MT5999: Constructing a Database of Primitive Permutation Groups

Christopher Russell
Supervised by Colva Roney-Dougal

April 22, 2016

Acknowledgements

I would like to Colva Roney-Dougal for her support and guidance throughout the project.

I certify that this project report has been written by me, is a record of work carried out by me, and is essentially different from work undertaken for any other purpose or assessment.

Abstract

This paper sets out to reproduce the proof of three out of the five cases of the O'Nan-Scott Theorem. Prior to this, the necessary background in permutation group theory is presented with detailed proofs of selected results and demonstrative examples. Wreath products and their product action are then defined in detail with personally adapted notation. Finally a description is provided of how the primitive group library in GAP has been extended to match the larger library in MAGMA. This conversion will be of use to researchers using GAP to check

Contents

1 Introduction 6
1.1 Background . . . 6
1.2 Aims . . . 6
1.3 The Journey . . . 6
1.4 Prerequisites . . . 7
1.5 Notation . . . 7

2 From Group Actions to Primitivity 8
2.1 Group Actions . . . 8
2.2 Orbits, Stabilizers and Transitivity . . . 11
2.3 Blocks and Primitivity . . . 15

3 Semidirect products and Wreath Products 19
3.1 Semidirect Products . . . 19
3.2 Wreath Products . . . 20

4 The Socle 25

5 The Diagonal Action 28

6 The O'Nan-Scott Theorem 30
6.1 The Types . . . 30
6.2 The O'Nan-Scott Theorem . . . 31
6.3 Proving the O'Nan-Scott Theorem . . . 31
6.3.1 Finite Primitive Groups with Regular Abelian Socles . . . 32
6.3.2 Finite Primitive Groups with Nonregular Socles . . . 35

7 The Primitive Database 40
7.1 Historical Background . . . 40
7.2 The Database Conversion . . . 40
7.3 Testing for accuracy . . . 42

8 Conclusion 43

9 Appendix 45
9.1 Creation of new database files . . . 45
9.1.1 The program . . . 45
9.1.2 Making the files . . . 52
9.2 Accuracy Checks . . . 53
9.2.1 Test 1 . . . 53
9.2.2 Test 2 . . . 54

1 Introduction

1.1 Background

The study of primitive permutation groups important to the most fundamental problem of group theory - classifying all groups up to isomorphism. The famous theorem of Cayley shows that all groups are isomorphic to permutation groups. Primitive groups are the building blocks of permutation groups in the sense that imprimitive groups can be constructed from primitive groups (see Example 3.8) and intransitive groups (see Theorem 2.16) can be constructed from transitive groups, so a classification of primitive groups leads to a classification of all permutation groups. The O'Nan-Scott Theorem provides a complete classification of the finite primitive groups and has enabled the creation of large computer databases for primitive groups. These databases are powerful tools for researchers, who may use them to disprove false conjectures or provide evidence for claims.

1.2 Aims

This project had two main aims: to understand the theory required to classify the finite primitive permutation groups via the O'Nan-Scott Theorem and to update the primitive permutation group library in the GAP computer software to match a larger database existing in MAGMA. The write up aims to present the theory I have learned and to detail the database conversion which I have performed. The vast majority of the theory presented will be from [1] which has been my guide to the subject. My intention has been to present, with as many proofs as possible, the minimum amount of the theory needed to prove the O'Nan-Scott Theorem. It has also been my aim to present the theory at a level of detail that I think myself, or another final year undergraduate, would appreciate when being introduced to this subject. To this end, I have tried to rewrite many of the proofs I use from [1] written in my own style and with more detail. I have also included my solutions to specific exercises from [1] and some of my own examples to demonstrate definitions.

1.3 The Journey

We begin with group actions which are the basis of the language of permutation groups. Equipped with actions, we define the transitive groups, primitive groups and prove key results whilst also hinting at their usefulness. We will then define the wreath product construction and its product action, both of which are key to the study of primitive groups. In Section 4 we study the socle of a group which turns out to be central to much of our later analysis. Next we indirectly use the product action of a wreath product to define the groups of diagonal type. With all of these tools we introduce the O'Nan-Scott Theorem and then prove three of the five cases, and part of the fourth. Finally there is a brief history of the classification of primitive permutation groups followed by a description of the GAP database and the conversion.

1.4 Prerequisites

A reader who has taken a final or penultimate year undergraduate course in group theory should be sufficiently equipped. In particular, Section 2 should be very accessible. Wreath products (Section 3) are tricky and are the main obstacle to the remaining sections, where they are often important. In particular, knowledge of symmetric groups, group homomorphisms, internal and external direction products and automorphism groups will be important throughout. In Section 6 there is some linear algebra and foreknowledge of the linear groups will be useful.

1.5 Notation

$Sym(\Omega)$	The symmetric group on the set Ω.
S_n	The symmetric group on the set $\{1, 2, .., n\}$.
A_n	The alternating group on the set $\{1, 2, .., n\}$
C_n	The cyclic group of order
1_G	The identity of the group G, often simply 1.
$\|\Omega\|$	The cardinality (size) of a set Ω
$\ker(\phi)$	The kernel of ϕ
$im(\phi)$	The image of ϕ
$Z(G)$	the center of a group G
$N_G(H)$	the normalizer of a subgroup H in G
$C_G(H)$	the certralizer of a subgroup H in G

2 From Group Actions to Primitivity

2.1 Group Actions

Let G be a subgroup of the symmetric group on some set Ω. Then each $x \in G$ moves (or fixes) the points in Ω and we describe this situation as G acting on Ω. Our aim is to allow abstract groups to behave like permutation groups, that is to act on a set. To do this we define a *group action* which generalises how permutation groups act on sets.

Definition 2.1. Let G be a group. An *action* of G on a set Ω is a function $\Omega \times G \to \Omega$ defined by $(\alpha, g) \mapsto \alpha^g$ which satisfies the following:

(i) $\alpha^1 = \alpha$ for all $\alpha \in \Omega$ (where 1 is the identity of G); and
(ii) $\alpha^{xy} = (\alpha^x)^y$ for all $\alpha \in \Omega$ and all $x, y \in G$.

An *action* of G on a group K *as a group* is a function $K \times G \to K$ defined by maps $(\alpha, g) \mapsto \alpha^g$ which acts on K as a set and also satisfies the additional condition:

(iii) $(hk)^x = h^x k^x$ for all $h, k \in K$ and all $x \in G$

There are a number of conventions in the language of group actions which we will follow. Herein the use of the words *act*, *acts* and *acting* will be used to imply the existence of an action. The superscript notation α^x will be used to denote the image of (α, x) in a group action, when the action is clear. When an action is defined on a set, it is implied that the set is nonempty. Finally whenever Ω is a set and $G \leqslant Sym(\Omega)$ the action of G on Ω will be the natural action unless otherwise stated.

Every group is isomorphic to a permutation group so we might also have thought to let abstract groups act on a set via an isomorphism to a subgroup of the symmetric group on that set. It would then also be reasonable to allow for more actions via homomorphisms that are not injective. There is at the very least one homomorphism from any abstract group into the symmetric group on any set - the homomorphism which sends everything to the identity. The following propositions start to explore the link between group actions and group homomorphisms into symmetric groups.

Proposition 2.2. *Let G be a group which acts on the set Ω. Then for all $x \in G$ the mapping $\overline{x} : \Omega \to \Omega$ defined by $\alpha \mapsto \alpha^x$ is an element of $Sym(\Omega)$. Moreover, if G acts on a group H as a group then $\overline{y} : K \to K$ defined by $k \mapsto k^x$ is an element of $Aut(K)$.*

Proof. We need to show that $\overline{x}$ is a bijection and then we know it is a permutation of Ω. The following statements hold for all $\alpha \in \Omega$ and are consequences of the definition of a group action:

$$(\alpha^{\overline{x^{-1}}})^{\overline{x}} = (\alpha^{x^{-1}})^{x} = \alpha^1 = (\alpha^x)^{x^{-1}} = (\alpha^{\overline{x}})^{\overline{x^{-1}}}$$
$$\alpha^1 = \alpha$$

and together they imply that the inverse of $\overline{x}$ is $\overline{x^{-1}}$. Thus $\overline{x}$ is a bijection because it has an inverse.

Now $\overline{y}$ is a bijection from K to K follows immediately by setting $\Omega := K$. Furthermore $\overline{y}$ is a group homomorphism since G acts on H as a group implies $(gh)\overline{y} = (gh)^y = g^y h^y = (g\overline{y})(h\overline{y})$ for all $g, h \in H$. Thus $\overline{y}$ is an automorphism of H. □

Proposition 2.3. *Let G be a group which acts on a set Ω. Then function $G \to Sym(\Omega)$ defined by $x \mapsto \overline{x}$ (where $\overline{x}$ is defined as it was in Proposition 2.2) is a group homomorphism.*

Proof. Let $x, y \in G$ and we will show that $\overline{xy}$ is equal to $\overline{x} \circ \overline{y}$. Let $\alpha \in \Omega$ then

$$\begin{aligned} \alpha\overline{xy} &= \alpha^{(xy)} && \text{by definition of } \overline{xy} \\ &= (\alpha^x)^y && \text{since G acts on } \Omega \\ &= (\alpha\overline{x})^y && \text{by definition of } \overline{x} \\ &= (\alpha\overline{x})\overline{y} && \text{by definition of } \overline{y} \end{aligned}$$

and so, since α was arbitrary, $\overline{xy}$ and $\overline{x} \circ \overline{y}$ agree on all of Ω. □

A group homomorphism $G \mapsto Sym(\Omega)$ is called a *permutation representation* of G on Ω. Proposition 2.3 shows that actions define permutation representations. In fact permutation representations also define actions and these are essentially two ways of describing the same thing, which we will show next.

Proposition 2.4. [1, Ex 1.3.31] *Let G be a group, let Ω be a set and let there be a permutation representation $\psi : G \to Sym(\Omega)$. Setting $\alpha^x := \alpha^{x\psi}$ gives an action of G on Ω. Furthermore the permutation representation of this action is ψ.*

Proof. First, ψ is a group homomorphism and so ψ maps the identity of G to the identity of $Sym(\Omega)$ and so the identity of G acts like the identity of $Sym(\Omega)$ (fixes all $\alpha \in \Omega$). Furthermore, if $x, y \in G$ then:

$$\begin{aligned} \alpha^{xy} &= \alpha^{(xy)\psi} && \text{by definition} \\ &= \alpha^{(x\psi y\psi)} && \text{since } \psi \text{ is a group homomorphism} \\ &= (\alpha^{x\psi})^{y\psi} && \text{since } x\psi, y\psi \in Sym(\Omega) \text{ which acts on } \Omega \\ &= (\alpha^x)^y && \text{by definition} \end{aligned}$$

which shows that G acts on Ω. Now Proposition 2.3 says that there is a permutation representation corresponding to this action where the image of each $x \in G$ is the mapping $\alpha \mapsto \alpha^x$. This is exactly ψ since $\alpha^x = \alpha^{x\psi}$. □

The following example makes use of the equivalence of permutation representations and actions to define some actions on a set. Then the subsequent example shows how group actions on groups (as sets and groups) occur within some familiar operations.

Example 2.5. Let $G = \langle a, b\rangle = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$ be a group. Let $\psi : G \to S_4$ be a permutation representation of G which sends the generators a, b of G to $(1, 2, 3, 4), (1, 3)$, respectively. Then ψ defines an action of G on $\{1, 2, 3, 4\}$ by and the image of ψ is $\langle(1, 2, 3, 4),(1, 3)\rangle$, which is isomorphic to the dihedral group on four points. This is not the only action of G on a set. Another example is given by the non-injective permutation representation $\rho : G \to S_4$ which maps the generators of G by $a\rho = (1, 2, 3, 4)$ and $b\rho = 1_{S_4}$. In this case $im(\rho) = \langle(1, 2, 3, 4)\rangle$ is isomorphic to a cyclic group of order four. In fact any group can act on any set via the permutation representation which sends every element in the group to the identity of the corresponding symmetric group. With G and the set $\{1, 2, 3, 4\}$ the specific homomorphism is τ where $x\tau = 1_{S_4}$ for all $x \in G$.

Example 2.6. Every group acts on itself (as a set) by right multiplication. For instance, let G be a group and set $g^h := gh$ for all $h, g \in G$. Then it is easy to show this satisfies the conditions for a group action on a set. An action of a group on itself as a group is the defined by conjugation. Specifically setting $g^h := g^{-1}hg$ for all $g, h \in G$ will define an action on G as a set because conjugation of a group by one of its elements is an (inner) automorphism and automorphisms are also permutations. Furthermore this is an action on G as a group because $h^gk^g = g^{-1}hgg^{-1}kg = g^{-1}hkg = (hk)^g$ holds for all $g, h, k \in G$.

We now define some standard terminology for group actions. Let G be a group which acts on a set Ω. The *degree* of the action is the size of Ω. Additionally, let ψ be the permutation representation of this action. Then the *kernel* of the action is the kernel of ψ, $ker(\psi)$, and the action is said to be *faithful* when the kernel of ψ is trivial. The next two examples will demonstrate these ideas.

Example 2.7. Let G, ψ, ρ and τ be as in Example 2.5. Then the degree of the actions defined by ψ, ρ and τ is four in every case since they all define actions on a four element set, namely $\{1, 2, 3, 4\}$. The kernel of ψ is trivial since ψ is an isomorphism and so the corresponding action is faithful. We see that $\ker(\rho) = \{1_G, b\}$ by noticing $1_G, b \in \ker(\rho)$ and $|\ker(\rho)| = |G|/|im(\rho)| = 8/4 = 2$, by the first isomorphism theorem and since G is finite. Clearly $\ker(\tau) = G$ and the actions of G on $\{1, 2, 3, 4\}$ defined by ρ and τ are not faithful.

Example 2.8. Revisiting Example 2.6, both actions have degree $|G|$. The kernel of the action by right multiplication is trivial since $x \in G$ is in the kernel if and only if $y^x = yx = y$ for all $y \in G$ but, in particular, $1_Gx = 1_G$ if and only if $x = 1_G$. The kernel of the conjugation action depends on G. Let $x \in G$ be in the kernel of the action. Then this happens precisely when $x^{-1}yx = y$ for all $y \in G$ and that holds if and only if $yx = xy$ for all $y \in G$. So x is in the kernel if and only if $x \in Z(G)$, the center of G.

2.2 Orbits, Stabilizers and Transitivity

It will turn out to be very useful to consider how actions interact with a single element of the set being acted on. The next two definitions are key to this approach.

Definition 2.9. Let G be a group which acts on a set Ω and let $\alpha \in \Omega$. The *orbit* of α is the set

$$\alpha^G := \{\alpha^x \mid x \in G\}$$

of elements of Ω which α can be mapped to by the action.

Definition 2.10. Let G be a group which acts on a set Ω and let $\alpha \in \Omega$. The *stabilizer* of α in G is the set

$$G_\alpha := \{x \in G \mid \alpha^x = \alpha\}$$

of elements of G which fix α under the action.

The usefulness of considering the orbits of an action will become clear by then end of this section. Orbits and stabilizers have many nice properties, also suggesting they may be useful, and we will prove several of them in the next theorem.

