Algebra & Number Theory

Volume 7

2013

No. 9

Regular permutation groups of order *mp* and Hopf Galois structures

Timothy Kohl

msp

ALGEBRA AND NUMBER THEORY 7:9 (2013)
dx.doi.org/10.2140/ant.2013.7.2203

Regular permutation groups of order mp and Hopf Galois structures

Timothy Kohl

Let Γ be a group of order mp where p is prime and $p > m$. We give a strategy to enumerate the regular subgroups of $\mathrm{Perm}(\Gamma)$ normalized by the left representation $\lambda(\Gamma)$ of Γ. These regular subgroups are in one-to-one correspondence with the Hopf Galois structures on Galois field extensions L/K with $\Gamma = \mathrm{Gal}(L/K)$. We prove that every such regular subgroup is contained in the normalizer in $\mathrm{Perm}(\Gamma)$ of the p-Sylow subgroup of $\lambda(\Gamma)$. This normalizer has an affine representation that makes feasible the explicit determination of regular subgroups in many cases. We illustrate our approach with a number of examples, including the cases of groups whose order is the product of two distinct primes and groups of order $p(p-1)$, where p is a "safe prime". These cases were previously studied by N. Byott and L. Childs, respectively.

Introduction

Let L/K be a finite Galois extension of fields with Galois group $\Gamma = \mathrm{Gal}(L/K)$. Then the action of the group ring $K[\Gamma]$ of the Galois group Γ makes L/K into a Hopf Galois extension, in the sense of Chase and Sweedler [1969]. However, the classical Hopf Galois structure on L/K may not be the only Hopf Galois structure. For many Galois groups Γ, every Γ-Galois extension L/K has Hopf Galois structures by cocommutative K-Hopf algebras other than the classical Hopf Galois structure by the group ring $K[\Gamma]$ of the Galois group. Greither and Pareigis [1987] demonstrated this lack of uniqueness, by showing that the Hopf Galois structures on L/K are in direct correspondence with the regular subgroups $N \leq \mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$, where λ is the left action of Γ on Γ.

Subsequently Byott [2000] showed that nonclassical Hopf Galois structures are of interest in local Galois module theory settings, involving wildly ramified Galois extensions of local fields. Byott showed that a nonclassical Hopf Galois structure can yield freeness of the valuation ring of the extension over the corresponding

MSC2010: primary 20B35; secondary 12F10, 20E22, 16W30.
Keywords: regular permutation group, Hopf–Galois extension, holomorph.

associated order, whereas freeness fails over the associated order for the classical Galois structure given by the Galois group.

The Greither–Pareigis correspondence is via Galois descent: if H is a cocommutative K-Hopf algebra and L is an H-module algebra via some Galois structure map $H \otimes_K L \to L$, then base changing to L yields a Galois structure map $(L \otimes_K H) \otimes_L (L \otimes_K L) \to (L \otimes_K L)$. But then $L \otimes_K L \cong \mathrm{Hom}_L(L[\Gamma], L) = L[\Gamma]^* \cong \sum_{\gamma \in \Gamma} L\varphi_\gamma$ and $L \otimes_K H \cong L[N]$, where N is a group that acts on $L \otimes_K L$ via acting as a regular group of permutations on the subscripts of the dual basis $\{\varphi_\gamma : \gamma \in \Gamma\}$ of $L[\Gamma]^*$. Then N is normalized by $\lambda(\Gamma)$. Conversely, given a regular subgroup N of $\mathrm{Perm}\,\Gamma$, then $L[N]$ yields a Hopf Galois structure on $L[\Gamma]^*$. If N is normalized by $\lambda(\Gamma)$, then Galois descent yields a K-Hopf algebra structure by $H = (L[N])^G$ on L/K.

Thus determining Hopf Galois structures on Galois extensions L/K of fields with Galois group Γ is translated into the purely group-theoretic problem of determining regular subgroups of $B = \mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$.

Nearly all of the work since [Greither and Pareigis 1987] on determining the Hopf Galois structures on a Galois extension L/K of fields with Galois group Γ, or on counting or estimating the number of Hopf Galois structures on such field extensions, has involved a further translation of the problem. The idea of the translation, as formulated by Byott [1996], is to stratify the problem into a set of problems, one for each isomorphism type of group of the same cardinality as Γ. For each such group M, one seeks regular embeddings (modulo a certain equivalence) of Γ into the holomorph $\mathrm{Hol}(M) \subset \mathrm{Perm}(M)$ of M, where $\mathrm{Hol}(M) \cong M \rtimes \mathrm{Aut}(M)$. The number of such regular embeddings is equal to the number of Hopf Galois structures on L/K via K-Hopf algebras H such that $L \otimes_K H \cong L[M]$: then the Hopf Galois structure is said to have *type* M. This translation turns the problem of classifying Hopf Galois structures into a collection of somewhat easier problems, easier because it has seemed more tractable to identify regular subgroups in $\mathrm{Hol}\,M$ than in the usually much larger group $\mathrm{Perm}\,\Gamma$.

On the other hand, once one has a regular embedding β of Γ in $\mathrm{Hol}\,M$, two translations are required to actually describe the corresponding Hopf Galois structure on L/K. It is typically not easy to identify the regular subgroup N of $\mathrm{Perm}\,\Gamma$ isomorphic to M that corresponds to the embedding β and the action of N on $L[G]^*$ on which one may apply Galois descent. For this reason, it is of interest to find groups Γ where regular subgroups of $\mathrm{Perm}\,\Gamma$ normalized by $\lambda(\Gamma)$ may be determined directly.

The aim of this paper is to do exactly that for a special class of groups. We consider groups Γ of order mp where p is prime and $p > m$. Then $\lambda(\Gamma)$ has a unique p-Sylow subgroup $\mathcal{P}$ of order p. Our main result is that every regular subgroup of $\mathrm{Perm}\,\Gamma$ normalized by Γ is contained in $\mathrm{Norm}_B(\mathcal{P})$, the normalizer in

$B = \mathrm{Perm}(\Gamma)$ of $\mathcal{P}$. The group $\mathrm{Norm}_B(\mathcal{P})$ may be identified as the subgroup of the affine group $\mathrm{AGL}_m(\mathbb{F}_p) \subset \mathrm{GL}_{m+1}(\mathbb{F}_p)$ consisting of $(m+1) \times (m+1)$ matrices of the form

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix},$$

where A is a scalar multiple of an $m \times m$ permutation matrix and v is in $\mathbb{F}_p^m$. For $m < p$, $\mathrm{Norm}_B(\mathcal{P})$ is far smaller and much more amenable than the symmetric group $\mathrm{Perm}(\Gamma) \cong S_{mp}$. (For example, for $p = 7$ and $m = 4$, $\mathrm{Norm}_B(\mathcal{P})$ has order $7^4 \cdot 6 \cdot 4! = 345779$, while S_{28} has order $28! \sim 3 \cdot 10^{29}$.)

The first application of our main result is to determine all regular subgroups of $\mathrm{Perm}\,\Gamma$ normalized by $\lambda(\Gamma)$ where Γ has order pq, distinct primes. N. Byott [2004] determined the Hopf Galois structures on a field extension L/K with Galois group Γ of order pq by looking at the holomorph $\mathrm{Hol}\,M$ of M for M a group of order pq and determining the regular embeddings of Γ whose intersection with $\mathrm{Aut}\,M$ has a given cardinality. The method of this paper is quite different; the reader may judge the relative efficiency of the two methods.

For our second application we consider the Hopf Galois structures on a Galois extension L/K where the Galois group Γ has order mp with $m = 2q$, q prime, and $p = 2q + 1$ prime: thus p is a safe prime and q is a Sophie Germain prime. L. Childs [2003] determined all of the Hopf Galois structures on a Galois extension L/K of fields with Galois group $\Gamma \cong \mathrm{Hol}(C_p)$ by determining embeddings of Γ into $\mathrm{Hol}\,M$ for each of the six isomorphism types of groups of order mp. We extend [Childs 2003] by determining the number of Hopf Galois structures for Γ and M running through all 36 pairs (Γ, M). Since the computations are in many cases similar to those in the pq case, we provide only a few sample cases to illustrate the variety of approaches needed.

This paper generalizes the results for $m = 4$ in [Kohl 2007]. Some of the ideas here are similar to those in that paper, but for the benefit of the reader we have made this paper independent of [Kohl 2007] and reasonably self-contained.

1. Preliminaries

Groups of order mp. We begin with some observations about abstract groups G of order mp, where $m < p$.

First, G has a p-Sylow subgroup P that is unique, and hence a characteristic subgroup of G. Also, by the Schur–Zassenhaus lemma, there exists a subgroup $Q \le G$ of order m, and $G \cong P \rtimes_\tau Q$ with $\tau : Q \to \mathrm{Aut}(P)$ induced by conjugation within G.

Lemma 1.1. *Let G have order mp with p prime and $p > m$, with $G \cong P \rtimes_\tau Q$ as above.*

(a) *If τ is trivial, that is, $G \cong P \times Q$, then p does not divide the order of* $\operatorname{Aut} G$.

(b) *If τ is not-trivial, then* $\operatorname{Aut} G$ *has a unique p-Sylow subgroup, consisting of inner automorphisms given by conjugation by elements of P.*

Proof. Since $P \leq G$ is unique and thus characteristic, if $\psi \in \operatorname{Aut}(G)$ then ψ induces $\bar{\psi} \in \operatorname{Aut}(G/P)$. Our claim is that $|\psi|$ cannot be p^k for any $k > 1$. Since $|G/P| = m < p$ then $p \nmid |\operatorname{Aut}(G/P)|$ so if ψ has order p^k then $\bar{\psi} = \mathrm{id}_{G/P}$. Therefore, for any $g \in G$ one has $\psi(gP) = gP$ and so $g^{-1}\psi(g) \in P$ and likewise $g^{-1}\psi^r(g) \in P$ for any power r. If $|\psi| = p^k$ for $k > 1$ then there exists $g \in G$ such that

$$g, \psi(g), \ldots, \psi^{p^k-1}(g)$$

are distinct elements of G, but then

$$1, g^{-1}\psi(g), \ldots, g^{-1}\psi^{p^k-1}(g)$$

are p^k distinct elements of P, which is impossible since $|P| = p$. Therefore the p torsion of $\operatorname{Aut} G$ cannot be larger than p. If τ is trivial then $G \cong P \times Q$ for Q of order m. As such, $\operatorname{Aut}(G) \cong \operatorname{Aut}(P) \times \operatorname{Aut}(Q)$ and neither $\operatorname{Aut} P$ nor $\operatorname{Aut} Q$ can have elements of order p so $p \nmid |\operatorname{Aut}(G)|$. If $\tau : Q \to \operatorname{Aut}(P)$ is nontrivial then one can show that $|P \cap Z(G)| = 1$, so that if $P = \langle x \rangle$ then conjugation by x provides an element of order p in $\operatorname{Aut} G$ which therefore generates the p-Sylow subgroup of $\operatorname{Aut} G$. □

Regular subgroups.

Definition. Let $\mathcal{P} \leq \lambda(\Gamma)$ be the unique p-Sylow subgroup of $\lambda(\Gamma)$.

Definition. A subgroup $N \leq B = \operatorname{Perm}(\Gamma)$ is *semiregular* [Wielandt 1955] if $\operatorname{Stab}_N(\gamma) = \{\eta \in N \mid \eta(\gamma) = \gamma\}$ is the trivial group for all $\gamma \in \Gamma$.

A subgroup $N \leq B$ is *regular* if N is semiregular and either $|N| = |\Gamma|$ or N acts transitively on Γ.

If N is semiregular and $\eta \neq e$ (the identity) of N, then η acts on Γ without fixed points. Thus for η in N, if η has order h, then for each γ in Γ,

$$(\gamma, \eta(\gamma), \ldots, \eta^{h-1}(\gamma))$$

is the cycle containing γ in the cycle decomposition of η in $B = \operatorname{Perm}(\Gamma)$. Hence η is a product of k cycles of length h, where $hk = |\Gamma|$.

Definition. For η in $B = \operatorname{Perm}(\Gamma)$,

$$\operatorname{Supp}(\eta) = \{\gamma \in \Gamma \mid \eta(\gamma) \neq \gamma\}.$$

Thus if N is semiregular and $\eta \in N$ is not the identity, then $\mathrm{Supp}(\eta) = \Gamma$.

Because of the connection to Hopf Galois structures, in this paper we are not interested in all the regular subgroups of B, but only in those normalized by $\lambda(\Gamma)$, the image of the left regular representation of Γ in B.

Definition. Let $R(\Gamma)$ denote the set of regular subgroups N of $B = \mathrm{Perm}(\Gamma)$ such that $\lambda(\Gamma) \leq \mathrm{Norm}_B(N)$, the normalizer in B of N.

We partition $R(\Gamma)$ as follows:

Definition. For M a group of order $|\Gamma|$, let $[M]$ denote the isomorphism type of M, and let $R(\Gamma, [M])$ denote the subset of $R(\Gamma)$ consisting of the regular subgroups N in $R(\Gamma)$ that are isomorphic to M.

Then $R(\Gamma)$ is the disjoint union of the sets $R(\Gamma, [M])$ where $[M]$ runs through the isomorphism types of groups of order equal to $|\Gamma|$.

To enumerate $R(\Gamma)$, we enumerate $R(\Gamma, [M])$ for each isomorphism type $[M]$. As noted in the introduction, the Hopf Galois structures on a Galois extension L/K with Galois group $\Gamma = \mathrm{Gal}(L/K)$ correspond in a one-to-one fashion to the elements of $R(\Gamma)$; if a Hopf Galois structure corresponds to N in $R(\Gamma, [M])$, then the K-Hopf algebra acting on L has *type M* (because $L \otimes_K H \cong L[M]$).

Our goal in this paper is to develop a new method to enumerate $R(\Gamma)$ for $|\Gamma| = mp$.

Cycle structures. Let N be a regular subgroup of $B = \mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$, and let $P(N)$ be the unique order-p subgroup of N. Then we can relate the cycle structure of a generator of $\mathcal{P} = P(\lambda(\Gamma))$ to the cycle structure of a generator of $P(N)$:

Proposition 1.2. *Let $\mathcal{P}$ be the unique subgroup of $\lambda(\Gamma)$ of order p, and let $\mathcal{P} = \langle\phi\rangle$, where $\phi = \pi_1\pi_2\cdots\pi_m$ with $\pi_1, \ldots, \pi_m$ disjoint p-cycles in* $\mathrm{Perm}(\Gamma) \cong S_{pm}$. *Let N be a regular subgroup of* $\mathrm{Perm}\,\Gamma$ *normalized by $\lambda(\Gamma)$ and let $P(N)$ be the p-Sylow subgroup of N. Then $P(N)$ is generated by $\theta = \pi_i^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m}$ where $a_i \in U_p = \mathbb{F}_p^\times$ for each i.*

Proof. N is normalized by $\lambda(\Gamma)$ and $P(N)$ is characteristic in N. Hence $\lambda(\Gamma)$, and therefore also $\mathcal{P}$, normalizes $P(N)$. But $\gcd(|\mathrm{Aut}(P(N))|, p) = 1$, so $\mathcal{P}$ centralizes $P(N)$, hence $P(N)$ centralizes $\mathcal{P}$.

Let θ be a generator of $P(N)$. Then

$$\pi_1\pi_2\cdots\pi_m = \phi = \theta\phi\theta^{-1} = \theta(\pi_1\pi_2\cdots\pi_m)\theta^{-1} = \pi_1\pi_2\cdots\pi_m,$$

and so θ permutes the cycles $\pi_1, \ldots, \pi_m$. But conjugation by θ has order dividing p, and $\mathrm{Perm}(\{\pi_1, \ldots, \pi_m\})$ has order $m!$ coprime to p, so for all i, $\theta\pi_i\theta^{-1} = \pi_i$.

For each i and for any c in $\operatorname{Supp}\pi_i$, π_i is the cycle

$$\pi_i = (c, \pi_i(c), \pi_i^2(c), \ldots, \pi_i^{p-1}(c)),$$

and $\theta\pi_i\theta^{-1}$ is the cycle

$$\theta\pi_i\theta^{-1} = (\theta(c), \theta\pi_i(c), \theta\pi_i^2(c), \ldots, \theta\pi_i^{p-1}(c)).$$

If $\theta(c) = \pi_i^a(c)$, then comparing the two cycles, we see that $\theta\pi_i^r(c) = \pi_i^{a+r}(c)$ for all r. Thus for each i, on $\operatorname{Supp}\pi_i$, $\theta = \pi_i^a$. Hence $\theta = \pi_i^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m}$ in B. No a_i can equal 0 modulo p; if it did, c_i would be fixed under θ, and θ is an element of the semiregular subgroup $P(N)$ of B. □

Let N be a regular subgroup of $B = \operatorname{Perm}(\Gamma)$, let $P(N)$ be the p-Sylow subgroup of N, and let $N = P(N)Q(N)$, where $Q(N)$ is a complementary subgroup of order m to $P(N)$ in N. Then $Q(N)$ normalizes $P(N) = \langle \pi_1^{a_1}\cdots\pi_m^{a_m}\rangle$. Let $Q(N) = \{q_1 = e, q_2, \ldots, q_m\}$. Since N is a regular subgroup of $\operatorname{Perm}\Gamma$,

$$\Gamma = Ne_\Gamma = \bigcup_{i=1}^{m} P(N)q_ie_\Gamma,$$

and $P(N) = \langle\theta\rangle$ acts on $P(N)q_ie_\Gamma$ via the left regular representation. After renumbering the elements of $Q(N)$ as needed, we have $\Pi_i = \operatorname{Supp}(\pi_i) = P(N)q_ie_\Gamma$.

