_i)
[ [ 1, 2 ] ]

R(C6,[C6]) i=2 j=2
[ [ 1 ] ]
[ [ 1 ] ]
```

```
gap> orbitlist(8);
R(C8,[C8]) i=1 j=1
[ [ 1 ], [ 2 ] ]
[ [ 1, 2 ] ]

R(C8,[C4 x C2]) i=1 j=2

R(C8,[D8]) i=1 j=3
[ [ 1 ], [ 2 ] ]
[ [ 1, 2 ] ]

R(C8,[Q8]) i=1 j=4
[ [ 1 ], [ 2 ] ]
[ [ 1, 2 ] ]

R(C8,[C2 x C2 x C2]) i=1 j=5
```

```
R(C4 x C2,[C8]) i=2 j=1
[ [ 1, 2, 4, 3 ] ]
[ [ 1, 2 ], [ 3, 4 ] ]

R(C4 x C2,[C4 x C2]) i=2 j=2
[ [ 1 ], [ 9, 7 ], [ 10, 8 ], [ 5, 3 ], [ 6, 4 ], [ 2 ] ]
[ [ 1, 2 ], [ 3, 4 ], [ 5, 6 ], [ 7, 8 ], [ 9, 10 ] ]

R(C4 x C2,[D8]) i=2 j=3
[ [ 1, 6 ], [ 3, 4 ], [ 2, 5 ] ]
[ [ 1, 2 ], [ 3, 4 ], [ 5, 6 ] ]

R(C4 x C2,[Q8]) i=2 j=4
[ [ 1, 2 ] ]
[ [ 1, 2 ] ]

R(C4 x C2,[C2 x C2 x C2]) i=2 j=5
[ [ 1 ], [ 2, 3 ], [ 4 ] ]
[ [ 1 ], [ 2 ], [ 3 ], [ 4 ] ]
```

```
R(D8,[C8]) i=3 j=1
[ [ 1, 2 ] ]
[ [ 1, 2 ] ]

R(D8,[C4 x C2]) i=3 j=2
[ [ 1, 10 ], [ 9, 2 ], [ 11, 13, 4, 6 ], [ 14, 12, 5, 3 ], [ 8, 7 ] ]
[[ 1, 2 ], [ 3, 4 ], [ 5, 6 ], [ 7, 8 ], [ 9, 10 ], [ 11, 12 ], [ 13, 14]

R(D8,[D8]) i=3 j=3
[ [ 1 ], [ 3, 6 ], [ 2 ], [ 4, 5 ] ]
[ [ 1, 2 ], [ 3, 4 ], [ 5, 6 ] ]

R(D8,[Q8]) i=3 j=4
[ [ 1 ], [ 2 ] ]
[ [ 1, 2 ] ]

R(D8,[C2 x C2 x C2]) i=3 j=5
[ [ 1, 6 ], [ 2, 3, 4, 5 ] ]
[ [ 1 ], [ 2 ], [ 3 ], [ 4 ], [ 5 ], [ 6 ] ]
```

```
R(Q8,[C8]) i=4 j=1
[ [ 1, 3, 4, 2, 5, 6 ] ]
[ [ 1, 3 ], [ 2, 4 ], [ 5, 6 ] ]

R(Q8,[C4 x C2]) i=4 j=2
[ [ 1, 3, 5, 6, 4, 2 ] ]
[ [ 1, 2 ], [ 3, 4 ], [ 5, 6 ] ]

R(Q8,[D8]) i=4 j=3
[ [ 1, 5, 4 ], [ 3, 2, 6 ] ]
[ [ 1, 2 ], [ 3, 4 ], [ 5, 6 ] ]

R(Q8,[Q8]) i=4 j=4
[ [ 1 ], [ 2 ] ]
[ [ 1, 2 ] ]

