Groups of Order 4p, Twisted Wreath Products and Hopf-Galois Theory

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

March 12, 2007

Abstract

The work of Greither and Pareigis details the enumeration of the Hopf-Galois structures (if any) on a given separable field extension. We consider the cases where L/K is already classically Galois with $\Gamma = Gal(L/K)$, where $|\Gamma| = 4p$ for $p > 3$ a prime. The goal is to determine those regular (transitive and fixed point free) subgroups N of $Perm(\Gamma)$ that are normalized by the left regular representation of Γ. A key fact that aids in this search is the observation that any such regular subgroup, necessarily of order $4p$, has a unique subgroup of order p. This allows us to show that all such N are contained in a 'twisted' wreath product, a subgroup of high index in $Perm(\Gamma)$ which has a very computationally convenient description that allows us to perform the aforementioned enumeration.

Key words: Hopf-Galois extension, Greither-Pareigis theory, regular subgroup, holomorph, block structure, wreath product

The author wishes to express his thanks to the referee for suggestions regarding the exposition, and to Lindsay Childs and Dan Replogle for getting me interested in this material again.

1 Preliminaries

The general theory of Hopf algebras and Hopf-Galois extensions can be found in references such as [4] and [24] which applies for general extensions of commutative rings. Our focus will be on the case of separable extensions of fields as elucidated in [11]. We give some of the background below.

Given a separable extension of fields L/K, and a K-Hopf algebra H, we say that L/K is H-Galois if there exists a K-algebra homomorphism

$$\mu : H \to End_K(L)$$

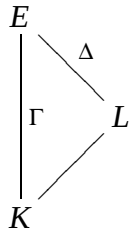
such that

$$\mu(h)(ab) = \sum_{(h)} \mu(h_{(1)})(a)\mu(h_{(2)})(b)$$

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

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

is precisely K and the induced map $1 \otimes \mu : L \otimes H \to End_K(L)$ is an isomorphism of K-algebras. It is easy to check, for example, that a classical Galois extension L/K with $G = Gal(L/K)$ is Hopf-Galois for the K-Hopf algebra $K[G]$. For a general separable extension L/K one proceeds as follows. Let E be the Galois closure of L/K and consider



where Γ and Δ are the relevant Galois groups. If we let $S = \Gamma/\Delta$ then S has a natural Γ-action and there is, correspondingly, an induced map $\Gamma \to B = Perm(S)$. A *regular* subgroup N of B is one that acts transitively and fixed-point freely, a consequence of this is that $|N| = |S| = [L : K]$. The following shows how one enumerates and describes what Hopf algebras (if any) act on L/K to make it Hopf-Galois.

Theorem 1.1: *[11, Theorem 2.1] Let L/K be a separable field extension with E, S and B as above, then there is a bijection between*

(a) K-Hopf algebras H making L/K H-Galois

(b) regular subgroups $N \leq B$ normalized by $\Gamma \leq B$.

If L/K is H-Galois then $E \otimes_K H \cong E[N]$ for N a regular subgroup B normalized by Γ. Conversely, if N is a regular subgroup of B normalized by Γ then $H = (E[N])^\Gamma$ (the fixed ring under the diagonal action of Γ) is a Hopf algebra which acts to make L/K an H-Galois extension. Although structural questions are interesting in their own right, our focus in this discussion is on determining the number and type of those N that arise for a given Γ.

The enumerative question requires the determination of the regular subgroups N normalized by the image of Γ under the induced map mentioned above. It may happen that some extensions may not afford any Hopf Galois structures. The condition 'Γ normalizes N' translates into the condition $\lambda(\Gamma) \leq Norm_B(N)$ which gives some initial restrictions on what N may arise. For example, if $[L:K] = p > 3$ (prime) and $\Gamma \cong S_p$ then, by necessity, $N \cong C_p$ and so $|Norm_B(N)| = p(p-1)$. But since $|\Gamma| = p!$ the aforementioned containment is impossible and there is no Hopf-Galois structure on L/K. Conversely, for a given extension, there may be more than one Hopf-Galois structure. Much recent work in this area has been on the case where L/K is already classically Galois, whence $E = L$, $\Delta = \{1\}$ and, $S = \Gamma$. For an extension L/K with $\Gamma = Gal(L/K)$, the classical action (i.e. $H = K[\Gamma]$) corresponds to $N = \rho(\Gamma)$ where ρ is the *right* regular representation of Γ in $B = Perm(\Gamma)$. The reason for this is that $\lambda(\Gamma)$ centralizes $\rho(\Gamma)$ so the diagonal action reduces to Γ acting on L. However, it is possible for other Hopf Galois structures to arise. Indeed, if Γ is non-abelian then $\lambda(\Gamma)$ certainly normalizes itself so $N = \lambda(\Gamma)$ will yield a *different* Hopf Galois structure on L/K since $\lambda(\Gamma) \neq \rho(\Gamma)$.

The search for N that satisfy the Greither-Pareigis criteria involves, ostensibly, searching in all of B. However, as $|\Gamma|$ increases, B obviously becomes very large. This motivated the approach developed in [2] by Byott. Specifically, if $N \leq B = Perm(\Gamma)$ is regular and normalized by $\lambda(\Gamma)$ then, by regularity, the map $b : N \to \Gamma$ given by $b(n) = ne_\Gamma$ induces an isomorphism

$$B = Perm(\Gamma) \to Perm(N)$$

where $\lambda(\Gamma) \mapsto \Gamma'$ (isomorphic to Γ) and $N \mapsto \lambda(N)$. Considering Γ' as a subgroup of $Hol(N) = Norm_{Perm(N)}(\lambda(N))$, Byott's technique is to enumerate the embeddings of Γ (regarded as Γ') into $Hol(N)$, modulo conjugation by $Aut(N)$. This requires, of course, considering the isomorphism classes of those N which can arise and then determining these 'regular embeddings' up to conjugation by $Aut(N)$.

The Galois extensions we shall be considering are those L/K for which $[L:K] = 4p$ for $p > 3$ a prime. The idea of exploring these is, in some sense, the next step up in complexity from the pq (for primes $p \neq q$) case studied recently in [3]. However, instead of the two possible classes of groups of order pq, there are five classes of groups of order $4p$ if $p \equiv 1 \ (mod\ 4)$, and four if $p \equiv 3$. As such we have either 16 or 25 possible 'pairings' of isomorphism classes of Γ and N to explore.

We also seek to avoid the problem of the growing size of B, while still working within the original Greither-Pareigis framework. We shall consider the N as distinct subgroups of $B = Perm(\Gamma) \cong S_{4p}$ and not use Byott's technique. Our approach is based on the fact that groups of order $4p$ for $p > 3$ have a unique p-Sylow subgroup. As such, we will show that all the N normalized by $\lambda(\Gamma)$ lie within a solvable, high index subgroup of B, and that the structure of this subgroup makes the determination of the given N rather straightforward, and allow us to examine the relationships between the various N. In addition, we shall examine when, for distinct N and N', one has $Norm_B(N) = Norm_B(N')$ since if $\lambda(\Gamma) \leq Norm_B(N)$ then obviously $\lambda(\Gamma) \leq Norm_B(N')$ as well. This symmetry exists, for example, between $N = \lambda(\Gamma)$ and $N' = \rho(\Gamma)$ for Γ non-abelian. We shall see that there are many N related in this way, some for which the underlying N are *not* isomorphic as abstract groups!

Definition 1.2:

- $B = Perm(\Gamma) \cong S_{|\Gamma|}$
- $R(\Gamma) = \{N \leq B | N \text{ regular, } \lambda(\Gamma) \leq Norm_B(N)\}$
- $R(\Gamma, [M]) = \{N \in R(\Gamma) |\ N \cong M\}$
- $Hol(\Gamma) = Norm_B(\lambda(\Gamma))$

Note that we shall, in general, use the term $Hol(N)$ to mean $Norm_{Perm(N)}(N)$ for any given N.

Observe that for a given Γ we determine $R(\Gamma)$ by determining $R(\Gamma,[M])$ for all isomorphism classes of groups $[M]$ where $|\Gamma| = |M|$. As such, one first needs to determine which classes are possible.

2 Groups of Order 4p

Proposition 2.1: *The groups Γ of order $4p$, for $p > 3$ a prime are*

$$
\begin{aligned}
C_{4p} &= \{x | x^{4p} = 1\} \\
C_p \times V &= \{x, t_1, t_2 | x^p = 1, t_1^2 = 1, t_2^2 = 1, abelian\} \\
D_{2p} &= \{x, t |\ x^{2p} = 1, t^2 = 1, xt = tx^{-1}\} \\
Q_p &= \{x, t |\ x^{2p} = 1, t^2 = x^p, xt = tx^{-1}\} \\
&\quad and\ for\ p \equiv 1 (mod 4) \\
E_p &= \{x, t | x^p = 1, t^4 = 1, txt^{-1} = x^\zeta\} \\
&\quad where\ \zeta, \overline{\zeta} = \zeta^{-1} = -\zeta\ are\ the\ elements\ of\ order\ 4\ in\ U_p = (\mathbb{Z}/p\mathbb{Z})^*
\end{aligned}
$$

Observe that D_{2p} may also be presented as a split extension of C_p by V (the Klein four group) that is $\langle x^2, x^p, t\rangle$, and that Q_p may be presented as $\{y, t | y^p = 1, t^4 = 1, yt = ty^{-1}\}$ (where $y = x^2$) so that both it and E_p are split extensions of C_p by C_4. Note, for $p = 3$ we have C_{12}, $C_3 \times C_2 \times C_2$,$D_6$, Q_3 and A_4, where A_4 is, of course, not a split extension. The reason we use the presentations for D_{2p} and Q_p in the statement of the proposition is to emphasize that both are extensions of C_{2p}, a fact which will be important in 3.10.

Since we will be considering regular subgroups normalized by the left regular representation of Γ, for each of the five possibilities above, we need to compute the cycle structure of the generators of the left regular representations.

Proposition 2.2: *We give the left regular representations of the generators of each group Γ of order $4p$ and include, for reference, the representations of elements of order p in C_{4p}, D_{2p} and Q_p.*

(a) For $\Gamma = C_{4p}$, we have $\Gamma = \{1, x, \cdots, x^{4p-1}\}$ and

$$\lambda(x) = (1 \;\; x \;\; \cdots \;\; x^{4p-1})$$
$$\lambda(x^4) = (1 \;\; x^4 \cdots x^{4(p-1)})(x^2 \cdots x^{4(p-1)+2})(x \cdots x^{4(p-1)+1})(x^3 \cdots x^{4(p-1)+3})$$

(b) For $\Gamma = C_p \times V$, we have

$$\Gamma = \{x^k t_1^i t_2^j | k = 0, \ldots, p-1; i = 0, 1; j = 0, 1\}$$

and

$$\lambda(x) = (1 \;\; x \cdots x^{p-1})(t_1 \;\; t_1 x \cdots t_1 x^{p-1})(t_2 \;\; t_2 x \cdots t_2 x^{p-1})(t_1 t_2 \;\; t_1 t_2 x \cdots t_1 t_2 x^{p-1})$$
$$\lambda(t_1) = (1 \;\; t_1)(x \;\; t_1 x) \cdots (x^{p-1} \;\; t_1 x^{p-1})(t_2 \;\; t_1 t_2)(t_2 x \;\; t_1 t_2 x) \cdots (t_2 x^{p-1} \;\; t_1 t_2 x^{p-1})$$
$$\lambda(t_2) = (1 \;\; t_2)(x \;\; t_2 x) \cdots (x^{p-1} \;\; t_2 x^{p-1})(t_1 \;\; t_1 t_2)(t_1 x \;\; t_1 t_2 x) \cdots (t_1 x^{p-1} \;\; t_1 t_2 x^{p-1})$$

(c) For $\Gamma = E_p$ we have $\Gamma = \{t^i x^j | i = 0, \ldots, 3; j = 0, \ldots, p-1\}$ and

$$\lambda(x) = (1 \;\; x \;\; x^2 \cdots x^{p-1})(t^2 \;\; t^2 x^{-1} \cdots t^2 x^{-(p-1)})(t \;\; t x^{\zeta} \cdots t x^{(p-1)\zeta})(t^3 \;\; t^3 x^{\overline{\zeta}} \cdots t^3 x^{(p-1)\overline{\zeta}})$$
$$\lambda(t) = (1 \;\; t \;\; t^2 \;\; t^3)(x \;\; tx \;\; t^2 x \;\; t^3 x) \cdots (x^{p-1} \;\; t x^{p-1} \;\; t^2 x^{p-1} \;\; t^3 x^{p-1})$$

(d) For $\Gamma = D_{2p}$ we have $\Gamma = \{t^i x^j | i = 0, 1; j = 0, \ldots, 2p-1\}$ and

$$\lambda(x) = (1 \;\; x \cdots x^{2p-1})(t \;\; t x^{2p-1} \cdots t x)$$
$$\lambda(t) = (1 \;\; t)(x \;\; tx) \cdots (x^{2p-1} \;\; t x^{2p-1})$$
$$\lambda(x^2) = (1 \;\; x^2 \cdots x^{2p-2})(x \;\; x^3 \cdots x^{2p-1})(t \;\; t x^{2p-2} \cdots t x^2)(t x \;\; t x^{2p-1} \cdots t x^3)$$

(e) For $\Gamma = Q_p$ we have $\Gamma = \{t^i x^j | i = 0, 1; j = 0, \ldots, 2p-1\}$ and

$$\lambda(x) = (1 \;\; x \cdots x^{2p-1})(t \;\; t x^{2p-1} \cdots t x)$$
$$\lambda(t) = (1 \;\; t \;\; x^p \;\; t x^p)(x \;\; tx \;\; x^{p+1} \;\; t x^{p+1}) \cdots (x^{p-1} \;\; t x^{p-1} \;\; x^{2p-1} \;\; t x^{2p-1})$$
$$\lambda(x^2) = (1 \;\; x^2 \cdots x^{2p-2})(x \;\; x^3 \cdots x^{2p-1})(t \;\; t x^{2p-2} \cdots t x^2)(t x \;\; t x^{2p-1} \cdots t x^3)$$

Proof. These calculations are based on the group laws in each of the five groups in question, based on the presentations in 2.1. □

As we will need this information later on when calculating normalizers, we include the following.

Proposition 2.3:

$$\begin{aligned}
Aut(C_{4p}) &\cong U_{4p} = (\mathbb{Z}/4p\mathbb{Z})^* \\
Aut(C_p \times V) &\cong U_p \times GL_2(\mathbb{Z}/2\mathbb{Z}) \cong U_p \times S_3 \\
Aut(D_{2p}) &= \{\phi_{i,j} | i \in \mathbb{Z}_{2p}; j \in U_{2p}\} \\
&\quad \text{where } \phi_{i,j}(t^a x^b) = t^a x^{ia+jb} \text{ and } \phi_{i_2,j_2} \circ \phi_{i_1,j_1} = \phi_{i_2+j_2 i_1, j_2 j_1} \\
Aut(Q_p) &= \{\phi_{i,j} | i \in \mathbb{Z}_{2p}; j \in U_{2p}\} \\
&\quad \text{where } \phi_{i,j}(t^a x^b) = t^a x^{ia+jb} \text{ and } \phi_{i_2,j_2} \circ \phi_{i_1,j_1} = \phi_{i_2+j_2 i_1, j_2 j_1} \\
Aut(E_p) &= \{\phi_{i,j} | i \in \mathbb{Z}_p; j \in U_p\} \\
&\quad \text{where } \phi_{i,j}(t^a x^b) = t^a x^{ia+jb} \text{ and } \phi_{i_2,j_2} \circ \phi_{i_1,j_1} = \phi_{i_2+j_2 i_1, j_2 j_1}
\end{aligned}$$

Proposition 2.4: *For $p > 3$ prime, each group of order $4p$ has a unique (hence characteristic) subgroup of order p.*

Proof. If n is the number of p-Sylow subgroups, then, of course, $n \equiv 1 (mod\ p)$ and $n|4$ imply $n = 1$. For $p = 3$ we observe that A_4 has three subgroups of order 3. □

Proposition 2.5: *If N is a regular subgroup of B and $K \leq N$ is characteristic, then $K \triangleleft Norm_B(N)$.*

Proof. This is essentially the definition of characteristic subgroup, as in [12, p.31] for example. We note that if $N = \Gamma$ then $Norm_B(\Gamma) = Hol(\Gamma)$ and we have exactly [23, 9.2.3]. □

With this in mind, we note also that if $\lambda(\Gamma) \leq Norm_B(N)$ with $K \leq N$ characteristic, then $\lambda(\Gamma) \leq Norm_B(K)$.

