Characteristic Subgroup Lattices and Hopf-Galois Structures

Timothy Kohl
Department of Mathematics and Statistics
Boston University
Boston, MA 02215
tkohl@math.bu.edu

Abstract

The Hopf-Galois structures on normal extensions K/k with $G = Gal(K/k)$ are in one-to-one correspondence with the set of regular subgroups $N \leq B = Perm(G)$ that are normalized by the left regular representation $\lambda(G) \leq B$. Each such N corresponds to a Hopf algebra $H_N = (K[N])^G$ that acts on K/k. Such regular subgroups N need not be isomorphic to G but must have the same order. One can subdivide the totality of all such N into collections $R(G,[M])$ which is the set of those regular N normalized by $\lambda(G)$ and isomorphic to a given abstract group M where $|M| = |G|$. There arises an injective correspondence between the characteristic subgroups of a given N and the set of subgroups of G stemming from the Galois correspondence between sub-Hopf algebras of H_N and intermediate fields $k \subseteq F \subseteq K$. We utilize this correspondence to show that for certain pairings $(G,[M])$, the collection $R(G,[M])$ must be empty.

key words: Hopf-Galois extension, Greither-Pareigis theory, regular subgroup, Galois correspondence

MSC: 16T05,20B35,20E07

1 Introduction

Hopf-Galois theory is a generalization of the ordinary Galois theory for fields. If one has a Galois extension of fields K/k with $G = Gal(K/k)$ then the elements of G act as automorphisms of course, but if one takes k-linear combinations of these automorphisms, one gets an injective homomorphism $\mu : k[G] \to End_k(K)$ where $\mu(\sum_{g\in G} c_g \cdot g)(a) = \sum_{g\in G} g(a)$, since a sum of automorphisms is no longer an automorphism but is an endomorphism of K. As such, we replace the group G by the group ring, and prototype Hopf algebra, $k[G]$. Furthermore, by linear independence of characters, one has that $K \otimes k[G] \cong End_k(K)$, which means that if we augment these sums of automorphisms by left-multiplication by elements of K then this yields all the k-endomorphisms of K. To be more precise, the previous isomorphism is actually $K\#k[G] \cong End_k(K)$ where $K\#k[G]$ is the so-called smash product of K with $k[G]$ which, as a vector space is $K \otimes_k k[G]$ but the multiplication is as follows $(a\#h)(a'\#h') = ah(a')\#hh'$ where $a, a' \in K$ and $h, h' \in k[G]$. Moreover, if $h = \sum_{g\in G} c_g \cdot g \in k[G]$ then if $x \in k$ then

$$h(x) = \sum_{g\in G} c_g g(x) = (\sum_{g\in G} c_g)x$$

namely, h acts by scalar multiplication on x. The idea behind Hopf-Galois theory is to find a Hopf algebra which acts in a similar fashion as $k[G]$ does when the extension is Galois in the usual sense. The formal definition is as follows.

Definition 1.1: 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 $I \otimes \mu : K\#H \xrightarrow{\cong} End_k(K)$

  where $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$ is the comultiplication in H and $\epsilon : H \to k$ is the co-unit map.

The original intended application [5] was to devise a Galois theory for purely inseparable extensions. However, it turned not to be suitable to extensions of exponent greater than 1. However, in [8] Greither and Pareigis showed that Hopf-Galois theory can be effectively applied to separable extensions, especially those which are non-normal. As such, one obtains a 'Galois structure' on extensions such as $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ which aren't Galois extensions in the usual sense. There are two particularly interesting features to this result, namely a given extension K/k may have more than one Hopf-Galois structure on it, and also, an extension which *is* Galois in the usual sense (and thus Hopf-Galois with respect to the group ring $k[G]$) but also Hopf-Galois with respect to other Hopf algebra actions. It is the latter case that we are looking at here, and we give the main theorem in [8] for such extensions:

Theorem 1.2:*[8] 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. 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. As such, the enumeration of Hopf-Galois structures on a normal extension K/k becomes a group theory problem. 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 $|G|$. Now, the enumeration of $R(G,[M])$ for different pairings of groups of different types has been extensively studied by the author and others, e.g. [13],[3],[6],[4]. One may consider the enumeration based on the different types or sizes of the groups in question, such as G cyclic, elementary abelian, $G = S_n$, $G = A_n$, $|G| = mp$, G simple, G,M nilpotent and more. What we shall consider is when $R(G,[M]) = \emptyset$.

