The O'Nan-Scott Theorem for Finite Primitive Permutation Groups, and Finite Representability

by

Joanna Fawcett

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2009

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

The O'Nan-Scott Theorem classifies finite primitive permutation groups into one of five isomorphism classes. This theorem is very useful for answering questions about finite permutation groups since four out of the five isomorphism classes are well understood. The proof of this theorem currently relies upon the classification of the finite simple groups as it requires a consequence of this classification, the Schreier Conjecture.

After reviewing some needed group theoretic concepts, I give a detailed proof of the O'Nan-Scott Theorem. I then examine how the techniques of this proof have been applied to an open problem which asks whether every finite lattice can be embedded as an interval into the subgroup lattice of a finite group.

Acknowledgements

I would like to thank my supervisor, Professor Ross Willard, for his help and insight, as well as for introducing me to this intriguing topic. I would also like to thank Professors John Lawrence and Yu-Ru Liu for being a part of my thesis committee. Lastly, I would like to thank NSERC for their financial support.

Dedication

To P and D Fawcett for their love,
support and humour and for putting up
with the din of my incessant blathering.

And to Ed Wang, who inspired my
love of group theory in the first place.

Contents

Introduction

Until the mid nineteenth century, the concept of a group was essentially that of a permutation group, and even though we now have a more abstract concept of a group, it is a simple result of Cayley's that any group can be embedded into a permutation group. Although it is often less beneficial to study groups within this framework, permutation groups are still quite important and not only appear in many other branches of mathematics (for example, combinatorics) but also form an active field of research today. Primitive finite permutation groups can be thought of as the building blocks of finite permutation groups, and questions about finite permutation groups can often be reduced to the primitive case. Thus it would be very useful to know the structure of these groups.

The largest achievement in finite (abstract) group theory in the last half century (and possibly ever) is the classification of all finite simple groups. Its proof, if it can be called that, spans thousands of pages and uses the research of hundreds of mathematicians, and although there is a widespread belief that the proof is complete, this is not certain. Still, the classification has been used to solve many open problems in group theory. One example is the famous Schreier Conjecture which states that the outer automorphism group of every finite simple group is solvable. This result turns out to be important for classifying finite primitive permutation groups.

In 1979 (just before the classification of the finite simple groups was first announced to be finished), O'Nan and Scott independently presented a classification of the maximal subgroups of the full symmetric group on n letters at the Santa Cruz conference on finite groups (see [22]). We will see that, in general, certain maximal subgroups and primitive permutation groups are closely related, and so this result led to a characterization of all finite primitive permutation groups. Because of the form in which the original theorem was presented, one case was omitted in the transfer to primitive groups, as pointed out by Aschbacher. Interestingly, it is the proof of this case that requires the Schreier Conjecture. This second and complete form of the theorem is referred to as the O'Nan-Scott Theorem, and it basically states that any finite primitive permutation group must be in one of five isomorphism classes. Four out of these five classes are well understood; for example, one of the classes consists of certain subgroups of the affine group, a group in which every element is a product of a translation and a linear bijection on a finite dimensional vector space. Thus this theorem is a useful tool for permutation group theorists (see [8, p. 137] for examples of how it is used).

The heart of the proof of the O'Nan-Scott Theorem lies with the actions of the socle of a primitive permutation group, which, in the case of a finite primitive permutation group, consists of a direct product of isomorphic simple groups. One natural question to ask, then, is if there are other group theoretic problems, not necessarily even permutation

group problems, that can be reduced to a case where the socle of the group has a structure similar to that of a finite primitive permutation group, and moreover, if the methods of the proof of the O'Nan-Scott Theorem can be applied to this case of the problem. One such example is an open problem dating back to the 1960s which essentially asks whether every finite lattice can be embedded as an interval into the subgroup lattice of a finite group; I will refer to this problem as *finite representability*.

This thesis is a synthesis of material relating to and including a proof of the O'Nan-Scott Theorem, as well as a description of the evolution of the problem of finite representability as it pertains to one specific lattice. My intent is to be as self-contained and detailed as possible. Of course, no proof of the classification of the finite simple groups is given! Indeed, only a brief description of the finite simple groups and an idea of how the Schreier Conjecture is proved is provided. Besides these and a few other results whose proofs are too far off topic, I give full proofs both of elementary and advanced results. My hope is that anyone with a first course in group theory will be able to understand the bulk of the material presented.

There seems to be little literature on the subject of the O'Nan-Scott Theorem, which should not be that surprising, considering how new it is. In [14], Liebeck, Praeger and Saxl give an outline of the five isomorphism classes and a complete, although dense, proof of the O'Nan-Scott Theorem. I found it to be the most straightforward presentation of the subject; as such, it served as my primary reference for the theorem. More details are given by Dixon and Mortimer in [8], though their descriptions of the isomorphism classes approach from a different angle than that of [14]; this book was very helpful for filling in gaps. In my descriptions of the isomorphism classes and in my proof of O'Nan-Scott, I am essentially following [14], providing proofs and details where they are missing; for example, I supply proofs to all of the properties of the isomorphism classes listed in [14] (with the exception of two claims which are not required for the proof of O'Nan-Scott). To get a better sense of how the proof of the O'Nan-Scott Theorem functions, I have reorganized and broken down the proof of [14] into several lemmas and propositions; two of the lemmas also form one of the main links to the problem of finite representability.

As for the problem of finite representability, I have included full proofs of the two results which describe the socle, filling in the details. In doing this, I also generalize one of these theorems (3.3.2), though it is certainly not a complicated generalization. Lastly, I give a proof of one of Lucchini's reductions to show how he uses the methods of the O'Nan-Scott Theorem proof. His proof is already quite detailed, but I have changed it somewhat to provide as much detail as possible while still preserving its length.

1 Preliminaries

In this section, I review and give notation for some standard concepts from group theory which will be used throughout this thesis. Note that function composition will be from left to right. Both [19] and [20] served as general references for this section. When definitions, results or proofs come from specific sources, those sources are mentioned.

1.1 Centralizers and Normalizers

Let G be a group, and let g and h be elements of G. The *commutator* of g and h is $[g,h] := g^{-1}h^{-1}gh$. If $[g,h] = 1$ then g and h *commute*. The *centralizer* of h in G is $C_G(h) := \{g \in G : gh = hg\}$; that is, the set of all elements of G that commute with h. If $H \leq G$, then the *centralizer* of H in G is $C_G(H) := \{g \in G : gh = hg \text{ for all } h \in H\}$. Both $C_G(h)$ and $C_G(H)$ are subgroups of G. Moreover, if $H \trianglelefteq G$, then $C_G(H) \trianglelefteq G$ since if $g \in G$ and $a \in C_G(H)$, then for all $h \in H$, $ghg^{-1} \in H$, and thus

$$(g^{-1}ag)^{-1}h(g^{-1}ag) = g^{-1}a^{-1}(ghg^{-1})ag = g^{-1}(ghg^{-1})g = h.$$

Let H and K be subgroups of G. If $K \leq C_G(H)$, we say that K *centralizes* H. Define $[H,K] := \langle\{[h,k] : h \in H, k \in K\}\rangle$. Then H and K centralize each other if and only if $[H,K] = \{1\}$.

Let H and G be groups. The *normalizer* of H in G is

$$N_G(H) := \{g \in G : g^{-1}Hg = H\}.$$

Then $N_G(H)$ is a subgroup of G, and if $H \leq G$, then H is clearly a normal subgroup of $N_G(H)$. In fact, $N_G(H)$ is the largest subgroup of G in which H is normal. H is said to *normalize* $K \leq G$ if $H \leq N_G(K)$, and H is said to be *self-normalizing* in G if $N_G(H) = H$. Lastly, note that $C_G(H) \trianglelefteq N_G(H)$ for all $H \leq G$.

The *center* of a group G, denoted by $Z(G)$, is of course the set of all elements of G that commute with every element of G. $Z(G)$ is clearly a normal subgroup of G. G is abelian if and only if $G = Z(G)$, and so the center of a simple nonabelian group must be trivial. Note also that if $H \leq G$, then $Z(H) = C_G(H) \cap H$.

The group of all isomorphisms of a group G onto itself is called the *automorphism group* of G, and is denoted by $Aut(G)$. Let $\varphi_h : G \to G$ be defined by $g\varphi_h = h^{-1}gh$. Then $\varphi_h \in Aut(G)$ and is called an *inner automorphism* of G. The *inner automorphism group* of G, denoted by $Inn(G)$, is the normal subgroup of $Aut(G)$ consisting of all inner automorphisms of G. Note that $\varphi : G \to Inn(G)$ defined by $g \mapsto \varphi_g$ is an onto homomorphism with kernel $Z(G)$. Hence, $G/Z(G) \simeq Inn(G)$; in particular, if T is simple and nonabelian, then $T \simeq Inn(T)$.

Proposition 1.1.1. *Let T be a nonabelian simple group. If $Inn(T) \leq G \leq Aut(T)$, then $C_G(Inn(T))$ is trivial.*

Proof. Let $\sigma \in C_G(Inn(T))$. Then $\sigma^{-1}\varphi_t\sigma = \varphi_t$ for all $t \in T$. So for every $x \in T$,

$$t^{-1}xt = x\varphi_t = x\sigma^{-1}\varphi_t\sigma = (t^{-1}(x\sigma^{-1})t)\sigma = (t\sigma)^{-1}x(t\sigma).$$

Thus $(t\sigma)t^{-1} \in Z(T) = \{1\}$ since T is nonabelian and simple, so $t\sigma = t$ for all $t \in T$. Thus σ is the identity and $C_G(Inn(T))$ is trivial. □

I conclude this section with some useful technical results. The first lemma will be used without reference throughout this thesis.

Lemma 1.1.2. *Let G be a group with subgroups H, K and L, where L normalizes K. Then $H \cap (KL) = (H \cap K)L$ if and only if $L \leq H$.*

Proof. If $H \cap KL = (H \cap K)L$, then $L \leq (H \cap K)L = H \cap (KL) \leq H$, as desired. On the other hand, suppose that $L \leq H$. Since L normalizes K, $H \cap KL$ and $(H \cap K)L$ are subgroups of G. Clearly $(H \cap K)L \leq H \cap KL$ since $L \leq H$. For the reverse inclusion, let $h = kl \in H \cap KL$. Then $hl^{-1} = k \in H \cap K$ since $L \leq H$. Thus $h = (hl^{-1})l \in (H \cap K)L$ and $H \cap (KL) \leq (H \cap K)L$. □

Lemma 1.1.3. *Let $G_1 \times G_2 \times \cdots \times G_k$ be a subgroup of a group G.*

(i) $\bigcap_{i=1}^{k}(C_G(G_i)G_i) = (\bigcap_{i=1}^{k} C_G(G_i))G_1 \cdots G_k$.

(ii) $\bigcap_{i=1}^{k} C_G(G_i) = C_G(G_1 \times G_2 \times \cdots \times G_k)$.

Proof. (i) Note that for each i, $G_i \leq C_G(G_j)$ for all $j \neq i$. Moreover, G_i and $C_G(G_i)$ normalize each other for all i as they are both normal subgroups of $N_G(G_i)$ for all i; it follows that $\bigcap_{i=1}^{l} C_G(G_i) \trianglelefteq \bigcap_{i=1}^{l} N_G(G_i)$ for all $l \in \{1, \ldots, k\}$. But $G_i \trianglelefteq G_1 \cdots G_l$ for all $i, l \in \{1, \ldots, k\}$ such that $i \leq l$, so $G_1 \cdots G_l \leq \bigcap_{i=1}^{l} N_G(G_i)$ for all $l \in \{1, \ldots, k\}$, and thus $(\bigcap_{i=1}^{l} C_G(G_i))G_1 \cdots G_l \leq G$ for all $l \in \{1, \ldots, k\}$.

