

Characteristic Subgroup Lattices and Hopf-Galois Structures

Timothy Kohl

Boston University

May 21, 2018

Hopf-Galois Theory

An extension K/k is Hopf-Galois if there is a k -Hopf algebra H and a k -algebra homomorphism $\mu : H \rightarrow \text{End}_k(K)$ 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 $I \otimes \mu : K \# H \xrightarrow{\cong} \text{End}_k(K)$

Hopf-Galois theory was developed to address the failure of ordinary Galois theory for non-separable extensions.

However, Greither and Pareigis [3] realized that separable, but not necessarily normal, extensions could be given Hopf-Galois structures.

Indeed, a field extension K/k which is Galois under the action of $G = \text{Gal}(K/k)$ is canonically Hopf-Galois with respect to the action of $H = k[G]$ by linear independence of characters.

What was also observed (which are the cases we will examine here), is that an already Galois extension K/k with $G = \text{Gal}(K/k)$ 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 $G = \text{Gal}(K/k)$. G acting on itself by left translation yields an embedding

$$\lambda : G \hookrightarrow B = \text{Perm}(G)$$

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

Theorem

[3] *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. $\lambda(G) \leq \text{Norm}_B(N)$ 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

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

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 presenter, as well as Byott, Caranti, Childs, and others.

For example, 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 $R(G, [M]) = \emptyset$.

(Characteristic) Subgroup Lattices

The technique we will employ is different than those used in earlier analyses, which relied on structural facts about groups of a given order or isomorphism type, in so far as what the embedding $\lambda(G) \leq \text{Norm}_B(N)$ permitted or prevented.

Rather we shall utilize the analog of the classical correspondence between sub-groups of the Galois group and intermediate fields.

In the setting of a Hopf-Galois extension K/k with action by a k -Hopf algebra H , one has:

Theorem

The correspondence

Fix : $\{k\text{-sub-Hopf algebras of } H\} \rightarrow \{\text{subfields } k \subseteq F \subseteq K\}$ given by

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

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

From Chase and Sweedler [1], and extrapolated in Greither-Pareigis, and in TARP-SES [6, Prop 2.2] we have:

Proposition

For a normal extension K/k with $G = \text{Gal}(K/k)$ 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 $\text{Fix}(H_P) = F = K^J$, one has a modification of the aforementioned Galois correspondence.

The following is basically [6, Thm. 2.4, Cor. 2.5 and 2.6].

The correspondence

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

given by

$$\Psi(P) = \text{Orb}_P(i_G) = \{q(i_G) \mid q \in P\} = J$$

is injective and $K^{H_P} = F = K^J$. (Note, J is a subgroup of G .)

Note 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 $m \mid |G|$ we let

$$Sub_m(G) = \{\text{subgroups of } G \text{ of order } m\}$$

$$CharSub_m(N) = \{\text{characteristic subgroups of } N \text{ of order } m\}$$

and thus we have an injective correspondence

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

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

The question we consider is, for a given N where $|N| = |G|$, can we discern whether $|CharSub_m(N)| > |Sub_m(G)|$ for at least one m , in which case one must conclude that $R(G, [N]) = \emptyset$?

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.

$$(G, [M]) = (A_4, Q_3) \rightarrow |Sub_6(G)| = 0 \text{ and } |CharSub_6(M)| = 1$$

$$(G, [M]) = (A_4, C_{12}) \rightarrow |Sub_6(G)| = 0 \text{ and } |CharSub_6(M)| = 1$$

$$(G, [M]) = (A_4, D_6) \rightarrow |Sub_6(G)| = 0 \text{ and } |CharSub_6(M)| = 1$$

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.

Index 2 Subgroups - One Versus None

Following Nganou [7] we can apply some basic, yet very useful, group theory facts to examine the index 2 subgroups of a given group.

Theorem ([7])

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

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

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

If $M = C_4 \times S_3$ or $(C_6 \times C_2) \times C_2$ 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 $C_6 \times C_2 \times C_2$.

[Note: 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 via this criterion.