Definition 2.6: Given Γ, let $\mathcal{P}$ be the unique p-Sylow subgroup of $\lambda(\Gamma)$

Our ultimate goal is to show:

Theorem 4.4 If $N \in R(\Gamma)$ then $N \leq Norm_B(\mathcal{P})$.

With this we shall be able to construct and enumerate all the $N \in R(\Gamma)$.

As a first step, we need to understand the relationships between $\mathcal{P}$ and the p-Sylow subgroup of any $N \in R(\Gamma)$.

Proposition 2.7: *If $\mathcal{P}$ is the unique order p subgroup of $\lambda(\Gamma) \leq B$ then $\mathcal{P} = \langle \pi_1\pi_2\pi_3\pi_4 \rangle$ where the π_i are disjoint p-cycles. Also, if P is any order p subgroup of a regular subgroup N then $\mathcal{P}$ normalizes P if and only if it centralizes P and, moreover, $P = \langle \pi_1^{a_1}\pi_2^{a_2}\pi_3^{a_3}\pi_4^{a_4} \rangle$ where $a_i \in \{1 \dots p-1\}$.*

Proof. In a regular permutation group, all non-identity elements act without fixed points. As such, if π is an element of order p in a regular permutation group of order $4p$, then it must be a product of the form $\pi_1\pi_2\pi_3\pi_4$ where the π_i are disjoint p-cycles. If P is generated by $\varepsilon = \varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4$, a product of disjoint p-cycles then, since $\pi_1\pi_2\pi_3\pi_4$ has order p, if it normalizes $\langle \varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4 \rangle$ then it must centralize since the automorphism group of a cyclic group of order p has no p-torsion. Therefore $\pi\varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4\pi^{-1} = \varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4$. As such, $\pi\varepsilon_i\pi^{-1} = \varepsilon_j$, i.e. π permutes the ε_i themselves, but as $|\pi| = p$ this must be a trivial permutation, therefore $\pi\varepsilon_i\pi^{-1} = \varepsilon_i$ for each i. As a consequence, we must have $\pi(Supp(\varepsilon_i)) = Supp(\varepsilon_i)$ for each i, where $Supp(\varepsilon_i)$ is the support of ε_i. What we wish to show is that $\pi_i(Supp(\varepsilon_j)) = Supp(\varepsilon_j)$ for each i and j. The point being that, after renumbering if necessary, $Supp(\pi_i) = Supp(\varepsilon_i)$. For example, if $x \in Supp(\pi_1) \cap Supp(\varepsilon_1)$ and $y \in Supp(\pi_1) \cap Supp(\varepsilon_2)$ then as a p-cycle, $\pi_1 = (\dots x \dots y \dots)$. Now if π centralizes then so does π^e for any e and so we may assume that

$\pi_1 = (\ldots x\ y \ldots)$, that is $\pi_1(x) = y$. As such $\pi(x) = \pi_1\pi_2\pi_3\pi_4(x) = \pi_1(x) = y$ since the π_i are disjoint cycles. However $x \in Supp(\varepsilon_1)$ but $y \in Supp(\varepsilon_2)$ which contradicts the fact that $\pi(Supp(\varepsilon_1)) = Supp(\varepsilon_1)$. Therefore, we may assume that, indeed, $Supp(\varepsilon_i) = Supp(\pi_i)$ and therefore that $\pi_i\varepsilon_i\pi_i^{-1} = \varepsilon_i$. If $\varepsilon_i = (z\ \varepsilon_i(z)\ \varepsilon_i^2(z) \ldots \varepsilon_i^{p-1}(z))$ for some $z \in Supp(\varepsilon_i)$ then

$$\begin{aligned}\pi_i\varepsilon_i\pi_i^{-1} &= (\pi_i(z)\ \pi_i(\varepsilon_i(z))\ \pi_i(\varepsilon_i^2(z))\ \ldots\ \pi_i(\varepsilon_i^{p-1}(z))) \\ &= (z\ \varepsilon_i(z)\ \varepsilon_i^2(z)\ \ldots\ \varepsilon_i^{p-1}(z))\end{aligned}$$

which means that $z = \pi_i(\varepsilon_i^k(z))$ for some non-zero k and so, as ordered sets,

$$\{z, \varepsilon_i(z), \ldots, \varepsilon_i^{p-1}(z)\} = \{\pi_i(\varepsilon_i^k(z)), \pi_i(\varepsilon_i^{k+1}(z)), \ldots, \pi_i(\varepsilon_i^{k+p-1}(z))\}$$

to wit $\pi_i\varepsilon_i^k = id$ that is π_i is a power of ε_i, but since k is non-zero (hence a unit mod p) and ε_i and π_i have order p, then similarly ε_i is a non-zero power of π_i. □

Definition 2.8: Given $\pi_1, \pi_2, \pi_3, \pi_4$ as above, and $(i_1, i_2, i_3, i_4) \in \mathbb{F}_p^4$ we define $[i_1, i_2, i_3, i_4] = \pi_1^{i_1}\pi_2^{i_2}\pi_3^{i_3}\pi_4^{i_4}$ and set $\hat{0} = [0, 0, 0, 0]$.

Definition 2.9: Given $\mathcal{P} = \langle \pi_1\pi_2\pi_3\pi_4 \rangle$ as in 2.6 and 2.7 above, let

$$\begin{aligned}\hat{p}_1 &= [\ 1,\ 1,\ 1,\ 1] \text{ and let } P_1 = \langle \hat{p}_1 \rangle \\ \hat{p}_2 &= [1, 1, -1, -1] \text{ and let } P_2 = \langle \hat{p}_2 \rangle \\ \hat{p}_3 &= [1, -1, 1, -1] \text{ and let } P_3 = \langle \hat{p}_3 \rangle \\ \hat{p}_4 &= [1, -1, -1, 1] \text{ and let } P_4 = \langle \hat{p}_4 \rangle\end{aligned}$$

and for $p \equiv 1\ (mod\ 4)$ with $\zeta, \overline{\zeta}$ the two elements of order 4 in U_p that arise in the presentation of E_p in 2.1, let

$$\begin{aligned}\hat{p}_5 &= [1, -1, \zeta, \overline{\zeta}] \text{ and let } P_5 = \langle \hat{p}_5 \rangle \\ \hat{p}_6 &= [1, -1, \overline{\zeta}, \zeta] \text{ and let } P_6 = \langle \hat{p}_6 \rangle\end{aligned}$$

Observe that $\mathcal{P} = P_1$ for all Γ.

Proposition 2.10: *If $N \in R(\Gamma)$ then $|N| = 4p$ and, as such, N has a unique p-Sylow subgroup $P(N)$ of order p. With respect to $\mathcal{P}$ associated to $\lambda(\Gamma)$, $P(N)$ must be one of the following (if necessary by renumbering the π_i for a given Γ):*

(a) If $\Gamma = C_{4p}$ then $P(N) \in \{P_1, P_2, P_5, P_6\}$ if $p \equiv 1 (mod\ 4)$,

otherwise $P(N) \in \{P_1, P_2\}$.

(b) If $\Gamma = C_p \times V$ then $P(N) \in \{P_1, P_2, P_3, P_4\}$.

(c) If $\Gamma = E_p$ then $P(N) \in \{P_1, P_2, P_5, P_6\}$ if $p \equiv 1 (mod\ 4)$.

(d) If $\Gamma = D_{2p}$ then $P(N) \in \{P_1, P_2, P_3, P_4\}$.

(e) If $\Gamma = Q_p$ then $P(N) \in \{P_1, P_2, P_5, P_6\}$ if $p \equiv 1 (mod\ 4)$,

otherwise $P(N) \in \{P_1, P_2\}$.

Proof. (a) For $\Gamma = C_{4p}$ we observe that

$$\begin{aligned}\hat{p}_1 = \lambda(x^4) &= (1x^4 \cdots x^{4(p-1)})(x^2 \cdots x^{4(p-1)+2})(x \cdots x^{4(p-1)+1})(x^3 \cdots x^{4(p-1)+3}) \\ &= \pi_1\pi_2\pi_3\pi_4\end{aligned}$$

and

$$\lambda(x^p) = (1\ x^p\ x^{2p}\ x^{3p})(x\ x^{p+1}\ x^{2p+1}\ x^{3p+1}) \cdots (x^{p-1}\ x^{2p-1}\ x^{3p-1}\ x^{4p-1})$$

and that $\lambda(x^p)$ centralizes P_1 which means that conjugating by $\lambda(x^p)$ shuffles the π_i in some fashion. Consider $\lambda(x^p)\pi_1\lambda(x^p)^{-1}$, this yields a p-cycle which contains x^p. The question is which π_i contains x^p in its support? Observe that $\pi_1 = (x^{4k})$, $\pi_2 = (x^{4k+2})$, $\pi_3 = (x^{4k+1})$ and $\pi_4 = (x^{4k+3})$ for $k = 0 \ldots p-1$, and therefore $x^p = x^{4k+i}$ for some i. If $p \equiv 1 (mod\ 4)$ then x^p is in the support of π_3 and if $p \equiv 3 (mod\ 4)$ then x^p lies in the support of π_4. In a similar

fashion, we find that $\lambda(x^p)\pi_2\lambda(x^p)^{-1} = \pi_4$ if $p \equiv 1$ or π_3 if $p \equiv 3$. In summary we have

$$\pi_1\pi_2\pi_3\pi_4 \overset{p\equiv 1}{\mapsto} \pi_3\pi_4\pi_2\pi_1$$
$$\pi_1\pi_2\pi_3\pi_4 \overset{p\equiv 3}{\mapsto} \pi_4\pi_3\pi_1\pi_2$$

As observed in 2.7, with respect to the π_i that generate $\mathcal{P}$, we must have that $P(N)$ is generated by $\pi_1^{a_1}\pi_2^{a_2}\pi_3^{a_3}\pi_4^{a_4} = [a_1, a_2, a_3, a_4]$ and so we observe that $P(N)$ must be normalized by the generators of $\lambda(\Gamma)$. We therefore determine what restrictions this places on the a_i. For $p \equiv 1(mod\ 4)$ we have

$$\lambda(x^p)[a_1, a_2, a_3, a_4]\lambda(x^p)^{-1} = [a_4, a_3, a_1, a_2]$$

but we must have $[a_4, a_3, a_1, a_2] = [ua_1, ua_2, ua_3, ua_4]$ for some $u \in U_p$ which means that

$$a_4 = ua_1$$
$$a_3 = ua_2$$
$$a_1 = ua_3$$
$$a_2 = ua_4$$

and based on this, we have that $u^4 = 1$ which means that u belongs to $\{1, -1, \zeta, \overline{\zeta}\}$. By direct calculation we have the following:

$$\begin{aligned}
u = 1 \qquad & P(N) = \langle [1,1,1,1] \rangle = P_1 \\
u = -1 \qquad & P(N) = \langle [1,1,-1,-1] \rangle = P_2 \\
u = \zeta \qquad & P(N) = \langle [1,-1,\overline{\zeta},\zeta] \rangle = P_6 \\
u = \overline{\zeta} \qquad & P(N) = \langle [1,-1,\zeta,\overline{\zeta}] \rangle = P_5
\end{aligned}$$

For example, if $u = -1$ then $a_4 = -a_1$, $a_3 = -a_2$, $a_1 = -a_3$, and $a_2 = -a_4$ which means that $[a_1, a_2, a_3, a_4] = [a_1, a_1, -a_1, -a_1] = a_1[1, 1, -1, -1]$. Now, for $p \equiv 3(mod\ 4)$ we have $\lambda(t)[a_1, a_2, a_3, a_4]\lambda(t)^{-1} = [a_3, a_4, a_2, a_1] = [ua_1, ua_2, ua_3, ua_4]$ which again implies that $u^4 = 1$ which means that $u \in \{\pm 1\}$ since these are

the only units in U_p with this property. As such, we have

$$u = 1 \to P(N) = \langle [1,1,1,1] \rangle = P_1$$
$$u = -1 \to P(N) = \langle [1,1,-1,-1] \rangle = P_2$$

(b) For $\Gamma = C_p \times V$ we have

$$\begin{aligned}\hat{p}_1 &= (1\ x \cdots x^{p-1})(t_1\ t_1 x \cdots t_1 x^{p-1})(t_2\ t_2 x \cdots t_2 x^{p-1})(t_1 t_2\ t_1 t_2 x \cdots t_1 t_2 x^{p-1}) \\ &= \pi_1 \pi_2 \pi_3 \pi_4\end{aligned}$$

and it is readily shown that

$$\lambda(t_1)(\pi_1 \pi_2 \pi_3 \pi_4)\lambda(t_1)^{-1} = \pi_2 \pi_1 \pi_4 \pi_3$$

and

$$\lambda(t_2)(\pi_1 \pi_2 \pi_3 \pi_4)\lambda(t_2)^{-1} = \pi_3 \pi_4 \pi_1 \pi_2$$

As to the possible choices of $P(N)$ we argue as in (a) but here we consider the action of two generators t_1 and t_2 and find that $\lambda(t_1)[a_1,a_2,a_3,a_4]\lambda(t_1)^{-1} = [a_2,a_1,a_4,a_3] = [ua_1,ua_2,ua_3,ua_4]$ and $\lambda(t_2)[a_1,a_2,a_3,a_4]\lambda(t_2)^{-1} = [a_3,a_4,a_1,a_2] = [va_1,va_2,va_3,va_4]$ for units u,v. Analyzing the resulting relations shows that $u^2 = 1$ and $v^2 = 1$ and as such, $u = \pm 1$ and $v = \pm 1$. We now see what $P(N)$ arise due to the four choices for (u,v), to wit

$$\begin{aligned}(u,v) &= (1,1) & P(N) &= \langle [1,1,1,1] \rangle = P_1 \\ (u,v) &= (1,-1) & P(N) &= \langle [1,1,-1,-1] \rangle = P_2 \\ (u,v) &= (-1,1) & P(N) &= \langle [1,-1,1,-1] \rangle = P_3 \\ (u,v) &= (-1,-1) & P(N) &= \langle [1,-1,-1,1] \rangle = P_4\end{aligned}$$

(c) For $\Gamma = E_p$ we have

$$\begin{aligned}\hat{p}_1 &= (1\ x\ x^2 \cdots x^{p-1})(t^2\ t^2 x^{-1} \cdots t^2 x^{-(p-1)})(t\ t x^{\zeta} \cdots t x^{(p-1)\zeta})(t^3\ t^3 x^{\overline{\zeta}} \cdots t^3 x^{(p-1)\overline{\zeta}}) \\ &= \pi_1 \pi_2 \pi_3 \pi_4\end{aligned}$$

and consequently that $\lambda(t)\pi_1\pi_2\pi_3\pi_4\lambda(t)^{-1} = \pi_3^{\overline{\zeta}}\pi_4^{\overline{\zeta}}\pi_2^{\overline{\zeta}}\pi_1^{\overline{\zeta}}$. Keeping in mind that $p \equiv 1(mod\ 4)$ we again have elements of order 4 in U_p and by the same method used in (a) and (b) we conclude that the only possibilities for $P(N)$ are $\{P_1, P_2, P_5, P_6\}$

(d) For $\Gamma = D_{2p}$ we have

$$\begin{aligned}\hat{p}_1 = \lambda(x^2) &= (1\ x^2 \cdots x^{2p-2})(x\ x^3 \cdots x^{2p-1})(t\ tx^{2p-2} \cdots tx^2)(tx\ tx^{2p-1} \ldots tx^3) \\ &= \pi_1\pi_2\pi_3\pi_4\end{aligned}$$

and we observe that

$$\lambda(x^p)(\pi_1\pi_2\pi_3\pi_4)\lambda(x^p)^{-1} = \pi_2\pi_1\pi_4\pi_3$$

and

$$\lambda(t)(\pi_1\pi_2\pi_3\pi_4)\lambda(t)^{-1} = \pi_3^{-1}\pi_4^{-1}\pi_1^{-1}\pi_2^{-1}$$

Here, the possible choices for $P(N)$ are $\{P_1, P_2, P_3, P_4\}$ regardless of whether $p \equiv 1$ or $p \equiv 3$.

(e) For $\Gamma = Q_p$ we have

$$\begin{aligned}\hat{p}_1 &= (1\ x^2 \cdots x^{2p-2})(x\ x^3 \cdots x^{2p-1})(t\ tx^{2p-2} \cdots tx^2)(tx\ tx^{2p-1} \cdots tx^3) \\ &= \pi_1\pi_2\pi_3\pi_4\end{aligned}$$

and calculate that $\lambda(t)(\pi_1\pi_2\pi_3\pi_4)\lambda(t)^{-1} = \pi_3^{-1}\pi_4^{-1}\pi_2^{-1}\pi_1^{-1}$. Here, we find that for $p \equiv 1(mod\ 4)$, $P(N) \in \{P_1, P_2, P_5, P_6\}$ and for $p \equiv 3(mod\ 4)$, $P(N) \in \{P_1, P_2\}$.

