NORMALITY AND SHORT EXACT SEQUENCES OF HOPF-GALOIS STRUCTURES

ALAN KOCH, TIMOTHY KOHL, PAUL J. TRUMAN, AND ROBERT UNDERWOOD

ABSTRACT. Every Hopf-Galois structure on a finite Galois extension K/k where $G = Gal(K/k)$ corresponds uniquely to a regular subgroup $N \leq B = \mathrm{Perm}(G)$, normalized by $\lambda(G) \leq B$, in accordance with a theorem of Greither and Pareigis. The resulting Hopf algebra which acts on K/k is $H_N = (K[N])^{\lambda(G)}$. For a given such N we consider the Hopf-Galois structure arising from a subgroup $P \triangleleft N$ that is also normalized by $\lambda(G)$. This subgroup gives rise to a Hopf sub-algebra $H_P \subseteq H_N$ with fixed field $F = K^{H_P}$. By the work of Chase and Sweedler, this yields a Hopf-Galois structure on the extension K/F where the action arises by base changing H_P to $F \otimes_k H_P$ which is an F-Hopf algebra. We examine this analogy with classical Galois theory, and also examine how the Hopf-Galois structure on K/F relates to that on K/k. We will also pay particular attention to how the Greither-Pareigis enumeration/construction of those H_P acting on K/F relates to that of the H_N which act on K/k. In the process we also examine short exact sequences of the Hopf algebras which act, whose exactness is directly tied to the descent theoretic description of these algebras.

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

MSC: 16T05,20B35,11S20

1. INTRODUCTION

A separable extension of fields K/k is Hopf-Galois if there exists a k-Hopf algebra H (with $\Delta : H \to H \otimes_k H$ the co-multiplication, and $\epsilon : H \to k$ the co-unit) together with a k-algebra homomorphism

$\mu : H \to End_k(K)$ such that

$$\mu(h)(xy) = \sum_{(h)} \mu(h_{(1)})(x)\mu(h_{(2)})(y),$$
$$\mu(h)(1) = \varepsilon(h)(1),$$

where $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$, the fixed ring

$$K^H = \{x \in K | \mu(h)(x) = \varepsilon(h)x \ \forall h \in H\}$$

is precisely k, and the induced map $1\#\mu : K\#H \to End_k(K)$ is an isomorphism of k-algebras. The canonical example of a Hopf-Galois extension is the case where K/k is Galois with $G = Gal(K/k)$. In this case, the group ring $k[G]$ acts as linear combinations of automorphisms which, by Dedekind's linear independence of characters, yields an action of $k[G]$ on K/k which makes it Hopf-Galois. For extensions which are normal or not, the determination of which Hopf-Galois structures that may arise (if any) and how they act are described and enumerated using a result of Greither and Pareigis, the setup of which we outline here.

Let $\tilde{K}/k$ be the normal closure of K/k where $G = Gal(\tilde{K}/k)$ and $G' = Gal(\tilde{K}/K)$. If $S = G/G'$ (left cosets) then G acts on S via $\lambda : G \hookrightarrow B = \text{Perm}(S)$ where $\lambda(a)(bG') = abG'$. One has that $\tilde{K}\otimes K \cong \text{Map}(S, \tilde{K})$ where $\text{Map}(S, \tilde{K})$ is the $\tilde{K}$-algebra of set maps from S to $\tilde{K}$ with basis e_s for $s \in S$ which is also a G-set via $g(e_s) = e_{\lambda(g)s}$. Moreover $\text{Map}(S, \tilde{K})/\tilde{K}$ is an N-Galois extension of rings precisely for any N which is a regular (transitive and fixed-point free) subgroup of B. The action of an $m \in N$ on an element of $\text{Map}(S, \tilde{K})$ arises from letting $n(e_s) = e_{n(s)}$. As such $\text{Map}(S, \tilde{K})/\tilde{K}$ is Hopf-Galois with respect to the action of $\tilde{K}[N]$. If N is normalized by $\lambda(G)$ inside B then one may descend this to get an action of $H = (\tilde{K}[N])^{\lambda(G)}$ on $\text{Map}(S, \tilde{K})^{\lambda(G)}/\tilde{K}^G$ where $(\tilde{K} \otimes K)^{\lambda(G)} \cong (\tilde{K})^G \otimes K \cong k \otimes K \cong K$ and $\tilde{K}^G = k$ of course. That is H yields a Hopf-Galois structure on K/k. Note,

$$\text{Map}(S, \tilde{K})^{\lambda(G)} = \Big\{ \sum_{gG' \in S} g(x)e_{gG'} \mid x \in K \Big\}$$

which the reader can verify is a ring isomorphic to K since the $e_{gG'}$ are orthogonal idempotents which form the basis of $\text{Map}(S, \tilde{K})$, together with the fact that $\tilde{K}^{G'} = K$. If K/k is already normal then G' is trivial, $\tilde{K} = K$, $S = G$, $\lambda(G)$ embeds in $\text{Perm}(S)$ as the usual left

regular representation, and

$$(1) \qquad K \cong \Big\{ \sum_{g \in G} g(x) e_g \mid x \in K \Big\}$$

where $n(e_g) = e_{n(g)}$ for $N \leq \mathrm{Perm}(G)$.

Whether K/k is normal or not, we have the following.

Theorem: [5, Thm. 2.1] Let K/k be a separable field extension, S and B as above, then there is a 1-1 correspondence between:

(a) Hopf-Galois structures on K/k

(b) regular subgroups $N \leq B$ that are normalized by $\lambda(G) \leq B$.

An important point to note is that the action of $H = (\tilde{K}[N])^{\lambda(G)}$ comes directly from the choice of regular subgroup, and not on the isomorphism class of H as a k-Hopf algebra. Indeed, one can frequently find regular groups $N, M \leq B$, normalized by $\lambda(G)$, which are isomorphic as abstract groups, but (being distinct) give rise to distinct actions on K/k. Moreover, actions aside, the resulting fixed rings $H_N = (\tilde{K}[N])^{\lambda(G)}$ and $H_M = (\tilde{K}[M])^{\lambda(G)}$ may be isomorphic as Hopf algebras. The point is that the correspondence is between regular subgroups and pairs (H, μ) where H is a k-Hopf algebra with a structure map $\mu : H \to End_k(K)$.

In the Greither-Pareigis framework, the 'classical' action of $k[G]$ on K/k when $G = Gal(K/k)$ corresponds to the regular subgroup $N = \rho(G)$ where $\rho : G \to B$ is the right regular representation, given by $\rho(g)(x) = xg^{-1}$. Since the left and right actions commute, then $H = (K[\rho(G)])^{\lambda(G)} = K^G[\rho(G)] \cong k[G]$. The point is that the action of $\lambda(G)$ in this situation is solely on the coefficients.

One of the interesting features of this theory is that a given extension K/k may be Hopf-Galois with respect to variety of different Hopf algebras, including those arising from different (non-isomorphic) regular subgroups N. This is especially interesting in the case where K/k is already classically Galois for then it is Hopf-Galois with respect to $k[G]$ and possibly for other forms of group rings $(K[N])^{\lambda(G)}$.