$G \downarrow M \rightarrow$	$C_3 \times C_8$	C_{24}	$SL_2(\mathbb{F}_3)$	$C_3 \times Q_2$	$C_4 \times S_3$	D_{12}	$C_2 \times (C_3 \times C_4)$	$(C_6 \times C_2) \times C_2$	$C_{12} \times C_2$	$C_3 \times D_4$	$C_3 \times Q_2$	S_4	$C_2 \times A_4$	$C_2 \times C_2 \times S_3$	$C_6 \times C_2 \times C_2$
$C_3 \times C_8$	4	6	24	4	0	4	0	0	0	6	6	0	0	0	0
C_{24}	4	2	0	4	0	4	0	0	0	2	2	0	0	0	0
$SL_2(\mathbb{F}_3)$	0	0	10	0	0	0	0	0	0	0	8	0	0	0	8
$C_3 \times Q_2$	28	18	0	28	56	28	28	56	18	18	6	0	0	28	6
$C_4 \times S_3$	16	12	0	28	56	28	52	56	30	18	6	24	0	40	12
D_{12}	4	6	0	28	56	28	76	56	42	18	6	0	0	52	18
$C_2 \times (C_3 \times C_4)$	24	12	0	28	56	28	36	56	30	18	6	0	48	32	12
$(C_6 \times C_2) \times C_2$	12	6	0	28	56	28	60	56	42	18	6	24	48	44	18
$C_{12} \times C_2$	8	4	0	12	24	12	20	24	10	6	2	0	0	16	4
$C_3 \times D_4$	4	2	0	12	24	12	28	24	14	6	2	16	0	20	6
$C_3 \times Q_2$	12	6	16	12	24	12	12	24	6	6	2	0	0	12	2
S_4	0	0	0	0	0	0	0	0	0	0	0	8	36	24	48
$C_2 \times A_4$	0	0	0	0	0	0	0	0	0	0	8	12	16	8	8
$C_2 \times C_2 \times S_3$	0	0	0	228	456	228	228	456	126	126	42	48	0	152	24
$C_6 \times C_2 \times C_2$	0	0	0	84	168	84	84	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 F/\mathbb{Q} where $\text{Gal}(F/\mathbb{Q}) \cong \text{SL}_2(\mathbb{F}_3)$.

For example, Heider and Kolvenbach [4], found that the splitting field of

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

is one such $\text{SL}_2(\mathbb{F}_3)$ Galois extension.

We use the notation

$$l_2(G) = [G : G^2] - 1$$

for the number of index 2 subgroups, as given in Crawford and Wallace [8] who, using Goursat's theorem, present a number of basic facts, namely

- $l_2(G_1 \times G_2) = l_2(G_1)l_2(G_2) + l_2(G_1) + l_2(G_2)$
- If $l_2(G) > 0$ then $l_2(G) \equiv 1, \text{ or } 3 \pmod{6}$

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 $l_2(G) = 0$ 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

$$\begin{aligned}l_2(C_2 \times A_4) &= l_2(C_2)l_2(A_4) + l_2(C_2) + l_2(A_4) &&= 1 \cdot 0 + 0 + 1 = 1 \\l_2(C_{12} \times C_2) &= l_2(C_{12})l_2(C_2) + l_2(C_{12}) + l_2(C_2) &&= 1 \cdot 1 + 1 + 1 = 3 \\l_2(C_3 \times D_4) &= l_2(C_3)l_2(D_4) + l_2(C_3) + l_2(D_4) &&= 0 \cdot 3 + 0 + 3 = 3 \\l_2(C_4 \times S_3) &= l_2(C_4)l_2(S_3) + l_2(C_4) + l_2(S_3) &&= 1 \cdot 1 + 1 + 1 = 3\end{aligned}$$

What is most interesting about the formula

$$l_2(G_1 \times G_2) = l_2(G_1)l_2(G_2) + l_2(G_1) + l_2(G_2)$$

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, $l_2(G_1) = 0$ and $l_2(G_2) = 0$ or 1 for then $l_2(G_1 \times G_2) = 0$ or 1 as well.

If $l_2(G_1) = 0$ and $l_2(G_2) = 0$ then, of course, $l_2(G_1 \times G_2) = 0$.

If G_1 has odd order then $l_2(G_1) = 0$ so if either G_1 has odd order and G_2 even, or both G_1 and G_2 are even, with $l_2(G_1) = l_2(G_2) = 0$ as in the table below, then $l_2(G_1 \times G_2) = 0$.

- 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 $l_2(G_1) = 0$ and $l_2(G_2) = 1$ then $l_2(G_1 \times G_2) = 1$.

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 l_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

$$\begin{aligned}l_2(C_3 \times C_3 \times C_4) &= l_2(C_3)l_2(C_3 \times C_4) + l_2(C_3) + l_2(C_3 \times C_4) \\ &= 0 \cdot 1 + 0 + 1 \\ &= 1\end{aligned}$$

which is in agreement with the computation done directly by $[M : M^2] - 1$.

Note: If we expand out $l_2(G_1 \times G_2 \times G_3)$ then we find that

$$\begin{aligned}l_2(G_1 \times G_2 \times G_3) &= e_1(l_2(G_1), l_2(G_2), l_3(G_3)) + e_2(l_2(G_1), l_2(G_2), l_3(G_3)) + \\ &\quad e_3(l_2(G_1), l_2(G_2), l_3(G_3)) \\ &= l_2(G_1) + l_2(G_2) + l_2(G_3) + l_2(G_1)l_2(G_2) + l_2(G_1)l_2(G_3) + l_2(G_2)l_2(G_3) \\ &\quad l_2(G_1)l_2(G_2)l_2(G_3)\end{aligned}$$

Also, it's not hard to prove that this 'product formula' for $l_2(G_1 \times G_2)$ holds for semi-direct products of cyclic groups, since one can show that

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

so that, for example:

$$l_2(C_3 \rtimes C_4) = l_2(C_3)l_2(C_4) + l_2(C_3) + l_2(C_4) = 0 \cdot 1 + 0 + 1 = 1$$

If we define

$z_2(n)$ = the number of groups of order n with no index two subgroups

$u_2(n)$ = the number of groups of order n with one index two subgroup

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

← note that the $|CharSub_{12}(M)| > |Sub_{12}(G)|$
criterion holds for 10 pairings overall

Beyond index two, there may be characteristic subgroups of different orders. For index p , one replaces G^2 with $G^p[G, G]$ where $G^p = \langle \{g^p \mid g \in G\} \rangle$ with the $[G, G]$ factor appearing in order to make $G/G^p[G, G]$ an elementary Abelian p group, whose index p subgroups are in bijective correspondence with the normal index p subgroups of G .