Proposition 1.3. *$Q(N)$ is a regular group of permutations of* $\{\Pi_1, \ldots, \Pi_m\}$.

Proof. For q in $Q(N)$,

$$q\Pi_i = qP(N)q_ie_\Gamma = qP(N)q^{-1}q_ie_\Gamma = P(N)qq_ie_\Gamma,$$

since $P(N)$ is a normal subgroup of N. So the action of $Q(N)$ on $\{\Pi_1, \ldots, \Pi_m\}$ is the same as the left regular representation $\lambda(Q(N))$ on $Q(N)$.

The partition $\{\Pi_1, \ldots, \Pi_m\}$ arising from $P(N)$ is the same as that from $\mathcal{P}$. So we conclude that each regular subgroup N of $\operatorname{Perm}\Gamma$ normalized by $\lambda(\Gamma)$ has the form $P(N)Q(N)$ where $P(N) = \langle\pi_1^{a_1}\cdots\pi_m^{a_m}\rangle$ and $Q(N)$ is a regular subgroup of $\operatorname{Perm}(\{\Pi_1, \ldots, \Pi_m\})$ with $\Pi_i = \operatorname{Supp}(\pi_i)$. □

2. Characters and generators of $P(N)$

In this section we determine the semiregular order-p subgroups of $B = \operatorname{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$.

Recall that $\lambda(\Gamma) = \mathcal{P}\mathcal{Q}$ where $\mathcal{P}$ is the unique p-Sylow subgroup of $\lambda(\Gamma)$ and $\mathcal{Q}$ is a complement of $\mathcal{P}$ in $\lambda(\Gamma)$. Then $\mathcal{P} = \langle\phi\rangle$ where $\phi = \pi_1\cdots\pi_m$, a product of p-cycles, $\Pi_i = \operatorname{Supp}(\pi_i)$ for $i = 1, \ldots, m$, and $\mathcal{Q}$ is a regular group of permutations of $\{\Pi_1, \ldots, \Pi_m\}$, hence may be viewed as a regular subgroup of S_m. From the last result of the previous section, every semiregular order-p subgroup P of B

normalized by $\lambda(\Gamma)$ has the form $P = \langle \pi_1^{a_1} \cdots \pi_m^{a_m} \rangle$ for $a_1, \ldots, a_m$ in $\mathbb{F}_p^\times$. Here we describe the possible P more precisely.

There is an isomorphism from $V = \langle \pi_1, \ldots, \pi_m \rangle$ to $\mathbb{F}_p^m$ by

$$\pi_1^{i_1} \cdots \pi_m^{i_m} \mapsto (i_1, \ldots, i_m).$$

Denote $\pi_1^{i_1} \cdots \pi_m^{i_m}$ by $[i_1, \ldots, i_m]$. Then $\hat{v}_i = (0, \ldots, 1, \ldots, 0)$ in $\mathbb{F}_p^m$ corresponds to π_i. By abuse of notation, we will identify $\hat{v}_i$ in $\mathbb{F}_p^m$ with π_i in V.

Let $\chi : \mathcal{Q} \to \mathbb{F}_p^\times$ be a homomorphism, that is, a degree-one representation or linear character of $\mathcal{Q}$ in $\mathbb{F}_p$ [Isaacs 1976].

Let $\hat{p}_\chi = \sum_{\gamma \in \mathcal{Q}} \chi(\gamma) \hat{v}_{\gamma(1)}$. As with $\hat{v}_i$, we will identify $\hat{p}_\chi$ with the corresponding element of V, as in the statement of the following result:

Theorem 2.1. *For each linear character $\chi : \mathcal{Q} \to \mathbb{F}_p^\times$, $\hat{p}_\chi$ is a generator of a semiregular order-p subgroup of V normalized by $\lambda(\Gamma)$. Conversely, let P be an order-p semiregular subgroup of V that is normalized by $\lambda(\Gamma)$. Then $P = \langle \hat{p}_\chi \rangle$ for some linear character $\chi : \mathcal{Q} \to \mathbb{F}_p^\times$.*

Proof. For the first part, we begin by observing that $\mathcal{Q}$ normalizes $\mathcal{P} = \langle \pi \rangle$, so for all μ in $\mathcal{Q}$, $\mu(\pi) = \mu \pi \mu^{-1} = \pi^{\tau(\mu)}$ for some $\tau(\mu)$ in $\mathbb{F}_p^\times$. Now

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

and so

$$\begin{aligned} \mu \hat{p}_\chi \mu^{-1} &= \sum_{\gamma \in \mathcal{Q}} \chi(\gamma)(\mu \hat{v}_{\gamma(1)} \mu^{-1}) = \sum_{\gamma \in \mathcal{Q}} \chi(\gamma) \tau(\mu) \hat{v}_{\mu\gamma(1)} \\ &= \tau(\mu) \sum_{\gamma \in \mathcal{Q}} \chi(\gamma) \hat{v}_{\mu\gamma(1)} = \tau(\mu) \chi(\mu)^{-1} \hat{p}_\chi. \end{aligned}$$

Hence $\langle \hat{p}_\chi \rangle$ is normalized by $\mathcal{Q}$. Since $\langle \hat{p}_\chi \rangle$ is a subgroup of V, $\langle \hat{p}_\chi \rangle$ is centralized by $\mathcal{P}$, hence $\langle \hat{p}_\chi \rangle$ is normalized by $\lambda(\Gamma)$.

Now we show the converse.

Let $[a_1, \ldots, a_m]$ be in V with all $a_i \neq 0$ in $\mathbb{F}_p$, such that $\langle [a_1, \ldots, a_m] \rangle$ is normalized by $\lambda(\Gamma)$. Then for γ in $\mathcal{Q}$,

$$\gamma [a_1, \ldots, a_m] \gamma^{-1} = [a_1, \ldots, a_m]^{d_\gamma} = [d_\gamma a_1, \ldots, d_\gamma a_m].$$

The map from $\mathcal{Q}$ to $\mathbb{F}_p^\times$ given by $\gamma \mapsto d_\gamma$ is a homomorphism, hence a linear character. Also, for every γ in $\mathcal{Q}$,

$$\gamma \pi_i \gamma^{-1} = \pi_{\gamma(i)}^{c_\gamma},$$

where $\mathcal{Q}$ acts as a regular subgroup of $\mathrm{Perm}(1, \ldots, m)$ as noted above, and c_γ is in $\mathbb{F}_p^\times$. Then $c_{\gamma'\gamma} = c_{\gamma'} c_\gamma$, so the map $\gamma \mapsto c_\gamma$ is a linear character from $\mathcal{Q}$ to $\mathbb{F}_p^\times$.

Since all $a_i \neq 0$, in the subgroup $\langle [a_1, \dots, a_m] \rangle$ we may replace the generator by a suitable power so that $a_1 = 1$, so we assume henceforth that $a_1 = 1$. Now for γ in $\mathfrak{Q}$,

$$\gamma[a_1, \dots, a_m]\gamma^{-1} = [c_\gamma a_{\gamma^{-1}(1)}, \dots, c_\gamma a_{\gamma^{-1}(m)}],$$

and so

$$c_\gamma a_{\gamma^{-1}(i)} = d_\gamma a_i,$$

for every i. Setting $i = \gamma(j)$, this becomes

$$c_\gamma a_j = d_\gamma a_{\gamma(j)},$$

or

$$a_{\gamma(j)} = \frac{c_\gamma}{d_\gamma} a_j.$$

In particular,

$$a_{\gamma(1)} = \frac{c_\gamma}{d_\gamma} a_1 = \frac{c_\gamma}{d_\gamma}.$$

Since $\mathfrak{Q}$ acts as a regular subgroup of permutations of $1, \dots, m$, this last formula determines a_i for all $i = 1, \dots, m$.

The mapping $\chi : \mathfrak{Q} \to \mathbb{F}_p^\times$ defined by $\chi(\gamma) = c_\gamma / d_\gamma$ is a homomorphism, hence a linear character of $\mathfrak{Q}$ in $\mathbb{F}_p^\times$, and we have:

$$[a_1, \dots, a_m] = \prod_{\gamma \in \mathfrak{Q}} \pi_{\gamma(1)}^{a_\gamma(1)} = \prod_{\gamma \in \mathfrak{Q}} \pi_{\gamma(1)}^{\chi(\gamma)} = \sum_{\gamma \in \mathfrak{Q}} \chi(\gamma) \hat{v}_{\gamma(1)} = \hat{p}_\chi. \qquad \square$$

Example 2.1. In [Kohl 2007] we examined groups of order $4p$. There were two cases. If $\mathfrak{Q} = C_p \times C_p = \langle x, y \rangle$, then there are four linear characters, defined by the following table:

	1	x	y	xy
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

For $\mathfrak{Q} = C_4 = \langle x \rangle$, we have two or four linear characters:

	1	x	x^2	x^3
ψ_1	1	1	1	1
ψ_2	1	-1	1	-1
ψ_3	1	ζ	-1	ζ^3
ψ_4	1	ζ^3	-1	ζ

with the last two characters occurring only when $p \equiv 1 \pmod 4$. These linear characters corresponded to the possible groups $P_1, \dots, P_6$ found in [Kohl 2007] by other methods.

The following lemma is critical for the results in the next section. Let $\iota : \mathcal{Q} \to \mathbb{F}_p^\times$ be the trivial linear character, $\iota(\gamma) = 1$ for all γ in $\mathcal{Q}$. Then $\hat{p}_\iota = [1, \dots, 1] = \pi$, the generator of $\mathcal{P}$.

Lemma 2.2. *Let χ_1 and χ_2 be distinct nontrivial linear characters of $\mathcal{Q}$. Then $\langle \hat{p}_{\chi_1}, \hat{p}_{\chi_2} \rangle$ cannot contain $\hat{p}_\iota$.*

Proof. If $\hat{p}_\iota = r\hat{p}_{\chi_1} + s\hat{p}_{\chi_2}$, then for all γ in $\mathcal{Q}$ we have

$$1 = r\chi_1(\gamma) + s\chi_2(\gamma).$$

Hence

$$m = r\sum_{\gamma \in \mathcal{Q}} \chi_1(\gamma) + s\sum_{\gamma \in \mathcal{Q}} \chi_2(\gamma). \tag{1}$$

But for $i = 1, 2$, if $T_i = \chi_i(\mathcal{Q}) \subset \mathbb{F}_p^\times$, then

$$\sum_{\gamma \in \mathcal{Q}} \chi_i(\gamma)$$

is $[\mathbb{F}_p^\times : T_i]$ times the sum of the elements of T_i. Since $\mathbb{F}_p^\times$ is a cyclic group, T_i is a cyclic subgroup of $\mathbb{F}_p^\times$, hence elements of T_i sum to $0 \pmod p$. So (1) becomes $m = 0 \pmod p$. Thus it is impossible for $\hat{p}_\iota = r\hat{p}_{\chi_1} + s\hat{p}_{\chi_2}$. □

3. The main theorem

Let N be a regular subgroup of $B = \mathrm{Perm}(\Gamma)$. Let $\lambda(\Gamma) = \mathcal{P} \cdot \mathcal{Q}$ where $\mathcal{P}$ is the p-Sylow subgroup of $\lambda(\Gamma)$. Our main theorem, Theorem 3.5, is

$$N \text{ is a subgroup of } \mathrm{Norm}_B(\mathcal{P}).$$

As we'll see in Theorem 3.7, $\mathrm{Norm}_B(\mathcal{P})$ can be viewed as a subgroup of the affine group of $\mathbb{F}_p^m$ generated by scalar matrices, permutation matrices, and $\mathbb{F}_p^m$. So this result reduces the question of determining regular subgroups of $\mathrm{Perm}(\Gamma) \cong S_{mp}$ to a question about subgroups of a much smaller group, a semidirect product of S_m with a metabelian group.

We begin by studying $\mathrm{Norm}_B(N)$, for N a regular subgroup of $B = \mathrm{Perm}(\Gamma)$.

Recall that the normalizer $\mathrm{Norm}_B(\lambda(\Gamma))$ in $\mathrm{Perm}\,\Gamma$ of $\lambda(\Gamma)$ is denoted by $\mathrm{Hol}\,\Gamma$ and is the group $\mathrm{Hol}(\Gamma) = \rho(\Gamma) \rtimes \mathrm{Aut}(\Gamma) \cong \Gamma \rtimes \mathrm{Aut}(\Gamma)$, where ρ is the right regular representation of Γ in $\mathrm{Perm}\,\Gamma$ and $\mathrm{Aut}\,\Gamma$ is embedded inside $\mathrm{Perm}\,\Gamma$ in the natural way. Since $\mathrm{Perm}(\Gamma) \cong \mathrm{Perm}(N)$ if N is a regular subgroup of $\mathrm{Perm}\,\Gamma$, we have:

Proposition 3.1. *Let N be a regular subgroup of $B = \mathrm{Perm}(\Gamma)$. Then*

$$\mathrm{Norm}_B(N) \cong \mathrm{Hol}(N).$$

Proof. Since N is regular in $\mathrm{Perm}\,\Gamma$, the map $b : N \to \Gamma$ by $b(\eta) = \eta(1)$ is a bijection. So $C(b^{-1}) : \mathrm{Perm}(\Gamma) \to \mathrm{Perm}(N)$, given by $C(b^{-1})(\pi) = b^{-1}\pi b$, is an isomorphism. Under this map, η in $N \subset \mathrm{Perm}(\Gamma)$ maps to $b^{-1}\eta b$, where for μ in N,

$$b^{-1}\eta b(\mu) = b^{-1}\eta(\mu(1)) = b^{-1}(\eta\mu(1)) = \eta\mu.$$

Thus inside $\mathrm{Perm}\,N$, the image $C(b^{-1})(N) = \lambda(N)$, and so

$$C(b^{-1})(\mathrm{Norm}_B(N)) = \mathrm{Norm}_{\mathrm{Perm}(N)}(\lambda(N)) \cong N \rtimes \mathrm{Aut}(N).$$

Since $C(b^{-1})$ is an isomorphism from $\mathrm{Perm}\,\Gamma$ to $\mathrm{Perm}\,N$, $C(b^{-1})$ is an isomorphism from $\mathrm{Norm}_B(N)$ to $\mathrm{Hol}(N) \cong N \rtimes \mathrm{Aut}(N)$. □

In order to obtain Theorem 3.5, we need to introduce the *opposite group*, $N^{\mathrm{opp}} = \mathrm{Cent}_B(N)$, the centralizer of N in $B = \mathrm{Perm}(\Gamma)$. We denote by 1 the identity element of the set Γ on which B acts. The following is a recapitulation of [Greither and Pareigis 1987, Lemma 2.4.2].

Lemma 3.2. *For N a regular subgroup of $B = \mathrm{Perm}(\Gamma)$, let ϕ be in $\mathrm{Cent}_B(N)$. Then $\phi(\gamma) = \eta_\gamma\phi(1)$, where η_γ is the unique element η of N such that $\eta(1) = \gamma$. Conversely, if ϕ is in B and $\phi(\gamma) = \eta_\gamma\phi(1)$ for all γ, then ϕ is in $\mathrm{Cent}_B(N)$.*

Proof. For ϕ in $\mathrm{Cent}_B(N)$, $\phi(\gamma) = \phi(\eta_\gamma(1)) = \eta_\gamma\phi(1)$. Let $\phi(1) = \sigma(1)$ for unique σ in N. Then ϕ is uniquely determined by σ: denote that ϕ by ϕ_σ. Thus $\phi_\sigma(\gamma) = \eta_\gamma\sigma(1)$.

Conversely, suppose ϕ is in B and there is some σ in N such that $\phi(\gamma) = \eta_\gamma\sigma(1)$ for all γ, so that $\phi = \phi_\sigma$. Then ϕ_σ is in $\mathrm{Cent}_B(N)$. Indeed,

$$\phi_\sigma\eta_\epsilon(\gamma) = \phi_\sigma\eta_{\eta_\epsilon}(\gamma) = \eta_{\eta_\epsilon}(\gamma)\sigma(1),$$

while

$$\eta_\epsilon\phi_\sigma(\gamma) = \eta_\epsilon\eta_\gamma\sigma(1).$$

We claim that $\eta_{\eta_\epsilon(\gamma)} = \eta_\epsilon\eta_\gamma$. Since elements η of N bijectively correspond with their images $\eta(1)$ in Γ, it suffices to observe that

$$\eta_{\eta_\epsilon(\gamma)}(1) = \eta_\epsilon(\gamma) = \eta_\epsilon(\eta_\gamma(1)) = (\eta_\epsilon\eta_\gamma)(1).$$

Thus $\mathrm{Cent}_B(N) = \{\phi_\sigma : \sigma \in N\}$. □

Corollary 3.3. *Let N be a regular subgroup of $\mathrm{Perm}\,\Gamma$. Then:*

(a) *N^{opp} is also a regular subgroup of $\mathrm{Perm}\,\Gamma$.*

(b) *$N \cap N^{\mathrm{opp}} = Z(N)$, the center of N.*

(c) *If N is abelian, then $N = N^{\mathrm{opp}}$.*

(d) $(N^{\mathrm{opp}})^{\mathrm{opp}} = N$.