Theorem 2.11. [1, Thm 1.4A] *Let G be a group which acts on a set Ω. Let $x, y \in G$ and let $\alpha, \beta \in \Omega$. Then:*

(i) *Two orbits α^G and β^G are either equal or disjoint and the set of all orbits is a partition of Ω*
(ii) *The stabilizer G_α is a subgroup of G*
(iii) *If $\beta = \alpha^x$ then $G_\beta = x^{-1}G_\alpha x$.*
(iv) *$\alpha^x = \alpha^y$ if and only if $G_\alpha x = G_\alpha y$*
(v) *$|\alpha^G| = |G : G_\alpha|$ for all $\alpha \in \Omega$. In particular, if G is finite then $|\alpha^G|\,|G_\alpha| = |G|$.*

Proof. Let G be a group which acts on a set Ω and let $\alpha, \beta \in \Omega$.

(i) We want to show that Ω is the disjoint union of the its distinct orbits. Assume the orbits α^G and β^G are not disjoint and that δ is an element of both. Then $\delta \in \beta^G$ implies that there exists $x \in G$ such that $\beta^x = \delta$ and so the orbits

$$\delta^G = \{\delta^y \mid y \in G\} = \{\beta^{xy} \mid y \in G\} = \{\beta^y \mid y \in G\} = \beta^G$$

are equal. Similarly $\delta \in \alpha^G$ implies that $\alpha^G = \delta^G$ and so the orbits α^G and β^G are equal. We have shown that orbits are either disjoint or equal. Furthermore every element of Ω is in at least one orbit, it's own, and so the union of the orbits is all of Ω.

(ii) The identity of G is certainly in G_α by the definition of an action. To show G_α is a subgroup of G we can show that if $x, y \in G_\alpha$ then $xy, y^{-1} \in G_\alpha$. If $x, y \in G_\alpha$ then

$$\alpha^{xy} = (\alpha^x)^y = \alpha^y = \alpha \implies xy \in G_\alpha.$$

Furthermore

$$\alpha^{y^{-1}} = (\alpha^y)^{y^{-1}} = \alpha^{yy^{-1}} = \alpha \implies y^{-1} \in G_\alpha$$

and we are done.

(iii) If $\beta = \alpha^x$ then:

$$\begin{aligned} y \in G_\beta &\iff \beta^y = \beta \text{ or, equivalently, } \alpha^{xy} = \alpha^x \\ &\iff \alpha^{xyx^{-1}} = \alpha \\ &\iff xyx^{-1} \in G_\alpha \\ &\iff y \in x^{-1}G_\alpha x \end{aligned}$$

and so $x^{-1}G_\alpha x = G_\beta$

(iv) It is quite easy to see that

$$\alpha^x = \alpha^y \iff \alpha^{xy^{-1}} = \alpha \iff xy^{-1} \in G_\alpha \iff G_\alpha xy^{-1} = G_\alpha$$

and right multiplying the final equation by y gives the result.

(v) We want to show that $|\alpha^G| = |G : G_\alpha|$ which is equivalent to showing that

$$|\{\alpha^x \mid x \in G\}| = |\{G_\alpha x \mid x \in G\}|.$$

Pick a set I of the same size as $|\alpha^G|$ and choose $\{x_i \mid i \in I\} \subseteq G$ such that $\{\alpha^{x_i} \mid i \in I\} = \alpha^G$. We claim that $\{G_\alpha x \mid x \in G\} = \{G_\alpha x_i \mid i \in I\}$ which would be sufficient since it would follow that

$$\begin{aligned} |G : G_\alpha| &= |\{G_\alpha x \mid x \in G\}| \\ &= |\{G_\alpha x_i \mid i \in I\}| \\ &= |\{x_i \mid i \in I\}| \\ &= |\alpha^G|. \end{aligned}$$

We will now prove our claim. First of all $\{G_\alpha x_i \mid i \in I\} \subseteq \{G_\alpha x \mid x \in G\}$ is clear. To see the reverse inequality consider any element y of G and the right coset $G_\alpha y$. Then since $\alpha^y \in \alpha^G = \{\alpha^{x_i} \mid i \in I\}$ there must be an $i \in I$ such that $\alpha^y = \alpha^{x_i}$ and then by (iv) we have that $G_\alpha y = G_\alpha x_i \in \{G_\alpha x_i \mid i \in I\}$ which proves the claim. Finally if G is finite then $|G : G_\alpha| = |G|/|G_\alpha|$ and this concludes the proof. □

With a certain perspective, the much studied simple groups are the most basic of groups. So with a similar mindset and a different perspective (orbits) we are interested in the permutation groups with only one orbit.

Definition 2.12. Let G be a group which acts on a set Ω. The action of G on Ω is said to be *transitive* if it has a single orbit. We will say that a group is *transitive* when it has a faithful transitive action. A group or action which is not transitive is said to be *intransitive.*

The definition of transitivity can be thought of intuitively as 'every point can be moved to every other point' and is often defined (equivalently) as: for all $\alpha, \beta \in \Omega$ then there exists $x \in G$ such that $\alpha^x = \beta$ holds. A *regular* action of some group G is a transitive action of G where all the point stabilizers, G_α for α in Ω, are trivial. The following corollary of Theorem 2.11 lists some properties of transitive groups.

Corollary 2.13. [1, Cor 1.4A] *Let G be a group which acts transitively on a set Ω. Then:*

(i) The point stabilizers form a conjugacy class of subgroups of G.

(ii) The index $|G : G_\alpha|$ is equal to $|\Omega|$ for all $\alpha \in \Omega$.

(iii) If G is finite then the action of G is regular if and only if $|G| = |\Omega|$.

Proof. Let $\alpha \in \Omega$.

(i) The stabilizers of G are subgroups by Theorem 2.11(ii). G acts transitively on Ω so $\alpha^G = \Omega$ and it follows from Theorem 2.11(iii) that every stabilizer is conjugate in G.

(ii) $\alpha^G = \Omega$ so this follows immediately from Theorem 2.11(v)

(iii) This also follows from Theorem 2.11(v), which states that $|\alpha^G||G_\alpha| = |G|$ when G is finite, because G acts regularly implies that the point stabilizer G_α is trivial. □

This section will end with concrete motivation for the study of transitive groups. The following proposition shows that intransitive groups are essentially constructed from transitive groups. All permutation groups are either transitive or intransitive since these properties complement each other. It follows that understanding the transitive groups is the key to understanding all permutation groups. Recall that K is said to be a subdirect product of groups $H_1, \dots, H_m$ if it is a subgroup of their direct product and the projection of K to any direct factor H_i is the whole of H_i.

Proposition 2.14. *Let G be a group acting intransitively on a set Ω. Then G is isomorphic to a subdirect product of transitive groups.*

Proof. Follows from Theorem 2.16. □

Actions are equivalent to their corresponding permutation representations, so it suffices to prove our proposition for any subgroup of $Sym(\Omega)$ which is intransitive. The proposition then follows in the general case because any intransitive action will have an intransitive subgroup of Ω as the image of its permutation representation. The key observation is that an instransitive action behaves like a transitive action on each of its orbits. We investigate this idea with the next lemma and then use it to prove our proposition.

Lemma 2.15. *Let $G \leqslant Sym(\Omega)$ be intransitive. Let $A \subsetneq \Omega$ be an orbit of G (since G is intransitive it has multiple orbits). Then:*

(i) For all $g \in G$, the restriction of g to A, denoted $g|_A$, is a permutation of A.

(ii) The mapping $G \to Sym(A)$ defined by $g \mapsto g|_A$ is a group homomorphism.

(iii) If $G|_A = \{g|_A \mid g \in G\}$ is the image of the homomorphism in (ii) then $G|_A$ is a transitive subgroup of $Sym(A)$.

Proof. (i) Let $g \in G$ then the restriction $g|_A$ is injective because g is injective. Moreover if $a \in A$ then $a^{g^{-1}} \in a^G = A$ and so $a = (a^{g^{-1}})^g = (a^{g^{-1}})^{g|_A} \in im(g|_A)$ for all $a \in A$. Thus we have shown $im(g|_A) = A$ so $g|_A$ is a bijection from A to A.

(ii) Let $g, h \in G$ and $a \in A$ then

$$\begin{aligned} a^{(gh)|_A} &= a^{gh} && \text{by definition} \\ &= (a^g)^h && \text{since G acts on } \Omega \\ &= (a^{g|_A})^h && \text{a is in A} \\ &= (a^{g|_A})^{h|_A} && a^{g|_A} \text{ is in A} \end{aligned}$$

and since a was arbitrary we have proved that $(gh)|_A = g|_A h|_A$ on all of A.

(iii) Let $\alpha, \beta \in A$. Then G is transitive so there exists $g \in G$ such that $\alpha^g = \beta$. Thus there is an element of $G|_A$ which maps α to β, namely $g|_A$ since $\alpha^{g|_A} = \alpha^g = \beta$. □

Theorem 2.16. *Let G be a group which acts intransitively on Ω and let the orbits of G be $A_1, \dots, A_m$. Then the groups $G|_{A_1}, \dots, G|_{A_m}$ (as defined in Lemma 2.15) are transitive on $A_1, \dots, A_m$ (respectively) and G embeds into $G|_{A_1} \times \cdots \times G|_{A_m}$ as a subdirect product.*

Proof. The groups $G|_{A_1}, \dots, G|_{A_m}$ are transitive by Lemma 2.15(iii). We prove the remainder of the theorem by defining an injective group homomorphism from G to $G|_{A_1} \times \cdots \times G|_{A_m}$ and showing the image is a subdirect product. Let ψ be defined as the function:

$$\begin{aligned} &G \to G|_{A_1} \times \cdots \times G|_{A_m} \\ &g \mapsto (g|_{A_1}, \dots, g|_{A_m}) \end{aligned}$$

which will prove our claim. The functions $g \mapsto g|_{A_i}$ are group homomorphisms (Lemma 2.15(ii)) and it follows that ψ is a group homomorphism. We now argue that ψ is injective. Let $g, h \in G$, then:

$$\begin{aligned} (gh)\psi &= ((gh)|_{A_1}, \dots, (gh)|_{A_m}) \\ &= (g|_{A_1} h|_{A_1}, \dots, g|_{A_m} h|_{A_m}) && \text{by Lemma 2.15(ii)} \\ &= (g|_{A_1}, \dots, g|_{A_m})(h|_{A_1}, \dots, h|_{A_m}) \\ &= (g\psi)(h\psi) \end{aligned}$$

and so we have shown G embeds into $G|_{A_1} \times \cdots \times G|_{A_m}$. Finally the projection of the image of G onto its i^{th} factor will be all of $G|_{A_i}$ since for every $g|_{A_i} \in G|_{A_i}$ there is the element $g\psi$ of the image of G which has $g|_{A_i}$ in the i^{th} position. □

2.3 Blocks and Primitivity

For this section we will need to make a slight extension to the notion of a group action. Let G be a group acting on Ω and define the action of an element x of G on a subset Γ of Ω to be $\Gamma^x = \{\gamma^x \mid \gamma \in \Gamma\}$. In this section we will be analysing transitive groups and the key to this will be investigating the action of a group on subsets of the set being acted on.

Definition 2.17. Let G be a group which acts transitively on a set Ω. A nonempty subset Δ of Ω is called a *block* for G if for all $x \in G$ either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \emptyset$ holds.

Every transitive action has blocks. In fact, if G is a group and Ω is a set then the singletons $\{\alpha\}$ (where $\alpha \in \Omega$) and the whole of the set Ω are blocks for any transitive action of G on Ω. These are called *trivial blocks*. Any other block, necessarily of size greater than 1 and less than $|\Omega|$, is called a *nontrival block*.

Example 2.18. Let $G = \langle(1, 2, 3, 4, 5, 6)\rangle$ be a subgroup of S_6. Then G is imprimitive and its nontrival block are $\{1, 4\}, \{2, 5\}, \{3, 6\}, \{1, 3, 5\}$ and $\{2, 4, 6\}$. The see that $\{1, 4\}$ is a block verify that

$$\{\{1, 4\}^x \mid x \in G\} = \{\{1, 4\}, \{2, 5\}, \{3, 6\}\}$$

and to see that $\{1, 3, 5\}$ is a block verify that

$$\{\{1, 3, 5\}^x \mid x \in G\} = \{\{1, 3, 5\}, \{2, 4, 6\}\}$$

We will not show that the other sets are blocks but it will immediately follow from the next proposition.

Proposition 2.19. *Let G be a group which acts transitively on a set Ω. Suppose Δ is a block for G and set $\Sigma := \{\Delta^x \mid x \in G\}$. Then:*

(i) Each set in Σ is a block for G.

(ii) Σ is a partition of Ω.

(iii) The size of Ω is equal to $|\Sigma||\Delta|$ and, in particular, if Ω is finite then $|\Delta|$ divides $|\Omega|$

Proof. (i) Let $x \in G$. We want to show that Δ^x is a block, that is for all $y \in G$ either $\Delta^{xy} = \Delta^x$ or $\Delta^{xy} \cap \Delta^x = \emptyset$. Let $y \in G$. If the intersection $\Delta^{xy} \cap \Delta^x$ is empty then there is nothing to show. Otherwise there exists $d \in \Delta^{xy} \cap \Delta^x$ and then:

$$\exists \delta, \gamma \in \Delta \text{ such that } \delta^{xy} = d = \gamma^x$$
$$\implies \delta^{xyx^{-1}} = \gamma \in \Delta.$$

Now since $\delta^{xyx^{-1}}$ is in both $\Delta^{xyx^{-1}}$ and Δ, and because Δ is a block, it follows that $\Delta^{xyx^{-1}}$ is equal to Δ. Finally, we use this to show

$$\Delta^x = (\Delta^{xyx^{-1}})^x = \Delta^{xyx^{-1}x} = \Delta^{xy}$$

which completes the proof.

(ii) The elements of Σ are pairwise disjoint because Δ is a block. The union of sets in Σ is Ω since for any $\delta \in \Delta$ we have

$$\begin{aligned} & \alpha \in \Omega \\ \implies & \exists x \in G \text{ such that } \delta^x = \alpha \text{ since } G \text{ acts transitively.} \\ \implies & \alpha \in \Delta^x \text{ which is a set in } \Sigma \\ \implies & \alpha \in \bigcup \{\Delta^x | \Delta^x \in \Sigma\} \end{aligned}$$

Thus Ω is contained in the union of sets in Σ. The reverse inclusion is clear from definition so we are done.

(iii) The blocks in Σ are of equal size because the elements of G act as permutations of Ω. Thus Σ contains $|\Sigma|$ blocks of size $|\Delta|$ and $|\Omega| = |\Sigma||\Delta|$ follows because these blocks partition Ω. □

We will call Σ the *system of blocks* containing Δ. Now our strategy is to investigate the most basic transitive groups (with respect to blocks).

Definition 2.20. Let G be a group which acts transitively on a set Ω. Then the action is said to be *primitive* if G has no nontrivial blocks on Ω. We will say a group is *primitive* if it has a primitive action. A group or action which is not primitive is said to be *imprimitive.*

Example 2.21. The group G from Example 2.18 has nontrivial blocks and is an imprimitive group. Any transitive group of prime degree is primitive because the size of blocks must divide the degree of G (Proposition 2.19(iii)). For $n \geq 2$ the symmetric group S_n is always primitive. To show this assume Δ is a nontrivial block for S_n and let $i, j \in \{1, \ldots, n\}$ such that $i \in \Delta$ but $j \notin \Delta$. Then $\Delta^{(i,j)} \neq \Delta$ and $\Delta^{(i,j)} \cap \Delta = \Delta \backslash \{i\}$ is non empty (since $|\Delta| > 1$) which contradicts Δ being a block.