What we shall consider is the Hopf-Galois analogs of the usual facts from Galois theory about the correspondence between subgroups $J \leq$

G and intermediate fields $F = K^J$, as well as the correspondence between (normal) subgroups $J \lhd G$ and the set of (normal) intermediate fields. In particular we explore how the Greither-Pareigis theory applies in these situations. We review some known facts and then introduce new results. One of the key objectives is to understand the relationships between the actions of the various regular subgroups of the different ambient symmetric groups. We shall primarily consider the case where K/k is already Galois with $G = Gal(K/k)$ and simultaneously Hopf-Galois with respect to $H_N = (K[N])^{\lambda(G)}$ for some regular subgroup $N \leq B$ where $N \neq \rho(G)$. We will also assume that N has a normal subgroup P which, under the right conditions, itself gives rise to a Hopf-Galois structure, much as the way a normal subgroup of a Galois group does classically. Moreover, since a normal subgroup $P \lhd N$ gives rise to the exact sequence of groups $1 \to P \to N \to N/P \to 1$, we wish to consider the corresponding short exact sequence of Hopf algebras which arise, specifically those Hopf algebras which act on K/k, K/F, and F/k.

2. FIXED FIELDS IN HOPF-GALOIS EXTENSIONS

Hopf-Galois extensions partially mirror some of the properties of ordinary Galois extensions. Assume K/k is a (classically) Galois extension with group G. Every intermediate field $k \subseteq F \subseteq K$ corresponds bijectively to a subgroup $J = Gal(K/F)$ such that K/F is Galois with group J; furthermore F/k is Galois if and only if $J \lhd G$, and if so, $Gal(F/k) \cong G/J$. For Hopf-Galois extensions, the correspondence is given as follows (including the broader case where K/k is not classically Galois), which is a synthesis of two related statements.

Theorem 2.1: [1, Thm. 7.6] *and* [5, Thm. 5.1]. *If K/k is Hopf-Galois with respect to a k-Hopf algebra H then there is a map*

Fix $: \{k$ *Hopf sub-algebras* $H' \subseteq H\} \to \{$*intermediate fields* $k \subseteq F \subseteq K\}$

where

$$F = \text{Fix}(H') = K^{H'} = \{x \in K \mid \mu(h)(x) = \varepsilon(h)x \; \forall h \in H'\}$$

is the fixed field with respect to H'. This correspondence is injective and inclusion reversing. Moreover, $F \otimes H'$ acts on K/F to make it Hopf-Galois.

For separable extensions, the Hopf algebras which arise are forms of group rings, which provides a fairly straightforward way of understanding what Hopf sub-algebras may appear. If $H' \subseteq H$ where $K \otimes H \cong K[N]$ then $K \otimes H'$ is a K-Hopf sub-algebra of $K[N]$. But being a Hopf sub-algebra of a group-ring one has, by for example [9, Prop. 2.1], or Exercise 2.1.25 in Radford [7], that $K \otimes H'$ must be of the form $K[P]$ for some $P \leq N$. However, in order that $H' = H_P = (K[P])^{\lambda(G)}$ be a sub-Hopf algebra of $H = H_N = (K[N])^{\lambda(G)}$ one must have that P be normalized by $\lambda(G)$. This is summarized in the following, which paraphrases a number of statements in [5] adapted to the case considered here where we are assuming K/k is classically Galois. (i.e. $\tilde{K} = K$)

Proposition 2.2: [5, Thm. 5.2 and Lemma p. 256] *The Hopf sub-algebras of $(K[N])^{\lambda(G)}$ correspond to subgroups of N that are stabilized by p_g for all $g \in G$ where $\{p_g \mid g \in G\}$ is the cocycles of automorphisms coming from conjugation by each $g \in G$. That is, a given $P \leq N$ gives rise to a Hopf sub-algebra $H_P = (K[P])^{\lambda(G)}$ if and only if $\lambda(G) \leq Norm_B(P)$.*

As such, if $P \leq N$ where N is regular, and where both are normalized by $\lambda(G)$ then $H_N = (K[N])^{\lambda(G)}$ yields a Hopf-Galois structure on K/k, and similarly $H_P = (K[P])^{\lambda(G)}$ is such that $F \otimes H_P$ yields a Hopf Galois structure on K/F where $F = K^{H_P}$.

Now, since F is an intermediate field between K and k, then $F = K^J$ the fixed field of some subgroup $J \leq G$ where $Gal(K/F) = J$. A natural question to ask is, since K/F is Galois with group J and acted on by $F \otimes H_P$ then how does it fit within the Greither-Pareigis framework? Since $F \otimes H_P$ acts on K/F then it too should be a form of a group ring over F, namely $F[P]$. As observed by Crespo et al. in [8, Prop. 8], one has $F \otimes H_P \cong (K[P])^{\lambda(J)}$ with the implication that the embedding of J in $Perm(J)$ normalizes a regular subgroup of $Perm(J)$ isomorphic to P which is certainly very natural.

Recall that a regular subgroup of B is one which is transitive and fixed-point free. As such, any subgroup of it will be fixed-point free, and such a subgroup is termed *semi-regular*. Note that regularity of $N \leq B$ can be defined as the property that N acts fixed-point freely and that $|N| = |G|$. In this section we will explore the relationship between P as a semi-regular subgroup of the regular subgroup $N \leq Perm(G)$ and P viewed as a regular subgroup of $Perm(J)$. In

particular, we shall look at how the action of $P \leq \mathrm{Perm}(G)$ on $J \leq G$ induces very naturally an embedding of $P \leq \mathrm{Perm}(J)$, as alluded to in [8, Prop. 8] mentioned above. One of our tasks will be to relate these regular and semi-regular subgroups, with a view toward quantifying the action(s) that induce a Hopf-Galois structure on F/k in the event that $P \triangleleft N$. Finally, the normality will also allow us to look at short exact sequences of Hopf algebras arising from actions on K/k, K/F and F/k.

2.1. **From subgroups of N to subgroups of G.** We begin with a question that has not yet been explored in the literature but which is in the background. How does P, giving rise to $F = K^{H_P}$, in turn give rise to that unique $J \leq G$ where $F = K^J$. We start with another variant of the Fix map, based on the equivalence

$$\{\text{subfields } F \,|\, k \subseteq F \subseteq K\} \leftrightarrow \{\text{subgroups } J \leq G\}$$

and examine the injective mapping from subgroups of $P \leq N$ normalized by $\lambda(G)$ to the set of subgroups $J \leq G$ due to the fact that P gives rise to $F = K^{H_P} = K^J$ for exactly one $J \leq G$.
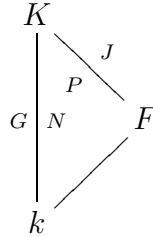
The correspondence $P \mapsto J$ is a bit mysterious, but we can show (combinatorially) how J arises from P. Also, since we wish to explore the possibility of putting a Hopf-Galois structure on F/k, then, following the analogy with ordinary Galois theory, we will ultimately restrict our attention to those P that are normal in N. This will be necessary in order to construct a form of the group ring $k[N/P]$ that will act on F/k. However, initially we shall look at how J arises from those P normalized by $\lambda(G)$.

As mentioned K/k is a Galois extension with $G = Gal(K/k)$ which is also Hopf-Galois with respect to the action of $H_N = (K[N])^{\lambda(G)}$ where $N \leq B = \mathrm{Perm}(G)$ is a regular subgroup, that is normalized by $\lambda(G)$. Since F is an intermediate field between K and k we have $F = K^J$ for J a subgroup of G. To determine J from P we shall consider, in some depth, the action of H_N and H_P on the copy of K

embedded in $\mathrm{Map}(G, K)$, namely

$$K \cong \{\sum_{g \in G} g(x)e_g \mid x \in K\}$$

mentioned above.

