Algebra & Number Theory

Volume 10

2016

No. 1

Hopf–Galois structures arising from groups with unique subgroup of order p

Timothy Kohl

msp

ALGEBRA AND NUMBER THEORY 10:1 (2016)
dx.doi.org/10.2140/ant.2016.10.37

Hopf–Galois structures arising from groups with unique subgroup of order p

Timothy Kohl

For Γ a group of order mp, where p is a prime with $\gcd(p, m) = 1$, we consider the regular subgroups $N \leq \mathrm{Perm}(\Gamma)$ that are normalized by $\lambda(\Gamma)$, the left regular representation of Γ. These subgroups are in one-to-one correspondence with the Hopf–Galois structures on separable field extensions L/K with $\Gamma = \mathrm{Gal}(L/K)$. Elsewhere we showed that if $p > m$ then all such N lie within the normalizer of the Sylow p-subgroup of $\lambda(\Gamma)$. Here we show that one only need assume that all groups of a given order mp have a unique Sylow p-subgroup, and that p not be a divisor of the order of the automorphism groups of any group of order m. We thus extend the applicability of the program for computing these regular subgroups N and concordantly the corresponding Hopf–Galois structures on separable extensions of degree mp.

Introduction

The motivation and antecedents for this work lie in the subject of Hopf–Galois theory for separable field extensions. Specifically, we extend the results of [Kohl 2013] on Hopf–Galois structures on Galois extensions of degree mp for p a prime where $p > m$. We will not delve into all the particulars of Hopf–Galois theory, since this discussion focuses on the group-theoretic underpinnings of this class of examples. For the general theory, one may consult [Chase and Sweedler 1969] for basic definitions and initial examples and [Greither and Pareigis 1987] for the theory as applied to separable extensions, which is the category in which our earlier paper and others fall. In brief, let L/K be a finite Galois extension with $\Gamma = \mathrm{Gal}(L/K)$. Such an extension is canonically Hopf–Galois for the K-Hopf algebra $H = K[\Gamma]$, but also for potentially many other K-Hopf algebras. Their enumeration is determined by the following paraphrased variant of the main theorem in [Greither and Pareigis 1987]. (Recall that a *regular* subgroup of the group of permutations of a set is one whose action on the set is transitive and free.)

MSC2010: primary 20B35; secondary 20D20, 20D45, 16T05.
Keywords: Hopf–Galois extension, regular subgroup.

Theorem [Greither and Pareigis 1987]. *If L/K is a finite Galois extension with $\Gamma = \mathrm{Gal}(L/K)$ then the Hopf algebras which act to make the extension Hopf–Galois correspond in a one-to-one fashion with regular subgroups $N \leq B = \mathrm{Perm}(\Gamma)$ such that $\lambda(\Gamma) \leq \mathrm{Norm}_B(N)$, where $\lambda(\Gamma)$ is the image of the left regular representation of Γ in B.*

Each such N gives rise to the Hopf algebra $H = L[N]^\Gamma$, the fixed ring of the group ring $L[N]$ under the action of Γ simultaneously on the coefficients, by virtue of $\Gamma = \mathrm{Gal}(L/K)$, and the group elements by virtue of $\lambda(\Gamma)$ normalizing N. The problem of enumerating such N for different classes of extensions has been the subject of much recent work by Byott (e.g., [2004]), Childs (e.g., [2003]), the author, and others. This discussion will be strictly focused on the enumeration of these groups, for a particular set of cases, keyed to the order of Γ and consequently of any such regular subgroup N which satisfies the conditions of the above theorem. Again, no discussion of Hopf–Galois structures is required from here on since we are looking at the purely group-theoretic translation arising from the above theorem.

1. Preliminaries

As it is so essential, let's briefly review regularity in the context of finite groups.

Definition 1.1. Let X be a finite set and let $N \leq \mathrm{Perm}(X)$ be a group of permutations of X. We say that N is *semiregular* if it acts freely, that is, if each element of N apart from the identity acts without fixed points. If N acts transitively on X and $|N| = |X|$ then N is semiregular; and if N is semiregular its action is transitive if and only if $|N| = |X|$. Thus any two of these conditions imply the third. A group satisfying these conditions is called *regular*.

In view of the cardinality condition, in order to organize the enumeration of the regular $N \leq \mathrm{Perm}(\Gamma)$ that may arise for a given Galois group Γ, we consider, for $[M]$ the isomorphism class of a given group of the same order as Γ, the set

$$R(\Gamma, [M]) = \{N \leq B \mid N \text{ regular},\ N \cong M,\ \lambda(\Gamma) \leq \mathrm{Norm}_B(N)\}$$

and let $R(\Gamma)$ be the union of the $R(\Gamma, [M])$ over *all* isomorphism classes of groups of the same order as Γ.

Since they are important in the enumeration of $R(\Gamma, [M])$, we recall some facts from [Kohl 2013], henceforth referred to as [K].

Lemma 1.2 [K, Corollary 3.3 and Proposition 3.4]. *Let N be a regular subgroup of B and define the* ***opposite of*** *N as $N^{\mathrm{opp}} = \mathrm{Cent}_B(N)$. Then:*

- *N^{opp} is also a regular subgroup of B.*
- *$N \cap N^{\mathrm{opp}} = Z(N)$ (so $N = N^{\mathrm{opp}}$ if and only if N is abelian).*

- $(N^{\mathrm{opp}})^{\mathrm{opp}} = N$.
- $N \in R(\Gamma, [M])$ *if and only if* $N^{\mathrm{opp}} \in R(\Gamma, [M])$.

Again, in the cases considered in [K] it was assumed that $|\Gamma| = mp$ for p prime and $p > m$. Our goal is to extend those results to groups of order mp where $\gcd(p, m) = 1$, but where one need not assume that $p > m$.

We begin by briefly reviewing the setup in [K], where we considered groups Γ of order mp with a unique and therefore characteristic Sylow p-subgroup due to the assumption that $p > m$. Since $p > m$ obviously implies $\gcd(p, m) = 1$, by the Schur–Zassenhaus lemma Γ may be written as PQ for P and Q subgroups of Γ where $|P| = p$ and $|Q| = m$. More specifically, there is a split exact sequence $P \to \Gamma \to Q$ whereby $\Gamma = P \rtimes_\tau Q$, with $\tau : Q \to \mathrm{Aut}(P)$ induced by conjugation within Γ by the complementary subgroup Q. Using Q for the quotient of Γ by P and the image of the section in Γ is admittedly a slight abuse of notation. The condition $p > m$ is sufficient, of course, to make the Sylow p-subgroup unique and have order p.

Going forward, we wish to drop the assumption that $p > m$ and consider groups of order mp for p prime, with $\gcd(p, m) = 1$ and where congruence conditions force *any* group of order mp, including Γ and *any* $N \in R(\Gamma)$, to have a unique Sylow p-subgroup.

With Γ as above, if $\lambda : \Gamma \to \mathrm{Perm}(\Gamma) = B$ is the left regular representation then we define $\mathcal{P} = P(\lambda(\Gamma))$ to be the Sylow p-subgroup of $\lambda(\Gamma)$ and $\mathcal{Q}$ to be the complementary subgroup to $\mathcal{P}$ in $\lambda(\Gamma)$. We wish to prove the following strengthening of [K, Theorem 3.5] which will allow us to apply the program developed in Sections 1–3 of [K] (and applied in subsequent sections therein) to a much larger class of groups.

Theorem 1.3. *Let Γ have order mp where $\gcd(p, m) = 1$ and $p \nmid |\mathrm{Aut}(Q)|$ for any group Q of order m, and assume any group of order mp has a unique Sylow p-subgroup. If $N \in R(\Gamma)$ then N is a subgroup of $\mathrm{Norm}_B(\mathcal{P})$.*

To prove this, we need to modify certain key results from [K], starting with Lemma 1.1 regarding the p-torsion of $\mathrm{Aut}(\Gamma)$.

Lemma 1.4. *Let Γ have order mp, where $\gcd(p, m) = 1$, and assume Γ has a unique Sylow p-subgroup, so that $\Gamma \cong P \rtimes_\tau Q$ as above. Assume also that p does not divide $|\mathrm{Aut}(Q)|$.*

(a) *If τ is trivial (whence $\Gamma \cong P \times Q$) then p does not divide $|\mathrm{Aut}(\Gamma)|$.*

(b) *If τ is nontrivial then $\mathrm{Aut}(\Gamma)$ has a unique Sylow p-subgroup, consisting of the inner automorphisms induced by conjugation by elements of P.*

Proof. In (a), if Γ is such a direct product then $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(P) \times \mathrm{Aut}(Q)$ and so if $p \nmid |\mathrm{Aut}(Q)|$ then $p \nmid |\mathrm{Aut}(\Gamma)|$. The proof is basically the same as in [K]. For (b), since $\Gamma/P \cong Q$, any $\psi \in \mathrm{Aut}(\Gamma)$ induces $\bar{\psi} \in \mathrm{Aut}(\Gamma/P) \cong \mathrm{Aut}(Q)$ and if ψ has p-power order then $\bar{\psi}$ is trivial since p does not divide $|\mathrm{Aut}(Q)|$. And, as also observed in [K], when Γ is not a direct product, $|P \cap Z(\Gamma)| = 1$ and conjugation in Γ by elements of P yields the order-p subgroup of $\mathrm{Aut}(\Gamma)$. □

The condition that $p \nmid |\mathrm{Aut}(Q)|$ was automatic when $p > m$, but it often holds true even when $p < m$. For example, if $p = 5$ and $m = 8$ then Sylow theory easily shows that any group of order 40 will have a unique Sylow p-subgroup. One could also consider the groups of order eight — C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_4 and Q_2 — whose automorphism groups have orders 4, 8, 168, 8, 24, respectively, *none* of which is divisible by 5.

The cycle structure of a regular permutation group's elements is greatly circumscribed by the condition that all nontrivial elements of the group act freely. Any such element, because it and all its nontrivial powers lack fixed points, must be a product of cycles of the same length, and the sum of the lengths must equal $|X|$. For example, if $X = \{1, 2, 3, 4, 5, 6\}$ then $(1, 2)(3, 4)(5, 6)$ and $(1, 2, 3)(4, 5, 6)$ satisfy this property. In contrast, $\mu = (1, 2, 3, 4)(5, 6)$ cannot belong to a regular subgroup of $\mathrm{Perm}(X)$ even though it does not have fixed points, because $\mu^2 = (1, 3)(2, 4)$ does.

Since $\mathcal{P}$ is a nontrivial subgroup of the canonically regular permutation group $\lambda(\Gamma)$, we must have

$$\mathcal{P} = \langle \pi \rangle = \langle \pi_1 \pi_2 \cdots \pi_m \rangle,$$

where the π_i are disjoint p-cycles. In a similar fashion, if N is any regular subgroup of B then its Sylow p-subgroup $P(N)$ is also cyclic of order p and therefore of the form

$$P(N) = \langle \theta \rangle = \langle \theta_1 \theta_2 \cdots \theta_m \rangle,$$

where the θ_i are also disjoint p-cycles. For $N \in R(\Gamma)$ we are looking at those regular N which are normalized by $\lambda(\Gamma)$. Now, $P(N)$ is characteristic in N, so $\lambda(\Gamma)$ normalizing N implies that $\lambda(\Gamma)$ (and therefore $\mathcal{P}$) normalizes $P(N)$. In [K] the assumption $p > m$ was used to show that $\mathcal{P}$ and $P(N)$ must, in fact, centralize each other. In particular Proposition 1.2 there showed that if $p > m$ then (after renumbering the θ_i if necessary) one has $\theta_i = \pi_i^{a_i}$ for $a_i \in \mathbb{F}_p^\times$. The reason for this was that for $p > m$ the group S_m contains no elements of order p, and so θ is a product of the same π_i that comprise the generator of $\mathcal{P}$.