The proof is by induction on $k \geq 1$. If $k = 1$ the result is trivial. Suppose that it is true for $k-1$ for some $k > 1$. Then

$$\begin{aligned}
& \textstyle\bigcap_{i=1}^{k}(C_G(G_i)G_i) \\
= \; & (\textstyle\bigcap_{i=1}^{k-1} C_G(G_i)G_i) \cap G_k C_G(G_k) \\
= \; & [(\textstyle\bigcap_{i=1}^{k-1} C_G(G_i))G_1 \cdots G_{k-1}] \cap G_k C_G(G_k) \qquad \text{(IH)} \\
= \; & (C_G(G_k) \cap [(\textstyle\bigcap_{i=1}^{k-1} C_G(G_i))G_1 \cdots G_{k-1}])G_k \quad (G_k \leq \textstyle\bigcap_{i=1}^{k-1} C_G(G_i)) \\
= \; & [C_G(G_k) \cap (\textstyle\bigcap_{i=1}^{k-1} C_G(G_i))](G_1 \cdots G_{k-1})G_k \quad (G_1 \cdots G_{k-1} \leq C_G(G_k)) \\
= \; & (\textstyle\bigcap_{i=1}^{k} C_G(G_i))G_1 \cdots G_k.
\end{aligned}$$

(ii) If $g \in G$ commutes with every element of G_i for all i, then g commutes with every element of $G_1 \times \cdots \times G_k$, so $\bigcap_{i=1}^{k} C_G(G_i) \leq C_G(G_1 \times G_2 \times \cdots \times G_k)$. But $G_i \leq G_1 \times G_2 \times \cdots \times G_k$ implies that $C_G(G_1 \times G_2 \times \cdots \times G_k) \leq C_G(G_i)$ for all i. □

1.2 Group Actions

Let G be a group and Ω a nonempty set. Let S^Ω denote the symmetric group on Ω. An *action* of G on Ω is a homomorphism $\phi : G \to S^\Omega$, while Ω is said to be a *G-space* if there exists a function mapping from $\Omega \times G$ to Ω that satisfies $(\alpha^g)^h = \alpha^{gh}$ and $\alpha^1 = \alpha$ for all $\alpha \in \Omega$ and $g, h \in G$, where the image of (α, g) is denoted by α^g.

If ϕ is an action of G on Ω, then $\alpha^g := \alpha(g\phi)$ satisfies the two conditions of a G-space, so that Ω is a G-space. On the other hand, if Ω is a G-space and $g \in G$, let $\pi_g : \Omega \to \Omega$ be defined by $\alpha \mapsto \alpha^g$. Then $\pi_g \in S^\Omega$ for all $g \in G$, and it is easy to check that $\phi : g \mapsto \pi_g$ is then an action of G on Ω. Thus these two concepts of an action of a group on a set are equivalent.

Here are some basic definitions about group actions. Let Ω be a G-space, and let $\alpha, \beta \in \Omega$. Define a relation $\sim$ on Ω by $\alpha \sim \beta$ if there exists a $g \in G$ with $\alpha^g = \beta$. Then $\sim$ is an equivalence relation whose equivalence classes we call *orbits* of G. Let α be in an orbit of G. Then the orbit can be written as $\{\alpha^g : g \in G\} =: \theta_G(\alpha)$, which we call the *orbit of α*. G is said to be *transitive*, or Ω is said to be a transitive G-space, if there is only one orbit, namely, Ω. The *stabilizer* of α in G is

$$G_\alpha := \{g \in G : \alpha^g = \alpha\},$$

which is a subgroup of G. The *setwise stabilizer* of $\Gamma \subseteq \Omega$ in G is

$$G_\Gamma := \{g \in G : \Gamma^g = \Gamma\},$$

which is also a subgroup of G, and of course when $\Gamma = \{\alpha\}$, $G_\Gamma = G_\alpha$. G is said to be *semiregular* if $G_\alpha = \{1\}$ for all $\alpha \in \Omega$, and G is said to be *regular* if it is both transitive and semiregular.

G is a *permutation group* on Ω if it is a subgroup of S^Ω. The image of an action ϕ is called the *permutation group* induced on Ω by G, denoted by G^Ω. An action is *faithful* if $ker(\phi) = \{1\}$, or, equivalently, Ω is a faithful G-space if whenever $\alpha^g = \alpha^h$ for all $\alpha \in \Omega$, we have that $g = h$. In this case, G acts as a permutation group on Ω as $G \simeq G\phi \leq S^\Omega$. In light of the fact that we have two equivalent definitions of an action, the action of $g \in S^\Omega$ will either be written on the right as αg or in the form α^g, depending on the context. Note that if $G \leq S^\Omega$ is transitive, then clearly every subgroup of S^Ω containing G is also transitive. Similarly, if $G \leq S^\Omega$ is semiregular, then every subgroup of G is semiregular.

Next is a quick proposition about centralizers in permutation groups which illustrates some of the above concepts and is also fundamental to the proof of the O'Nan-Scott Theorem.

Proposition 1.2.1 ([25, p. 155])**.** *Let G be a permutation group on Ω.*

(i) If $C_{S^\Omega}(G)$ is transitive on Ω, then G is semiregular.

(ii) If G is transitive on Ω, then $C_{S^\Omega}(G)$ is semiregular.

Proof. (i) Let $\alpha \in \Omega$ and $g \in G_\alpha$. Since $C_{S^\Omega}(G)$ is transitive on Ω, for each $\beta \in \Omega$ there exists an $h \in C_{S^\Omega}(G)$ such that $\beta = \alpha^h$. Then

$$\beta^g = \alpha^{hg} = \alpha^{gh} = (\alpha^g)^h = \alpha^h = \beta.$$

Thus $g = 1$ and so $G_\alpha = \{1\}$.

(ii) Clearly $G \leq C_{S^\Omega}(C_{S^\Omega}(G))$, which implies that $C_{S^\Omega}(C_{S^\Omega}(G))$ is transitive as G is. Then by part (i), $C_{S^\Omega}(G)$ is semiregular. □

Now we look at some particular G-spaces. Define an action of G on G by right multiplication; that is, $x^g = xg$ for all $g, x \in G$. This is called the *right regular representation* of G. The *left regular representation* of G is given by the action $x^g = g^{-1}x$ of G on itself. Both actions are regular. G also acts on itself by conjugation; that is, $x^g := g^{-1}xg$ for all $g, x \in G$. This action is very important and is used often. It is routine to verify that these three definitions do give rise to legitimate actions.

Let $H \leq G$. The *right coset space* of H in G, denoted by $G\backslash H$, is simply the set of right cosets of H in G. The backslash is used to avoid confusion with the quotient G/H. It is routine to verify that $G\backslash H$ is a transitive G-space with action $(Ha)^g := Hag$ for all $Ha \in G\backslash H$ and $g \in G$. Moreover, $G_{Hg} = g^{-1}Hg$ for all $g \in G$ since $h \in G_{Hg} \iff Hgh = Hg \iff ghg^{-1} \in H \iff h \in g^{-1}Hg$. In particular, $G_H = H$. It is not hard to see that the kernel of this action is $\bigcap_{g\in G} g^{-1}Hg$, which is called the *core* of H in G. Note that the core of H in G is a normal subgroup of G contained in H. If the core of H is trivial, then H is said to be *core-free*. Hence, the action of G on the coset space $G\backslash H$ is faithful if and only if H is a core-free subgroup of G. In order to show that H is core-free, we typically show that any normal subgroup of G contained in H must be trivial. The *left coset space* of H in G is defined analogously.

The following proposition is a collection of basic well-known results about G-spaces which are very useful and which will be used repeatedly and freely without reference. First, we need one more definition: two G-spaces Ω and Γ are *isomorphic* if there exists a bijection $\varphi : \Omega \to \Gamma$ such that $(\alpha^g)\varphi = (\alpha\varphi)^g$ for all $\alpha \in \Omega$ and $g \in G$. Note that $G_\alpha = G_{\alpha\varphi}$ for all $\alpha \in \Omega$ since $g \in G_\alpha \iff \alpha^g = \alpha \iff \alpha^g\varphi = \alpha\varphi \iff (\alpha\varphi)^g = \alpha\varphi \iff g \in G_{\alpha\varphi}$.

Proposition 1.2.2. *Let Ω be a G-space. Let $\alpha \in \Omega$ and $g \in G$ be arbitrary.*

(i) $G_{\alpha^g} = g^{-1}G_\alpha g$.

(ii) If Ω contains at least two elements, then G_α is not transitive on Ω.

(iii) The coset space $G\backslash G_\alpha$ is isomorphic to the orbit $\theta_G(\alpha)$. It follows that G_α is a proper subgroup of G so long as $\theta_G(\alpha)$ contains an element different from α.

(iv) If G is transitive on Ω, then $G\backslash G_\alpha \simeq \Omega$, and if G is regular on Ω, then $G \simeq \Omega$, where G acts on itself by right multiplication.

(v) If G is finite, then $[G : G_\alpha] = |\theta_G(\alpha)|$; if G is finite and transitive on Ω, then $[G : G_\alpha] = |\Omega|$; and if G is finite and regular on Ω, then $|G| = |\Omega|$.

Proof. (i) $h \in G_{\alpha^g} \iff \alpha^{gh} = \alpha^g \iff \alpha^{ghg^{-1}} = (\alpha^{gh})^{g^{-1}} = (\alpha^g)^{g^{-1}} = \alpha \iff ghg^{-1} \in G_\alpha \iff h \in g^{-1}G_\alpha g$.

(ii) Suppose that G_α is transitive on Ω. Let $\beta \in \Omega$. Then there exists a $g \in G_\alpha$ with $\beta = \alpha^g$ as G_α is transitive on Ω. But $\alpha^g = \alpha$ so $\beta = \alpha$. Thus $\Omega = \{a\}$.

(iii) Define $\varphi : G\backslash G_\alpha \to \theta_G(\alpha)$ by $G_\alpha g \mapsto \alpha^g$. Then $G_\alpha g = G_\alpha h \iff gh^{-1} \in G_\alpha \iff \alpha^{gh^{-1}} = \alpha \iff \alpha^g = \alpha^h$. Thus φ is well-defined and 1-1. φ is clearly onto and $(G_\alpha g)^h\varphi = (G_\alpha gh)\varphi = \alpha^{gh} = (\alpha^g)^h = ((G_\alpha g)\varphi)^h$, so φ is a G-space isomorphism.

(iv) Since G is transitive, $\theta_G(\alpha) = \Omega$, so $G\backslash G_\alpha \simeq \Omega$ by (iii). If G is also semiregular, then $G\backslash\{1\} \simeq \Omega$, and it is easy to verify that the obvious map from G to $G\backslash\{1\}$ is a G-space isomorphism if G acts on itself by right multiplication. Hence, $G \simeq \Omega$.

(v) Each follows immediately from (iii) and (iv). □

Now for the final definition of this section. We say that $G \leq S^\Omega$ is *permutation isomorphic* to $H \leq S^\Gamma$ if there is a bijection $\varphi : \Omega \to \Gamma$ and an isomorphism $\psi : G \to H$ such that $(\alpha g)\varphi = (\alpha\varphi)(g\psi)$ for all $\alpha \in \Omega$ and $g \in G$. In other words, G and H only differ in the labelling of their elements. Often, we simply say that ψ is a permutation isomorphism of G onto H. I conclude this section with several results about permutation isomorphisms. The first result gives us a sufficient condition for permutation isomorphism when the actions are transitive that is very useful in practice.

Proposition 1.2.3. *Suppose that $G \leq S^\Omega$ and $H \leq S^\Gamma$ where both actions are transitive. If there is an isomorphism $\psi : G \to H$ such that $G_\alpha\psi = H_\gamma$ for some $\alpha \in \Omega$ and $\gamma \in \Gamma$, then G is permutation isomorphic to H.*

Proof. Since G acts transitively on Ω, every element of Ω has the form αg for some $g \in G$. Define $\varphi : \Omega \to \Gamma$ by $\alpha g \mapsto \gamma(g\psi)$. Then since $G_\alpha\psi = H_\gamma$,

$$\alpha g = \alpha g' \iff g'g^{-1} \in G_\alpha \iff (g'g^{-1})\psi \in H_\gamma \iff \gamma(g\psi) = \gamma(g'\psi),$$

so φ is well-defined and 1-1. Since H acts transitively on Γ, a typical element of Γ has the form γh for some $h \in H$, and $(\alpha h\psi^{-1})\varphi = \gamma(h\psi^{-1})\psi = \gamma h$. Thus φ is onto. Lastly, let $g, g' \in G$. Then

$$((\alpha g')g)\varphi = (\alpha g'g)\varphi = \gamma(g'g\psi) = (\gamma g'\psi)g\psi = (\alpha g'\varphi)(g\psi).$$

Thus G is permutation isomorphic to H. □

The following is an exercise in [8, p. 18].

Proposition 1.2.4. *If G and H are both permutation groups on Ω, then G and H are permutation isomorphic if and only if G and H are conjugate in S^Ω.*

Proof. Suppose that G and H are permutation isomorphic. Then there exists a bijection $\varphi : \Omega \to \Omega$ and an isomorphism $\psi : G \to H$ with $(\alpha g)\varphi = (\alpha\varphi)(g\psi)$ for all $\alpha \in \Omega$ and $g \in G$. Then $\alpha g = ((\alpha\varphi)(g\psi))\varphi^{-1} = \alpha(\varphi(g\psi)\varphi^{-1})$ for all $\alpha \in \Omega$ and $g \in G$, which implies that $g = \varphi(g\psi)\varphi^{-1}$ for all $g \in G$. Thus $G = \varphi(G\psi)\varphi^{-1} = \varphi H\varphi^{-1}$, and we are done since $\varphi \in S^\Omega$.