For $h \in H_N$ one has $h = \sum_{m \in N} c_m \cdot n$ where $c_m \in K$ and $m \in N$ where $\gamma(c_m) = c_{\lambda(\gamma)m\lambda(\gamma)^{-1}}$ for all $\gamma \in G$, since h is fixed by all of $\lambda(G)$. Since N acts on G, it is useful to consider certain 'slices' of $N \times G$ that arise from this action. We define

$$Z_{N,t} = \{(m, g) \in N \times G \mid m(g) = t\}$$

for each $t \in G$. The element h of H_N acts on a typical element of K as follows

$$h(\sum_{g \in G} g(x)e_g) = \sum_{m \in N} c_m \left(\sum_{g \in G} g(x)e_{m(g)} \right)$$

$$= \sum_{g \in G} \sum_{m \in N} c_m g(x)e_{m(g)}$$

$$= \sum_{t \in G} \left(\sum_{(m,g) \in Z_{N,t}} c_m g(x) \right) e_t$$

$$= \sum_{g \in G} g(y)e_g$$

for some $y \in K$. This implies that

$$t(y) = \left(\sum_{(m,g) \in Z_{N,t}} c_m g(x) \right)$$

for all $t \in G$, in particular for $t = i_G$ (the identity) which means

$$y = \sum_{(m,g) \in Z_{m,i_G}} c_m g(x)$$

$$= \sum_{m \in N} c_m m^{-1}(i_G)(x)$$

by regularity of the action of N on G. Now, since K/k is Hopf-Galois with respect to H_N then $\mathrm{Fix}(H_N) = K^{H_N}$ which are those elements $x \in K$ such that

$$h(x) = \varepsilon(h)x = (\sum_{m \in N} c_m)x$$

which, since $\{m^{-1}(i_G) \mid m \in N\} = G$, is precisely the field k since $K^G = k$. Similarly, for H_P we have $F = K^{H_P}$. Now, $H_P \subseteq H_N$ in a natural way since $P \leq N$, in particular those $h \in H_N$ of the form $\sum_{q \in P} d_q \cdot q$ where $\gamma(d_q) = d_{\lambda(\gamma)q\lambda(\gamma)^{-1}}$ for all $\gamma \in G$. For these elements of H_P we have, for $x \in K$, that

$$
h(x) = h(\sum_{g \in G} g(x)e_g) = \sum_{q \in P} d_q \left(\sum_{g \in G} g(x)e_{q(g)} \right)
$$

$$
= \sum_{t \in G} \left(\sum_{(q,g) \in Z_{P,t}} d_q(x) \right) e_t
$$

$$
= \sum_{q \in P} d_q q^{-1}(i_G)(x)
$$

and since P is a subgroup of the regular permutation group N, it is semi-regular. As such, $|\{q^{-1}(i_G) \mid q \in P\}| = |P|$. Also $x \in K^{H_P}$ if

$$
h(x) = \sum_{q \in P} d_q q^{-1}(i_G)(x) = \varepsilon(h)x = (\sum_{q \in P} d_q)x
$$

and since $F = K^{H_P}$ is an intermediate field, then $F = K^J$ for some $J \leq G$ where $|J| = \dim_k(H_P) = |P|$. We can relate J to P by considering the action of an element which is guaranteed to lie in H_P, namely $h = \sum_{q \in P} 1 \cdot q$. For $x \in F$ one has $h(x) = |P|x$ which implies that

$$
\sum_{q \in P} q^{-1}(i_G)(x) = |P|x
$$

$$
= |J|x
$$

where $\{q^{-1}(i_G) \mid q \in P\}$ is some subset of G. What we wish to show is that this subset is precisely J. To show this we use the following (somewhat more general statement) which seems standard, but no reference could be found.

Proposition 2.3: *For $G = Gal(K/k)$ with $F = K^J$ for $J \leq G$ as above, if $S = \{\sigma_1, \ldots, \sigma_r\} \subseteq G$ such that*

$$
\sum_{i=1}^{r} \sigma_i(x) = rx
$$

for all $x \in F$, then $S \subseteq J$.

Proof. The key to the proof is to show that if the sum of the elements of S acts like a scalar multiple of the identity on F, then all $\sigma_i \in S$ are actually elements of J. So let's assume that for each $x \in F$ one has $\sigma_i(x) = x + \delta_{x,i}$. Since $\sum_{i=1}^r \sigma_i(x) = rx$ then we must have $\sum_{i=1}^r \delta_{x,i} = 0$. If we use the fact that each σ_i is an automorphism of K (in particular that it is multiplicative), and if we assume $\sum_{i=1}^r \delta_{x,i}^l = 0$ for $j = 1 \ldots n-1$ for each n then

$$
\begin{aligned}
rx^n &= \sum_{i=1}^r \sigma_i(x^n) \\
&= \sum_{i=1}^r (x + \delta_{x,i})^n \\
&= \sum_{i=1}^r \sum_{j=0}^n \binom{n}{j} x^j \delta_{x,i}^{n-j} \\
&= \sum_{j=0}^n \sum_{i=1}^r \binom{n}{j} x^j \delta_{x,i}^{n-j} \\
&= \sum_{j=0}^n \binom{n}{j} x^j \sum_{i=1}^r \delta_{x,i}^{n-j} \\
&= \sum_{i=1}^r \delta_{x,i}^n + rx^n
\end{aligned}
$$

which means $\sum_{i=1}^r \delta_{x,i}^n = 0$. To complete the proof we invoke the Newton-Girard formulæ which, stated formally as [3, Thm. 8 - Ch. 7] are that (over a field containing $\mathbb{Q}$) the ring of symmetric functions in r variables $t_1, \ldots, t_r$ is generated by the power sum polynomials $\sum_{i=1}^r t_i^n$. Thus, for any $x \in F$ if we let $f(z) = (z - \delta_{x,1}) \cdots (z - \delta_{x,r})$ then the coefficients of every term of $f(z)$ of degree lower than r must be zero. That is, $f(z) = z^r$ so all its roots, namely the $\delta_{x,i}$, are identically zero. As such, $\sigma_i(x) = x$ for all $x \in F$ for $i = 1, \ldots, r$ so that each $\sigma_i \in J$. □

We use this now to show how J corresponds to P.

Theorem 2.4: *For K/k with $G = Gal(K/k)$ and N, P and $F = K^{H_P}$ as above, $\{q^{-1}(i_G) \mid q \in P\} = J$.*

Proof. As seen above, for $x \in F$ one has $\sum_{q \in P} q^{-1}(i_G)(x) = |J|x$ where $\{q^{-1}(i_G) \mid q \in P\} \subseteq G$. By Prop. 2.3 above this set must consist of elements of J and since $|P| = |J|$ this set is exactly J. $\square$

We will need the following in the next section.

Corollary 2.5: *Given N, P, G and J as above, for $g \in G$, $Orb_P(g) = \{q(g) \mid q \in P\} = gJ$, the left coset of g in J.*

Proof. Since G normalizes P then $\lambda(g)^{-1}P\lambda(g) = P$ and by Thm. 2.4 above, $Orb_P(i_G) = J$ which implies

$$J = \{\lambda(g)^{-1}q\lambda(g)(i_G) \mid q \in P\} = \{g^{-1}q(g) \mid q \in P\}$$

and so left multiplying both sides by g yields the result. $\square$

Now, given that sub-Hopf algebras of H_N correspond injectively to intermediate fields $k \subseteq F \subseteq K$, which, in turn, corresponds bijectively to subgroups of $J \leq G$, we also have

Corollary 2.6: *The correspondence*

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

given by $\Psi(P) = Orb_P(i_G)$ is injective where the subset $Orb_{\lambda(J)}(i_G)$ is the subgroup corresponding to the Galois group of K/K^{H_P}.