One would hope that primitive groups are the key to understanding the transitive groups. Indeed it turns out that the imprimitive groups are subgroups of constructions of primitive groups. We will explain this statement in more detail after we define wreath products in Section 3.2. For now, we will describe the relationship between blocks and the structure of a group. First we will need to generalize the notion of a point stabilizer.

Definition 2.22. Let G be a group acting on a set Ω and let $\Delta \subseteq \Omega$. Then the *setwise stabilizer* of Δ in G is

$$G_{\{\Delta\}} := \{x \in G \mid \Delta^x = \Delta\}$$

Proposition 2.23. *The setwise stabilizer $G_{\{\Delta\}}$ is a subgroup of G. Furthermore, if G acts transitively and Δ is a block then Δ is an orbit of $G_{\{\Delta\}}$.*

Proof. Let G act on Ω and let $\Delta \subseteq \Omega$. Certainly 1_G fixes Δ so it we proceed by showing that $x, y \in G_{\{\Delta\}}$ implies xy and y^{-1} are in $G_{\{\Delta\}}$. If $x, y \in G_{\{\Delta\}}$ then

$$\Delta^{xy} = (\Delta^x)^y = \Delta^y = \Delta \implies xy \in G_{\{\Delta\}}.$$

Furthermore

$$\Delta^{y^{-1}} = (\Delta^y)^{y^{-1}} = \Delta^{yy^{-1}} = \Delta \implies y^{-1} \in G_{\{\Delta\}}$$

and thus $G_{\{\Delta\}}$ is a subgroup of G. Now assume G is transitive and Δ is a block and let $\alpha \in \Delta$. If $\beta \in \Delta$ then there exists $x \in G$ such that $\alpha^x = \beta$ because G is transitive. Since Δ is a block and $\beta \in \Delta \cap \Delta^x$ it must be the case that $x \in G_{\{\Delta\}}$ and so $\beta \in \alpha^{G_{\{\Delta\}}}$. We have shown $\Delta \subseteq \alpha^{G_{\{\Delta\}}}$ and the opposite inclusion is clear because $G_{\{\Delta\}}$ fixes Δ. □

We are now ready to describe the link between blocks and the setwise stabilizers of G. The next theorem will also yield a useful characterization of primitive groups as a corollary.

Theorem 2.24. [1, Thm 1.5A] *Let G be a group which acts transitively on a set Ω and let $\alpha \in \Omega$. Define the set of blocks containing α*

$$\mathcal{B} = \{\Delta \mid \Delta \textit{ is a block for } G \textit{ and } \alpha \in \Delta\}$$

and the set of groups containing the point stabilizer of α

$$\mathcal{S} = \{H \mid G_\alpha \leqslant H \leqslant G\}.$$

Then:

(i) There exists mappings $\psi : \mathcal{B} \to \mathcal{S}$ defined by $\psi(\Delta) = G_{\{\Delta\}}$ and $\phi : \mathcal{S} \mapsto \mathcal{B}$ defined by $\phi(H) = \alpha^H$.

(ii) The mappings ψ and ϕ are mutually inverse bijections.

(iii) If $\Delta, \Gamma \in \mathcal{B}$ then $\Delta \subseteq \Gamma$ if and only if $\psi(\Delta) \leqslant \psi(\Gamma)$. Intuitively, ψ respects (the partial orders) $\subseteq$ on $\mathcal{B}$ and $\leqslant$ on $\mathcal{S}$.

Proof. (i) We want to show that $\phi(\mathcal{B}) \subseteq \mathcal{S}$ and $\phi(\mathcal{S}) \subseteq \mathcal{B}$. To show the former, let $\Delta \in \mathcal{B}$ then

$$\begin{aligned} x \in G_\alpha &\implies \alpha \in \Delta \cap \Delta^x && \text{since } \alpha \in \Delta \\ &\implies \Delta = \Delta^x && \text{since } \Delta \text{, is a block} \\ &\implies x \in G_{\{\Delta\}} \end{aligned}$$

which shows that $G_\alpha \subseteq G_{\{\Delta\}} = \psi(\Delta)$ for an arbitrary $\Delta \in \mathcal{B}$ and so $\psi(\mathcal{B}) \subseteq \mathcal{S}$ holds. We now show the other inclusion. Let $H \in \mathcal{S}$ and let $\Delta := \alpha^H$ be the image of H in ϕ. We want to show that Δ is a block. Let $x \in G$ then if $x \in H$ we have

$$\Delta^x = (\alpha^G)^x = \{(\alpha^g)^x \mid g \in G\} = \alpha^G = \Delta$$

Otherwise $x \notin H$ which implies $\Delta \cap \Delta^x = \emptyset$, which we show by contradiction. Let $x \notin H$ then

$$\begin{aligned} \Delta \cap \Delta^x \neq \emptyset &\implies \exists h, g \in H \text{ such that } \alpha^g = \alpha^{hx} \\ &\implies hxg^{-1} \in G_\alpha \end{aligned}$$

but $H \in \mathcal{S}$ implies G_α is a subgroup of H. It follows that $x \in H$ which is a contradiction. We now have that Δ is a block and $\alpha \in \Delta$ so we have that $\Delta = \phi(H)$ is in $\mathcal{B}$. The choice H in $\mathcal{S}$ was arbitrary, so $\psi(\mathcal{S}) \subseteq \mathcal{B}$ holds.

(ii) We want to show that $\psi\phi$ and $\phi\psi$ are identity mappings. First we show $\phi\psi$ is the identity on $\mathcal{B}$. Let $\Delta \in \mathcal{B}$ then Δ is an orbit of $G_{\{\Delta\}}$ by Proposition 2.23 and so we have $\phi(\psi(\Delta)) = \phi(G_{\{\Delta\}}) = \alpha^{G_{\{\Delta\}}} = \Delta$, as required. On the other hand, if $H \in \mathcal{S}$ and we set $\Delta := \phi(H)$ then we proved in part (i) that if $g \in G$ we have $\Delta = \Delta^x$ if and only if $x \in H$. It follows that $\psi(\phi(H)) = \psi(\Delta) = G_{\{\Delta\}} = H$ so $\psi\phi$ fixes H, as required. This completes the proof.

(iii) Let $\Delta, \Gamma \in \mathcal{B}$. If $G_{\{\Delta\}} \leqslant G_{\{\Gamma\}}$ then the orbit Δ of $G_{\{\Delta\}}$ must be contained in an orbit of $G_{\{\Gamma\}}$. Since $\alpha \in \Delta$ and $\alpha \in \Gamma$, which is an orbit of $G_{\{\Gamma\}}$, it must be the case that $\Delta \subseteq \Gamma$. On the other hand, when $\Delta \subseteq \Gamma$ holds we have that $x \in G_{\{\Delta\}}$ implies $\Gamma^x \cap \Gamma \neq \emptyset$ which then implies $x \in G_{\{\Gamma\}}$ because Γ is a block. So $\Delta \subseteq \Gamma$ implies $G_{\{\Delta\}} \leqslant G_{\{\Delta\}}$ and the proof is complete. □

Corollary 2.25. [1, Cor 1.5A] *Let G be a group which acts transitively on a set Ω containing at least two points. Then G is primitive if and only if there is a point stabilizer which is a maximal subgroup of G.*

Proof. For each $\alpha \in \Omega$ the blocks containing α are in bijective correspondence with the subsets of G containing G_α. The trivial blocks $\{\alpha\}$ and Ω correspond to G_α and G, respectively, so any non-trivial block containing α would correspond to a proper subgroup of G which properly contains G_α. Thus G_α is maximal if and only if G has no nontrivial blocks containing α. Thus G has no nontrivial blocks if and only if all the point stabilizers are maximal subgroups of G. In fact the point stabilizers form a conjugacy class of subgroups of G (Theorem 2.13(i)) so if any point stabilizer is maximal then all the points stabilizers are maximal. □

3 Semidirect products and Wreath Products

In this section we define two constructions. First we define the Semidirect product of two groups, of which the direct product on two groups is a special case. Then we will be able to define the wreath product construction and we will indicate why it is crucial to the study of permutation groups.

3.1 Semidirect Products

The construction in the following proposition is the semidirect product

Proposition 3.1. [1, Ex 2.5.1] *Let H and K be groups such that there is an action of H on K as a group. Set*

$$G = \{(k, h) \mid k \in K \text{ and } h \in H\}$$

and define the product of two elements of G as:

$$(a, b)(c, d) = (ac^{b^{-1}}, bd)$$

for all $(a, b), (c, d) \in G$. Then G is a group.

Proof. The product of two elements of G is an element of G because H acts as an automorphism of K and since K, H are groups (closed under multiplication). The identity of G is $(1_K, 1_H)$. Let (a, b) be arbitrary in G then its inverse is $((a^{-1})^b, b^{-1}) \in G$ since

$$(a, b)((a^{-1})^b, b^{-1}) = (a(a^{-1})^{bb^{-1}}, bb^{-1}) = (aa^{-1}, 1_H)$$

and

$$((a^{-1})^b, b^{-1})(a, b) = ((a^{-1})^b a^b, b^{-1}b) = ((a^b)^{-1}a^b, 1_H) = (1_K, 1_H)$$

Finally we can show G is associative:

$$\begin{aligned}
((a, b)(c, d))(e, f) &= (ac^{b^{-1}}, bd)(e, f) \\
&= (ac^{b^{-1}}e^{(bd)^{-1}}, bdf) \\
&= (a(ce^{d^{-1}})^{b^{-1}}, bdf) \\
&= (a, b)(ce^{d^{-1}}, df) \\
&= (a, b)((c, d)(e, f))
\end{aligned}$$

□

Definition 3.2. If G is a group defined with K and H as in Proposition 3.1 then G is called the *semidirect product* of K by H, written:

$$G = K \rtimes H$$

In the special case where $H \leqslant G$, $K \lhd G$, $KH = G$ and $K \cap H = 1_G$ we have that H acts on K by conjugation and call $K \rtimes H$ an *internal semidirect product.* Otherwise we call G an *external semidirect product.*

Example 3.3. [1, Ex 2.5.2] Let H and K be groups then if we let G be the semidirect product of K by H with respect to the trivial action

$$k^h := k \qquad \text{for all } k \in K \text{ and } h \in H$$

we see that G is equal to the direct product $K \times H$. These groups have the same elements and the same multiplication. To see that the multiplication is the same we check that the product of arbitrary $(k_1, h_1), (k_2, h_2) \in K \rtimes H$ is $(k_1, h_1)(k_2, h_2) = (k_1 k_2^{h_1}, h_1 h_2) = (k_1 k_2, h_1 h_2)$ which is identical to the product of these elements in $K \times H$.

3.2 Wreath Products

If K is a group and $\Gamma = \{1, \ldots, m\}$ is the set containing the first m natural numbers then we will denote the direct product of m copies of K by

$$K^m = K_1 \times \cdots \times K_m$$

where $K_1, \ldots, K_m$ are equal to K. It is normal to represent the elements of K^m by tuples such as $(k_1, \ldots, k_m)$ where $k_1, \ldots, k_m$ are elements of K.

If we define the cartesian product of m copies of a set Δ to be

$$\Delta^m = \{(\delta_1, \ldots, \delta_m) \mid \delta_1, \ldots, \delta_m \in \Delta\}$$

then there is a natural extension of an action of a group K on Δ to an action of K^m on Δ^m. It is defined by

$$(\delta_1, \ldots, \delta_m)^{(k_1, \ldots, k_m)} := (\delta_1^{k_1}, \ldots, \delta_m^{k_m})$$

and it is a simple task to check that this is an action. Herein this action will arise often. When a group K acts on a set Δ it is safe to assume the action of K^m on Δ^m is the action we have just defined, at least until we introduce the diagonal action in section 5.

In general one can also index direct products by an arbitrary set. If this set, say Γ, is finite of size, say m, then the direct product of m copies of a group indexed by Γ is isomorphic one which is indexed by $\{1, \ldots, m\}$. For this reason we will not worry about indexing direct products by arbitrary finite set. When we write K^Γ for an arbitrary Γ we will treat it as $K^{|\Gamma|}$ with an implicit bijection from Γ to $\{1, \ldots, |\Gamma|\}$.

We now define an action that will be integral to the rest of this section and so defining it carefully will save us plenty of work later. The interpretation of what this action does is fairly simple, if H acts on $\{1, \ldots, m\}$ then we define an action of H on the cartesian product of m sets or a direct product of m groups, and this action permutes the components. Unlike the interpretation, the definition turns out to be a bit tricky.

Proposition 3.4. *Let H be a group which acts on the finite set $\Gamma = \{1, \ldots, m\}$ and let Δ be a set. Then H acts on Δ^m (the cartesian product of m copies of Δ) by*

$$\underline{\delta}^h = (\delta_1, \ldots, \delta_m)^h := (\pi_{1^{h^{-1}}}(\underline{\delta}), \ldots, \pi_{m^{h^{-1}}}(\underline{\delta}))$$

where each $\pi_i : \Delta^m \to \Delta$ is the projection onto the i^{th} factor of Δ^m. We use projection maps because the more obvious definition is ambiguous[1]*. Furthermore if K is a group then H acts on K^m as a group by*

$$\underline{k}^h = (k_1, \dots, k_m)^h := (\rho_{1^{h^{-1}}}(\underline{k}), \dots, \rho_{m^{h^{-1}}}(\underline{k}))$$

where each $\rho_i : K^m \to K$ is the projection onto the i^{th} factor of K^m.

Proof. The identity of H clearly fixes Δ^m because it fixes Γ. Now if $\underline{\delta} = (\delta_1, \dots, \delta_m) \in \Delta^m$ and $g, h \in H$ then we have

$$\begin{aligned}
(\underline{\delta}^g)^h &= (\pi_{1^{g^{-1}}}(\underline{\delta}), \dots, \pi_{m^{g^{-1}}}(\underline{\delta}))^h \\
&= (\delta_{1^{g^{-1}}}, \dots, \delta_{m^{g^{-1}}})^h \\
&= (\omega_1, \dots, \omega_m)^h && \text{where each } \omega_i = \delta_{i^{g^{-1}}} \\
&= (\pi_{1^{h^{-1}}}(\underline{\omega}), \dots, \pi_{m^{h^{-1}}}(\underline{\omega})) && \text{where } \underline{\omega} = (\omega_1, \dots, \omega_m) \\
&= (\omega_{1^{h^{-1}}}, \dots, \omega_{m^{h^{-1}}}) \\
&= (\delta_{(1^{h^{-1}})^{g^{-1}}}, \dots, \delta_{(m^{h^{-1}})^{g^{-1}}}) && \text{since } \omega_i = \delta_{i^{g^{-1}}} \\
&= (\delta_{1^{(gh)^{-1}}}, \dots, \delta_{m^{(gh)^{-1}}}) && \text{since } H \text{ acts on } \Delta \text{ and } h^{-1}g^{-1} = (gh)^{-1} \\
&= \underline{\delta}^{(gh)}
\end{aligned}$$

which shows that this is an action on Δ^m. We can immediately deduce H acts on K^m as a set by our previous action applied to $\Delta := K$. Now let $\underline{k} = (k_1, \dots, k_m)$ and $\underline{l} = (l_1, \dots, l_m)$ be elements of K^m then for all $h \in H$ we have

$$\begin{aligned}
(\underline{kl})^h &= (k_1 l_1, \dots, k_m l_m)^h \\
&= (k_{1^{h^{-1}}} l_{1^{h^{-1}}}, \dots, k_{m^{h^{-1}}} l_{m^{h^{-1}}}) \\
&= (k_{1^{h^{-1}}}, \dots, k_{m^{h^{-1}}})(l_{1^{h^{-1}}}, \dots, l_{m^{h^{-1}}}) \\
&= \underline{k}^h \underline{l}^h
\end{aligned}$$

and so H acts acts on K^m as a group. □

This action allows us to define a wreath product. Remember that this action should be interpreted as permuting the components of a product. In the case of wreath products, we will have this action permuting the components of a direct product of m copies of a group. An element of this product is a tuple and so the action permutes the entries in these tuples.