As it turns out, this is *not* automatically true if we just assume that $\gcd(p, m) = 1$. For example, if $p = 5$ and $m = 8$ then in S_{40} let

$$\pi_i = (1 + (i-1)5,\ 2 + (i-1)5,\ 3 + (i-1)5,\ 4 + (i-1)5,\ 5 + (i-1)5)$$

for $i = 1, \ldots, 8$ and let $\theta_j = (j,\ j+5,\ j+10,\ j+15,\ j+20)$ for $j = 1, \ldots, 5$ and $\theta_6 = \pi_6$, $\theta_7 = \pi_7$, $\theta_8 = \pi_8$. One may verify that $\pi = \pi_1 \cdots \pi_8$ is centralized by $\theta = \theta_1 \cdots \theta_8$ but θ_j, for $j = 1, \ldots, 5$, is not a power of any π_i.

This example shows that the $P(N) \leq N$ being normalized, and thus centralized, by $\mathcal{P}$ is insufficient to guarantee that $P(N) \leq \langle \pi_1, \pi_2, \ldots, \pi_m \rangle$. This does not nullify the possibility of the program in [K] being generalized. This example merely shows that $\mathrm{Cent}_B(\mathcal{P})$ contains many semiregular subgroups of order p that are not subgroups of $\langle \pi_1, \pi_2, \ldots, \pi_m \rangle$. However, it turns out that for those N normalized by $\lambda(\Gamma)$, since $P(N)$ is characteristic in N and therefore normalized by $\lambda(\Gamma)$, the possible $P(N)$ that can arise are still contained in $\langle \pi_1, \pi_2, \ldots, \pi_m \rangle$. To arrive at this conclusion, we need to recall some facts about the structure of $\mathrm{Norm}_B(\mathcal{P})$ and $\mathrm{Cent}_B(\mathcal{P})$.

With $\mathcal{P} = \langle \pi \rangle = \langle \pi_1 \cdots \pi_m \rangle$, where the π_i are disjoint p-cycles, we can define $\mathcal{V} = \langle \pi_1, \pi_2, \ldots, \pi_m \rangle$, the elementary abelian subgroup of B generated by the π_i. Also, we can choose $\gamma_i \in \Gamma$ for $i = 1, \ldots, m$ such that $\pi_i = (\gamma_i, \pi(\gamma_i), \ldots, \pi^{p-1}(\gamma_i))$ and if we let Π_i be the support of π_i, then the Π_i are, of course, disjoint and their union is Γ as a set. Define $\mathcal{S} \leq B$ to be those permutations $\bar{\alpha}$ such that for each $i \in \{1, \ldots, m\}$ there exists a single $j \in \{1, \ldots, m\}$ satisfying $\bar{\alpha}(\pi^t(\gamma_i)) = \pi^t(\gamma_j)$ for each $t \in \mathbb{Z}_p$. Equivalently, $\bar{\alpha}$ operates on the *blocks* Π_i as follows:

$$\bar{\alpha}(\{\gamma_i, \pi(\gamma_i), \ldots, \pi^{p-1}(\gamma_i)\}) = \{\gamma_j, \pi(\gamma_j), \ldots, \pi^{p-1}(\gamma_j)\}.$$

It is clear that $\mathcal{S}$ is isomorphic to S_m viewed as $\mathrm{Perm}(\{\Pi_1, \ldots, \Pi_m\})$, where $\bar{\alpha} \in \mathcal{S}$ corresponds to a permutation $\alpha \in S_m$ which permutes the m blocks Π_i amongst each other. In a similar fashion, we may define another subgroup $\mathcal{U} \leq B$ keyed to π and the π_i. For a cyclic group $C = \langle x \rangle$ of order p, the automorphisms are given by $x \mapsto x^c$ for $c \in U_p = \mathbb{F}_p^\times = \langle u \rangle$. Within B, therefore, since $\mathcal{P}$ is cyclic of order p, there exists a product $u_1 \cdots u_m$ of m disjoint $(p-1)$-cycles with the property that $u_i \pi_i u_i^{-1} = \pi_i^u$, and $u_i \pi_j u_i^{-1} = \pi_j$ for $j \neq i$. (Note that the support of each u_i is $\Pi_i - \{\text{one point}\}$.) Therefore, $(u_1 \cdots u_m)\pi(u_1 \cdots u_m)^{-1} = \pi^u$ and we define $\mathcal{U} = \langle u_1 \cdots u_m \rangle$. With these three subgroups of B so defined, we can easily describe $\mathrm{Cent}_B(\mathcal{P})$ and $\mathrm{Norm}_B(\mathcal{P})$ as in [K] by

$$\mathrm{Cent}_B(\mathcal{P}) = \mathcal{V}\mathcal{S} \cong C_p \wr S_m \cong C_p^m \rtimes S_m,$$
$$\mathrm{Norm}_B(\mathcal{P}) = \mathcal{V}\mathcal{U}\mathcal{S} \cong C_p^m \rtimes (\mathrm{Aut}(C_p) \times S_m),$$

where C_p denotes the cyclic group of order p and S_m is the m-th symmetric group.

The semidirect product formulation is useful and may be closely connected to the intrinsic (as a subgroup of B) description. We may view $\mathcal{V} = \langle \pi_1, \ldots, \pi_m \rangle$ naturally as C_p^m but also, more fruitfully, as $\mathbb{F}_p^m$, the dimension-m vector space over $\mathbb{F}_p$, so that we may equate $\pi_1^{a_1} \cdots \pi_m^{a_m}$ with $[a_1, \ldots, a_m]$, a vector in $\mathbb{F}_p^m$. As the group $\mathcal{S}$ permutes the π_i amongst themselves, we may identify it with permutations $\alpha \in S_m$ acting by coordinate shifts on the vectors $\hat{a} = [a_1, \ldots, a_m]$ and where $u \in U_p$ acts by scalar multiplication. Thus we may represent a typical element of $\mathrm{Norm}_B(\mathcal{P})$ by a triple $(\hat{a}, u^r, \alpha)$, with $\hat{a} \in \mathbb{F}_p^m$, $u \in U_p$ and $\alpha \in S_m$, where (as permutations)

$(\hat{a}, u^r, \alpha)(\pi_i^k(\gamma_i)) = \pi_{\alpha(i)}^{ku^r+a_{\alpha(i)}}(\gamma_{\alpha(i)})$ and where the multiplication (and resulting conjugation operations) are defined by

$$(\hat{a}, u^r, \alpha)(\hat{b}, u^s, \beta) = (\hat{a} + u^r\alpha(\hat{b}), u^{r+s}, \alpha\beta), \tag{1}$$

$$(\hat{b}, u^s, \beta)(\hat{a}, u^r, \alpha)(\hat{b}, u^s, \beta)^{-1} = (\hat{b} + u^s\beta(\hat{a}) - u^r(\beta\alpha\beta^{-1})(\hat{b}), u^r, \beta\alpha\beta^{-1}), \tag{2}$$

$$(\hat{a}, u^r, \alpha)^n = \Big(\sum_{t=0}^{n-1} u^{rt}\alpha^t(\hat{a}), u^{rn}, \alpha^n\Big). \tag{3}$$

In this setting the elements of $\mathcal{V}$ correspond to tuples of the form $(\hat{v}, 1, I)$, where I is the identity of S_m; in particular $\pi = \pi_1\pi_2\cdots\pi_m = ([1, 1, \dots, 1], 1, I)$. The elements of $\mathrm{Cent}_B(\mathcal{P})$ correspond to those tuples where $r = 0$ (i.e., the middle coordinate is 1), which leads us back to the discussion of $P(N)$ for N a regular subgroup of B normalized by $\lambda(\Gamma)$. In this situation we have $P(N) = \langle\theta\rangle$, where $\theta = (\hat{a}, 1, \alpha)$ has order p and no fixed points. If $P(N) \not\leq \mathcal{V}$ then $\alpha \neq I$, implying (since $\alpha \in S_m$ with m coprime to p) that α has fixed points in $\{1, \dots, m\}$. If $\alpha(i) = i$ then

$$\theta(\pi_i^k(\gamma_i)) = \pi_{\alpha(i)}^{k+a_{\alpha(i)}}(\gamma_{\alpha(i)}) = \pi_i^{k+a_i}(\gamma_i),$$

which means that $a_i \neq 0$ and more importantly that θ restricted to Π_i equals $\pi_i^{a_i}$. And for those j *not* fixed by α, the restriction of θ to Π_j is not a power of π_j. That is, $\theta = \theta_1\theta_2\cdots\theta_m$, where $\theta_i = \pi_i^{a_i}$ for at least one i, and $\theta_j \notin \mathcal{V}$ for at least one j. The example given above for S_{40} is an instance of this; in particular, the fixed-point-free element of order 5 is $([1,1,1,1,1,1,1,1], 1, (1,2,3,4,5))$, which is in $\mathrm{Cent}_{S_{40}}(\langle\pi_1\pi_2\cdots\pi_8\rangle)$.

The above example motivates the following.

Definition 1.5. For $\theta \in B$ and π_i as above, we say π_i divides θ (denoted $\pi_i \mid \theta$) if the cycle structure of θ contains some nontrivial power of π_i. Similarly we write $\pi_i \nmid \theta$ if no power of π_i is a factor in the cycle structure of θ.

Observe that $\pi_i \mid \theta$ if and only if $\pi_i \mid \theta^e$ for all $e \in U_p$.

The requirement that N be normalized by $\lambda(\Gamma)$, together with the fact that $P(N)$ is characteristic, means that $P(N)$ is normalized by $\lambda(\Gamma)$. The upshot of this is the following recapitulation of [K, Proposition 1.2], which (together with Lemma 1.4) will allow us to deduce our main result, namely that $N \in R(\Gamma)$ implies $N \leq \mathrm{Norm}_B(\mathcal{P})$ under weaker hypotheses:

p and m are coprime, p does not divide $|\mathrm{Aut}(Q)|$ for any group Q of order m, and any group of order mp has a unique Sylow p-subgroup. (4)

This is the core result, since it guarantees that $P(N) \leq \mathcal{V} \leq \mathrm{Norm}_B(\mathcal{P})$ for all $N \in R(\Gamma)$.