The condition that $\lambda(G) \leq Norm_B(N)$ is the deciding factor as to whether a given regular subgroup $N \leq B$ gives rise to a Hopf-Galois structure. And, as such, this condition may, for N of a given isomorphism type $[M]$, imply that $R(G,[M]) = \emptyset$. In some instances, basic structural properties of the groups G and N preclude the containment $\lambda(G) \leq Norm_B(N)$, for example in [13] it is shown that $R(C_{p^n},[M]) = \emptyset$ if M is non-cyclic by comparing the exponent of C_{p^n} versus that of the Sylow p-subgroup of $Norm_B(N)$ when N is a p-group. For other cases, some deeper analysis is needed. In [1], Byott proved that if G is simple then if $M \not\cong G$ then $R(G,[M])$ is empty, but the proof of this required the classification of finite simple groups.

We note that if N is any regular subgroup of B then (by basically [9, Theorem 6.3.2]) $Norm_B(N)$ is canonically isomorphic to $Hol(N) \cong N \rtimes Aut(N)$. More generally, one can enumerate $R(G,[M])$ by first enumerating

$$S(M,[G]) = \{U \leq Norm_B(M) \mid U \text{ regular and } U \cong G\}$$

where, again, for M a regular subgroup of B, $Norm_B(M) \cong Hol(M)$. That is we consider those regular subgroups of $Norm_B(M) \cong Hol(M)$ that are regular and isomorphic to G. The correspondence between $|R(G,[M])|$ and $|S([M,[G])|$ is given by the following result due to Byott [2, p.3220] which we translate into the terminology we have already established.

Proposition 1.3: *For G and $[M]$ as given above*

$$|R(G,[M])| = \frac{|Aut(G)|}{|Aut(M)|}|S(M,[G])|$$

where $Aut(M)$ and $Aut(G)$ are the automorphism groups of M and G.

This approach has advantages and disadvantages in that, while it doesn't easily yield the element of $R(G,[M])$ from an element of $S(M,[G])$, it does give the counts of one in terms of the other, where the computation of $S(M,[G])$ is feasible at the very least, by brute force using a system such as GAP. We utilize this later on to obtain some of the information in some of the tables we shall give. What is more desirable, typically, is to derive $|R(G,[M])|$ or $|S(M,[G])|$ from first principles. In our analysis, we will take a slightly different tack, by inferring that $R(G,[M])$ is empty in certain circumstances, by utilizing one of the consequences of the existence of a Hopf-Galois structure on a field extension. In the setting of a Hopf-Galois extension K/k with action by a k-Hopf algebra H, one has:

Theorem 1.4: *The correspondence* $Fix : \{k - \textit{sub-Hopf algebras of } H\} \rightarrow \{subfields\ k \subseteq F \subseteq K\}$ *given by*

$$Fix(H') = \{z \in K \mid h(z) = \epsilon(h)z\ \forall h \in H'\}$$

(where $H' \subseteq H$) is injective and inclusion reversing.

From Chase and Sweedler [5], and extrapolated in Greither-Pareigis, and in [12, Prop 2.2] we have:

Proposition 1.5: *For a normal extension K/k with $G = Gal(K/k)$ which is Hopf-Galois with respect to the action of $H_N = (K[N])^G$ the sub-Hopf algebras of H_N are of the form $H_P = (K[P])^G$ where P is any G-invariant subgroup of N.*

And as any intermediate field between k and K corresponds to a subgroup $J \leq G$, where $Fix(H_P) = F = K^J$, one has a modification of the aforementioned Galois correspondence. The following is basically [12, Thm. 2.4, Cor. 2.5 and 2.6].

Theorem 1.6: *The correspondence*

$$\Psi : \{\textit{subgroups } of\ N \textit{ normalized by} \lambda(G)\} \longrightarrow \{\textit{subgroups of } G\}$$

given by

$$\Psi(P) = Orb_P(i_G) = \{q(i_G) \mid q \in P\} = J$$

is injective and $K^{H_P} = F = K^J$.

We note that J *is* a subgroup of G and also that $|P| = [K : F] = |J|$. We observe that if P is a characteristic subgroup of N then it is automatically normalized by $\lambda(G)$, and, as mentioned above $|\Psi(P)| = |P|$. As such, since $|N| = |G|$ by regularity, if $m\big||G|$ we let

$$\begin{aligned} Sub_m(G) &= \{\text{subgroups of } G \text{ of order } m\} \\ CharSub_m(N) &= \{\text{characteristic subgroups of } N \text{ of order } m\} \end{aligned}$$

and thus we have an injective correspondence

$$\Psi : CharSub_m(N) \to Sub_m(G)$$

for each $m\big||G|$ so that $|CharSub_m(N)| \leq |Sub_m(G)|$.