This is intriguing in that we know that P *must* correspond to $J = Gal(K/K^{H_P})$, but the precise relationship (as subgroups of $\mathrm{Perm}(G)$) between P and $\lambda(J)$ is still a bit mysterious. Of course, $\Psi(e_N) = \{i_G\}$ and $\Psi(N) = G$ but when looking at different specific examples by hand or using GAP [4], it does not seem that one can recover J in any kind of obvious way from P as say a normalizer or centralizer of something in $\mathrm{Perm}(G)$. Rather the correspondence here is seemingly based on purely combinatorial considerations, namely that the elements of P must give rise to a bijection (at the level of sets) from J to itself within $\mathrm{Perm}(G)$. This will be of key importance in examining the relationship between the actions of $\lambda(G)$ and $\lambda(J)$ as compared to the actions of N and P, in particular the role that P being normal in N plays, as well as the differences that arise when $J \triangleleft G$ versus when it isn't.

At this stage, there are two natural questions to ask. Is Ψ onto, and for each such $P \leq N$, is $\Psi(P) \cong P$? From computations done

using GAP in degree 42, based on the second author's work in [6], the answer to both question is *no*. The 6 groups of order 42 are C_{42}, $C_7 \times D_3$, $(C_7 \rtimes C_3) \times C_2$, $C_3 \times D_7$, D_{21}, and $(C_7 \rtimes C_3) \rtimes C_2$. One of the reasons for looking at this class of examples is that they are well understood, and also, since 42 is the product of three primes, there is a lot more variety in the number of isomorphism classes of subgroups. The distribution of N for each G (where the column entries are G and the rows are the number of N of the given isomorphism class) are summarized below, where we show (in {}) how many of the given N give rise to Ψ which are onto.

$G \downarrow \backslash N \rightarrow$	C_{42}	$C_7 \times D_3$	$C_2 \times (C_7 \rtimes C_3)$	$C_3 \times D_7$	D_{21}	$(C_7 \rtimes C_3) \rtimes C_2$
C_{42}	1 {1}	2 {1}	4 {2}	2 {1}	4 {1}	4 {2}
$C_7 \times D_3$	3 {0}	2{1}	0	6 {0}	4 {1}	0
$C_2 \times (C_7 \rtimes C_3)$	7 {0}	14 {0}	16 {1}	14 {0}	28 {0}	28 {0}
$C_3 \times D_7$	7 {0}	14 {0}	28 {0}	2 {1}	4 {1}	28 {0}
D_{21}	21 {0}	14 {0}	0	6 {0}	4 {1}	0
$(C_7 \rtimes C_3) \rtimes C_2$	7 {0}	14 {0}	28 {0}	14 {0}	28 {0}	16 {1}

For $N = \rho(G)$ we have that every subgroup of N is normalized by $\lambda(G)$ since $\rho(G)$ and $\lambda(G)$ centralize each other. In this case Ψ is trivially onto, and the above table shows that frequently Ψ is onto *only* for $N = \rho(G)$. Other than the fact that $|P| = |\Psi(P)|$, the groups P and J can be in different isomorphism classes. For example, when $G \cong C_{42}$ there is an $N \cong C_3 \times D_7$ with $P \leq N$ where $P \cong C_{14}$ but $\Psi(P) \cong D_7$. In the final section we shall summarize more information about the degree 42 cases.

2.2. **Semi-regular subgroups and orbits.** As mentioned above, $P \leq N \leq \mathrm{Perm}(G)$, normalized by $\lambda(G) \leq B$ gives rise to $J = \Psi(P)$ where, since N is regular, we have that P is semi-regular but not transitive. Moreover, we also have that $\lambda(J) \leq \lambda(G) \leq \mathrm{Perm}(G)$ also normalizes P. And, as also mentioned earlier, $F \otimes H_P \cong (K[P])^{\lambda(J)}$ due to the fact K/F is Hopf-Galois with respect to the action of a copy of P embedded as a regular subgroup of $\mathrm{Perm}(J)$ normalized by $\lambda(J) \leq \mathrm{Perm}(J)$. These two views are tied together by Thm. 2.4 which implies that $P \leq \mathrm{Perm}(G)$ restricted to J yields this afore-mentioned regular subgroup of $\mathrm{Perm}(J)$. The virtue of this is that it mirrors the fact that $\lambda(G)$ restricted to J is naturally equal to $\lambda(J) \leq \mathrm{Perm}(J)$. In order to construct a Hopf-Galois structure on F/k we shall assume from this point onward that $P \triangleleft N$. What this yields for us is a way to view $\lambda(G)$, $\lambda(G)/\lambda(J)$ (if $J \triangleleft G$), and N/P

as subgroups of a fixed $\mathrm{Perm}(S)$ for a specifically chosen set S, where N/P acts regularly and $\lambda(G)/\lambda(J)$ normalizes this regular subgroup. This will lead naturally to a Hopf-Galois structure on F/k with associated group N/P. If J is not a normal subgroup then we can still construct a Hopf-Galois structure on F/k corresponding to N/P but the argument will be somewhat different.

We start by establishing some additional notation, namely

- $[K : F] = |J| = |P| = p$
- $[F : k] = [G : J] = [N : P] = m$
- $[K : k] = |N| = |G| = mp = n$

where p is not necessarily a prime. Our first step is to find this common set on which N/P and G/J both act. Again, we shall initially assume that $J \lhd G$ and later on relax this condition. However, we will choose the sets/actions so that in the non-normal case, we won't have to modify the arguments that much. With Cor. 2.5 in mind, together with the fact that G acts naturally on the left cosets of J in G, even if J is not normal in G, we have

$$G = g_1 J \cup g_2 J \cup \cdots \cup g_m J,$$

where $\{g_1, \ldots, g_m\}$ are a transversal of J in G, where we may assume $g_1 = i_G$. We start with the following basic fact.

Lemma 2.7: *For G, J, N and P as above, the quotient groups $\lambda(G)/\lambda(J)$ and N/P act on the cosets $\{g_1 J, \ldots, g_m J\}$ as regular permutation groups.*

Proof. We start by observing that $\lambda(G)$ acts transitively on $\{g_i J\}$ due to $\lambda(G)$ being regular, hence transitive on G itself. Similarly, since $J \lhd G$ then $\lambda(G)/\lambda(J)$ also acts transitively on $\{g_i J\}$ since given $g_i J$ and $g_j J$, then for $h \in J$,

$$\lambda(g_j g_i^{-1} h)(g_i J) = g_j g_i^{-1} h g_i J$$
$$= g_j g_i^{-1} g_i h' J \text{ for some } h' \in J \text{ by normality}$$
$$= g_j J$$

and since $|G/J| = m$ then this transitive action of $\lambda(G)/\lambda(J)$ is regular. If $m \in N$ then by Cor. 2.5

$$
\begin{aligned}
n(gJ) &= \{n(q(g)) \mid q \in P\} \\
&= \{q(n(g)) \mid q \in P\} \text{ since } P \triangleleft G \\
&= n(g)J
\end{aligned}
$$

which means N operates transitively on the cosets, so that N/P acts transitively and therefore regularly since $[N : P] = [G : J]$.   □

Before proceeding further it is worth noting how the normality of the given subgroups J and P strongly impacts the choice of object on which both $\lambda(G)/\lambda(J)$ and N/P act. By itself, $\lambda(J)$ gives rise to orbits which are precisely the *right* cosets of J in G, and, as seen above, the orbits of P on G are precisely the left cosets of J in G. When J is normal in G these coincide of course, but if J is not normal in G then G would still act naturally on its left cosets, i.e. the orbits of P. Note also, in the second half of the above proof that the transitivity of the action of N on the orbits of P uses the normality of P in N. This is partly why we require that $P \triangleleft N$ but allow for the possibility of J not being normal in G. The fact that N and P are normalized by $\lambda(G)$ yields the following.