Theorem 1.6. *If N is a regular subgroup of B normalized by $\lambda(\Gamma)$ and $P(N)$ is its Sylow p-subgroup, then $P(N)$ is a semiregular subgroup of $\mathcal{V} = \langle \pi_1, \pi_2, \dots, \pi_m \rangle$. That is, $P(N) = \langle \pi_1^{a_1} \cdots \pi_m^{a_m} \rangle$, where $a_i \in U_p = \mathbb{F}_p^\times$ for $i = 1, \dots, m$.*

Proof. If $P(N) = \langle \theta \rangle$ is not a subgroup of $\mathcal{V}$ then, as shown above, $\theta = \theta_1\theta_2 \cdots \theta_m$, where $\pi_i \mid \theta$ for some i and $\pi_j \nmid \theta$ for some $j \neq i$. In [K, Proposition 3.8] it is shown that if $(\hat{b}, u^s, \beta) \in \mathrm{Norm}_B(\mathcal{P})$ has order coprime to p then the permutation coordinate β acts without fixed points. It is important to note that the proof of this is not dependent on whether $p < m$ or $p > m$. Applying this to $\lambda(\Gamma)$, which normalizes $\mathcal{P} = \langle \pi_1 \cdots \pi_m \rangle$, has no fixed points, and contains elements $(\hat{b}, u^s, \beta)$ of order coprime to p, we conclude that $\beta \in S_m$ is fixed-point-free. In fact, if $\mathcal{Q}$ is the complementary subgroup of $\mathcal{P}$ in $\lambda(\Gamma)$ and if t maps $(\hat{b}, u^s, \beta)$ to β then $t(\mathcal{Q})$ must be a regular subgroup of S_m. The reason is that the elements of $\mathcal{Q}$ have order relatively prime to p, so $t(\mathcal{Q})$ is a semiregular subgroup of S_m; but if $|t(\mathcal{Q})| < m$ there would exist $(\hat{a}, u^r, \alpha)$ and $(\hat{a}', u^{r'}, \alpha)$ in $\mathcal{Q}$, which would imply that $(\hat{a}' - u^{r'-r}\hat{a}, u^{r'-r}, I) \in \mathcal{Q}$, which, again by [K, Proposition 3.8], must have order divisible by p. But since this element is in $\mathcal{Q}$ it must be the identity, whence $r = r'$ and so $\hat{a} = \hat{a}'$. This means that $t(\mathcal{Q})$ is regular; by transitivity we pick an element $g = (\hat{b}, u^s, \beta)$ in $\mathcal{Q}$ with $\beta(i) = j$, and then $g([1, 1, \dots, 1], 1, I)g^{-1} = (u^s\beta([1, 1, \dots, 1]), 1, I) = (u^s[1, 1, \dots, 1], 1, I)$, where, in particular,

$$g\pi_1\pi_2 \cdots \pi_m g^{-1} = \pi_{\beta(1)}^{u^s}\pi_{\beta(2)}^{u^s} \cdots \pi_{\beta(m)}^{u^s}.$$

And since $g(\theta_1\theta_2 \cdots \theta_m)g^{-1} = (g\theta_1 g^{-1})(g\theta_2 g^{-1}) \cdots (g\theta_m g^{-1})$, we have $g\theta_i g^{-1} = g\pi_i^{a_i} g^{-1} = \pi_{\beta(i)}^{u^s a_i} = \pi_j^{u^s a_i}$; therefore $\pi_j \mid g\theta g^{-1}$. The problem now is that $g\theta g^{-1} = \theta^e$ for some $e \in U_p$ implies that $\pi_j \mid \theta$, contrary to the assumption that $\pi_j \nmid \theta$. We conclude that any such θ must, in fact, be a fixed-point-free subgroup of $\mathcal{V}$ and therefore of the form asserted in the statement of the theorem. □

With this in place, we can review the remaining foundational elements in [K], which, without serious modifications, imply, under the weaker hypotheses (4), that $N \leq \mathrm{Norm}_B(\mathcal{P})$ for all $N \in R(\Gamma)$. We do this also in order to provide some applications for classes of groups where these weaker hypotheses hold.

We have just shown that $N \in R(\Gamma)$ implies $P(N) \leq \mathrm{Norm}_B(\mathcal{P})$ and that $P(N) = \langle \pi_1^{a_1} \cdots \pi_m^{a_m} \rangle$. Define $Q(N)$ to be the complementary subgroup to $P(N)$ inside N. Then, since $Q(N)$ normalizes $P(N)$, we have $q\pi_i^{a_i}q^{-1} = \pi_j^{b_j}$ for $q \in Q(N)$, where the mapping of $i \mapsto j = q(i)$ for $i, j \in \{1, \dots, m\}$ makes $Q(N)$ (abstractly) a regular subgroup of S_m. Let $\mathcal{Q} = Q(\lambda(\Gamma))$ be the complementary subgroup to $\mathcal{P}$ inside $\lambda(\Gamma)$. If $N \in R(\Gamma)$, then the elements of $\lambda(\Gamma)$ that act nontrivially on $P(N)$ are those in $\mathcal{Q}$. If we define $\hat{v}_i = [0, \dots, 1, \dots, 0] = \pi_i$ then we have the following result (whose proof does not require that $p < m$) about the possibilities for $P(N)$ for any $N \in R(\Gamma)$.

Theorem 1.7 [K, Theorem 2.1]. *Any semiregular subgroup of $\mathcal{V}$ of order p that is normalized by $\mathcal{Q}$ is generated by*

$$\hat{p}_\chi = \sum_{\gamma \in \mathcal{Q}} \chi(\gamma)\hat{v}_{\gamma(1)},$$

where $\chi : \mathcal{Q} \to U_p = \mathbb{F}_p^*$ is a linear character of $\mathcal{Q}$.

This theorem allows one to compute "potential" $P(N)$, one for each such linear character. For example, $\mathcal{P}$ is generated by $[1, 1, \ldots, 1] = \hat{p}_\iota$ where $\iota : \mathcal{Q} \to \mathbb{F}_p^*$ is the trivial character. All of these order-p elements have the form $(\hat{p}_\chi, 1, I)$ in the semidirect product formulation of $\mathrm{Norm}_B(\mathcal{P})$. The remaining component is to show that not only does $N \in R(\Gamma)$ imply $P(N) \leq \mathrm{Norm}_B(\mathcal{P})$ but also that N itself is contained in $\mathrm{Norm}_B(\mathcal{P})$. The assumption $p > m$ in [K] was not actually used in the proof of this main result, but rather in the following lemma:

Lemma 1.8 [K, Lemma 2.2]. *Let χ_1, χ_2 be distinct linear characters of $\mathcal{Q}$ in $\mathbb{F}_p^*$. Then $\langle \hat{p}_{\chi_1}, \hat{p}_{\chi_2} \rangle$ cannot contain $\hat{p}_\iota$.*

A careful reading of the proof of this in [K] shows it is not necessary to assume that $p > m$, but merely $\gcd(p, m) = 1$. With this completed, Theorem 1.3, saying that $N \in R(\Gamma)$ implies $N \leq \mathrm{Norm}_B(\mathcal{P})$, follows in the exact same fashion as in [K], since the proof does not hinge on the relationship between p and m beyond the fact that they are relatively prime. It *does* require that p not divide the order of $\mathrm{Aut}(Q)$, as in Lemma 1.4. This assumption on $|\mathrm{Aut}(Q)|$ is needed to control the size and structure of the Sylow p-subgroup of $\mathrm{Norm}_B(N)$. Specifically, it is either cyclic of order p if $P(N)$ is central in N, or elementary abelian of order p^2 if $P(N)$ is noncentral. Again, in [K] this was automatic from assuming that $p > m$.

The application of this theorem, which is the actual program in [K] (demonstrated in Sections 4 and 5 therein), is based on the observation (in [K, Proposition 3.11]) that any two regular subgroups of B that are isomorphic as abstract groups are, in fact, conjugate subgroups of B. That being said, to enumerate $R(\Gamma)$, one can avoid the complications of working with left regular representations and instead:

(1) replace $B = \mathrm{Perm}(\Gamma)$ by $S_{mp} = \mathrm{Perm}(\{1, \ldots, mp\})$,

(2) choose $\mathcal{P} = \langle \pi_1 \cdots \pi_m \rangle$ where $\pi_i = (1 + (i-1)p, \ldots, pi)$,

(3) determine $\mathcal{Q}$ corresponding to each such Γ where $\Gamma = \mathcal{P}\mathcal{Q}$,

(4) embed the Γ as subgroups of the semidirect product formulation of $\mathrm{Norm}_{S_{mp}}(\mathcal{P})$,

(5) enumerate the characters $\chi : \mathcal{Q} \to \mathbb{F}_p^*$ and concordantly the potential $P(N)$ as $\langle \hat{p}_\chi \rangle$ also embedded in $\mathrm{Norm}_{S_{mp}}(\mathcal{P})$,

(6) compute the possible $N \in R(\Gamma)$ that may arise, also as subgroups of $\mathrm{Norm}_{S_{mp}}(\mathcal{P})$.

If one is more interested in the sizes of the different $R(\Gamma, [M])$ one may use the fact (in [K, Theorem 3.5]) that, for each $N \in R(\Gamma, [M])$, if $P(N)$ is central in N then $P(N) = P(N^{\text{opp}})$, and otherwise either $P(N) = \mathcal{P}$ or $P(N^{\text{opp}}) = \mathcal{P}$. The point is that one can enumerate those $N \in R(\Gamma, [M])$ for which $P(N) = \mathcal{P}$ and, depending on whether $P(N)$ is central, use the above fact to infer the count of those for N for which $P(N) \neq \mathcal{P}$ (if any). The virtue of this is that one need not calculate the characters of Q in $\mathbb{F}_p^*$, nor the resulting potential $P(N)$.

We shall demonstrate applications of this program, where we now have a wider class of examples to choose from, based upon the conditions on p, m and $|\text{Aut}(Q)|$ as discussed above.

2. Groups of order $p_1 p_2 p_3$

To be slightly formal, if n_p denotes the number of Sylow p-subgroups of a group, we define the following subsets of $\mathbb{N} \times \mathbb{N}$:

$$F_Q = \{(p, m) \mid p \text{ prime}, \gcd(p, m) = 1, p \nmid |\text{Aut}(Q)| \text{ for all groups } Q \text{ of order } m\},$$

$$F_S = \{(p, m) \mid p \text{ prime}, \gcd(p, m) = 1, n_p = 1 \text{ for all groups of order } mp\}.$$

The program in [K] for enumerating Hopf–Galois structures on Galois extensions of order mp may be used for those $(p, m) \in F_Q \cap F_S$. As in [K], $(p, m) \in F_Q \cap F_S$ for p prime when $p > m$, but we want to now consider other p and m. The case of $p = 5$ and $m = 8$ as indicated already is one such example. In lieu of working out the enumeration of all the 14^2 possible pairings $R(\Gamma, [M])$ for order 40, we shall instead conclude with an overview of some (classes of) choices for $|\Gamma| = |N| = n = pm$ which force $(p, m) \in F_Q \cap F_S$. Such forcing conditions have appeared in group theory literature including recent examples such as [Pakianathan and Shankar 2000]. Our example will be somewhat more narrow, but is in this same spirit.