Proof. (a) Observe that for σ in N, $\phi_\sigma(1) = \eta_1\sigma(1)$. But η_1 is the unique element of N that maps 1 to 1 in Γ, hence η_1 is the identity element of N. Thus $\phi_\sigma(1) = \sigma(1)$. Thus if N is regular, then so is N^{opp}.

(b), and hence (c), are clear since $N^{\mathrm{opp}} = \mathrm{Cent}_B(N)$.

(d) Clearly N is contained in the centralizer of $\mathrm{Cent}_B(N)$, so is in $(N^{\mathrm{opp}})^{\mathrm{opp}}$. But by (a), this last group is regular; hence it has the same cardinality as N. So $N = (N^{\mathrm{opp}})^{\mathrm{opp}}$. □

Proposition 3.4. $\mathrm{Norm}_B(N) = \mathrm{Norm}_B(N^{\mathrm{opp}})$. *Hence N is normalized by $\lambda(\Gamma)$ if and only if N^{opp} is normalized by $\lambda(\Gamma)$.*

Proof. We show that $N^{\mathrm{opp}} = \mathrm{Cent}_B(N)$ is a normal subgroup of $\mathrm{Norm}_B(N)$. Let α be in $\mathrm{Cent}_B(N)$, δ in $\mathrm{Norm}_B(N)$. We show $\delta\alpha\delta^{-1}$ is in $\mathrm{Cent}_B(N)$. Since every element η of N has the form $\delta\sigma\delta^{-1}$ for some σ in N and $\alpha\sigma = \sigma\alpha$, we have

$$\begin{aligned}\delta\alpha\delta^{-1}\eta &= \delta\alpha\delta^{-1}(\delta\sigma\delta^{-1}) = \delta\alpha\sigma\delta^{-1}\\ &= \delta\sigma\alpha\delta^{-1} = \delta\sigma\delta^{-1}\delta\alpha\delta^{-1} = \eta\delta\alpha\delta^{-1}.\end{aligned}$$

Thus $\delta\alpha\delta^{-1}$ is in $\mathrm{Cent}_B(N)$, and so N^{opp} is a normal subgroup of $\mathrm{Norm}_B(N)$. Hence

$$\mathrm{Norm}_B(N) \subset \mathrm{Norm}_B(N^{\mathrm{opp}}).$$

The same is true replacing N by N^{opp}. Equality then follows by part (d) of Corollary 3.3. The last sentence follows easily from the equality $\mathrm{Norm}_B(N) = \mathrm{Norm}_B(N^{\mathrm{opp}})$. □

Now we can prove the main theorem.

Theorem 3.5. *Let N be a regular subgroup of $B = \mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma) = \mathcal{P}\cdot\mathcal{Q}$, with $\mathcal{P}$ the p-Sylow subgroup of $\lambda(\Gamma)$. Then N is a subgroup of $\mathrm{Norm}_B(\mathcal{P})$.*

Proof. Since $\lambda(\Gamma)$ is contained in $\mathrm{Norm}_B(N)$, we have $\mathcal{P}$ inside $\mathrm{Norm}_B(N) = \mathrm{Norm}_B(N^{\mathrm{opp}})$.

Since $\mathrm{Norm}_B(N) \cong \mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$, we know by Proposition 1.2 what the p-Sylow subgroup of $\mathrm{Norm}_B(N)$ is:

- If $N = P(N) \times Q(N)$, then the p-Sylow subgroup of $\mathrm{Norm}_B(N)$ is $P(N)$, which is unique and has order p. Hence $\mathcal{P} = P(N) = P(N^{\mathrm{opp}})$.

- If $N = P(N) \rtimes_\tau Q(N)$ where τ is nontrivial, then $\mathrm{Norm}_B(N) \cong \mathrm{Hol}(N) \cong N \rtimes \mathrm{Aut}(N)$ has a p-Sylow subgroup isomorphic to $C_p \times C_p$, where one copy of C_p is $P(N)$ and the other copy is the group $C(P(N))$ of inner automorphisms of N obtained by conjugation by the elements of $P(N)$ (see Lemma 1.1). We check that the subgroup $P(N)\cdot C(P(N))$ is normal in $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$. Take $\sigma, \tau \in P$, $h \in G$, $\alpha \in \mathrm{Aut}\, G$. Then

$$(\alpha(h)^{-1}\alpha)(h\alpha^{-1}) = 1,$$

so conjugating an element $\sigma C(\tau)$ of $P(N)\cdot C(P(N))$ by $(h\alpha^{-1})^{-1}$ yields:

$$\begin{aligned}(\alpha(h)^{-1}\alpha)(\sigma C(\tau))(h\alpha^{-1}) &= \alpha(h)^{-1}\alpha(\sigma)\alpha(\tau h\tau^{-1})\cdot \alpha C(\tau)\alpha^{-1}\\ &= \alpha(h)^{-1}\alpha(\sigma)\alpha(\tau)\alpha(h)\alpha(\tau^{-1})\cdot C(\alpha(\tau))\\ &= C(\alpha(h)^{-1})(\alpha(\sigma\tau))\alpha(\tau^{-1})\cdot C(\alpha(\tau)).\end{aligned}$$

Since P is a characteristic subgroup of G, $C(\alpha(h)^{-1})(\alpha(\sigma\tau))$ is in P, as are $\alpha(\tau^{-1})$ and $\alpha(\tau)$. Hence $P(N)\cdot C(P(N))$ is a normal subgroup of $\mathrm{Hol}\, N$, hence is the unique p-Sylow subgroup of $\mathrm{Hol}\, N$.

Since N in this case is nonabelian, $Z(N)$ has no p-torsion, and so since $N \cap N^{\mathrm{opp}} = Z(N)$, $P(N) \cap P(N^{\mathrm{opp}}) = (1)$. Since $P(N)$ and $P(N^{\mathrm{opp}})$ centralize each other, $P(N)\cdot P(N^{\mathrm{opp}}) \cong C_p \times C_p$, and hence $P(N)\cdot P(N^{\mathrm{opp}})$ is the p-Sylow subgroup of $\mathrm{Hol}(N) = \mathrm{Norm}_B(N)$.

Now we identify $\mathcal{P}$, the p-Sylow subgroup of $\lambda(\Gamma)$, inside $\mathrm{Norm}_B(N)$. Clearly, $\mathcal{P} \subset P(N)\cdot P(N^{\mathrm{opp}})$. The groups $\mathcal{P}$, $P(N)$, and $P(N^{\mathrm{opp}})$ are order-p semiregular subgroups of $\mathrm{Perm}\,\Gamma$ normalized by $\lambda(\Gamma)$; hence they have generators $\hat{p}_\iota$, $\hat{p}_{\chi_1}$, and $\hat{p}_{\chi_2}$ that correspond to linear characters ι, χ_1, and χ_2 from $\mathcal{Q} = Q(\lambda(\Gamma))$ to $\mathbb{F}_p^\times$, where ι, corresponding to $\mathcal{P}$, is the trivial character. Since $P(N)$ and $P(N^{\mathrm{opp}})$ are distinct subgroups, χ_1 and χ_2 are distinct characters. Since $\mathcal{P}$ is contained in $P(N)\cdot P(N^{\mathrm{opp}})$, we have

$$\iota = r\chi_1 + s\chi_2,$$

for some integers r and s. But by Lemma 2.2, this can only occur if χ_1 or χ_2 is the trivial character, that is, $\mathcal{P} = P(N)$ or $\mathcal{P} = P(N^{\mathrm{opp}})$.

If $\mathcal{P} = P(N^{\mathrm{opp}})$, then N centralizes $\mathcal{P}$, so N is contained in $\mathrm{Norm}_B(\mathcal{P})$.

If $\mathcal{P} = P(N)$, then N normalizes $P(N) = \mathcal{P}$, so N is contained in $\mathrm{Norm}_B(\mathcal{P})$. □

Definition. For groups Γ and M of order mp and P an order-p semiregular subgroup of $\mathrm{Norm}_B(\mathcal{P})$ that is normalized by $\mathrm{Norm}_B(\mathcal{P})$ (see Theorem 2.1), let $R(\Gamma, [M]; P)$ be the set of regular subgroups N of $\mathrm{Norm}_B(\mathcal{P})$ isomorphic to M and normalized by $\lambda(\Gamma)$ such that $P(N) = P$.

Then $R(G, [M])$ is the disjoint union of $R(\Gamma, [M]; P)$ for P running through all order-p semiregular subgroups of $\mathrm{Norm}_B(\mathcal{P})$.

To count $R(G, [M])$, we combine Proposition 3.4 with the proof of Theorem 3.5:

Corollary 3.6. *With Γ and M as above, let $\mathcal{P} = P(\lambda(\Gamma))$, the p-Sylow subgroup of $\lambda(\Gamma)$.*

If $M = P(N) \times Q(N)$, then $R(\Gamma, [M]) = R(\Gamma, [M]; \mathcal{P})$.
If M is a nontrivial semidirect product of $P(N)$ and $Q(N)$, then

$$|R(G, [M])| = 2|R(G, [M]; \mathcal{P})|.$$

Proof. Lemma 1.1 showed that if N is the direct product of $P(N)$ and $Q(N)$, then $\mathcal{P}$ is the unique order-p subgroup of $\mathrm{Norm}_B(\mathcal{P})$, hence $P(N) = \mathcal{P}$ for all regular subgroups of $\mathrm{Norm}_B(\mathcal{P})$ normalized by $\lambda(\Gamma)$. Otherwise, N and N^{opp} are regular subgroups of $\mathrm{Perm}\,\Gamma$ normalized by $\lambda(\Gamma)$ such that $P(N)$ and $P(N^{\mathrm{opp}})$ are distinct subgroups of $\mathrm{Norm}_B(\mathcal{P})$, and as observed at the end of the proof of Theorem 3.5, exactly one of $P(N)$ and $P(N^{\mathrm{opp}})$ is equal to $\mathcal{P}$. Thus when M is a nontrivial semidirect product, counting $R(\Gamma, [M]; \mathcal{P})$ counts half of the set $R(\Gamma, [M])$. $\square$

Now we identify $\mathrm{Norm}_B(\mathcal{P})$ as a semidirect product and as a subgroup of the affine group of $\mathbb{F}_p^m$. The first description makes computing regular subgroups of $\mathrm{Norm}_B(\mathcal{P})$ feasible in many cases.

Theorem 3.7. *Let $\lambda(\Gamma) = \mathcal{P}\mathcal{Q}$, where $\mathcal{P} = \langle \pi \rangle$, $\pi = \pi_1\pi_2 \cdots \pi_m$, a product of disjoint p-cycles in $B = \mathrm{Perm}(\Gamma)$. Let $V = \langle \pi_1, \dots, \pi_m \rangle \cong \mathbb{F}_p^m$, as before. Then* $\mathrm{Norm}_B(\mathcal{P}) \cong \mathbb{F}_p^m \rtimes (\mathbb{F}_p^\times \cdot S_m)$ *and embeds in*

$$\mathrm{AGL}_m(\mathbb{F}_p) = \left\{ \begin{pmatrix} A & \hat{v} \\ 0 & 1 \end{pmatrix} : A \in \mathrm{GL}_m(\mathbb{F}_p),\, \hat{v} \in \mathbb{F}_p^m \right\},$$

the affine group of $\mathbb{F}_p^m$.

Proof. We first show that $\mathrm{Norm}_B(\mathcal{P}) \cong \mathbb{F}_p^m \rtimes (\mathbb{F}_p^\times \cdot S_m)$.

Given an element τ of $\mathrm{Norm}_B(\mathcal{P})$, $\tau\pi\tau^{-1} = \pi^{c(\tau)}$, and so τ induces a permutation, denoted by t_τ, of the set $\{1, 2, \dots, m\}$ by

$$\tau\pi_j\tau^{-1} = \pi_{t_\tau(i)}^{c(\tau)}.$$

This defines homomorphisms $c : \mathrm{Norm}_B(\mathcal{P}) \to \mathbb{F}_p^\times$, $t : \mathrm{Norm}_B(\mathcal{P}) \to S_m$, and $\phi : \mathrm{Norm}_B(\mathcal{P}) \to \mathbb{F}_p^\times \cdot S_m$ by $\phi(\tau) = (c(\tau), t(\tau))$. The kernel $\ker\phi$ of ϕ is the set of elements τ in $\mathrm{Norm}_B(\mathcal{P})$ such that $\tau\pi_j\tau^{-1} = \pi_j$ for all j, that is, the centralizer of V. We show that $\ker\phi = V$.

For $i = 1, \dots, m$, choose γ_i in $\Pi_i = \mathrm{Supp}(\pi_i)$. Then π_i is the p-cycle

$$\pi = (\gamma_i, \pi(\gamma_i), \dots, \pi^{p-1}(\gamma_i)),$$

hence

$$\Gamma = \{\pi_i^k(\gamma_i) \mid i = 1, \dots, m, k = 0, \dots, p-1\}.$$

If τ in $\mathrm{Perm}\,\Gamma$ centralizes π_i, then since

$$\tau\pi_i\tau^{-1} = \big(\tau(\gamma_i), \tau(\pi(\gamma_i)), \dots, \tau(\pi^{p-1}(\gamma_i))\big) = \pi_i,$$

τ conjugates $\mathrm{Supp}(\pi_i) = \Pi_i$ to itself, and hence yields a permutation of the set Π_i. But the only permutations in $S_p = \mathrm{Perm}(\Pi_i)$ that centralize the p-cycle π_i are the powers of π_i. Thus τ commutes with π_i for all $i = 1, \dots, m$ if and only if τ is in V. Therefore $V = \ker \phi$ and we have a short exact sequence:

$$1 \to V \to \mathrm{Norm}_B(\mathcal{P}) \to \mathbb{F}_p^\times \cdot S_m \to 1.$$

The sequence splits. For inside $\mathrm{Norm}_B(\mathcal{P})$ are the permutations σ_c for c in $\mathbb{F}_p^\times$ induced by the c-th power map $\pi \mapsto \pi^c$, for $(c, p) = 1$, that take $\pi_i^k(\gamma_i)$ to $\pi_i^{ck}(\gamma_i)$ for all $i = 1, \dots, m$ and $k = 0, \dots, p-1$. The σ_c generate a subgroup $\mathcal{U}$ of $\mathrm{Norm}_B(\mathcal{P})$ isomorphic to $\mathbb{F}_p^\times$. Also, a permutation $\bar{\alpha}$ of S_m defines a permutation α of $\mathrm{Perm}\,\Gamma$ by

$$\alpha(\pi_i^k(\gamma_i)) = \pi_{\bar{\alpha}(i)}^k(\gamma_{\bar{\alpha}(i)}).$$

Then $\{\alpha \in \mathrm{Perm}(\Gamma) : \bar{\alpha} \in S_m\}$ is a subgroup $\mathcal{S}$ of $\mathrm{Norm}_B(\mathcal{P})$ isomorphic to S_m. Clearly $\mathcal{S}$ and $\mathcal{U}$ centralize each other, so the group $\mathcal{S}\mathcal{U} \subset \mathrm{Norm}_B(\mathcal{P})$ is a preimage of $\mathbb{F}_p^\times \cdot S_m$ under ϕ. So ϕ splits, and $\mathrm{Norm}_B(\mathcal{P}) = V \cdot (\mathcal{U}\mathcal{S}) \cong \mathbb{F}_p^m \rtimes (\mathbb{F}_p^\times \cdot S_m)$.