□

3 Regular Subgroups with Identical Normalizers

As alluded to in the introduction, there are certain symmetries amongst the $R(\Gamma)$ which arise due to having $Norm_B(N) = Norm_B(N')$ for distinct N,N'.

The first of these parallels the relationship between $\lambda(\Gamma)$ and $\rho(\Gamma)$, culminating in 3.9. The second, 3.11, is due to a classical relationship between the holomorphs of dihedral and quaternionic groups of the same order. Along the way, we shall make a number of general observations about the structure of $Norm_B(N)$ which will be crucial in the next section. We remind the reader that $R(\Gamma)$ is the set of those regular subgroups $N \leq B = Perm(\Gamma)$ normalized by $\lambda(\Gamma)$.

For a given regular subgroup N embedded in B, there is a related group which is presented in different ways, e.g. in [19] or [11], but which is essentially the following.

Definition 3.1: If $N \leq B$ is a regular subgroup, then let $N^{opp} = Cent_B(N)$, the centralizer of N in B.

One key fact about the opposite group is this.

Proposition 3.2: *For $N \leq B$ a regular subgroup, N^{opp} is also a regular subgroup.*

Proof. One can construct N^{opp} directly as in [11, Lemma 2.4.2]. For $\gamma \in \Gamma$ let n_γ be the element of N such that $n_\gamma(1) = \gamma$. Then for any $n \in N$, let ϕ_n be given by $\phi_n(\gamma) = n_\gamma n(1)$ whereby $Cent_B(N) = \{\phi_n | n \in N\}$. The regularity of N^{opp} is readily verified. Note also that, for $N = \lambda(\Gamma)$, one has $N^{opp} = \rho(\Gamma)$. □

Various other facts about a regular subgroup and its opposite must also be noted.

Proposition 3.3: $N \cap N^{opp} = Z(N)$

Proof. If $n \in N \cap N^{opp}$ then for all $n' \in N$, we have $nn' = n'n$, as such $n \in Z(N)$, the reverse containment is trivial as $Z(N) \leq N^{opp}$. □

Corollary 3.4: *If N is regular and abelian, then $N = N^{opp}$.*

In 4.1 we will see a subtle but important consequence of this property. We should also mention this relatively obvious fact about the $(\ )^{opp}$ operation.

Lemma 3.5: *For N a regular subgroup of B, $(N^{opp})^{opp} = N$.*

Proof. The elements of $(N^{opp})^{opp}$ are those which commute with all elements of N^{opp}, hence $N \leq (N^{opp})^{opp}$. However, since the opposite of a regular subgroup is regular, then $(N^{opp})^{opp}$ is regular and so $|\Gamma| = |N| = |(N^{opp})^{opp}|$ and the result follows. □

One of our goals is to show that if $N \in R(\Gamma)$ then $N^{opp} \in R(\Gamma)$ as well. To do this, we examine the structure of $Norm_B(N)$.

Proposition 3.6: *If N is a regular subgroup of B and $z \in \Gamma$ is chosen arbitrarily then $Norm_B(N) = MA_z$ where M is any normal transitive subgroup of $Norm_B(N)$ and $A_z = \{\alpha \in Norm_B(N) | \alpha(z) = z\}$.*

Proof. First observe that if $M \triangleleft Norm_B(N)$ then A_z normalizes M and so MA_z is defined, and clearly $MA_z \leq Norm_B(N)$. Now, if $\delta \in Norm_B(N)$ then $\delta(z) = z'$ and by transitivity, we may choose $\mu \in M$ such that $\mu^{-1}(z') = z$ and therefore $\mu^{-1}\delta(z) = z$ and therefore $\mu^{-1}\delta \in A_z$, and so $Norm_B(N) \leq MA_z$. Note, if M is regular then $M \cap A_z = \{e\}$ and therefore $Norm_B(N) \cong M \rtimes A_z$. □

One should observe how this parallels the classical construction of the holomorph of a group G as a subgroup of $Perm(G)$, as presented in [12], for example. One has that $Hol(G) = Norm_{Perm(G)}(\lambda(G)) = \rho(G)Aut(G)$ where $\rho(G) = \lambda(G)^{opp}$ and $Aut(G)$, the automorphisms of G viewed as an abstract group and as permutations, consists of those elements in $Hol(G)$ that fix the identity element of G, i.e. $Aut(G) = A_{e_G}$. As $\lambda(G)$ is obviously a transitive normal subgroup of $Hol(G)$, one sees that $Hol(G) = \lambda(G)Aut(G)$ as well.

Proposition 3.7: *If N is a regular subgroup of B then all A_z are conjugate, and moreover, $A_z \cong Aut(N)$ and $Norm_B(N) \cong Hol(N)$ as abstract groups.*

Proof. If N is a regular subgroup of $Perm(\Gamma)$ then, as in [2] and [5], we may consider the isomorphism $\phi : Perm(\Gamma) \to Perm(N)$ given by $\phi(\pi) = b^{-1}\pi b$ induced by the bijection $b : N \to \Gamma$ where $b(n) = ne_\Gamma$. Under this mapping N corresponds to $\lambda(N)$ and therefore $Norm_B(N)$ corresponds to $Hol(N)$. One can show that $\phi(A_z) = A_{b^{-1}(z)} \leq Perm(N)$ and $\phi^{-1}(Aut(N)) = \phi^{-1}(A_{e_N}) = A_{e_\Gamma}$. We conclude by observing that $nA_z n^{-1} = A_{n(z)}$ for any $n \in N$ and so $A_z \cong A_{e_\Gamma} \cong Aut(N)$. □

As a consequence, we can, for a given $N \in R(\Gamma)$, find other $N' \in R(\Gamma)$ by looking amongst the subgroups of $Norm_B(N)$ and determining which have the same normalizer.

Proposition 3.8: *Given a regular subgroup N of B and its normalizer $Norm_B(N)$. If M is a normal regular subgroup of $Norm_B(N)$ then $Norm_B(N) \leq Norm_B(M)$. If $Aut(M)$ and $Aut(N)$ have the same order, (in particular if they are isomorphic), then $Norm_B(N) = Norm_B(M)$.*

Proof. If we define

$$A_{z,N} = \{\alpha \in Norm_B(N) | \alpha(z) = z\}$$

and

$$A_{z,M} = \{\alpha \in Norm_B(M) | \alpha(z) = z\}$$

then we have that $Norm_B(N) = NA_{z,N}$ and if M is normal in $Norm_B(N)$ then M is certainly normalized by $A_{z,N}$ and therefore $A_{z,N} \leq A_{z,M}$. By 3.6, $Norm_B(N) = NA_{z,N}$ and also $Norm_B(N) = MA_{z,N}$ and so $Norm_B(N) = NA_{z,N} \leq MA_{z,N} \leq MA_{z,M} = Norm_B(M)$. If $|Aut(N)| = |Aut(M)|$ then by 3.7 we have $|A_{z,N}| = |A_{z,M}|$ and so, by regularity, $|Norm_B(N)| = |N| \cdot |A_{z,N}| = |M| \cdot |A_{z,M}| = |Norm_B(M)|$ and therefore M and N have the same normalizer. □

Corollary 3.9: *$N \in R(\Gamma)$ if and only if $N^{opp} \in R(\Gamma)$.*

Proof. As $N \cong N^{opp}$ then obviously $|Aut(N)| = |Aut(N^{opp})|$ and therefore $Norm_B(N) = Norm_B(N^{opp})$. Thus, $\lambda(\Gamma) \leq Norm_B(N)$ if and only if $\lambda(\Gamma) \leq Norm_B(N^{opp})$. □

There is another possible 'pairing' of two N in a given $R(\Gamma)$. In 2.3, we gave the automorphism groups of the various groups of order $4p$. We observe, and this is well known [9, pp.169–170], [25] and others, that D_{2n} and Q_n have isomorphic automorphism groups for $n \geq 3$, specifically $Aut(D_{2n}) \cong Aut(Q_n) \cong Hol(C_{2n})$. In fact, not only are the automorphism groups of D_{2n} and Q_n isomorphic, but surprisingly, so are their holomorphs. This fact is quoted in [16] and is a consequence of this isomorphism of the automorphism groups. If D_{2n} is presented as $\{t^a x^b | t^2 = 1, x^{2n} = 1, xt = tx^{-1}\}$ and Q_n as $\{t^a x^b | t^2 = x^n, x^{2n} = 1, xt = tx^{-1}\}$ then, as sets, both have the same elements $\{t^a x^b | a = 0,1; b = 0,\ldots,2n-1\}$. If we call this set Z then the left (and right) regular representations of D_{2n} and Q_n (and their resulting normalizers) can all be viewed as subgroups of $Perm(Z)$. We have then the following.

Proposition 3.10: *For $n \geq 3$, $Hol(D_{2n}) = Hol(Q_n)$ as subgroups of $Perm(Z)$.*

Proof. If $t^a x^b$ is in Z then we can define $\rho_d(t^a x^b)(z)$ to be $z(t^a x^b)^{-1}$ where the product is viewed with respect to the group law in D_{2n} and $\rho_q(t^a x^b)(z) = z(t^a x^b)^{-1}$ viewed with respect to the group law in Q_n. If we define $\mathcal{A} = \{\phi_{i,j}\}$ to be the subgroup of $Perm(Z)$ given by $\phi_{i,j}(t^c x^d) = t^c x^{ic+jd}$, then, in the notation of 3.8, $\mathcal{A} = A_{1,D_{2n}}$ and $\mathcal{A} = A_{1,Q_n}$, that is $\mathcal{A}$ is the automorphism group of both D_{2n} and Q_n simultaneously. One can then verify that:

(a) $\rho_q(x^b)\phi_{i,j} = \rho_d(x^b)\phi_{i,j}$

(b) $\rho_q(tx^b)\phi_{i,j} = \rho_d(tx^{b+n})\phi_{i+n,j}$

as permutations of Z, keeping in mind that in the dihedral groups $t^{-1} = t$ while in the quaternionic groups $t^2 = x^n$ and $t^{-1} = t^3 = tx^n$, and that $n \equiv -n \ (mod\ 2n)$. The point is that $Hol(D_{2n}) = \{\rho_d(t^a x^b)\phi_{i,j}\} = \{\rho_q(t^a x^b)\phi_{i,j}\} = Hol(Q_n)$ and that the image of the right regular representation of D_{2n},(resp. Q_n) is a normal subgroup of $Hol(Q_n)$ (resp. $Hol(D_{2n})$) and the result follows by 3.8. □

In light of 3.9 and 3.10 above, we have that $Hol(D_{2n}) = Hol(Q_n)$ and that this single holomorph (normalizer) contains four regular subgroups whose normalizer *is* this one holomorph.

Proposition 3.11: *If D is regular subgroup of B, isomorphic to D_{2p}, then there exists a regular subgroup Q, isomorphic to Q_p, such that*

$$Norm_B(Q) = Norm_B(D) = Norm_B(D^{opp}) = Norm_B(Q^{opp})$$

where D, Q are, of course, distinct from D^{opp} and Q^{opp}.

We then have the following neat fact about dihedral and quaternionic N in $R(\Gamma)$.

Corollary 3.12: *For each Γ of order $4p$, $|R(\Gamma,[D_{2p}])| = |R(\Gamma,[Q_p])|$, and both are divisible by 4.*

4 Containing N inside $Norm_B(\mathcal{P})$

As before, $|\Gamma| = 4p$, $B = Perm(\Gamma)$ and we are looking for regular subgroups N of B normalized by $\lambda(\Gamma)$. In this section we show that any such N is contained in $Norm_B(\mathcal{P})$ for $\mathcal{P}$ the p-Sylow subgroup of $\lambda(\Gamma)$.

Proposition 4.1: *If $N \cong C_{4p}$ or $N \cong C_p \times V$ then the p-Sylow subgroup of $Norm_B(N)$ is $P(N)$, the p-Sylow subgroup of N.*

Proof. First, as observed above, for N a regular subgroup of B, $Norm_B(N) \cong Hol(N) = N \rtimes Aut(N)$. For $N \cong C_{4p}$, $Aut(N) \cong U_{4p}$ and so a typical element of the holomorph is of the form (x^i, u) and this has order p if and only if $u = 1$ and x^i has order p in N, i.e. the unique subgroup of N of order p. For $N \cong C_p \times V$, $Aut(N) \cong U_p \times GL_2(\mathbb{F}_2)$, as such a typical element of the holomorph has the form $(x^i, t_1^j, t_2^k, u, M)$ for $M \in GL_2(\mathbb{F}_2)$ and one can show that this only has order p if it has the form $(x^i, 1, 1, 1, I)$ for $i \neq 0$, i.e. C_p itself. □

Corollary 4.2: *If $N \cong C_{4p}$ or $N \cong C_p \times V$ and $N \in R(\Gamma)$ then $P(N) = \mathcal{P}$.*

Proof. Since the p-Sylow subgroup of $Norm_B(N)$ is $P(N)$ (which has order p) then $\mathcal{P} \leq \lambda(\Gamma) \leq Norm_B(N)$ implies $P(N) = \mathcal{P}$ since $\mathcal{P}$ has order p as well. □

Note that this is a slight refinement of 2.10 (a) and (b) since the above shows that for N abelian we must have $P(N) = \mathcal{P} = P_1$.

Proposition 4.3: *If $N \in R(\Gamma)$ is non-abelian then the p-Sylow subgroup of $Norm_B(N)$ is $P(N) \cdot P(N^{opp}) = P_i P_j$ for $i \neq j$. Moreover, either $P(N) = P_1$ or $P(N^{opp}) = P_1$.*

Proof. For N equal to D_{2p}, Q_p and E_p, we have the automorphism groups as given in 2.3 and therefore can calculate the holomorph of each, and show that each has a unique p-Sylow subgroup isomorphic to $C_p \times C_p$. Now for N non-abelian, 3.3 shows that N and N^{opp} are distinct subgroups, and, in each case, their intersection $Z(N)$ is not of order p. As such, $P(N) \neq P(N^{opp})$ but since the Sylow subgroup of $Norm_B(N)$ is isomorphic to $C_p \times C_p$ and both N and N^{opp} are contained in $Norm_B(N)$ it must be that it is the product $P(N) \cdot P(N^{opp})$. Now, by 2.10 this must be of the form $P_i \cdot P_j$ for the allowable P_i, P_j for the given Γ. The point is that $P_1 = \mathcal{P} \leq P(N) \cdot P(N^{opp})$ and given the way the P_i are defined, one must be P_1. For example, P_1 cannot be contained in $P_2 \cdot P_3$ since this would imply (viewing $[i_1, i_2, i_3, i_4]$ as an element of $\mathbb{F}_p^4$) that $[1,1,1,1] = [r,r,-r,-r] + [s,-s,s,-s]$. □

As a consequence, we have:

Theorem 4.4: *Given Γ, with associated $\mathcal{P}$, and $N \in R(\Gamma)$, then $N \leq Norm_B(\mathcal{P})$.*

Proof. If N is abelian, then $P(N) = \mathcal{P}$ and so N obviously normalizes $\mathcal{P}$. If N is non-abelian then either $\mathcal{P} = P(N)$ and the result again follows immediately, or $\mathcal{P}$ is the (unique) p-Sylow subgroup of N^{opp}, in which case it is characteristic and so, since N centralizes N^{opp}, it normalizes $\mathcal{P}$. □

5 Wreath Products and Structure of $Norm_B(\mathcal{P})$

As any $N \in R(\Gamma)$ must be contained in $Norm_B(\mathcal{P})$, our approach then will require an elucidation of the structure of this normalizer. The following, in its original form is due to Burnside [1, Section 171]. We will subsequently recast it in terms of the definitions and notation we have developed.

Proposition 5.1: *$Cent_B(\mathcal{P}) \cong C_p \wr S_4$, the wreath product of the cyclic group C_p of order p, and S_4 the symmetric group on 4 letters.*

Wreath products arise in a variety of contexts, in particular when one considers permutations which have blocks associated to them.

Definition 5.2: If G is a permutation group acting transitively on a set Z, then a block is a subset $X \subseteq Z$ such that for all $g \in G$ one has $g(X) = X$ or $g(X) \cap X = \emptyset$.

For example, if $G = \langle(1\ 2\ 3\ 4\ 5\ 6)\rangle \leq S_6$ then $X = \{1,3,5\}$ is a block for G. When G acts transitively on Z (for example if G is a *regular* subgroup of $Perm(Z)$) and X is a block for G then the distinct $\{g(X)|g \in G\}$ give a partition of Z and moreover, each $g(X)$ is itself a block for G and all the blocks have the same size.