On the other hand, suppose that $G = \varphi H\varphi^{-1}$ for some $\varphi \in S^\Omega$. Define $\psi : G \to H$ by $g\psi = \varphi^{-1}g\varphi$; it is routine to verify that ψ is an isomorphism. Then for all $g \in G$ and $\alpha \in \Omega$, $\alpha g = \alpha(\varphi(\varphi^{-1}g\varphi)\varphi^{-1}) = \alpha(\varphi(g\psi)\varphi^{-1})$, so $(\alpha g)\varphi = (\alpha\varphi)(g\psi)$ and G is permutation isomorphic to H. □

This next result is fairly intuitive but is proved here for the sake of being thorough.

Proposition 1.2.5. *Suppose that θ is a permutation isomorphism from G onto H where $G \leq S^\Omega$ and $H \leq S^\Gamma$. Then there exists a permutation isomorphism $\psi : S^\Omega \to S^\Gamma$ such that $\psi|_G = \theta$. In particular, $N_{S^\Omega}(G)\psi = N_{S^\Gamma}(H)$.*

Proof. Let $\varphi : \Omega \to \Gamma$ be the bijection for which $(\alpha g)\varphi = (\alpha\varphi)(g\theta)$ for all $\alpha \in \Omega$ and $g \in G$. Let $\pi \in S^\Omega$ and $\gamma \in \Gamma$. Then $\gamma = \alpha\varphi$ for some unique $\alpha \in \Omega$. Define $\psi_\pi : \Gamma \to \Gamma$ by $\gamma \mapsto (\alpha\pi)\varphi$. Suppose that $\gamma\psi_\pi = \gamma'\psi_\pi$ where $\gamma = \alpha\varphi$ and $\gamma' = \alpha'\varphi$. Then $(\alpha\pi)\varphi = (\alpha'\pi)\varphi$ which implies that $\alpha = \alpha'$ since $\pi\varphi$ is 1-1. Thus $\gamma = \gamma'$ so ψ_π is 1-1. Let $\gamma \in \Gamma$, and define $\gamma' := \gamma\varphi^{-1}\pi^{-1}\varphi \in \Gamma$. Then $\gamma'\psi_\pi = ((\gamma\varphi^{-1}\pi^{-1})\pi)\varphi = \gamma$, so ψ_π is onto. Thus $\psi_\pi \in S^\Gamma$ for all $\pi \in S^\Omega$, so we may define $\psi : S^\Omega \to S^\Gamma$ by $\pi \mapsto \psi_\pi$. Let $\pi, \pi' \in S^\Omega$. Then $\gamma\psi_\pi\psi_{\pi'} = (\alpha\pi)\varphi\psi_{\pi'} = ((\alpha\pi)\pi')\varphi = \gamma\psi_{\pi\pi'}$ for all $\gamma \in \Gamma$, so $\psi_\pi\psi_{\pi'} = \psi_{\pi\pi'}$ for all $\pi, \pi' \in S^\Omega$. Thus ψ is a homomorphism. If ψ_π is the identity, then $\alpha\varphi = (\alpha\pi)\varphi$ for all $\alpha \in \Omega$, so $\alpha = \alpha\pi$ for all $\alpha \in \Omega$. Thus ψ is 1-1. Let $\pi \in S^\Gamma$. Define $\pi' := \varphi\pi\varphi^{-1} \in S^\Omega$. Then $\gamma\psi_{\pi'} = (\alpha\varphi\pi\varphi^{-1})\varphi = \gamma\pi$ for all $\gamma \in \Gamma$, so ψ is onto. Then ψ is a permutation isomorphism since $(\alpha\pi)\varphi = (\alpha\varphi)\psi_\pi = (\alpha\varphi)(\pi\psi)$ for all $\alpha \in \Omega$ and $\pi \in S^\Omega$.

Let $g \in G$. Then

$$\gamma(g\psi) = \gamma\psi_g = (\alpha g)\varphi = (\alpha\varphi)(g\theta) = \gamma(g\theta)$$

for all $\gamma \in \Gamma$, so $g\psi = g\theta$ for all $g \in G$. Thus $\psi|_G = \theta$.

Let $n \in N_{S^\Omega}(G)$ and $h \in H$. Then there exists a $g \in G$ with $g\theta = h$, so $(\psi_n)^{-1}h\psi_n = \psi_{n^{-1}}\psi_g\psi_n = \psi_{n^{-1}gn} \in G\psi = H$, so $\psi_n \in N_{S^\Gamma}(H)$. Conversely, let $n \in N_{S^\Gamma}(H)$ and $g \in G$. Then $n = \psi_{n'}$ for some $n' \in S^\Omega$, and again, $\psi_{n'^{-1}gn'} = n^{-1}\psi_g n \in H = G\psi$, so $n'^{-1}gn' \in G$, which implies that $n' \in N_{S^\Omega}(G)$. Thus $N_{S^\Omega}(G)\psi = N_{S^\Gamma}(H)$, as desired. □

This next and last proposition is referred to in [14] but is not proved. It, like Proposition 1.2.1, is fundamental to the proof of the O'Nan-Scott Theorem.

Proposition 1.2.6. *If G is a regular permutation group on Ω, then G is permutation isomorphic to $C_{S^\Omega}(G)$.*

Proof. Let $g \in G$. Define $\rho_g : G \to G$ by $x \mapsto xg$ and $\lambda_g : G \to G$ by $x \mapsto g^{-1}x$. Then $\rho_g, \lambda_g \in S^G$ for all $g \in G$. Let $R := \{\rho_g : g \in G\}$ and $L := \{\lambda_g : g \in G\}$. Note that R and L are both subgroups of S^G; in fact, R is the image of the right regular representation of G, and L is the image of the left regular representation of G. I claim first of all that $L = C_{S^G}(R)$. Let $\lambda_g \in L$, $\rho_h \in R$ and $x \in G$. Then

$$x\lambda_g\rho_h = (g^{-1}x)\rho_h = (g^{-1}x)h = g^{-1}(xh) = g^{-1}(x\rho_h) = x\rho_h\lambda_g,$$

so λ_g commutes with every element of R. Thus $L \leq C_{S^G}(R)$. Conversely, let $\pi \in C_{S^G}(R)$. Then $\pi\rho_g = \rho_g\pi$ for all $g \in G$, so $(x\pi)g = (xg)\pi$ for all $x, g \in G$. In particular, take $g = x^{-1}$, so that for all $x \in G$, $(x\pi)x^{-1} = (xx^{-1})\pi = 1\pi$. But then

$$x\lambda_{(1\pi)^{-1}} = (1\pi)x = ((x\pi)x^{-1})x = x\pi$$

for all $x \in G$, so $\pi = \lambda_{(1\pi)^{-1}} \in L$. Thus $L = C_{S^G}(R)$.

Let $\alpha \in \Omega$. G is transitive and semiregular on Ω by assumption, so $\varphi : \Omega \to G$ defined by $\alpha g \mapsto g$ is a well-defined bijection. Define $\psi : S^\Omega \to S^G$ by $\pi \mapsto \varphi^{-1}\pi\varphi$. It is routine to verify that ψ is a permutation isomorphism of S^Ω onto S^G. Further,

$$x(g\psi) = x(\varphi^{-1}g\varphi) = (\alpha xg)\varphi = xg = x\rho_g$$

for all $x, g \in G$, so $g\psi = \rho_g$ for all $g \in G$. Then $G\psi = R$, and it follows that $C_{S^\Omega}(G)\psi = C_{S^G}(R) = L$. Thus $C_{S^\Omega}(G)$ is permutation isomorphic to L. Moreover, note that if $\varphi : \Omega \to G$ were instead defined by $\alpha g \mapsto g^{-1}$, then the proof we just saw would carry through, but we would get that G is permutation isomorphic to L in place of R since we would have that

$$x(g\psi) = x(\varphi^{-1}g\varphi) = (\alpha x^{-1}g)\varphi = g^{-1}x = x\lambda_g.$$

Thus G is permutation isomorphic to $C_{S^\Omega}(G)$. □

1.3 Sylow Subgroups

Let p be a prime. A finite group G is a *p-group* if the order of G is a power of p.

Proposition 1.3.1 ([20, p. 75])**.** *If G is a nontrivial p-group, then $Z(G)$ is not trivial.*

Proof. Let G act on itself by conjugation. Let $h \in G$. Then $G_h = \{g \in G : g^{-1}hg = h\} = C_G(h)$. Since we then have that $G\backslash C_G(h) \simeq \theta_G(h)$, $h \in Z(G)$ if and only if $\theta_G(h) = \{h\}$. Then $Z(G)$ is the union of the orbits of G containing only one element. Since the orbits of G partition G, if $\{\theta_G(h_i)\}_{i\in I}$ is a disjoint collection of all orbits of G containing at least two elements, then $|G| = |Z(G)| + \sum_{i\in I} |\theta_G(h_i)|$. If $G = Z(G)$, then since G is nontrivial, $Z(G)$ is nontrivial, so we may assume that $Z(G) < G$. Then I is not empty. $[G : C_G(h_i)] = |\theta_G(h_i)| > 1$ and G is a p-group, so $p \mid |\theta_G(h_i)|$ for all $i \in I$. Thus $p \mid |Z(G)|$ so $Z(G)$ is not trivial. □

The equation $|G| = |Z(G)| + \sum_{i\in I}[G : C_G(h_i)]$, where $\{\theta_G(h_i)\}_{i\in I}$ is a disjoint collection of all orbits of G containing at least two elements, is called the *class equation* of G.

Proposition 1.3.2. *If G has order p^2 where p is a prime, then G is abelian.*

Proof. By Proposition 1.3.1, $Z(G)$ is not trivial, so $Z(G)$ has order p or p^2. Assume for a contradiction that $Z(G)$ has order p. Then $G/Z(G)$ also has order p, so is cyclic. Let $Z(G)a$ be a generator, and let $g, h \in G$. Then $g = xa^m$ and $h = ya^n$ for some positive integers m and n and for some $x, y \in Z(G)$. Then $gh = xa^m ya^n = ya^n xa^m = hg$ since $x, y \in Z(G)$, so G is abelian, a contradiction. Thus $Z(G)$ has order p^2, so $Z(G) = G$ and G is abelian. □

Theorem 1.3.3 (Cauchy, [20, p. 74])**.** *If G is a finite group and p is a prime where p divides the order of G, then G contains an element of order p.*

Proof. First suppose that G is abelian. Write $|G| = pn$, where $n \geq 1$. The proof is by induction on n. If $|G| = p$, then G is cyclic and so contains an element of order p. Suppose that the result is true for some $n > 1$. Let $g \in G$ with order $m > 1$. If $p \mid m$, then $g^{m/p}$ has order p, and we are done. So we may assume that $p \nmid m$. Note that $G/\langle g\rangle$ is an abelian group of order $\frac{pn}{m}$. Since $p \nmid m$ and $\frac{pn}{m}$ is an integer, $\frac{n}{m}$ must be an integer. But $\frac{n}{m} < n$ as $m > 1$, so by induction, $G/\langle g\rangle$ contains an element of order p, say $\langle g\rangle h$. Then if h has order k, $(\langle g\rangle h)^k = \langle g\rangle$ so $p \mid k$. Again, G contains an element of order p, and we are done.

Suppose that now that G is any finite group with $p \mid |G|$. The proof is by induction on $|G|$. If $p \mid |Z(G)|$, then since $Z(G)$ is abelian, $Z(G)$ contains an element of order p, and we are done. Thus we may assume that $p \nmid |Z(G)|$. Then by the class equation, there exists a $g \in G$ for which $[G : C_G(g)] > 1$ and $p \nmid [G : C_G(g)]$. Since $p \mid |G|$, $p \mid |C_G(g)|$. But $C_G(g) < G$, so by induction, $C_G(g)$ contains an element of order p, and we are done. □

Suppose that G is a finite group such that $|G| = p^k m$ where p is a prime and $p \nmid m$. A *Sylow p-subgroup* of G is a maximal p-subgroup of G. Since G must contain an element of order p by Cauchy's Theorem, every finite group has a Sylow p-subgroup. Clearly, if $P \leq G$ and $|P| = p^k$, then P is a Sylow p-subgroup of G.