A convenient way to view $\mathbb{F}_p^m \rtimes (\mathbb{F}_p^\times \cdot S_m)$ is as the subgroup of $\mathrm{AGL}_m(\mathbb{F}_p)$ consisting of matrices

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix},$$

where $v \in V = \mathbb{F}_p^m$, and A in $\mathrm{GL}_m(\mathbb{F}_p)$ is a nonzero scalar multiple of a permutation matrix. In other words, we view S_m as $m \times m$ permutation matrices of the components of $\mathbb{F}_p^m$ and $\mathbb{F}_p^\times$ as nonzero scalar multiples (in $\mathbb{F}_p$) of the $m \times m$ identity matrix. Such matrices are examples of monomial matrices, whose properties in general are explored by various authors such as Ore [1942]. $\square$

In the sequel we will need to understand $\mathrm{Norm}_B(\mathcal{P})$ as a subgroup of $B = \mathrm{Perm}(\Gamma)$. Writing the elements of $\mathrm{Norm}_B(\mathcal{P}) = V \cdot (\mathcal{U}\mathcal{S})$ as $(\hat{a}, u^r, \alpha)$, the explicit action of elements of $\mathrm{Norm}_B(\mathcal{P})$ on $\Gamma = \{\pi_i^k(\gamma_i) \mid i = 1, \dots, m, k = 0, \dots, p-1\}$ is given by

$$(\hat{a}, u^r, \alpha)(\pi_i^k(\gamma_i)) = \pi_1^{a_1} \cdots \pi_m^{a_m}(\pi_{\alpha(i)}^{ku^r}(\gamma_{\alpha(i)})) = \pi_{\alpha(i)}^{ku^r + a_{\alpha(i)}}(\gamma_{\alpha(i)}).$$

Then we have the following easily verified formulas:

$$(\hat{a}, u^r, \alpha)^k = \left(\sum_{i=0}^{k-1} u^{ir}\alpha^r(\hat{a}),\ u^{rk},\ \alpha^k\right). \tag{2}$$

The inverse of $(\hat{b}, u^s, \beta)$ is $(-u^{-s}\beta^{-1}(\hat{b}), u^{-s}, \beta^{-1})$, so

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

In particular, elements of $\mathrm{Norm}_B(\mathcal{P})$ act on $\mathcal{P}$ by:

$$(\hat{b}, u^s, \beta)(\hat{p}_\iota, 1, I)(\hat{b}, u^s, \beta)^{-1} = (u^s \hat{p}_\iota, 1, I).$$

Let N be a regular subgroup of $\mathrm{Perm}\,\Gamma$ normalized by $\lambda(\Gamma)$ and recall that $N = P(N)Q(N)$ where $P(N)$ is the p-Sylow subgroup of N and $Q(N)$ is a group of order m. We know that $N \subset \mathrm{Norm}_B(\mathcal{P})$ and that $P(N) = \langle(\hat{p}_\chi, 1, I)\rangle$ for some linear character from $\mathfrak{Q} = Q(\lambda(\Gamma))$ to $\mathbb{F}_p^\times$. We need to examine $Q(N)$.

Now N is a regular subgroup of $\mathrm{Perm}\,\Gamma$, so $Q(N)$ acts fixed-point-freely on Γ. We need to identify fixed-point-free elements of $\mathrm{Norm}_B(\mathcal{P})$.

Proposition 3.8. *If the order of* $(\hat{a}, u^r, \alpha) \neq 1$ *in* $\mathrm{Norm}_B(\mathcal{P})$ *is coprime to* p, *then* $(\hat{a}, u^r, \alpha)$ *is fixed-point free on* Γ *if and only if* α *is fixed-point free in* S_m.

Proof. Suppose α is fixed-point free in S_m. Then for all i, $1 \le i \le m$, $\alpha(i) \neq i$, so $(\hat{a}, u^r, \alpha)(\pi_i^k(\gamma_i))$ is in $\Pi_{\alpha(i)} \neq \Pi_i$. So $(\hat{a}, u^r, \alpha)$ is fixed-point free.

Suppose $\alpha(i) = i$ for some i. Then

$$(\hat{a}, u^r, \alpha)(\pi_i^k(\gamma_i)) = \pi_i^{u^r k + a_i} = \pi_i^k,$$

for k satisfying $(1-u^r)k \equiv a_i \pmod{p}$. If $u^r \neq 1$, then such a k exists, so $(\hat{a}, u^r, \alpha)$ has a fixed point whenever α has a fixed point and $u^r \neq 1$.

If $\alpha(i) = i$ and $u^r = 1$, then

$$(\hat{a}, 1, \alpha)^s(\pi_i^k(\gamma_i)) = \pi_i^{k+a_i s}(\gamma_i),$$

for all s. If s is the order of $(\hat{a}, 1, \alpha)$, then $\pi_i^{k+a_i s}(\gamma_i) = \pi_i^k(\gamma_i)$, so $a_i s \equiv 0 \pmod{p}$. If s and p are coprime, then $a_i = 0$. But then $\pi_i^k(\gamma_i)$ is a fixed point for $(\hat{a}, 1, \alpha)$. □

Let $t : \mathrm{Norm}_B(\mathcal{P}) \to S_m$ be the map sending $(\hat{a}, u^r, \alpha)$ to $\bar{\alpha}$ in S_m defined by $\alpha(\pi_i^k(\gamma_i)) = \pi_{\bar{\alpha}(i)}^k(\gamma_{\bar{\alpha}(i)})$. Proposition 3.8 implies immediately:

Corollary 3.9. *Let* Q *be a subgroup of* $\mathrm{Norm}_B(\mathcal{P})$ *of order* m, *and suppose* $t : \mathrm{Norm}_B(\mathcal{P}) \to S_m$ *is one-to-one on* Q. *Then* Q *is fixed-point free on* Γ, *hence a semiregular subgroup of* $\mathrm{Norm}_B(\mathcal{P})$, *if and only if* $t(Q)$ *is a regular subgroup of* S_m.

Corollary 3.10. *If* N *is a regular subgroup of* $\mathrm{Norm}_B(\mathcal{P})$, *then* $t(Q(N^{\mathrm{opp}})) = (t(Q(N)))^{\mathrm{opp}}$, *where the right-hand group is viewed within* $\mathcal{S} \cong S_m$.

Proof. For $(\hat{a}, u^r, \alpha)$ in $Q(N)$ and $(\hat{c}, u^s, \delta)$ in $Q(N^{\mathrm{opp}})$, we have $\alpha\delta = \delta\alpha$, so $t(\hat{a}, u^r, \alpha) = \bar{\alpha}$ and $t(\hat{c}, u^s, \delta) = \bar{\delta}$ commute in S_m. So $t(Q(N^{\mathrm{opp}})) \subset (t(Q(N)))^{\mathrm{opp}}$. But because $Q(N)$ is regular in S_m, both sides have cardinality m. Hence the two groups are equal. □

It is interesting to observe that $\mathrm{Cent}_B(\mathcal{P})$ consists precisely of those elements of the form $(\hat{b}, 1, \beta)$, which is consistent with the classical fact (due to Burnside [1911, §170]) that $\mathrm{Cent}_B(\mathcal{P})$ is isomorphic to the wreath product $C_p \wr S_m$. This wreath product is isomorphic to the semidirect product $(C_p \times \cdots \times C_p) \rtimes S_m$ where the action of S_m on the m-fold product of the C_p's is given by the natural action on the coordinates. The group $\mathrm{Norm}_B(\mathcal{P})$ is also not unknown. It is an example of a *twisted* wreath product whose precise definition (which may be found in [Neumann 1963]) is not so important here since we have the semidirect product description given above. The appearance of wreath products, by the way, is a natural consequence of the action of $\mathrm{Norm}_B(\mathcal{P})$ (as well as any other subgroups thereof, such as $\mathrm{Cent}_B(\mathcal{P})$) on the blocks $\{\Pi_1, \ldots, \Pi_m\}$. We may, in fact, frame part of Theorem 3.5 in terms of one of the important consequences of the so-called universal embedding theorem of Krasner and Kaloujnine [1951]. Specifically, if one has an exact sequence $1 \to P \to N \to Q \to 1$, expressing N as an extension of P by Q, then $P \wr Q$ contains a subgroup isomorphic to N. In the setting of this work, where $|N| = |P| \cdot |Q| = pm$ our group Q may, of course, be embedded as a subgroup of S_m. As such we have an embedding of N into $P \wr S_m$. This dovetails with the above observation that $\mathrm{Cent}_B(\mathcal{P}) \cong C_p \wr S_m$ since, for a given $N \in R(\Gamma, [M])$, either N or N^{opp} centralizes $\mathcal{P}$ and $N \cong N^{\mathrm{opp}}$ so that indeed $\mathrm{Cent}_B(\mathcal{P})$ contains a subgroup isomorphic to N. One of the upshots of Corollary 3.6, in fact, is that either all $N \in R(\Gamma, [M])$ are subgroups of $\mathrm{Cent}_B(\mathcal{P})$ (when $P(N)$ is a direct factor) or (when $P(N)$ is not a direct factor) exactly half of the elements centralize $\mathcal{P}$, indeed all those for which $P(N) \neq \mathcal{P}$. As such, one *could* enumerate only those N that lie in $\mathrm{Cent}_B(\mathcal{P})$ and then apply Corollary 3.6 in order to determine $|R(\Gamma, [M])|$.

What the affine representation above yields for us is a very concrete way of performing the enumeration of these subgroups of $\mathrm{Norm}_B(\mathcal{P})$.

In order to apply Theorem 3.5 to deal with all possible Γ and all possible N of a given order mp, it is convenient to apply the following (in the author's opinion quite important) observation:

Proposition 3.11 [Dixon 1971, Lemma 1]. *If N and N' are regular subgroups of S_n that are isomorphic as abstract groups, they are conjugate as subgroups of S_n.*

Proof. Identify $S_n = \mathrm{Perm}(Z/nZ) = \mathrm{Perm}(C_n)$. Let $\phi : N \to N'$ be an isomorphism. Then the conjugation map $C(\phi) : \mathrm{Perm}(N) \to \mathrm{Perm}(N')$ is an isomorphism, under which $\lambda(N)$ maps to $\lambda(N')$, as is easily verified. If $b : N \to C_n$ and $c : N' \to C_n$ are bijections, then $C(b^{-1}) : \mathrm{Perm}(C_n) \to \mathrm{Perm}(N)$ maps N in $\mathrm{Perm}\, C_n$ to $\lambda(N)$ in $\mathrm{Perm}\, N$, and $C(c^{-1}) : \mathrm{Perm}(C_n) \to \mathrm{Perm}(N')$ maps N' in $\mathrm{Perm}\, C_n$ to $\lambda(N')$. The composition $C(c^{-1})C(\phi)C(b) = C(c^{-1} \circ \phi \circ b)$ maps N in $\mathrm{Perm}\, C_n$ to N' in $\mathrm{Perm}\, C_n$. □

This result allows us to determine $R(\Gamma, [M])$, for all pairings of groups of order mp, while working entirely within the single group $B = S_{mp}$.

Here is an outline of the strategy.

Let $B = S_{mp}$.

Suppose that $\mathcal{P} = \langle \pi \rangle$ is a cyclic semiregular subgroup of B of order p and that $\pi = \pi_1 \cdot \pi_2 \cdot \dots \cdot \pi_m$, where $\pi_1, \dots, \pi_m$ are disjoint p-cycles. We may choose $\mathcal{P}$ at our convenience.

Let $\mathfrak{Q}_1, \dots, \mathfrak{Q}_s$ be subgroups of $\mathrm{Norm}_B(\mathcal{P})$ that act regularly on the set $\{\Pi_1, \dots, \Pi_m\}$, where $\Pi_i = \mathrm{Supp}(\pi_i)$, and represent all isomorphism classes of groups of order m.

For each $\mathfrak{Q}_i$, find the $\mathbb{F}_p$-linear characters χ_{ij} of $\mathfrak{Q}_i$. Then $\langle \hat{p}_{\chi_{ij}} \rangle$ is normalized by $\mathfrak{Q}_i$, so, as we shall show below, $\langle \hat{p}_{\chi_{ij}} \rangle \mathfrak{Q}_i$ is a regular subgroup of S_{mp} and is contained in $\mathrm{Norm}_B(\mathcal{P})$. If $\langle \hat{p}_{\chi_{ij}} \rangle \mathfrak{Q}_i$ is a direct product or χ_{ij} is not the trivial character, we find $(\langle \hat{p}_{\chi_{ij}} \rangle \mathfrak{Q}_i)^{\mathrm{opp}}$ in S_{mp}. Then $(\langle \hat{p}_{\chi_{ij}} \rangle \mathfrak{Q}_i)^{\mathrm{opp}}$ is contained in $\mathrm{Norm}_B(\mathcal{P})$ and its p-Sylow subgroup is $\mathcal{P}$. We represent the isomorphism types of groups Γ by suitable groups $(\langle \hat{p}_{\chi_{ij}} \rangle \mathfrak{Q}_i)^{\mathrm{opp}}$.

Having done so, we then seek to construct regular subgroups N normalized by Γ by looking for fixed-point-free elements in $\mathrm{Norm}_B(\mathcal{P})$ of suitable orders that are normalized by Γ.

In the next sections we demonstrate this program.

4. Groups of order pq

N. Byott [2004] determined the number of Hopf Galois structures on a Galois extension of fields L/K with Galois group Γ of order pq where p and q are primes and $p \equiv 1 \pmod q$. As Byott notes, the case where $p \not\equiv 1 \pmod q$ is of little interest because then pq and $\phi(pq)$ are coprime, in which case Byott [1996] shows that the only Hopf Galois structure on LK is the classical structure given by the Galois group Γ.

Let G_1 and G_2 be the two isomorphism types of groups of order pq. Byott's [2004] approach for counting Hopf Galois structures is to apply the strategy, suggested in [Childs 1989] and codified in [Byott 1996], of looking for regular subgroups isomorphic to G_i inside $\mathrm{Hol}(G_j) \cong G_j \rtimes \mathrm{Aut}(G_j)$ for $i, j = 1, 2$. Equivalence classes of such regular subgroups correspond to Hopf Galois structures on field extensions with Galois group G_i whose Hopf algebra has type G_j.

In this section we count the number of Hopf Galois structures on L/K with Galois group G_i whose Hopf algebra has type G_j by looking for regular subgroups G_j inside $\mathrm{Norm}_{\mathrm{Perm}(G_i)}(\mathcal{P}) \subset \mathrm{Perm}(G_i)$. Thus we obtain Byott's count by a refinement of the direct Greither–Pareigis approach. As may be observed, the two methods are rather different.

Let $\mathbb{F}_p^\times = \langle u \rangle$. The two groups of order pq are the cyclic group $C_{pq} \cong \mathbb{F}_p \times \langle u^d \rangle$ and the group $C_p \rtimes_\tau C_q = \mathbb{F}_p \rtimes \langle u^d \rangle$, where in $C_p \rtimes_\tau C_q$ we have $(0, u^d)(x, 1) = (u^d x, 1)(0, u^d)$ and $qd = p - 1$; hence u^d is an element of $\mathbb{F}_p^\times$ of order q.

The result is:

Theorem 4.1. *Let $R(\Gamma, [G])$ be the regular subgroups of* $\operatorname{Perm}\Gamma$ *isomorphic to G and normalized by $\lambda(\Gamma)$. Then*

$$\begin{aligned}|R(C_{pq}, [C_{pq}])| &= 1,\\ |R(C_{pq}, [C_p \rtimes_\tau C_q])| &= 2(q-1),\\ |R(C_p \rtimes_\tau C_q, [C_{pq}])| &= p,\\ |R(C_p \rtimes_\tau C_q, [C_p \rtimes_\tau C_q])| &= 2(1+p(q-2)).\end{aligned}$$

By [Greither and Pareigis 1987], in each case the right-hand side equals the number of Hopf Galois structures on a Galois extension of fields with Galois group Γ with Hopf algebra of type $[M]$.

Before doing the particular cases, we obtain some preliminary information that applies in all four cases. Also, some notational conventions will be used throughout the rest of the paper. In $\mathbb{F}_p^m$ we shall denote the vectors $[0, 0, \dots, 0]$ and $[1, 1, \dots, 1] = \hat{p}_\iota = \langle \pi \rangle$ (both of which are fixed by any $\alpha \in S_m$) by $\hat{0}$ and $\hat{1}$, respectively, and any scalar multiple $[c, c, \dots, c]$ of $\hat{1}$ shall be expressed as $c\hat{1}$. Also, an arbitrary $\hat{a} \in \mathbb{F}_p^m$ has the form $[a_1, a_2, \dots, a_m]$ for $a_i \in \mathbb{F}_p$.

Lemma 4.2. *Suppose*

$$G = \langle (\hat{1}, 1, I), (\hat{a}, u^r, \sigma) \rangle \subset \mathrm{Norm}_B(\mathcal{P}),$$

where $x = (\hat{1}, 1, I)$ and $y = (\hat{a}, u^r, \sigma)$ satisfy $x^p = y^q = 1$ and $yx = x^{u^d} y$ and σ is a nontrivial permutation of S_q. Then σ is a q-cycle in S_q and $u^r = u^d$.

Proof. If $(\hat{a}, u^r, \sigma)^q = (\hat{1}, 1, I)$, then $\sigma^q = 1$. Since σ is nontrivial, it must have order q, hence be a q-cycle since q is prime. From the defining relation

$$(\hat{a}, u^r, \sigma)(\hat{1}, 1, I) = (\hat{1}, 1, I)^{u^d} (\hat{a}, u^r, \sigma),$$

we have $\hat{a} + u^r \hat{1} = u^d \hat{1} + \hat{a}$, hence $u^r = u^d$. □

Lemma 4.3. *Suppose G is as in Lemma 4.2 and*

$$H = \langle (\hat{1}, 1, I), (\hat{b}, u^s, \alpha) \rangle \subset \mathrm{Norm}_B(\mathcal{P}),$$

with α a q-cycle. If H is normalized by G, then $\alpha = \sigma^t$ for some $t \in \mathbb{F}_p^\times$.