The question we consider is, for a given N where $N \cong M$, can we discern whether $|CharSub_m(N)| > |Sub_m(G)|$ for at least one m, in which case one must conclude that $R(G, [M]) = \emptyset$? What is seemingly unlikely about this approach yielding anything is that one expects the class of characteristic subgroups to be somewhat meager, certainly in comparison to the collection of all subgroups. But, for those of a given order m dividing $|G|$ this actually happens relatively often. We start with the first class of examples where this analysis applies. The 5 groups of order 12 are Q_3, C_{12}, A_4, D_6, and $C_6 \times C_2$ and by direct computation we find three pairings $R(G, [M])$ which are empty by this criterion.

$$\begin{aligned} (G, [M]) = (A_4, Q_3) \to &\quad |Sub_6(G)| = 0 \text{ and } |CharSub_6(M)| = 1 \\ (G, [M]) = (A_4, C_{12}) \to &\quad |Sub_6(G)| = 0 \text{ and } |CharSub_6(M)| = 1 \\ (G, [M]) = (A_4, D_6) \to &\quad |Sub_6(G)| = 0 \text{ and } |CharSub_6(M)| = 1 \end{aligned}$$

which is a modest set of examples, but representative of some basic motifs which we'll explore in more detail presently. Examining the full table of $|R(G, [M])|$ we see where these fit in, and also observe the two other empty pairings.

$G \downarrow \ M \rightarrow$	Q_3	C_{12}	A_4	D_6	$C_6 \times C_2$
Q_3	2	3	12	2	3
C_{12}	2	1	0	2	1
A_4	0	0	10	0	4
D_6	14	9	0	14	3
$C_6 \times C_2$	6	3	4	6	1

We highlight the fact that for $G = A_4$ and $M = Q_3, D_6,$ and C_{12} that $|Sub_6(G)| = 0$ and $|CharSub_6(M)| = 1$.

That is, G has no-subgroup of index 2, which is a basic exercise in group theory, and $Q_3, D_6,$ and $C_6 \times C_2$ have unique (hence characteristic) subgroups of index 2. As it turns out, examples like this are quite common instances of the $|CharSub_m(N)| > |Sub_m(G)|$ condition.

2 Index Two Subgroups

Following Nganou [14] we can apply some basic, yet very useful, group theory facts to examine the index 2 subgroups of a given group.

Theorem 2.1:*[[14]] For a finite group G, where $n = |G|$, the subgroup $G^2 = \langle \{g^2 \mid g \in G\} \rangle$ is such that*

$$|Sub_{n/2}(G)| = |Sub_{n/2}(G/G^2)|$$

where, since $[G,G] \subseteq G^2$, G/G^2 is an elementary Abelian group of order 2^m. Moreover, $|Sub_{n/2}(G/G^2)| = 2^m - 1$ since the index 2 subgroups correspond to hyperplanes in the finite vector space G/G^2.

i.e. $|Sub_{n/2}(G)| = [G : G^2] - 1$. As a corollary to this, he also notes:

Corollary 2.2: *If G is a finite group then G has no index 2 subgroups iff $[G : G^2] = 1$ iff G is generated by squares. And G has a unique index 2 subgroup iff $[G : G^2] = 2$.*

And indeed, A_4 has no index 2 subgroups since it is generated by squares since every three cycle is the square of its inverse. There are other examples of even order groups without index 2 subgroups. In degree 24, let

$G = SL_2(\mathbb{F}_3)$. There are 15 groups M of order 24, of which 12 have the property that $|CharSub_{12}(M)| > 0$.

If $M = C_3 \rtimes C_8, C_{24}, S_4, C_2 \times A_4$ then $|Sub_{12}(M)| = 1$ so $|CharSub_{12}(M)| = 1$.

If $M = C_3 \rtimes Q_2, D_{12}, C_2 \times (C_3 \rtimes C_4), C_{12} \times C_2, C_3 \times D_4$ then $|Sub_{12}(M)| = 3$ and $|CharSub_{12}(M)| = 1$.

If $M = C_4 \times S_3, (C_6 \times C_2) \rtimes C_2$ then $|CharSub_{12}(M)| = 3$.

If $M = C_2 \times C_2 \times S_3$ then $|Sub_{12}(M)| = 7$ and $|CharSub_{12}(M)| = 1$.

In fact, there are only 3 non-empty $R(SL_2(\mathbb{F}_3), [M])$, namely $M = SL_2(\mathbb{F}_3)$, $C_3 \times Q_2$ and $C_6 \times C_2 \times C_2$. Of course, not all the cases where the pairing is empty correspond to M having a unique subgroup of index 2. Nonetheless, the number of characteristic subgroups of M of index 2 is larger than the number of index 2 subgroups of G. We present the full table of $|R(G, [M])|$ values, highlighting those determined to be zero via this criterion. As it turns out, all of the cases where $|CharSub_m(M)| > |Sub_m(G)|$ occur when $m = 12$.