If $p_1 < p_2 < p_3$ are primes, then by Sylow theory $n_{p_3} \equiv 1 \pmod{p_3}$ and $n_{p_3} \mid p_1 p_2$. However, $n_{p_3} \neq p_1$ and $n_{p_3} \neq p_2$ since p_3 is larger than p_1 and p_2. If $n_{p_3} = p_1 p_2$ then one must have $p_1 p_2 (p_3 - 1)$ elements of order p_3 and so, by necessity, $n_{p_2} = 1$. Thus Γ has a normal subgroup P_2 of order p_2 and so Γ / P_2 (having order $p_1 p_3$) has a normal subgroup of order p_3, which gives rise to a normal abelian subgroup $\Delta \leq \Gamma$ of order $p_2 p_3$. We have that $P_2 \leq \Delta$ but also that Δ must contain a normal (in particular characteristic) subgroup P_3 of order p_3, which means that $P_3 \lhd \Gamma$, so that, in fact, $n_{p_3} = 1$. Hence $(p_3, p_1 p_2)$ is guaranteed to be in F_S. Moreover, the complementary subgroup Q is either a cyclic or metacyclic group of order $p_1 p_2$. The question then is whether $(p_3, p_1 p_2) \in F_Q$ as well. However, this is easy since

$$|\text{Aut}(Q)| = \begin{cases} (p_1 - 1)(p_2 - 1) & \text{if } Q \text{ is abelian,} \\ p_2(p_2 - 1) & \text{if } Q \text{ is nonabelian,} \end{cases}$$

and so, if $p_1 < p_2 < p_3$ one has $(p_3, p_1 p_2) \in F_S \cap F_Q$.

If $|\Gamma| = p_1p_2p_3$ then $\Gamma = PQ$ where P is cyclic of order p_3, of course, and normalized by Q which has order p_1p_2, which is itself either a direct or semidirect product of cyclic groups. That is, $\Gamma \cong C_{p_3} \rtimes_g (C_{p_2} \rtimes_f C_{p_1})$ where $f : C_{p_1} \to \mathrm{Aut}(C_{p_2})$ and $g : C_{p_2} \rtimes_f C_{p_1} \to \mathrm{Aut}(C_{p_3})$. There are at most two groups Q of order p_1p_2 depending on whether f is nontrivial. The group Γ being an iterated (semi)direct product, the role of g must also be factored into the enumeration of the distinct groups of order $p_1p_2p_3$. In particular, we must consider whether the C_{p_2} and/or the C_{p_1} components of Q act nontrivially on C_{p_3}. These possibilities for f and g are keyed to congruence conditions on the p_i, in particular, whether $p_1 \mid (p_2 - 1)$ and/or $p_1 \mid (p_3 - 1)$ and/or $p_2 \mid (p_3 - 1)$. Alonso [1976] (while exploring an explicit formula due to Hölder [1895] for the number of groups of square-free order) works through the enumeration of groups having order equal to the product of three distinct primes. In particular we give Table 1 therein of the number of groups of order $p_1p_2p_3$ (with our notation for the three primes):

$p_2 \mid (p_3 - 1)$	$p_1 \mid (p_3 - 1)$	$p_1 \mid (p_2 - 1)$	# groups
no	no	no	1
no	no	yes	2
no	yes	no	2
no	yes	yes	$p_1 + 2$
yes	no	no	2
yes	no	yes	3
yes	yes	no	4
yes	yes	yes	$p_1 + 4$

For two of the eight cases, the number of groups varies linearly with p_1 (specifically when C_{p_1} acts nontrivially on *both* C_{p_2} and C_{p_3}) but for the others the size is constant. For the case of $p_2 \mid (p_3 - 1)$, $p_1 \mid (p_3 - 1)$, and $p_1 \mid (p_2 - 1)$, it follows that $p_3 > p_1p_2 = m$ which falls into the category of cases dealt with in [K]. Indeed, therein we enumerated $R(\Gamma, [M])$ for all groups of order mp where $p = 2q + 1$ for q a prime (making p a safe-prime) and $m = \phi(p) = 2q$ so that $mp = 2 \times q \times (2q + 1)$, the product of three distinct primes! Therefore we will instead consider the case where $p_3 \not\equiv 1 \pmod{p_2}$ but where p_1 divides both $p_2 - 1$ and $p_3 - 1$, for this includes cases where $p_3 < m = p_1p_2$, for example, $(p_1, p_2, p_3) = (3, 7, 13)$. The $p_1 + 2$ cases can be presented explicitly and again we refer to [Alonso 1976] for the particulars with a slight modification of his notation.

Given (p_1, p_2, p_3), the groups of order $p_1p_2p_3$ are iterated semidirect products, the number of which, as mentioned above, are keyed to elements of order p_1 in U_{p_2} and U_{p_3}. Specifically, if $U_{p_3} = \langle u_3 \rangle$ and $U_{p_2} = \langle u_2 \rangle$, then the conditions

$$p_3 \equiv 1 \pmod{p_1}), \quad p_2 \equiv 1 \pmod{p_1})), \quad v_3 = u_3^{(p_3-1)/p_1}, \quad v_2 = u_2^{(p_2-1)/p_1}$$

together imply that then $|v_3| = p_1$ and $|v_2| = p_1$. We have the following presentations for groups of order $p_1 p_2 p_3$ which are the cases listed as (10)–(13) in [Alonso 1976, p. 634]. (Note that Alonso adopts the ordering $p_3 < p_2 < p_1$, the reverse of our convention.)

Proposition 2.1. *If p_1, p_2 and p_3 are distinct odd primes, where $p_1 < p_2 < p_3$ and where $p_3 \equiv 1 \pmod{p_1}$, $p_2 \equiv 1 \pmod{p_1}$, but $p_3 \not\equiv 1 \pmod{p_2}$, then the groups of order $p_1 p_2 p_3$ are*

$$\begin{aligned}
C_{p_3p_2p_1} &= \langle x, y, z \mid x^{p_3}, y^{p_2}, z^{p_1}, yxy^{-1} = x,\ zxz^{-1} = x,\ zyz^{-1} = y\rangle,\\
C_{p_2} \times (C_{p_3} \rtimes C_{p_1}) &= \langle x, y, z \mid x^{p_3}, y^{p_2}, z^{p_1}, yxy^{-1} = x,\ zxz^{-1} = x^{v_3},\ zyz^{-1} = y\rangle,\\
C_{p_3} \times (C_{p_2} \rtimes C_{p_1}) &= \langle x, y, z \mid x^{p_3}, y^{p_2}, z^{p_1}, yxy^{-1} = x,\ zxz^{-1} = x,\ zyz^{-1} = y^{v_2}\rangle,\\
C_{p_3p_2} \rtimes_i C_{p_1} &= \langle x, y, z \mid x^{p_3}, y^{p_2}, z^{p_1}, yxy^{-1} = x, zxz^{-1} = x^{v_3}, zyz^{-1} = y^{v_2^i}\rangle,
\end{aligned}$$

where $i = 1, \dots, p_1 - 1$.

Our goal is to examine $R(\Gamma, [M])$ for all groups of this order, as presented above. Following the program as laid out at the end of Section 1, we shall work within the ambient symmetric group $B = S_{mp}$ where, in this case, $p = p_3$ and $m = p_1 p_2$. Also, we will choose representative regular subgroups of $\mathrm{Norm}_B(\mathcal{P})$ where $\mathcal{P}$ is generated by the product of m disjoint p-cycles. The elements of $\mathrm{Norm}_B(\mathcal{P})$ shall be tuples $(\hat{x}, u, \xi)$ where $\hat{x}$ is a vector in $\mathbb{F}_p^m$, and where $u \in U_p$, $\xi \in S_m$. We note that $\mathcal{P}$ is embedded in $\mathrm{Norm}_B(\mathcal{P})$ as $\langle([1, 1, \dots, 1], 1, I)\rangle$. The representation of each Γ (as a regular subgroup of $\mathrm{Norm}_B(\mathcal{P})$) from among the $p_1 + 2$ different isomorphism classes is somewhat arbitrary but will be selected for computational convenience. Also, all will be chosen to have their Sylow p-subgroup be $\mathcal{P}$. The differences will lie in the representation of the complementary subgroups of order m, of which there are two possibilities, up to isomorphism, given that $p_2 \equiv 1 \pmod{p_1}$.

Lemma 2.2. *If we define $\bar{v}_2 = v_2^{-1}$ in U_{p_2} and*

$$\begin{aligned}
\sigma &= \prod_{k=1}^{p_1} (k, k + p_1, k + 2p_1, \dots, k + (p_2 - 1)p_1),\\
\tilde{\sigma} &= \prod_{k=1}^{p_1} (k, k + p_1, k + 2p_1, \dots, k + (p_2 - 1)p_1)^{\bar{v}_2^k},\\
\tau &= \prod_{i=0}^{p_2-1} (1 + ip_1, 2 + ip_1, \dots, p_1 + ip_1),\\
\delta &= \left(\prod_{i=0}^{p_2-1} (1 + ip_1, 2 + \bar{v}_2 ip_1, \dots, p_1 + \bar{v}_2{}^{p_1-1} ip_1)\right)^{-1},
\end{aligned}$$

then $\langle\sigma,\tau\rangle \cong C_{p_2p_1}$ and $\langle\sigma,\delta\rangle \cong C_{p_2} \rtimes C_{p_1}$, and both are regular subgroups of S_m where $m = p_1p_2$. Moreover, $\langle\tilde{\sigma},\tau\rangle = (\langle\sigma,\delta\rangle)^{\mathrm{opp}} = \mathrm{Cent}_{S_m}(\langle\sigma,\delta\rangle)$.

Proof. For the metacyclic group $C_{p_2} \rtimes C_{p_1}$, there exist generators of orders p_2 and p_1 where conjugating the order-p_2 generator by the order-p_1 generator raises the order-p_2 generator to the power v_2, where v_2 has order p_1 in U_{p_2}. This is possible given that $p_2 \equiv 1 \pmod{p_1}$. For $C_{p_2p_1}$, the two generators must, of course, centralize each other. If one writes σ above as $\sigma_1\cdots\sigma_{p_1}$ then one may verify that $\tau\sigma_i\tau^{-1} = \sigma_{i+1}$ and that $\delta\sigma_i\delta^{-1} = \sigma_{i-1}^{v_2}$. As to regularity, one recalls that if N is a semiregular subgroup of S_n of order n then N is regular, which is certainly the case for the groups $\langle\sigma,\tau\rangle$ and $\langle\sigma,\delta\rangle$. The last assertion is a matter of verifying that the respective generators centralize each other, for example, that $\sigma\tilde{\sigma}\sigma^{-1} = \tilde{\sigma}$. □

For the groups of order $p_1p_2p_3$, the generators of order p_2 centralize the order-p_3 generator, but the order-p_1 generator may or may not centralize the generators of orders p_2 and p_3 as presented in Proposition 2.1. Using these presentations, we define the following Γ of each isomorphism class embedded in $\mathrm{Norm}_B(\mathcal{P})$, just as in [K, p. 2230].

Proposition 2.3. *The regular subgroups of* $\mathrm{Norm}_B(\mathcal{P})$ *from each of the isomorphism classes of groups of order $mp = (p_1p_2)p_3$ given in Proposition 2.1 are*

$$\Gamma = C_{p_3p_2p_1} = \langle(\hat{1},1,I),(\hat{0},1,\sigma),(\hat{0},1,\tau)\rangle,$$
$$\Gamma = C_{p_2} \times (C_{p_3} \rtimes C_{p_1}) = \langle(\hat{1},1,I),(\hat{0},1,\sigma),(\hat{0},v_3,\tau)\rangle,$$
$$\Gamma = C_{p_3} \times (C_{p_2} \rtimes C_{p_1}) = \langle(\hat{1},1,I),(\hat{0},1,\tilde{\sigma}),(\hat{0},1,\tau)\rangle,$$
$$\Gamma = C_{p_3p_2} \rtimes_j C_{p_1} = \langle(\hat{1},1,I),(\hat{0},1,\tilde{\sigma}),(\hat{0},v_3,\tau^j)\rangle,$$

where $j = 1,\ldots,p_1-1$.