R(Q8,[C2 x C2 x C2]) i=4 j=5
[ [ 1, 2 ] ]
[ [ 1 ], [ 2 ] ]
```

```
R(C2 x C2 x C2,[C8]) i=5 j=1

R(C2 x C2 x C2,[C4 x C2]) i=5 j=2
[ [ 1, 25, 37, 41, 14, 9, 33, 21, 35, 39, 28, 6, 11, 23, 4, 19, 30, 8, 16, 18, 32 ],
  [ 27, 3, 17, 13, 5, 20, 24, 31, 29, 22, 40, 7, 36, 38, 12, 42, 10, 34, 15, 26, 2 ] ]
[ [ 1, 2 ], [ 3, 8 ], [ 4, 5 ], [ 6, 7 ], [ 9, 10 ], [ 11, 12 ], [ 13, 18 ], [ 14, 15
  [ 21, 22 ], [ 23, 24 ], [ 25, 26 ], [ 27, 32 ], [ 28, 29 ], [ 30, 31 ], [ 33, 34 ],
  [ 39, 40 ], [ 41, 42 ] ]

R(C2 x C2 x C2,[D8]) i=5 j=3
[ [ 1, 2, 25, 33, 26, 32, 9, 10, 21, 15, 30, 22, 14, 29, 7, 28, 40, 12, 42, 6, 27, 39,
      23, 19, 31, 16, 38, 36, 17, 37, 13, 18, 8, 3 ] ]
[ [ 1, 2 ], [ 3, 8 ], [ 4, 5 ], [ 6, 7 ], [ 9, 10 ], [ 11, 12 ], [ 13, 18 ], [ 14, 15
  [ 21, 22 ], [ 23, 24 ], [ 25, 26 ], [ 27, 28 ], [ 29, 30 ], [ 31, 36 ], [ 32, 33 ],
  [ 39, 40 ], [ 41, 42 ] ]

R(C2 x C2 x C2,[Q8]) i=5 j=4
[ [ 1, 2, 13, 14, 9, 10, 11, 12, 7, 6, 4, 5, 3, 8 ] ]
[ [ 1, 2 ], [ 3, 8 ], [ 4, 5 ], [ 6, 7 ], [ 9, 10 ], [ 11, 12 ], [ 13, 14 ] ]

R(C2 x C2 x C2,[C2 x C2 x C2]) i=5 j=5
[ [ 1 ], [ 8, 6, 5, 3, 2, 4, 7 ] ]
[ [ 1 ], [ 2 ], [ 3 ], [ 4 ], [ 5 ], [ 6 ], [ 7 ], [ 8 ] ]
```

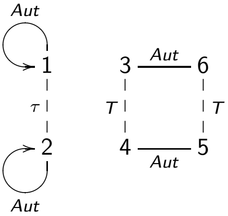
There are a few 'motifs' present when looking at the orbits of $Aut(G)$ and $T(M)$.

For example, the orbits can be 'perpendicular', namely that $Orb_{Aut(G)}(N) \cap Orb_{T(N)}(N) = \{N\}$.

```
R(D8,[D8]) i=3 j=3
[ [ 1 ], [ 3, 6 ], [ 2 ], [ 4, 5 ] ]
[ [ 1, 2 ], [ 3, 4 ], [ 5, 6 ] ]
```

For N_1 and N_2 which are $\lambda(G)$ and $\rho(G)$, one has that $Aut(G)$ acts trivially, while $T(G) = \langle \tau \rangle \cong C_2$ which maps $\lambda(G)$ to $\rho(G)$.

And, $Orb_{T(N_3)} = \{N_3, N_4\}$ and $Orb_{Aut(G)}(N_3) = \{N_3, N_6\}$ and $Orb_{T(N_6)} = \{N_6, N_5\}$ and $Orb_{Aut(G)}(N_4) = \{N_4, N_5\}$

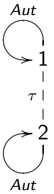


A somewhat more interesting example of this occurs in degree 40 with $R(C_5 \rtimes C_8, [C_5 \rtimes' C_8])$

$$
\begin{tikzcd}
1 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 9 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 11 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 5 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 7 \arrow[d, dash, dashed, "T"'] \\
2 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 10 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 12 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 6 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 8 \arrow[d, dash, dashed, "T"'] \\
4 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 18 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 20 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 14 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 16 \arrow[d, dash, dashed, "T"'] \\
3 \arrow[r, dash, "Aut"] & 17 \arrow[r, dash, "Aut"] & 19 \arrow[r, dash, "Aut"] & 13 \arrow[r, dash, "Aut"] & 15
\end{tikzcd}
$$

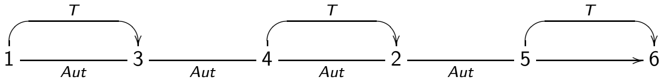
It is also possible for the orbits with respect to $Aut(G)$ to be contained in the orbits of T and vice versa, for example:

```
R(C24,[C24]) i=2 j=2
[ [ 1 ], [ 2 ] ]
[ [ 1, 2 ] ]
```



or

```
R(Q8,[C8]) i=4 j=1
[ [ 1, 3, 4, 2, 5, 6 ] ]                    <- Aut-orbit
[ [ 1, 3 ], [ 2, 4 ], [ 5, 6 ] ]            <- T-orbits
```



which corresponds to a non-trivial intersection of $Aut(G)$ and $T(N)$.

The containments can be mixed, as with this example in degree 40 with $R(C_5 \rtimes Q_2, [C_5 \rtimes C_8])$

$$\begin{tikzcd}
1 \arrow[r, dash, dashed, "T"'] \arrow[r, bend left, "Aut"] & 5 \arrow[r, dash, dashed, "T"'] & 2 \arrow[r, dash, dashed, "T"'] \arrow[r, bend left, "Aut"] & 6
\end{tikzcd}$$

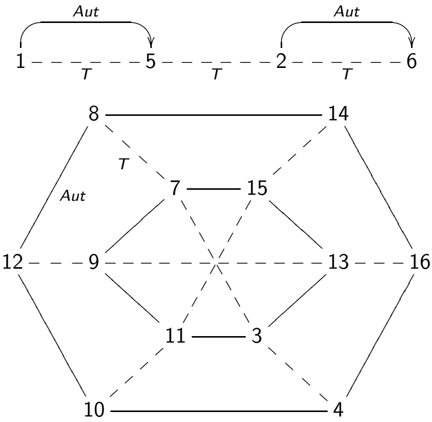
$$\boxed{\begin{tikzcd}
3 \arrow[d, dash, dashed, "T"'] & 10 \arrow[d, dash, dashed, "T"'] & 12 \arrow[d, dash, dashed, "T"'] & 25 \arrow[d, dash, dashed, "T"'] & 29 \arrow[d, dash, dashed, "T"'] \\
4 \arrow[d, dash, dashed, "T"'] & 15 \arrow[d, dash, dashed, "T"'] & 13 \arrow[d, dash, dashed, "T"'] & 26 \arrow[d, dash, dashed, "T"'] & 30 \arrow[d, dash, dashed, "T"'] \\
7 \arrow[d, dash, dashed, "T"'] & 18 \arrow[d, dash, dashed, "T"'] & 20 \arrow[d, dash, dashed, "T"'] & 27 \arrow[d, dash, dashed, "T"'] & 37 \arrow[d, dash, dashed, "T"'] \\
8 & 23 & 21 & 28 & 38
\end{tikzcd}}
\quad
\boxed{\begin{tikzcd}
9 \arrow[d, dash, dashed, "T"'] & 11 \arrow[d, dash, dashed, "T"'] & 31 \arrow[d, dash, dashed, "T"'] & 33 \arrow[d, dash, dashed, "T"'] & 35 \arrow[d, dash, dashed, "T"'] \\
16 \arrow[d, dash, dashed, "T"'] & 14 \arrow[d, dash, dashed, "T"'] & 32 \arrow[d, dash, dashed, "T"'] & 34 \arrow[d, dash, dashed, "T"'] & 36 \arrow[d, dash, dashed, "T"'] \\
17 \arrow[d, dash, dashed, "T"'] & 19 \arrow[d, dash, dashed, "T"'] & 39 \arrow[d, dash, dashed, "T"'] & 41 \arrow[d, dash, dashed, "T"'] & 43 \arrow[d, dash, dashed, "T"'] \\
24 & 22 & 40 & 42 & 44
\end{tikzcd}}$$

where the boxed entries correspond to separate orbits under $Aut(G)$.

```
R(C5 : Q8,[C5 : C8]) i=4 j=1
[[1,5], [2,6], [25,33,35,29,31,27,41,43,37,39,8,20,18,24,22,4,12,10,16,14],
 [26,34,36,30,32,28,42,44,38,40,7,21,23,17,19,3,13,15,9,11] ]
[[1,2,5,6],[3,4,7,8],[9,16,17,24],[10,15,18,23],[11,14,19,22],[12,13,20,21],
 [25,26,27,28], [29,30,37,38], [31,32,39,40], [33,34,41,42], [35,36,43,44] ]
```

There are also in-between motifs.