$G \downarrow \ M \rightarrow$	$C_3 \rtimes C_8$	C_{24}	$SL_2(\mathbb{F}_3)$	$C_3 \rtimes Q_2$	$C_4 \times S_3$	D_{12}	$C_2 \times (C_3 \rtimes C_4)$
$C_3 \rtimes C_8$	4	6	24	4	0	4	0
C_{24}	4	2	0	4	0	4	0
$SL_2(\mathbb{F}_3)$	0	0	10	0	0	0	0
$C_3 \rtimes Q_2$	28	18	0	28	56	28	28
$C_4 \times S_3$	16	12	0	28	56	28	52
D_{12}	4	6	0	28	56	28	76
$C_2 \times (C_3 \rtimes C_4)$	24	12	0	28	56	28	36
$(C_6 \times C_2) \rtimes C_2$	12	6	0	28	56	28	60
$C_{12} \times C_2$	8	4	0	12	24	12	20
$C_3 \times D_4$	4	2	0	12	24	12	28
$C_3 \times Q_2$	12	6	16	12	24	12	12
S_4	0	0	0	0	0	0	0
$C_2 \times A_4$	0	0	0	0	0	0	0
$C_2 \times C_2 \times S_3$	0	0	0	228	456	228	228
$C_6 \times C_2 \times C_2$	0	0	0	84	168	84	84

$G \downarrow \ M \rightarrow$	$(C_6 \times C_2) \rtimes C_2$	$C_{12} \times C_2$	$C_3 \times D_4$	$C_3 \times Q_2$	S_4	$C_2 \times A_4$	$C_2 \times C_2 \times S_3$	$C_6 \times C_2 \times C_2$
$C_3 \rtimes C_8$	0	0	6	6	0	0	0	0
C_{24}	0	0	2	2	0	0	0	0
$SL_2(\mathbb{F}_3)$	0	0	0	8	0	0	0	8
$C_3 \rtimes Q_2$	56	18	18	6	0	0	28	6
$C_4 \times S_3$	56	30	18	6	24	0	40	12
D_{12}	56	42	18	6	0	0	52	18
$C_2 \times (C_3 \rtimes C_4)$	56	30	18	6	0	48	32	12
$(C_6 \times C_2) \rtimes C_2$	56	42	18	6	24	48	44	18
$C_{12} \times C_2$	24	10	6	2	0	0	16	4
$C_3 \times D_4$	24	14	6	2	16	0	20	6
$C_3 \times Q_2$	24	6	6	2	0	0	12	2
S_4	0	0	0	0	8	36	24	48
$C_2 \times A_4$	0	0	0	8	12	16	8	8
$C_2 \times C_2 \times S_3$	456	126	126	42	48	0	152	24
$C_6 \times C_2 \times C_2$	168	42	42	14	0	112	56	8

We note that there are total of 76 different $(G,[M])$ for which $R(G,[M]) = \emptyset$, of which this method predicted 20. As an interesting aside, one *can* find extensions $K/\mathbb{Q}$ where $Gal(K/\mathbb{Q}) \cong SL_2(\mathbb{F}_3)$. For example, Heider and Kolvenbach [10], found that the splitting field of

$$f(x) = x^8 + 9x^6 + 23x^4 + 14x^2 + 1 \in \mathbb{Z}[x]$$

is one such $SL_2(\mathbb{F}_3)$ Galois extension.

We use the notation

$$I_2(G) = [G : G^2] - 1$$

for the number of index 2 subgroups, as given in Crawford and Wallace [15] who, using Goursat's theorem, present a number of basic facts, namely

- $I_2(G_1 \times G_2) = I_2(G_1)I_2(G_2) + I_2(G_1) + I_2(G_2)$
- If $I_2(G) > 0$ then $I_2(G) \equiv 1$, or 3 $(mod\ 6)$

Nganou also shows this by observing that $(G_1 \times G_2)^2 = G_1^2 \times G_2^2$ and therefore that $[G_1 \times G_2 : (G_1 \times G_2)^2] = [G_1 : G_1^2][G_2 : G_2^2]$, and also that if $|G|$ is odd then $I_2(G) = 0$ automatically. In actuality, the full machinery of Goursat's theorem, which is used to count subgroups of arbitrary direct products, is not needed since, for subgroups of index 2, and later on index p, it's straightforward to enumerate the subgroups via the subgroup indices. Some examples of this were seen in the degree 24 examples earlier, such as

$$\begin{aligned}
I_2(C_2 \times A_4) &= I_2(C_2)I_2(A_4) + I_2(C_2) + I_2(A_4) &&= 1 \cdot 0 + 0 + 1 = 1 \\
I_2(C_{12} \times C_2) &= I_2(C_{12})I_2(C_2) + I_2(C_{12}) + I_2(C_2) &&= 1 \cdot 1 + 1 + 1 = 3 \\
I_2(C_3 \times D_4) &= I_2(C_3)I_2(D_4) + I_2(C_3) + I_2(D_4) &&= 0 \cdot 3 + 0 + 3 = 3 \\
I_2(C_4 \times S_3) &= I_2(C_4)I_2(S_3) + I_2(C_4) + I_2(S_3) &&= 1 \cdot 1 + 1 + 1 = 3
\end{aligned}$$