Proof. We note that $\mathcal{P} \le \mathrm{Norm}_B(\mathcal{P})$ is generated by $(\hat{1},1,I)$. We can prove that these groups have the asserted structure by using (2) above. First, we note that $(\hat{0},1,\beta)$ centralizes $(\hat{1},1,I)$ for any $\beta \in S_m$, and that $(\hat{0},1,\sigma)$ is centralized by $(\hat{0},1,\tau)$. Next we have

$$\begin{aligned}(\hat{0},v_3,\tau)(\hat{1},1,I)(\hat{0},v_3,\tau)^{-1} &= (\hat{0}+v_3\tau(\hat{1})-\hat{0},\, v_3\cdot 1\cdot v_3^{-1},\, \tau I\tau^{-1})\\ &= (v_3\tau(\hat{1}),1,I) = (v_3\hat{1},1,I) = (\hat{1},1,I)^{v_3}\end{aligned}$$

and similarly $(\hat{0},v_3,\tau^j)(\hat{1},1,I)(\hat{0},v_3,\tau^j)^{-1} = (\hat{1},1,I)^{v_3}$. We also have

$$(\hat{0},1,\tau)(\hat{0},1,\tilde{\sigma})(\hat{0},1,\tau)^{-1} = (\hat{0},1,\tau\tilde{\sigma}\tau^{-1}) = (\hat{0},1,\tilde{\sigma}^{v_2}) = (\hat{0},1,\tilde{\sigma})^{v_2}$$

and $(\hat{0},v_3,\tau^j)(\hat{0},1,\tilde{\sigma})(\hat{0},v_3,\tau^j)^{-1} = (\hat{0},1,\tilde{\sigma})^{v_2^j}$. The proof is finished by recalling [K, Proposition 3.8], which states that if $(\hat{a},u,\alpha)$ in $\mathrm{Norm}_B(\mathcal{P})$ has order coprime to p then it is fixed-point-free if and only if $\alpha \in S_m$ is fixed-point-free. In each of the groups listed here, the order-p subgroup $\mathcal{P}$ is unique and acts freely, and the elements outside of $\mathcal{P}$ have fixed-point-free permutation coordinates. Thus each group Γ given in the statement of the proposition is semiregular of order mp and therefore regular. □

Theorem 2.4. *The cardinality of* $R(\Gamma, [M])$ *for the* $p_1 + 2$ *classes of groups of order* $p_1p_2p_3$ *given in Proposition 2.1 is as follows, where the rows correspond to different* Γ *and the columns are the classes* $[M]$:

$\Gamma\downarrow$ $M\rightarrow$	$C_{p_3p_2p_1}$	$C_{p_3}\times(C_{p_2}\rtimes C_{p_1})$	$C_{p_2}\times(C_{p_3}\rtimes C_{p_1})$	$C_{p_3p_2}\rtimes_i C_{p_1}$
$C_{p_3p_2p_1}$	1	$2(p_1-1)$	$2(p_1-1)$	$4(p_1-1)$
$C_{p_3}\times(C_{p_2}\rtimes C_{p_1})$	p_2	$2(1+p_2(p_1-2))$	$2p_2(p_1-1)$	$4(1+p_2(p_1-2))$
$C_{p_2}\times(C_{p_3}\rtimes C_{p_1})$	p_3	$2p_3(p_1-1)$	$2(1+p_3(p_1-2))$	$4(1+p_3(p_1-2)$
$C_{p_3p_2}\rtimes_j C_{p_1}$	p_3p_2	$2p_3(1+p_2(p_1-2))$	$2p_2(1+p_3(p_1-2))$	—

The cardinality of $R(\Gamma, [C_{p_3p_2} \rtimes_i C_{p_1}])$ *is independent of* $i \in U_{p_1}$ *for the* Γ *listed on the first three rows, and for the last it depends on the relationship between i and j in* U_{p_1} *thus*:

i, j	$\lvert R(C_{p_3p_2} \rtimes_j C_{p_1}, [C_{p_3p_2} \rtimes_i C_{p_1}])\rvert$
$j = i, -i$	$2(1 + p_3 + p_2 + (2p_1 - 5)p_2p_3)$
$j \neq i, -i$	$2(2p_3 + 2p_2 + (2p_1 - 6)p_2p_3)$

As there are $p_1 + 2$ classes of groups of order $(p_1p_2)p_3$ and therefore $(p_1 + 2)^2$ different possible $R(\Gamma, [M])$, segmented into different classes depending on the different possibilities for $P(N)$, fully detailing the enumeration of all these would tax the patience of the reader. Moreover, given that many pairings give rise to very similar calculations, we shall instead give a sampling of the computations of $R(\Gamma, [M])$. In particular, we shall focus on the enumeration of $R(C_{p_3p_2} \rtimes_j C_{p_1}, [C_{p_3p_2} \rtimes_i C_{p_1}])$ since these can effectively be captured in one single computational framework. We will enumerate those N where $P(N) = \mathcal{P}$ and double the resulting figure to account for the corresponding N^{opp} which arise, and therefore have the full count.

Proof. We have $\Gamma \cong C_{p_3p_2} \rtimes_j C_{p_1}$ which is embedded in $\mathrm{Norm}_B(\mathcal{P})$ as

$$\langle(\hat{1}, 1, I), (\hat{0}, 1, \tilde{\sigma}), (\hat{0}, v_3, \tau^j)\rangle$$

and we are looking at those regular $N \leq \mathrm{Norm}_B(\mathcal{P})$ isomorphic to $C_{p_3p_2} \rtimes_i C_{p_1}$ and normalized by this Γ, where $i, j \in U_{p_1}$. Moreover, as we will be focusing on those N such that $P(N) = \mathcal{P}$, we have

$$N = \langle(\hat{1}, 1, I), (\hat{a}, u_3^r, \alpha), (\hat{b}, u_3^s, \beta)\rangle,$$

where $(\hat{a}, u_3^r, \alpha)$ has order p_2 and centralizes $(\hat{1}, 1, I)$, and $(\hat{b}, u_3^s, \beta)$ has order p_1 and conjugates $(\hat{1}, 1, I)$ to $(\hat{1}, 1, I)^{v_3} = (v_3\hat{1}, 1, I)$ and $(\hat{a}, u_3^r, \alpha)$ to $(\hat{a}, u_3^r, \alpha)^{v_2^i}$, in accordance with the presentations of the abstract groups as in Proposition 2.1. We will consider those conditions on the components of these 3-tuples which govern order and (semi)regularity and guarantee that Γ normalizes N. The computations themselves will require the basic operational facts about $\mathrm{Norm}_B(\mathcal{P})$ as given in (1), (2), and (3) together with the fact, mentioned earlier, that if $(\hat{v}, v, \zeta)$ has order coprime to $p = p_3 = |\mathcal{P}|$ and acts without fixed points, then $\zeta \in S_m$ $(m = p_2p_3)$ must act without fixed points on the m coordinates of $\hat{v}$. We shall proceed *ad hoc*, playing off the different requirements against each other in order to limit the choices for the components.

To begin with, we have (by virtue of the isomorphism class of N)

$$(\hat{a}, u_3^r, \alpha)(\hat{1}, 1, I)(\hat{a}, u_3^r, \alpha)^{-1} = (u_3^r\alpha(\hat{1}), 1, \alpha I\alpha^{-1}) = (u_3^r\hat{1}, 1, I) = (\hat{1}, 1, I)^{u_3^r},$$

which means that $u_3^r = 1$ since the order-p_2 generator of N must centralize $\mathcal{P}$, so that $(\hat{a}, u_3^r, \alpha) = (\hat{a}, 1, \alpha)$. And since $|(\hat{a}, 1, \alpha)| = p_2$, we have

$$\left(\sum_{t=0}^{p_2-1}\alpha^t(\hat{a}), 1, \alpha^{p_2}\right) = (\hat{0}, 1, I),$$

which, since $(\hat{a}, 1, \alpha)$ is fixed-point-free of order coprime to p_3, means that α equals $\alpha_1\alpha_2\cdots\alpha_{p_1}$, a product of p_1 disjoint p_2-cycles.

Also, in N we have

$$(\hat{b}, u_3^s, \beta)(\hat{1}, 1, I)(\hat{b}, u_3^s, \beta)^{-1} = (u_3^s\beta(\hat{1}), 1, I) = (u_3^s\hat{1}, 1, I) = (\hat{1}, 1, I)^{u_3^s},$$

which means that $u_3^s = v_3$, so that $(\hat{b}, u_3^s, \beta) = (\hat{b}, v_3, \beta)$. And since this must have order p_1, we have

$$\left(\sum_{t=0}^{p_1-1}v_3^t\beta^t(\hat{b}), v_3^{p_1}, \beta^{p_1}\right) = (\hat{0}, 1, I),$$

which, again by the fixed-point-freeness condition on this element of order coprime to p_3, means that β is a fixed-point-free element of order p_1 in S_m.

Again in N, we must have, by virtue of how the order-p_1 generator must act on the order-p_2 generator, that

$$(\hat{b}, v_3, \beta)(\hat{a}, 1, \alpha)(\hat{b}, v_3, \beta)^{-1} = (\hat{b} + v_3\beta(\hat{a}) - (\beta\alpha\beta^{-1})(\hat{b}), 1, \beta\alpha\beta^{-1}),$$

where the right-hand side must equal

$$(\hat{a}, 1, \alpha)^{v_2^i} = \left(\sum_{t=0}^{v_2^i-1}\alpha^t(\hat{a}), 1, \alpha^{v_2^i}\right).$$

In particular, we have $\beta\alpha\beta^{-1} = \alpha^{v_2^i}$ and, more broadly, $\beta \in \mathrm{Norm}_{S_m}(\langle\alpha\rangle)$ where α is a product of p_1 disjoint p_2-cycles in S_m where $m = p_1 p_2$. The implications of this are that $\mathrm{Norm}_{S_m}(\langle\alpha\rangle)$ is itself another twisted wreath product just like $\mathrm{Norm}_B(\mathcal{P})$ and so we shall use the same sort of 3-tuple representation for understanding the relationship between α and β within this smaller normalizer. We shall return to the analysis of this relationship shortly.