Lemma 1.3.4 ([20, p. 78]). *Let P be a Sylow p-subgroup of a finite group G. Then $N_G(P)/P$ contains no element of order p.*

Proof. Suppose that $N_G(P)/P$ does have an element of order p, say Pg. $P\langle g\rangle$ is a subgroup of G since g normalizes P. Moreover, $P < P\langle g\rangle$ since if $g \in P$, then Pg has order 1, a contradiction. Since $g^p \in P$, the order of g is a power of p. Then $|P\langle g\rangle| = \frac{|P||\langle g\rangle|}{|P\cap\langle g\rangle|}$ is a power of p, but this is a contradiction because P is a maximal p-subgroup of G. □

Theorem 1.3.5 (Sylow, [20, p. 79]). *Suppose that G is a finite group such that $|G| = p^k m$ where p is a prime and $p \nmid m$. Then every Sylow p-subgroup has order p^k, and any two Sylow p-subgroups are conjugate in G. Further, if n_p is the number of Sylow p-subgroups of G, then $n_p \equiv 1 (mod\ p)$ and $n_p \mid |G|$.*

Proof. Let P be a Sylow p-subgroup of G. Let $\Omega := \{g^{-1}Pg : g \in G\}$. Note that every member of Ω is a Sylow p-subgroup of G since $g^{-1}Pg$ must also be a maximal p-group. Let $Q, R \in \Omega$. Then Q acts on Ω by conjugation, and $|\theta_Q(R)| = [Q : Q_R]$. But Q is a p-group, so $|\theta_Q(R)| = 1$ or $p \mid |\theta_Q(R)|$. If $|\theta_Q(R)| = 1$, then $q^{-1}Rq = R$ for all $q \in Q$, so $Q \leq N_G(R)$. Then $RQ \leq G$ and $|RQ| = \frac{|R||Q|}{|R\cap Q|}$, which is a power of p, so we must have that $R = RQ = Q$ as R and Q are both maximal p-subgroups of G. Take $Q = P$. If $R \neq P$, then $p \mid |\theta_P(R)|$ by the above, and clearly $\theta_P(P) = \{P\}$, so $\theta_P(P)$ is the only orbit of P containing exactly one element. Thus $|\Omega| \equiv 1 (mod\ p)$.

Suppose that there exists a Sylow p-subgroup S which is not in Ω. Again, S acts on Ω by conjugation, and if $R \in \Omega$, then $p \mid |\theta_S(R)|$ since $R \neq S$. But then $p \mid |\Omega|$, contradicting $|\Omega| \equiv 1 (mod\ p)$. Thus Ω is the set of all Sylow p-subgroups of G. It follows that every Sylow p-subgroup is conjugate in G and that $n_p \equiv 1 (mod\ p)$.

Since $G_P = \{g \in G : g^{-1}Pg = P\} = N_G(P)$, $n_p = |\Omega| = |\theta_G(P)| = [G : N_G(P)]$. Thus $n_p \mid |G|$. Moreover, $|G| = |P|[N_G(P) : P][G : N_G(P)]$, but $p \nmid [N_G(P) : P]$ (by Lemma 1.3.4 and Cauchy's Theorem) and $p \nmid n_p = [G : N_G(P)]$, so $p^k \mid |P|$ as $p^k \mid |G|$. But $|P|$ is at most p^k, so $|P| = p^k$. It follows that every Sylow p-subgroup has order p^k, and we are done. □

Proposition 1.3.6. *Let P be a Sylow p-subgroup of a group G. Then $N_G(P)$ is self-normalizing in G.*

Proof. Of course $N_G(P) \leq N_G(N_G(P))$. Let $g \in N_G(N_G(P))$. P is a Sylow p-subgroup of $N_G(P)$, so $g^{-1}Pg$ is a Sylow p-subgroup of $g^{-1}N_G(P)g = N_G(P)$. Then there exists an $h \in N_G(P)$ with $P = h^{-1}(g^{-1}Pg)h$, so $P = hPh^{-1} = g^{-1}Pg$. Thus $g \in N_G(P)$ and $N_G(P) = N_G(N_G(P))$. □

1.4 Subdirect Products

The following definitions can be found in [3]. Let $G := G_1 \times G_2 \times \cdots \times G_k$ be a direct product of groups G_i. Let $\rho_i : G \to G_i$ be the projection map for each i. A group H is a *subdirect product* of G if there exists an embedding $\phi : H \to G$ such that $\phi\rho_i : H \to G_i$ is an onto homomorphism for all i. If H is actually a subgroup of G, then of course we may take ϕ to be the inclusion map, and we call the subdirect product H a *subdirect subgroup* of G. If H is a subgroup of G and $\rho_i|_H$ is 1-1 for all i, then H is called a *diagonal subgroup* of G (where H is not necessarily subdirect). Lastly, if H is a subgroup of G, then H is a *full diagonal subgroup* of G if it is both a subdirect subgroup and a diagonal subgroup.

If $h := (h_1, h_2, \ldots, h_k)$ is any element of a subgroup H of G, then

$$h = (h_1, h_2, \ldots, h_k) = (h\rho_1, h\rho_2, \ldots, h\rho_k).$$

Thus $H = \{(h\rho_1, \ldots, h\rho_k) : h \in H\}$. If H is a full diagonal subgroup of G, note that $\rho_i|_H$ is then an isomorphism of H onto G_i for each i. Consequently, all of the G_i must themselves be isomorphic to one another.

For the next result, the proof of (i) is from [4], and the proofs of (ii) and (iii) are from [3].

Lemma 1.4.1. *Let $G = T_1 \times T_2 \times \cdots \times T_k$ be a direct product of simple nonabelian groups ($k \geq 1$). Let H be a subgroup of G and $I := \{1, \ldots, k\}$.*

(i) If H is a full diagonal subgroup of G, then H is self-normalizing in G.

(ii) If H is a subdirect subgroup of G, then H is a direct product $\prod H_j$, where H_j is a full diagonal subgroup of some subproduct $\prod_{i \in I_j} T_i$ such that I is partitioned by the I_j.

(iii) If H is a nontrivial normal subgroup of G, then $H = \prod_{j \in J} T_j$ where J is some nonempty subset of I.

Proof. (i) Define $\gamma_i := (\rho_1|_H)^{-1}\rho_i$ for each $i \in I$. Then each γ_i is an isomorphism of T_1 onto T_i since H is a full diagonal subgroup of G. Note that γ_1 is the identity on T_1. Now, if $h \in H$ then $h\rho_1 = t$ for some $t \in T_1$, and $h\rho_i = (t(\rho_1|_H)^{-1})\rho_i = t\gamma_i$ for each $i \in \{2, \ldots, k\}$. On the other hand, if $t \in T_1$, then $t = h\rho_1$ for some $h \in H$, and $t\gamma_i = t(\rho_1|_H)^{-1}\rho_i = h\rho_i$ for each $i \in \{2, \ldots, k\}$. Thus

$$H = \{(h\rho_1, h\rho_2, \ldots, h\rho_k) : h \in H\} = \{(t, t\gamma_2, \ldots, t\gamma_k) : t \in T_1\}. \tag{1}$$

Let $n := (t_1, t_2, \ldots, t_k) \in N_G(H)$. Fix $i \in \{2, \ldots, k\}$ and let $x \in T_i$. Then $x = t\gamma_i$ for some $t \in T_1$ and $h := (t, t\gamma_2, \ldots, t\gamma_k) \in H$ by (1). Note that since $n \in N_G(H)$,

$$(t_1^{-1}tt_1, t_2^{-1}(t\gamma_2)t_2, \ldots, t_k^{-1}(t\gamma_k)t_k) = n^{-1}hn \in H.$$

Again by (1) we must have that $t_i^{-1}(t\gamma_i)t_i = (t_1^{-1}tt_1)\gamma_i$, and γ_i is a homomorphism, so $(t_1\gamma_i)^{-1}(t\gamma_i)(t_1\gamma_i) = (t_1^{-1}tt_1)\gamma_i = t_i^{-1}(t\gamma_i)t_i$. Then $(t_1\gamma_i)t_i^{-1} \in Z(T_i)$ since

$$((t_1\gamma_i)t_i^{-1})x = ((t_1\gamma_i)t_i^{-1})(t\gamma_i) = (t\gamma_i)((t_1\gamma_i)t_i^{-1}) = x((t_1\gamma_i)t_i^{-1})$$

and $x \in T_i$ was arbitrary. But $Z(T_i)$ is trivial since T_i is simple and nonabelian, so $t_i = t_1\gamma_i$. As this can be done for all $i \in \{2, \ldots, k\}$,

$$n = (t_1, t_2, \ldots, t_k) = (t_1, t_1\gamma_2, \ldots, t_1\gamma_k) \in H.$$

Thus $N_G(H) = H$, as desired.

(ii) The proof is by induction on k. If $k = 1$, then $H = T_1 := H_1$. Suppose that $k > 1$. Choose $S \subseteq I$ to be minimal such that $D := H \cap \prod_{i\in S} T_i \neq \{1\}$. H is clearly not trivial so $|S| \geq 1$. $\prod_{i\in S} T_i$ is a normal subgroup of G so D is a normal subgroup of H. Then $D\rho_i$ is a normal subgroup of $(H)\rho_i = T_i$ for all $i \in S$. If $D\rho_{i_o}$ is trivial for some $i_o \in S$, then the i_o-th component of every (nontrivial) element of D is 1. But then $H \cap \prod_{i\in(S\setminus\{i_o\})} T_i \neq \{1\}$, contradicting the minimality of S. Thus $D\rho_i$ is nontrivial for all $i \in S$, but T_i is simple, so $D\rho_i = T_i$ for all $i \in S$. Moreover, if there exists a nontrivial $d \in ker(\rho_{i_o}|_D)$ for some $i_o \in S$, then again, $H \cap \prod_{i\in(S\setminus\{i_o\})} T_i \neq \{1\}$, contradicting the minimality of S. Thus $\rho_i|_D$ is 1-1 for all $i \in S$, and we conclude that D is a full diagonal subgroup of $\prod_{i\in S} T_i$. Let $H_1 := D$ and $S := I_1$. If $S = I$, then we are done, so we may assume otherwise.

Let $\rho_S : G \to \prod_{i\in S} T_i$ be the projection map. D is a normal subgroup of H, so $D = D\rho_S$ is a normal subgroup of $H\rho_S$. By part (i), D is self-normalizing in $\prod_{i\in S} T_i$, so $D = H\rho_S$.

Let $H' := H \cap \prod_{i\in I\setminus S} T_i$. Then H' is a normal subgroup of H and clearly $D \cap H'$ is trivial. Let $h \in H$, and let $d \in G$ be defined by

$$d\rho_i := \begin{cases} h\rho_i & \text{if } i \in S, \\ 1 & \text{otherwise.} \end{cases}$$

Clearly $d \in H\rho_S = D$, so $h' := d^{-1}h \in DH = H$. Then $h' \in H'$ since for all $i \in S$, $h'\rho_i = (d\rho_i)^{-1}h\rho_i = 1$. Hence, $h = dh' \in DH'$, so $H = DH'$. It follows that $H = D \times H'$.

Let $G' := \prod_{i\in I\setminus S} T_i$. Fix $i_o \in I \setminus S$, and let $1 \neq t \in T_{i_o}$. Since $T_{i_o} = H\rho_{i_o}$, there exists an $h \in H$ with $t = h\rho_{i_o}$. Let h' be defined by

$$h'\rho_i := \begin{cases} h\rho_i & \text{if } i \in I \setminus S, \\ 1 & \text{otherwise.} \end{cases}$$

This implies that

$$(h'h^{-1})\rho_i = \begin{cases} h^{-1}\rho_i & \text{if } i \in S, \\ 1 & \text{otherwise.} \end{cases}$$

Then $h'h^{-1} \in H\rho_S = D \leq H$, so $h' \in H$. Since $h' \in G'$, $h' \in H'$, and by definition, $h'\rho_{i_o} = h\rho_{i_o} = t \neq 1$, so $H'\rho_{i_o}$ is nontrivial. But H' is a normal subgroup of H, so $H'\rho_{i_o}$ is

normal in $H\rho_{i_o} = T_{i_o}$, which is simple, so $H'\rho_{i_o} = T_{i_o}$. $i_o \in I \setminus S$ was arbitrary so H' is a subdirect subgroup of G'. By induction, H' is a direct product $\prod H_j$ $(j \geq 2)$ where H_j is a full diagonal subgroup of some subproduct $\prod_{i \in I_j} T_i$ such that the I_j partition $I \setminus I_1$, and we are done.