Definition 3.5. Let K and H be groups, let Γ be a finite set and suppose H acts on Γ. Then the *wreath product* of K by H with respect to Γ is the group:

$$K \; wr_\Gamma \; H = K^\Gamma \rtimes H$$

with the action of H on K^Γ being the action on a group from Proposition 3.4.

[1] The more obvious definition of this action might seem to be $(\delta_1, \dots, \delta_m)^h := (\delta_{1^{h^{-1}}}, \dots, \delta_{m^{h^{-1}}})$ but this may be interpreted as implying that $((\delta_1, \dots, \delta_m)^g)^h$ is equal to $(\delta_{1^{g^{-1}h^{-1}}}, \dots, \delta_{m^{g^{-1}h^{-1}}})$.

Much of the importance of wreath products comes from a specific action, which we define next. The idea behind this action is to combine the actions we defined earlier in this section. Using the notation from the previous definiton, an element of $(k_1, \ldots, k_m)$ of $K \ wr_\Gamma \ H$ will act on an element $(\delta_1, \ldots, \delta_m)$ of Δ^m by first the action of K^m on Δ^m (which has k_1 act on δ_1 and so on) and then the resulting tuple will have its entries permuted by the action of H. This is called the *product action* of the wreath product W and it is defined in the following proposition.

Proposition 3.6. [1, Sec 2.7] *Let K and H be groups which act on Δ and $\Gamma = \{1, \ldots, m\}$, respectively. Set $W := K \ wr_\Gamma \ H$ and let H act on Δ^m with the action from Proposition 3.4. Then W acts on Δ^m by*

$$(\delta_1, \ldots, \delta_m)^{((k_1,\ldots,k_m),h)} := (\delta_1^{k_1}, \ldots, \delta_m^{k_m})^h$$

Proof. The identity of W is $((1_K, \ldots, 1_K), 1_H)$ and it fixes Δ^m because the each 1_K fixes each Δ component of Δ^m and 1_H fixes Δ^m. Let $w_1 := ((k_1, \ldots, k_m), h)$ and $w_2 := ((l_1, \ldots, l_m), g)$ be elements of W. If we set $\rho_i := k_i l_{i^h}$ then for all $(\delta_1, \ldots, \delta_m) \in \Delta^m$ we have

$$\begin{aligned}
(\delta_1, \ldots, \delta_m)^{(w_1 w_2)} &= (\delta_1, \ldots, \delta_m)^{((\rho_1,\ldots,\rho_m),hg)} && \text{where } \rho_i = k_i l_{i^h} \\
&= (\delta_1^{\rho_1}, \ldots, \delta_m^{\rho_m})^{(hg)} \\
&= ((\delta_1^{\rho_1}, \ldots, \delta_m^{\rho_m})^h)^g && \text{since } H \text{ acts on } \Delta^m
\end{aligned}$$

To see that this is equal to acting by w_1 followed by w_2 we set $a_i := i^{h^{-1}}$ and $b_i := k_{a_i}$ then we show

$$\begin{aligned}
((\delta_1, \ldots, \delta_m)^{w_1})^{w_2} &= ((\delta_1^{k_1}, \ldots, \delta_m^{k_m})^h)^{w_2} \\
&= (\delta_{a_1}^{b_1}, \ldots, \delta_{a_m}^{b_m})^{w_2} && \text{where } a_i = i^{h^{-1}} \text{ and } b_i = k_{a_i} \\
&= (\delta_{a_1}^{b_m l_1}, \ldots, \delta_{a_m}^{b_m l_m})^g \\
&= ((\delta_1^{k_1 l_{1^h}}, \ldots, \delta_m^{k_m l_{m^h}})^h)^g && \text{since } a_{i^h} = i \text{ and } b_{i^h} = k_i \\
&= ((\delta_1^{\rho_1}, \ldots, \delta_m^{\rho_m})^h)^g && \text{where } \rho_i = k_i l_{i^h}
\end{aligned}$$

This concludes the proof. □

As mentioned before, we will want to use the wreath product to study primitive groups. The following theorem gives necessary and sufficient conditions for the product action to be primitive. Recall the normalizer of a subgroup H of G is $N_G(H) := \{g \in G \mid g^{-1}Hg = H\}$ we will say that a subgroup S of G normalizes H if $S \leqslant N_G(H)$. Then if (i) $S \cap H$ is trivial, (ii) S is normal in G and (iii) S normalizes H all hold we have that SH is an internal direct product of S and H in G.

Theorem 3.7. [1, Lem 2.7A] *Suppose that H is a non-trivial group which acts on the finite set $\Gamma = \{1, \ldots, m\}$ and that K is a group which acts non-trivially on the set Δ. Then the wreath product $W = K \ wr_\Gamma \ H$ is primitive in the product action on $\Omega = \Delta^{|\Gamma|}$ if and only if:*

(i) K acts primitively but not reguarly on Δ; and

(ii) H acts transitively on Γ.

Proof. Before we begin we will set up some notation. First, let

$$\pi_1, \ldots, \pi_m : K^m \to K$$

be the projection maps from K to the $1^{st}, \ldots, m^{th}$ factors of K^m, respectively. Next, set

$$B := \{(\underline{k}, 1) \in W \mid \underline{k} \in K^m\}$$

and also define

$$H_0 := \{(1, h) \in W \mid h \in H\}$$

then notice these are disjoint normal subgroups of W which together generate W, that is to say $W = BH_0$ is an internal direct product. Now we fix a $\delta \in \Delta$ where $K_\delta \neq K$ and set $\sigma_\delta := (\delta, \ldots, \delta) \in \Delta^m$, then

$$L := \{(\underline{k}, h) \in W \mid \pi_1(\underline{k}), \ldots, \pi_m(\underline{k}) \in K_\delta \text{ and } h \in H\}$$

is the point stabilizer of σ_δ in W. By Corollary 2.25 W is primitive if and only if W is transitive and L is a maximal subgroup of W.

We will begin by proving conditions (i) and (ii) are necessary for W to act primitively on Δ^m. If H is not transitive and $A \subset \Gamma$ is an orbit of H then

$$M := \{(\underline{k}, 1) \in B \mid \pi_i(\underline{k}) \in K_\delta \text{ for all } i \in A\}$$

is a subgroup of B. For any $(\underline{k}, h) \in L$ it is true that $(\underline{k}, 1) \in M$ and then $(\underline{k}, 1)(1, h) = (\underline{k}, h) \in MH_0$ implies $L \leqslant MH_0$. In fact this containment is strict because $K_\delta \neq K$ so for any $j \in \Gamma \backslash A$ there is some $(\underline{m}, h) \in M$ where $\pi_j(\underline{m}) \notin K_\delta$ and so $(\underline{m}, h) \notin L$. Then because L is not maximal we have that W is not primitive so we have shown condition (ii) is necessary. If K is intransitive and $d_1, \ldots, d_m$ are elements of Δ which aren't in the orbit of δ then $(d_1, \ldots, d_m)$ cannot be mapped to σ_δ by W, so W is intransitive. When K is transitive but imprimitive the pointwise stabilizer K_δ is not maximal in K so we may find a proper subgroup R of K which properly contains K_δ. If we choose such an R then

$$N := \{(\underline{k}, h) \in W \mid \pi_1(\underline{k}), \ldots, \pi_m(\underline{k}) \in R \text{ and } h \in H\}$$

is a proper subgroup of W which properly contains L so the action of W is not primitive when the action of K on Δ is imprimitive. Finally, when K acts regularly on Δ the group

$$D := \{(\underline{k}, 1) \in B \mid \pi_1(\underline{k}) = \cdots = \pi_m(\underline{k})\}$$

is a proper subgroup of B which is normalized by H_0, so DH_0 is a proper subgroup of W. Furthermore $L = H_0$ since K being regular implies the point stabilizers are trivial (Corollary 2.13). Thus $L < DH_0 < W$ and W does not act primitively when K acts regularly. This completes the proof that (i) and (ii) are necessary conditions for W to act primitively.

To finish the proof we must show that (i) and (ii) together imply W acts primitively. Let P be a group satisfying $L < P \leqslant W$ and we will show that P must equal W. It will be helpful if we distinguish the following subset and subgroup, respectively, of B so we let

$$B^1 := \{(\underline{k}, 1) \in B \mid \pi_i(\underline{k}) \neq 1 \text{ for at most one } i \in \{1, \dots, m\}\}$$

and let

$$B_i^1 := \{(\underline{k}, 1) \in B^1 \mid \pi_j(\underline{k}) = 1 \text{ if } j \neq i\}$$

Since $L \leq P$ and $W = \langle B, L \rangle$ we have that $P = \langle P \cap B, L \rangle$ which implies $L \cap B < P \cap B$ holds. It follows that there exists $(\underline{f}, 1) \in P \cap B$ such that $\pi_i(\underline{f}) \notin K_\delta$, in other words $(\underline{f}, 1) \notin L \cap B$, for some $i \in \Gamma$. Now we will use $(\underline{f}, 1)$ to show that P contains B_i^1 as a subgroup. Since K is primitive, K_δ is maximal which implies $\langle K_\delta, \pi_i(\underline{f}) \rangle = K$ and this in turn implies that

$$\{(\underline{k}, 1) \mid \pi_i(\underline{k}) \in K_\delta \cup \{\pi_i(\underline{f})\}\} \subset P$$

generates B_i^1. By noticing that $(1, h)B_i^1 = B_{i^h}^1$ we see that $B^1 \subset P$ and because B^1 generates B we have that B is a subgroup of P. Since H_0 is also a subgroup of P and $W = BH_0$ we have that $P = W$, as required, and the proof is complete. □

The result of [1, Ex 2.6.2] is now presented to illustrate how wreath products can be used to construct imprimitive groups from primitive groups. This result combined with Theorem 2.16 suggests that a classification of primitive groups will lead to a classification of all permutation groups. This is why we might justifiably call the primitive groups the building blocks of permutation groups and why we wish to study them.

Example 3.8. Let $G \leqslant Sym(\Omega)$ be an imprimitive group and let $\Sigma := \{\Gamma_i \mid i \in I\}$ be a system of blocks for G. Then there is an embedding

$$G \to Sym(\Gamma)\ wr_\Gamma\ Sym(I).$$

That is to say, G is isomorphic to a subgroup of this wreath product. As shown in Example 2.21, the symmetric groups are primitive so we have constructed G using primitive groups. Wreath products are well understood when the two groups used in the construction are well understood and this justifies our focus on the primitive groups.

4 The Socle

In this section we define the socle of a group. The socle will turn out to be one of the keys to analysing the finite primitive groups and central to the classification shown in Section 6. Recall the following definitions of normalizers and centralizers. The normalizer of a subgroup H of the group G is denoted $N_G(H) := \{g \in G \mid gH = Hg\}$ and it is the elements of G which commute with H as a whole. The centralizer of H in G is denoted $C_G(H) := \{g \in G \mid gh = hg \text{ for all } h \in H\}$ and it is the elements of G which commute with all elements of H. Additionally if $K \leqslant N_G(H)$ we say that K normalizes H and if $K \leqslant C_G(H)$ we say that K centralizes H. We begin by defining the socle.

Definition 4.1. A minimal normal subgroup of a nontrivial group G is a normal subgroup $K \neq 1$ of G which does not properly contain any other nontrivial normal subgroup of G.

Definition 4.2. The socle of a group G is the subgroup generated by the set of all minimal normal subgroups of G and it is denoted by $soc(G)$. By convention, $soc(G) = 1$ if G has non nontrivial normal subgroups but this situation does not occur when G is a finite nontrivial group.

There is actually quite a lot we can say about the socle of a finite group. We will need the following two lemmas to analyse the structure of the socle.

Lemma 4.3. [1, Thm 4.3A(i)] *Let K and L be normal subgroups of a group G. Then $K \cap L$ is normal in G. If, additionally, K is a minimal normal subgroup and L is non-trivial then either $\langle K, L\rangle = L$ or $\langle K, L\rangle = K \times L$ is an internal direct product.*

Proof. The intersection of two subgroups is also a group. If x is in both K and L then for all $g \in G$ it follows that $g^{-1}xg$ is in both K and L, because they are normal, and thus $K \cap L \lhd G$. Let K be a minimal normal subgroup and let L be a non-trivial normal subgroup. If $K \leqslant L$ then $\langle K, L\rangle = L$. Otherwise, $K \cap L \lhd G$ is a subgroup of K and normal in G so anything other than $K \cap L = 1$ would contradict the minimality of K. Then the two conditions $K \cap L = 1$ and $K, L \lhd G$ imply $\langle K, L\rangle$ is equal to the internal direct product of K and L. □

Lemma 4.4. *Let N be a normal subgroup of a group G and let $\psi \in Aut(G)$. Then $\psi(N)$ is a normal subgroup of G. Moreover, if N is a minimal normal subgroup of G then $\psi(N)$ is also a minimal normal subgroup of G.*

Proof. Let N be a normal subgroup of G and let $\psi \in Aut(G)$. Then for all $g \in G$ we have

$$\begin{aligned}\psi^{-1}(g^{-1}\psi(H)g) &= \psi^{-1}(g^{-1})\ \psi^{-1}(\psi(H))\ \psi^{-1}(g) \ \text{ (since } \psi \text{ is a homomorphism)}\\ &= (\psi^{-1}(g))^{-1}H\psi^{-1}(g)\\ &= H \ \text{ (because } \psi^{-1}(g) \in G \text{ and } H \lhd G)\end{aligned}$$

which implies $g^{-1}\psi(H)g = \psi(H)$ (by applying ψ to the LHS and the last RHS above) and so we have shown that $\psi(H) \lhd G$. Now let N be a minimal normal subgroup of G and, to reach a contradiction, assume that $\psi(N)$ is not a minimal normal subgroup of G. Then there must exist $S \lhd G$ such that $1 < S < \psi(N)$. However S being normal implies that $\psi^{-1}(S)$ is normal, by the first part of this lemma, and $1 < S < \psi(N)$ implies that $1 < \psi^{-1}(S) < N$ which contradicts N being a minimal normal subgroup. □

The structure of the socle of a finite group turns out to be rather distinguishable. The follow theorem shows how the socle is a direct product of simple groups.

Theorem 4.5. [1, Thm 4.3A] *Let G be a nontrivial finite group.*

(i) There exist minimal normal subgroups $K_1, \dots, K_m$ of G such that $soc(G) = K_1 \times \cdots \times K_m$.

(ii) Every minimal normal subgroup K of G is a direct product $K = T_1 \times \cdots \times T_k$ where the T_i are simple normal subgroups of K which are conjugate under G.

(iii) If the subgroups $K_1, \dots, K_m$ from (i) are all nonabelian then they are the only minimal normal subgroups of G.