What is most interesting about the formula

$$I_2(G_1 \times G_2) = I_2(G_1)I_2(G_2) + I_2(G_1) + I_2(G_2)$$

is that it allows us to readily generate examples of (even order) groups with 0 or 1 index two subgroups given that, without loss of generality, $I_2(G_1) = 0$

and $I_2(G_2) = 0$ or 1 for then $I_2(G_1 \times G_2) = 0$ or 1 as well. If $I_2(G_1) = 0$ and $I_2(G_2) = 0$ then, of course, $I_2(G_1 \times G_2) = 0$. If G_1 has odd order then $I_2(G_1) = 0$ so if either G_1 has odd order and G_2 even, or both G_1 and G_2 are even, with $I_2(G_1) = I_2(G_2) = 0$ as in the table below, then $I_2(G_1 \times G_2) = 0$.

- A_4
- $SL_2(\mathbb{F}_3)$
- $(C_2 \times C_2) \rtimes C_9$
- $(C_4 \times C_4) \rtimes C_3$
- $C_2^4 \rtimes C_3$
- $C_2^3 \rtimes C_7$
- $C_2^4 \rtimes C_5$
- any non-Abelian simple group

If $I_2(G_1) = 0$ and $I_2(G_2) = 1$ then $I_2(G_1 \times G_2) = 1$.

For example:

G_1

- C_r for r odd
- A_4
- $SL_2(\mathbb{F}_3)$
- $(C_2 \times C_2) \rtimes C_9$
- $(C_4 \times C_4) \rtimes C_3$
- $C_2^4 \rtimes C_3$
- $C_2^3 \rtimes C_7$
- $C_2^4 \rtimes C_5$
- any non-Abelian simple group

G_2

- C_s for s even
- S_n for $n \geq 3$
- D_n for n odd
- $C_3 \rtimes C_4$
- $(C_3 \times C_3) \rtimes C_2$
- the non-split extension of $SL_2(\mathbb{F}_3)$ by C_2 (AKA the non-split extension of C_2 by S_4)

The formula for computing I_2 of a direct product of two groups can be generalized to a direct product of any number of groups. For example, in degree 36

$$\begin{aligned} I_2(C_3 \times C_3 \times C_4) &= I_2(C_3)I_2(C_3 \times C_4) + I_2(C_3) + I_2(C_3 \times C_4) \\ &= 0 \cdot 1 + 0 + 1 \\ &= 1 \end{aligned}$$

which is in agreement with the computation done directly by $[M : M^2] - 1$. Note: If we expand out $I_2(G_1 \times G_2 \times G_3)$ then we find that

$$\begin{aligned} I_2(G_1 \times & G_2 \times G_3) \\ &= e_1(I_2(G_1), I_2(G_2), I_3(G_3)) + e_2(I_2(G_1), I_2(G_2), I_3(G_3)) + \\ &\quad e_3(I_2(G_1), I_2(G_2), I_3(G_3)) \\ &= I_2(G_1) + I_2(G_2) + I_2(G_3) + I_2(G_1)I_2(G_2) + I_2(G_1)I_2(G_3) + I_2(G_2)I_2(G_3) + \\ &\quad I_2(G_1)I_2(G_2)I_2(G_3) \end{aligned}$$

Also, it's not hard to prove that this 'product formula' for $I_2(G_1 \times G_2)$ holds for semi-direct products of cyclic groups.

Proposition 2.3: *If C_r and C_s are cyclic groups then*

$$(C_r \rtimes C_s)^2 = C_r^2 \rtimes C_s^2$$

and therefore that

$$\begin{aligned} [C_r \rtimes C_s : (C_r \rtimes C_s)^2] &= [C_r : C_r^2][C_s : C_s^2] \\ I_2(C_r \rtimes C_s) &= I_2(C_r)I_2(C_s) + I_2(C_r) + I_2(C_s) \end{aligned}$$

Proof. If $C_r = \langle x \rangle$ and $C_s = \langle y \rangle$ then

$$C_r^2 = \begin{cases} \langle x \rangle & r \text{ odd} \\ \langle x^2 \rangle & r \text{ even} \end{cases}$$

and similarly for C_s^2. In either case, C_r^2 is characteristic in C_r meaning that $C_r^2 \rtimes C_s^2$ *is* a subgroup of $C_r \rtimes C_s$ where clearly $C_r^2 \rtimes C_s^2 \leq (C_r \rtimes C_s)^2$. Now any semi-direct product $C_r \rtimes C_s$ arises due to an action of the form $y(x) = x^u$ for $u \in U_r$. If $(x^i, y^j) \in C_r \rtimes C_s$ then $(x^i, y^j)^2 = (x^{i+u^j i}, y^{2j})$, where y^{2j} clearly lies in C_s^2. The question is whether the first coordinate $x^{i+u^j i}$ lies in C_r^2. However, this is easy since if r is even then u must be odd and thus $1+u^j$ is even, which means $i(1+u^j)$ is even. And if r is odd then, as observed above, $C_r = C_r^2$ so that, either way, $x^{i(1+u^j)} \in C_r^2$. $\square$