The following is presented as [8, Exercise 2.6.2] and we paraphrase it here.

Proposition 5.3: *If G acts transitively on Z and X is a block for G, then if $g_1(X), g_2(X), \ldots, g_k(X)$ partition Z then G may be embedded as a subgroup of $Perm(X) \wr S_k \leq Perm(Z)$.*

Given a group H, one has $H \wr S_k \cong (H \times H \cdots \times H) \rtimes S_k$ with k factors of H acted on by S_k via coordinate permutation. For $Perm(X) \wr S_k$ above, the structure is $(Perm(g_1(X)) \times Perm(g_2(X)) \cdots \times Perm(g_k(X))) \rtimes S_k$ where the coordinate shift is obtained by ordering each $g_i(X)$ and letting $\sigma \in S_k$ move the r-th element of $g_i(X)$ to the r-th element of $g_{\sigma(i)}(X)$. In each $Perm(g_i(X))$ any permutation of the elements of $g_i(X)$ is allowed. This object can therefore be embedded in $Perm(Z)$ since, for a given $z \in Z$ (which lies in exactly one $g_i(X)$) one first has the option of moving z to a corresponding element (at the same position) in some other $g_j(X)$ and then acting on *this* by an

element of $Perm(g_j(X))$. As such, this is the maximal subgroup of $Perm(Z)$ which has $g_1(X),\ldots,g_k(X)$ as a system of blocks. The point is, if we replace any of the $Perm(g_i(X))$ by some smaller subgroup then we still have a group which preserves this system of blocks.

So what does this have to do with $Cent_B(\mathcal{P})$ and $Norm_B(\mathcal{P})$? We have $\mathcal{P}$ generated by the product of disjoint p-cycles $\pi_1\pi_2\pi_3\pi_4$ and if $\Pi_i = Supp(\pi_i)$, the support of π_i, then the Π_i are a partition of Γ into blocks. As we saw in the discussion in 2.7, an order p element centralizes if and only if it is the product of powers of the π_i which, of course, map each Π_i to itself. However, if ε is in the centralizer, then it is possible for $\varepsilon(\Pi_i) = \Pi_j$ for $i \neq j$, provided the ordering provided by the cycle structure of the underlying π_i is preserved, for then $\varepsilon\pi_i\varepsilon^{-1} = \pi_j$.

Specifically, we may impose an ordering on the Π_i as follows. Pick arbitrary $z_i \in \Pi_i$ and write $\Pi_i = \{z_i, \pi_i(z_i), \pi_i^2(z_i), \ldots, \pi_i^{p-1}(z_i)\}$ where, of course, $\pi_i = (z_i\ \pi_i(z_i)\ \pi_i^2(z_i)\ldots\pi_i^{p-1}(z_i))$ Now, let $\sigma_{ij} : \Pi_i \to \Pi_j$, for $i \neq j$ be defined by $\sigma_{ij}(\pi_i^k(z_i)) = \pi_j^k(z_j)$ and extend these bijections to permutations of Γ, by regarding them to be the identity outside the given (sub) sets Π_i where they are defined. With this, one can see that $\Sigma = \langle\sigma_{12}, \sigma_{23}, \sigma_{34}\rangle \cong S_4$.

For example, if p=5 and $\pi_1 = (1\ 2\ 3\ 4\ 5)$, $\pi_2 = (6\ 7\ 8\ 9\ 10)$, $\pi_3 = (11\ 12\ 13\ 14\ 15)$ and $\pi_4 = (16\ 17\ 18\ 19\ 20)$ then we can choose

$$\begin{aligned}
\Pi_1 &= \{1,2,3,4,5\}\\
\Pi_2 &= \{6,7,8,9,10\}\\
\Pi_3 &= \{11,12,13,14,15\}\\
\Pi_4 &= \{16,17,18,19,20\}
\end{aligned}$$

and thus

$$\begin{aligned}
\sigma_{12} &= (1\ 6)(2\ 7)(3\ 8)(4\ 9)(5\ 10)\\
\sigma_{23} &= (6\ 11)(7\ 12)(8\ 13)(9\ 14)(10\ 15)\\
\sigma_{34} &= (11\ 16)(12\ 17)(13\ 18)(14\ 19)(15\ 20)
\end{aligned}$$

and find that $\langle\sigma_{12}, \sigma_{23}, \sigma_{34}\rangle \cong S_4$.

However, if we chose $\Pi_2 = \{7,8,9,10,6\}$ (i.e. let $z_2 = 7$) then we could define

$$\begin{aligned}\sigma'_{12} &= (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 6)\\ \sigma'_{23} &= (7\ 11)(8\ 12)(9\ 13)(10\ 14)(6\ 15)\\ \sigma'_{34} &= \sigma_{34}\end{aligned}$$

and here too $\langle \sigma'_{12}, \sigma'_{23}, \sigma'_{34}\rangle \cong S_4$. Note that each copy of S_4 preserves the blocks Π_i.

Proposition 5.4: *$Cent_B(\mathcal{P}) = \langle \pi_1, \pi_2, \pi_3, \pi_4\rangle\Sigma$ where, for $\gamma \in \Gamma$ we define $\pi_1^{a_1}\pi_2^{a_2}\pi_3^{a_3}\pi_4^{a_4}\alpha(\gamma) = \pi_j^{a_j}(\alpha(\gamma))$ where $\alpha(\gamma) \in \Pi_j$*

Proof. If $\varepsilon \in Cent_B(\mathcal{P})$ then by the argument in 2.7, we have that $\varepsilon\pi_i\varepsilon_i^{-1} = \pi_i$ for all i if and only if $\varepsilon \in \langle \pi_1, \pi_2, \pi_3, \pi_4\rangle$ and, as $\mathcal{P} \triangleleft Cent_B(\mathcal{P})$, we may write $\varepsilon = \pi_1^{a_1}\pi_2^{a_2}\pi_3^{a_3}\pi_4^{a_4}\alpha$ where either $\alpha = id$ or $\alpha\pi_i\alpha^{-1} = \pi_j$ for some $i \neq j$. The claim is that we may choose the a_i such that $\alpha \in \Sigma$ as defined above. For example, if $\alpha\pi_1\alpha^{-1} = \pi_2$ then we have

$$(\alpha(z_1)\ \alpha(\pi_1(z_1))\ \alpha(\pi_1^2(z_1)) \ldots \alpha(\pi_1^{p-1}(z_1))) = (z_2\ \pi_2(z_2)\ \pi_2^2(z_2) \ldots \pi_2^{p-1}(z_2))$$

and as such, $\alpha(\Pi_1) = \Pi_2$ so that for some r, $\alpha(\pi_1^k(z_1)) = \pi_2^{r+k}(z_2)$ for each $k = 0, \ldots, p-1$. If we let $\alpha' = \pi_2^{-r}\alpha$ then not only does $\alpha'\pi_1\alpha'^{-1} = \pi_2$ still hold, and of course $\alpha'(\Pi_1) = \Pi_2$, but $\alpha'(\pi_1^k(z_1)) = \pi_2^k(z_2)$, that is α' preserves the ordering given above. So depending on how α acts on all the blocks we can always rewrite it as $\pi_1^{r_1}\pi_2^{r_2}\pi_3^{r_3}\pi_4^{r_4}\alpha'$ where $\alpha' \in \Sigma$. The point being that any deviation from the ordering of a Π_i given above arises from the action of some power of π_i. If $\gamma \in \Gamma$ then γ is in some Π_i and therefore $\alpha(\gamma) \in \Pi_j$ for some j, as such $\pi_1^{a_1}\pi_2^{a_2}\pi_3^{a_3}\pi_4^{a_4}\alpha(\gamma) = \pi_j^{a_j}(\gamma)$. □

The key fact is that $Cent_B(\mathcal{P})$ acts transitively on Γ and partitions it into blocks $\Pi_1, \Pi_2, \Pi_3, \Pi_4$, so with 5.3 in mind, we are not allowing all permutations in $Perm(\Pi_i)$ but rather those generated by the π_i. As such, we can

make the following association:

$$\{\text{permutations which centralize } \pi_1\pi_2\pi_3\pi_4\}$$
$$\updownarrow$$
$$\{\text{permutations which preserve the blocks } \Pi_i \text{ and the ordering of the } \Pi_i\}$$

Recall the 'vector' notation $[a_1,a_2,a_3,a_4] = \pi_1^{a_1}\pi_2^{a_2}\pi_3^{a_3}\pi_4^{a_4}$ as in 2.8. An element of $\Sigma \cong S_4$ will not only act on points $\gamma \in \Gamma$ but also on the coordinates of such a vector, yielding the following.

Proposition 5.5: *$Cent_B(\mathcal{P}) \cong C_p^4 \rtimes S_4$ where*

$$([b_1,b_2,b_3,b_4],\beta)([a_1,a_2,a_3,a_4],\alpha) = \\ ([b_1,b_2,b_3,b_4] + [a_{\beta^{-1}(1)},a_{\beta^{-1}(2)},a_{\beta^{-1}(3)},a_{\beta^{-1}(4)}],\beta\alpha)$$

Proof. If $\gamma \in \Pi_i$ then $([a_1,a_2,a_3,a_4],\alpha)(\gamma) = \pi_{\alpha(i)}^{a_{\alpha(i)}}(\alpha(\gamma))$ where $\alpha(\gamma)$ comes from $\alpha \in \Sigma$ (which chooses which block to move γ to) and $\alpha(i)$ is the index of the block to which γ was moved. We observe that:

$$\pi_{\alpha(i)}^{a_{\alpha(i)}}(\alpha(\gamma)) = \alpha(\pi_i^{a_{\alpha(i)}}(\gamma))$$

so that if we let $([b_1,b_2,b_3,b_4],\beta)$ act on $([a_1,a_2,a_3,a_4],\alpha)(\gamma)$ we have

$$\pi_{\beta(\alpha(i))}^{b_{\beta(\alpha(i))}}(\beta(\pi_{\alpha(i)}^{a_{\alpha(i)}}(\alpha(\gamma))))$$

$$= \beta(\pi_{\alpha(i)}^{b_{\beta(\alpha(i))}}(\pi_{\alpha(i)}^{a_{\alpha(i)}}(\alpha(\gamma))))$$

$$= \beta(\pi_{\alpha(i)}^{b_{\beta(\alpha(i))}+a_{\alpha(i)}}(\alpha(\gamma))))$$

$$= \pi_{\beta(\alpha(i))}^{b_{\beta(\alpha(i))}+a_{\alpha(i)}}(\beta\alpha(\gamma))))$$

$$= \pi_{\beta(\alpha(i))}^{b_{\beta(\alpha(i))}+a_{\beta^{-1}(\beta(\alpha(i)))}}(\beta\alpha(\gamma))))$$

The reason for the last line in the above computation is to show that the semi-direct product multiplication corresponds to composition of the corresponding permutations (from right to left), to wit,

$$\hat{b}+\beta(\hat{a}) = [b_1+a_{\beta^{-1}(1)}, b_2+a_{\beta^{-1}(2)}, b_3+a_{\beta^{-1}(3)}, b_4+a_{\beta^{-1}(4)}]$$

□

Now, as to the normalizer of $\mathcal{P}$, this is not quite a wreath product, (as the above centralizer is) but what Wells [27] (and others) term a 'twisted' wreath product. As it contains $Cent_B(\mathcal{P})$ it certainly acts transitively on Γ and moreover, respects the blocks Π_i so by 5.3 it is embedded in a certain wreath product. Unlike the centralizer, however, the embedding is not of one wreath product into another. We present an explicit construction here in order to facilitate the computations we will need to do later in order to determine the $N \in R(\Gamma)$. First consider the case of the centralizer and normalizer of a cyclic subgroup $C = \langle\pi\rangle$ of order p inside S_p. In this case, the centralizer of C is merely C itself, and the normalizer is generated by π and an 'automorphism', namely a cycle a of length $p-1$ (hence fixing one point) such that $a\pi a^{-1} = \pi^u$ where $U_p = \langle u\rangle$. For the case of $\mathcal{P}$, since $\langle\pi_i\rangle$ is a cyclic subgroup of $Perm(\Pi_i)$, there is a cycle u_i of length $p-1$ with $u_i\pi_i u_i^{-1} = \pi_i^u$ where $U_p = \langle u\rangle$. We may choose each such u_i so that it raises π_i to the same power u, and, by abuse of notation, denote $u = u_1u_2u_3u_4$ which we view as an element of $B = Perm(\Gamma = \Pi_1 \cup \Pi_2 \cup \Pi_3 \cup \Pi_4)$. We observe that $u[i_1, i_2, i_3, i_4]u^{-1} = [ui_1, ui_2, ui_3, ui_4]$ and so we may view u as acting by 'scalar multiplication' on elements of $\mathbb{F}_p^4$. With this in mind, we have the following.

Proposition 5.6: *In the notation of 5.5 and the previous paragraph, we have*

$$Norm_B(\mathcal{P}) \cong (C_p^4 \rtimes U_p) \rtimes S_4$$

where

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

with β *acting on* $\hat{a}$ *by coordinate shift, and where for* $\gamma \in \Gamma$ *we define*

$$([a_1, a_2, a_3, a_4], u^r, \alpha)(\gamma) = \pi_j^{a_j}(u^r(\alpha(\gamma))) \text{ where } \alpha(\gamma) \in \Pi_j.$$

Proof. We again consider the collection of blocks $\Pi_1, \Pi_2, \Pi_3, \Pi_4$ which partition Γ and realize that if $\varepsilon \in B$ normalizes $\langle \pi_1\pi_2\pi_3\pi_4 \rangle$ then it must map $\pi_1\pi_2\pi_3\pi_4$ (by conjugation) to $\pi_1^e\pi_2^e\pi_3^e\pi_4^e$ for some unit e and therefore has $\Pi_1, \Pi_2, \Pi_3, \Pi_4$ as a system of blocks.

Therefore, in a similar fashion as with $Cent_B(\mathcal{P})$, since $\mathcal{P} \triangleleft Norm_B(\mathcal{P})$, the action of ε can be factored into a product, of the form $\pi_1^{a_1}\pi_2^{a_2}\pi_3^{a_3}\pi_4^{a_4}u^r\alpha$ where $\alpha \in \Sigma$ and u is the product of the four $p-1$ cycles mentioned above.

Note, when we work with the semi-direct product on the left hand side, we view α as an element of S_4 permuting the coordinates of $[i_1, i_2, i_3, i_4]$ and, on the right, as permutations in $\Sigma \leq B$ preserving the blocks $\Pi_1, \Pi_2, \Pi_3, \Pi_4$ and their ordering, as per the discussion following 5.3. Note that $u^t\pi u^{-t} = \pi^{u^t}$ and therefore that:

$$\pi_{\alpha(i)}^{a_{\alpha(i)}}(u^r(\alpha(g)) = u^r\pi_{\alpha(i)}^{u^{-r}a_{\alpha(i)}}(\alpha(g))$$

and, as in 5.5, the semi-direct product multiplication is compatible with the permutation composition, that is

$$\pi_{\beta(\alpha(i))}^{b_{\beta(\alpha(i))}}u^s\beta(u^r\pi_{\alpha(i)}^{u^{-r}a_{\alpha(i)}}\alpha(g))$$

$$= \pi_{\beta(\alpha(i))}^{b_{\beta(\alpha(i))}+u^s a_{\beta^{-1}(\beta(\alpha(i)))}}(u^{s+r}(\beta\alpha(g)))$$

and we note that the exponent of $\pi_{\beta(\alpha(i))}$ is the $\beta(\alpha(i))^{th}$ entry of the vector $\hat{b} + u^s(\beta(\hat{a}))$. □

As the permutations in S_4 and units in U_p commute with each other, we could represent $Norm_B(\mathcal{P})$ as $C_p^4 \rtimes (U_p \times S_4)$, which is consistent with the group law given in 5.6 above. However, recalling 5.3, $Norm_B(\mathcal{P})$ acts transitively on $\Pi_1 \cup \Pi_2 \cup \Pi_3 \cup \Pi_4$ and is therefore isomorphic to a subgroup of $S_p \wr S_4$. In particular, we view $(C_p^4 \rtimes U_p)$ as a subgroup of $S_p^4 = Perm(\Pi_1) \times Perm(\Pi_2) \times Perm(\Pi_3) \times Perm(\Pi_4)$. Note also that $Cent_B(\mathcal{P})$ is embedded in $Norm_B(\mathcal{P})$ as those permutations $(\hat{a}, u^r, \alpha)$ where $r = 0$, that is $u^0 = 1$.