Proof. Since G normalizes H, G must conjugate the generator of H of order q to an element of H. Thus

$$(\hat{a}, u^r, \sigma)(\hat{b}, u^s, \alpha)(\hat{a}, u^r, \sigma)^{-1} = (\hat{1}, 1, I)^f (\hat{b}, u^s, \alpha)^e,$$

for some $f \in \mathbb{F}_p$ and $e \in \mathbb{F}_p^\times$. Looking at the rightmost components, we have

$$\sigma\alpha\sigma^{-1} = \alpha^e.$$

Since conjugation by the order-q element σ is an automorphism of the cyclic q group $\langle\alpha\rangle$, whose automorphism group has order $q-1$, conjugation by σ must be trivial on $\langle\alpha\rangle$. Hence $\alpha\sigma = \sigma\alpha$. Now α is the q-cycle

$$\alpha = (1, \alpha(1), \ldots, \alpha^r(1), \ldots).$$

So

$$\alpha = \sigma\alpha\sigma^{-1} = (\sigma(1), \sigma\alpha(1), \ldots, \sigma\alpha^r(1), \ldots).$$

If $\sigma(1) = \alpha^k(1)$ for $k \neq 0$, then for all $s > 0$,

$$\sigma(\alpha^s(1)) = \alpha^s\sigma(1) = \alpha^s\alpha^k(1) = \alpha^k(\alpha^s(1)).$$

Hence $\sigma = \alpha^k$. □

We outline the strategy of the proof of Theorem 4.1.

Given that

$$\Gamma = \langle(\hat{1}, 1, I), (\hat{0}, u^r, \sigma)\rangle, \quad N = \langle(\hat{1}, 1, I), (\hat{a}, u^s, \sigma^t)\rangle,$$

we know that $N \subset \mathrm{Norm}_B(\mathcal{P})$. The constraints on N arise from the requirements that, first, Γ normalizes N, and, second, $(\hat{a}, u^s, \sigma^t)$ has order q. Regarding the first constraint, conjugating $(\hat{a}, s^s, \sigma^t)$ by $(\hat{1}, 1, I)$ poses no constraint on N since

$$(\hat{1}, 1, I)(\hat{a}, u^s, \sigma^t) = ((1-u^s)\hat{1}, 1, I)(\hat{a}, u^s, \sigma^t) \in N.$$

But the condition

$$(\hat{0}, u^r, \sigma)(\hat{a}, u^s, \sigma^t)(\hat{0}, u^r, \sigma) \text{ is in } N \tag{3}$$

typically yields conditions on $\hat{a}$.

Now we do each case in turn.

$|R(C_{pq}, [C_{pq}])| = 1$. We identify $\Gamma = C_p \times C_q$ inside $\mathrm{Norm}_B(\mathcal{P})$ as

$$\Gamma = \langle(\hat{1}, 1, I), (0, 1, \sigma)\rangle,$$

where σ is a fixed q-cycle in S_q. Then, since $N \cong C_p \times C_q$, N must have the form

$$N = \langle(\hat{1}, 1, I), (\hat{a}, 1, \sigma^t)\rangle,$$

for some integer t modulo $p-1$ by Lemmas 4.2 and 4.3.

Since $Q(N)$ is characteristic in N, condition (3) becomes the condition that $(0, 1, \sigma)$ conjugates the generator $(\hat{a}, 1, \alpha)$ of $Q(N)$ to a power of itself:

$$(\hat{0}, 1, \sigma)(\hat{a}, 1, \sigma^t)(\hat{0}, 1, \sigma^{-1}) = (\hat{a}, 1, \sigma)^e,$$

for some integer e. Looking at the rightmost components shows that $e = 1$. Thus

$$N = \langle(\hat{1}, 1, I), (\hat{a}, 1, \sigma^t)\rangle,$$

and looking at the leftmost components yields that $\sigma(\hat{a}) = \hat{a}$, hence $\hat{a} = k\hat{1}$. Then

$$(k\hat{1}, 1, \sigma^t) = (\hat{1}, 1, I)^k(\hat{0}, 1, \sigma)^t$$

is in Γ. Hence $N = \Gamma$.

$|R(C_{pq}, [C_p \rtimes_\tau C_q])| = 2(q-1)$. Since $C_p \rtimes_\tau C_q$ is a nontrivial semidirect product, to count the regular subgroups N, by Corollary 3.6 we may restrict to those N such that $P(N) = \mathcal{P}$, hence $P(N) = \langle(\hat{1}, 1, I)\rangle$. Again, $\Gamma = \langle(\hat{1}, 1, I), (0, 1, \sigma)\rangle$. By Lemmas 4.2 and 4.3,

$$N = \langle(\hat{1}, 1, I), (\hat{a}, u^d, \sigma^t)\rangle,$$

where $(t, q) = 1$. We claim that $\hat{a} = \hat{0}$.

We first observe that we may replace the generator $(\hat{a}, u^d, \sigma^t)$ by $(\hat{a}, u^d, \sigma^t)(l\hat{1}, 1, I)$ for any l, and choose l so that $a_1 = 0$, where a_1 is the first component of $\hat{a} \in \mathbb{F}_p^q$. The normalization condition (3) becomes

$$(\hat{0}, 1, \sigma)(\hat{a}, u^d, \sigma^t)(\hat{0}, 1, \sigma^{-1}) = (f\hat{1}, 1, I)(\hat{a}, u^d, \sigma^t),$$

for some f. Looking at the leftmost components yields

$$\sigma(\hat{a}) = \hat{a} + f\hat{1}. \tag{4}$$

This equation implies that

$$a_{\sigma^{-1}(k)} = a_k + f,$$

for all k. In particular, since $a_1 = 0$, we have

$$a_{\sigma^{-n}(1)} = nf,$$

for all n.

Now we consider the condition that $(\hat{a}, u^d, \sigma^t)$ have order q. Looking at the leftmost components in $(\hat{0}, 1, I) = (\hat{a}, u^d, \sigma^t)^q$ yields

$$\hat{0} = \sum_{j=1}^{q-1} u^{dj}\sigma^{tj}(\hat{a}). \tag{5}$$

Since σ is a q-cycle, we may write

$$\hat{a} = [a_1, a_{\sigma(1)}, \ldots, a_{\sigma^r(1)}, \ldots, a_{\sigma^{q-1}(1)}]. \tag{6}$$

Now σ cyclically permutes the components of $\hat{a}$, so

$$\sigma(\hat{a}) = [a_{\sigma^{-1}(1)}, a_1, \ldots, a_{\sigma^{r-1}(1)}, \ldots, a_{\sigma^{q-2}(1)}]. \tag{7}$$

Thus looking at the first components of (5), we obtain

$$0 = \sum_{j=1}^{q-1} u^{dj} a_{\sigma^{-tj}(1)} = \sum_{j=1}^{q-1} u^{dj} tjf = tf \sum_{j=1}^{q-1} j u^{dj}. \tag{8}$$

Now for any indeterminate x, we have

$$\sum_{j=0}^{q-1} j x^j = x \frac{d}{dx}(1 + x + \cdots + x^q) = x \frac{d}{dx}\left(\frac{x^q - 1}{x - 1}\right) = x\left(\frac{q x^{q-1}}{x-1} - \frac{x^q - 1}{(x-1)^2}\right).$$

Setting $x = u^d$, the second term is $(u^{dq} - 1)/(u^d - 1)^2 = 0$, and so (8) becomes

$$0 = tfu^d \frac{qu^{d(q-1)}}{u^d - 1}. \tag{9}$$

Since $u^d \neq 1$ is a unit modulo p and $0 < t < q$, this equation only holds when $f = 0$. Hence $\hat{a} = \hat{0}$ and

$$N = \langle (\hat{1}, 1, I), (\hat{0}, u^d, \sigma^t) \rangle.$$

We have a distinct group N for each t coprime to q. Hence there are $q - 1$ regular subgroups of $\mathrm{Norm}_B(\mathcal{P})$ normalized by Γ such that $P(N) = \mathcal{P}$. By Corollary 3.6, $R(C_{pq}, [C_p \rtimes_\tau C_q]) = 2(q - 1)$.

$|R(C_p \rtimes_\tau C_q, [C_{pq}])| = p$. Let

$$\Gamma = C_p \rtimes_\tau C_q = \langle (\hat{1}, 0, I), (\hat{0}, u^d, \sigma) \rangle$$

and assume $P(N) = \mathcal{P}$. Then

$$N = \langle (\hat{1}, 1, I), (\hat{a}, 1, \sigma^t) \rangle,$$

for some $\hat{a}$ and some t coprime to q. Now Γ normalizes N, and $Q(N)$ is characteristic in N, so the normalization equation (3) becomes

$$(\hat{0}, u^d, \sigma)(\hat{a}, 1, \sigma^t)(\hat{0}, u^{-d}, \sigma^{-1}) = (\hat{a}, 1, \sigma^t).$$

Looking at the leftmost components gives

$$\sigma(\hat{a}) = u^{-d}\hat{a}.$$

Then

$$\sigma^k(\hat{a}) = u^{-dk}\hat{a},$$

hence

$$a_{\sigma^{-k}(1)} = u^{-dk} a_1,$$

for all k.

Thus $\hat{a}$ is uniquely determined by a_1, and, in fact, $\hat{a} = a_1\hat{p}_{\psi_d}$. So

$$N = \langle(\hat{1}, 1, I), (a_1\hat{p}_{\psi_d}, 1, \sigma^t)\rangle.$$

Now $\sigma(\hat{p}_{\psi_d}) = u^{-d}\hat{p}_{\psi_d}$ (see Lemma 5.2). So if $st \equiv 1 \pmod q$, then we may replace the generator $(a_1\hat{p}_{\psi_d}, 1, \sigma^t)$ by its s-th power:

$$(a_1\hat{p}_{\psi_d}, 1, \sigma^t)^s = \left(a_1\left(\frac{u^{-dst}-1}{u^{-dt}-1}\right)\hat{p}_{\psi_d}, 1, \sigma\right).$$

Since d and t are coprime to q, $((u^{-dst}-1)/(u^{-dt}-1))$ is a unit modulo q. The constraint that $(b_1\hat{p}_{\psi_d}, 1, \sigma)^q = (\hat{1}, 1, I)$ poses no further constraint, for the first component of $(b_1\hat{p}_{\psi_d}, 1, \sigma)^q$ is

$$\sum_{i=0}^{q-1}\sigma^i(b_1\hat{p}_{\psi_d}) = b_1\Big(\sum_{i=0}^{q-1}u^{-di}\Big)\hat{p}_{\psi_d} = b_1\left(\frac{u^{-dq}-1}{u^d-1}\right)\hat{p}_{\psi_d} = \hat{0}.$$

Thus we may choose a generator of $Q(N)$ to be $(b_1\hat{p}_{\psi_d}, 1, \sigma)$ for any b_1 modulo p, and the p choices for b_1 yield different N. Thus $R(C_p \rtimes_\tau C_q, [C_{pq}]) = p$.

$\boldsymbol{|R(C_p \rtimes_\tau C_q, [C_p \rtimes_\tau C_q])| = 2(1 + p(q-2))}$. Let

$$\Gamma = C_p \rtimes_\tau C_q = \langle(\hat{1}, 0, I), (\hat{0}, u^d, \sigma)\rangle$$

and assume $P(N) = \mathcal{P}$. Then we may assume that

$$N = \langle(\hat{1}, 1, I), (\hat{a}, u^d, \sigma^t)\rangle,$$

with $(t, q) = 1$. Constraint (3) is that conjugation by $(\hat{0}, u^d, \sigma)$ sends $(\hat{a}, u^d, \alpha)$ to an element of order q in N:

$$(\hat{0}, u^d, \sigma)(\hat{a}, u^d, \sigma^t)(\hat{0}, u^{-d}, \sigma^{-1}) = (\hat{a}, u^d, \sigma^t)^e(f\hat{1}, i, I), \tag{10}$$

for some e and f, where e is necessarily equal to 1 since σ commutes with σ^t. Looking at the left components of (10), we obtain $u^d\sigma(\hat{a}) = \hat{a} + u^d f\hat{1}$, since $\sigma(\hat{1}) = \hat{1}$. Thus

$$\sigma(\hat{a}) = u^{-d}\hat{a} + f\hat{1}.$$

Recalling (6) and (7), the action

$$\sigma(\hat{a}) = u^{-d}\hat{a} + f\hat{1}$$

translates at the component level to

$$a_{\sigma^{r-1}(1)} = u^{-d}a_{\sigma^r(1)} + f,$$

for all r. This implies that $\hat{a}$ is determined by a_1 and f, and so N is determined by (a_1, f, t).

From $a_{\sigma^{r-1}(1)} = u^{-d} a_{\sigma^r(1)} + f$, we obtain

$$a_{\sigma^{-r}(1)} = u^{-rd} a_1 + (1 + u^{-d} + \cdots + u^{-(r-1)d)}) f,$$

for all r. Letting $u^{-d} = w$, we have

$$a_{\sigma^{-r}(1)} = w^r a_1 + \Big(\frac{w^r - 1}{w-1}\Big) f,$$

for all r, where $w^q \equiv 1 \pmod{p}$.

The condition that $(\hat{a}, u^d, \sigma^t)^q = 1$ places potential constraints on (a_1, f, t). We have

$$(\hat{a}, u^d, \sigma^t)^q = (\hat{a} + u^d \sigma^t \hat{a} + \cdots + u^{d(q-1)} \sigma^{t(q-1)} \hat{a}, u^{dq}, \sigma^{tq}),$$

which equals $(\hat{0}, 1, I)$ provided that

$$\hat{a} + u^d \sigma^t \hat{a} + \cdots + u^{d(q-1)} \sigma^{t(q-1)} \hat{a} = \hat{0}.$$

Looking at the leftmost component of this last equation gives

$$a_1 + u^d a_{\sigma^{-t}(1)} + u^{2d} a_{\sigma^{-2t}(1)} + \cdots + u^{(q-1)d} a_{\sigma^{-(q-1)t}(1)} = 0.$$

Setting $u^{-d} = w$, this is

$$\begin{aligned} 0 = \sum_{r=0}^{q-1} w^{-r} a_{\sigma^{-rt}(1)} &= \sum_{r=0}^{q-1} w^{-r} \Big(w^{rt} a_1 + \frac{w^{rt} - 1}{w-1} f \Big) \\ &= \sum_{r=0}^{q-1} w^{r(t-1)} a_1 + \frac{f}{w-1} \sum_{r=0}^{q-1} (w^{r(t-1)} - w^{-r}). \end{aligned}$$

If $t \neq 1$, then this is equal to

$$a_1 \Big(\frac{w^{(t-1)q} - 1}{w^{t-1} - 1} \Big) + \frac{f}{w-1} \Big(\frac{w^{(t-1)q} - 1}{w^{t-1} - 1} - \frac{w^{-q} - 1}{w^{-1} - 1} \Big).$$

Since $w^q \equiv 1 \pmod{p}$, this is congruent to $0 \pmod{p}$.

If $t = 1$, then this yields

$$f = (1 - w) a_1 = (1 - u^{-d}) a_1. \tag{11}$$

For $t \neq 1$, every pair (a, f) yields a group N. But if we vary the generator $(\hat{a}, u^d, \sigma^t)$ of N of order q by multiplying it by $(k\hat{1}, 1, I)$, we obtain a new generator

$$(k\hat{1}, 1, I)(\hat{a}, u^d, \sigma^t) = (\hat{a} + k\hat{1}, u^d, \sigma^t) = (\hat{b}, u^d, \sigma^t),$$

where $\hat{b} = \hat{a} + k\hat{1}$. Then, since $\sigma(\hat{a}) = u^{-d}\hat{a} + f\hat{1}$, we have

$$\sigma(\hat{b}) = \sigma(\hat{a}) + k\hat{1} = (u^{-d}\hat{a} + f\hat{1}) + k\hat{1} = u^{-d}\hat{b} + (f + (1 - u^{-d})k)\hat{1}.$$

So changing the generator of order q changes (a_1, f, t) to $(a_1+k, f+(1-u^{-d})k, t)$. Since $1-u^{-d}$ is a unit modulo p, the p^2 pairs (a, f) for each $t \neq 1$ yield p different groups N. Thus there are $(q-2)p$ different regular subgroups N isomorphic to $C_p \rtimes_\tau C_q$ with $t \neq 1$.

For $t = 1$,

$$N = \langle(\hat{1}, 1, I), (\hat{a}, u^d, \sigma)\rangle$$

and for the second generator to have order q, we must have (11):

$$(1-u^{-d})a_1 = f,$$

where $\sigma(\hat{a}) = u^{-d}\hat{a} + f\hat{1}$. Replacing $(\hat{a}, u^d, \sigma)$ by $(k\hat{1}, 1, I)(\hat{a}, u^d, \sigma)$ gives an order-q generator $(\hat{b}, u^d, \sigma)$ for N where

$$\hat{b} = \hat{a} + k\hat{1}.$$

Then

$$\begin{aligned}\sigma(\hat{b}) &= \sigma(\hat{a}) + k\hat{1} = (u^{-d}\hat{a} + f\hat{1}) + k\hat{1}\\ &= u^{-d}(\hat{b} - k\hat{1}) + (f+k)\hat{1} = u^{-d}b + f'\hat{1},\end{aligned}$$

where

$$f' = f + k(1-u^{-d}).$$

By choosing k so that $f' = 0$, then $\sigma(\hat{b}) = u^{-d}\hat{b}$, and the condition on the order-q generator becomes

$$(1-u^{-d})b_1 = 0.$$

Hence $b_1 = 0$ and since

$$b_{\sigma^{-r}(1)} = u^{-rd}b_1,$$

we have $\hat{b} = \hat{0}$ and $N = \Gamma$. Thus we obtain $1 + (q-1)p$ regular subgroups N of $\mathrm{Norm}_B(\mathcal{P})$ isomorphic to $C_p \rtimes_\tau C_q$ with $P(N) = \mathcal{P}$ that are normalized by $\Gamma \cong C_p \rtimes_\tau C_q$. By Corollary 3.6, we conclude $R(C_p \rtimes_\tau C_q, [C_p \rtimes_\tau C_q]) = 2(1+(q-1)p)$.