We have seen examples already in degree 12 and 24,

$$
\begin{aligned}
I_2(C_3 \rtimes C_4) &= I_2(C_3)I_2(C_4) + I_2(C_3) + I_2(C_4) = 0 \cdot 1 + 0 + 1 = 1 \\
I_2(C_3 \rtimes C_8) &= I_2(C_3)I_2(C_8) + I_2(C_3) + I_2(C_8) = 0 \cdot 1 + 0 + 1 = 1
\end{aligned}
$$

and similarly, we can control $I_2(C_r \rtimes C_s)$ by careful choices of r and s, to make it 0 and/or 1. If we define

$$
\begin{aligned}
z_2(n) &= \text{the number of groups of order } n \text{ with no index two subgroups} \\
u_2(n) &= \text{the number of groups of order } n \text{ with one index two subgroup}
\end{aligned}
$$

then we have empty pairings $R(G, [M])$ corresponding to $z_2(n) * u_2(n)$ for $n \leq 256$.

n	z_2	u_2	$z_2 * u_2$	(# of groups of order n)^2
12	1	2	2	25
24	1	4	4	225
36	2	6	12	196
48	2	8	16	2704
56	1	2	2	169
60	2	6	12	169
72	2	13	26	2500
80	1	3	3	2704
84	2	6	12	225
96	3	15	45	53361
108	7	18	126	2025
120	2	12	24	2209
132	1	4	4	100
144	5	25	125	38809
156	2	9	18	324
160	1	5	5	56644
168	5	12	60	3249
180	3	18	54	1369
192	9	39	351	2380849
204	1	6	6	144
216	8	45	360	31329
228	2	6	12	225
240	4	26	104	43264
252	5	18	90	2116

3 Non Index Two Examples

Even though index 2 subgroups are a convenient source of 'counterexamples' to the condition $|Sub_m(G)| \geq |CharSub_m(N)|$ condition, there are of course many other possible subgroup orders where our method applies. For example, $R(A_5, [C_5 \times A_4]) = \emptyset$ which is known already by Byott's result since A_5 is simple, of course, but can be inferred by our method because $C_5 \times A_4$ has a unique subgroup of order 20 since A_4 has a unique subgroup of order 4. Another example is $((C_5 \times C_5) \rtimes C_3, [C_{75}])$ since $|Sub_{15}(C_{75})| = 1$

of course, and $|CharSub_{15}((C_5 \times C_5) \rtimes C_3)| = 0$ since any subgroup of order 15 in $(C_5 \times C_5) \rtimes C_3$ would have to be cyclic and intersect the $(C_5 \times C_5) \cong \mathbb{F}_5^2$ component in a subgroup of order 5. And since no automorphism of $C_5 \times C_5$ of order 3 could arise due to scalar multiplication, this aforementioned subgroup of order 5 would not be normal in $C_5 \times C_5$. One other example we can consider is the case of $R(S_5, [C_{120}])$. Of course, C_{120} has one subgroup of order 15, but since any group of order 15 is cyclic, then it's clear that S_5 has no such subgroup.

Index two or not, using GAP, [7] one can readily enumerate the subgroups, both characteristic and otherwise, of each group of a given low order. We present a table of some compiled counts of the number of pairs $R(G, [M])$ which are forced to be empty because $|Sub_m(G)| < |CharSub_m(M)|$ for some m, which we denote $|Z|$, as compared with square of the number of groups of order n, denoted $|R|^2$, representing all possible pairings of groups of order n. We also should point out that, if the criterion applied, it frequently happened in index 2.