Even though $Norm_B(\mathcal{P})$ contains all N in a given $R(\Gamma, [M])$, we have the following amusing fact about $R(\Gamma)$ and $Cent_B(\mathcal{P})$.

Proposition 5.7: *For $N \in R(\Gamma, [M])$, we have:*

(a) If N is abelian then $N \leq Cent_B(\mathcal{P})$ for all Γ.

(b) If N is non-abelian then $N \leq Cent_B(\mathcal{P})$ if and only if $P(N) \neq P_1$.

Proof. If N is abelian then, by 4.2, $\mathcal{P} \leq N$ and since N centralizes itself, it centralizes $\mathcal{P}$. If N is non-abelian and $P(N) \neq P_1$ then, by 4.3, $P(N^{opp}) = P_1 = \mathcal{P}$ and so N centralizes $\mathcal{P}$. □

The above fact will be seen when we calculate the generators of all the groups in a given $R(\Gamma, [M])$ in the next section. However, if one were strictly concerned with determining $|R(\Gamma)|$ then the above is very useful. It shows that all the abelian N in a given $R(\Gamma)$ are contained in $Cent_B(\mathcal{P})$, while for N non-abelian (i.e. $[M]$ non-abelian) $R(\Gamma, [M])$ has twice as many elements as those which are contained in $Cent_B(\mathcal{P})$. So if we were not looking for explicit generators for all the N in a given $R(\Gamma)$, we could look strictly within $Cent_B(\mathcal{P})$ and apply the above proposition. Of course, when Γ is non-abelian, $\lambda(\Gamma)$ will not be contained in $Cent_B(\mathcal{P})$.

However, we do, in fact, wish to explicitly calculate, for each Γ, the possible regular subgroups N of $Norm_B(\mathcal{P})$ that are normalized by $\lambda(\Gamma)$. We shall take the point of view that any such N consists of the identity plus $4p - 1$ elements, each of which acts fixed point freely. As the groups we are considering are generated by elements of order p, 2 and 4, we begin by classifying the elements of $Norm_B(\mathcal{P})$ of these orders.

Proposition 5.8: *Using the semi-direct product representation for* $Norm_B(\mathcal{P})$ *we have the following:*

(a) The elements of order 2 *are of the form* $([b_1,b_2,b_3,b_4],v,\beta)$ *where*

$$\begin{aligned}
&\{\mathbf{T1}\}\ v=1, \quad \beta=(ij) \text{ and } b_i=-b_j\\
&\{\mathbf{T2}\}\ v=1, \quad \beta=(ij)(kl) \text{ and } b_i=-b_j, b_k=-b_l\\
&\{\mathbf{T3}\}\ v=-1, \ \beta=(ij) \text{ and } b_i=b_j\\
&\{\mathbf{T4}\}\ v=-1, \ \beta=(ij)(kl) \text{ and } b_i=b_j, b_k=b_l
\end{aligned}$$

(b) The elements of order 4 *are of the form* $([b_1,b_2,b_3,b_4],v,\beta)$ *where*

$$\begin{aligned}
&\{\mathbf{F1}\}\ v=1, \quad \beta=(ijkl), \quad b_i+b_j+b_k+b_l=0\\
&\{\mathbf{F2}\}\ v=-1, \ \beta=(ijkl), \quad b_i+b_k=b_j+b_l\\
&\{\mathbf{F3}\}\ v=\zeta,\overline{\zeta}, \ \beta=e, \quad \hat{b}+\zeta\hat{b}-\hat{b}+\overline{\zeta}\hat{b}=\hat{0}\\
&\{\mathbf{F4}\}\ v=\zeta,\overline{\zeta}, \ \beta=(ij), \quad \hat{b}+\zeta\beta(\hat{b})-\hat{b}+\overline{\zeta}\beta(\hat{b})=\hat{0}\\
&\{\mathbf{F5}\}\ v=\zeta,\overline{\zeta}, \ \beta=(ij)(kl), \ \hat{b}+\zeta\beta(\hat{b})-\hat{b}+\overline{\zeta}\hat{b}=\hat{0}\\
&\{\mathbf{F6}\}\ v=\zeta,\overline{\zeta}, \ \beta=(ijkl), \quad \hat{b}+\zeta\beta(\hat{b})-\beta^2(\hat{b})+\overline{\zeta}\beta^3(\hat{b})=\hat{0}
\end{aligned}$$

The only elements of order p *in* $Norm_B(\mathcal{P})$ *are of the form* $(\hat{b},1,e)$.

Proof. This is based upon consideration of a general n^{th} power of $(\hat{b},v,\beta)$, specifically

$$(\hat{b},v,\beta)^n=(\sum_{i=0}^{n-1}v^i\beta^i(\hat{b}),v^n,\beta^n)$$

and so, for the order 2 elements we are constrained by the requirement that $\beta^2=e$ and $v^2=1$ which, in turn, gives us the relations on the components of $\hat{b}$, the case for order 4 elements is similar, only that the relations on $\hat{b}$ are somewhat more complicated. The order p elements are as indicated, because neither S_4 nor U_p have elements of order p. □

Now we find conditions on elements of $Norm_B(\mathcal{P})$ in order that they act fixed-point freely on Γ.

Proposition 5.9: *An element* $([a_1,a_2,a_3,a_4],u^r,\alpha)$ *in* $Norm_B(\mathcal{P})$ *has a fixed point if either of the following hold:*

(a) $r=0$ *and* α *fixes any block* Π_i *where* $a_i=0$

(b) $r\neq 0$ *and* α *fixes* **any** Π_i

Proof. Recalling the above discussion of the structure of $Norm_B(\mathcal{P})$ we have, for $\gamma\in\Gamma$, that $\gamma\in\Pi_i$ for some i and therefore that $\alpha(\gamma)\in\Pi_j$ for some j, as such:

$$([a_1,a_2,a_3,a_4],u^r,\alpha)(\gamma)=\pi_j^{a_j}(u^r(\alpha(\gamma)))$$

If $r=0$, γ is fixed if and only if $\pi_j^{a_j}(\alpha(\gamma))=\gamma$. If $i\neq j$ then this is impossible since γ and $\alpha(\gamma)$ lie in different blocks and π_j preserves Π_j. If $i=j$ then $\alpha(\gamma)=\gamma$ and so $\pi_i^{a_i}(\gamma)=\gamma$ if and only if $a_i=0$.

If $r\neq 0$ then γ is fixed if $\pi_j^{a_j}(u^r(\alpha(\gamma)))=\gamma$. If $i\neq j$ then this is impossible since again, γ and $\alpha(\gamma)$ lie in different blocks and π_j and u^r map elements in given block to the same block. If $i=j$ then $\alpha(\gamma)=\gamma$ and so γ is fixed if and only if $\pi_i^{a_i}(u^r(\gamma))=\gamma$, that is $u^r(\gamma)=\pi_i^{-a_i}(\gamma)$ which happens for at least one $\gamma\in\Gamma$ since $\langle\pi_i\rangle$ acts transitively on Π_i and u^r restricts to a permutation of Π_i.

Note, α (viewed as an element of Σ) fixing Π_i corresponds, in the semidirect product, to it fixing the i^{th} coordinate of $[a_1,a_2,a_3,a_4]$, that is it fixes $i\in\{1,2,3,4\}$ when viewed as an element of S_4. □

With this in mind we can limit the possible elements to build $N\in R(\Gamma)$ by restricting the elements in 5.8 to those which are fixed point free. Moreover, if $n\in N$ is fixed point free then, in order for N to be regular, n^k must be fixed point free for any k such that $n^k\neq e$.

Proposition 5.10: *Of the elements in 5.8 only those of type* **T2**,**T4**,**F1**,**F2**, *and* **F6** *satisfy the property of being fixed point free, and of all non-trivial powers being fixed point free. The order p element* $(\hat{b},1,e)$ *acts fixed point freely provided all* $b_i\neq 0$.

Proof. This is simply an application of 5.9 to 5.8. For the order 4 elements, we omit **F5** as the square of any such element has $e = ((ij)(kl))^2$ in the third coordinate and therefore has fixed point points by 5.9. □

Now we need to check that the groups generated by these fixed point free elements are regular subgroups of B.

Lemma 5.11: *If σ, $\tau \in B$ act fixed point freely and $(|\sigma|, |\tau|) = 1$ then $\sigma^i\tau^j$ acts fixed point freely provided $\sigma^i\tau^j \neq e$.*

Using this lemma we obtain all regular subgroups isomorphic to C_{4p}, E_p and Q_p. As to the others, which are generated by an element of order p and two elements of order 2 which commute, we have the following, which is a consequence of 5.9.

Lemma 5.12: *Of the elements of type* **T2** *and* **T4***, the product of two such elements will have fixed points if and only if they have the same third coordinate.*

For regular subgroups isomorphic to $C_p \times V$ and D_{2p} we have the following.

Lemma 5.13: *If τ_1 and τ_2 are elements of order 2 in the class* **T2** *or* **T4** *that commute and have differing third coordinates, and σ is fixed point free and has order p then $\sigma^i\tau_1\tau_2$ acts fixed point freely.*

Proof. If $\sigma^i\tau_1\tau_2(\gamma) = \gamma$ then $\tau_1\tau_2(\gamma) = \sigma^{-i}(\gamma)$ and so $\sigma^{-2i}(\gamma) = \gamma$ which implies $i = 0$ but then $\tau_1\tau_2(\gamma) = \gamma$ which is impossible by the previous result. □

6 The Regular Subgroups Normalized by $\lambda(\Gamma)$

The goal of this section is to determine $R(\Gamma, [M])$ for all possible combinations of Γ and M. Keeping in mind that each N uniquely contains P_i, we present the size(s) of each $R(\Gamma, [M])$ and indicate how many contain a given P_i.

Proposition 6.1: *The distribution of the $R(\Gamma,[M])$ are as follows, subject to the constraints imposed by the class of p mod 4, specifically that for $p \equiv 3$ $R(E_p) = \emptyset$ and $R(\Gamma,[E_p]) = \emptyset$ for all Γ.*

- $|R(C_{4p})| = 10$ *if* $p \equiv 1(mod\ 4)$ *or* 6 *if* $p \equiv 3(mod\ 4)$

	P_1	P_2	P_3	P_4	P_5	P_6
$R(C_{4p},[C_{4p}])$	1	0	0	0	0	0
$R(C_{4p},[C_p \times V])$	1	0	0	0	0	0
$R(C_{4p},[E_p])$	2	0	0	0	1	1
$R(C_{4p},[D_{2p}])$	1	1	0	0	0	0
$R(C_{4p},[Q_p])$	1	1	0	0	0	0

- $|R(C_p \times V)| = 16$

	P_1	P_2	P_3	P_4	P_5	P_6
$R(C_p \times V,[C_{4p}])$	3	0	0	0	0	0
$R(C_p \times V,[C_p \times V])$	1	0	0	0	0	0
$R(C_p \times V,[E_p])$	0	0	0	0	0	0
$R(C_p \times V,[D_{2p}])$	3	1	1	1	0	0
$R(C_p \times V,[Q_p])$	3	1	1	1	0	0

- $|R(E_p)| = 8p+2$ *if* $p \equiv 1(mod\ 4)$

	P_1	P_2	P_3	P_4	P_5	P_6
$R(E_p,[C_{4p}])$	p	0	0	0	0	0
$R(E_p,[C_p \times V])$	p	0	0	0	0	0
$R(E_p,[E_p])$	$p+1$	0	0	0	p	1
$R(E_p,[D_{2p}])$	p	p	0	0	0	0
$R(E_p,[Q_p])$	p	p	0	0	0	0

- $|R(D_{2p})| = 12p+4$

	P_1	P_2	P_3	P_4	P_5	P_6
$R(D_{2p},[C_{4p}])$	$3p$	0	0	0	0	0
$R(D_{2p},[C_p \times V])$	p	0	0	0	0	0
$R(D_{2p},[E_p])$	0	0	0	0	0	0
$R(D_{2p},[D_{2p}])$	$2p+1$	1	p	p	0	0
$R(D_{2p},[Q_p])$	$2p+1$	1	p	p	0	0

- $|R(Q_p)| = 6p+4$ *if* $p \equiv 1(mod\ 4)$ *or* $2p+4$ *if* $p \equiv 3(mod\ 4)$

	P_1	P_2	P_3	P_4	P_5	P_6
$R(Q_p,[C_{4p}])$	p	0	0	0	0	0
$R(Q_p,[C_p \times V])$	p	0	0	0	0	0
$R(Q_p,[E_p])$	$2p$	0	0	0	p	p
$R(Q_p,[D_{2p}])$	1	1	0	0	0	0
$R(Q_p,[Q_p])$	1	1	0	0	0	0

Observe that for Γ abelian, the size of $R(\Gamma)$ is due to the structure of S_4 and is independent of p. The fact that the p-Sylow subgroup of $Norm_B(N)$ has order p^2 when N is non-abelian accounts for $R(\Gamma)$ being larger for $\Gamma = E_p$, D_{2p}, and Q_p. To demonstrate this, and, moreover, to give explicit generators for each such N we shall construct regular subgroups of B of each isomorphism type and determine which are normalized by a given $\lambda(\Gamma)$. We begin by determining the generators of each $\lambda(\Gamma)$ as elements of $Norm_B(\mathcal{P})$.

Proposition 6.2: *As elements of* $Norm_B(\mathcal{P})$*, the generators of each* $\lambda(\Gamma)$ *(of order not p) are as follows:*

(a) $\Gamma = C_{4p}$*,* $\lambda(x) = ([1,0,0,0],1,(1324))$

(b) $\Gamma = C_p \times V$*,* $\lambda(t_1) = (\hat{0},1,(12)(34))$ *and* $\lambda(t_2) = (\hat{0},1,(13)(24))$

(c) $\Gamma = E_p$*,* $\lambda(t) = (\hat{0},\overline{\zeta},(1324))$

(d) $\Gamma = D_{2p}$*,* $\lambda(x) = ([1,0,0,1],1,(12)(34))$ *and* $\lambda(t) = (\hat{0},-1,(13)(24))$

(e) $\Gamma = Q_p$*,* $\lambda(x) = ([1,0,0,1],1,(12)(34))$ *and* $\lambda(t) = ([\mathfrak{h},-\mathfrak{h},0,0],-1,(1324))$ *where* $\mathfrak{h} = 2^{-1} \in \mathbb{F}_p$.

The presentations of each $\lambda(\Gamma)$ are as in 2.1 and 2.2. As elements of $Norm(\mathcal{P})$ the $\hat{p}_i$ are embedded as $(\hat{p}_i,1,e)$ which, by abuse of notation, we will still denote by $\hat{p}_i$. In order to construct the various N that may arise, we observe the following, which details how the various fixed point free elements of orders two and four act by conjugation on the various $\hat{p}_i$. We will use the term invert or inverted to mean that, by conjugation, a given generator maps $\hat{p}_i$ to $\hat{p}_i^{-1}$ and by ζ-inverted (or $\overline{\zeta}$-inverted) to mean that $\hat{p}_i$ is mapped to respectively $\hat{p}_i^{\zeta}$ or $\hat{p}_i^{\overline{\zeta}}$.

For the next result and subsequent computations, we recall from 5.6 that the multiplication in $Norm_B(\mathcal{P})$ is given by

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

and the inverse is given by

$$(\hat{b}, v, \beta)^{-1} = (-v^{-1}\beta^{-1}(\hat{b}), v^{-1}, \beta^{-1})$$

Also, from 5.6, for $v \in U_p$, $\beta \in S_4$ and $\hat{a} = [a_1, a_2, a_3, a_4] \in C_p^4$ we have

$$v\beta(\hat{a}) = [va_{\beta^{-1}(1)}, va_{\beta^{-1}(2)}, va_{\beta^{-1}(3)}, va_{\beta^{-1}(4)}]$$

Also recall that ζ and $\overline{\zeta} = \zeta^{-1} = -\zeta$ are the elements of order 4 in U_p when $p \equiv 1 \ (mod\ 4)$.