```
R(C4 x S3,[C3 : C8]) i=5 j=1
[ [ 1, 5 ], [ 2, 6 ], [ 7, 15, 13, 3, 11, 9 ], [ 8, 14, 16, 4, 10, 12 ] ]
[ [ 1, 2, 5, 6 ], [ 3, 4, 7, 8 ], [ 9, 12, 13, 16 ], [ 10, 11, 14, 15 ] ]
```



Going back to low degree examples, the conjecture holds in degree 12.

```
gap> conjecture(12);
[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ false, true, true, false, true ]          <- |R(G,[M])| <= |Aut(G)|
[ true, true, true, true, true ]

[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]
gap> List([1..Size(G[12])],t->Size(AutG[12][t]));
[ 12, 4, 24, 12, 12 ]
gap> List([1..Size(G[12])],t->Index(NHolG[12][t],HolG[12][t]));
[ 2, 1, 2, 2, 1 ]
gap> aprint(List([1..Size(G[12])],i->List([1..Size(G[12])],j->Size(R[12][i][j]))));
[ 2, 3, 12, 2, 3 ]
[ 2, 1, 0, 2, 1 ]
[ 0, 0, 10, 0, 4 ]
[ 14, 9, 0, 14, 3 ]
[ 6, 3, 4, 6, 1 ]
gap> aprint(List([1..Size(G[12])],i->List([1..Size(G[12])],j->Size(AutG[12][i])*Index(NHolG[12][j],
[ 24, 12, 24, 24, 12 ]
[ 8, 4, 8, 8, 4 ]
[ 48, 24, 48, 48, 24 ]
[ 24, 12, 24, 24, 12 ]
[ 24, 12, 24, 24, 12 ]
```

Alas, this conjecture is **not** true for all classes of groups.

```
gap> Read("../RLIB/R18.g");
gap> Read("conjecture.g");
gap> conjecture(18);
[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ true, true, false, false, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]

[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ true, true, true, false, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]

gap> aprint(List([1..Size(G[18])],i->List([1..Size(G[18])],j->Size(R[18][i][j]))));
[ 2, 9, 0, 0, 0 ]
[ 6, 3, 0, 0, 0 ]
[ 0, 0, 24, 30, 9 ]
[ 0, 0, 72, 62, 9 ]
[ 0, 0, 24, 30, 9 ]
gap> aprint(List([1..Size(G[18])],i->List([1..Size(G[18])],j->Size(AutG[18][i])*Index(NHolG[18][j
[ 108, 54, 108, 108, 54 ]
[ 12, 6, 12, 12, 6 ]
[ 24, 12, 24, 24, 12 ]        <- Note Aut(C3xS3)=12 and T((C3 x C3):C2)=2
[ 864, 432, 864, 864, 432 ]
[ 96, 48, 96, 96, 48 ]
```

but the failure for $R(C_3xS_3, [(C_3xC_3) \rtimes C_2])$ is interesting...

We have that $|R(C_3xS_3, [(C_3xC_3) \rtimes C_2])| = 30$ whereas $|Aut(C_3 \times S_3)| = 12$ and $|T((C_3xC_3) \rtimes C_2)| = 2$ so that $|R|$ is 'approximately' $|Aut(G)| \cdot |T(M)|$.
Also, there is a curious interaction of the actions of $Aut(G)$ and $T(M)$, namely

$$
\begin{tikzcd}
1 \arrow[loop above, "Aut"] \arrow[d, dash, dashed, "T"'] & 4 \arrow[loop above, "Aut"] \arrow[d, dash, dashed, "T"'] & 3 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 2 \arrow[d, dash, dashed, "T"] & 17 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 23 \arrow[d, dash, dashed, "T"] & 26 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"'] & 29 \arrow[d, dash, dashed, "T"] \\
20 \arrow[loop below, "Aut"] & 14 \arrow[loop below, "Aut"] & 22 \arrow[r, dash, "Aut"'] & 21 & 10 \arrow[r, dash, "Aut"'] & 7 & 30 \arrow[r, dash, "Aut"'] & 28
\end{tikzcd}
$$

$$
\begin{tikzcd}
12 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"] & 9 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"] & 6 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"] & 8 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"] & 11 \arrow[r, dash, "Aut"] \arrow[d, dash, dashed, "T"] & 5 \arrow[d, dash, dashed, "T"] \\
19 \arrow[r, dash, "Aut"'] & 25 \arrow[r, dash, "Aut"'] & 16 \arrow[r, dash, "Aut"'] & 24 \arrow[r, dash, "Aut"'] & 18 \arrow[r, dash, "Aut"'] & 15
\end{tikzcd}
$$

but also..

$$
\begin{tikzcd}
13 \arrow[r, bend left, "Aut"] \arrow[r, bend right, "T"'] & 17
\end{tikzcd}
$$

namely that $Orb_{T(N_{13})}(N_{13}) = Orb_{Aut(G)}(N_{13})$.

Going further, there are cases where the conjecture is true for all $R(G,[M])$ of a given size.