(iii) Proof is again by induction on k. If $k = 1$, then we're done since T_1 is simple. Suppose that $k > 1$. Let $J := \{i \in I : H\rho_i \neq \{1\}\}$. H is not trivial so $J \neq \emptyset$. $H \trianglelefteq G$, so $H\rho_i \trianglelefteq G\rho_i = T_i$ for all $i \in J$. But T_i is simple, so $H\rho_i = T_i$ for all $i \in J$. Thus H is a subdirect subgroup of $\prod_{i \in J} T_i$. By part (ii), H is a direct product of full diagonal subgroups of subproducts of $\prod_{i \in J} T_i$. As in the proof of part (ii), let $D := H \cap \prod_{i \in S} T_i$ where S is an appropriate minimal subset of J. $H \trianglelefteq G$ so $D \trianglelefteq \prod_{i \in S} T_i$, but D is full diagonal in $\prod_{i \in S} T_i$ by the proof of part (ii), hence is self-normalizing in $\prod_{i \in S} T_i$, and so $D = \prod_{i \in S} T_i$ by part (i). It follows from the remainder of the proof of part (ii) and from induction that $H = \prod_{i \in J} T_i$. □

The following may appear to be quite simple but is immensely useful.

Proposition 1.4.2 ([3])**.** *Let G be a group that normalizes $N := T_1 \times \cdots \times T_k$ where the T_i are all simple and nonabelian. Then G acts by conjugation on the set $\{T_1, \ldots, T_k\}$.*

Proof. Let $g \in G$. T_i is a normal subgroup of N, so $g^{-1}T_i g$ is a normal subgroup of $g^{-1}Ng = N$. Thus by Lemma 1.4.1(iii), $g^{-1}T_i g = \prod_{j \in J} T_j$ where J is some nonempty subset of $\{1, \ldots, k\}$. But $g^{-1}T_i g$ is simple since T_i is, so $g^{-1}T_i g = T_j$ for some j. Thus G acts on $\{T_1, \ldots, T_k\}$ by conjugation. □

The next result will be used both to prove the O'Nan-Scott Theorem and to make a reduction to the problem of finite representability. The formulation and proof of the lemma are mine, but its existence is implied by the proof of the O'Nan-Scott Theorem in [14].

Lemma 1.4.3. *Let G be a group containing subgroups A and M such that A normalizes M and $M \simeq T^k$ where T is a nonabelian simple group and k is a positive integer. Let K be a subgroup of M containing $M \cap A$ such that K is also normalized by A. Suppose that there exist groups $X_1, \ldots, X_n$ which satisfy the following:*

(i) $M = X_1 \times \cdots \times X_n$;

(ii) $K = X_1 \cap K \times \cdots \times X_n \cap K$;

(iii) X_l *is simple for all* l *or* $X_l \cap K$ *is a full diagonal subgroup of* X_l *for all* l.

Then A acts by conjugation both on $\{X_1, \ldots, X_n\}$ and $\{X_1 \cap K, \ldots, X_n \cap K\}$. Moreover, if $a \in A$ and $a^{-1}X_i a = X_j$, then $a^{-1}X_i \cap Ka = X_j \cap K$, and in the case where $X_l \cap K$ is full diagonal for all l, if $a^{-1}X_i \cap Ka = X_j \cap K$, then $a^{-1}X_i a = X_j$.

Proof. Fix $i \in \{1, \ldots, n\}$ and $a \in A$. If X_l is simple for all l, then since $M \simeq T^k$, X_l is also nonabelian for all l. If $X_l \cap K$ is a full diagonal subgroup of X_l for all l, then X_l is a direct product of isomorphic simple groups, but $X_l \trianglelefteq M \simeq T^k$, so by Lemma 1.4.1(iii), $X_l \simeq T^{m_l}$ for some $m_l \in \{1, \ldots, k\}$ for all l. Then $X_l \cap K \simeq T$, hence is simple and nonabelian for all l. A normalizes M and K, so by Proposition 1.4.2, when X_l is simple for all l, A acts on $\{X_1, \ldots, X_n\}$ by conjugation, and when $X_l \cap K$ is a full diagonal subgroup of X_l for all l, A acts on $\{X_1 \cap K, \ldots, X_n \cap K\}$ by conjugation. Thus A acts by conjugation on both sets in either case if we can prove the second claim of the lemma.

Suppose first that $a^{-1}X_i a = X_j$. Then $a^{-1}X_i \cap Ka = a^{-1}X_i a \cap a^{-1}Ka = X_j \cap K$ since A normalizes K.

Now suppose that $a^{-1}X_i \cap Ka = X_j \cap K$ and that $X_l \cap K$ is a full diagonal subgroup of X_l for all l. For notational ease, let $X := X_i$. We may write $M = T_1 \times \cdots \times T_k$ and $X = T_1 \times \cdots \times T_m$ for some $m \in \{1, \ldots, k\}$ where $T_l \simeq T$ for all l. $X \cap K$ is a full diagonal subgroup of X, so for all $l \in \{2, \ldots, m\}$, there exist isomorphisms $\gamma_l : T_1 \to T_l$ such that $X \cap K = \{(t, t\gamma_2, \ldots, t\gamma_m) : t \in T_1\}$ (see equation (1) in the proof of Lemma 1.4.1(i)). Let $1 \neq x \in T_l$ where $l \in \{1, \ldots, m\}$. Note that $a^{-1}T_l a = T_s$ for some $s \in \{1, \ldots, k\}$ by Proposition 1.4.2 since A normalizes M; in particular, $a^{-1}xa \in T_s$. There exists an element $t \in T_1$ with $t\gamma_l = x$, so $(t, t\gamma_2, \ldots, t\gamma_m) \in X \cap K$. Then $a^{-1}(t, t\gamma_2, \ldots, t\gamma_m)a \in X_j \cap K \leq X_j$. X_j is some subproduct of the simple factors of M, so $a^{-1}xa$ is in one of these simple factors, but $1 \neq a^{-1}xa$ is already in T_s, so this simple factor must be T_s. Thus $T_s \leq X_j$. It follows that if I_i and I_j denote the set of indices of the simple nonabelian factors of X_i and X_j respectively, then a maps $\{T_s : s \in I_i\}$ to $\{T_s : s \in I_j\}$ by conjugation; in fact, this map is a bijection as it is onto by symmetry and is clearly 1-1. Thus $a^{-1}X_i a = X_j$. □

Here is another quick application of Lemma 1.4.1. A proper normal subgroup N of a group G is said to be a *maximal normal subgroup* of G if N is the only proper normal subgroup of G containing N. Let $N \trianglelefteq G$. Note that N is a maximal normal subgroup of G if and only if G/N is simple since G and N are the only two normal subgroups of G containing N if and only if G/N has exactly two normal subgroups, namely, G/N and N/N.

Lemma 1.4.4 ([8, p. 113])**.** *Let H be a group with distinct normal subgroups $H_1, \ldots, H_k$ satisfying $\bigcap_{i=1}^{k} H_i = \{1\}$ such that for each i, $H/H_i \simeq T_i$ where T_i is a nonabelian simple group. Then $H \simeq T_1 \times \cdots \times T_k$.*

Proof. The proof is by induction on $k \geq 1$. The result is trivial if $k = 1$. Suppose that $k > 1$. Let $H_0 := \bigcap_{i=1}^{k-1} H_i \trianglelefteq H$. Then clearly $H_1/H_0, \ldots, H_{k-1}/H_0$ are distinct normal subgroups of H/H_0. Moreover, if $H_0 g \in \bigcap_{i=1}^{k-1} H_i/H_0$, then $g \in \bigcap_{i=1}^{k-1} H_i = H_0$, so $\bigcap_{i=1}^{k-1} H_i/H_0 = \{H_0\}$, and also $(H/H_0)/(H_i/H_0) \simeq H/H_i \simeq T_i$ for all $i \in \{1, \ldots, k-1\}$. Thus $H/H_0 \simeq T_1 \times \cdots \times T_{k-1}$ by induction.

Let N be a maximal normal subgroup of H/H_0. Then by part (iii) of Lemma 1.4.1, N is a direct product of some of the T_i. But in order for N to be maximal, N must then have the form $T_1 \times \cdots \times T_{i-1} \times T_{i+1} \times \cdots \times T_{k-1}$ for some i. It follows that H/H_0 has exactly $k-1$ maximal normal subgroups. However, since H/H_i is simple for all $i \in \{1, \ldots, k\}$ and the $H_1, \ldots, H_k$ are all distinct, H has at least k maximal normal subgroups (namely, the H_i). Thus H is not isomorphic to H/H_0, so $H_0 \neq \{1\}$. Then if $H_0 \leq H_k$, $H_0 = H_0 \cap H_k = \bigcap_{i=1}^{k} H_i = \{1\}$, a contradiction; it follows that $H_k < H_k H_0 \trianglelefteq H$, but H_k is maximal normal in H, so $H = H_k H_0$. Since $H_k \cap H_0 = \{1\}$, $H \simeq H_k \times H_0$. Then

$$H_0 \simeq (H_0 \times H_k)/H_k \simeq H/H_k \simeq T_k,$$

and

$$H_k \simeq (H_0 \times H_k)/H_0 \simeq H/H_0 \simeq T_1 \times \cdots \times T_{k-1}.$$

Thus $H \simeq T_1 \times \cdots \times T_k$, as desired. □

1.5 Minimal Normal Subgroups

Let G be a group. A nontrivial normal subgroup N of G is said to be a *minimal normal subgroup* of G if N is the only nontrivial normal subgroup of G contained in N. If G is finite and nontrivial, then G is guaranteed to have minimal normal subgroups.

The next few results illuminate the structure of a minimal normal subgroup.

Proposition 1.5.1. *Any two distinct minimal normal subgroups of a group G must intersect trivially. It follows that any two distinct minimal normal subgroups centralize each other.*

Proof. Let N_1 and N_2 be any two minimal normal subgroups of G. Then $N_1 \cap N_2$ is normal in G, but $N_1 \cap N_2 \leq N_1$ and $N_1 \cap N_2 \leq N_2$, so if $N_1 \cap N_2$ is not trivial, then $N_1 = N_1 \cap N_2 = N_2$ by the minimality of N_1 and N_2. Thus two distinct minimal normal subgroups intersect trivially. Moreover, if N_1 and N_2 are distinct minimal normal subgroups of G, then $[N_1, N_2] \leq N_1 \cap N_2 = \{1\}$, so N_1 and N_2 centralize each other. □

Recall from Proposition 1.4.2 that G acts by conjugation on $\{T_1, \ldots, T_k\}$ if the T_i are all simple and nonabelian and if $T_1 \times \cdots \times T_k$ is normalized by G.

Proposition 1.5.2 ([3])**.** *Let G be a group. Suppose that $N := T_1 \times \cdots \times T_k$ is a normal subgroup of G where the T_i are all simple and nonabelian. Then G acts transitively by conjugation on $\{T_1, \ldots, T_k\}$ if and only if N is a minimal normal subgroup of G.*

Proof. Suppose that G is transitive. Let M be a nontrivial normal subgroup of G with $M \leq N$. Then $M \trianglelefteq N$, so by Lemma 1.4.1, $M = \prod_{j \in J} T_j$ where J is some nonempty

subset of $\{1, \ldots, k\}$. Let $j_o \in J$. Since the action of G is transitive, given $i \in I$, there exists a $g_i \in G$ such that $T_i = g_i^{-1} T_{j_o} g_i$. M is a normal subgroup of G, so $T_{j_o} \leq M$ implies that $T_i \leq M$ for all $i \in \{1, \ldots, k\}$. Thus $N = M$, so N is a minimal normal subgroup of G.

On the other hand, suppose that G is not transitive on $\{T_1, \ldots, T_k\}$. Relabelling the indices as needed, let $\{T_1, \ldots, T_m\}$ be an orbit of the action (so we must have that $m < k$), and let $M := T_1 \times \cdots \times T_m$. Then for all $g \in G$ and $i \in \{1, \ldots, m\}$, $g^{-1} T_i g \subseteq \{T_1, \ldots, T_m\}$. Thus M is a normal subgroup of G, but $\{1\} \neq M < N$, so N is not a minimal normal subgroup of G. □

We have just seen that a minimal normal subgroup can be a direct product of isomorphic simple groups (they are isomorphic because they are conjugate). It turns out that, at least in a finite group, every minimal normal subgroup is a direct product of isomorphic simple groups. This will take some work to prove.

A subgroup H of G is *characterstic* in G, denoted by H char G, if $H\gamma = H$ for all $\gamma \in Aut(G)$. To show that H char G, it suffices to show that $H\gamma \leq H$ for all $\gamma \in Aut(G)$ (since then $H\gamma^{-1} \leq H$, which implies that $H = (H\gamma^{-1})\gamma \leq H\gamma$). Note that since conjugation by an element of G is an automorphism of G, H char G implies that H is normal in G (the converse is not necessarily true).