Theorem 2.8: *For $\lambda(J) \triangleleft \lambda(G)$ and $P \triangleleft N$ as above, $\lambda(G)/\lambda(J)$ normalizes N/P as a subgroup of $\mathrm{Perm}(\{g_i J\})$.*

Proof. Let $m \in N, q \in P, \gamma \in G, h_1, h_2 \in J$ and consider $\lambda(\gamma h_1)nq\lambda(\gamma^{-1}h_2) \in (\lambda(\gamma J)(nP)(\lambda(\gamma^{-1}J))$ and observe that

$$
\begin{aligned}
\lambda(\gamma h_1)nq\lambda(\gamma^{-1}h_2)[g_i J] &= \lambda(\gamma h_1)nq[\gamma^{-1}h_2 g_i J] \\
&= \lambda(\gamma h_1)nq[\gamma^{-1}g_i J] \text{ since } J \triangleleft G \\
&= \lambda(\gamma h_1)[n(\gamma^{-1}g_i)J] \text{ since } P \text{ acts trivially on } \{g_i J\} \\
&= \lambda(\gamma)h_1[n(\gamma^{-1}g_i)J)] \\
&= \lambda(\gamma)[n(\gamma^{-1}g_i)J] \text{ again since } J \triangleleft G \\
&= [\gamma n(\gamma^{-1}g_i)J].
\end{aligned}
$$

The last set above is therefore $\lambda(\gamma)n\lambda(\gamma^{-1})P[g_i J]$. That is

$$
\lambda(\gamma J)(nP)\lambda(\gamma^{-1}J) = \lambda(\gamma)n\lambda(\gamma^{-1})P \in N/P
$$

describes the action of $\lambda(G)/\lambda(J)$ on N/P in $\mathrm{Perm}(\{g_iJ\})$. $\qquad\square$

We can now prove the following.

Theorem 2.9: *The extension F/k is Hopf-Galois with respect to the Hopf algebra $H_{N/P} = (F[N/P])^{\lambda(G)/\lambda(J)}$.*

Proof. By Lemma 2.7 $\lambda(G)/\lambda(J)$ and N/P act on $\{g_iJ\}$ (which are the cosets of J in G) where N/P is a regular subgroup of $\mathrm{Perm}(\{g_iJ\})$. This implies that $\mathrm{Map}(G/J, F)/F$ is Galois with respect to N/P and therefore that

$$(\mathrm{Map}(G/J, F))^{G/J}/F^{G/J} \leftrightarrow F/k$$

is Galois with respect to N/P as well. As such by Thm. 2.8, $H_{N/P}$ acts on F/k to make it Hopf-Galois $\qquad\square$

2.3. J **not normal in** G. What happens when J is not normal in G? Even though we assume $P \triangleleft N$, there is no reason to expect that $J = \Psi(P)$ given in Cor. 2.6 is normal in G. Using GAP we generated the following example in degree 24:

$$\begin{aligned} G = \langle &(1,2)(3,13)(4,8)(5,7)(6,9)(10,21)(11,20)(12,16)(14,18)(15,17)(19,24)(22,23), \\ &(1,3,9)(2,6,13)(4,11,23)(5,19,17)(7,15,24)(8,22,20)(10,18,12)(14,21,16), \\ &(1,4)(2,7)(3,10)(5,12)(6,14)(8,16)(9,17)(11,19)(13,20)(15,22)(18,23)(21,24) \\ &(1,5)(2,8)(3,11)(4,12)(6,15)(7,16)(9,18)(10,19)(13,21)(14,22)(17,23)(20,24)\rangle \\ &\cong S_4. \end{aligned}$$

$$\begin{aligned} \text{Then } N = \langle &(1,6,9,2,3,13)(4,15,23,7,11,24)(5,22,17,8,19,20)(10,21,12,14,18,16), \\ &(1,9,3)(2,13,6)(4,23,11)(5,17,19)(7,24,15)(8,20,22)(10,12,18)(14,16,21), \\ &(1,4)(2,7)(3,10)(5,12)(6,14)(8,16)(9,17)(11,19)(13,20)(15,22)(18,23)(21,24), \\ &(1,12)(2,16)(3,19)(4,5)(6,22)(7,8)(9,23)(10,11)(13,24)(14,15)(17,18)(20,21)\rangle \\ &\cong A_4 \times C_2 \end{aligned}$$

is regular and normalized by G, and N has a normal subgroup P

$$P = \langle (1,4)(2,7)(3,10)(5,12)(6,14)(8,16)(9,17)(11,19)(13,20)(15,22)(18,23)(21,24),$$
$$(1,5)(2,8)(3,11)(4,12)(6,15)(7,16)(9,18)(10,19)(13,21)(14,22)(17,23)(20,24),$$
$$(1,2)(3,6)(4,7)(5,8)(9,13)(10,14)(11,15)(12,16)(17,20)(18,21)(19,22)(23,24)\rangle$$
$$\cong C_2 \times C_2 \times C_2$$

which is also normalized by G, but G has no normal subgroups of order 8. Now, working with this $G \leq S_{24}$ as opposed to $\lambda(G) \leq \mathrm{Perm}(G)$ it is not so easy to directly apply Cor. 2.6 to get $J = Orb_P(i_G)$. However, one can show that G above (being isomorphic to S_4) contains only three subgroups of order 8, all isomorphic to D_4. If we make the identification $1 \leftrightarrow i_G$ then we can infer which is *the $J = \Psi(P)$*. To see this, one first observes that P gives rise to the following orbits

$$\{1, 2, 4, 5, 7, 8, 12, 16\}$$
$$\{3, 6, 10, 11, 14, 15, 19, 22\}$$
$$\{9, 13, 17, 18, 20, 21, 23, 24\}$$

and for the three subgroups of order 8, J_1, J_2 and J_3 we have orbits

$J_1 \rightarrow \{1, 2, 4, 5, 7, 8, 12, 16\}, \{3, 10, 11, 13, 19, 20, 21, 24\}, \{6, 9, 14, 15, 17, 18, 22, 23\}$
$J_2 \rightarrow \{1, 4, 5, 6, 12, 14, 15, 22\}, \{2, 3, 7, 8, 23, 10, 11, 16, 19\}, \{9, 13, 17, 18, 20, 21, 24\}$
$J_3 \rightarrow \{1, 4, 5, 12, 13, 20, 21, 24\}, \{2, 7, 8, 9, 16, 17, 18, 23\}, \{3, 6, 10, 11, 14, 15, 19, 22\}$

which, again identifying 1 with i_G implies that $J_1 = \Psi(P)$ since the orbit containing 1 that matches $[1, 2, 4, 5, 7, 8, 12, 16]$ is that belonging to J_1 above. What one also notices is that the other two orbits

$$\{3, 10, 11, 13, 19, 20, 21, 24\} \text{ and } \{6, 9, 14, 15, 17, 18, 22, 23\}$$

do not match

$$\{3, 6, 10, 11, 14, 15, 19, 22\} \text{ and } \{9, 13, 17, 18, 20, 21, 23, 24\}$$

above arising from P, which is, of course, due to the fact that the orbits of J (resp. P) are the right (resp. left) cosets of J in G.