Proposition 6.3: *With the P_i defined as in 2.9,*

- $\hat{p}_1$ *is*
  - *centralized by* $(\hat{b}, 1, (ijkl)), (\hat{b}, 1, (ij)(kl))$
  - *inverted by* $(\hat{b}, -1, (ijkl)), (\hat{b}, -1, (ij)(kl))$
  - ζ*-inverted by* $(\hat{b}, \zeta, (ijkl))$
- $\hat{p}_2$ *is*
  - *centralized by* $(\hat{b}, -1, (1423)^{\pm 1}), (\hat{b}, 1, (12)(34)), (\hat{b}, -1, (13)(24)), (\hat{b}, -1, (14)(23))$
  - *inverted by* $(\hat{b}, 1, (1423)^{\pm 1}), (\hat{b}, -1, (12)(34)), (\hat{b}, 1, (13)(24)), (\hat{b}, 1, (14)(23))$
  - ζ*-inverted by* $(\hat{b}, \overline{\zeta}, (1423)^{\pm 1})$
- $\hat{p}_3$ *is*
  - *centralized by* $(\hat{b}, -1, (1234)^{\pm 1}), (\hat{b}, -1, (12)(34)), (\hat{b}, 1, (13)(24)), (\hat{b}, -1, (14)(23))$
  - *inverted by* $(\hat{b}, 1, (1234)^{\pm 1}), (\hat{b}, 1, (12)(34)), (\hat{b}, -1, (13)(24)), (\hat{b}, 1, (14)(23))$
  - ζ*-inverted by* $(\hat{b}, \overline{\zeta}, (1234)^{\pm 1})$
- $\hat{p}_4$ *is*
  - *centralized by* $(\hat{b}, -1, (1243)^{\pm 1}), (\hat{b}, -1, (12)(34)), (\hat{b}, -1, (13)(24)), (\hat{b}, 1, (14)(23))$

  - *inverted by* $(\hat{b},1,(1243)^{\pm 1}),(\hat{b},1,(12)(34)),(\hat{b},1,(13)(24)),(\hat{b},-1,(14)(23))$
  - ζ*-inverted by* $(\hat{b},\overline{\zeta},(1243)^{\pm 1})$
- $\hat{p}_5$ *is*
  - *centralized by* $(\hat{b},\zeta,(1324)),(\hat{b},\overline{\zeta},(1423)),(\hat{b},-1,(12)(34))$
  - *inverted by* $(\hat{b},\overline{\zeta},(1324)),(\hat{b},\zeta,(1423)),(\hat{b},1,(12)(34))$
  - ζ*-inverted by* $(\hat{b},-1,(1324)),(\hat{b},1,(1423))$
- $\hat{p}_6$ *is*
  - *centralized by* $(\hat{b},\overline{\zeta},(1324)),(\hat{b},\zeta,(1423)),(\hat{b},-1,(12)(34))$
  - *inverted by* $(\hat{b},\zeta,(1324)),(\hat{b},\overline{\zeta},(1423)),(\hat{b},1,(12)(34))$
  - ζ*-inverted by* $(\hat{b},1,(1324)),(\hat{b},-1,(1423))$

Proof. Using the remarks before the statement of the proposition, we find that

$$\begin{aligned}(\hat{b},v,\beta)(\hat{a},w,\alpha)(\hat{b},v,\beta)^{-1} &= (\hat{b},v,\beta)(\hat{a},w,\alpha)(-v^{-1}\beta^{-1}(\hat{b}),v^{-1},\beta^{-1})\\ &= (\hat{b}+v\beta(\hat{a})-vwv^{-1}(\beta\alpha\beta^{-1})(\hat{b}),vwv^{-1},\beta\alpha\beta^{-1})\\ &= (\hat{b}+v\beta(\hat{a})-w(\beta\alpha\beta^{-1})(\hat{b}),w,\beta\alpha\beta^{-1}) \quad \textbf{[1]}\end{aligned}$$

and for $\alpha = e$ and $w = 1$, **[1]** becomes $(v\beta(\hat{a}),1,e)$. We observe also that if we regard the action of Σ on a given $\hat{b} = [b_1,b_2,b_3,b_4]$ via the action of an element of S_4 on the coordinates as in 5.5 and 5.6, then we find that

$\beta(P_1) = P_1 \ for\ all\ \beta \in S_4$
$\beta(P_2) = P_2 \ for\ \beta \in \{e,(12),(34),(13)(24),(14)(23),(12)(34),(1324),(1423)\}$
$\beta(P_3) = P_3 \ for\ \beta \in \{e,(13),(24),(13)(24),(14)(23),(12)(34),(1234),(1432)\}$
$\beta(P_4) = P_4 \ for\ \beta \in \{e,(14),(23),(13)(24),(14)(23),(12)(34),(1243),(1342)\}$
$\beta(P_5) = P_5 \ for\ \beta \in \{e,(12)(34),(1423),(1324)\}$
$\beta(P_6) = P_6 \ for\ \beta \in \{e,(12)(34),(1423),(1324)\}$

since a given β may either fix $\hat{p}_i$ or send it to $u\hat{p}_i$ for some $u \in U_p$. For example, if $\beta = (13)(24)$ then for $\hat{p}_2 = [1,1,-1,-1]$, $\beta(\hat{p}_2) = [-1,-1,1,1]$ and so $(-1)\beta(\hat{p}_2) = -[-1,-1,1,1] = [1,1,-1,-1] = \hat{p}_2$. The different cases are computed in a similar fashion. □

We note the following basic facts about S_4 which are used throughout these calculations

Lemma 6.4: *In S_4, if $\alpha = (xy)(zw)$, $\alpha' = (x'y')(z'w')$ and $\beta = (ijkl)$, $\beta' = (i'j'k'l')$ then*

(a) $\beta\beta' = \beta'\beta$ *if and only if* $\beta' = \beta$ *or* $\beta' = \beta^{-1}$
(b) $\alpha\beta = \beta\alpha$ *if and only if* $\alpha = \beta^2$ *otherwise* $\alpha\beta\alpha^{-1} = \beta^{-1}$
(c) $\alpha\alpha' = \alpha'\alpha$

Additionally, as $C_p \times V$ and D_{2p} both contain subgroups isomorphic to V we note when certain fixed point free elements of order 2 commute.

Lemma 6.5: *The following relations hold*

$[(\hat{a},1,(12)(34)),(\hat{b},1,(13)(24))] = (\hat{0},1,e)$ *if and only if* $a_1 - a_3 = b_1 - b_2$
$[(\hat{a},1,(12)(34)),(\hat{b},-1,(13)(24))] = (\hat{0},1,e)$ *if and only if* $a_1 + a_3 = b_1 - b_2$
$[(\hat{a},-1,(12)(34)),(\hat{b},1,(13)(24))] = (\hat{0},1,e)$ *if and only if* $a_1 - a_3 = b_1 + b_2$
$[(\hat{a},-1,(12)(34)),(\hat{b},-1,(13)(24))] = (\hat{0},1,e)$ *if and only if* $a_1 + a_3 = b_1 + b_2$

Proof. This is a simple application of 5.6 and 5.9, together with the observation (from 5.8) that for $(\hat{a},1,(ij)(kl))$ to have order 2, we must have $a_j = -a_i$ and $a_l = -a_k$ and likewise for $(\hat{a},-1,(ij)(kl))$ to have order 2, we must have $a_j = a_i$ and $a_l = a_k$. □

Now we determine the groups in each $R(\Gamma,[M])$. We shall give the generators of the groups in each $R(\Gamma,[M])$. However, as there are 25 cases total, and many are determined using similar arguments, we shall only work out in detail the enumeration of $R(C_{4p},[M])$ for each isomorphism class $[M]$, $R(C_p\times V,[E_p])$, $R(E_p,[C_{4p}])$, and $R(D_{2p},[D_{2p}])$ when $P(N)=P_1$. Recall that, by 3.9 and 4.3, when $[M]$ is non-abelian, a given N and its opposite will both be present in $R(\Gamma,[M])$, one containing P_1 and the other some *different* P_i, as governed by 2.10. Also, the relationship between $R(\Gamma,[D_{2p}])$ and $R(\Gamma,[Q_p])$, as given in 3.11 and 3.12, will be manifested. Additionally, we shall note in 6.8 a recent result, [7], of Childs which agrees with our count of $|R(E_p,[E_p])|$.

Again, we note some basic facts about the multiplication in $Norm_B(\mathcal{P})$.

- $(\hat{b},u^s,\beta)(\hat{a},u^r,\alpha)=(\hat{b}+u^s\beta(\hat{a}),u^{s+r},\beta\alpha)$
- $(\hat{b},v,\beta)^{-1}=(-v^{-1}\beta^{-1}(\hat{b}),v^{-1},\beta^{-1})$
- $v\beta(\hat{a})=[va_{\beta^{-1}(1)},va_{\beta^{-1}(2)},va_{\beta^{-1}(3)},va_{\beta^{-1}(4)}]$
- $\overline{\zeta}=\zeta^{-1}=-\zeta$ when $p\equiv 1\ (mod\ 4)$

Proposition 6.6: *For $\Gamma=C_{4p}$ we have (where $\mathfrak{h}=2^{-1}$ in $\mathbb{F}_p$)*

$$R(C_{4p},[C_{4p}])=\{\ \langle\ \hat{p}_1,\ ([1-\mathfrak{h}^2,-\mathfrak{h}^2,-\mathfrak{h}^2,-\mathfrak{h}^2],1,(1324))\ \rangle\ \}$$

$$R(C_{4p},[C_p\times V])=\{\ \langle\ \hat{p}_1,\ ([\mathfrak{h},-\mathfrak{h},\mathfrak{h},-\mathfrak{h}],1,(12)(34)),([\mathfrak{h}^2,\mathfrak{h}^2,-\mathfrak{h}^2,-\mathfrak{h}^2],1,(13)(24))\ \rangle\ \}$$

$$\begin{aligned}R(C_{4p},[E_p])=\{\ &\langle\ \hat{p}_1,\ ([0,2\mathfrak{h}^2(\overline{\zeta}+1)-1,3\mathfrak{h}^2(\overline{\zeta}+1)-1,\mathfrak{h}^2(\overline{\zeta}+1)-1],\zeta,(1324))\ \rangle,\\ &\langle\ \hat{p}_1,\ ([0,-2\mathfrak{h}^2(\overline{\zeta}+1),-\mathfrak{h}^2(\overline{\zeta}+1),\mathfrak{h}^2(\overline{\zeta}+1)-1],\zeta,(1423))\ \rangle,\\ &\langle\ \hat{p}_5,\ ([0,\mathfrak{h},\mathfrak{h}(1-\zeta)^{-1},\overline{\zeta}\mathfrak{h}(1-\zeta)^{-1},\mathfrak{h}(1-\zeta)^{-1}-1],1,(1423))\ \rangle,\\ &\langle\ \hat{p}_6,\ ([0,\mathfrak{h},(\mathfrak{h}+1)(1+\zeta)^{-1}\zeta-1,\mathfrak{h}-(\mathfrak{h}+1)(1+\zeta)^{-1}\overline{\zeta}],1,(1324))\ \rangle\}\end{aligned}$$

$$R(C_{4p},[D_{2p}]) = \{\langle\ \hat{p}_1,\ ([\mathfrak{h},-\mathfrak{h},\mathfrak{h},-\mathfrak{h}],1,(12)(34)),\ ([0,-1,0,-1],-1,(13)(24))\ \rangle$$
$$\langle\ \hat{p}_2,\ ([\mathfrak{h},-\mathfrak{h},\mathfrak{h},-\mathfrak{h}],1,(12)(34)),\ (\hat{0},1,(13)(24))\ \rangle\}$$

$$R(C_{4p},[Q_p]) = \{\langle\ \hat{p}_1,\ ([0,0,\mathfrak{h},-\mathfrak{h}],-1,(1324))\ \rangle,$$
$$\langle\ \hat{p}_2,\ ([0,0,\mathfrak{h},-\mathfrak{h}],1,(1423))\ \rangle\}$$

Proof. Case $R(C_{4p},[C_{4p}])$

By 6.2 the generator of $\lambda(\Gamma)$ is $([1,0,0,0],1,(1324))$ with inverse $([0,0,0,-1],1,(1423))$. If N is a regular subgroup with $P(N)=P_1$ then $N=\langle\hat{p}_1,(\hat{b},1,(ijkl))\rangle$ where $(\hat{b},1,(ijkl))$ is order 4 and fixed point free in accordance with 5.8. Moreover, $(\hat{b},1,(ijkl))^{-1}=(-(ilkj)(\hat{b}),1,(ilkj))$. By direct calculation

$$([1,0,0,0],1,(1324))(\hat{b},1,(ijkl))([0,0,0,-1],1,(1423)) =$$
$$([1,0,0,0]+(1324)(\hat{b})+(1324)(ijkl)([0,0,0,-1]),1,(1324)(ijkl)(1423))\ \textbf{[2]}$$

Now, in order that the right hand of **[2]** above lie in N, then $(1324)(ijkl)(1423)$ must equal either $(ijkl)$ or $(ilkj)$ which implies that $(ijkl)=(1324)$ or (1423). As $(\hat{b},1,(ijkl))$ and its inverse both generate the same N then we may assume that $(ijkl)=(1324)$ and so the right side of **[2]** becomes

$$([1,0,-1,0]+(1324)(\hat{b}),1,(1324))$$

But, as the order 4 subgroup of N is unique, this element must be $(\hat{b},1,(1324))$ and so we have $[1,0,-1,0]+[b_4,b_3,b_1,b_2]=[b_1,b_2,b_3,b_4]$, that is

$$\begin{aligned} 1+b_4 &= b_1 \\ b_3 &= b_2 \\ -1+b_1 &= b_3 \\ b_2 &= b_4 \end{aligned}$$

but the above together with the relation $b_1+b_2+b_3+b_4=0$, imposed by 5.10, implies that $4b_2+1=0$ and so $b_2=-4^{-1}=-\mathfrak{h}^2$. Thus $\hat{b}=[-\mathfrak{h}^2+1,-\mathfrak{h}^2,-\mathfrak{h}^2,-\mathfrak{h}^2]$. This shows that N (with $P(N)=P_1$) must be unique.

By 4.1 there are no N with $P(N) \neq P_1$.

Case $R(C_{4p}, [C_p \times V])$

With $P(N) = P_1$ we may assume, by 6.3 and 6.5, that

$$N = \langle \hat{p}_1, (\hat{a}, 1, (12)(34)), (\hat{b}, 1, (13)(24)) \rangle$$

since 'V' is generated by two elements of order 2 which centralize $\hat{p}_1$ and each other. Note, that the other order 2 element in V here will have $(14)(23)$ in its third coordinate. Also, recall from 5.12 that N can't contain $(\hat{a}, 1, (12)(34))$ and $(\hat{a}', 1, (12)(34))$ simultaneously since then the product of two such order 2 elements would have fixed points by 5.12.

By direct calculation,

$$\begin{aligned}([1,0,0,0], 1, (1324))(\hat{a}, 1, (12)(34))([0,0,0,-1], 1, (1423)) = \\ ((1324)(\hat{a}) + [1,1,0,0], 1, (12)(34))\end{aligned}$$

which means that $(\hat{a}, 1, (12)(34)) = ((1324)(\hat{a}) + [1,1,0,0], 1, (12)(34))$ and since $a_1 = -a_2$ and $a_3 = -a_4$ (due to 5.10), we find that $\hat{a} = [\mathfrak{h}, -\mathfrak{h}, \mathfrak{h}, -\mathfrak{h}]$. Similarly, we find that $\hat{b} = [\mathfrak{h}^2, \mathfrak{h}^2, -\mathfrak{h}^2, -\mathfrak{h}^2]$ which means that N is unique.

Again, by 4.1 there are no N with $P(N) \neq P_1$.

Case $R(C_{4p}, [E_p])$

First, we recall that E_p is generated by an element x of order p and an element t of order 4 and that all the other elements of order 4 in E_p are of the form $x^k t$ or $x^k t^{-1}$ for $k = 0, \ldots, p-1$. If $P(N) = P_1$ then N is of the form $\langle \hat{p}_1, (\hat{b}, \zeta, (ijkl)) \rangle$ and we observe that $(\hat{b}, \zeta, (ijkl))^{-1} = (\zeta(ilkj)(\hat{b}), \overline{\zeta}, (ilkj))$. If $\lambda(\Gamma)$ normalizes N then this order 4 element must be mapped to another of order 4 in N. By the above remarks, these are of the form $(k\hat{p}_1 + \hat{b}, \zeta, (ijkl))$ or $(k\hat{p}_1 + \zeta(ilkj)(\hat{b}), \overline{\zeta}, (ilkj))$. Observe that

$$\begin{aligned}&([1,0,0,0], 1, (1324))(\hat{b}, \zeta, (ijkl))([0,0,0,-1], 1, (1423)) = \\ &([1,0,0,0] + (1324)(\hat{b}) + (1324)(ijkl)([0,0,0,\overline{\zeta}]), \zeta, (1324)(ijkl)(1423))\end{aligned}$$

so we therefore must have that $(1324)(ijkl)(1423) = (ijkl)$ or $(ilkj)$ which implies that $(ijkl) = (1324)$ or (1423). If $(ijkl) = (1324)$ then the right hand

side of the above equation becomes $([1,0,\overline{\zeta},0]+(1324)(\hat{b}),\zeta,(1324))$ and so we must have

$$([1,0,\overline{\zeta},0]+(1324)(\hat{b}),\zeta,(1324))=(k\hat{p}_1+\hat{b},\zeta,(1324))$$

which implies that $[b_4+1,b_3,b_1+\overline{\zeta},b_2]=[b_1+k,b_2+k,b_3+k,b_4+k]$. The four resulting equations imply that $b_1=b_1+4k-1-\overline{\zeta}$ which implies that $k=\mathfrak{h}^2(\overline{\zeta}+1)$ and therefore that $\hat{b}=[b_1,b_1+2k-1,b_1+3k-1,b_1+k-1]$ for $b_1\in\mathbb{F}_p$ which accounts for p distinct elements of order 4. When $b_1=0$ we obtain the generator in the statement of the proposition. The other p elements of order 4 are therefore of the form $(\zeta(1423)(\hat{b}),\overline{\zeta},(1423))$ for each $\hat{b}$ above.