A nontrivial group G is *characteristically simple* if G has no proper nontrivial characteristic subgroups.

Proposition 1.5.3. *Let G be a group.*

(i) If H char K and $K \trianglelefteq G$, then $H \trianglelefteq G$.

(ii) If N is a minimal normal subgroup of G, then N is characteristically simple.

Proof. (i) Let $g \in G$ and let φ_g be the automorphism of G which conjugates by g. $K \trianglelefteq G$ so $K\varphi_g = K$, but then $\varphi_g|_K \in Aut(K)$. Since H char K, $H\varphi_g|_K = H$; that is, $g^{-1}Hg = H$ for all $g \in G$. Thus $H \trianglelefteq G$.

(ii) Suppose that H char N. N is normal in G so by part (i) we have that $H \trianglelefteq G$. But N is minimal normal and $H \leq N$, so we must have that $H = N$ or $H = \{1\}$. Thus N is characteristically simple. □

Theorem 1.5.4 ([20, p. 106])**.** *A finite characteristically simple group G is a direct product of isomorphic simple groups.*

Proof. Let N be a minimal normal subgroup of G with minimal order. Put $N_1 := N$. Let $H := N_1 \times N_2 \times \cdots \times N_k$ be the subgroup of G of largest possible order of this form, where $k \geq 1$, $N_i \simeq N$ for all i and $N_i \trianglelefteq G$ for all i. Note that $H \trianglelefteq G$.

Suppose that H char G. Since H is not trivial and G is characteristically simple, $H = G$. But then N must be simple, for if $\{1\} \neq M \trianglelefteq N$, then $M \trianglelefteq N_1 \times N_2 \times \cdots \times N_k = G$ and by the minimality of N, $M = N$. Thus G is a direct product of isomorphic simple groups.

Assume now for a contradiction that H is not characteristic in G. Then for some $\gamma \in Aut(G)$ and for some j, $N_j\gamma \not\leq H$. $N_j \trianglelefteq G$, so $N_j\gamma \trianglelefteq G\gamma = G$. Moreover, $N_j\gamma$ must be minimal normal in G, for if $N_j\gamma$ properly contains a nontrivial normal subgroup N' of G, then $|N'| < |N_j\gamma| = |N_j| = |N|$, contradicting the minimality of the order of N. Now, $N_j\gamma \cap H$ is a normal subgroup of G contained in $N_j\gamma$, but $N_j\gamma \not\leq H$, so by the minimality of $N_j\gamma$, $N_j\gamma \cap H = \{1\}$. Then since $N_j\gamma \simeq N_j \simeq N$, $N_j\gamma \times H$ is a subgroup of G of the same form as H with larger order, a contradiction.

□

Note that Theorem 1.5.4 can be generalized to infinite groups that contain at least one minimal normal subgroup, but only the finite version of the result is needed. Next is the result we are looking for.

Corollary 1.5.5. *A minimal normal subgroup of a finite group is a direct product of isomorphic simple groups.*

Proof. Follows immediately from Proposition 1.5.3(ii) and Theorem 1.5.4. □

The *socle* of a group G, denoted by $soc(G)$, is defined to be the subgroup generated by the set of all minimal normal subgroups of G, where $soc(G) := \{1\}$ if G has no minimal normal subgroups (which can only occur if G is infinite or trivial). Note that $soc(G)$ is a normal subgroup of G.

Every minimal normal subgroup of a finite group G is a product of isomorphic simple groups. More often than not, we are concerned with the case when all of these simple groups are nonabelian. The next result gives a handy condition for proving when a product of simple nonabelian groups is actually the socle of a finite group G.

Proposition 1.5.6. *Let G be a finite group with subgroup $M := T_1 \times \cdots \times T_k$ where $k \geq 1$ and T_i is simple and nonabelian for all i. Then M is the socle of G if and only if $C_G(M) = \{1\}$ and $M \trianglelefteq G$.*

Proof. Suppose that M is the socle of G. Of course $M \trianglelefteq G$. Moreover, this implies that $C_G(M) \trianglelefteq G$. If $C_G(M)$ is nontrivial, then $C_G(M)$ must contain some minimal normal subgroup of G, say N. $N \trianglelefteq soc(G) = M$, so $N = \prod_{j\in J} T_j$ for some $\emptyset \neq J \subseteq I$ by Lemma 1.4.1. In particular, $T_j \leq C_G(M)$ for any $j \in J$. But $C_G(M) \leq C_G(T_j)$, so $T_j \leq C_G(T_j)$, a contradiction since T_j is nonabelian. Thus $C_G(M) = \{1\}$.

Conversely, suppose that $C_G(M) = \{1\}$ and $M \trianglelefteq G$. Let N be a minimal normal subgroup of G. Then $N \cap M \trianglelefteq G$ and $N \cap M \leq N$, so either $N \leq M$ or $N \cap M = \{1\}$.

But if $N \cap M = \{1\}$, then $[N, M] \leq N \cap M = \{1\}$, so $N \leq C_G(M) = \{1\}$, a contradiction. Thus $N \leq M$, which implies that $soc(G) \leq M$. G acts on $\{T_1, \ldots, T_k\}$ by conjugation by Proposition 1.4.2; let $O_1, \ldots, O_m$ be the orbits of this action. For each $j \in \{1, \ldots, m\}$, let $N_j := \prod_{T_i \in O_j} T_i$. Then $g^{-1} N_j g = N_j$ for all j and $g \in G$, so $N_j \trianglelefteq G$ for all j. But G acts transitively on O_j for each j, so N_j is a minimal normal subgroup of G for each j by Proposition 1.5.2. Thus $M = N_1 \times \cdots \times N_m \leq soc(G)$, and we are done. □

1.6 Wreath Products

Let H and K be groups. A *group action* of K on H is a homomorphism $\varphi : K \to Aut(H)$. K is then said to be an *operator group* on H. Equivalently, K is an operator group on H if H is a K-space for which the action also satisfies $(h_1 h_2)^k = h_1^k h_2^k$ for all $h_1, h_2 \in H$ and $k \in K$.

If K is an operator group on H, then the *semidirect product* $H \rtimes K$ is the set $H \times K$ with multiplication defined as follows:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2^{k_1^{-1}}, k_1 k_2) \text{ for all } h_1, h_2 \in H \text{ and } \ k_1, k_2 \in K,$$

(where the k_1^{-1} is required for associativity). Then $H \rtimes K$ is a group with identity $(1, 1)$, in which $(h, k)^{-1} = ((h^{-1})^k, k^{-1})$. Note that $H \trianglelefteq H \rtimes K$.

A group G is an *internal semidirect product* of subgroups H and K if $H \trianglelefteq G$, $G = HK$, and $H \cap K = \{1\}$. We can define a group action of K on H by $h^k := k^{-1} h k$ for all $k \in K$ and $h \in H$; it is straightforward to show that $G \simeq H \rtimes K$ with this action. On the other hand, if $G = H \rtimes K$, define $H^* := \{(h, 1) : h \in H\}$ and $K^* := \{(1, k) : k \in K\}$. Then it is easy to see that G is the internal semidirect product of H^* and K^*; of course, $H \simeq H^*$ and $K \simeq K^*$. Thus these two concepts of a semidirect product are equivalent, and I will use either form as needed.

Suppose that G is an operator group on A, and suppose that H and B are groups with $G \simeq H$ and $A \simeq B$. Let ϕ and ψ denote the isomorphisms from G onto H and A onto B respectively. Then it is routine to verify that H is an operator group on B with action defined by $b^h := (a^g)\psi$ where $b = a\psi$ and $h = g\phi$. It follows that $A \rtimes G \simeq B \rtimes H$.

The following definitions can be found in [8, p. 46]. Let G and A be groups, and let Ω be a G-space. Let $B := A^\Omega = \{b : \Omega \to A\}$. Define multiplication on B by $\alpha(bb') := (\alpha b)(\alpha b')$ for all $b, b' \in B$ and $\alpha \in \Omega$. The multiplication is clearly associative, B has identity 1_B where $\alpha 1_B := 1$ for all $\alpha \in \Omega$, and $b \in B$ has inverse b^{-1} defined by $\alpha b^{-1} := (\alpha b)^{-1}$ for all $\alpha \in \Omega$. Thus B is a group.

Define an action of G on B by $\alpha b^g := (\alpha^{g^{-1}})b$ for all $g \in G$, $b \in B$ and $\alpha \in \Omega$. It is routine to verify that $b^1 = b$, $b^{gh} = (b^g)^h$, and $(bb')^g = b^g b'^g$ for all $b, b' \in B$ and $g, h \in G$, so we do actually have an action of G on B. Then the *wreath product* of A and G, denoted

by $A\ wr_\Omega\ G$, is defined to be the semidirect product $B \rtimes G = A^\Omega \rtimes G$. B is called the *base group* of the wreath product.

Note that if Ω is finite, then we can take G to act on $\Omega = \{1, \ldots, |\Omega|\}$, so that $A\ wr_\Omega\ G \simeq A^{|\Omega|} \rtimes G$. Then g acts on $(a_1, \ldots, a_{|\Omega|})$ by moving a_i to the i^g-th coordinate, which is written as $(a_1, \ldots, a_{|\Omega|})^g = (a_{1^{g^{-1}}}, \ldots, a_{|\Omega|^{g^{-1}}})$. To see how this notation works (as it is counter-intuitive), I will quickly verify that we still have an action. Let $g, h \in G$ and $(a_1, \ldots, a_{|\Omega|}) \in A^{|\Omega|}$. Then $a_{i^{g^{-1}}}$ is in the i-th coordinate of $(a_1, \ldots, a_{|\Omega|})^g$, so h will move $a_{i^{g^{-1}}}$ to the i^h-th coordinate. Thus $a_{i^{h^{-1}g^{-1}}}$ is in the i-th coordinate of $((a_1, \ldots, a_{|\Omega|})^g)^h$, so

$$(a_{1^{g^{-1}}}, \ldots, a_{|\Omega|^{g^{-1}}})^h = (a_{1^{h^{-1}g^{-1}}}, \ldots, a_{|\Omega|^{h^{-1}g^{-1}}}) = (a_{1^{(gh)^{-1}}}, \ldots, a_{|\Omega|^{(gh)^{-1}}}),$$

from which it follows that $((a_1, \ldots, a_{|\Omega|})^g)^h = (a_1, \ldots, a_{|\Omega|})^{gh}$.

The next result is an exercise in [8, p. 114].

Proposition 1.6.1. *Let T be a nonabelian simple group, and let $\Omega = \{1, \ldots, k\}$ where $k \geq 1$. Then $Aut(T^k) \simeq Aut(T)\ wr_\Omega\ S_k$.*

Proof. By the above, we have that $Aut(T)\ wr_\Omega\ S_k \simeq (Aut(T))^k \rtimes S_k$. Let

$$T_i := \{(1, \ldots, t, \ldots, 1) : t \in T, t \text{ in } i\text{-th coordinate}\},$$

so that $T^k = T_1 \times \cdots \times T_k$. Let $(a_1, \ldots, a_k)\pi \in (Aut(T))^k \rtimes S_k$ (using this notation for simplicity). Define $\psi_{(a_1,\ldots,a_k)\pi} : T^k \to T^k$ by $(t_1, \ldots, t_k) \mapsto (t_{1\pi^{-1}}a_{1\pi^{-1}}, \ldots, t_{k\pi^{-1}}a_{k\pi^{-1}})$. First, I claim that $\psi_{(a_1,\ldots,a_k)\pi} \in Aut(T^k)$. Since a_i is a homomorphism for all i, clearly $\psi_{(a_1,\ldots,a_k)\pi}$ is also a homomorphism. Suppose that $(t_1, \ldots, t_k) \in ker(\psi_{(a_1,\ldots,a_k)\pi})$. Then $(t_{1\pi^{-1}}a_{1\pi^{-1}}, \ldots, t_{k\pi^{-1}}a_{k\pi^{-1}}) = (1, \ldots, 1)$, so $t_i \in ker(a_i) = \{1\}$ for all i. Thus $\psi_{(a_1,\ldots,a_k)\pi}$ is 1-1. Lastly, let $(t_1, \ldots, t_k) \in T^k$ and define $x_j := t_{j\pi}a_j^{-1} \in T$ for all j. Then

$$(t_1, \ldots, t_k) = (x_{1\pi^{-1}}a_{1\pi^{-1}}, \ldots, x_{k\pi^{-1}}a_{k\pi^{-1}}) = (x_1, \ldots, x_k)\psi_{(a_1,\ldots,a_k)\pi},$$

so $\psi_{(a_1,\ldots,a_k)\pi}$ is onto, and we are done.