That completes the proof of Theorem 4.1.

5. Groups of order $(2q+1)2q$

In this section we consider $R(\Gamma)$ for groups of order mp where $p = 2q+1$ with q an odd prime and $m = 2q = \phi(p)$; p is then a safe prime. Such groups were explored in some detail in [Childs 2003] (and in [Moody 1994, Example 8.7, p. 133 ff.] for $q = 3$). There are six isomorphism classes of groups of order $p(p-1)$ where $p-1 = 2q$ with q prime:

$$\begin{aligned}
C_{mp} &= C_p \times C_m = \langle x, y \mid x^p = y^m = 1\rangle,\\
F \times C_2 &= (C_p \rtimes C_q) \times C_2\\
&= \langle x, y \mid x^p = y^m = 1;\ yxy^{-1} = x^{u^2}\rangle,\\
C_p \times D_q &= C_p \times (C_q \rtimes C_q)\\
&= \langle x, a, b \mid x^p = a^q = b^2 = 1;\ bx = xb;\ ax = xa,\ bab^{-1} = a^{-1}\rangle,\\
D_{pq} &= C_p \rtimes (C_q \rtimes C_2)\\
&= \langle x, a, b \mid x^p - a^q = b^2 = 1;\ bab^{-1} = x^{-1};\ ax = xa;\ bab^{-1} = a^{-1}\rangle,\\
D_p \times C_q &= (C_p \rtimes C_m = \langle x, y \mid x^p = y^m = 1;\ yxy^{-1} = x^{-1}\rangle,\\
\mathrm{Hol}(C_p) &= C_p \rtimes C_m = \langle x, y \mid x^p = y^m = 1;\ yxy^{-1} = x^u\rangle.
\end{aligned}$$

Here u is a primitive root modulo p: $\langle u\rangle = \mathbb{F}_p^\times = U_p = \mathrm{Aut}(C_p)$.

The main result in this section is:

Theorem 5.1. *Let $R(\Gamma, [M])$ be the set of regular subgroups N isomorphic to M in* $\mathrm{Perm}\,\Gamma_i$ *that are normalized by $\lambda(\Gamma)$. Then the cardinality of $R(\Gamma, [M])$ is given by the following table*:

$\Gamma\downarrow \quad M\rightarrow$	C_{mp}	$C_p\times D_q$	$F\times C_2$	$C_q\times D_p$	D_{pq}	$\mathrm{Hol}\,C_p$
C_{mp}	1	2	$2(q-1)$	2	4	$2(q-1)$
$C_p\times D_q$	q	2	0	$2q$	4	0
$F\times C_2$	p	$2p$	$2(p(q-2)+1)$	$2p$	$4p$	$2p(q-1)$
$C_q\times D_p$	p	$2p$	$2p(q-1)$	2	4	$2p(q-1)$
D_{pq}	qp	$2p$	0	$2q$	4	0
$\mathrm{Hol}\,C_p$	p	$2p$	$2p(q-1)$	$2p$	$4p$	$2(p(q-2)+1)$

For each pair (Γ, M), the table shows $|R(\Gamma, [M])|$, the number of Hopf Galois structures of type M on a Galois extension L/K with Galois group Γ. Thus the row sum for that Γ is the number of Hopf Galois structures on L/K. Observe that whenever M is not a direct product of the p-Sylow subgroup of M with a group of order m, the entries in the M-column are even: that is a consequence of Corollary 3.6.

We now construct subgroups $\mathcal{PQ}$ of S_{mp} isomorphic to Γ for each isomorphism type of groups Γ of order mp. We will work within $B = S_{mp}$ and set $\mathcal{P} = \langle \pi_1\pi_2\cdots\pi_m\rangle$, where π_i is the p-cycle

$$\pi_i = \big((i-1)p+1 \;\; (i-1)p+2 \;\; \ldots \;\; ip\big).$$

Then $\mathrm{Norm}_B(\mathcal{P})$ is isomorphic to the group of 3-tuples $(\hat{a}, u^s, \alpha)$, where $\hat{a} = [a_1, \ldots, a_m]$ with a_i in $\mathbb{F}_p$, $\langle u\rangle = U_p$, and $\alpha \in S_m$. We set

$$\Pi_i = \mathrm{Supp}(\pi_i) = \{(i-1)p+1, (i-1)p+2, \ldots, ip\}.$$

Then we choose regular subgroups $\mathcal{Q}_1$ and $\mathcal{Q}_2$ of $\mathrm{Perm}(\{\Pi_1, \ldots, \Pi_m\}) \cong S_m$ representing the isomorphism types of groups of order $m = 2q$, namely $\mathcal{Q}_1 \cong C_m$ and $\mathcal{Q}_2 \cong D_q$, and embed them in $\mathrm{Norm}_B(\mathcal{P})$ by

$$\alpha \in \mathcal{Q} \mapsto (\hat{0}, 1, \alpha) \in \mathrm{Norm}_B(\mathcal{P}).$$

By slight abuse of notation, we denote the image of $\mathcal{Q}_i$ in $\mathrm{Norm}_B(\mathcal{P})$ also by $\mathcal{Q}_i$.

We choose $\mathcal{Q}_1$ and $\mathcal{Q}_2$ as follows: let $\mathcal{Q}_1 = \langle\sigma\rangle \cong C_m$ and $\mathcal{Q}_2 = \langle\sigma^2, \delta\rangle \cong D_q$, where

$$\begin{aligned} \sigma &= (1, 4, 5, 8, 9, \ldots, 2q-1, 2, 3, 6, \ldots, 2q), \\ \sigma^2 &= (1, 5, 9, \ldots, 2q-3)(2, 6, 10, \ldots, 2q-2), \text{ which we denote by } \sigma_L\sigma_R, \\ \delta &= (1, 2)(3, 2q)(4, 2q-1)(5, 2q-2)\cdots(q, q+3)(q+1, q+2). \end{aligned}$$

Then $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are regular subgroups of S_m. We observe that $(\mathcal{Q}_1)^{\mathrm{opp}} = \mathcal{Q}_1$ (since $\mathcal{Q}_1$ is abelian), and that $\mathcal{Q}_2^{\mathrm{opp}} = \langle\sigma_L\sigma_r^{-1}, \sigma^q\rangle$, where

$$\sigma^q = (1, 2)(3, 4)\cdots(2q-1, 2q).$$

To find the possible order-p subgroups of $N \in R(\Gamma)$, we follow Theorem 2.1 and consider linear characters $\psi_i : C_m \to \mathbb{F}_p^\times$,

$$\psi_i(\sigma) = u^i, \text{ for } i = 0, \ldots, m-1,$$

and $\chi_i : D_q \to \mathbb{F}_p^\times$,

$$\chi_i(\sigma^2) = 1, \chi_i(\delta) = u^{qi} = (-1)^i, \text{ for } i = 0, 1.$$

Since $\mathcal{Q}_1$ and $\mathcal{Q}_2$ centralize $\langle\hat{p}_\iota\rangle = \mathcal{P}$ (since the elements of $\mathcal{Q}_1$ and $\mathcal{Q}_2$ act as permutations of $\{\pi_1, \ldots, \pi_m\}$), the proof of Theorem 2.1 shows that $\mathcal{Q}_i$ normalizes $\langle\hat{p}_\chi\rangle$ for each linear character χ of $\mathcal{Q}_i$. In fact, from Theorem 2.1, if $\mathcal{Q}$ is a regular subgroup of $\mathrm{Perm}(\pi_1, \ldots, \pi_m)$ and χ is a character of $\mathcal{Q}$, then for all μ in $\mathcal{Q}$, $\mu\pi\mu^{-1} = \pi$, so

$$\mu\hat{p}_\chi\mu^{-1} = \chi(\mu)^{-1}\hat{p}_\chi.$$

Hence $\hat{p}_\chi$ is an eigenvector under the action of $\mathcal{Q}$.

More precisely, we have

Lemma 5.2. *For σ the generator of $\mathcal{Q}_1 \cong C_m$ and σ^2 and δ the generators of $\mathcal{Q}_2 \cong D_q$, we have*:

$$\sigma(\hat{p}_{\chi_0}) = \delta(\hat{p}_{\chi_0}) = \hat{p}_{\chi_0}, \quad \sigma(\hat{p}_{\psi_i}) = u^{-1}\hat{p}_{\psi_i}, \quad \sigma^2(\hat{p}_{\chi_1}) = \hat{p}_{\chi_1},$$
$$\delta(\hat{p}_{\chi_1}) = u^q\hat{p}_{\chi_1}, \quad \delta(\hat{p}_{\psi_i}) = \hat{p}_{\psi_{-i}}.$$

Proof. All of these follow from

$$\mu\hat{p}_\chi\mu^{-1} = \mu(\hat{p}_\chi) = \chi(\mu)^{-1}\hat{p}_\chi$$

except the last, in which ψ_i is not a character of $\mathcal{Q}_2$. For the last, we have

$$\hat{p}_{\psi_i} = \sum_{\gamma \in \mathcal{Q}_1} \psi_i(\gamma)\hat{v}_{\gamma(1)} = \sum_{j=0}^{m-1} \psi_i(\sigma^j)\hat{v}_{\sigma^j(1)}.$$

Now $\delta(\sigma) = \sigma^{-1}$, so

$$\begin{aligned}\delta(\hat{p}_{\psi_i}) &= \sum_{j=0}^{m-1} \psi_i(\sigma^j)\hat{v}_{\delta(\sigma^j)(1)} = \sum_{j=0}^{m-1} \psi_i(\sigma^j)\hat{v}_{\sigma^{-j}(1)} = \sum_{j=0}^{m-1} u^{ij}\hat{v}_{\sigma^{-j}(1)} \\ &= \sum_{j=0}^{m-1} u^{-ij}\hat{v}_{\sigma^j(1)} = \sum_{j=0}^{m-1} \psi_{-i}(\sigma^j)\hat{v}_{\sigma^j(1)} = \hat{p}_{\psi_{-i}}.\end{aligned}$$ □

We set $P_i = \langle \hat{p}_{\psi_i} \rangle$ for $i = 0, \dots, m-1$. In particular, $P_0 = \langle \hat{p}_{\chi_0} \rangle = \langle \hat{p}_{\psi_0} \rangle = \langle [1, 1, \dots, 1] \rangle = \langle \hat{1} \rangle = \mathcal{P}$. We also have that

$$\hat{p}_{\chi_1} = \sum_{\gamma \in \mathcal{Q}_2} \chi_1(\gamma)\hat{v}_{\gamma(1)} = \sum_{i=0}^{m-1} (-1)^i \hat{v}_{\delta^i\sigma^{2i}(1)}$$

while

$$\hat{p}_{\psi_q} = \sum_{\gamma \in \mathcal{Q}_1} \psi_q(\gamma)\hat{v}_{\gamma(1)} = \sum_{i=0}^{m-1} (-1)^i \hat{v}_{\sigma(1)}.$$

Both are equal to $\langle [1, -1, 1, -1, \dots, 1, -1] \rangle$.

We thus have subgroups of $\mathrm{Norm}_B(\mathcal{P})$ of the form $P_i\mathcal{Q}_j$ for certain pairs (i, j). We identify their isomorphism types as follows:

Proposition 5.3. *With P_i and $\mathcal{Q}_j$ as defined above, we have*

$$\begin{aligned} P_0\mathcal{Q}_1 &\cong C_p \times C_m, \\ P_i\mathcal{Q}_1 &\cong F \times C_2 \textit{ for } i \textit{ even}, i \neq 0, \\ P_i\mathcal{Q}_1 &\cong \mathrm{Hol}(C_p) \textit{ for } i \textit{ odd}, i \neq q, \\ P_q\mathcal{Q}_1 &\cong D_p \times C_q, \\ P_0\mathcal{Q}_2 &\cong D_q \times C_p, \\ P_q\mathcal{Q}_2 &\cong D_{pq}. \end{aligned}$$

Proof. This follows from Lemma 5.2 and the definitions for the P_i. □

Each group $\mathcal{P}_i\mathcal{Q}_j$ above centralizes $\mathcal{P} = P_0 = \langle [1, 1, \dots, 1] \rangle = \langle \hat{1} \rangle$, so each opposite group $(\mathcal{P}_i\mathcal{Q}_j)^{\mathrm{opp}}$ will contain $\mathcal{P}$. We will use those opposite groups for the groups Γ in the computations.

We need to observe:

Proposition 5.4. *Each group $P_i\mathcal{Q}_j$ is a regular subgroup of* $\mathrm{Norm}_B(\mathcal{P})$.

Proof. Each $P_i\mathfrak{Q}_j$ is a subgroup of order mp by Proposition 5.3. To show regularity we show that each nonidentity element of $P_i\mathfrak{Q}_j$ acts fixed-point-freely. Now each element of $P_i\mathfrak{Q}_j$ has the form $(\hat{a}, 1, \alpha)$ for $\hat{a}$ in $\mathbb{F}_p^n$ and α in S_m. Since $\mathfrak{Q}_j$ is a regular subgroup of S_m acting on $\{\Pi_1, \dots, \Pi_m\}$, $(\hat{a}, 1, \alpha)$ is fixed-point free for $\alpha \neq 1$ by Proposition 3.8. If an element $(\hat{a}, 1, I)$ is not the identity, then $\hat{a} = [a_1, a_2, \dots, a_m]$ with all $a_i \neq 0$ (since $\hat{a}$ is a power of $\hat{p}_\chi$ for some linear character with values in $\mathbb{F}_p^\times$). Hence for t in Π_i, $(\hat{a}, 1, I)(t) = a_i + t \neq t$; hence $(\hat{a}, 1, I)$ has no fixed points. □

For each isomorphism type of Γ, we have the following (recall that $P(\Gamma) = P_0 = \mathcal{P} = \langle [1, 1, \dots, 1]\rangle = \langle\hat{1}\rangle$):

$$\begin{aligned}
\Gamma = C_p \times C_m &= (P_0\mathfrak{Q}_1)^{\text{opp}} = P_0\mathfrak{Q}_1 \\
&= P_0\langle(\hat{0}, 1, \sigma)\rangle, \\
\Gamma = C_p \times D_q &= (P_0\mathfrak{Q}_2)^{\text{opp}} \\
&= P_0\langle(\hat{0}, 1, \sigma^q)(\hat{0}, 1, \sigma_L\sigma_R^{-1})\rangle, \\
\Gamma = D_p \times C_q &= (P_q\mathfrak{Q}_1)^{\text{opp}} \\
&= P_0\langle(\hat{0}, u^q, \sigma)\rangle, \\
\Gamma = D_{pq} &= (P_q\mathfrak{Q}_2)^{\text{opp}} \\
&= P_0\langle(\hat{0}, u^q, \sigma^q)\rangle, \\
\Gamma = F \times C_2 &= (P_2\mathfrak{Q}_1)^{\text{opp}} \\
&= P_0\langle(\hat{0}, u^2, \sigma)\rangle, \\
\Gamma = \text{Hol}(C_p) &= (P_1\mathfrak{Q}_1)^{\text{opp}} \\
&= P_0\langle(\hat{0}, u, \sigma)\rangle.
\end{aligned}$$

There is a certain arbitrariness concerning these last two choices.

Recall from Proposition 3.8 that if $(\hat{a}, 1, \alpha)$ in $\text{Norm}_B(\mathcal{P})$ has order coprime to p, then $(\hat{a}, 1, \alpha)$ is fixed-point free in $\text{Norm}_B(\mathcal{P})$ if and only if α is fixed-point free in S_m.

Lemma 5.5. *Let* $\alpha = [a_1, \dots, a_m] \in \mathbb{F}_p^m$ *and* $\alpha \in S_m$.

If the element $(\hat{a}, 1, \alpha)$ *has order* 2, *then* $\alpha = x_1 \cdots x_q$, *a product of* q *disjoint* 2-*cycles such that for each* $x_i = (r, s)$, $a_r + a_s = 0$.

If the element $(\hat{a}, 1, \alpha)$ *has order* q, *then* $\alpha = x_1x_2$, *disjoint* q-*cycles, and* $\sum_{i\in\text{Supp}(x_j)} a_i = 0$ *for* $i = 1, 2$.

If the element $(\hat{a}, 1, \alpha)$ *has order* $m = 2q$, *then* α *is an* m-*cycle and* $\sum_{i=0}^{m-1} a_i = 0$.