```
gap> Read("../RLIB/R20.g");
gap> Read("conjecture.g");
gap> conjecture(20);
[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]          <- |R(G,[M])| <= |Aut(G)|
[ true, true, true, true, true ]
[ true, true, true, true, true ]

[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]
[ true, true, true, true, true ]
gap> List([1..Size(G[20])],t->Size(AutG[20][t]));
[ 40, 8, 20, 40, 24 ]
gap> List([1..Size(G[20])],t->Index(NHolG[20][t],HolG[20][t]));
[ 2, 1, 2, 2, 1 ]
gap> aprint(List([1..Size(G[20])],i->List([1..Size(G[20])],j->Size(R[20][i][j]))));
[ 2, 5, 20, 2, 5 ]            {40}
[ 2, 1, 4, 2, 1 ]             {8}
[ 10, 5, 12, 10, 5 ]          {20}
[ 22, 15, 0, 22, 5 ]          {40}
[ 6, 3, 0, 6, 1 ]             {24}
```

And others where there are a few $(G,[M])$ where it does not hold.

```
gap> Read("../RLIB/R24.g");
gap> Read("conjecture.g");
gap> needT:=Filtered(Tuples([1..Size(G[24])],2),v->(Size(R[24][v[1]][v[2]])<=
Size(AutG[24][v[1]])*Index(NHolG[24][v[2]],HolG[24][v[2]])) and
(Size(R[24][v[1]][v[2]])>Size(AutG[24][v[1]])));
[ [ 4, 5 ], [ 4, 8 ], [ 5, 4 ], [ 5, 5 ], [ 5, 6 ], [ 5, 7 ], [ 5, 8 ], [ 5, 9 ], [ 5, 14 ], [
  [ 6, 8 ], [ 6, 14 ], [ 7, 5 ], [ 7, 8 ], [ 8, 4 ], [ 8, 5 ], [ 8, 6 ], [ 8, 7 ], [ 8, 8 ], [
  [ 8, 14 ], [ 9, 5 ], [ 9, 7 ], [ 9, 8 ], [ 10, 5 ], [ 10, 7 ], [ 10, 8 ], [ 10, 14 ], [ 12, 1
  [ 14, 5 ], [ 14, 6 ], [ 14, 7 ], [ 14, 8 ], [ 14, 14 ] ]
gap> notnhc:=Filtered(Tuples([1..Size(G[24])],2),v->Size(R[24][v[1]][v[2]])>
Size(AutG[24][v[1]])*Index(NHolG[24][v[2]],HolG[24][v[2]]));
[ [ 12, 15 ] ]
gap> Size(G[24])^2;
225
gap>
gap> Read("../RLIB/R36.g");
gap> Read("conjecture.g");
gap> needT:=Filtered(Tuples([1..Size(G[36])],2),v->(Size(R[36][v[1]][v[2]])<=
Size(AutG[36][v[1]])*Index(NHolG[36][v[2]],HolG[36][v[2]])) and
(Size(R[36][v[1]][v[2]])>Size(AutG[36][v[1]])));
[ [ 6, 7 ], [ 6, 11 ], [ 6, 13 ], [ 11, 11 ], [ 12, 6 ], [ 12, 9 ], [ 12, 12 ] ]
gap> notnhc:=Filtered(Tuples([1..Size(G[36])],2),v->Size(R[36][v[1]][v[2]])>
Size(AutG[36][v[1]])*Index(NHolG[36][v[2]],HolG[36][v[2]]));
[[ 10, 6 ],[ 10, 7 ],[ 10, 10 ],[ 10, 12 ],[ 10, 13 ],[ 12, 7 ],[ 12, 8 ],[ 12, 10 ],[ 12, 13 ]
gap> Size(G[36])^2;
196
```

A few more examples to consider.