The case where J is non normal in G synchronizes naturally with the initial setup of Greither-Pareigis as mentioned earlier. They start with a non-Galois extension and then look to the normal closure of

this extension in order to construct a Hopf-Galois structure if possible on the original extension. In the case where J is not normal in G, the extension F/k is not classically Galois of course, but we will show that it is Hopf-Galois, which begins by looking to its normal closure. The normal closure $\tilde{F}/k$ has as its Galois group G/I where $I = \cap_{g \in G} gJg^{-1}$, and clearly $\tilde{F} \subseteq K$ as diagrammed below.
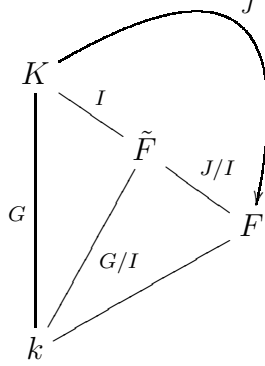
Looking back at the basic setup in [5], principally [5, Lemma 1.1 and Lemma 1.2] we have that S (the quotient of the respective Galois groups) is going to be $(G/I)/(J/I)$. This quotient of quotients looks formidable, but there is a natural identification of it with G/J where, of course, $|G/J| = |N/P| = [F : k]$. Following this development further leads to the question of finding a regular subgroup $Q \leq \mathrm{Perm}(S)$ which leads to an action making $\mathrm{Map}(S, \tilde{F})/\tilde{F}$ Hopf-Galois with respect to $\tilde{F}[Q]$. If Q is normalized by $\lambda(G)/\lambda(I)$ then $\mathrm{Map}(S, \tilde{F})^{\lambda(G)/\lambda(I)}/\tilde{F}^{G/I}$ (i.e. F/k) is Hopf-Galois with respect to $(\tilde{F}[Q])^{G/I}$. However, we can replace $\tilde{F}$ with any field which contains it, most naturally K since $Gal(K/k)$ maps onto $Gal(\tilde{F}/k)$. Indeed, if I is trivial then $\tilde{F} = K$. Therefore we look for regular $Q \leq \mathrm{Perm}(S)$ normalized by $\lambda(G)$ giving rise to $H_Q = (K[Q])^{\lambda(G)}$. We may thereby dispense with the need to worry about I at all since (as indicated earlier) S can be identified with the (set) G/J.

By Lemma 2.7 we have that N/P acts regularly, and G acts (transitively) on $S = \{g_i J\}$. The only question is whether the analog of Thm. 2.8 holds for the action of G on N/P within $\mathrm{Perm}(S)$. The answer is yes by simply setting $h_1 = i_G$ and $h_2 = i_G$ in $\lambda(\gamma h_1)$ and $\lambda(\gamma^{-1}h_2)$ in the proof. This yields the action $\lambda(\gamma)(\eta P)\lambda(\gamma)^{-1} = \lambda(\gamma)\eta\lambda(\gamma)^{-1}P$, so that, indeed, $\lambda(G)$ normalizes N/P in $\mathrm{Perm}(S)$ which yields the following variation on Thm. 2.9.

Theorem 2.10: *The extension F/k is Hopf-Galois with respect to the Hopf algebra $H_{N/P} = (K[N/P])^{\lambda(G)}$ where $\lambda(G) \leq \mathrm{Perm}(S)$.*

3. SHORT EXACT SEQUENCES

As seen above, the analysis of how to construct Hopf-Galois structures on intermediate fields is dependent on when the relevant subgroups, P and $J = \Psi(P)$ are normal or not. One basic consequence of normality at the level of groups is the existence of an exact sequence. Such an exact sequence gives rise to a sequence of group rings, which are Hopf algebras. We consider these sequences, as well as those corresponding to the fixed rings which are the Hopf-algebras which act on the different intermediate fields.

In ordinary Galois theory, if K/k is Galois with $J \triangleleft G := Gal(K/k)$ then K^J/k is Galois with group G/J. One has an exact sequence of groups

$$1 \to J \to G \to G/J \to 1$$

where, since $J \triangleleft G$, then by [2, Prop 4.14], the induced Hopf-algebra maps $k[J] \to k[G]$ (resp. $k[G] \to k[G/J]$) are normal (resp. conormal). As such,

$$k \to k[J] \to k[G] \to k[G/J] \to k$$

is a short exact sequence of k-Hopf algebras.

But in terms of the actions on the relevant (intermediate) fields, these are not exactly the Hopf algebras that act to make the given field extensions Hopf-Galois. If we look at the Hopf-Galois actions induced by the Galois groups J, G, and G/J then the Hopf algebras are group rings

$$K/K^J \text{ is acted on by } (K[\rho(J)])^{\lambda(J)} \cong K^J[J]$$
$$\text{where } \rho(J), \lambda(J) \leq \mathrm{Perm}(J)$$

$$K/k \text{ is acted on by } (K[\rho(G)])^{\lambda(G)} \cong k[G]$$

$$K^J/k \text{ is acted on by } (K^J[\rho(G/J)])^{\lambda(G/J)} \cong k[G/J]$$
$$\text{where } \lambda(G/J), \rho(G/J) \leq \mathrm{Perm}(G/J)$$

The latter two Hopf algebras are defined over k but the first is not, which is not unexpected since it is acting with respect to the ground field K^J.

Since $\rho(J)$ is normalized by $\rho(G)$ and $\lambda(G)$ then $(K[\rho(J)])^{\lambda(G)}$ is a Hopf sub-algebra of $(K[\rho(G)])^{\lambda(G)}$ by [1, Thm. 7.6], and

$$(K[\rho(J)])^{\lambda(J)} \cong K^J \otimes (K[\rho(J)])^{\lambda(G)}$$

.

Part of the simplicity of the classical case above is that the Hopf-Algebras are group rings. For K/k Hopf-Galois under the action of $H_N = (K[N])^{\lambda(G)}$, where N is a regular subgroup of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$, we would like to consider $P \triangleleft N$, also normalized by $\lambda(G)$ and the Hopf-Galois structures arising from P and N/P. Since P is normalized by N, then, as discussed earlier $H_P = (K[P])^{\lambda(G)}$ is a k-sub-Hopf algebra of $H_N = (K[N])^{\lambda(G)}$ which fixes a subfield F, and that $F \otimes H_P$ acts to make K/F Hopf-Galois, and by Thm. 2.9 F/k is Hopf-Galois with respect to $H_{N/P} = (F[N/P])^{\lambda(G)/\lambda(J)}$. As such, we have the following.

Theorem 3.1: *The following sequence of Hopf-algebras*

$$1 \to (K[P])^{\lambda(G)} \to (K[N])^{\lambda(G)} \to (F[N/P])^{\lambda(G)/\lambda(J)} \to 1$$

is exact.

Proof. The reason this is exact is that we can rewrite the last term $(F[N/P])^{\lambda(G)/\lambda(J)}$ as

$$(\underbrace{\underbrace{(K[N/P])^{\lambda(J)}}_{descend\ from\ K\ to\ F})^{\lambda(G)/\lambda(J)}}_{descend\ from\ F\ to\ k} = (K[N/P])^{\lambda(G)}$$

since $(K[N/P])^{\lambda(J)} = F[N/P]$ due to $\lambda(J)$ acting trivially on N/P as one can see from the proof of Thm. 2.8. So in the second row below

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & K[P] & \longrightarrow & K[N] & \longrightarrow & K[N/P] & \longrightarrow & 1 \\
& & \downarrow{\scriptstyle \lambda(G)} & & \downarrow{\scriptstyle \lambda(G)} & & \downarrow{\scriptstyle \lambda(G)} & & \\
1 & \longrightarrow & (K[P])^{\lambda(G)} & \longrightarrow & (K[N])^{\lambda(G)} & \longrightarrow & (K[N/P])^{\lambda(G)} & \longrightarrow & 1
\end{array}
$$

exactness is due to faithful flatness. That is, the upper row being exact implies that the lower row, consisting of the fixed rings, under the action of $\lambda(G)$, is exact. □

Note, unsurprisingly, that by Thm. 2.10 $(K[N/P])^{\lambda(G)}$ is exactly the Hopf algebra which acts on F/k when J is not normal in G. Of course, in that setting G/J does not act on F/k since each coset representative corresponds to a different conjugate field of F.

4. EXAMPLES

We conclude with a set of examples whose definition partly explains the notational choices for the sizes of the relevant groups given earlier. The condition that $P \lhd N$ is, in itself, not a rare one at all. However, the requirement that P be normalized by G as well is much more stringent.