Now, observe that an element of the form $(\hat{b},\zeta,(1423))$ is not an element of the 'N' above since the order 4 elements in that N are of the form $(*,\zeta,(1324))$ and $(*,\overline{\zeta},(1423))$. Therefore, if $(ijkl)=(1423)$ we have

$$\begin{aligned}&([1,0,0,0],1,(1324))(\hat{b},\zeta,(ijkl))([0,0,0,-1],1,(1423)))=\\&([1,0,0,0]+(1324)(\hat{b})+(1324)(ijkl)([0,0,0,\overline{\zeta}]),\zeta,(1324)(ijkl)(1423))\\&([1,0,0,\overline{\zeta}]+(1324)(\hat{b}),\zeta,(1423))\end{aligned}$$

and this must therefore equal $(k\hat{p}_1+\hat{b},\zeta,(1423))$ for some k. As such, $[b_4+1,b_3,b_1,b_2+\overline{\zeta}]=[b_1+k,b_2+k,b_3+k,b_4+k]$ which implies that $b_1=b_1-4k+\overline{\zeta}+1$ and so $k=\mathfrak{h}^2(\overline{\zeta}+1)$ which implies that $\hat{b}=[b_1,b_1-2k,b_1-k,b_1+k-1]$ for $b_1\in\mathbb{F}_p$. For $b_1=0$ we have the generator listed in the statement of the proposition.

If $P(N)=P_2$ then an element of order 4 would, by 6.3, be of the form $(\hat{b},\overline{\zeta},(1324)^{\pm1})$ and conjugating this by $\hat{p}_1$ would give

$$(\hat{b}+(1+\overline{\zeta})\hat{p}_1,\overline{\zeta},(1324)^{\pm1})$$

which would have to be of the form $(\hat{b}+k\hat{p}_2,\overline{\zeta},(1324)^{\pm1})$ which would imply that $k\hat{p}_2=(1+\overline{\zeta})\hat{p}_1$ which is impossible.

If $P(N)=P_5$ then, by 6.3, the order 4 generator is either of the form $(\hat{b},1,(1423))$ or $(\hat{b},-1,(1324))$, but we can't have the latter as conjugating it

by $\hat{p}_1$ would not yield an element of N, i.e. $\hat{b}+2\hat{p}_1 = \hat{b}+k\hat{p}_5$ is impossible. To see how $(\hat{b},1,(1423))$ is moved by conjugation we find

$$([1,0,0,0],1,(1324))(\hat{b},1,(1423))([0,0,0,-1],1,(1423)) = \\ ([1,0,0,-1]+(1324)(\hat{b}),1,(1423))$$

which implies that $[b_4+1,b_3,b_1,b_2-1] = \hat{b}+k\hat{p}_5 = [b_1+k,b_2-k,b_3+k\zeta,b_4+k\overline{\zeta}]$. To determine k we take a slightly different approach than above. In N, given the generator $(\hat{b},1,(1423))$ there must be another element of order 4 of the form $(\hat{b}',1,(1423))$ where ${b_1}' = 0$, i.e. choose k such that $k+b_1 = 0$. This element must also be a generator and so we may assume that $b_1 = 0$ to begin with. As such we get $b_4+1 = k$, $b_3 = b_2-k$, $b_3 = -k\zeta = k\overline{\zeta}$ and $b_2-1 = b_4+k\zeta$ which implies that $\hat{b} = [0,b_2,k\overline{\zeta},b_2-1+k\zeta]$ but now, we must have (by 5.10) that the sum of the components of $\hat{b}$ equals 0. As such, $b_2 = \mathfrak{h}$ and as $b_3 = k\overline{\zeta}$ then $k\overline{\zeta} = \mathfrak{h}-k$ which implies that $k = \mathfrak{h}(1-\zeta)^{-1}$ and so $b_3 = \overline{\zeta}\mathfrak{h}(1-\zeta)^{-1}$ and $b_4 = \tau(1-\zeta)^{-1}-1$. Hence $\hat{b}$ with $b_1 = 0$ is unique, and therefore N is unique as well. A parallel argument for $P(N) = P_6$ yields $N = \langle \hat{p}_6,(\hat{b},1,(1324))\rangle$ with $\hat{b} = [0,\mathfrak{h},(\mathfrak{h}+1)(1+\zeta)^{-1}\zeta-1,\mathfrak{h}-(\mathfrak{h}+1)(1+\zeta)^{-1}\zeta]$. Note that these two N are the opposites of those whose p-Sylow subgroup is P_1 as determined above. As such, there are none with P_2 as their p-Sylow subgroup.

Case $R(C_{4p},[D_{2p}])$

Each possible copy of D_{2p} shall be viewed as an extension of C_p by V, generated by an element of order p, and two elements of order 2, one of which generates the center and one which inverts the order p element. So, by 6.3, for $P(N) = P_1$, we have three possibilities for a fixed point free copy of D_{2p},

$$\langle \hat{p}_1,(\hat{a},1,(12)(34))(\hat{b},-1,(13)(24))\rangle \\ \langle \hat{p}_1,(\hat{b},1,(13)(24)),(\hat{a},-1,(12)(34))\rangle \\ \langle \hat{p}_1,(\hat{c},1,(14)(23)),(\hat{a},-1,(12)(34))\rangle$$

where the first order two element in each case is central. As $Z(N)$ is characteristic, then $\lambda(x)$ must centralize each such order 2 element, which, since $(1324)(ij)(kl)(1423) = (ij)(kl)$ if and only if $(ij)(kl) = (1324)^2$ rules out the

latter two possibilities. We calculate the action of $\lambda(x)$ on $(\hat{a},1,(12)(34))$ and find that $(\hat{a},1,(12)(34)) = ([1,-1,0,0]+(1324)(\hat{a}),1,(12)(34))$. Since, by 5.10, $a_1 = -a_2$ and $a_3 = -a_4$ then we must have, for instance, that $2a_4 = -1$ and therefore that $\hat{a} = [\mathfrak{h},-\mathfrak{h},\mathfrak{h},-\mathfrak{h}]$. Now if x is the generator of order p and z the centralizing element of order 2 and t the non-central generator of order 2 then the other non-central order 2 elements are of the form $x^k t$ and $x^k tz$. This means that if $(\hat{b},-1,(13)(24))$ is non-central, then all other non-central elements of order 2 are of the form $(k\hat{p}_1+\hat{b},-1,(13)(24))$ and $(\hat{a},1,(12)(34))(k\hat{p}_1+\hat{b},-1,(13)(24)) = (k\hat{p}_1+\hat{b}-\hat{a},-1,(14)(23))$. Conjugating $(\hat{b},-1,(13)(24))$ by $\lambda(x)$ yields $([1,0,0,1]+(1324)(\hat{b}),-1,(14)(23))$ which therefore must equal $(k\hat{p}_1+\hat{b}-[\mathfrak{h},-\mathfrak{h},\mathfrak{h},-\mathfrak{h}],-1,(14)(23))$ and so we find that $b_1 = b_1+4k-2$ and thus $k = \mathfrak{h}$. This means that all the $\hat{b}$ in N are of the form $[b_1,b_1-1,b_1,b_1-1]$ for $b_1 \in \mathbb{F}_p$. The point is that there is only one N with $P(N) = P_1$.

If $P(N) = P_2$ then $N = \langle \hat{p}_2,(\hat{a},1,(12)(34)),(\hat{b},1,(13)(24))\rangle$ since, of the elements of order 2 in 6.3 that centralize $\hat{p}_2$, only those of the form $(\hat{a},1,(12)(34))$ are centralized by $\hat{p}_1$. Conjugating $(\hat{a},1,(12)(34))$ by $\lambda(x)$ yields $([1,-1,0,0]+(1324)(\hat{a}),1,(12)(34))$ and as this must equal $(\hat{a},1,(12)(34))$ we conclude that $\hat{a} = [\mathfrak{h},-\mathfrak{h},\mathfrak{h},-\mathfrak{h}]$. For $\hat{b}$ we conjugate by $\lambda(x)$ and obtain $([1,0,0,-1]+(1324)(\hat{b}),1,(14)(23))$ which must equal $(k\hat{p}_2+\hat{b}-\hat{a},1,(14)(23))$ and, if we choose the unique $\hat{b}$ with $b_1 = 0$ (whence $b_3 = 0$) we find that, in fact, b_2 and b_4 are both 0 also, hence $\hat{b} = \hat{0}$.

As there is one N with $P(N) = P_1$ and one with $P(N) \neq P_1$ we are done.

Case $R(C_{4p},[Q_p])$

A given N is generated by an element of order p and one of order 4 where the order 4 generator inverts the order p generator. If $P(N) = P_1$ then $N = \langle \hat{p}_1,(\hat{b},-1,(ijkl))\rangle$. Conjugating $(\hat{b},-1,(ijkl))$ by $\lambda(x)$ yields

$$([1,0,0,0]+(1342)(\hat{b})-(1324)(ijkl)([0,0,0,-1]),-1,(1324)(ijkl)(1423))$$

and as $(1324)(ijkl)(1423)$ cannot equal $(ilkj)$ then $(ijkl) = (1324)$ or (1423). Now if $(\hat{b},-1,(ijkl))$ has order 4 then all other order 4 elements must have the form $(k\hat{p}_1+\hat{b},-1,(ijkl))$ or $(k\hat{p}_1+(ilkj)(\hat{b}),-1,(ilkj))$. As such, we may assume that $(ijkl) = (1324)$ and so we have

$$((1324)(\hat{b})+[1,0,1,0],-1,(1324)) = (k\hat{p}_1+\hat{b},-1,(1324))$$

which leads to $\hat{b} = [b_1, b_1, b_1 + \mathfrak{h}, b_1 - \mathfrak{h}]$ for $b_1 \in \mathbb{F}_p$ (i.e. $k = \mathfrak{h}$). As such, N with $P(N) = P_1$ is unique. For $P(N) = P_2$ we have $N = \langle \hat{p}_2, (\hat{b}, 1, (1423)) \rangle$ or $\langle \hat{p}_2, (\hat{b}, 1, (1324)) \rangle$ and since $(\hat{b}, 1, (1423))^{-1} = (-(1324)(\hat{b}), 1, (1324))$ we may assume that $N = \langle \hat{p}_2, (\hat{b}, 1, (1423)) \rangle$. In order for $\lambda(x)$ to normalize N we find that the $(\hat{b}, 1, (1324))$ with $b_1 = 0$ is uniquely $[0, 0, \mathfrak{h}, -\mathfrak{h}]$ and as such N is unique also.

As with $[D_{2p}]$ above there are no N with $P(N) = P_5$ or P_6.

□

Proposition 6.7: *For $\Gamma = C_p \times V$ we have,*

$$\begin{aligned} R(C_p \times V, [C_{4p}]) = \{ & \langle\ \hat{p}_1,\ (\hat{0}, 1, (1324))\ \rangle, \\ & \langle\ \hat{p}_1,\ (\hat{0}, 1, (1243))\ \rangle, \\ & \langle\ \hat{p}_1,\ (\hat{0}, 1, (1234))\ \rangle \} \end{aligned}$$

$$R(C_p \times V, [C_p \times V]) = \{\ \langle\ \hat{p}_1,\ (\hat{0}, 1, (12)(34)),\ (\hat{0}, 1, (13)(24))\ \rangle\ \}$$

$$R(C_p \times V, [E_p]) = \emptyset$$

$$\begin{aligned} R(C_p \times V, [D_{2p}]) = \{ & \langle\ \hat{p}_1,\ (\hat{0}, 1, (12)(34)), (\hat{0}, -1, (13)(24))\ \rangle, \\ & \langle\ \hat{p}_1,\ (\hat{0}, 1, (13)(24)),\ (\hat{0}, -1, (12)(34))\ \rangle, \\ & \langle\ \hat{p}_1,\ (\hat{0}, 1, (14)(23)),\ (\hat{0}, -1, (12)(34))\ \rangle, \\ & \langle\ \hat{p}_2,\ (\hat{0}, 1, (12)(34)),\ (\hat{0}, 1, (13)(24))\ \rangle, \\ & \langle\ \hat{p}_3,\ (\hat{0}, 1, (13)(24)),\ (\hat{0}, 1, (12)(34))\ \rangle, \\ & \langle\ \hat{p}_4,\ (\hat{0}, 1, (14)(23)),\ (\hat{0}, 1, (12)(34))\ \rangle \} \end{aligned}$$

$$\begin{aligned} R(C_p \times V, [Q_p]) = \{ & \langle\ \hat{p}_1,\ (\hat{0}, -1, (1234))\ \rangle, \\ & \langle\ \hat{p}_1,\ (\hat{0}, -1, (1324))\ \rangle, \\ & \langle\ \hat{p}_1,\ (\hat{0}, -1, (1243))\ \rangle, \\ & \langle\ \hat{p}_2,\ (\hat{0}, 1, (1324))\ \rangle, \\ & \langle\ \hat{p}_3,\ (\hat{0}, 1, (1234))\ \rangle, \\ & \langle\ \hat{p}_4,\ (\hat{0}, 1, (1243))\ \rangle\ \} \end{aligned}$$

Proof. The generators of $\lambda(\Gamma)$ are $\hat{p}_1$, $\lambda(t_1) = (\hat{0}, 1, (12)(34))$ and $\lambda(t_1) = (\hat{0}, 1, (13)(24))$. Using 5.10 and 6.3 one argues as before to determine generators of possible (regular) N and then determine which are, in fact, normalized by $\lambda(\Gamma)$. The case of $R(C_p \times V, [E_p])$ bears some explanation. If $P(N) = P_1$ then $N = \langle \hat{p}_1, (\hat{b}, \zeta, (ijkl)) \rangle$ where $(\hat{b}, \zeta, (ijkl))^{-1} = (\zeta(ilkj)\hat{b}, \overline{\zeta}, (ilkj))$. By direct calculation

$$\lambda(t_1)(\hat{b}, \zeta, (ijkl))\lambda(t_1) = ((12)(34)(\hat{b}), \zeta, (12)(34)(ijkl)(12)(34))$$

which requires that $(12)(34)(ijkl)(12)(34) = (ijkl)$, that is $(ijkl)^2 = (12)(34)$. If $(ijkl) = (1324)$ then

$$\lambda(t_2)(\hat{b}, \zeta, (1324))\lambda(t_2) = ((13)(24)(\hat{b}), \zeta, (1423))$$

but $((13)(24)(\hat{b}), \zeta, (1423)) \notin N$. A similar contradiction arises if $(ijkl) = (1423)$. As there are no N with $P(N) = P_1$ then, by 4.3, there are no N with $P(N) \neq P_1$ either. □

We note how $|R(C_p)|$ and $|R(C_p \times V)|$ are combinatorially determined. For $\Gamma = E_p$, D_{2p}, and Q_p the number of N that arise depends on p in a linear fashion.