n	$\lvert Z\rvert$	$\lvert R\rvert^2$	n	$\lvert Z\rvert$	$\lvert R\rvert^2$	n	$\lvert Z\rvert$	$\lvert R\rvert^2$
1	0	1	33	0	1	65	0	1
2	0	1	34	0	4	66	0	16
3	0	1	35	0	1	67	0	1
4	0	4	36	34	196	68	0	25
5	0	1	37	0	1	69	0	1
6	0	4	38	0	4	70	0	16
7	0	1	39	0	4	71	0	1
8	0	25	40	11	196	72	422	2500
9	0	4	41	0	1	73	0	1
10	0	4	42	0	36	74	0	4
11	0	1	43	0	1	75	1	9
12	3	25	44	0	16	76	0	16
13	0	1	45	0	4	77	0	1
14	0	4	46	0	4	78	0	36
15	0	1	47	0	1	79	0	1
16	5	196	48	244	2704	80	149	2704
17	0	1	49	0	4	81	5	225
18	2	25	50	2	25	82	0	4
19	0	1	51	0	1	83	0	1
20	0	25	52	0	25	84	28	225
21	0	4	53	0	1	85	0	1
22	0	4	54	8	225	86	0	4
23	0	1	55	0	4	87	0	1
24	20	225	56	15	169	88	4	144
25	0	4	57	0	4	89	0	1
26	0	4	58	0	4	90	8	100
27	0	25	59	0	1	91	0	1
28	0	16	60	28	169	92	0	16
29	0	1	61	0	1	93	0	4
30	0	16	62	0	4	94	0	4
31	0	1	63	0	16	95	0	1
32	38	2601	64	1576	71289	96	4197	53361

n	$\|Z\|$	$\|R\|^2$
97	0	1
98	2	25
99	0	4
100	20	256
101	0	1
102	0	16
103	0	1
104	11	196
105	0	4
106	0	4
107	0	1
108	327	2025
109	0	1
110	0	36
111	0	4
112	92	1849
113	0	1
114	0	36
115	0	1
116	0	25
117	0	16
118	0	4
119	0	1
120	350	2209
121	0	4
122	0	4
123	0	1
124	0	16
125	0	25
126	24	256
127	0	1
128	481816	5419584

n	$\|Z\|$	$\|R\|^2$
129	0	4
130	0	16
131	0	1
132	12	100
133	0	1
134	0	4
135	0	25
136	14	225
137	0	1
138	0	16
139	0	1
140	6	121
141	0	1
142	0	4
143	0	1
144	6790	38809
145	0	1
146	0	4
147	2	36
148	0	25
149	0	1
150	26	169
151	0	1
152	4	144
153	0	4
154	0	16
155	0	4
156	37	324
157	0	1
158	0	4
159	0	1
160	3145	56644

n	$\|Z\|$	$\|R\|^2$
161	0	1
162	70	3025
163	0	1
164	0	25
165	0	4
166	0	4
167	0	1
168	448	3249
169	0	4
170	0	16
171	0	25
172	0	16
173	0	1
174	0	16
175	0	4
176	54	1764
177	0	1
178	0	4
179	0	1
180	276	1369
181	0	1
182	0	16
183	0	4
184	4	144
185	0	1
186	0	36
187	0	1
188	0	16
189	6	169
190	0	16
191	0	1
192	219139	2380849

4 $R(C_{p^n}, [A])$ Revisited

Lastly, we consider an already solved problem! For $G = C_{p^n}$, for each $p^r | p^n$ one has, of course, $|Sub_{p^r}(G)| = 1$.

For a non-cyclic Abelian p-group M of order p^n, one has that $M \cong C_{p^{\lambda_1}} \times C_{p^{\lambda_2}} \cdots \times C_{p^{\lambda_t}}$ where $\lambda_1 + \lambda_2 + \cdots + \lambda_t = n$ is a partition, where, without loss of generality, $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_t$. Not unexpectedly, a given non-cyclic Abelian p-group has *many* subgroups for each order. Tarnauceanu and Toth, [16], aggregate a number of older results as:

Theorem 4.1: *For every partition $\mu \preceq \lambda$ (i.e. $\mu_i \leq \lambda_i$) the number of subgroups of type μ in G_λ is*

$$\alpha_\lambda(\mu; p) = \prod_{i \geq 1} p^{(a_i - b_i) b_{i+1}} \binom{a_i - b_{i+1}}{b_i - b_{i+1}}_p,$$

where $\lambda' = (a_1, \ldots)$ and $\mu' = (b_1, \ldots)$ are the partitions conjugate to λ and μ, respectively, and

$$\binom{n}{k}_p = \frac{\prod_{i=1}^{n}(p^i - 1)}{\prod_{i=1}^{k}(p^i - 1) \prod_{i=1}^{n-k}(p^i - 1)}$$

is the Gaussian binomial coefficient (it is understood that $\prod_{i=1}^{m}(p^i - 1) = 1$ for $m = 0$).

In [11] Kerby and Rode (extending an old result due to Reinhold Baer) show that the characteristic subgroups of M of order p^r correspond to partitions/tuples of r, $\mathbf{a} = \{a_i\}$ termed 'canonical', namely

- $a_i \leq a_{i+1}$ for all $i \in \{2, \ldots, t\}$ and
- $a_{i+1} - a_i \leq \lambda_{i+1} - \lambda_i$ for all $i \in \{1, \ldots, t-1\}$

where, the total number of subgroups of order r would be the total number of such partitions for each r from 1 to n.