Proof. (i) G is finite and so has a finite set of minimal normal subgroups $\{K_1, \dots, K_n\}$. If we let $H_1 = K_1$ and then iteratively define

$$H_i = \langle K_i, H_{i-1} \rangle = \begin{cases} H_{i-1} & \text{if } K_i \leqslant H_{i-1} \\ K_i \times H_{i-1} & \text{if } K_i \nleqslant H_{i-1} \end{cases}$$

for $i = 2, \dots, n$ it follows from Lemma 4.3 that each H_i is well defined. Notice that $H_i = \langle K_1 \dots K_i \rangle$, in particular $H_n = soc(G)$ by definition. Clearly H_n is a direct product of some of the K_i (the K_i where $K_i \nleq H_{i-1}$) and by relabelling the K_i we may write $soc(G) = H_n = K_1 \times \cdots \times K_m$ for some $m \leq n$.

(ii) Let T be a minimal normal subgroup of K. Then for all $x \in G$ we have that the conjugate $x^{-1}Tx$ of T is a minimal normal subgroup of K by Lemma 4.4, because $g \mapsto x^{-1}gx$ is an automorphism of G. Now let $T_1, \dots, T_j$ be all the distinct conjugates of T in G. If we let $L_1 = T_1$ and then iteratively define

$$L_i = \langle T_i, L_{i-1} \rangle = \begin{cases} L_{i-1} & \text{if } T_i \leqslant L_{i-1} \\ T_i \times L_{i-1} & \text{if } T_i \nleqslant L_{i-1} \end{cases}$$

for $i = 2, \dots, j$ it follows from Lemma 4.3 that each L_i is well defined. Similar to when proving (i), notice that $L_i = \langle T_1 \dots T_i \rangle$ and that L_j is a direct product of some of the T_i (the T_i where $T_i \nleq L_{i-1}$) which can be relabelled so that we can write $L_j = T_1 \times \cdots \times T_k$ for some $k \leq j$.

We now show that $L_j = K$. It follows from $L_j = \langle T_1 \dots T_j \rangle$ that an arbitrary element can be written as a product $\tau_1 \dots \tau_p$ where each τ_i can belong to any of $T_1, \dots, T_j$. Let $x \in G$ then the conjugate of an element of L_j by x may be rewritten as a product of conjugates of elements from the T_i as shown:

$$x^{-1}\tau_1 \dots \tau_p x = (x^{-1}\tau_1 x)(x^{-1} \dots x)(x^{-1}\tau_p x).$$

Then each $x^{-1}\tau_q x$ is in one of the T_i ($\leqslant L_j$) and so the product $(x^{-1}\tau_1 x)\dots(x^{-1}\tau_p x)$ is in L_j. Thus that $L_j \lhd G$ and because L_j is a subgroup of the minimal normal subgroup K then the only possibility is that $L_j = K$. The normal subgroups of the direct factors of $K = L_j = T_1 \times \cdots \times T_k$ are also normal in K because each direct factor commutes with the others in a direct product and it then follows from the minimality of $T_1, \dots, T_k$ in K that $T_1, \dots, T_k$ must be simple.

(iii) Suppose that G has a minimal normal subgroup M which is distinct from each of $K_1, \dots, K_m$. Then Lemma 4.3 shows that the elements of M commute with the elements of each K_i, that is M centralizes all the K_i. Then, since the K_i generate $soc(G)$, we have $M \leqslant Z(soc(G))$. However, if the K_i are nonabelian then they are direct products of nonabelian simple groups by (ii) and so must have trivial center. Then $Z(soc(G)) = 1$ so the minimal normal subgroup M must be trivial which is a contradiction. □

When we look at the socle of a finite primitive group the situation is even clearer. Although we do not prove it, we now state [1, Thm 4.B] because it is easily appreciable at this point and we will refer to it multiple times later.

Theorem 4.6. [1, Thm 4.3B] *If G is a finite primitive subgroup of $Sym(\Omega)$, and K is a minimal normal subgroup of G, then exactly one of the following holds:*

(i) for some prime p and some integer d, K is a regular elemntary abelian group of order p^d, and $soc(G) = K = C_G(K)$;

(ii) K is a regular nonabelian group, $C_G(K)$ is a minimal normal subgroup of G which is permutation isomorphic[2] to K, and $soc(G) = K \times C_G(G)$;

(iii) K is nonabelian, $C_G(K) = 1$ and $soc(G) = K$.

For now, this concludes our study of the socle but it will return to play a large part in the classification of finite primitive groups.

[2] If, for example, $G \leqslant Sym(\Sigma)$ and $H \leqslant Sym(\Gamma)$ then we say that H and G are *permutation isomorphic* if there is a bijection $\lambda : \Sigma \to \Gamma$ and a group isomorphism $\phi : G \to H$ such that $\lambda(\sigma^x) = \lambda(\sigma)^{\phi(x)}$

5 The Diagonal Action

In this section we indirectly use the product action to construct primitive groups with nonregular socles. This action and the primitive groups it can construct will be of interest in the following chapter when we attempt to classify the finite primitive groups.

Take a finite nonabelian simple group T as a regular subgroup of $Sym(\Delta)$ and let $\Gamma := \{1, \ldots, m\}$. We will be considering the wreath product $W := T\ wr_\Gamma\ Sym(\Gamma)$ with the product action on Δ^m. This action is not primitive because T is regular (Theorem 3.7) but we will create a primitive action from it. Let C be the centralizer of T in $Sym(\Delta)$, so C is also regular and $C \cong T$ by [1, Thm 4.2A]. There is an action of C on Δ^m defined by

$$(\delta_1, \ldots, \delta_m)^c := (\delta_1^c, \ldots, \delta_m^c)$$

and this action commutes with the action of W. To see this, first see that the action of C commutes with the action of T^m because C centralizes T, that is if $c \in C$ and $(t_1, \ldots, t_m) \in T^m$ then:

$$(\delta_1, \ldots, \delta_m)^{(t_1,\ldots,t_m)c} = (\delta_1^{t_1}, \ldots, \delta_m^{t_m})^c = (\delta_1^{t_1 c}, \ldots, \delta_m^{t_m c});\text{ and}$$

$$(\delta_1, \ldots, \delta_m)^{c(t_1,\ldots,t_m)} = (\delta_1^c, \ldots, \delta_m^c)^{(t_1,\ldots,t_m)} = (\delta_1^{ct_1}, \ldots, \delta_m^{ct_m}) = (\delta_1^{t_1 c}, \ldots, \delta_m^{t_m c})$$

Also notice that this action commutes with the action of the $Sym(\Gamma)$ component of W, that is if $c \in C$ and $r \in \Gamma$ then:

$$(\delta_1, \ldots, \delta_m)^{cr} = (\delta_1^c, \ldots, \delta_m^c)^r = (\delta_{1^{r^{-1}}}^c, \ldots, \delta_{m^{r^{-1}}}^c);\text{ and}$$

$$(\delta_1, \ldots, \delta_m)^{rc} = (\delta_{1^{r^{-1}}}, \ldots, \delta_{m^{r^{-1}}})^c = (\delta_{1^{r^{-1}}}^c, \ldots, \delta_{m^{r^{-1}}}^c)$$

We now prove the following proposition.

Proposition 5.1. *The orbits of C form a system of blocks for W.*

Proof. Let $\gamma \in \Delta^m$ and consider $B := \gamma^C$, an orbit of C. Let $x \in W$ then either $B^x \cap B = \emptyset$ or there is point d in the intersection $B^x \cap B$. In the latter case there exists an element in the intersection $d = \gamma^{c_1 x} = \gamma^{c_2}$, for some $c_1, c_2 \in C$, and so $\gamma^x = \gamma^{c_2 c_1^{-1}}$ because c_1 and x commute. Then

$$\begin{aligned}
(\gamma^C)^x &= \{\gamma^{cx} \mid c \in C\} \\
&= \{\gamma^{xc} \mid c \in C\} && \text{because } c \text{ and } x \text{ commute} \\
&= \{\gamma^{c_2 c_1^{-1} c} \mid c \in C\} && \text{since } x = c_2 c_1^{-1} \\
&= \gamma^C
\end{aligned}$$

and so $B^x \cap B = B$. Then, since the element x was arbitrary in G and since G is transitive, we have shown that B is a block for G, as required. □

We let Ω be the set of orbits of C in Δ^m and write $[\delta_1, \ldots, \delta_m] \in \Omega$ to denote the orbit of C containing $(\delta_1, \ldots, \delta_m)$. The action of T^m on Ω defined by

$$[\delta_1, \ldots, \delta_m]^{(t_1, \ldots, t_m)} := [\delta_1^{t_1}, \ldots, \delta_m^{t_m}]$$

is called the *diagonal action* of T^m [1, page 121].

It can be shown [1, Ex 4.5.2] that W acts faithfully on Ω. If we denote the image of T^m in the permutation representation of W by $H \leqslant Sym(\Omega)$ then a group G is said to be of *diagonal type* if G is a subgroup of the normalizer N of H in $Sym(\Omega)$. If we identify W with its image in $Sym(\Omega)$ then [1, Lem 4.5B] states that $N/W \cong Out(T)$, the outer automorphism group of T. The significance of this is that W is, in general, not the normalizer of H, which is why *diagonal type* groups are defined as the subgroups of the normalizer. It can be shown [1, Thm 4.5A] that G is a primitive group of diagonal type in $Sym(\Omega)$ precisely when: $m = 2$; or $m \geq 3$ and G acts primitively on the set of minimal normal subgroups of H by conjugation.

6 The O'Nan-Scott Theorem

In this section we state and prove the O'Nan-Scott Theorem, which classifies the finite primitive groups, in three out of the five cases, and cover part of another case. Before this, we introduce the types of primitive groups that will appear in the classification.

6.1 The Types

Let G be a finite primitive group which acts on Ω and let the socle of G be $H = T_1 \times \cdots \times T_m$ where $T_1, \ldots, T_m$ are isomorphic simple groups. In this section we will label four types of primitive groups. However we must begin with a detour to linear groups.

Let F be a field then the *general linear group* of degree m over F is the group containing all invertible $m \times m$ matrices with entries from F. This group is denote by $GL_m(F)$ and it has a natural action on F^m by matrix multiplication. Now the affine group of degree m over F is defined as the semidirect product

$$(F)^m \rtimes GL_m(F)$$

Finally if F_q is the unique finite field of order q (which must be a prime power) then we will denote $AGL_m(F_q)$ by $AGL_m(q)$. Now we are ready to define the first type.

Definition 6.1. (Affine Type) We will say G is of *affine type* if G is isomorphic to a subgroup of $AGL_m(p)$ for some prime p.

Definition 6.2. (Almost Simple Type) In general, a group K is an *almost simple* group if it has a nonabelian simple subgroup S which satisfies

$$S \leqslant K \leqslant Aut(S)$$

We will say G is of *almost simple type* if it is an almost simple group.

Definition 6.3. (Diagonal Type) We will say G is of *diagonal type* if it is one of the groups described in Section 5.

Definition 6.4. (Product Action Type) Assume there is a group U with a (necessarily) primitive action on Ω and a finite set Γ (of size greater than 1) such that

$$W := U \; wr_{\Gamma} \; Sym(\Gamma)$$

acts primitively on Ω with the product action. Then we will say G is of *product action type* if G is isomorphic to a subgroup of such a W.

6.2 The O'Nan-Scott Theorem

Let G be a finite primitive group of degree n, and let the socle of G be $H = T_1 \times \cdots \times T_m$ where $T_1, \ldots, T_m$ are isomorphic to the simple group T. Then either:

(i) T is abelian, G is of affine type and, for some prime p, H is a regular elementary abelian p-group of degree $p^m = |H|$, which is also the degree of G.

(ii) T is nonabelian, $m = 1$, G is isomorphic to a subgroup of $Aut(T)$ and $n = |T|$.

(iii) T is nonabelian, $m \geq 1$, G is of diagonal type and $n = |T|^{m-1}$.

(iv) T is nonabelian, $m \geq 2$ and G is of product type. In particular, for some proper divisor d of m, there is a primitive nonregular group U with socle T^d and G is isomorphic to a subgroup of $U \; wr_\Gamma \; Sym(\Gamma)$ where $\Gamma = \{1, \ldots, m/d\}$.

(v) T is nonabelian, $m \geq 6$, H is regular and G has degree $n = |T|^m$.

We will conveniently refer to groups that satisfy (i), (ii), (iii) and (iv) by their respective types: affine, almost simple, diagonal and product action. The groups that satisfy (v) are said to be of *twisted wreath* type. Some authors split the theorem into eight types so that (iii) has the two subcases and (iv) has three subcases. The subcases of (iii) are: (iii)a the socle has two minimal normal subgroups and (iii)b the socle is the minimal normal subgroup. Both subcases first occur as groups of degree 60 which have socle isomorphic to $A_5 \times A_5$, since A_5 is the lowest order nonabelian simple group. The subcases of (iv) are (iv)a, (iv)b and (iv)c which correspond to U being primitive of type (ii), (iii)a or (iii)b, respectively. Of these, only (iv)c occurs in groups of degree less than 2500. Subcases (iii)a, (iii)b first occur 2 and 3 times, respectively, as groups of degree 3600 (corresponding to the first occurrences of types (iii)a, (iii)b at degree 60). Any example of (v) must have degree greater than or equal to 60^6 (so this case is not relevant to primitive group databases) and the author has decided not to cover this case in any more detail.

6.3 Proving the O'Nan-Scott Theorem

We will prove the O'Nan-Scott Theorem for all cases except twisted wreath type. Throughout all of this section we will let G be a finite primitive group which acts on Ω and set $H := soc(G)$. By Corollary 4.3B, the socle of G is a direct product of isomorphic simple groups. If $H \cong T^m$ we say that G has socle type T. We will set T to be the socle type of G and let $H = T_1 \times \ldots T_m$ where $T_1, \ldots, T_m$ are isomorphic to T, for some positive integer m.

We begin by distinguishing some of the cases. The socle H may be regular or nonregular but (by Theorem 4.3B) it may only be abelian if it is regular. The possibilities are the following cases:

(a) H is regular and abelian
(b) H is regular and nonabelian
(c) H is nonregular and $m = 1$ so $H = T$ is a nonabelian simple group
(d) H is nonregular and $m \geq 2$

We will start with the regular abelian case and then cover the nonregular cases afterwards.

6.3.1 Finite Primitive Groups with Regular Abelian Socles

Definition 6.5. Let p be a prime number. An *elementary abelian p-group* is an abelian group where every nontrivial element has order p. In particular, such a group is isomorphic to a direct product of cyclic groups of order p.

Let G be a finite primitive subgroup of $Sym(\Omega)$ with regular and abelian socle. Let $H := soc(G) \cong T^m$ for some simple group T, then it can be shown [1, Thm 4.3B] that $H = T_1 \times \cdots \times T_m$ is an elementary abelian p-group. Let N be the normalizer of H in $Sym(\Omega)$, then it follows from [1, Cor 4.2B] that $N \cong H \rtimes Aut(H)$ and that the action of a point stabilzier N_α of N on Ω is permutation isomorphic[3] to the natural action of $Aut(H)$ on H. We have $H \leqslant G \leqslant N$ and so N is primitive which implies N_α is maximal. Since H is regular we also have that $N_\alpha \cap H = N_\alpha \cap H_\alpha$ is trivial and together with the maximality of N_α this implies $N_\alpha H = N$. By a similar argument we have that $G = HG_\alpha$ holds. Finally we note that G_α acts *irreducibly* in the sense that G_α does not normalize any proper nontrivial subgroup of H. To see that this holds let G_α normalize K where $1 \leqslant K \leqslant H$, but then $G_\alpha \leqslant KG_\alpha \leqslant G$ so either $K = H$ or $K = 1$, because G_α is maximal. The following proposition will allow us to describe a faithful primitive action of $G = H \rtimes Aut(H)$ which is permutation isomorphic to the action of G on Ω.