Proof. Let $d = |(\hat{a}, 1, \alpha)|$. If d is coprime to p, then $|\alpha| = d$; for otherwise $|\alpha| = e < d$, in which case $(\hat{a}, 1, \alpha)^e = (\hat{b}, 1, I)$, with $\hat{b} \neq 0$. But then $(\hat{b}, 1, I)$ has order p, and so p divides $|(\hat{a}, 1, \alpha)|$, a contradiction.

So if d is coprime to p, then α has order d. Since α is fixed-point free, if $d = 2$, then α is a product of q disjoint 2-cycles; if $d = q$ then α is a product of two disjoint

q-cycles, and if α has order $m = 2q$ then α is an m-cycle. Now

$$(\hat{a}, 1, \alpha)^n = \left(\sum_{k=0}^{n-1} \alpha^k(\hat{a}),\ 1,\ \alpha^n \right).$$

If n is the order of $(\hat{a}, 1, \alpha)$, hence also the order of α, then by what was just observed,

$$\sum_{k=0}^{n-1} \alpha^k(\hat{a}) = \hat{0},$$

and hence for each a_i,

$$\sum_{k=0}^{n-1} a_{\alpha^{-k}(i)} = \sum_{k=0}^{n-1} a_{\alpha^k(i)} = 0.$$

The conclusions of the lemma follow. □

Using that

$$(\hat{a}, u^r, \alpha)^n = \left(\sum_{k=0}^{n-1} u^{rk} \alpha^k(\hat{a}),\ u^{rn},\ \alpha^n \right),$$

the same argument gives:

Lemma 5.6. *Let $\hat{a} = [a_1, \dots, a_m] \in \mathbb{F}_p^m$, $r \neq 0$ in $\mathbb{F}_p^\times$, and $\alpha \in S_m$.*

If the element $(\hat{a}, u^r, \alpha)$ has order 2, then $r = q$ and $u^r = u^q = -1$, and $\alpha = (x_1, \dots, x_q)$, a product of q disjoint 2-cycles such that for each $x_i = (r, \alpha(r))$, $a_r - a_{\alpha(r)} = 0$.

If the element $(\hat{a}, u^r, \alpha)$ has order q, then $\alpha = x_1 x_2$, where x_1 and x_2 are disjoint q-cycles, and for t_i in $\operatorname{Supp} x_i$,

$$\sum_{k=0}^{q-1} u^{kr} a_{\alpha^{-k}(t_i)} = 0,$$

for $i = 1, 2$.

If the element $(\hat{a}, u^r, \alpha)$ has order $m = 2q$, then α is an m-cycle and

$$\sum_{i=0}^{m-1} u^{ri} \alpha^{-i}(a_1) = 0.$$

Enumeration of the $R(\Gamma, [M])$ for each of the 36 pairs (Γ, M) in Theorem 5.1 breaks up into subcases. Recall that $R(\Gamma, [M]; P_i)$ is the set of regular subgroups N of $\operatorname{Norm}_B(\mathcal{P}) \subset S_{mp}$ such that the p-Sylow subgroup of N is $P(N) = P_i$. By Corollary 3.6, if $M \cong C_{mp}$ or $C_p \times D_q$, $R(\Gamma, [M]) = R(\Gamma, [M]; P_0)$. For other M, Corollary 3.6 shows that to count $R(\Gamma, [M])$ we need only count $R(\Gamma, [M]; P_0)$ (where $P_0 = \mathcal{P}$). But given that regular subgroups N yield Hopf Galois structures on Galois extensions of fields with Galois group Γ, it is useful to explicitly consider $R(\Gamma, [M]; P_i)$ for $i \neq 0$.

Thus, rather than just the 36 cases described in Theorem 5.1, a more complete story would involve 57 cases: 36 of the form $R(\Gamma, [M]; P_0)$, and 21 of the form $R(\Gamma, [M]; P_i)$ with $i \neq 0$ where for each $[M]$, the possible P_i with $i \neq 0$, where $P(N) = P_i$ and $N \cong M$, are as listed in Proposition 5.3. The counts in those cases are as follows.

For $N \cong M = D_p \times C_q$ or D_{pq}, we have $P(N) = P_0$ or P_q and Corollary 3.6 shows that $|R(\Gamma, [M]; P_q)| = |R(\Gamma, [M]; P_0)|$.

For $N \cong M = F \times C_2$ or $\mathrm{Hol}\, C_p$, there are $\phi(2q)$ possible i, and $|R(\Gamma, [M]; P_i)| = |R(\Gamma, [M]; P_j)|$ for all possible $i \neq j$ and $i, j \neq 0$, except when $\Gamma \cong M$.

For $\Gamma = M = F \times C_2$ we have

$$|R(F \times C_2, [F \times C_2]; P_2)| = 1,$$
$$|R(F \times C_2, [F \times C_2]; P_i)| = p \quad \text{for } i = 4, 6, \ldots, 2q-2.$$

The case $\Gamma = M = \mathrm{Hol}(C_p)$ is similar and will be described below.

Since most of the computations are very similar in outline and details to those in Section 4, we will limit ourselves to just three cases. Before we begin, we pause to give the reader some perspective, with a view toward dealing with other classes of groups of order mp, beyond those considered here. There are some common themes that arise in the enumeration of $N \in R(\Gamma, [M])$, in particular in the determination of the 3-tuples $(\hat{a}, v, \alpha)$ that generate $Q(N)$, some of which have been seen already in the work in Section 4.

- The given generator of $Q(N)$ must, of course, normalize (and possibly even centralize) $P(N)$.
- Any $Q(N)$ is semiregular so any generator of $Q(N)$ must act without fixed points, which imposes restrictions on its components as seen above. And if one is dealing with several generators of $Q(N)$, the products of these generators also cannot have fixed points.
- The order of a given generator of $Q(N)$ imposes restrictions on its components.
- Any N is normalized by Γ, so when a given generator of $Q(N)$ is conjugated by an element of Γ it is mapped to another element of N and the form of this conjugate is determined by whether $Q(N)$ is a direct factor of N or not.
- The restrictions imposed by order, semiregularity, and being normalized by Γ will frequently imply that $\hat{a}$ is the solution to a particular set of linear equations and so linear algebra techniques may be applied.
- The number of free variables that determine the solution sets for the aforementioned linear systems determines whether or not the resulting generators

$(\hat{a}, v, \alpha)$ lie in $Q(N)$ for a *single* N or, in fact, multiple N. As such, the count of $|R(\Gamma, [M])|$ may vary linearly with p (as when we showed that $|R(C_p \rtimes_\tau C_q, [C_{pq}])| = p$ earlier) or be "combinatorially" determined, that is, in terms of some intrinsic property of regular subgroups of S_m, as will be seen at the end of the determination of $|R(C_{mp}, [C_p \times D_q])|$ later on.

$R(C_p \times D_q, [F \times C_2])$.

Proposition 5.7. *With $p > q$ primes, $|R(C_p \times D_q, [F \times C_2])| = 0$.*

Proof. We have

$$\Gamma = \mathcal{P}\langle(\hat{0}, 1, \sigma^2), (\hat{0}, q, \delta)\rangle.$$

Since $N \cong F \times C_2 \cong (C_p \rtimes C_q) \times C_2$, it has the form

$$N = \langle(\hat{0}, 1, I), (\hat{a}, u^r, \alpha)\rangle,$$

where $(\hat{a}, u^r, \alpha)$ has order $m = 2q$, and therefore α is an m-cycle in S_m. Now $(\hat{a}, u^r, \alpha)$ conjugates the order-p generator of N to its u^2 power

$$(\hat{a}, u^r, \alpha)(\hat{1}, 1, I)(\hat{a}, u^r, \alpha)^{-1} = (u^2\hat{1}, 1, I),$$

so $r = 2$.

Also α has order $m = 2q$, and being fixed-point free, must be an m-cycle.

If Γ normalizes N, then conjugation by $(\hat{0}, 1, \sigma^2)$ and $(\hat{0}, 1, \delta)$ are automorphisms of N. Every automorphism of $F \times C_2$ sends the order-m element y to xy for some element x of order p. Thus conjugating the order-m generator $(\hat{a}, u^2, \alpha)$ of N by $(\hat{0}, 1, \sigma^2)$ and $(\hat{0}, 1, \delta)$, and looking at the rightmost S_m components of the result, we have that $\sigma^2\alpha\sigma^{-2} = \alpha$ and $\delta\alpha\delta^{-1} = \alpha$. Thus σ^2 and δ commute with α. But since α is an m-cycle in S_m, the centralizer in S_m of α is $\langle\alpha\rangle$. So σ^2 and δ are powers of α in S_m, and hence commute. But that's impossible. Thus no α exists, and hence there is no N isomorphic to $F \times C_2$ that is normalized by $\Gamma \cong C_p \times D_q$.

By Corollary 3.6, $R(C_p \times D_q, [F \times C_2]; P_0) = 0$. $\square$

Essentially the same argument shows that $|R(C_p \times D_q), [\mathrm{Hol}(C_p)])|$, $|R(D_{pq}, [F \times C_2])|$, and $|R(D_{pq}, [\mathrm{Hol}(C_p)])|$ are all zero.

$R(C_{mp}, [C_p \times D_q]) = R(C_{mp}, [C_p \times D_q]; P_0)$. We will need the following technical information.

Lemma 5.8. *If $x = (a_1, a_2, \ldots, a_q)$ and $y = (b_1, b_2, \ldots, b_q)$ are elements with disjoint support in $S_{2q} = \mathrm{Perm}(\{1, \ldots, 2q\})$ then $\mathrm{Norm}_{S_{2q}}(\langle xy\rangle)$ contains $2q(q-1)$ elements z of order $2q$ with no fixed points (which are therefore $2q$-cycles), half of which centralize xy and are such that $\langle z^2\rangle = \langle(xy)^2\rangle$ and the other half invert xy and satisfy $\langle z^2\rangle = \langle(xy^{-1})^2\rangle$. Also, $\mathrm{Norm}_{S_{2q}}(\langle xy\rangle)$ contains two subgroups isomorphic to D_q, which are opposites of each other, one of which is contained in $\mathrm{Cent}_{S_{2q}}(xy)$.*

Proof. First we observe that $\mathrm{Norm}_{S_{2q}}(\langle xy\rangle)$ is isomorphic to $\mathbb{F}_q^2 \rtimes (\langle u\rangle \times S_2)$ where $\langle u\rangle = \mathbb{F}_q^\times$. As such, one may readily count how many elements have order $2q$. In particular, since a typical element is a 3-tuple $(\hat{v}, u^r, \alpha)$ with $\hat{v} = (v_1, v_2) \in \mathbb{F}_q^2$, $\langle u\rangle = \mathbb{F}_q^*$, and $\alpha \in S_2$, then, using (2), one may show that $|(\hat{v}, u^r, \alpha)| = 2q$ provided that $\alpha = (1, 2)$, and either $v_1 \neq v_2$ and $u^r = -1$ or $v_1 \neq -v_2$ and $u^r = 1$. This yields precisely $2(q^2 - q) = 2q(q - 1)$ elements as claimed. We can exhibit the particular elements of order $2q$ (as elements in S_{2q}) as follows. First, let

$$
\begin{aligned}
t_0 &= (a_1, b_1)(a_2, b_2)\cdots(a_q, b_q),\\
t_1 &= (a_1, b_2)(a_2, b_3)\cdots(a_q, b_1),\\
&\vdots\\
t_{q-1} &= (a_1, b_q)(a_2, b_1)\cdots(a_q, b_{q-1}),\\
\tau_0 &= (a_1, b_1)(a_2, b_q)\cdots(a_q, b_2),\\
\tau_1 &= (a_1, b_2)(a_2, b_1)\cdots(a_q, b_3),\\
&\vdots\\
\tau_{q-1} &= (a_1, b_q)(a_2, b_{q-1})\cdots(a_q, b_1),
\end{aligned}
$$

and consider the elements xyt_i and $xy^{-1}\tau_i$. One may verify that each t_i interchanges x and y, so that xyt_i centralizes xy and that $\tau_i x \tau_i^{-1} = y^{-1}$ and $\tau_i y \tau_i^{-1} = x^{-1}$; therefore $xy^{-1}\tau_i$ inverts xy. Each of the elements xyt_i and $xy^{-1}\tau_i$ are $2q$-cycles and each generates a distinct subgroup. Moreover $(xyt_i)^2 = (xy)^2 \in \langle xy\rangle$ while $(xy^{-1}\tau_i)^2 = (xy^{-1})^2 \in \langle xy^{-1}\rangle$. The conclusion we get is that if a $2q$-cycle z inverts or centralizes xy then $z^2 \in \langle xy^{-1}\rangle$ or $\langle xy\rangle$. The groups $\langle xy^{-1}, t_i\rangle$ for each i are all equal and isomorphic to D_q (and are contained in $\mathrm{Cent}_{S_{2q}}(xy)$), and the groups $\langle xy, \tau_i\rangle$ are all equal and isomorphic to D_q but are not subgroups of $\mathrm{Cent}_{S_{2q}}(xy)$. Moreover $\langle xy^{-1}, t_i\rangle^{\mathrm{opp}} = \langle xy, \tau_i\rangle$ since each clearly centralizes the other. One may also observe that each of the $2q$-cycles above clearly normalize each of these two copies of D_q. □

If C is a cyclic regular subgroup of S_{2q} and $\langle xy\rangle = Q(C)$, then C must be generated by one of the $2q$-cycles given in Lemma 5.8. If $N \cong D_q \subset S_{2q}$ is normalized by C, then $Q(N) = \langle xy\rangle$, and so $N = \langle xy, \tau_i\rangle$. Thus $|R(C_{2q}, [D_q]; P_0)| = 1$. This is in agreement with Theorem 4.1 (if in Theorem 4.1 we set $p = 2$ and exchange the roles of p and q).

Proposition 5.9. $|R(C_{mp}, [C_p \times D_q])| = 2$.

Proof. Here $P(N) = \mathcal{P}$, since $Q(N)$ is a direct factor of N. In this case $Q(N)$ is generated by $(\hat{a}, 1, \alpha)$ of order q and $(\hat{b}, 1, \beta)$ of order 2. Note that both $Q(N)$ and

$\langle(\hat{a}, 1, \alpha)\rangle$ are characteristic subgroups of N. So

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

must equal $(\hat{a}, 1, \alpha)^k$ for some k. By Lemma 5.8, σ must either centralize or invert α, so $k = 1$ or -1.

First, we look at the case where σ *centralizes* α. Then

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

so $\sigma(\hat{a}) = \hat{a}$, and therefore $\hat{a} = a\hat{1}$ for some a in $\mathbb{F}_p$. Consequently, $\alpha(\hat{a}) = \hat{a}$. Since $(\hat{a}, 1, \alpha)$ has order q, we have that $q\hat{a} = qa\hat{1} = \hat{0}$, and so $a = 0$ and $\hat{a} = \hat{0}$.

Now, since $(\hat{b}, 1, \beta)$ normalizes $\langle(\hat{a}, 1, \alpha)\rangle$ then

$$\begin{aligned}(\hat{b}, 1, \beta)(\hat{a}, 1, \alpha)(-\beta^{-1}(\hat{b}), 1, \beta^{-1}) &= (\hat{b}, 1, \beta)(\hat{0}, 1, \alpha)(-\beta^{-1}(\hat{b}), 1, \beta^{-1})\\ &= (\hat{b} - (\beta\alpha\beta^{-1})(\hat{b}), 1, \beta\alpha\beta^{-1}),\end{aligned}$$

which must equal

$$(\hat{0}, 1, \alpha)^{-1} = (\hat{0}, 1, \alpha^{-1}).$$

As $\beta\alpha\beta^{-1} = \alpha^{-1}$ we have $\hat{b} - \alpha^{-1}(\hat{b}) = \hat{0}$, so that $\alpha(\hat{b}) = \hat{b}$. Now, we must have that $(\hat{0}, 1, \sigma)$ conjugates $(\hat{b}, 1, \beta)$ to another order-2 element of $Q(N)$, ergo

$$\begin{aligned}(\hat{0}, 1, \sigma)(\hat{b}, 1, \beta)(\hat{0}, 1, \sigma^{-1}) &= (\hat{0}, 1, \alpha)^k(\hat{b}, 1, \beta)\\ &= (\alpha^k(\hat{b}), 1, \alpha^k\beta)\\ &= (\hat{b}, 1, \alpha^k\beta), \quad \text{since } \alpha(\hat{b}) = \hat{b}.\end{aligned}$$

So we must have $\sigma(\hat{b}) = \hat{b}$, which means $\hat{b} = b\hat{1}$ for some b in $\mathbb{F}_p$. But $\beta(\hat{b}) = -\hat{b}$ since $(\hat{b}, 1, \beta)$ has order 2. Thus $b = 0$. We conclude that

$$Q(N) = \langle(\hat{0}, 1, \alpha), (\hat{0}, 1, \beta)\rangle,$$

where $\langle\alpha, \beta\rangle \cong D_q$ and is centralized by σ.