(Note: If G is a p -group already then $G^p[G, G]$ is the Frattini subgroup.)

As such, one replaces $I_2(G)$ with $N_p(G)$ ([8, remarks following Thm. 7]) where

$$\begin{aligned} N_p(G) &= \frac{p^k - 1}{p - 1} \\ &= \frac{[G : G^p[G, G]] - 1}{p - 1} \end{aligned}$$

which is, again, the number of hyperplanes in the resulting finite vector space.

Using GAP, [2] one can readily enumerate the subgroups, both characteristic or not, of each of the different groups of a given order

We present a table of some compiled counts of the number of pairs $R(G, [M])$ which are forced to be empty by this criterion (which we denote $|RZ|$) as compared with square of the number of groups of order n (denoted $|R|^2$) representing all possible pairings of groups of order n .

n	$ RZ $	$ R ^2$
4	0	4
5	0	1
6	0	4
7	0	1
8	0	25
9	0	4
10	0	4
11	0	1
12	3	25
13	0	1
14	0	4
15	0	1
16	5	196
17	0	1
18	2	25
19	0	1
20	0	25
21	0	4
22	0	4
23	0	1
24	20	225
25	0	4
26	0	4
27	0	25
28	0	16
29	0	1
30	0	16
31	0	1
32	38	2601
33	0	1

n	$ RZ $	$ R ^2$
34	0	4
35	0	1
36	34	196
37	0	1
38	0	4
39	0	4
40	11	196
41	0	1
42	0	36
43	0	1
44	0	16
45	0	4
46	0	4
47	0	1
48	244	2704
49	0	4
50	2	25
51	0	1
52	0	25
53	0	1
54	8	225
55	0	4
56	15	169
57	0	4
58	0	4
59	0	1
60	28	169
61	0	1
62	0	4
63	0	16

n	$ RZ $	$ R ^2$
64	1576	71289
65	0	1
66	0	16
67	0	1
68	0	25
69	0	1
70	0	16
71	0	1
72	422	2500
73	0	1
74	0	4
75	1	9
76	0	16
77	0	1
78	0	36
79	0	1
80	149	2704
81	5	225
82	0	4
83	0	1
84	28	225
85	0	1
86	0	4
87	0	1
88	4	144
89	0	1
90	8	100
91	0	1
92	0	16
93	0	4

n	$ RZ $	$ R ^2$
94	0	4
95	0	1
96	4197	53361
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

n	$ RZ $	$ R ^2$
124	0	16
125	0	25
126	24	256
127	0	1
128	366329	5419584
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

$R(C_{p^n}, [A])$ 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, WLOG $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_t$.

Not unexpectedly, a given non-cyclic Abelian p -group has *many* subgroups for each order. Tarnauceanu and Toth, [9], aggregate a number of older results as:

Theorem

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 $\lambda' = (a_1, \dots)$ and $\mu' = (b_1, \dots)$ 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 [5] Kerby and Turner (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 $i \in \{2, \dots, t\}$ and
- $a_{i+1} - a_i \leq \lambda_{i+1} - \lambda_i$ for all $i \in \{1, \dots, t-1\}$

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 observe that the fraction 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
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

Here nc denotes the number of partitions of n which give rise to more than one canonical partition for a given $r \leq n$, and np is the number of partitions of n .

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 as compared to the usual argument which relies on the impossibility of $G \leq \text{Hol}(N)$ if G is cyclic of order p^n and N is a non-cyclic p -group of the same order.

Thank you!



S.U. Chase and M. Sweedler.

Hopf Algebras and Galois Theory.

Number 97 in Lecture Notes in Mathematics. Springer Verlag, Berlin, 1969.

9



The GAP Group.

GAP – Groups, Algorithms, and Programming, Version 4.3, 2002.

<http://www.gap-system.org>.

29



C. Greither and B. Pareigis.

Hopf Galois theory for separable field extensions.

J. Algebra, 106:239–258, 1987.

3, 5




F-P Heider and P. Kolvenbach.


The Construction of $SL(2,3)$ -Polynomials.

J. Number Theory, 19:392–411, 1984.

19

 B. Kerby and E. Turner.
Characteristic subgroups of finite abelian groups.
Arxiv preprint GR, 2017.


33

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

9, 10

 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.

20, 28



M. Tarnauceanu and L. Toth.

On the number of subgroups of a given exponent in a finite abelian group.

Arxiv preprint GR, 2017.

32