Now, we may define $\psi : (Aut(T))^k \rtimes S_k \to Aut(T^k)$ by $(a_1, \ldots, a_k)\pi \mapsto \psi_{(a_1,\ldots,a_k)\pi}$. Let $(a'_1, \ldots, a'_k)\pi' \in (Aut(T))^k \rtimes S_k$ and $(t_1, \ldots, t_k) \in T^k$. Then

$$\begin{aligned}
& (t_1, \ldots, t_k)\psi_{(a_1,\ldots,a_k)\pi}\psi_{(a'_1,\ldots,a'_k)\pi'} \\
= \ & (t_{1\pi^{-1}}a_{1\pi^{-1}}, \ldots, t_{k\pi^{-1}}a_{k\pi^{-1}})\psi_{(a'_1,\ldots,a'_k)\pi'} \\
= \ & (t_{1\pi'^{-1}\pi^{-1}}a_{1\pi'^{-1}\pi^{-1}}a'_{1\pi'^{-1}}, \ldots, t_{k\pi'^{-1}\pi^{-1}}a_{k\pi'^{-1}\pi^{-1}}a'_{k\pi'^{-1}}) \\
= \ & (t_{1(\pi\pi')^{-1}}a_{1(\pi\pi')^{-1}}a'_{1(\pi\pi')^{-1}\pi}, \ldots, t_{k(\pi\pi')^{-1}}a_{k(\pi\pi')^{-1}}a'_{k(\pi\pi')^{-1}\pi}) \\
= \ & (t_1, \ldots, t_k)\psi_{(a_1a'_{1\pi}, \ldots, a_ka'_{k\pi})\pi\pi'} \\
= \ & (t_1, \ldots, t_k)\psi_{(a_1,\ldots,a_k)\pi(a'_1,\ldots,a'_k)\pi'},
\end{aligned}$$

so ψ is a homomorphism.

Suppose that $\psi_{(a_1,\dots,a_k)\pi}$ is the identity. In particular, we then have that for all $t \in T$,

$$(t,\dots,t) = (t,\dots,t)\psi_{(a_1,\dots,a_k)\pi} = (ta_{1\pi^{-1}},\dots,ta_{k\pi^{-1}}),$$

so a_i is the identity on T_i for all i. Let $1 \neq t \in T$ and fix $i \in \{1,\dots,k\}$. If $t^* := (1,\dots,t,\dots,1) \in T_i$, then

$$(1,\dots,t,\dots,1) = t^* = t^*\psi_\pi = (1,\dots,t,\dots,1) \in T_{i\pi}$$

But $t \neq 1$, so $i\pi = i$. As i was arbitrary, $\pi = 1$. Thus ψ is 1-1.

Let $a \in Aut(T^k)$. Since $T_i \trianglelefteq T^k$, $T_i a \trianglelefteq T^k$, but $T \simeq T_i a$, so $T_i a$ is simple. Thus for each i, $T_i a = T_j$ for some j by Lemma 1.4.1. Let $\pi : \Omega \to \Omega$ be defined by $i \mapsto j$ if $T_i a = T_j$. Clearly $\pi \in S_k$. Fix $i \in \{1,\dots,k\}$ and let $t \in T$. If $(1,\dots,t,\dots,1) \in T_i$, then there exists a unique $(1,\dots,t',\dots,1) \in T_{i\pi}$ such that $(1,\dots,t,\dots,1)a = (1,\dots,t',\dots,1)$. Define $a_i : T \to T$ by $t \mapsto t'$. Then $a_i \in Aut(T)$ since $a|_{T_i} : T_i \to T_{i\pi}$ is an isomorphism. Moreover,

$$\begin{aligned}
& (t_1,\dots,t_k)\psi_{(a_1,\dots,a_k)\pi} \\
= \ & (t_{1\pi^{-1}}a_{1\pi^{-1}},\dots,t_{k\pi^{-1}}a_{k\pi^{-1}}) \\
= \ & (t'_{1\pi^{-1}},\dots,t'_{k\pi^{-1}}) \\
= \ & (t'_{1\pi^{-1}},1,\dots,1)\cdots(1,\dots,1,t'_{k\pi^{-1}}) \\
= \ & (1,\dots,t_{1\pi^{-1}},\dots,1)a|_{T_{1\pi^{-1}}}\cdots(1,\dots,t_{k\pi^{-1}},\dots,1)a|_{T_{k\pi^{-1}}} \\
= \ & (t_1,\dots,t_k)a
\end{aligned}$$

for all $(t_1,\dots,t_k) \in T^k$, so $\psi_{(a_1,\dots,a_k)\pi} = a$ and ψ is onto. □

I now investigate one way to turn a wreath product into a permutation group. Let G and H be groups acting on sets Δ and Γ respectively. Let W be the wreath product $H\ wr_\Delta\ G = B \rtimes G$ where $B = H^\Delta$. Let $\Omega := \Gamma^\Delta$. Define an action of W on Ω as follows: for each $(b,g) \in W$ and $\alpha \in \Omega$, let $\alpha^{(b,g)} : \Delta \to \Gamma$ be defined by

$$\delta \mapsto ((\delta^{g^{-1}})\alpha)^{(\delta^{g^{-1}})b}.$$

Then for all $(b,g),(b',g') \in W$ and $\delta \in \Delta$,

$$\delta\alpha^{(1_B,1)} = (\delta^1\alpha)^{(\delta^1)1_B} = \delta\alpha$$

and

$$\begin{aligned}
\delta(\alpha^{(b,g)})^{(b',g')} &= (\delta^{g'^{-1}}\alpha^{(b,g)})^{\delta^{g'^{-1}}b'} \\
&= (\delta^{g'^{-1}g^{-1}}\alpha)^{(\delta^{g'^{-1}}g^{-1}b)(\delta^{g'^{-1}}b')} \\
&= (\delta^{(gg')^{-1}}\alpha)^{\delta^{(gg')^{-1}}(bb'^{g^{-1}})} \\
&= \delta\alpha^{(bb'^{g^{-1}},gg')} \\
&= \delta\alpha^{(b,g)(b',g')},
\end{aligned}$$

so we do have an action of W on Ω. This action is called the *product action* of W on Ω.

The next proposition tells us that W acts as a permutation group under the product action exactly when both G and H act as permutation groups. This result is mentioned in [8, p. 50].

Proposition 1.6.2. *Let G and H be groups acting on sets Δ and Γ respectively, where $|\Gamma| \geq 2$. Then the product action of $W = H\ wr_\Delta\ G$ on $\Omega = \Gamma^\Delta$ is faithful if and only if the respective actions of G and H on Δ and Γ are faithful.*

Proof. Suppose that the product action of $W = H\ wr_\Delta\ G$ on $\Omega = \Gamma^\Delta$ is faithful and that $\delta^g = \delta^{g'}$ for all $\delta \in \Delta$ where $g, g' \in G$. Then

$$\delta\alpha^{(1_B, g^{-1})} = \delta^g\alpha = \delta^{g'}\alpha = \delta\alpha^{(1_B, g'^{-1})}$$

for all $\delta \in \Delta$, so $\alpha^{(1,g^{-1})} = \alpha^{(1,g'^{-1})}$ for all $\alpha \in \Omega$, but the action is faithful, so we must have that $(1, g^{-1}) = (1, g'^{-1})$, hence that $g = g'$. Thus the action of G on Δ is faithful. Suppose now that $\gamma^h = \gamma^{h'}$ for all $\gamma \in \Gamma$ where $h, h' \in H$. Define $b_h \in B$ by $\delta \mapsto h$. Define $b_{h'}$ similarly. Then for all $\delta \in \Delta$,

$$\delta\alpha^{(b_h,1)} = (\delta\alpha)^{\delta b_h} = (\delta\alpha)^h = (\delta\alpha)^{h'} = (\delta\alpha)^{\delta b_{h'}} = \delta\alpha^{(b_{h'},1)},$$

so $\alpha^{(b_h,1)} = \alpha^{(b_{h'},1)}$ for all $\alpha \in \Omega$. It follows that $h = h'$, so H is faithful on Γ.

On the other hand, suppose that the respective actions of G and H on Δ and Γ are faithful, and suppose that $\alpha^{(b,g)} = \alpha^{(b',g')}$ for all $\alpha \in \Omega$, where $(b, g), (b', g') \in W$. Then

$$(\delta^{g^{-1}}\alpha)^{\delta^{g^{-1}}b} = (\delta^{g'^{-1}}\alpha)^{\delta^{g'^{-1}}b'}$$

for all $\delta \in \Delta$ and $\alpha \in \Omega$. Let $\gamma \in \Gamma$ and define $\alpha_\gamma \in \Omega$ by $\delta \mapsto \gamma$. Then for each $\delta \in \Delta$,

$$\gamma^{\delta^{g^{-1}}b} = (\delta^{g^{-1}}\alpha_\gamma)^{\delta^{g^{-1}}b} = (\delta^{g'^{-1}}\alpha_\gamma)^{\delta^{g'^{-1}}b'} = \gamma^{\delta^{g'^{-1}}b'}.$$

Since γ was arbitrary and H is faithful on Γ, it follows that $\delta^{g^{-1}}b = \delta^{g'^{-1}}b'$ for all $\delta \in \Delta$. But then $\delta^{g^{-1}}\alpha = \delta^{g'^{-1}}\alpha$ for all $\delta \in \Delta$ and $\alpha \in \Omega$. If $\delta^{g^{-1}} \neq \delta^{g'^{-1}}$ for some $\delta \in \Delta$, then since $|\Gamma| \geq 2$, there is an $\alpha \in \Omega$ which will separate $\delta^{g^{-1}}$ and $\delta^{g'^{-1}}$, contradicting the above. Thus $\delta^{g^{-1}} = \delta^{g'^{-1}}$ for all $\delta \in \Delta$, but G is faithful on Δ so $g = g'$. Lastly, $\delta b^g = \delta^{g^{-1}}b = \delta^{g'^{-1}}b' = \delta b'^{g'}$ for all $\delta \in \Delta$, which implies that $b^g = b'^{g'}$, but $g = g'$, so $b = b'$. □

Let us consider another type of wreath product called the twisted wreath product, which is not quite a full generalization of a wreath product but is built from a wreath product. The twisted wreath product was originally constructed by B.H. Neumann in [17], but the constructions found in [24, p. 269] and [14] are my primary references.

Let G and A be groups where G contains a subgroup H that is an operator group on A, and let G act on itself by left multiplication (so that $\Omega = G$). Let

$$ {}_HB := \{b : G \to A : (xh)b = (xb)^h \text{ for all } x \in G, h \in H\}.$$

Then ${}_HB \subseteq B$ since $\Omega = G$. In fact, ${}_HB \leq B$: clearly $1_B \in {}_HB$, and if $b, b' \in {}_HB$, then for all $x \in G$ and $h \in H$,

$$\begin{aligned}(xh)b^{-1}b' &= ((xh)b)^{-1}((xh)b') \\ &= ((xb)^h)^{-1}(xb')^h \\ &= ((xb)^{-1})^h(xb')^h \\ &= ((xb)^{-1}(xb'))^h \\ &= (xb^{-1}b')^h,\end{aligned}$$

as desired. Moreover, note that if $b \in {}_HB$, then for all $x, g \in G$,

$$xb^g = x^{g^{-1}}b = ((g^{-1})^{-1}x)b = (gx)b,$$

so for all $h \in H$,

$$(xh)b^g = (gxh)b = ((gx)b)^h = (xb^g)^h.$$

Thus $b^g \in {}_HB$ for all $g \in G$ and $b \in {}_HB$, so we have an action of G on ${}_HB$. The *twisted wreath product* of A and G, denoted by $A\ twr_H\ G$, is defined to be the semidirect product ${}_HB \rtimes G$. ${}_HB$ is called the *base group* of the twisted wreath product. Note that when $H = \{1\}$, ${}_HB = B$ and the twisted wreath product is a wreath product.

A brief aside on transversal set notation: let $H \leq G$, and let L be a set of left transversals of H in G. Then every element $x \in G$ can be written uniquely as $x = \overline{x}h_x$ for some $h_x \in H$ where $\overline{x} \in L$. Whenever I refer to transversal sets, this notation will be used (with the appropriate adjustment for right transversal sets).