```
gap> Read("../RLIB/R27.g");
gap> Read("conjecture.g");
gap> needT:=Filtered(Tuples([1..Size(G[27])],2),v->(Size(R[27][v[1]][v[2]])<=Size(AutG[27][v[
[ [ 4, 4 ] ]
gap> notnhc:=Filtered(Tuples([1..Size(G[27])],2),v->Size(R[27][v[1]][v[2]])>Size(AutG[27][v[1
[  ]

and other 'mp' examples


gap> Read("../RLIB/R28.g");
gap> Read("conjecture.g");
gap> needT:=Filtered(Tuples([1..Size(G[28])],2),v->(Size(R[28][v[1]][v[2]])<=Size(AutG[28][v[
[  ]
gap> notnhc:=Filtered(Tuples([1..Size(G[60])],2),v->Size(R[60][v[1]][v[2]])>Size(AutG[60][v[1
[  ]
gap>

gap> Read("../RLIB/R40.g");
gap> Read("conjecture.g");
gap> needT:=Filtered(Tuples([1..Size(G[40])],2),v->(Size(R[40][v[1]][v[2]])<=Size(AutG[40][v[
[ [ 5, 5 ], [ 5, 7 ], [ 5, 8 ], [ 8, 5 ], [ 8, 7 ], [ 8, 8 ], [ 12, 4 ], [ 12, 5 ], [ 12, 6 ]
  [ 12, 9 ], [ 12, 12 ], [ 12, 13 ], [ 13, 5 ], [ 13, 8 ] ]
gap> notnhc:=Filtered(Tuples([1..Size(G[40])],2),v->Size(R[40][v[1]][v[2]])>Size(AutG[40][v[1
[  ]
gap>
```

```
gap> Read("../RLIB/R42.g");
gap> Read("conjecture.g");
gap> needT:=Filtered(Tuples([1..Size(G[42])],2),v->(Size(R[42][v[1]][v[2]])<=Size(
[  ]
gap> notnhc:=Filtered(Tuples([1..Size(G[42])],2),v->Size(R[42][v[1]][v[2]])>Size(A
[  ]
gap>
```

And one nearly 'mp' case.

```
gap> Read("../RLIB/R60.g");
gap> Read("conjecture.g");
gap> needT:=Filtered(Tuples([1..Size(G[60])],2),v->(Size(R[60][v[1]][v[2]])<=Size(
[ [ 8, 8 ], [ 10, 8 ], [ 11, 8 ] ]
gap> notnhc:=Filtered(Tuples([1..Size(G[60])],2),v->Size(R[60][v[1]][v[2]])>Size(A
[  ]
```

Recall that when $n = mp$ for $gcd(m, p) = 1$ where p is prime and does not divide the automorphism group of any group of order m, and where the Sylow p-subgroup is unique, if $N \in R(G, [M])$ then $N \leq Norm_B(\mathcal{P})$ where $\mathcal{P}$ is the Sylow p-subgroup of $\lambda(G)$.

For groups of order 60 these conditions are satisfied for all groups except A_5.
However $R(A_5, [M]) = \emptyset$ unless $M = A_5$ and that $R(A_5, [A_5]) = \{\lambda(A_5), \rho(A_5)\}$, and there are only 4 $[M]$ for which $R(A_5, [M])$ is non-empty.

Thank you!

F. Dalla Volta A. Caranti.
Groups that have the same holomorph as a finite perfect group.
Arxiv preprint GR, 2017.
11

N. P. Byott.
Hopf-galois structures on field extensions with simple galois groups.
Bull. London Math. Soc., 36:23–29, 2004.
11

A. Caranti.
The multiple holomorphs of finite p-groups of class two.
Arxiv preprint GR, 2018.
11

C. Greither and B. Pareigis.
Hopf Galois theory for separable field extensions.
J. Algebra, 106:239–258, 1987.
3, 4

T. Kohl.

Multiple holomorphs of dihedral and quaternionic groups.
Comm. Alg., 43:4290–4304, 2015.
11