Looking outward, we now start imposing restrictions on the generators of N imposed by N being normalized by Γ. To start with, we observe that in $C_{p_2 p_3} \rtimes_i C_{p_1}$ the order-p_2 and order-p_3 subgroups are characteristic since they are unique of those orders. Thus

$$(\hat{0}, v_3, \tau^j)(\hat{a}, 1, \alpha)(\hat{0}, v_3, \tau^j)^{-1} = (v_3 \tau^j(\hat{a}), 1, \tau^j \alpha \tau^{-j}),$$

where the right-hand side must be an element of $\langle(\hat{a}, 1, \alpha)\rangle$; hence τ^j lies in $\mathrm{Norm}_{S_m}(\langle\alpha\rangle)$, and thus $\tau \in \mathrm{Norm}_{S_m}(\langle\alpha\rangle)$. We also have

$$(\hat{0}, 1, \tilde{\sigma})(\hat{a}, 1, \alpha)(\hat{0}, 1, \tilde{\sigma})^{-1} = (\tilde{\sigma}(\hat{a}), 1, \tilde{\sigma}\alpha\tilde{\sigma}^{-1}),$$

where the right-hand side must equal $(\hat{a}, 1, \alpha)$, since $\mathrm{Aut}(C_{p_2})$ has no p_2-torsion. This implies that $\tilde{\sigma}(\hat{a}) = \hat{a}$ and $\tilde{\sigma} \in \mathrm{Cent}_{S_m}(\alpha)$ which means that $\alpha \in \mathrm{Cent}_{S_m}(\tilde{\sigma})$. The latter observation implies that $\alpha \in \langle\sigma_1, \sigma_2, \ldots, \sigma_{p_1}\rangle$, where $\tilde{\sigma} = \sigma_1 \sigma_2^{\bar{v}_2} \cdots \sigma_{p_1}^{\bar{v}_2{}^{p_1-1}}$. The reason for this is that $\mathrm{Cent}_{S_m}(\tilde{\sigma})$ is isomorphic to the wreath product $C_{p_2} \wr S_{p_1} \cong C_{p_2}^{p_1} \rtimes S_{p_1}$, where the base group of the wreath product, $C_{p_2}^{p_1}$, corresponds to $\langle\sigma_1, \sigma_2^{\bar{v}_2}, \ldots, \sigma_{p_1}^{\bar{v}_2{}^{p_1-1}}\rangle = \langle\sigma_1, \ldots, \sigma_{p_1}\rangle$. Therefore, in $C_{p_2}^{p_1} \rtimes S_{p_1}$ the only p_2-torsion is in this base group since S_{p_1} cannot have any p_2-torsion. As to $\hat{a} = [a_1, \ldots, a_m]$, the condition $\tilde{\sigma}(\hat{a}) = \hat{a}$ means that, for any $k \in \{1, \ldots, m\}$,

$$a_k = a_{\tilde{\sigma}(k)} = a_{\tilde{\sigma}^2(k)} = \cdots = a_{\tilde{\sigma}^{p_2-1}(k)}.$$

But now, since $|(\hat{a}, 1, \alpha)| = p_2$, we have $\sum_{t=0}^{p_2-1} \alpha^t(\hat{a}) = \hat{0}$, and since α is in $\langle\sigma_1, \sigma_2, \ldots, \sigma_{p_1}\rangle$, the orbit of $k \in \{1, \ldots, m\}$ under α is the same as under $\tilde{\sigma}$. Thus $p_2 a_k$ vansishes for any a_k in $\hat{a}$. Since $\hat{a} \in \mathbb{F}_{p_3}^m$, this means $a_k = 0$ since $p_2 \neq 0$ in $\mathbb{F}_{p_3}$. The end result is that $(\hat{a}, 1, \alpha) = (\hat{0}, 1, \alpha)$.

As we saw above, α belongs to $\langle\sigma_1, \sigma_2, \ldots, \sigma_{p_1}\rangle$, and since α acts freely, we must have $\alpha = \sigma_1^{q_1} \sigma_2^{q_2} \cdots \sigma_{p_1}^{q_{p_1}}$, where $q_k \in U_{p_2}$ for $k = 1, \ldots, p_1$. Since $\tau\sigma_i\tau^{-1} = \sigma_{i+1}$, if $\tau\alpha\tau^{-1} = \alpha^w$ for some $w \in U_{p_2}$ then, given that $|\tau| = p_1$, we have $w^{p_1} \equiv 1 \pmod{p_2}$ and so $w = v_2^f$ for some $f \in \mathbb{Z}_{p_1}$. And since

$$\tau(\sigma_1^{q_1} \sigma_2^{q_2} \cdots \sigma_{p_1}^{q_{p_1}})\tau^{-1} = \sigma_1^{q_{p_1}} \sigma_2^{q_1} \cdots \sigma_{p_1}^{q_{p_1-1}},$$

we have $wq_1 = q_{p_1}, wq_2 = q_1, \ldots, wq_{p_1} = q_{p_1-1}$, which means that

$$\hat{q} = [q_1, q_2, \ldots, q_{p_1}] = q_1[1, w^{p_1-1}, w^{p_1-2}, \ldots, w^2, w],$$

where now $q_1 w = q_1 w'$ if and only if $w = w'$, and if $q_1 \neq q_1'$ then $\hat{q} \neq \hat{q}'$, which gives, ostensibly, $\phi(p_2)p_1$ choices for α. However, recalling that $(\hat{0}, 1, \alpha)^k = (\hat{0}, 1, \alpha^k)$, we may divide this count by $\phi(p_2)$ (i.e., assume $q_1 = 1$) to get p_1 unique choices for $\langle\alpha\rangle$ and thus p_1 unique $\langle(\hat{0}, 1, \alpha)\rangle$, one of each $w = v_2^f$ for $f \in \mathbb{Z}_{p_1}$.

Now that we have the enumeration of $(\hat{0}, 1, \alpha)$ given above, how many $(\hat{b}, v_3, \beta)$ are there? What first must be observed is that $C_{p_2 p_3} \rtimes_i C_{p_1}$ has $p_3 p_2 \phi(p_1)$ elements of order p_1. In the presentation

$$\langle x, y, z \mid x^{p_3}, y^{p_2}, z^{p_1}, yxy^{-1} = x,\ zxz^{-1} = x^{v_3},\ zyz^{-1} = y^{v_2^i}\rangle$$

the elements of order p_1 are of the form $x^r y^s z^t$ for $r \in \mathbb{Z}_{p_3},\ s \in \mathbb{Z}_{p_2},\ t \in U_{p_1}$, so the Sylow p_1-subgroups are *far* from characteristic. Thus, when a generator of Γ acts on $(\hat{b}, v_3, \beta)$ by conjugation, the result is one of these $p_3 p_2 \phi(p_1)$ other elements of order p_1. Consider the action of conjugation by $(\hat{0}, 1, \tilde{\sigma})$

$$(\hat{0}, 1, \tilde{\sigma})(\hat{b}, v_3, \beta)(\hat{0}, 1, \tilde{\sigma})^{-1} = (\tilde{\sigma}(\hat{b}), v_3, \tilde{\sigma}\beta\tilde{\sigma}^{-1}) = (\hat{1}, 1, I)^r(\hat{0}, 1, \alpha)^s(\hat{b}, v_3, \beta)^t,$$

which implies that t must equal 1 and so

$$(\hat{0}, 1, \tilde{\sigma})(\hat{b}, v_3, \beta)(\hat{0}, 1, \tilde{\sigma})^{-1} = (r\hat{1} + \alpha^s(\hat{b}), v_3, \alpha^s\beta).$$

For the action of $(\hat{0}, v_3, \tau^j)$ we get

$$\begin{aligned}(\hat{0}, v_3, \tau^j)(\hat{b}, v_3, \beta)(\hat{0}, v_3, \tau^j)^{-1} &= (v_3\tau^j(\hat{b}), v_3, \tau^j\beta\tau^{-j})\\ &= (\hat{1}, 1, I)^{r'}(\hat{0}, 1, \alpha)^{s'}(\hat{b}, v_3, \beta)^{t'},\end{aligned}$$

which implies that t' must equal 1 and so

$$(\hat{1}, 1, I)^{r'}(\hat{0}, 1, \alpha)^{s'}(\hat{b}, v_3, \beta)^{t'} = (r'\hat{1} + \alpha^{s'}(\hat{b}), v_3, \alpha^{s'}\beta).$$

This leads to four "normalization conditions" which must be satisfied:

$$\tilde{\sigma}(\hat{b}) - \alpha^s(\hat{b}) \in \langle\hat{1}\rangle, \tag{n1}$$

$$\tilde{\sigma}\beta\tilde{\sigma}^{-1} = \alpha^s\beta, \tag{n2}$$

$$v_3\tau^j(\hat{b}) - \alpha^{s'}(\hat{b}) \in \langle\hat{1}\rangle, \tag{n3}$$

$$\tau^j\beta\tau^{-j} = \alpha^{s'}\beta. \tag{n4}$$

We can deal with (n1) immediately by looking once more at how the generators of N interact. We have

$$(\hat{b}, v_3, \beta)(\hat{0}, 1, \alpha)(\hat{b}, v_3, \beta)^{-1} = (\hat{b} - (\beta\alpha\beta^{-1})(\hat{b}), 1, \beta\alpha\beta^{-1}),$$

which must equal $(\hat{0}, 1, \alpha)^{v_2^i} = (\hat{0}, 1, \alpha^{v_2^i})$, implying that $\hat{b} = (\beta\alpha\beta^{-1})(\hat{b}) = \alpha^{v_2^i}(\hat{b})$. By a similar argument to that above, the components of $\hat{b} \in \mathbb{F}_{p_3}^m$ are also constant along the supports of $\sigma_1, \ldots, \sigma_{p_1}$, so in fact we may simply observe that $\alpha(\hat{b}) = \hat{b}$.

Thus $\tilde{\sigma}(\hat{b}) - \alpha^s(\hat{b}) = \hat{b} - \hat{b} = \hat{0}$, which lies in $\langle \hat{1} \rangle$ automatically. This allows us, by the way, to rewrite (n3) as $v_3 \tau^j(\hat{b}) - \hat{b} \in \langle \hat{1} \rangle$. For (n2) and (n4) we must use that $\beta \in \mathrm{Norm}_{S_m}(\langle \alpha \rangle)$ and represent β as an element of this normalizer. Since $\alpha = \sigma_1 \sigma_2^{w^{p_1-1}} \cdots \sigma_{p_1}^{w}$ (a product of p_1 disjoint p_2-cycles), given that $m = p_1 p_2$ we have

$$\mathrm{Norm}_{S_m}(\langle \alpha \rangle) \cong \langle \sigma_1, \sigma_2^{w^{p_1-1}}, \dots, \sigma_{p_1}^{w} \rangle \rtimes (U_{p_2} \times S_{p_1}) \cong \mathbb{F}_{p_2}^{p_1} \rtimes (U_{p_2} \times S_{p_1}).$$

Thus we may write α as the 3-tuple $(\hat{1}, 1, I)$; moreover $\beta = (\hat{c}, v_2^i, \mu)$ for some $\hat{c}$ and μ, since β normalizes $\langle \alpha \rangle$ and in view of the following calculation, which uses (2) and the fact that $\mu(\hat{1}) = \hat{1}$ for all μ:

$$(\hat{c}, v_2^i, \mu)(\hat{1}, 1, I)(\hat{c}, v_2^i, \mu)^{-1} = (v_2^i \hat{1}, 1, I) = \alpha^{v_2^i}.$$

At first glance, this permits a fairly large number of possible β for a given α, but the requirement that Γ normalizes N imposes quite a number of restrictions. We begin by observing that

$$\begin{aligned} \alpha &= (\hat{1}, 1, I), \\ \tilde{\sigma} &= ([1, w\bar{v}_2, w^2\bar{v}_2{}^2, \dots, w^{p_1-1}\bar{v}_2{}^{p_1-1}], 1, I) = (\hat{d}, 1, I), \\ \tau &= (\hat{0}, w, (1, 2, \dots, p_1)), \end{aligned}$$

and, with this in mind, we see that (n4) translates into conditions on the components of these 3-tuples in $\mathrm{Norm}_{S_m}(\langle \alpha \rangle)$. In particular, with respect to $\beta = (\hat{c}, v_2^i, \mu)$,

$$\begin{aligned} \tau^j \beta \tau^{-j} &= (\hat{0}, w, (1, \dots, p_1))^j (\hat{c}, v_2^i, \mu)(\hat{0}, w, (1, \dots, p_1))^{-j} \\ &= \big(w^j (1, \dots, p_1)^j (\hat{c}), v_2^i, (1, \dots, p_1)^j \mu (1, \dots, p_1)^{-j}\big), \\ \alpha^{s'} \beta &= (s'\hat{1}, 1, I)(\hat{c}, v_2^i, \mu) = (s'\hat{1} + \hat{c}, v_2^i, \mu). \end{aligned}$$