Letting $\alpha = xy$ in Lemma 5.8, σ is an element of $\mathrm{Norm}_{S_{2q}}(\langle\alpha\rangle)$ of order $2q$ that centralizes α, hence by Lemma 5.8 $\sigma^2 \in \langle\alpha\rangle$, hence $\langle\sigma^2\rangle = \langle\alpha\rangle$. Now $\mathrm{Norm}_{S_{2q}}(\langle\alpha\rangle)$ contains a unique copy of D_q that does not centralize α. That copy must be $\langle\alpha, \beta\rangle$, since clearly $\langle\alpha, \beta\rangle$ does not centralize α,

We show that $\mathcal{Q}_2$ is also in $\mathrm{Norm}_{S_{2q}}(\langle\alpha\rangle)$ and does not centralize α. Recall (from Lemma 5.2) that $\mathcal{Q}_2 = \langle\sigma^2, \delta\rangle \cong D_q$, hence $\delta\sigma^2 = \sigma^{-2}\delta$. Since $\langle\sigma^2\rangle = \langle\alpha\rangle$, δ normalizes but does not centralize $\langle\alpha\rangle$. Hence $\mathcal{Q}_2$ is contained in $\mathrm{Norm}_{S_{2q}}(\langle\alpha\rangle)$ and does not centralize α. By the uniqueness, $\mathcal{Q}_2 = \langle\alpha, \beta\rangle$. We conclude that the group N above is the unique regular subgroup of $\mathrm{Norm}_B(\mathcal{P})$ such that $Q(N)$ maps to $\mathcal{Q}_2$ in S_{2m}.

Now assume that σ *inverts* α. We show that $\mathfrak{Q}_2$ is in $\mathrm{Norm}_{S_{2q}}(\langle\alpha\rangle)$. We have that σ is in $\mathrm{Norm}_{S_{2q}}(\langle\alpha\rangle)$ and σ^2 is in $\langle xy^{-1}\rangle$. So σ^2 centralizes α by the proof of Lemma 5.8. Now δ inverts σ^2, hence inverts xy^{-1}. Since $\delta(xy^{-1})\delta^{-1} = x^{-1}y$, either $\delta x\delta^{-1} = x^{-1}$ or $\delta x\delta^{-1} = y$. But δ is a fixed-point-free product of transpositions in S_{2m}. If $\delta x\delta^{-1} = x^{-1}$ then δ restricts to a fixed-point-free product of transpositions of $\mathrm{Supp}\, x$, a set with an odd number of elements. That is not possible. So $\delta x\delta^{-1} = y$ and $\delta y\delta^{-1} = x$, so δ centralizes $\alpha = xy$. Thus $\mathfrak{Q}_2 = \langle\sigma^2, \delta\rangle \in \mathrm{Norm}_{S_{2q}}(\langle\alpha\rangle)$ and centralizes α. Since $\langle\alpha, \beta\rangle \in \mathrm{Norm}_{S_{2q}}(\langle\alpha\rangle)$ and does not centralize α, therefore $\langle\alpha, \beta\rangle = \mathfrak{Q}_2^{\mathrm{opp}}$ by Lemma 5.8.

Now

$$Q(N) = \langle(\hat{a}, 1, \alpha), (\hat{b}, 1, \beta)\rangle.$$

Since $(\hat{0}, 1, \sigma)$ normalizes $\langle(\hat{a}, 1, \alpha)\rangle$, which is characteristic in N, and $\sigma\alpha\sigma = \alpha^{-1}$, we have

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

hence $\sigma(\hat{a}) = -\alpha(\hat{a})$, and so

$$\alpha\sigma(\hat{a}) = -\hat{a}.$$

Since σ inverts α, σ has order $2q$, and α has order q, one sees easily that $\alpha\sigma$ has order $2q$. Hence

$$\hat{a} = [a_1, a_{\alpha\sigma(1)}, \ldots, a_{(\alpha\sigma)^{2q-1}(1)}],$$

while

$$\alpha\sigma(\hat{a}) = [a_{(\alpha\sigma)^{-1}(1)}, a_1, a_{\alpha\sigma(1)}, \ldots, a_{(\alpha\sigma)^{2q-2}(1)}].$$

We have $\alpha\sigma(\hat{a}) = -\hat{a}$, while $(\alpha\sigma)^2(\hat{a}) = \hat{a}$. Thus

$$a_{(\alpha\sigma)^r(1)} = \begin{cases} a_1 & \text{if } r \text{ is even,} \\ -a_1 & \text{if } r \text{ is odd.} \end{cases}$$

Now $(\hat{a}, 1, \alpha)$ has order q, so

$$\sum_{i=0}^{q-1} \alpha^i(\hat{a}) = \hat{0};$$

hence

$$\sum_{i=0}^{q-1} a_{\alpha^{-i}(1)} = 0.$$

But the sum of an odd number of elements of $\mathbb{F}_p$ from a set consisting of copies of a and $-a$ can equal 0 only when $a = 0$.

Thus $\hat{a} = \hat{0}$. Since $(\hat{b}, 1, \beta)$ normalizes $(\hat{0}, 1, \alpha)$, the same argument as in the first case of this proof shows that $\hat{b} = \hat{0}$. Thus

$$N = \mathcal{P} \cdot \langle(\hat{0}, 1, \alpha), (\hat{0}, 1, \beta)\rangle,$$

where $\langle\alpha, \beta\rangle = \mathfrak{Q}_2^{\mathrm{opp}}$, hence N is the unique regular subgroup of $\mathrm{Norm}_B(\mathcal{P})$ with $Q(N)$ mapping to $\mathfrak{Q}_2^{\mathrm{opp}}$ in S_{2q}. □

***R*(Hol(C_p), [Hol(C_p)]).**

Proposition 5.10. $|R(\mathrm{Hol}(C_p), [\mathrm{Hol}(C_p)])| = 2(1 + p(q-2))$.

Proof. Hol C_p is not a direct product of a group of order p and a group of order $m = 2q$, so it suffices to show that $|R(\mathrm{Hol}(C_p), [\mathrm{Hol}(C_p)]; P_0)| = 1 + p(q-2)$. This case is essentially similar to the computation for $R(C_p \rtimes_\tau C_q, [C_p \rtimes_\tau C_q])$ in Section 5, and yields the same cardinality. So instead, we focus here on the case where $P(N) \neq P_0$.

Let $\Gamma = \langle(\hat{1}, 1, I), (\hat{0}, u, \sigma)\rangle$ and let $N = \langle(\hat{p}_{\psi_i}, 1, I), (\hat{b}, u^s, \beta)\rangle$, where $(\hat{b}, u^s, \beta)$ has order m. Since N is regular, β is fixed-point free of order $m = 2q$, so must be an m-cycle, and by the argument of Lemma 4.3 using that $(\hat{b}, u^s, \beta)$ is normalized by Γ, we find that $\beta = \sigma^t$ for some t coprime to m.

Since $N \cong \mathrm{Hol}(C_p)$, the two generators of N, x of order p and y of order m, must satisfy the defining relation $yx = x^u y$, so we must have

$$(\hat{b}, u^s, \sigma^t)(\hat{p}_{\psi_i}, 1, I)(\hat{b}, u^s, \sigma^t)^{-1} = (u\hat{p}_{\psi_i}, 1, I),$$

and hence $u^s\sigma^t\,\hat{p}_{\psi_i} = u\hat{p}_{\psi_i}$. Since $\sigma(\hat{p}_{\psi_i}) = u^{-i}\,\hat{p}_{\psi_i}$, this becomes

$$u^{s-it}\,\hat{p}_{\psi_i} = u\hat{p}_{\psi_i},$$

hence

$$s - it \equiv 1 \pmod{m}. \tag{12}$$

Also, Γ normalizes N. Thus we require that

$$(\hat{1}, 1, I)(\hat{b}, u^s, \sigma^t)(-\hat{1}, 1, I) \in N,$$

hence

$$\hat{b} + (1 - u^s)\hat{1} = f\,\hat{p}_{\psi_i} + \hat{b}.$$

Thus $(1 - u^s)\hat{1} = f\,\hat{p}_{\psi_i}$, which for $i \neq 0$ can only occur when both sides equal zero. Thus $s = 0$ and $f = 0$. From (12) we obtain

$$-it \equiv 1 \pmod{m}, \tag{13}$$

hence t is odd and coprime to m.

Since Γ normalizes N, conjugation by $(\hat{0}, u, \sigma^t)$ is an automorphism of N. Every automorphism of N must take the generator y of order m to $x^k y$ for some power x^k of the generator of order p. Thus (noting that $u^s = 1$),

$$(\hat{0}, u, \sigma)(\hat{b}, 1, \sigma^t)(\hat{0}, u^{-1}, \sigma^{-1}) = (k\hat{p}_{\psi_i}, 1, I)(\hat{b}, 1, \sigma^t),$$

for some k, so

$$u\sigma(\hat{b}) = \hat{b} + k\sigma^t(\hat{p}_{\psi_i}) = \hat{b} + ku^{-it}\hat{p}_{\psi_i},$$

which, in view of (13), yields

$$\sigma(\hat{b}) = u^{-1}\hat{b} + k\hat{p}_{\psi_i}.$$

Setting $u^{-1} = w$, we have

$$\sigma(\hat{b}) = w\hat{b} + k\hat{p}_{\psi_i}.$$

For $(\hat{b}, 1, \sigma^t)^m = (\hat{0}, 1, I)$, we need that

$$\hat{b} + \sigma^t(\hat{b}) + \cdots + \sigma^{(m-1)t}(\hat{b}) = 0.$$

This holds if the first elements of the terms on the left side sum to 0:

$$b_1 + b_{\sigma^{-t}(1)} + \cdots + b_{\sigma^{-tj}(1)} + \cdots + b_{\sigma^{-t(m-1)}(1)} = 0. \tag{14}$$

First assume $i \neq 1$. Then for all r, we have

$$\sigma^r(\hat{b}) = w^r\hat{b} + \frac{w^r - w^{ri}}{w - w^i}k\hat{p}_{\psi_i}.$$

Thus, since $(\hat{p}_{\psi_i})_1 = 1$, the first component of $\sigma^r(\hat{b})$ is

$$b_{\sigma^{-r}(1)} = (\sigma^r(\hat{b}))_1 = w^r b_1 + \frac{w^r - w^{ri}}{w - w^i}k.$$

Thus (14) is

$$\begin{aligned}\sum_{l=0}^{m-1} b_{\sigma^{-tl}(1)} &= \sum_{l=0}^{m-1}\left(w^{tl}b_1 + k\left(\frac{w^{tl} - w^{tli}}{w - w^i}\right)\right)\\ &= b_1\left(\frac{w^{tm} - 1}{w^t - 1}\right) + k\sum_{l=0}^{m-1}\left(\frac{w^{tl} - w^{tli}}{w - w^i}\right).\end{aligned}$$

Since $w^m = 1$, the first sum is 0; so this becomes

$$\begin{aligned}&= \frac{k}{w - w^i}\sum_{l=0}^{m-1} w^{tl} - \sum_{l=0}^{m-1} w^{tli}\\ &= \frac{k}{w - w^i}\,\frac{w^{tm} - 1}{w^t - 1} - \frac{w^{tim} - 1}{w^{ti} - 1}.\end{aligned}$$

Now $ti \equiv -1 \pmod{m}$, so $w^{ti} = w^{-1}$ and so both terms in this last equation equal zero. Thus (14) holds if $i \neq 1$.

If $i = 1$, then $t = -1$ and $\sigma^r(\hat{b}) = w^r\hat{b} + rw^{r-1}k\hat{p}_{\psi_i}$ for all r. Thus (14) becomes

$$\sum_{l=0}^{m-1} b_{\sigma^{-tl}(1)} = \sum_{l=0}^{m-1} w^{tl}b_1 + k\sum_{l=0}^{m-1}(tlw^{tl} - 1).$$

The first sum on the right is equal to zero. By the same observation as with (9), the second sum on the right equals zero if and only if $k = 0$. Thus when $i = 1$ and $t = -1$, the generator $(\hat{b}, 1, \sigma^t)$ has order m if and only if $\sigma(\hat{b}) = u^{-1}\hat{b}$. In that case, $\hat{b} = b_1 \hat{p}_{\psi_1}$, and so replacing the generator $(\hat{b}, 1, \sigma^{-1})$ of N by $(-b_1 \hat{p}_{\psi_1}, 1, I)(\hat{b}, 1, \sigma^{-1}) = (0, 1, \sigma^{-1})$ yields

$$N = \langle (\hat{p}_{\psi_1}, 1, I), (\hat{0}, 1, \sigma^{-1}) \rangle.$$

Thus there is a unique regular subgroup N when $t = -1$. For $t \neq -1$, each b_1 yields a different N, hence we have a total of $1 + (q-2)p$ regular subgroups N with $P(N) \neq \mathcal{P}$. By Corollary 3.6, this implies that $|R(\mathrm{Hol}(C_p), [\mathrm{Hol}(C_p)])| = 2(1 + (q-2)p)$. □

The enumeration of $R(\mathrm{Hol}(C_p), [\mathrm{Hol}(C_p)])$ is in agreement with that in [Childs 2003].

6. Conclusion

The program developed here to enumerate $R(\Gamma, [M])$ may be readily applied to any class of groups of order mp with $p > m$. The primary requirement is to start with the groups of order m and for the particular p determine the set of linear characters for each group of order m. One may find that, depending on congruence conditions between m and p the number of possible characters may vary greatly. Nonetheless, one is presented with a very interesting set of calculations, wherein one may apply many different techniques. What is most interesting is the interplay between the linear and combinatorial information in the different cases. For small m and p these computations may be readily implemented in a computer algebra system such as GAP [2002]. This was done by the author in the development of this work, especially in gathering empirical information about some specific cases, for example, with $mp = 42$. Lastly, and this is mildly conjectural, it seems that the theory developed here applies to certain cases where actually $p < m$. Specifically, one might consider those cases where $p \nmid m$ and the order-p subgroup is automatically characteristic due to basic Sylow theory, for example, $p = 5$ and $m = 8$.

Acknowledgements

The author wishes to thank the referee, Lindsay Childs, for the time and attention spent on reading this article. His insights greatly improved the exposition of the results and the concision of many of the arguments.

References

[Burnside 1911] W. Burnside, *Theory of groups of finite order*, 2nd ed., Cambridge University Press, Cambridge, 1911. Reprinted by Dover in 1955. MR 16,1086c JFM 42.0151.02

[Byott 1996] N. P. Byott, "Uniqueness of Hopf Galois structure for separable field extensions", *Comm. Algebra* **24**:10 (1996), 3217–3228. MR 97j:16051a Zbl 0878.12001

[Byott 2000] N. P. Byott, "Galois module theory and Kummer theory for Lubin–Tate formal groups", pp. 55–67 in *Algebraic number theory and Diophantine analysis* (Graz, 1998), edited by F. Halter-Koch and R. F. Tichy, de Gruyter, Berlin, 2000. Zbl 0958.11076

[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, 1969. MR 41 #5348 Zbl 0197.01403

[Childs 1989] L. N. Childs, "On the Hopf Galois theory for separable field extensions", *Comm. Algebra* **17**:4 (1989), 809–825. MR 90g:12003 Zbl 0692.12007

[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

[Dixon 1971] J. D. Dixon, "Maximal abelian subgroups of the symmetric groups", *Canad. J. Math.* **23** (1971), 426–438. MR 43 #7496 Zbl 0213.03301

[GAP Group 2002] GAP Group, "GAP: groups, algorithms, and programming", 2002, Available at http://www.gap-system.org. Version 4.3.

[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

[Isaacs 1976] I. M. Isaacs, *Character theory of finite groups*, Pure and Applied Mathematics **69**, Academic Press, New York, 1976. MR 57 #417 Zbl 0337.20005

[Kohl 2007] T. Kohl, "Groups of order $4p$, twisted wreath products and Hopf–Galois theory", *J. Algebra* **314**:1 (2007), 42–74. MR 2008e:12001 Zbl 1129.16031

[Krasner and Kaloujnine 1951] M. Krasner and L. Kaloujnine, "Produit complet des groupes de permutations et problème d'extension de groupes, III", *Acta Sci. Math. Szeged* **14** (1951), 69–82. MR 14,242d Zbl 0045.30301

[Moody 1994] J. A. Moody, *Groups for undergraduates*, World Scientific, River Edge, NJ, 1994. MR 96e:20001 Zbl 0832.20001

[Neumann 1963] B. H. Neumann, "Twisted wreath products of groups", *Arch. Math.* (*Basel*) **14** (1963), 1–6. MR 26 #5040 Zbl 0108.02602

[Ore 1942] O. Ore, "Theory of monomial groups", *Trans. Amer. Math. Soc.* **51**:1 (1942), 15–64. MR 3,197e Zbl 0028.00304

[Wielandt 1955] H. Wielandt, *Permutationsgruppen*, Mathematische Institut, Tübingen, 1955. Translated as *Finite permutation groups*, Academic Press, New York, 1964. MR 32 #1252 Zbl 0138.02501

Communicated by Susan Montgomery
Received 2012-09-08 Revised 2013-02-02 Accepted 2013-03-11

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

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

The subscription price for 2013 is US $200/year for the electronic version, and $350/year (+$40, 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 Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 7 No. 9 2013

1937-0652(2013)7:9;1-4