One class of examples where this is automatic are those subgroups P which are characteristic in N. Being characteristic is a feature of certain classes of subgroups, for example centers, Frattini subgroups, commutators etc.

Another more basic condition is uniqueness based on order considerations. Specifically suppose $|G| = |N| = mp$ where p is prime, $gcd(p, m) = 1$, and the Sylow p-subgroup is unique, such as when $p > m$. In this situation the Sylow p-subgroup is characteristic, and moreover $J = \Psi(P)$ must therefore be the similarly unique Sylow p-subgroup of G as well. As such, $J \lhd G$ and therefore F/k is Galois with respect to G/J and Hopf-Galois with respect to $(F[N/P])^{\lambda(G)/\lambda(J)}$.

We include below tables for the 6 groups of order 42 mentioned above, $C_2 \times (C_7 \rtimes C_3)$, $C_3 \times D_7$, C_{42}, $(C_7 \rtimes C_3) \rtimes C_2$, $C_7 \times D_3$, and D_{21} where $p = 7$ and $m = 6$. In these tables below, we restrict to those P normal in N. We denote by $[N]$ the isomorphism class of N, and similarly $[P]$ and $[J]$, and where the first column is the number of such triples $([N], [P], [J])$ for the given G, and the last column indicates whether J was normal in G or $|I| = [K : \tilde{F}]$ if not. One point to reiterate is that for each P, the group $J = \Psi(P)$ need not be isomorphic to P.

$G \cong D_{21}$

$\#N$	$[N]$	$[P]$	$[J]$	J normal in G or not
6	$C_3 \times D_7$	C_{21}	C_{21}	$J \triangleleft G$
6	$C_3 \times D_7$	C_3	C_3	$J \triangleleft G$
6	$C_3 \times D_7$	C_7	C_7	$J \triangleleft G$
6	$C_3 \times D_7$	D_7	D_7	$|I| = 7$
21	C_{42}	C_{14}	D_7	$|I| = 7$
21	C_{42}	C_{21}	C_{21}	$J \triangleleft G$
21	C_{42}	C_2	C_2	$|I| = 1$
21	C_{42}	C_3	C_3	$J \triangleleft G$
21	C_{42}	C_6	D_3	$|I| = 3$
21	C_{42}	C_7	C_7	$J \triangleleft G$
14	$C_7 \times D_3$	C_{21}	C_{21}	$J \triangleleft G$
14	$C_7 \times D_3$	C_3	C_3	$J \triangleleft G$
14	$C_7 \times D_3$	C_7	C_7	$J \triangleleft G$
14	$C_7 \times D_3$	D_3	D_3	$|I| = 3$
4	D_{21}	C_{21}	C_{21}	$J \triangleleft G$
4	D_{21}	C_3	C_3	$J \triangleleft G$
4	D_{21}	C_7	C_7	$J \triangleleft G$

$G \cong C_2 \times (C_7 \rtimes C_3)$

$\#N$	$[N]$	$[P]$	$[J]$	J normal in G or not
16	$C_2 \times (C_7 \rtimes C_3)$	C_{14}	C_{14}	$J \triangleleft G$
16	$C_2 \times (C_7 \rtimes C_3)$	C_2	C_2	$J \triangleleft G$
16	$C_2 \times (C_7 \rtimes C_3)$	$C_7 \rtimes C_3$	$C_7 \rtimes C_3$	$J \triangleleft G$
16	$C_2 \times (C_7 \rtimes C_3)$	C_7	C_7	$J \triangleleft G$
14	$C_3 \times D_7$	C_{21}	$C_7 \rtimes C_3$	$J \triangleleft G$
14	$C_3 \times D_7$	C_3	C_3	$|I| = 1$
14	$C_3 \times D_7$	C_7	C_7	$J \triangleleft G$
14	$C_3 \times D_7$	D_7	C_{14}	$J \triangleleft G$
7	C_{42}	C_{14}	C_{14}	$J \triangleleft G$
7	C_{42}	C_{21}	$C_7 \rtimes C_3$	$J \triangleleft G$
7	C_{42}	C_2	C_2	$J \triangleleft G$
7	C_{42}	C_3	C_3	$|I| = 1$
7	C_{42}	C_6	C_6	$|I| = 2$
7	C_{42}	C_7	C_7	$J \triangleleft G$
28	$(C_7 \rtimes C_3) \rtimes C_2$	$C_7 \rtimes C_3$	$C_7 \rtimes C_3$	$J \triangleleft G$
28	$(C_7 \rtimes C_3) \rtimes C_2$	C_7	C_7	$J \triangleleft G$
28	$(C_7 \rtimes C_3) \rtimes C_2$	D_7	C_{14}	$J \triangleleft G$
14	$C_7 \times D_3$	C_{21}	$C_7 \rtimes C_3$	$J \triangleleft G$
14	$C_7 \times D_3$	C_3	C_3	$|I| = 1$
14	$C_7 \times D_3$	C_7	C_7	$J \triangleleft G$
14	$C_7 \times D_3$	D_3	C_6	$|I| = 2$
28	D_{21}	C_{21}	$C_7 \rtimes C_3$	$J \triangleleft G$
28	D_{21}	C_3	C_3	$|I| = 1$
28	D_{21}	C_7	C_7	$J \triangleleft G$

$G \cong C_3 \times D_7$

#N	$[N]$	$[P]$	$[J]$	J normal in G or not
28	$C_2 \times (C_7 \rtimes C_3)$	C_{14}	D_7	$J \vartriangleleft G$
28	$C_2 \times (C_7 \rtimes C_3)$	C_2	C_2	$|I| = 1$
28	$C_2 \times (C_7 \rtimes C_3)$	$C_7 \rtimes C_3$	C_{21}	$J \vartriangleleft G$
28	$C_2 \times (C_7 \rtimes C_3)$	C_7	C_7	$J \vartriangleleft G$
2	$C_3 \times D_7$	C_{21}	C_{21}	$J \vartriangleleft G$
2	$C_3 \times D_7$	C_3	C_3	$J \vartriangleleft G$
2	$C_3 \times D_7$	C_7	C_7	$J \vartriangleleft G$
2	$C_3 \times D_7$	D_7	D_7	$J \vartriangleleft G$
7	C_{42}	C_{14}	D_7	$J \vartriangleleft G$
7	C_{42}	C_{21}	C_{21}	$J \vartriangleleft G$
7	C_{42}	C_2	C_2	$|I| = 1$
7	C_{42}	C_3	C_3	$J \vartriangleleft G$
7	C_{42}	C_6	C_6	$|I| = 3$
7	C_{42}	C_7	C_7	$J \vartriangleleft G$
28	$(C_7 \rtimes C_3) \rtimes C_2$	$C_7 \rtimes C_3$	C_{21}	$J \vartriangleleft G$
28	$(C_7 \rtimes C_3) \rtimes C_2$	C_7	C_7	$J \vartriangleleft G$
28	$(C_7 \rtimes C_3) \rtimes C_2$	D_7	D_7	$J \vartriangleleft G$
14	$C_7 \times D_3$	C_{21}	C_{21}	$J \vartriangleleft G$
14	$C_7 \times D_3$	C_3	C_3	$J \vartriangleleft G$
14	$C_7 \times D_3$	C_7	C_7	$J \vartriangleleft G$
14	$C_7 \times D_3$	D_3	C_6	$|I| = 3$
4	D_{21}	C_{21}	C_{21}	$J \vartriangleleft G$
4	D_{21}	C_3	C_3	$J \vartriangleleft G$
4	D_{21}	C_7	C_7	$J \vartriangleleft G$