Since $\beta = (\hat{c}, v_2^i, \mu)$ has order p_1 (and is therefore coprime to $|\alpha|$ in $\mathrm{Norm}_{S_m}(\langle \alpha \rangle)$), μ must be fixed-point-free of order p_1 in S_{p_1} and thus a p_1-cycle. But now (n4) implies that $(1, \dots, p_1)^j \mu (1, \dots, p_1)^{-j} = \mu$, which means that $\mu = (1, \dots, p_1)^e$ for some $e \in U_{p_1}$. Furthermore, (n4) also implies that $w^j (1, \dots, p_1)^j (\hat{c}) - \hat{c} \in \langle \hat{1} \rangle$, a condition which we shall get back to shortly. Since

$$\begin{aligned} \tilde{\sigma} \beta \tilde{\sigma} &= (\hat{d}, 1, I)(\hat{c}, v_2^i, \mu)(\hat{d}, 1, I)^{-1} = (\hat{d} + \hat{c} - v_2^i \mu(\hat{d}), v_2^i, \mu), \\ \alpha^s \beta &= (s\hat{1} + \hat{c}, v_2^i, \mu), \end{aligned}$$

condition (n2) implies that $\hat{d} - v_2^i \mu(\hat{d}) \in \langle \hat{1} \rangle$. (All instances of $\hat{1}$ here refer to the vector $[1, \dots, 1] \in \mathbb{F}_{p_2}^{p_1}$ which is the base group for the twisted wreath product $\mathrm{Norm}_{S_m}(\langle \alpha \rangle)$.)

Recalling that $\hat{d} = [1, w\bar{v}_2, w^2\bar{v}_2{}^2, \dots, w^{p_1-1}\bar{v}_2{}^{p_1-1}]$ and that $\mu = (1, \dots, p_1)^e$, the condition $\hat{d} - v_2^i \mu(\hat{d}) \in \langle \hat{1} \rangle$ can be analyzed by looking at the components and observing that, in $\langle \hat{1} \rangle$, all the components of a given vector are equal. That is,

$$\begin{aligned}\hat{d} &= [1, w\bar{v}_2, w^2\bar{v}_2{}^2, \dots, w^{p_1-1}\bar{v}_2{}^{p_1-1}],\\ v_2^i\mu(\hat{d}) &= [(w\bar{v}_2)^{p_1-e}v_2^i, (w\bar{v}_2)^{p_1-e+1}v_2^i, \dots, (w\bar{v}_2)^{p_1-e+(p_1-1)}v_2^i].\end{aligned}$$

In particular, the difference of the first components of $\hat{d}$ and $v_2^i\mu(\hat{d})$ equals the difference of their second components, and so

$$[1 - w^{p_1-e}\bar{v}_2{}^{p_1-e-i}] = w\bar{v}_2[1 - w^{p_1-e}\bar{v}_2{}^{p_1-e-i}]$$

in $\mathbb{F}_{p_2}$. If we let $x = 1 - w^{p_1-e}\bar{v}_2{}^{p_1-e-i}$ then the above implies that $x = w\bar{v}_2 x$, so either $x = 0$, or $w\bar{v}_2 = 1$ regardless of x. If $w\bar{v}_2 = 1$, then, since (as determined above) $w = v_2^f$ for some $f \in \mathbb{Z}_{p_1}$, it must be that $f = 1$. Otherwise, if $x = 0$ then $w^{p_1-e} = v_2^{p_1-e-i}$ and, since (as determined above) $w = v_2^f$, this means that $fe \equiv e + i \pmod{p_1}$, which, by the way, is impossible if $f = 1$ since $i \neq 0$.

Thus, if $f = 1$ then there are no restrictions on $e \in U_{p_1}$, and if $f \neq 1$ then $fe = e + i$ which implies that $e = i(f-1)^{-1} \pmod{p_1}$.

Now if we go back to (n4), we have the condition $w^j(1, \dots, p_1)^j(\hat{c}) - \hat{c} \in \langle\hat{1}\rangle$ which means that

$$[c_1, \dots, c_{p_1}] = [l, l, \dots, l] + w^j[c_{-j+1}, c_{-j+2}, \dots, c_{-j+p_1}]$$

for some $l \in \mathbb{F}_{p_2}$. Looking at the coordinates of $\hat{c}$ we get

$$\begin{aligned}c_{1+j} &= l + w^j c_1,\\ c_{1+2j} &= l + w^j c_{1+j} = l(1 + w^j) + w^{2j}c_1,\\ &\vdots\\ c_{1+kj} &= l(1 + w^j + (w^j)^2 + \cdots + (w^j)^{k-1}) + w^{kj}c_1,\\ &= \begin{cases} lk + c_1 & \text{if } w = 1 \text{ (i.e., } f = 0),\\ l\left(\frac{1-(w^j)^k}{1-w^j}\right) + w^{kj}c_1 & \text{if } w \neq 1 \text{ (i.e., } f \neq 0).\end{cases}\end{aligned}$$

This gives a partial parametrization of the possible $\hat{c}$, but we must also include the conditions imposed by the fact that $|\beta| = |(\hat{c}, v_2^i, \mu)| = p_1$, that is,

$$\sum_{t=0}^{p_1-1} v_2^{it}\mu^t(\hat{c}) = \hat{0}, \tag{$*$}$$

which, since $\mu^t = (1, \dots, p_1)^{et}$, means that $\sum_{t=0}^{p_1-1} v_2^{it}(1, \dots, p_1)^{et}(\hat{c}) = \hat{0}$. So if we let $\hat{c} = [c_1, \dots, c_{p_1}]$ then $(1, \dots, p_1)^{et}(\hat{c}) = [c_{-et+1}, c_{-et+2}, \dots, c_{-et+p_1}]$, which translates into the (single) condition

$$\sum_{t=0}^{p_1-1} v_2^{it}c_{-et+1} = 0 \tag{$**$}$$

since the vector equation $(*)$ consists of a system of equations, all of which are equivalent to $(**)$. To utilize this information, together with the above parametrization of $\hat{c}$ (in terms of c_1 and 'l' above), we first observe that $1+kj=-et+1$ implies $k=j^{-1}(-et)$ and so

$$c_{-et+1}=\begin{cases} l(j^{-1}(-et))+c_1 & \text{if } w=1 \text{ i.e., } f=0,\\ l\big(\frac{1-w^{-et}}{1-w^j}\big)+w^{-et}c_1 & \text{if } w\neq 1 \text{ i.e., } f\neq 0.\end{cases}$$

For the case $w=1$ ($f=0$), we have $e=i(-1)^{-1}=-i$ and so

$$\begin{aligned}\sum_{t=0}^{p_1-1} v_2^{it}c_{-et+1} &= \sum_{t=0}^{p_1-1} v_2^{it}(l(j^{-1}(-et))+c_1)=\sum_{t=0}^{p_1-1} v_2^{it}(l(j^{-1}(it))+c_1)\\ &= \sum_{t=0}^{p_1-1} v_2^{it}(lj^{-1}it+c_1)=c_1\sum_{t=0}^{p_1-1} v_2^{it}+l\sum_{t=0}^{p_1-1} j^{-1}itv_2^{it}\\ &= lj^{-1}i\sum_{t=0}^{p_1-1} tv_2^{it}=lj^{-1}i\frac{p_1}{v_2^{it}-1}.\end{aligned}$$

The last two lines of the above calculation are justified as follows. Since $v_2^{p_1}=1$ in $\mathbb{F}_{p_2}$, we have

$$\sum_{t=0}^{p_1-1} v_2^{it}=0,\qquad \sum_{t=0}^{p_1-1} tx^t=x\left(\frac{p_1x^{p_1-1}}{x-1}-\frac{x^{p_1}-1}{(x-1)^2}\right),$$

and substituting in $x=v_2^i$ we get

$$\sum_{t=0}^{p_1-1} tv_2^{it}=\frac{p_1v_2^{ip_1}}{v_2^i-1}=\frac{p_1}{v_2^i-1}.$$

This being the case, $\sum_{t=0}^{p_1-1} v_2^{it}c_{-et+1}=0$ if and only if $l=0$, which means that $c_{1+kj}=c_1$ for all k, and therefore $\hat{c}\in\langle\hat{1}\rangle$.

For the case where $w\neq 1$ (i.e., $f\neq 0$), we have

$$\begin{aligned}\sum_{t=0}^{p_1-1} v_2^{it}c_{-et+1} &= \sum_{t=0}^{p_1-1} v_2^{it}\left(l\left(\frac{1-(w^j)^{j^{-1}(-et)}}{1-w^j}\right)+w^{-et}c_1\right)\\ &= \frac{l}{1-w^j}\sum_{t=0}^{p_1-1} v_2^{it}(1-w^{-et})+\sum_{t=0}^{p_1-1} v_2^{it}w^{-et}c_1\\ &= \frac{l}{1-w^j}\sum_{t=0}^{p_1-1} v_2^{it}-\frac{l}{1-w^j}\sum_{t=0}^{p_1-1} v_2^{it}w^{-et}+c_1\sum_{t=0}^{p_1-1} v_2^{it}w^{-et}\end{aligned}$$

$$= \frac{-l}{1-w^j}\sum_{t=0}^{p_1-1} v_2^{it+f(-et)} + c_1 \sum_{t=0}^{p_1-1} v_2^{it+f(-et)}$$

$$= \frac{-l}{1-w^j}\sum_{t=0}^{p_1-1} v_2^{it-fet} + c_1 \sum_{t=0}^{p_1-1} v_2^{it-fet}$$

$$= \left(c_1 - \frac{l}{1-w^j}\right)\sum_{t=0}^{p_1-1} v_2^{(i-fe)t}.$$

If $i \neq fe$ then the last sum above equals 0 for all $c_1, l \in \mathbb{F}_{p_2}$, yielding p_2^2 choices. If $i = fe$ then the last sum is 0 only when $c_1 = l/(1-w^j)$, which means only p_2 choices.