Proposition 6.6. [1, Ex 4.7.1] *Let K and H be finite groups and suppose that K acts faithfully and irreducibly as a group of automorphisms of H. Then $G := H \rtimes K$ acts faithfully and primitively by right multiplication on the set Γ of right cosets of $\mathbb{K} := \{(1,k) \mid k \in K\}$.*

Proof. First we show that this action of G is faithful. Let $(a,b) \in G$ then the right coset $\mathbb{K}(a,b) \in \Gamma$ is equal to $\mathbb{K}(a^b,1)$ since

$$\begin{aligned}(1,kb)(a^b,1) = (a^{bb^{-1}k^{-1}},kb) = (a^{k^{-1}},kb) = (1,k)(a,b)\\ \implies \mathbb{K}(a,b) = \{(1,k)(a,b) \mid k \in K\} = \{(1,kb)(a^b,1) \mid k \in K\} = \mathbb{K}(a^b,1)\end{aligned}$$

Now we have that all elements of Γ may be represented by $\mathbb{K}(a,1)$ for some $a \in H$. Furthermore, since there are $|G : \mathbb{K}| = |H|$ right cosets of $\mathbb{K}$, it must be the case that $\mathbb{K}(a,1) = \mathbb{K}(b,1)$ if and only if a and b are equal. We can now

[3] If, for example, $G \leqslant Sym(\Sigma)$ and $H \leqslant Sym(\Gamma)$ then we say that H and G are *permutation isomorphic* if there is a bijection $\lambda : \Sigma \to \Gamma$ and a group isomorphism $\phi : G \to H$ such that $\lambda(\sigma^x) = \lambda(\sigma)^{\phi(x)}$

show that only $(1,1) \in G$ acts as an identity on Γ. Let (c,d) be in the kernel of the action of G, then for all $a \in H$ we have

$$\begin{aligned} & \mathbb{K}(a,1)(c,d) = \mathbb{K}(a,1) \\ \iff & \mathbb{K}(ac,d) = \mathbb{K}(a,1) \\ \iff & \mathbb{K}((ac)^d,1) = \mathbb{K}(a,1) \qquad \text{by rewriting in the form } \mathbb{K}(h,1) \\ \iff & (ac)^d = a \end{aligned}$$

and in particular this holds for $a = c^{-1}$ so we have that c is the identity of H which in turn implies d is equal to the identity of K. Thus (a,c) is in the kernel of G if and only if $(a,c) = (1,1)$, so G is faithful. Next we show G act primitively. The point stabilizer of $\gamma := \mathbb{K}(1,1) \in \Gamma$ is $G_\gamma = \mathbb{K}$ since

$$\begin{aligned} & (c,d) \in G_\gamma \\ \iff & \mathbb{K}(1,1)(c,d) = \mathbb{K}(1,1) \\ \iff & \mathbb{K}(c,d) = \mathbb{K}(1,1) \\ \iff & \mathbb{K}(c^d,1) = \mathbb{K}(1,1) \\ \iff & c^d = 1 \\ \iff & c = 1, d \in K \end{aligned}$$

so $G_\gamma = \{(1,d) \mid d \in K\} = \mathbb{K}$, as required. Now, since $HG_\gamma = G$, if there is an M such that $G_\gamma < M \leqslant G$ then $M = (M \cap H)G_\gamma$ where $M \cap H$ is non trivial. However we assumed that $K = G_\gamma$ acts irreducibly on H so $M \cap H = H = M$ must hold. Thus we have proved G_γ is a maximal subgroup of G and so G acts primitively. □

By applying the proposition to $G := H \rtimes G_\alpha$ we obtain a faithful primitive action of G on the set Γ of right cosets of G_α, of which there are $|G : G_\alpha| = |H|$ many. Then since G_α is a point stabilizer for both actions we have that these actions are permutation isomorphic from [1, Lem 1.6A]. We will now show there is an isomorphism from $Aut(H)$ to $GL_m(p)$ which could then combine with an isomorphism from H to $V := (F_p)^m$, the m dimensional vector space over the finite field of order p, to create an isomorphism from N to $V \rtimes GL(V)$.

Proposition 6.7. [1, Ex 4.7.4] *Let H be an elementary abelian p-group of order p^m for some p. Then $Aut(H) \cong GL_m(p)$, the general linear group of all invertible $m \times m$ matrices over the finite field of order p.*

Proof. Let $H := T_1 \times \cdots \times T_m$ where the T_i are isomorphic cyclic groups of order p and choose elements $a_1, \ldots, a_m \in H$ such that $\langle a_i \rangle = T_i$ for each i. Then we will represent (uniquely) the elements of H by products of the form $a_1^{k_1} \ldots a_m^{k_m}$ for integers $0 \leq k_1, \ldots, k_m \leq p-1$ (where $a_i^{k_i}$ is the k_i^{th} power of a_i). Let $L \cong GL_m(p)$ be the set of all invertible $m \times m$ matrices with entries from $\mathbb{Z}_p$ and let V be the m dimensional vector space over $\mathbb{Z}_p$. For $1 \leq i \leq m$ let b_i be the row vector with all entries 0 except the i^{th} position which is 1, for example $b_1 = (1, 0, \dots, 0)$, then $b_1, \dots, b_m$ generate V. We represent elements of V (uniquely) by products of the form $b_1^{k_m}, \dots, b_m^{k_m}$ for integers $0 \le k_1, \dots, k_m \le p - 1$ (where $b_i^{k_i}$ represents $k_i b_i$ under scalar multiplication). Then $\psi : H \to V$ defined by $\psi(a_1^{k_1} \dots a_m^{k_m}) = b_1^{k_m}, \dots, b_m^{k_m}$ is an isomorphism.

We now build an isomorphism from $Aut(H)$ to L. For each $x \in Aut(H)$ we let the entries $\{x_{i,j} \mid 1 \le i, j \le m\}$ of the $m \times m$ matrix $[x_{i,j}]$ be defined to satisfy:

$$a_i x = a_1^{x_{1,i}} \dots a_m^{x_{m,i}} \text{ for } 1 \le i \le m \tag{1}$$

then we claim that $\phi : Aut(H) \to L$ defined by $x \mapsto [x_{i,j}]$ is an isomorphism. First we show that it is an injection. Let $x, y \in Aut(H)$ be such that $[x_{i,j}] = \phi(x) = \phi(y) = [y_{i,j}]$, then for any $a_1^{k_1} \dots a_m^{k_m} \in H$ we have

$$\begin{aligned}
(a_1^{k_1} \dots a_m^{k_m})x &= (a_1^{k_1})x \dots (a_m^{k_m})x && \text{since } x \text{ is a homomorphism} \\
&= (a_1 x)^{k_1} \dots (a_m x)^{k_m} && \text{since } x \text{ is a homomorphism} \\
&= (a_1 y)^{k_1} \dots (a_m y)^{k_m} && \text{since } x_{i,j} = y_{i,j} \text{ for all } 1 \le i, j \le m \\
& && \text{then (1) gives } a_i x = a_i y \text{ for all } 1 \le i \le m \\
&= (a_1^{k_1})y \dots (a_m^{k_m})y && \text{since } y \text{ is a homomorphism} \\
&= (a_1^{k_1} \dots a_m^{k_m})y && \text{since } y \text{ is a homomorphism}
\end{aligned}$$

so ϕ is injective. To show that ϕ is surjective we take an arbitrary $X = [x_{i,j}] \in L$ and show it is the image of some element of $Aut(H)$. It is known from Linear Algebra that the columns of X are linearly independent and thus $B := \{b_k X \mid 1 \le k \le m\}$ is a set of m linearly independent vectors which must span V because $b_1, \dots, b_m$ span V. Equivalently, in the group V the elements in B generate V and so $\psi^{-1}(B)$ generates H. If we let $c_i := \psi^{-1}(b_k X) = a_1^{x_{1,i}}, \dots, a_m^{x_{m,i}}$ Then there is an automorphism (and it is an automorphism because it maps a generating set to a generating set) of x which maps a_i to c_i for each i. Then this automorphism satisfies $\phi(x) = [x_{i,j}]$, as required. □

The next theorem follows from out prior work in this section. First we have that the images of $G := H \rtimes G_\alpha$ in $Sym(\Omega)$ and $Sym(\Gamma)$ are permutation isomorphic with regular abelian socle H, which is an elementary abelian p-group of some order p^m. If we choose a m dimension vector space over a field of order p then Proposition 6.7 shows there is an isomorphism from $N_\alpha \cong Aut(H)$ onto $GL(V)$. Let K be the image of G_α in this isomorphism and then we have that K acts irreducibly on V since G_α acts irreducibly on $H \cong V$ and we have that $H \rtimes G_\alpha \cong V \rtimes K$. Finally we have that the image of the point stabilizer $\{(1, g_\alpha) \in G \mid g_\alpha \in G_\alpha\}$ in $V \rtimes K$ is $\{(1, k) \in V \rtimes K \mid k \in K\}$, as required.

Theorem 6.8. *[1, Thm 4.7A] Let G be a finite primitive group with a regular abelian socle. Then G has degree p^m, for some prime p, and integer $m \ge 1$. If V is a m dimensional vector space over a field of order p then there is a subgroup $K \le GL(V)$ which acts irreducibly on V and there is an isomorphism from G onto $V \rtimes K$ which maps a point stabilizer of G onto the subgroup isomorphic to K that is $\mathbb{K} := \{(1, k) \mid k \in K\}$.*

In particular, the image of the normalizer N of H is the full affine group $AGL(V)$ which is the maximal primitive group of degree p^k with regular abelian socle, up to permutation isomorphism. We have now completed the classification in this case.

6.3.2 Finite Primitive Groups with Nonregular Socles

We continue by examining the nonregular case where $m = 1$, which we aim to show corresponds to the primitive groups of almost simple type.

Proposition 6.9. *Let H act nonregularly on Ω. Let $m = 1$ so that $H = T_1$. Then G is isomorphic to some group K where $K \leqslant Aut(T)$.*

Proof. For all $g \in G$ we have that $g^{-1}T_1g = T_1$, because T_1 is normal in G, and so $t \mapsto g^{-1}tg$ is an automorphism of T_1. The centralizer of T_1 in G is trivial because H is nonregular (Theorem 4.3B) and so the group homomorphism $\rho : G \to Aut(T_1)$ defined by $t^{\rho(g)} := g^{-1}tg$ is injective. Then $im(\rho)$ is isomorphic to G and satisfies $im(\rho) \leqslant Aut(T_1)$. This is sufficient since $Aut(T_1) \cong Aut(T)$. □

The following Theorem will classify all primitive groups with nonregular socles. We prove the majority of this theorem and provide reference for the final case. This is a lengthy proof so we break it up with a number of lemmas and cases.

Theorem 6.10. *Let G be a finite primitive group acting on Ω with a nonregular socle H and socle type T. Then G is isomorphic to one of the following:*

(i) a primitive group U with $soc(U) \cong T$;

(ii) a primitive group U of diagonal type with $soc(U) \cong T^m$ and degree $|T|^{m-1}$; or

(iii) a primitive subgroup of a wreath product $U\ wr_\Gamma\ Sym(\Gamma)$ with the product action, where $|\Gamma| > 1$ and U is a primitive nonregular group of either almost simple or diagonal type.

We will identify G with the image of its permutation representation in $Sym(\Omega)$ and identify H with its image in the same representation. With Proposition 6.9 we have already shown that when $m = 1$ we have a primitive group of type (i). We proceed by proving two lemmas and we will retain the notation defined in these lemmas for the remainder of the proof.

Lemma 6.11. *Let N be the normalizer of H in $Sym(\Omega)$ and let N_α be the point stabilizer in N of some point $\alpha \in \Omega$. Then N is primitive, $N = N_\alpha H$ and H is transitive.*

Proof. Since $H \trianglelefteq G$ we have $G \leqslant N$ and so N is primitive because G is primitive. Next we show that $N = N_\alpha H$.

As N_α is a maximal subgroup of N, since N is primitive, then either $N = N_\alpha H$ or $N_\alpha = N_\alpha H$ holds. Suppose that $N_\alpha H = N_\alpha$, which implies $H \subseteq N_\alpha$, then since $H \trianglelefteq N$ we have that $H \subseteq g^{-1}N_\alpha g$ for all g in N. Since N_α is conjugate to all other point stabilizers we conclude that H is contained in all of the point stabilizers and so H acts trivially on Ω, a contradiction. Therefore $N_\alpha H = N$ and we will finish by showing H is transitive.

For all $\beta \in \Omega$ we can choose $x \in N$ such that $\alpha^x = \beta$ and since $N_\alpha H = N$ we may find $x_\alpha \in N_\alpha$ and $h \in H$ such that $x = x_\alpha h$. Then we have that $\alpha^x = \alpha^{x_\alpha h} = \alpha^h$, because $x_\alpha \in N_\alpha$, and so H is transitive because $\alpha^H = \Omega$ is its only orbit. □

Lemma 6.12. *Let $\pi_i : H \to T_i$ denote the projection map*

$$(a_1, \ldots, a_m) \mapsto a_i$$

for $i = 1, \ldots, m$. Define

$$T_i' := \{h \in H \mid \pi_j(h) = 1 \textit{ if and only if } j \neq i\}; \textit{ and}$$

$$R_i := \{h \in H_\alpha \mid \pi_j(h) = 1 \textit{ if and only if } j \neq i\}$$

then N_α acts transitively on both $\{T_1', \ldots, T_m'\}$ and $\{R_1, \ldots, R_m\}$ by conjugation. Furthermore N_α normalizes the internal direct product $K := R_1 \ldots R_m$.

Proof. First we show that N acts transitively on $\{T_1', \ldots, T_m'\}$ by conjugation. Theorem 4.5(ii) states that every minimal normal subgroup of a nontrivial finite group is a direct product of simple groups which are conjugate. H is the nonregular socle of N so it is the unique minimal normal subgroup of N (Corollary **??** gives uniqueness) and thus N acts transitively on $\{T_1', \ldots, T_m'\}$ by conjugation.

Now let $1 \leq i, j \leq m$ and then, since N acts transitively on $\{T_1', \ldots, T_m'\}$, there is an $x \in N$ such that $x^{-1}T_i'x = T_j'$ holds. Since $N = N_\alpha H$ (Lemma 6.11) we can choose $x_\alpha \in N_\alpha$ and $h \in H$ such that $x_\alpha h = x$. Then we have that $T_j' = x^{-1}T_i'x^{-1} = x_\alpha^{-1}h^{-1}T_i'hx_\alpha$ and so if we can show that $h^{-1}T_i'h = T_i'$ that will show T_i' and T_j' are conjugate in N_α. We may express $h = (h_1, \ldots, h_m)$ and take an arbitrary element $t = (1, \ldots, t_i, \ldots, 1)$ of T_i'. Then $h^{-1}th = (h_1^{-1}1h_1, \ldots, h_i^{-1}t_ih_i, \ldots, h_m^{-1}1h_m) = (1, \ldots, h_i^{-1}t_ih_i)$ is in T_i', so $h^{-1}T_i'h \subseteq T_i'$. On the other hand, $h_i \in T_i$ implies $h_i^{-1}T_ih_i = T_i$ and $h^{-1}T_i'h \supseteq T_i'$ follows. Thus we have shown N_α acts transitively on $\{T_1', \ldots, T_m'\}$.