What one discovers is that for sufficiently large n there are various $r \leq n$ for which there are more than one canonical partitions of r. For example, if

$M = C_p \times C_{p^3}$ ($n = 4$) there are two canonical partitions of 2, namely $\{1, 1\}$ and $\{0, 2\}$, which therefore correspond to two characteristic subgroups of order p^2. As such $R(C_{p^4}, [C_p \times C_{p^3}]) = \emptyset$. Another example is for $M = C_p \times C_{p^4}$, where there are two characteristic subgroups of order p^2 and two of order p^3.

For $n = 6$ we have four different partitions of n which each give rise to more than one canonical tuples for subgroups of particular orders, namely $6 = 1 + 2 + 3 = 1 + 1 + 4 = 2 + 4 = 1 + 5$, and thus

- $R(C_{p^6}, [C_p \times C_{p^2} \times C_{p^3}]) = \emptyset$
- $R(C_{p^6}, [C_p \times C_p \times C_{p^4}]) = \emptyset$
- $R(C_{p^6}, [C_{p^2} \times C_{p^4}]) = \emptyset$
- $R(C_{p^6}, [C_p \times C_{p^5}]) = \emptyset$

Looking at larger n, we can consider all the partitions of n, which we denote np and then count those which give rise to *more than one* canonical tuples for some $r \leq n$, which we denote nc. One observes that the fraction nc/np of partitions of n which give rise to > 1 characteristic subgroups of some order approaches 1.

n	nc	np	nc/np
1	0	1	0
2	0	2	0
3	0	3	0
4	1	5	0.2
5	1	7	0.142
6	4	11	0.363
7	4	15	0.266
8	10	22	0.454
9	13	30	0.433
10	23	42	0.547
11	27	56	0.482
12	52	77	0.675
13	60	101	0.594

n	nc	np	nc/np
14	94	135	0.696
15	118	176	0.670
16	175	231	0.757
17	213	297	0.717
18	310	385	0.805
19	373	490	0.761
20	528	627	0.842
21	643	792	0.811
22	862	1002	0.860
23	1044	1255	0.832
24	1403	1575	0.891
25	1699	1958	0.868
26	2199	2436	0.903

The takeaway from this is that we should expect $R(C_{p^n}, [M])$ to be empty for most non-cyclic Abelian p-groups. Of course, this is not a new result, but it's interesting to compare this method to the usual argument which relies on the impossibility of $G \leq Hol(N)$ if G is cyclic of order p^n and N is a non-cyclic p-group of the same order.

References

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

[2] N.P. Byott. Uniqueness of Hopf Galois structure of seperable field extensions. *Comm. Algebra*, 24:3217–3228, 1996.

[3] N.P. Byott. Hopf-Galois structures on Galois field extensions of degree pq. *J. Pure Appl. Algebra*, 188(1-3):45–57, 2004.

[4] S. Carnahan and L. Childs. Counting Hopf Galois Structures on Non-Abelian Galois Field Extensions. *J. Algebra*, 218:81–92, 1999.

[5] S.U. Chase and M. Sweedler. *Hopf Algebras and Galois Theory*. Number 97 in Lecture Notes in Mathematics. Springer Verlag, Berlin, 1969.

[6] S. C. Featherstonhaugh, A. Caranti, and L. N. Childs. Abelian hopf galois structures on prime-power galois field extensions. *Trans. Amer. Math. Soc.*, 364:3675–3684, 2002.

[7] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.3*, 2002. http://www.gap-system.org.

[8] C. Greither and B. Pareigis. Hopf Galois theory for separable field extensions. *J. Algebra*, 106:239–258, 1987.

[9] M. Hall. *The Theory of Groups*. Macmillan, New York, 1959.

[10] F-P Heider and P. Kolvenbach. The Construction of SL(2,3)-Polynomials. *J. Number Theory*, 19:392–411, 1984.

[11] B. Kerby and E. Rode. Characteristic subgroups of finite abelian groups. *Comm. Algebra*, 39(4):1315–1343, 2011.

[12] A. Koch, T.Kohl, P. Truman, and R. Underwood. Normality and short exact sequences of hopf-galois structures. *Arxiv preprint GR*, 2017.

[13] T. Kohl. Classification of the hopf galois structures on prime power radical extensions. *J. Algebra*, 207:525–546, 1998.

[14] J. Nganou. How rare are subgroups of index 2? *Mathematics Magazine*, 85:215–220, 2012.

[15] K.D. Wallace R.R. Crawford. On the number of subgroups of index two - an application of goursat's theorem for groups. *Mathematics Magazine*, 48(3):172–174, 1975.

[16] M. Tarnauceanu and L. Toth. On the number of subgroups of a given exponent in a finite abelian group. *Publ. Inst. Math (Beograd) (N.S.)*, 101:121–133, 2017.