Proposition 6.8: *For $\Gamma = E_p$ we have*

$$R(E_p,[C_{4p}]) = \{\ \langle \hat{p}_1,\ (b[1,-1,\overline{\zeta},\zeta],1,(1324))\ \rangle | b \in \mathbb{F}_p\ \}$$

$$\begin{aligned} R(E_p,[C_p \times V]) = \{\ \langle\ \hat{p}_1,\ & (a[1,-1,\overline{\zeta},\zeta],1,(12)(34)), \\ & (a[(\overline{\zeta}+1)^{-1},(\zeta-1)^{-1},-(\overline{\zeta}+1)^{-1},-(\zeta-1)^{-1}],1,(13)(24))\ \rangle | a \in \mathbb{F}_p\ \} \end{aligned}$$

$$\begin{aligned} R(E_p,[E_p]) = \big\{ & \{\ \langle\ \hat{p}_1,\ (b[0,\zeta-1,-1,\zeta],\zeta,(1423))\ \rangle | b \in \mathbb{F}_p\ \}, \\ & \langle\ \hat{p}_1,\ (\hat{0},\zeta,(1324))\ \rangle, \\ & \{\ \langle\ \hat{p}_5,\ (b[0,0,\overline{\zeta},\zeta],1,(1324))\ \rangle | b \in \mathbb{F}_p\ \}, \\ & \langle\ \hat{p}_6,\ (\hat{0},1,(1324))\ \rangle \big\} \end{aligned}$$

$$\begin{aligned} R(E_p,[D_{2p}]) = \big\{ & \{\ \langle\ \hat{p}_1,\ (a[1,-1,\overline{\zeta},\zeta],1,(12)(34)), \\ & (a[0,-(\overline{\zeta}+1),0,-(\overline{\zeta}+1)],-1,(13)(24))\ \rangle | a \in \mathbb{F}_p\ \}, \\ & \{\ \langle\ \hat{p}_2,\ (a[1,-1,\overline{\zeta},\zeta],1,(12)(34)), \\ & (a[0,-(\zeta+1),0,(\overline{\zeta}+1)],1,(13)(24))\ \rangle | a \in \mathbb{F}_p\ \}\big\} \end{aligned}$$

$$\begin{aligned} R(E_p,[Q_p]) = \big\{ & \{\ \langle\ \hat{p}_1,\ (b[0,(\zeta-1),-1,\zeta],-1,(1324))\ \rangle | b \in \mathbb{F}_p\ \} \\ & \{\ \langle\ \hat{p}_2,\ (b[0,(\overline{\zeta}-1),1,\zeta],1,(1324))\ \rangle | b \in \mathbb{F}_p\ \}\big\} \end{aligned}$$

Proof. Recall, from 6.2, that $\lambda(\Gamma)$ is generated by $\hat{p}_1$ and $\lambda(t) = (\hat{0},\overline{\zeta},(1324))$ and so we again look for N which are normalized by these generators.

Case $R(E_p,[C_{4p}])$

For $P(N) = P_1$ we have (by 6.3) that $N = \langle \hat{p}_1, (\hat{b}, 1, (ijkl)) \rangle$. Conjugating $(\hat{b}, 1, (ijkl))$ by $\lambda(t)$ yields

$$(\overline{\zeta}(1324)(\hat{b}), 1, (1324)(ijkl)(1423))$$

and since $(\hat{b}, 1, (ijkl))^{-1} = (-(ilkj)(\hat{b}), 1, (ilkj))$ we may assume that $(ijkl) = (1324)$. This implies that $(\overline{\zeta}(1324)(\hat{b}), 1, (1324)) = (k\hat{p}_1 + \hat{b}, 1, (1324))$ and, by 5.10, that the sum of the coordinates of $\hat{b}$ must add to zero. Thus $4k = 0$, hence $k = 0$ and therefore

$$\begin{aligned} b_1 &= \zeta b_4 \\ b_2 &= \zeta b_3 \\ b_3 &= \zeta b_1 \\ b_4 &= \zeta b_2 \end{aligned}$$

which implies that $\hat{b} = b[1, -1, \overline{\zeta}, \zeta]$. However, given $(\hat{b}, 1, (ijkl))$, an order 4 element (and consequently a generator), all other order 4 elements of N must be of the form $(k\hat{p}_1 + \hat{b}, 1, (ijkl))$ and $(k\hat{p}_1 - (ilkj)(\hat{b}), 1, (ilkj))$. As such, no *two* elements of the form $b[1, -1, \overline{\zeta}, \zeta]$ can lie in the same subgroup N, i.e. $k\hat{p}_1 + b[1, -1, \overline{\zeta}, \zeta] = b'[1, -1, \overline{\zeta}, \zeta]$ is impossible. Thus, each choice of $b \in \mathbb{F}_p$ gives rise to a distinct group N.

Case $R(E_p, [E_p])$

In [7], Childs, with Byott's technique in mind, considers regular embeddings of groups G into $InHol(G) = G \cdot Inn(G) \leq Perm(G)$ and counts the Hopf Galois structures resulting from this class of embeddings. Two results from this intersect with ours in the count of $|R(E_p, [E_p])|$.

Theorem: [7, Theorem 6.5] *Let $G = \mathbb{Z}_h \rtimes \mathbb{Z}_k$ with $h = p^e$, p odd, and $k = qp^f$ with $q > 1$ and coprime to p. The number of fixed-point free endomorphisms of G is*

$$\mathcal{E}(G) = \phi(p^f)p^f + \phi(p^f)(\phi(q) - 1)p^e$$

and there are exactly $2\mathcal{E}(G)$ equivalence classes of regular embeddings of G into $InHol(G)$.

For $G = E_p$, $e = 1$, $q = 4$, and $f = 0$, therefore $\mathcal{E}(G) = p + 1$ and so $2\mathcal{E}(G) = 2p + 2$. As Byott's technique establishes a 1-1 correspondence between regular embeddings of G into $Hol(G)$ and $R(G, [G])$, this value (2p+2) is a

lower bound, as Childs points out in the paragraph preceding [7, Theorem 8.1]. However, through our method we know that this lower bound is, in fact, the exact value for $|R(E_p,[E_p])|$. In [7, Corollary 8.3], Childs considers the number of Hopf Galois actions of $H_1 = (L[G])^G$ on an extension of fields L/K with $G = Gal(L/K)$ where G is a semidirect product as given above, and shows that there are exactly $\mathcal{E}(G)$ different actions by H_1 on L/K. So, for $G = E_p$, this is, again, $p+1$ which corresponds precisely to the N in $R(E_p,[E_p])$ where $P(N) = P_1 = \mathcal{P}$. □

Proposition 6.9: *For $\Gamma = D_{2p}$ we have (where $\mathfrak{h} = 2^{-1}$ in $\mathbb{F}_p$)*

$$\begin{aligned}
R(D_{2p},[C_{4p}]) = \big\{ &\{ \langle\ \hat{p}_1,\ ([b,b,-b-\mathfrak{h},-b+\mathfrak{h}],1,(1324))\ \rangle | b\in\mathbb{F}_p\},\\
&\{ \langle\ \hat{p}_1,\ ([b,-\mathfrak{h},-b,\mathfrak{h}],1,(1234))\ \rangle | b\in\mathbb{F}_p\ \},\\
&\{ \langle\ \hat{p}_1,\ ([b,-\mathfrak{h},-\mathfrak{h},-b+1],1,(1243))\ \rangle | b\in\mathbb{F}_p\ \}\big\}
\end{aligned}$$

$$\begin{aligned}
R(D_{2p},[C_p\times V]) = \{ &\langle\ \hat{p}_1,\ ([\mathfrak{h},-\mathfrak{h},-\mathfrak{h},\mathfrak{h}],1,(12)(34)),\\
&([b,b-1,-b,-b+1],1,(13)(24))\rangle | b\in\mathbb{F}_p\}
\end{aligned}$$

$$R(D_{2p},[E_p]) = \emptyset$$

$$\begin{aligned}
R(D_{2p},[D_{2p}]) = \big\{ &\langle\ \hat{p}_1,\ ([\mathfrak{h},-\mathfrak{h},-\mathfrak{h},\mathfrak{h}],1,(12)(34)),(\hat{0},-1,(13)(24))\rangle\\
&\{ \langle\ \hat{p}_1,\ ([b,b-1,-b,-b+1],1,(13)(24)),\\
&([0,0,1-2b,1-2b],-1,(12)(34))\ \rangle | b\in\mathbb{F}_p\ \},\\
&\{ \langle\ \hat{p}_1,([c,c,-c,-c],1,(14)(23)),\\
&([0,0,c\mathfrak{h},c\mathfrak{h}],-1,(12)(34))\ \rangle | c\in\mathbb{F}_p\ \},\\
&\langle\ \hat{p}_2,\ ([\mathfrak{h},-\mathfrak{h},-\mathfrak{h},\mathfrak{h}],1,(12)(34)),\ ([0,-1,0,1],1,(13)(24))\ \rangle,\\
&\{ \langle\ \hat{p}_3,\ ([b,b-1,-b,-b+1],1,(13)(24)),\\
&([0,0,-1,1],1,(12)(34))\ \rangle | b\in\mathbb{F}_p\ \},\\
&\{ \langle\ \hat{p}_4,\ ([c,c,-c,-c],1,(14)(23)),\\
&(\hat{0},1,(12)(34))\ \rangle | c\in\mathbb{F}_p\ \}\ \}
\end{aligned}$$

$$
\begin{aligned}
R(D_{2p},[Q_p]) = \{ & \langle\ \hat{p}_1,\ ([0,-1,-\mathfrak{h},-\mathfrak{h}],-1,(1324))\ \rangle, \\
& \{\ \langle\ \hat{p}_1,\ ([0,b,b,2b],-1,(1342))\ \rangle | b \in \mathbb{F}_p\ \}, \\
& \{\ \langle\ \hat{p}_1,\ ([0,b,-1,-b-1],-1,(1234))\ \rangle | b \in \mathbb{F}_p\ \}, \\
& \langle\ \hat{p}_2,\ ([0,-1,\mathfrak{h},\mathfrak{h}],1,(1423))\ \rangle, \\
& \{\ \langle\ \hat{p}_3,\ ([0,\mathfrak{h}(b-1),-b,\mathfrak{h}(b+1)],1,(1234))\ \rangle | b \in \mathbb{F}_p\ \}, \\
& \{\ \langle\ \hat{p}_4,\ ([0,\mathfrak{h}(b-1),\mathfrak{h}(b-1),1-b],1,(1243))\ \rangle | b \in \mathbb{F}_p\ \}\ \}
\end{aligned}
$$

Proof. For all candidate N we check for normalization by $\lambda(x) = ([1,0,0,1],1,(12)(34))$ and $\lambda(t) = (\hat{0},-1,(13)(24))$ as given in 6.2.

Case $R(D_{2p},[D_{2p}])$ with $P(N) = P_1$

For $P(N) = P_1$ we have three cases, one for each possible choice of center of N. When $Z(N) = \langle(\hat{a},1,(12)(34))\rangle$ we find that $\hat{a}$ must be $[\mathfrak{h},-\mathfrak{h},-\mathfrak{h},\mathfrak{h}]$ and the other generator must be $(\hat{0},-1,(13)(24))$. For $Z(N) = \langle(\hat{b},1,(13)(24))\rangle$ we have that $\hat{b} = [b,b-1,-b,-b+1]$ for $b \in \mathbb{F}_p$ which means that we have p different N. And for each choice of b we have that the other generator $(\hat{a},-1,(12)(34))$ (where $a_1 = 0$) requires, by the commutativity relations in 6.5, that $\hat{a} = ([0,0,1-2b,1-2b]$. For $Z(N) = \langle(\hat{c},1,(14)(23))\rangle$ we again have a parameterization $\hat{c} = [c,c,-c,-c]$ for $c \in \mathbb{F}_p$. For each such $\hat{c}$, the other generator (uniquely chosen to have its first coordinate 0) must, again by commutativity relations as in 6.5, be of the form $([0,0,\mathfrak{h}c,\mathfrak{h}c],-1,(12)(34))$.

□

Proposition 6.10: *For $\Gamma = Q_p$ we have (where $\mathfrak{h} = 2^{-1}$ in $\mathbb{F}_p$)*

$$R(Q_p,[C_{4p}]) = \{\langle \hat{p}_1, ([b,b,-\mathfrak{h}-b,\mathfrak{h}-b],1,(1324))\rangle | b \in \mathbb{F}_p\}$$

$$\begin{aligned} R(Q_p,[C_p\times V]) = \{&\langle \hat{p}_1, ([\mathfrak{h},-\mathfrak{h},-\mathfrak{h},\mathfrak{h}],1,(12)(34)),\\ &([b,b-1,-b,-b+1],1,(13)(24))\rangle | b \in \mathbb{F}_p\} \end{aligned}$$

$$\begin{aligned} R(Q_p,[E_p]) = \big\{&\{\langle \hat{p}_1, ([0,\mathfrak{h}(\zeta-1),b,b+\mathfrak{h}(\zeta+1)],\zeta,(1324))\rangle | b \in \mathbb{F}_p\},\\ &\{\langle \hat{p}_1, ([0,\mathfrak{h}(\zeta-1),b,b+\mathfrak{h}(1-\zeta)],\zeta,(1423))\rangle | b \in \mathbb{F}_p\},\\ &\{\langle \hat{p}_5, ([0,b(\zeta+1)-1,-b\zeta+\mathfrak{h},-b+\mathfrak{h}],1,(1423))\rangle | b \in \mathbb{F}_p\},\\ &\{\langle \hat{p}_6, ([0,b(1-\zeta),b\zeta-\mathfrak{h},-b+\mathfrak{h}],1,(1324))\rangle | b \in \mathbb{F}_p\}\big\} \end{aligned}$$

$$\begin{aligned} R(Q_p,[D_{2p}]) = \{&\langle \hat{p}_1, ([\mathfrak{h},-\mathfrak{h},-\mathfrak{h},\mathfrak{h}],1,(12)(34)),(\hat{0},-1,(13)(24))\rangle,\\ &\langle \hat{p}_2, ([\mathfrak{h},-\mathfrak{h},-\mathfrak{h},\mathfrak{h}],1,(12)(34)),([0,-1,0,1],1,(13)(24))\rangle\} \end{aligned}$$

$$\begin{aligned} R(Q_p,[Q_p]) = \{&\langle \hat{p}_1, ([0,-1,-\mathfrak{h},-\mathfrak{h}],-1,(1324))\rangle,\\ &\langle \hat{p}_2, ([0,0,-\mathfrak{h},\mathfrak{h}],1,(1324))\rangle\} \end{aligned}$$

Proof. By 6.2, the generators of $\lambda(\Gamma)$ are $\lambda(x) = ([1,0,0,1],1,(12)(34))$ and $\lambda(t) = ([\mathfrak{h},-\mathfrak{h},0,0],-1,(1324))$ and the various cases are computed in a similar fashion to $R(E_p)$. □

References

[1] W. Burnside. *Theory of groups of finite order*. Cambridge University Press, 1911.

[2] N.P. Byott. Uniqueness of hopf galois structure of separable field extensions. *Comm. Algebra*, 24:3217–3228, 1996.

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

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

[5] L. Childs. On the hopf galois theory for separable field extensions. *Comm. Algebra*, 17(4):809–825, 1989.

[6] L. Childs. *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, volume 80 of *Amer. Math. Soc. Mathematical Surveys and Monographs*. American Mathematical Society, 2000.

[7] L. Childs. Cayley's theorem and hopf galois structures arising from semidirect products of cyclic groups (w/ j. corradino). *J. Algebra*, 308(1):236–251, 2007.

[8] J. Dixon and B. Mortimer. *Permutations Groups*. Number 163 in GTM. Springer, New York, 1996.

[9] L.E. Dickson G. Miller, H. Blichfeldt. *Theory and Applications of Finite Groups*. Wiley, New York, 1916.

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

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

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

[13] F. Hoffman. Subgroups of holomorphs of groups. *Amer. Math. Monthly*, 83:126–127, 1976.

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

[15] J.J. Malone. The group of automorphisms of a distributively generated near ring. *Proc. Amer. Math. Soc.*, 88:11–15, 1983.

[16] W.H. Mills. Multiple holomorphs for finitely generated abelian groups. *Trans. Amer. Math. Soc.*, 71:379–392, 1951.

[17] W.H. Mills. On the non-isomorphism of certain holomorphs. *Trans. Amer. Math. Soc.*, 74:428–443, 1953.

[18] H. Nakano. Representation of a group by transformations on its subgroups. *Math. Ann.*, 181:173–180, 1969.

[19] H. Nakano. Transformation groups on a group. *Math. Ann.*, 181:81–96, 1969.

[20] H. Nakano. Automoration groups. *Proc. London Math. Soc.*, 24, 1972.

[21] B.H. Neumann. Twisted wreath products of groups. *Arch. Math.*, 14:1–6, 1963.

[22] P.M. Neumann. On the structure of standard wreath products. *Math. Zeitschr.*, 84:343–373, 1964.

[23] W.R. Scott. *Group Theory*. Prentice Hall, Englewood Cliffs, New Jersey, 1964.

[24] M. Sweedler. *Hopf Algebras*. Benjamin, New York, 1968.

[25] G. Walls. Automorphism groups. *Amer. Math. Monthly*, 93:459–462, 1986.

[26] H. Weilandt. *Finite Permutation Groups*. Academic Press, New York, 1964.

[27] C. Wells. Some applications of the wreath product construction. *Amer. Math. Monthly*, 83:317–338, 1976.