It remains to show that N_α acts transitively on $\{R_1, \ldots, R_m\}$ by conjugation. Let $1 \leq i, j \leq m$ then choose an $x \in N_\alpha$ such that $x^{-1}T_ix = T_j$ and see that $x^{-1}R_ix \subseteq x^{-1}T_i'x = T_j$ because R_i is a subset of T_i'. Now if $h \in H_\alpha$ we may express h as a product $r_1, \ldots, r_m$ where $r_k \in R_k$ for $k = 1, \ldots, m$ and it follows that

$$\begin{aligned} x^{-1}hx &= x^{-1}r_1r_2 \ldots r_mx \\ &= x^{-1}r_1xx^{-1}r_2x \ldots x^{-1}r_mx \\ &= s_1 \ldots s_m && \text{where } s_n := x^{-1}r_nx \end{aligned}$$

Since conjugation by x permutes the T_k' and sends T_i' to T_j' we have that $s_k \in T_j'$ if and only if $k = i$ or $s_k = 1$. Furthermore because H_α is normal in N_α we have that $x^{-1}hx \in H_\alpha$ and so, in particular, $s_i \in R_j$. Thus we have shown $x^{-1}R_ix \subseteq R_j$ and since $xT_j'x^{-1} = T_i'$ we can apply a similar argument to show that $xR_jx^{-1} \subseteq R_i$, so equality holds. Thus N_α acts transitively on $\{R_1, \dots, R_m\}$ and it follows immediately that N_α normalizes $R_1 \dots R_m = K$. □

Notice that $H_\alpha \leqslant K \leqslant H$, by definition. We now split our analysis into two cases, which are $R_1 < T_1'$ and $R_1 = T_1'$. We start with the case $R_1 < T_1'$,

Case $\mathbf{R_1 < T_1'}$.

Here we have that $H_\alpha \leqslant K < H$ and either $N_\alpha K = N_\alpha$ or $N_\alpha K = N$ holds because N_α is a maximal subgroup of N, The next lemma proves that it is the former which holds.

Lemma 6.13. *Assume $R_1 < T_1'$ holds. Then $N_\alpha K = N_\alpha$ and $K = H_\alpha$.*

Proof. We first show $N_\alpha K = N_\alpha$, by contradiction. Since N_α is a maximal subgroup of N we have that either $N_\alpha K = N_\alpha$ or $N_\alpha K = N$ holds. Assume that $N_\alpha K = N$ and let $x \in N$. By our assumption, we may choose $x_\alpha \in N_\alpha$ and $k \in K$ so that $x = kn_\alpha$. Then $x^{-1}Kx = x_\alpha^{-1}k^{-1}Kkx_\alpha = x_\alpha^{-1}Kx_\alpha$ and $x_\alpha^{-1}Kx_\alpha = K$ follows because N_α normalizes K. Our choice of $x \in N$ was arbitrary so $K \lhd N$ and this is a contradiction because K is a proper subgroup of H, which is the minimal normal subgroup of N.

Now we have that $K \leqslant N_\alpha$ (because $N_\alpha K = N_\alpha$) and $K < H$ which together imply $K \leqslant H \cap N_\alpha = H_\alpha$, as required. This completes the proof. □

Denote the set of right cosets of R_1 in T_1' by Δ and consider the natural (transitive) action of T_1' on Δ. Then R_1 stabilizes a point in Δ. This action is also faithful because T_1' is a simple group and so the kernel of this action, which is a normal subgroup of T_1', must be trivial. Since $T_2', \dots, T_m'$ are isomorphic to T_1' and $R_2, \dots, R_m$ are isomorphic to R_1 there are transitive faithful actions of $T_2', \dots, T_m'$ on Δ such that $R_2, \dots, R_m$ are point stabilizers of the respective actions. Combining these by

$$(\delta_1, \dots, \delta_m)^{t_1 \dots t_m} := (\delta_1^{t_1}, \dots, \delta_m^{t_m})$$

we obtain a faithful transitive action of H on Δ^m. Moreover $H_\alpha = K = R_1 \dots R_m$ is a point stabilizer of the point $(d_1, \dots, d_m) \in \Delta^m$ where each d_i is the point which R_i stabilizes in Δ. Thus, by [1, Lem 1.6A], the actions of H on Ω and Δ^m are equivalent because H_α is a point stabilizer for both actions. It can be shown [1, Lem 4.5A] that $N \leqslant Sym(\Omega)$ is permutation isomorphic to a wreath product of the form $M\ wr_\Gamma\ Sym(\Gamma)$ where M is the normalizer of the image, T_Δ, of the permutation representation of T_1' in $Sym(\Delta)$ and $\Gamma := \{1, \dots, m\}$. By Theorem 3.7 and because N is primitive we have that M is necessarily primitive. Observe that $soc(M) \leqslant T_\Delta$ because T_Δ is normal in M. However $T_\Delta \cong T_1'$ is simple so no nontrivial normal subgroup of T_Δ is normalized by M. Thus $soc(M) = T_\Delta$ and M is of almost simple type. This shows G is one of the groups of type (iii), a primitive group of product action type.

Case $\mathbf{R_1 = T_1'}$.

In this case, $R_i = T_i'$ for all i since each R_i is conjugate to R_1.

Lemma 6.14. *For $i = 1, \ldots, m$ define $K_i := H_\alpha \cap \ker(pi_i)$, then we have*

$$H_\alpha / K_i \cong \pi_i(H_\alpha) = T_i$$

Proof. By using the second isomorphism theorem[4] we obtain

$$H_\alpha \ker(\pi_i)/\ker(\pi_i) \cong H_\alpha/(H_\alpha \cap \ker(\pi_i)) \tag{2}$$

Furthermore $H_\alpha \ker(\pi_i) = H$ since if $h = (h_1, \ldots, h_m) \in H$ then there is $a = (a_1, \ldots, a_m) \in H_\alpha$ with $a_i = h_i$ (since $R_i = T_i'$) and there is $p = (p_1, \ldots, p_m) \in \ker(\pi_i)$ where $p_j = h_j a_i^{-1}$ for $j \neq i$. Then $h = pa \in H_\alpha \ker(\pi_i)$ so we have $H \leqslant H_\alpha \ker(\pi_i)$ and the reserve inclusion holds because H_α and K_i are both subgroups of H. Applying this and $H_\alpha \cap \ker(\pi_i) = K_i$, which is clear from the definition, to (2) we obtain:

$$H/\ker(\pi_i) \cong H_\alpha/K_i$$

and finally $H/\ker(\pi_i) \cong im(\pi_i) = T_i$ follows from the first isomorphism theorem. □

Now suppose that d of the $K_1, \ldots, K_m$ are distinct. We then choose $1 \leq i_1, \ldots, i_d \leq m$ such that $K_{i_1}, \ldots, K_{i_d}$ are distinct from each other. We have the following result

$$K_{i_1} \cap \cdots \cap K_{i_d} = K_1 \cap \cdots \cap K_m = 1$$

because $k_j \in K_j$ implies $\pi_j(k_j) = 1$ for each $j \in \{1, \ldots, m\}$ so any element of this intersection has an identity in every entry. Now we may apply [1, Lem 4.3A] to obtain that $H_\alpha = V_1 \times \cdots \times V_d$ where each $V_i \cong T$, and $d < m$ because $H_\alpha < H$. We divide the argument into two further subcases:

Subcase: $\mathbf{R_1 = T_1'}$ and $\mathbf{d = 1}$.

Here we have that $H_\alpha \cong T_1' \cong T$ so we may construct the isomorphism $\psi : T \to H_\alpha$. Then we have that, for $(t_1, \ldots, t_m) \in T^m$, the mapping ψ defined by

$$(t_1, \ldots, t_m) \mapsto (\pi_1(\psi_1(t_1)), \ldots, \pi_m(\psi_m(t_m))$$

[4] Let G be a group. Let S be a subgroup of G and let N be a normal subgroup of G, then:
(i) $SN \leq G$;
(ii) $S \cap N \lhd G$ and
(iii) $(SN)/N \cong S/(S \cap N)$.

is an isomorphism from T^m onto H. Furthermore the image in ψ of the group

$$C := \{(t, \dots, t) \mid t \in T\}$$

is H_α. Comparing with the Section 5, where C was the centralizer of T and a point stabilizer of the action, we see that H is permutation isomorphic to socle of a primitive wreath product with diagonal action. Since G is contained in the normalizer of H we conclude that G is permutation isomorphic to a group of diagonal type, case (ii).

It can be shown [1, page 128-129] that in the final case G is of product action type (iii) with socle of diagonal type (ii), which concludes the proof.

7 The Primitive Database

7.1 Historical Background

The classification of the primitive permutation groups is a long standing problem which began to generate real interest in the late 19th Century. The early effort made by Jordan[2] (1871) to count the primitive permutation groups of degree up to 17 was the first big step forward. Others made corrections to his work and extended it resulting in the correct counts being published for the primitive permutation groups up to degree 20 by 1912. At this point hand calculations became too cumbersome and interest dwindled until the appearance of symbolic computation in the 1960s. With the use of this new tool Sims[3] classified the primitive permutation groups of degree up to 50 and his work was widely distributed but never published.

The next great turn of fortune for the problem came after the announcement of the Classification of Finite Simple Groups in 1983, which allowed Dixon and Mortimer[4] to use the O'Nan-Scott Theorem to classify the non affine type primitive groups of degree less than 1000. The classification of the affine type primitive groups is equivalent to the classification of irreducible* subgroups of $GL_n(p)$ for prime p. The classification of primitive groups of affine type was (mostly) completed up to degree 255 by Short[5] in 1991 and completed up to degree 6561 by Eick and Höfling[**?**] in 2003.

Many of the classifications since Sims became databases in GAP, MAGMA or both including all of the following. The primitive groups of degree less than 1000 were classified by Roney-Dougal and Unger[7] in 2003 and subsequently the classification for degree less than 2500 was completed by Roney-Dougal[6] in 2005. Most recently, the classification primitive groups of degree less than 4095 was completed by Courtts, Roney-Dougal and Quick[8] in 2009.

*Irreducible, in the context of an *irreducible* subgroup of $GL_n(p)$, is essentially a vector space equivalent of the property *transitive* for permutation groups. A subgroup of $GL_n(p)$ is irreducible if it does not act trivally on any subspace of the n dimensional vector space over the finite field of order p by the natural action.

7.2 The Database Conversion

The database of primitive permutation groups exists in MAGMA up to degree 4095. In GAP the database existed up to degree 2499. My objective was to create GAP database files for the groups of degrees 2500 to 4095 by using the MAGMA database. I also changed three parameters in GAP to allow the new files to be accessed. In GAP 4.8.3, the primitive database can be found in the *prim* folder which is in the main GAP directory. Inside *prim*, the GAP parameters that were changed can be found in the file *primitiv.grp* and both the old and the new database files can be found in the *grps* folder, with the new files named $gps25, \ldots, gps39$. The GAP database files are collections of lists, one for each degree, written in the following format:

PRIMGRP[n]:=[[GROUP], ... ,[GROUP]];
PRIMGRP[n+1]:=[[GROUP], ... ,[GROUP]];
. . .

Each element of these lists is a primitive group of the given degree (n). Each group is stored as a list with the following format:

[ID, Size, Simple+2*Soluble, O'Nan-Scott type, Suborbits, Transitivity, Name, Socle type, Generators, Sims Number]

A description of each parameter given in the following table.

Parameter	Meaning
ID	Integer between 1 and the number of Primitive Groups of this degree which identifies this particular primitive group, together with its degree.
Size	Integer, the order of the group
Simple + 2*Soluble	0 if the group is neither simple nor soluble, 1 if it is simple but not soluble, 2 if it is soluble but not simple, 3 if it is simple and soluble.
O'Nan-Scott type	The O'Nan-Scott type of the group, "1", "2", "3a", "3b", "4a", "4b" or "4c".
Suborbit lengths	The lengths of the suborbits
Transitivity	The largest integer n such that the group is n-transitive
Name	A name for the group. Not all groups of degree greater than 2499 are named.
Socle type	The socle type (simple group), parameters (of the simple group) and width (m such that the socle is isomorphic to the direct product of m simple groups)
Generators	The generators of the group or, if the group is of affine type, the generators of the matrix quotient.
Sims Number	Not relevant for groups of degrees greater than 50. Identifier of the group in an older database, created by Charles C. Sims.

The three parameters in *primitiv.grp* that were changed to make the extended database accessible are named PRIMRANGE, PRIMINDEX and PRIMLENGTHS. The parameter PRIMRANGE is a list of the degrees for which the database has entries, the change made was simply from [1..2499] to [1..4095]. The parameter PRIMINDEX is a list integers of where the i^{th} entry tells GAP which database file the groups of degree i are in. The required change was carried out by appending the list of locations of the new groups in the new database files. Finally, PRIMLENGTHS is a list of integers where the i^{th} entry is the number of primitive groups of that degree and I updated this for degrees 2500 to 4095.

7.3 Testing for accuracy

The following tests for accuracy were performed on the groups in the database with degree 2500 to 4095:
Test 1: For each degree, count the number of groups of each O'Nan-Scott type (affine, almost simple, diagonal and product type) in both databases and confirm they match. This also shows that the number of primitive groups of each degree is the same in each database.
Test 2: For each degree list the orders of the groups of that degree and confirm that they match.

In doing this it has demonstrated my understanding this theory. This is further demonstrated by the added detail I have included whilst reproducing proofs from my source [1].

8 Conclusion

This paper has provided the necessary background to understand and prove four of the five cases in the O'Nan-Scott Theorem for classifying finite primitive groups and contains reproductions of the proofs for three of these five cases. Reproducing these and other proofs with added detail has highlighted my understanding of the theory. This is furthered by the personally adapted notation I used when defining wreath products. This paper has also documented the database conversion which was performed to extend the primitive group library in GAP, which provides evidence that I have successfully and carefully carried out the aims of this project.

The theory covered in this paper is fundamental to the study of groups. As mentioned earlier, all groups are isomorphic to permutation groups which are, in short, constructed from primitive groups. For this reason, the classification of finite primitive groups which the O'Nan-Scott Theorem provides is of great importance.

References

[1] John D. Dixon and Brian Mortimer, *Permutation Groups*, Springer, New York, 1996. 5-22, 44-51, 106-132

[2] C. Jordan, *Traite des Substitutions et des Equations Algebriques*, Gauthier-Villers, Paris, 1871.

[3] C.C. Sims *Computational methods for permutation groups*, in: Computational Problems in Abstract Algebra, ed. J. Leech, Pergamon, (1970), 169-183.

[4] J.D. Dixon, B. Mortimer, *The primitive permutation groups of degree less than 1000*, Math. Proc. Cambridge Philos. Soc. (1988)

[5] M.W. Short, *The Primitive Soluble Permutation Groups of Degree less than 256*, Springer-Verlag, Berlin, (1991)

[6] C.M. Roney-Dougal, *The primitive permutation groups of degree less than 2500*, (2005)

[7] C.M. Roney-Dougal, W.R. Unger, *The primitive affine groups of degree less than 1000*, J. Symbolic Comput., 35, (2003), 421439.