The requirements of condition (n3), that $v_3\tau^j(\hat{b}) - \hat{b} \in \langle\hat{1}\rangle$, demand that one use the fact seen earlier, namely that $\tilde{\sigma}(\hat{b}) = \hat{b}$ and equivalently $\alpha(\hat{b}) = \hat{b}$. We also must factor in order considerations, just as in the above enumeration of $\hat{c}$, namely that $\sum_{t=0}^{p_1-1} v_3^t\beta^t(\hat{b}) = \hat{0}$. Since the components of $\hat{b}$ (a vector in $\mathbb{F}_{p_3}^{p_1p_2}$) are equal on the supports of the cycles that make up $\tilde{\sigma}$ (a product of p_1 disjoint p_2-cycles) and since $\tau\sigma_i\tau^{-1} = \sigma_{i+1}$, by identifying together these identical components, we can proceed, for the moment, as if $\hat{b}$ were a vector in $\mathbb{F}_{p_3}^{p_1}$. With this identification, τ acts on this $\hat{b}$ as $(1, \dots, p_1)$ and therefore τ^j acts like $(1, \dots, p_1)^j$. Similarly, since $\beta = (\hat{c}, v_2^i, (1, \dots, p_1)^e)$, it acts on $\hat{b}$ as $(1, \dots, p_1)^e$. Consequently, if we set $\hat{b} = [b_1, b_2, \dots, b_{p_1}]$ then (n3) implies that $[b_1, \dots, b_{p_1}] = [l, l, \dots, l] + v_3[b_{-e+1}, b_{-e+2}, \dots, b_{-e}]$ for some $l \in \mathbb{F}_{p_3}$ so that, in a similar fashion to the computation of $\hat{c}$ a few pages back, we have

$$b_{1+kj} = l(1 + v_3 + v_3^2 + \dots + v_3^{k-1}) + v_3^k b_1 = l\left(\frac{1-v_3^k}{1-v_3}\right) + v_3^k b_1.$$

Since $1 + kj = 1 - et$ implies $k = -j^{-1}et$, we get

$$b_{1-et} = l\left(\frac{1-v_3^{-j^{-1}et}}{1-v_3}\right) + v_3^{-j^{-1}et} b_1$$

for the parametrization of $\hat{b}$. The question is: how many ‘degrees of freedom’ do we have since, ostensibly, we can choose $l, b_1 \in \mathbb{F}_{p_3}$? The order requirement becomes $\sum_{t=0}^{p_1-1} v_3^t(1, \dots, p_1)^{et}(\hat{b}) = \hat{0}$ which reduces to $\sum_{t=0}^{p_1-1} v_3^t b_{1-et} = 0$. In a similar fashion to the calculations above, we get that $|(\hat{b}, v_3, \beta)| = p_1$ if and only if

$$\left(b_1 - \frac{l}{1-v_3}\right)\sum_{t=0}^{p_1-1} v_3^{t(1-j^{-1}e)} = 0,$$

which comes down to two possibilities given that $v_3^{p_1} \equiv 1 \pmod{p_3}$. If $e \neq j$ then we may choose b_1 and l in $\mathbb{F}_{p_3}$ arbitrarily (i.e., p_3^2 choices); otherwise, one must choose b_1 and l such that $b_1 = l/(1-v_3)$, which yields p_3 choices.

The enumeration of the possible $(\hat{b}, v_3, \beta)$ comes down to the interaction between the parameters f, e, i, and j as determined by order conditions on $(\hat{b}, v_3, \beta)$, where $\beta = (\hat{c}, v_2, (1, \dots, p_1)^e)$, and the normalization conditions (n1)–(n4). The parameters i and j are chosen at the outset, but the core parameter is $f \in \mathbb{Z}_{p_1}$ which determines the possible α. Subsequently, e is determined by β since $(\hat{b}, v_3, \beta)$ normalizes $\langle(\hat{0}, 1, \alpha)\rangle$. The different possibilities are summarized as follows:

$$\begin{aligned}
&f = 0 \text{ implies } e = i(f-1)^{-1} = -i,\\
&f = 1 \text{ allows } e = 1, \dots, p_1 - 1,\\
&f = 2, \dots, p_1 - 1 \text{ implies } e = i(f-1)^{-1},\\
&f = 0 \text{ implies } p_2 \text{ choices for } \hat{c},\\
&f > 0 \text{ implies } \begin{cases} p_2 \text{ choices for } \hat{c} \text{ when } i = fe,\\ p_2^2 \text{ choices for } \hat{c} \text{ when } i \neq fe,\end{cases}\\
&j = e \text{ implies } p_3 \text{ choices of } \hat{b},\\
&j \neq e \text{ implies } p_3^2 \text{ choices of } \hat{b}.
\end{aligned}$$

If we denote by s_0, s_1, $s_{>1}$ the number of $(\hat{b}, v_3, \beta)$ for the different choices of f, then we want to know $s_0 + s_1 + s_{>1}$.

For $f = 0$ we have $e = -i$ and so there are p_2 different $\beta = (\hat{c}, v_3, (1, \dots, p_1)^e)$. If $j = -i = e$ there are p_3 choices for $\hat{b}$, and if $j \neq -i$ there are p_3^2. Hence

$$s_0 = \begin{cases} p_2 p_3 & j = -i,\\ p_2 p_3^2 & j \neq -i.\end{cases}$$

For $f = 1$ we have $e = 1, \dots, p_1 - 1$ and $fe = f$, so $fe = i$ for *exactly one* e and $j = e$ also exactly once. Depending on whether $i = j$ or not, for potentially the *same* e, this results in different possibilities for the number of $\hat{c}$ and $\hat{b}$. We have

$$s_1 = \begin{cases} p_2 p_3 + (p_1 - 2) p_2^2 p_3^2 & j = i,\\ p_2 p_3^2 + p_2^2 p_3 + (p_1 - 3) p_2^2 p_3^2 & j \neq i.\end{cases}$$

For $f > 1$ we have $e = i(f-1)^{-1}$ and so fe equals $if(f-1)^{-1}$ which is *never* equal to i; thus there are p_2^2 choices for $\hat{c}$. If $j = i(f-1)^{-1} = e$ then $f - 1 = ij^{-1}$ which is impossible if $f - 1 = -1$, that is, $j = -i$; thus there are p_3^2 different $\hat{b}$ for each $f > 1$. We have then the count for $f > 1$:

$$s_{>1} = \begin{cases} (p_1 - 2) p_2^2 p_3^2 & j = -i,\\ (p_1 - 3) p_2^2 p_3^2 + p_2^2 p_3 & j \neq -i.\end{cases}$$

Now, for $i, j \in U_{p_1}$, we have that $j = i$ implies $j \neq -i$ since $p_1 > 2$ and, similarly, if $j = -i$ then $j \neq i$. So we have

$$s_0 + s_1 + s_{>1} = \begin{cases} p_2 p_3 + p_2 p_3^2 + p_2^2 p_3 + (2p_1 - 5) p_2^2 p_3^2 & j = i, -i,\\ 2p_2 p_3^2 + 2p_2^2 p_3 + (2p_1 - 6) p_2^2 p_3^2 & j \neq i, -i.\end{cases}$$

What $s_0+s_1+s_{>1}$ represents is the number of those

$$\{(\hat{0},1,\alpha),(\hat{b},v_2,\beta)\}$$

which generate $Q(N)$, where $P(N)=\mathcal{P}$ and where, for distinct f, the resulting $\langle\alpha\rangle$ and thus $\langle(\hat{0},1,\alpha)\rangle$ are distinct. Thus, to remove duplicate $Q(N)$s (arising from $(\hat{b},v_3,\beta)$ which generate the same $Q(N)$ with $(\hat{0},1,\alpha)$) we must divide by p_2p_3. The reason for this is that, as we mentioned above, in the abstract groups $C_{p_2p_3}\rtimes_i C_{p_1}$, if one multiplies a given element of order p_1 by an element of order p_2 or p_3 (or both) one gets another element of order p_1.

We have now completely enumerated those $N\in R(C_{p_2p_3}\rtimes_j C_{p_1},[C_{p_2p_3}\rtimes_i C_{p_1}])$ where $P(N)=\mathcal{P}$. Since the order-p_3 subgroup is not a direct factor, we now double this figure since the groups in $R(C_{p_2p_3}\rtimes_j C_{p_1},[C_{p_2p_3}\rtimes_i C_{p_1}])$ are evenly distributed between those classes where $P(N)=\mathcal{P}$ versus those for which $P(N)\neq\mathcal{P}$. The count given in the statement of the theorem for $|R(C_{p_2p_3}\rtimes_j C_{p_1},[C_{p_2p_3}\rtimes_i C_{p_1}])|$ is now verified. □

3. Square-free groups where $p<m$

There are *many* prime triples (p_1,p_2,p_3), where $p_3\equiv 1 \pmod{p_1}$, $p_2\equiv 1 \pmod{p_1}$, and $p_3\not\equiv 1 \pmod{p_2}$ (which give rise to groups of the type studied in Theorem 2.4) but where $p=p_3<p_1p_2=m$. Indeed, if one takes prime triples from $\{2,\dots,113\}$ then, of these, 474 have the property implying that groups of order $p_1p_2p_3$ are in the category studied in Theorem 2.4, and, of *these*, 246 have the property $p<m$. If we look beyond to groups of order $p_1p_2p_3p_4$, where $p_1<p_2<p_3<p_4$, which are also explored in [Alonso 1976], then the analog of Theorem 2.4 is the case where $\{p_4,p_3,p_2\}$ are all equivalent to 1 (mod p_1) but none of $\{p_4,p_3,p_2\}$ are equivalent to 1 mod each other. In this case, the number of groups of order $p_1p_2p_3p_4$ is $p_1^2+p_1+2$. If one looks at the 4-tuples of distinct primes chosen in $\{2,\dots,113\}$ then, of these, 3173 satisfy the congruence conditions of this class, and if $m=p_1p_2p_3$ and $p=p_4$ then, of *these*, 3151 have the property that $p<m$.

Acknowledgement

The author wishes to thank the referee for the careful reading given to this paper and for the helpful comments and suggestions.

References

[Alonso 1976] J. Alonso, "Groups of square-free order, an algorithm", *Math. Comp.* **30**:135 (1976), 632–637. MR 58 #22295 Zbl 0335.20002

[Byott 2004] N. P. Byott, "Hopf–Galois structures on Galois field extensions of degree *pq*", *J. Pure Appl. Algebra* **188**:1–3 (2004), 45–57. MR 2004j:16041 Zbl 1047.16022

[Chase and Sweedler 1969] S. U. Chase and M. E. Sweedler, *Hopf algebras and Galois theory*, Lecture Notes in Mathematics **97**, Springer, Berlin-New York, 1969. MR 41 #5348 Zbl 0197.01403

[Childs 2003] L. N. Childs, "On Hopf Galois structures and complete groups", *New York J. Math.* **9** (2003), 99–115. MR 2004k:16097 Zbl 1038.12003

[Greither and Pareigis 1987] C. Greither and B. Pareigis, "Hopf Galois theory for separable field extensions", *J. Algebra* **106**:1 (1987), 239–258. MR 88i:12006 Zbl 0615.12026

[Hölder 1895] O. Hölder, "Die Gruppen mit quadratfreier Ordnungzahl", *Nachr. Königl. Gesell. Wissenschaft. Göttingen Math.-Phys. Kl.* (1895), 211–229.

[Kohl 2013] T. Kohl, "Regular permutation groups of order mp and Hopf Galois structures", *Algebra Number Theory* **7**:9 (2013), 2203–2240. MR 3152012 Zbl 1286.12002

[Pakianathan and Shankar 2000] J. Pakianathan and K. Shankar, "Nilpotent numbers", *Amer. Math. Monthly* **107**:7 (2000), 631–634. MR 2001i:20051 Zbl 0986.20026

Communicated by Susan Montgomery
Received 2014-08-05 Revised 2015-10-01 Accepted 2015-11-27

tkohl@math.bu.edu
Department of Mathematics and Statistics, Boston University,
111 Cummington Mall, Boston, MA 02215, United States

Algebra & Number Theory

msp.org/ant

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2016 is US $290/year for the electronic version, and $485/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 10 No. 1 2016

1937-0652(2016)10:1;1-O