$G \cong C_{42}$

$\#N$	$[N]$	$[P]$	$[J]$	J normal in G or not
4	$C_2 \times (C_7 \rtimes C_3)$	C_{14}	C_{14}	$J \triangleleft G$
4	$C_2 \times (C_7 \rtimes C_3)$	C_2	C_2	$J \triangleleft G$
4	$C_2 \times (C_7 \rtimes C_3)$	$C_7 \rtimes C_3$	C_{21}	$J \triangleleft G$
4	$C_2 \times (C_7 \rtimes C_3)$	C_7	C_7	$J \triangleleft G$
2	$C_3 \times D_7$	C_{21}	C_{21}	$J \triangleleft G$
2	$C_3 \times D_7$	C_3	C_3	$J \triangleleft G$
2	$C_3 \times D_7$	C_7	C_7	$J \triangleleft G$
2	$C_3 \times D_7$	D_7	C_{14}	$J \triangleleft G$
1	C_{42}	C_{14}	C_{14}	$J \triangleleft G$
1	C_{42}	C_{21}	C_{21}	$J \triangleleft G$
1	C_{42}	C_2	C_2	$J \triangleleft G$
1	C_{42}	C_3	C_3	$J \triangleleft G$
1	C_{42}	C_6	C_6	$J \triangleleft G$
1	C_{42}	C_7	C_7	$J \triangleleft G$
4	$(C_7 \rtimes C_3) \rtimes C_2$	$C_7 \rtimes C_3$	C_{21}	$J \triangleleft G$
4	$(C_7 \rtimes C_3) \rtimes C_2$	C_7	C_7	$J \triangleleft G$
4	$(C_7 \rtimes C_3) \rtimes C_2$	D_7	C_{14}	$J \triangleleft G$
2	$C_7 \times D_3$	C_{21}	C_{21}	$J \triangleleft G$
2	$C_7 \times D_3$	C_3	C_3	$J \triangleleft G$
2	$C_7 \times D_3$	C_7	C_7	$J \triangleleft G$
2	$C_7 \times D_3$	D_3	C_6	$J \triangleleft G$
4	D_{21}	C_{21}	C_{21}	$J \triangleleft G$
4	D_{21}	C_3	C_3	$J \triangleleft G$
4	D_{21}	C_7	C_7	$J \triangleleft G$

$G \cong (C_7 \rtimes C_3) \rtimes C_2$

$\#N$	$[N]$	$[P]$	$[J]$	J normal in G or not
28	$C_2 \times (C_7 \rtimes C_3)$	C_{14}	D_7	$J \lhd G$
28	$C_2 \times (C_7 \rtimes C_3)$	C_2	C_2	$|I| = 1$
28	$C_2 \times (C_7 \rtimes C_3)$	$C_7 \rtimes C_3$	$C_7 \rtimes C_3$	$J \lhd G$
28	$C_2 \times (C_7 \rtimes C_3)$	C_7	C_7	$J \lhd G$
14	$C_3 \times D_7$	C_{21}	$C_7 \rtimes C_3$	$J \lhd G$
14	$C_3 \times D_7$	C_3	C_3	$|I| = 1$
14	$C_3 \times D_7$	C_7	C_7	$J \lhd G$
14	$C_3 \times D_7$	D_7	D_7	$J \lhd G$
7	C_{42}	C_{14}	D_7	$J \lhd G$
7	C_{42}	C_{21}	$C_7 \rtimes C_3$	$J \lhd G$
7	C_{42}	C_2	C_2	$|I| = 1$
7	C_{42}	C_3	C_3	$|I| = 1$
7	C_{42}	C_6	C_6	$|I| = 1$
7	C_{42}	C_7	C_7	$J \lhd G$
16	$(C_7 \rtimes C_3) \rtimes C_2$	$C_7 \rtimes C_3$	$C_7 \rtimes C_3$	$J \lhd G$
16	$(C_7 \rtimes C_3) \rtimes C_2$	C_7	C_7	$J \lhd G$
16	$(C_7 \rtimes C_3) \rtimes C_2$	D_7	D_7	$J \lhd G$
14	$C_7 \times D_3$	C_{21}	$C_7 \rtimes C_3$	$J \lhd G$
14	$C_7 \times D_3$	C_3	C_3	$|I| = 1$
14	$C_7 \times D_3$	C_7	C_7	$J \lhd G$
14	$C_7 \times D_3$	D_3	C_6	$|I| = 1$
28	D_{21}	C_{21}	$C_7 \rtimes C_3$	$J \lhd G$
28	D_{21}	C_3	C_3	$|I| = 1$
28	D_{21}	C_7	C_7	$J \lhd G$

$G \cong C_7 \times D_3$

#N	[N]	[P]	[J]	J normal in G or not
6	$C_3 \times D_7$	C_{21}	C_{21}	$J \triangleleft G$
6	$C_3 \times D_7$	C_3	C_3	$J \triangleleft G$
6	$C_3 \times D_7$	C_7	C_7	$J \triangleleft G$
6	$C_3 \times D_7$	D_7	C_{14}	$|I| = 7$
3	C_{42}	C_{14}	C_{14}	$|I| = 7$
3	C_{42}	C_{21}	C_{21}	$J \triangleleft G$
3	C_{42}	C_2	C_2	$|I| = 1$
3	C_{42}	C_3	C_3	$J \triangleleft G$
3	C_{42}	C_6	D_3	$J \triangleleft G$
3	C_{42}	C_7	C_7	$J \triangleleft G$
2	$C_7 \times D_3$	C_{21}	C_{21}	$J \triangleleft G$
2	$C_7 \times D_3$	C_3	C_3	$J \triangleleft G$
2	$C_7 \times D_3$	C_7	C_7	$J \triangleleft G$
2	$C_7 \times D_3$	D_3	D_3	$J \triangleleft G$
4	D_{21}	C_{21}	C_{21}	$J \triangleleft G$
4	D_{21}	C_3	C_3	$J \triangleleft G$
4	D_{21}	C_7	C_7	$J \triangleleft G$

REFERENCES

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

[2] L. N. Childs. *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, volume 80. American Mathematical Society, Mathematical Surveys and Monographs, 2000.

[3] D. O'Shea D. Cox, J. Little. *Ideals, Varieties, and Algorithms*. Springer, 2015.

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

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

[6] T. Kohl. Regular permutation groups of order mp and Hopf-Galois structures. *Algebra and Number Theory*, 7(9):2203–2240, 2013.

[7] D. Radford. *Hopf Algebras*. World Scientific, 2011.

[8] M. Vela T. Crespo, A. Rio. Induced hopf galois structures. *J. Algebra*, 457:312–322, 2016.

[9] M. Vela T. Crespo, A. Rio. On the galois correspondence theorem in separable hopf galois theory. *Publicacions Matem'tiques*, 60(1):221–234, 2016.

26   ALAN KOCH, TIMOTHY KOHL, PAUL J. TRUMAN, AND ROBERT UNDERWOOD

DEPARTMENT OF MATHEMATICS, AGNES SCOTT COLLEGE, 141 E. COLLEGE AVE., DECATUR, GA 30030 USA

E-mail address: akoch@agnesscott.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, BOSTON UNIVERSITY, 111 CUMMINGTON MALL, BOSTON, MA 02215 USA

E-mail address: tkohl@math.bu.edu

SCHOOL OF COMPUTING AND MATHEMATICS, KEELE UNIVERSITY, STAFFORDSHIRE, ST5 5BG, UK

E-mail address: P.J.Truman@Keele.ac.uk

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, AUBURN UNIVERSITY AT MONTGOMERY, MONTGOMERY, AL 36124 USA

E-mail address: runderwo@aum.edu