[8] H.J. Courtts, M. Quick, C.M. Roney-Dougal, *The Primitive Permutation Groups of Degree Less Than 4096*

9 Appendix

This Appendix contains programs and code used for the database conversion described in Section 7.2.

9.1 Creation of new database files

9.1.1 The program

Most of this code was written by the authors supervisor, Colva Roney-Dougal, when she performed an earlier conversion. The exceptions are MakeSocleForGap (written by the author), get_ons (which the author updated to account for 4a and 4b occuring) and some of the comments.

```
// Takes a permutation group in MAGMA and writes it as a list
// of generators in GAP readable form

MakeGapFormat:= procedure(grp)
  printf "[";
  for i in [1..Ngens(grp)-1] do
    printf "%o,", grp.i;
  end for;
  printf "%o]", grp.Ngens(grp);
end procedure;


// takes a primitive group of affine type in MAGMA and writes the matrix
// quotient as a list of generators in GAP readable form.

MakeMatGapFormat:= procedure(grp)
  mat_grp:= MatrixQuotient(grp);
  if Ngens(mat_grp) eq 0 then
    printf "[]";
  else
    p:= #BaseRing(mat_grp.1);

    // this assertion is safe since getting these from groups of
    // affine type
    assert IsPrime(p);

    d:= Dimension(mat_grp);

    // The mat_grp.i are the generators of the matrix group mat_grp
    // and the x[i][j] are the entries of these generators.
    for i in [1..Ngens(mat_grp)] do
      x:= mat_grp.i;
      for j in [1..d] do
    if i eq 1 and j eq 1 then
     printf "[ [[";
    elif j eq 1 then
     printf "[[";
    else
     printf "[";
    end if;
    for k in [1..d-1] do
     printf "%o*Z(%o )^0,", x[j][k], p;
    end for;
    if j lt d then
     printf "%o*Z(%o)^0],", x[j][d], p;
    else
     printf "%o*Z(%o)^0]]", x[j][d], p;
    end if;
   end for;
   if i lt Ngens(mat_grp) then
    " ,\n ";
   end if;
  end for;
  "]\n";
 end if;
end procedure;


// Finds suborbit lengths for the GAP Database

sub_lengths:= function(g)
 orbits:= Orbits(Stabiliser(g, 1));
 assert #orbits[1] eq 1;
 Exclude(~orbits, orbits[1]);
 lengths:= [#x : x in orbits];
 Sort(~lengths);
 dif_lengths:= Seqset(lengths);
 new_lengths:=[];
 for x in dif_lengths do
  i:= 0;
  for j in [1..#lengths] do
   if lengths[j] eq x then
    i:= i+1;
   end if;
  end for;
  Append(~new_lengths, [x, i]);
 end for;
 return new_lengths;
end function;
```

```
// Converts O'Nan Scott Types to Gap Format. The MAGMA database does not
// specify between the two types of Diagonal Action (3a and 3b in GAP) nor the
// three types of Product Action (4a, 4b and 4c in GAP) so this function
// distinguishes these cases. In the cases of 4a and 4b the function is coded
// to know where they are found because they only occur at degree 3600
// (2 and 3 times, respectively). This seemed appropriate as the next occurance
// of type 4a, 4b would be at degree 168^2 which is far beyond the current
// extent of this database.

get_ons:= function(g, ons, i)
   if ons eq "Affine" then
      id:= "1";
    elif ons eq "AlmostSimple" then
      id:= "2";

    // When there is a diagonal action, either the socle is the minimal normal
    // subgroup of the primitive group and it is case 3b otherwise it is case 3a.
    elif ons eq "DiagonalAction" then
      soc:= Socle(g);
      ns:= NormalSubgroups(soc);
      num_norms:= 0;
      for x in ns do
        if (x`order gt 1) and (x`order lt #g) and IsNormal(g, x`subgroup) then
          num_norms:= num_norms+1;
        end if;
      end for;
      if num_norms gt 1 then
        id:= "3a";
      else
        id:= "3b";
      end if;

      // There are only 2 cases of 4a and 3 cases of 4b for groups of degree
      // less than 28224. These are recognised by their position in the database.
      // All other occurences of a product action are type 4c.
    elif ons eq "ProductAction" then
      if Degree(g) ne 3600 then
       id:= "4c";
      elif i in {6,16} then
       id:= "4a";
      elif i in {14,22,29} then
       id:="4b";
      else
       id:="4c";
      end if;
    else
      "error in ONS, i =", i;
    end if;
    return id;
end function;


// Finds the socle type of a primitive group (if it is one of the socle types
// of a group currently in the MAGMA database) and converts it to the form
// required for the socle type entry in the GAP primitive group database

function MakeSocleForGap(g)
   S:=Socle(g);
   C:=CompositionFactors(S);
   type:=C[1][1];
   p:=C[1][2];
   q:=C[1][3];
   width:=#C;

   case type:
   when 1:
      soc:=[*"\"L\"",[p+1,q],width*];
   when 2:
      soc:=[*"\"B\"",[p,q],width*];
   when 3:
      soc:=[*"\"C\"",[p,q],width*];
   when 4: // Does not occur for degrees in [2500..4095]
      soc:=[*"\"D\"",[p,q],width*];
   when 5:
      soc:=[*"\"G\"",[2,q],width*];
   when 10:
      soc:=[*"\"^2A\"",[p,q],width*];
   when 11: // Does not occur for degrees in [2500..4095]
      soc:=[*"\"^2B\"",[2,q],width*];
   when 12: // Does not occur for degrees in [2500..4095]
      soc:=[*"\"^2D\"",[p,q],width*];
   when 13: // Does not occur for degrees in [2500..4095]
      soc:=[*"\"^3D\"",[4,q],width*];
   when 15:
      soc:=[*"\"2F\"",[4,q],width*];
   when 17:
      soc:=[*"\"A\"",p,width*];

   // Case 18: socle type is a sporadic group
   when 18:
      case p:
      when 1:
         p:="M(11)";
      when 2:
         p:="M(12)";
      when 3:
         p:="M(22)";
      when 4:
         p:="M(23)";
      when 5:
         p:="M(24)";
      when 6:
         p:="J(1)";
      when 7:
         p:="HS";
      when 8:
         p:="J(2)"; // HJ = J(2) = F(5-)
      when 9:
         p:="Mc";
      when 10:
         p:="Suz";
      when 14:
         p:="Co(3)";
      when 15:
         p:="He"; // He = F(7)
      when 16:
         p:="Fi(22)"; // does not occur in gap lib of <2500
      when 20:
         p:="Ru"; // does not occur in gap lib of <2500
      end case;
      soc:=[*"\"Spor\"",p,width*];

   when 19:
      soc:=[*"\"Z\"",q,width*];
   end case;

   // With the information we have found,
   // create a string that is a GAP readable socle type.
   if type eq 18 then
      out:="["*soc[1]*", \""*soc[2]*"\", "*IntegerToString(soc[3])*"]";
   else
      out:="["*soc[1]*", "*Sprint(soc[2])*", "*IntegerToString(soc[3])*"]";
   end if;

   return out;
end function;
```

```
// Uses the above procedures to create the GAP database files for primitive
// groups of degree in [d1..d2]. We will avoid calculating many properties
// of S_n and A_n directly since they are known and to be efficent.

procedure GetGapFiles(d1, d2)
  for d in [d1..d2] do
    printf "PRIMGRP[%o]:= \n[", d;
    max:= NumberOfPrimitiveGroups(d);
    for i in [1..max] do
      g, name, ons:= PrimitiveGroup(d, i);

      // get order
      if i lt (max-1) then
      s:= #g;
      elif i eq max-1 then
        s:= "Factorial(" cat IntegerToString(d) cat ")/2";
      else
        s:= "Factorial(" cat IntegerToString(d) cat ")";
      end if;

      // get simple+2*soluble
      if IsSimple(g) then b1:= 1; else b1:= 0; end if;
      if IsSoluble(g) then b2:= 2; else b2:= 0; end if;
      b:= b1+b2;

      // get o'nan scott type
      // first deal with S_n and A_n
      if i gt max-2 then
        id:= "2";
      else
        id:= get_ons(g, ons, i);
      end if;

      // get suborbit lengths
      // first deal with S_n and A_n
      if i gt max-2 then
        sl:= [[d-1, 1]];
      else
        sl:= sub_lengths(g);
      end if;

      // get transitivity
      // first deal with S_n and A_n
      if i eq max-1 then
        t:= d-2;
      elif i eq max then
        t:= d;
      else
        t:= Transitivity(g);
      end if;

      // get socle type
      // first deal with S_n and A_n
      if i gt max-2 then
         soc:="[\"A\"," * IntegerToString(i) * ",1]";
      else
         soc:=MakeSocleForGap(g);
      end if;

      // combine everything into a GAP readable primitive group for the database
      printf "[%o,%o,%o,\"%o\",[ %o", i, s, b, id, sl[1];
      for k:=2 to #sl do
            printf ", %o ", sl[k];
      end for;
      printf " ],%o,\"%o\",%o,", t, name, soc;

      // get generators
      // first deal with S_n and A_n
      if i eq max-1 then
        printf "\"Alt\"";
      elif i eq max then
        printf "\"Sym\"";
      // deal with affine type
      elif id eq "1" and (d gt 3) then
        MakeMatGapFormat(g);
      elif IsPrime(d-1) and g eq PSL(2, d-1) then
        printf "\"psl\"";
      elif IsPrime(d-1) and g eq PGL(2, d-1) then
        printf "\"pgl\"";
      elif i eq max-1 then
        printf "\"Alt\"";
      elif i eq max then
        printf "\"Sym\"";
      else
      // deal with other types
        MakeGapFormat(g);
      end if;

      // leave space for sims number if degree less than 51
      if d lt 51 then
```

```
        printf ",";
      end if;

      // format appropriately depending on whether or not there are more groups
      // of this degree still to be done.
      if i lt max then
        printf "],\n";
      else
        printf "]];\n";
      end if;
    end for;
  end for;
end procedure;
```

9.1.2 Making the files

After loading the above program into MAGMA, the following code will create the new database files.

```
SetOutputFile("gps25.g");
GetGapFiles(2500, 2607);
UnsetOutputFile();

SetOutputFile("gps26.g");
GetGapFiles(2608, 2713);
UnsetOutputFile();

SetOutputFile("gps27.g");
GetGapFiles(2714, 2809);
UnsetOutputFile();

SetOutputFile("gps28.g");
GetGapFiles(2810, 2928);
UnsetOutputFile();

SetOutputFile("gps29.g");
GetGapFiles(2929, 3049);
UnsetOutputFile();

SetOutputFile("gps30.g");
GetGapFiles(3050, 3136);
UnsetOutputFile();

SetOutputFile("gps31.g");
GetGapFiles(3137, 3251);
UnsetOutputFile();
```

```
SetOutputFile("gps32.g");
GetGapFiles(3252, 3355);
UnsetOutputFile();

SetOutputFile("gps33.g");
GetGapFiles(3356, 3465);
UnsetOutputFile();

SetOutputFile("gps34.g");
GetGapFiles(3466, 3557);
UnsetOutputFile();

SetOutputFile("gps35.g");
GetGapFiles(3558, 3672);
UnsetOutputFile();

SetOutputFile("gps36.g");
GetGapFiles(3673, 3722);
UnsetOutputFile();

SetOutputFile("gps37.g");
GetGapFiles(3723, 3851);
UnsetOutputFile();

SetOutputFile("gps38.g");
GetGapFiles(3852, 3969);
UnsetOutputFile();

SetOutputFile("gps39.g");
GetGapFiles(3970, 4095);
UnsetOutputFile();
```

9.2 Accuracy Checks

9.2.1 Test 1

The following (MAGMA) code counts the number of groups of each O'Nan-Scott type (affine, almost simple, diagonal action and product action) for each degree from 2500 to 4095, in the MAGMA database. The information for degree $2499 + i$ in stored the i^{th} position of a list called *mag_test_*1. The list called *mag_test_*1 was then made made into a file so it could be read into GAP.

```
mag_test_1:=[];
for i:=2500 to 4095 do
  count:=[0,0,0,0];
  for j:=1 to NumberOfPrimitiveGroups(i) do;
```

```
    G,n,ons:=PrimitiveGroup(i,j);
    if ons eq "Affine" then count[1]:=count[1]+1; end if;
    if ons eq "AlmostSimple" then count[2]:=count[2]+1; end if;
    if ons eq "DiagonalAction" then count[3]:=count[3]+1; end if;
    if ons eq "ProductAction" then count[4]:=count[4]+1; end if;
  end for;
  test:=Append(mag_test_1,count);
end for;
```

The next piece of (GAP) code counts the number of groups of each O'Nan-Scott type (affine, almost simple, diagonal action and product action) for each degree from 2500 to 4095, in the GAP database. The information for degree $2499 + i$ in stored the i^{th} position of a list called *gap_test_1*.

```
gap_test_1:=[];
for i in [2500..4095] do
  count:=[0,0,0,0];
  for j in [1..NrPrimitiveGroups(i)] do
    ons:=ONanScottType(PrimitiveGroup(i,j));
    if ons = "1" then count[1]:=count[1]+1; fi;
    if ons = "2" then count[2]:=count[2]+1; fi;
    if ons = "3a" then count[3]:=count[3]+1; fi;
    if ons = "3b" then count[3]:=count[3]+1; fi;
    if ons = "4a" then count[4]:=count[4]+1; fi;
    if ons = "4b" then count[4]:=count[4]+1; fi;
    if ons = "4c" then count[4]:=count[4]+1; fi;
  od;
  Add(gap_test_1,count);
od;
```

Finally the lists *gap_test_1* and *mag_test_1* were compared in GAP with the following test, which confirmed that they were equal.

```
pass:=true;
for i in [1..1596] do
  if (gap_test_1[1]<>mag_test_1[1]) then
    Print("fail at degree = ",  i);
      pass:=false;
    fi;
od;
pass;
```

9.2.2 Test 2

The following (MAGMA) code finds the order of each group in the database with degree from 2500 and 4095, in the MAGMA database. The information for degree $2499 + i$ in stored the i^{th} position of a list called *mag_test_2*. The list called *mag_test_2* was then made made into a file so that it could be read into GAP.

```
mag_test_2:=[];
for i:=2500 to 4095 do
orders:=[];
for j:=1 to NumberOfPrimitiveGroups(i)-2 do;
orders:=Append(orders,Order(PrimitiveGroup(i,j)));
end for;
mag_test_2:=Append(mag_test_2,orders);
end for;
```

The following (GAP) code finds the order of each group in the database with degree from 2500 and 4095, in the GAP database. The information for degree $2499 + i$ in stored the i^{th} position of a list called *gap_test_2*.

```
gap_test_2:=[];
for i in [2500..4095] do
orders:=[];
for j in [1..NrPrimitiveGroups(i)-2] do
Add(orders,Size(PrimitiveGroup(i,j)));
od;
Add(gap_test_2,orders);
od;
```

Finally the lists *gap_test_2* and *mag_test_2* were compared in GAP with the following test, which confirmed that they were equal. Order matters when comparing lists with <> so we need to know the groups are ordered the same in GAP and MAGMA to stop the test returning a misleading false. The indexing of the primitive groups is the same for both databases from degree 2500 to 4095 because our conversion created the GAP database using the MAGMA indexing.

```
pass:=true;
for i in [1..1596] do
if (gap_test_2[1]<>mag_test_2[1]) then Print("fail at degree = ", i); pass:=false; fi;
od;
Print(pass);
```