Proposition 1.6.3 ([24, p. 270])**.** *The base group ${}_HB$ of $A\ twr_H\ G$ is isomorphic to $\prod_{i\in I} A_i$ where $A_i = A$ for all $i \in I$ and I has the same cardinality as the set of cosets of H in G.*

Proof. Let $\{g_i : i \in I\}$ be a set of left transversals of H in G. Let $i \in I$, and let $A_i := \{g_ib : b \in {}_HB\}$. $A_i \leq A$ since $1 = g_i1_B \in A_i$ and $(g_ib)^{-1}(g_ib') = g_i(b^{-1}b') \in A_i$ for all $b, b' \in {}_HB$. On the other hand, let $a \in A$. Define $b_a : G \to A$ by $x \mapsto a^{h_x}$. $b_a \in {}_HB$ since if $h \in H$, then

$$(xh)b_a = (\overline{x}(h_xh))b_a = a^{h_xh} = (a^{h_x})^h = (xb_a)^h.$$

But $a = g_ib_a \in A_i$, so $A = A_i$ for all $i \in I$.

Now for each $b \in {}_HB$, define $f_b : I \to \bigcup_{i\in I} A_i$ by $i \mapsto g_ib \in A_i$. Then $f_b \in \prod_{i\in I} A_i$ for all $b \in {}_HB$. Define a function mapping from ${}_HB$ into $\prod_{i\in I} A_i$ by $b \mapsto f_b$. It is a homomorphism since for all $i \in I$,

$$if_{bb'} = g_i(bb') = (g_ib)(g_ib') = if_bif_{b'} = if_bf_{b'}.$$

It is 1-1 since if f_b is the identity of $\prod_{i\in I} A_i$, then $g_i b = i f_b = 1$ for all $i \in I$ (where 1 is the identity of $A_i = A$ for all $i \in I$), which implies that $xb = (\overline{x}b)^{h_x} = 1^{h_x} = 1 = x1_B$ for all $x \in G$, so $b = 1_B$. To see that it is onto, let $f \in \prod_{i\in I} A_i$. Then $if \in A_i$ for all $i \in I$, so for each $i \in I$ there exists a $b_i \in {}_H B$ with $if = g_i b_i$. Define $b_f : G \to A$ by $x \mapsto (\overline{x}b_i)^{h_x}$ when $\overline{x} = g_i$. Then $if_{b_f} = g_i b_f = g_i b_i = if$ for all $i \in I$ so $f_{b_f} = f$, and it is routine to verify that $b_f \in {}_H B$ (mimic the proof that $b_a \in {}_H B$ above), so we are done. Thus ${}_H B \simeq \prod_{i\in I} A_i$. $\square$

In the notation of the above proof, let $B_i := \{b \in {}_H B : g_j b = 1 \text{ for all } j \neq i\}$ for all $i \in I$. Then B_i is the preimage of A_i since $b \in B_i \iff 1 = g_j b = j f_b$ for all $j \neq i \iff f_b \in A_i$. Thus if $I = \{1, \ldots, k\}$, then ${}_H B = B_1 \times \cdots \times B_k$ (internally).

1.7 Solvable Groups

Let G be a group. A *solvable series* of a group G is a sequence of subgroups

$$\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

where G_i/G_{i+1} is abelian for all $i \in \{0, \ldots, n-1\}$. A group G is said to be *solvable* if G has a solvable series.

The *derived subgroup* or *commutator subgroup* of G is $G' := [G, G]$, which is a characteristic subgroup of G since for any $\gamma \in Aut(G)$, $[g, h]\gamma = [g\gamma, h\gamma]$ for all $g, h \in G$. In particular, G' is a normal subgroup of G. The *higher commutator subgroups* of G, denoted by $G^{(i)}$, are defined inductively by $G^{(0)} := G$ and $G^{(i+1)} := (G^{(i)})'$. The series

$$\cdots \leq G^{(i)} \leq \cdots \leq G^{(1)} \leq G^{(0)} = G$$

is called the *derived series* of G.

The following is a collection of well-known results about solvable groups.

Proposition 1.7.1. *Let G be a group.*

(i) If $H \trianglelefteq G$, then G/H is abelian if and only if $G' \leq H$.

(ii) If $\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$ is a solvable series, then $G^{(i)} \leq G_i$ for all $i \in \{0, \ldots, n\}$.

(iii) G is solvable if and only if $G^{(n)} = \{1\}$ for some $n \geq 0$.

(iv) If G is solvable, then any subgroup or homomorphic image of G is solvable; in particular, every quotient of G is solvable.

(v) If H is a normal solvable subgroup of G and if G/H is solvable, then G is solvable.

(vi) If H and K are solvable subgroups of a group G where H normalizes K, then HK is solvable.

Proof. (i) G/H is abelian $\iff hHgH = gHhH$ for all $g, h \in G \iff [g,h] = g^{-1}h^{-1}gh \in H$ for all $h, g \in G \iff G' \leq H$.

(ii) The proof is by induction on $i \geq 0$. If $i = 0$, then the result is trivial. Suppose that $G^{(i)} \leq G_i$ for some $i \geq 0$. Since G_i/G_{i+1} is abelian, $G_i' \leq G_{i+1}$ by part (i). Then $G^{(i+1)} = (G^{(i)})' \leq G_i'$ by induction, so $G^{(i+1)} \leq G_{i+1}$, as desired.

(iii) Suppose that G is solvable, and let $\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$ be a solvable series for G. Then by part (ii), $G^{(n)} \leq G_n = \{1\}$, as desired.

Suppose that $G^{(n)} = \{1\}$ for some $n \geq 0$. $G^{(i)}/G^{(i+1)}$ is abelian by part (i) since $G^{(i+1)} = (G^{(i)})'$. Thus the derived series is a solvable series for G, and G is solvable.

(iv) Let $H \leq G$. If $H^{(i)} \leq G^{(i)}$, then $H^{(i+1)} = (H^{(i)})' \leq (G^{(i)})' = G^{(i+1)}$, so by induction $H^{(i)} \leq G^{(i)}$ for all $i \geq 0$. Since G is solvable, $G^{(n)}$ is trivial for some n, so $H^{(n)}$ is also trivial. Thus H is solvable.

Let $\varphi : G \to H$ be an onto homomorphism. $(G\varphi)^{(i)} = G^{(i)}\varphi$ for all $i \geq 0$ since $[g\varphi, h\varphi] = [g,h]\varphi$ for all $g, h \in G$. Then $H^{(n)} = (G\varphi)^{(n)} = G^{(n)}\varphi = 1\varphi = 1$, so H is solvable.

(v) Let $\varphi : G \to G/H$ be the natural map. G/H is solvable so $(G/H)^{(n)} = \{1\}$ for some $n \geq 0$. Then $G^{(n)}\varphi = (G\varphi)^{(n)} = (G/H)^{(n)} = \{1\}$, so $G^{(n)} \leq ker(\varphi) = H$. H is solvable, so $H^{(m)} = \{1\}$ for some $m \geq 0$. Similar to the proof of part (iv), it can be shown by induction that for a fixed $i \geq 0$, $G^{(j+i)} \leq (G^{(i)})^{(j)}$ for all $j \geq 0$. But then $G^{(m+n)} \leq (G^{(n)})^{(m)} \leq H^{(m)} = \{1\}$. Thus G is solvable.

(vi) H normalizes K so HK/K is isomorphic to $H/H \cap K$ by the second isomorphism theorem. H is solvable so $H/H \cap K$ is solvable by part (iv). Thus HK/K is solvable, but K is solvable, so HK is solvable by part (v). □

Let p be a prime. An *elementary abelian p-group* is an abelian group G in which every nontrivial element has order p. Then G is a finite elementary abelian p-group if and only if $G \simeq \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.

Proposition 1.7.2 ([20, p. 105])**.** *If N is a finite solvable minimal normal subgroup of a group G, then it is an elementary abelian p-group for some prime p.*

Proof. N is a minimal normal subgroup of G, so it is characteristically simple by Proposition 1.5.3. Moreover, if $N' = N$, then since N is solvable, N must be trivial, a contradiction. Thus N is abelian since N' char N implies that N' is trivial. Let P be a Sylow p-subgroup of N. Since N is abelian, P is normal in N and hence is the only Sylow p-subgroup of N. If $\gamma \in Aut(N)$, then $P\gamma$ is also a Sylow p-subgroup of N, so $P\gamma = P$. Thus P char N, so $P = N$ and N is a p-group. Let $M := \{n \in N : n^p = 1\} \leq N$; note that M is an

elementary abelian p-group. Let n be a nontrivial element of M. Then for all $\gamma \in Aut(N)$, $n\gamma$ has order p, hence is in M. Thus M char N, but M is not trivial as N contains an element of order p by Cauchy's Theorem, so $M = N$. $\square$

1.8 Nilpotent Groups

Let G be a group. A *central series* of a group G is a sequence of subgroups

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

where $G_{i+1}/G_i \leq Z(G/G_i)$ for all $i \in \{0, \ldots, n-1\}$. A group G is said to be *nilpotent* if G has a central series. Clearly a nilpotent group is solvable.

The *higher centers* of G, denoted by $\zeta^i(G)$, are defined inductively by $\zeta^0(G) := \{1\}$ and $\zeta^{i+1}(G) := \{x \in G : [x, g] \in \zeta^i(G) \text{ for all } g \in G\}$. $\zeta^i(G) \leq G$ for all i since for all $g \in G$,

$$[xy, g] = [y, x][x, gy][y, g] \text{ and } [x^{-1}, g] = [x, gx^{-1}]^{-1}.$$

The *higher central series* of G is

$$\{1\} = \zeta^0(G) \leq \zeta^1(G) \leq \cdots \leq \zeta^n(G) \leq \cdots.$$

Note that $\zeta^i(G) \trianglelefteq G$ for all i since for all $g, h \in G$,

$$[h^{-1}xh, g] = [x, h]^{-1}[x, hg].$$

Moreover $\zeta^{i+1}(G)/\zeta^i(G) = Z(G/\zeta^i(G))$ for all i since $\zeta^i(G)x \in \zeta^{i+1}(G)/\zeta^i(G) \iff x \in \zeta^{i+1}(G) \iff [x, g] \in \zeta^i(G)$ for all $g \in G \iff \zeta^i(G)xg = \zeta^i(G)gx$ for all $g \in G \iff \zeta^i(G)x \in Z(G/\zeta^i(G))$. Note also that $\zeta^1(G) = Z(G)$.

The *lower centers* of G, denoted by $\gamma_i(G)$, are defined inductively by $\gamma_0(G) := G$ and $\gamma_{i+1}(G) := [\gamma_i(G), G]$. Clearly $\gamma_i(G) \trianglelefteq G$ for all i, which implies that $\gamma_{i+1}(G) \leq \gamma_i(G)$ for all i. Note that if $x \in \gamma_i(G)$, then $[x, g] \in \gamma_{i+1}(G)$ for all $g \in G$, so $\gamma_i(G)/\gamma_{i+1}(G) \leq Z(G/\gamma_{i+1}(G))$ for all i. The *lower central series* of G is

$$G = \gamma_0(G) \geq \gamma_1(G) \geq \cdots \geq \gamma_n(G) \geq \cdots.$$

The following is a collection of well-known results about nilpotent groups.

Proposition 1.8.1. *Let G be a group.*

(i) Let $\{1\} = G_0 \leq G_1 \leq \cdots \leq G_n = G$ be a central series in a nilpotent group G. Then $G_i \leq \zeta^i(G)$ and $\gamma_i(G) \leq G_{n-i}$ for all $i \in \{0, \ldots, n\}$.

(ii) G is nilpotent if and only if $G = \zeta^n(G)$ for some $n \geq 0$.

(iii) *G is nilpotent if and only if $\{1\} = \gamma_n(G)$ for some $n \geq 0$.*

(iv) *If G is nilpotent, then any subgroup or homomorphic image of G is nilpotent.*

(v) *If H is a normal subgroup of G contained in $Z(G)$ and if G/H is nilpotent, then G is nilpotent.*

(vi) *If G is a finite p-group, then G is nilpotent.*

(vii) *If G is nilpotent and N is a nontrivial normal subgroup of G, then N intersects nontrivially with $Z(G)$.*

(viii) *If G is nilpotent, then no proper subgroup of G is self-normalizing.*

(ix) *If G is a finite nilpotent group and $p \mid |G|$, then G has a unique Sylow p-subgroup P.*

Proof. (i) First I show that $G_i \leq \zeta^i(G)$ for all i; the proof is by induction on i. If $i = 0$, the result is trivial. Suppose that the result is true for some $i \geq 0$. Let $x \in G_{i+1}$. Since $G_{i+1}/G_i \leq Z(G/G_i)$, $[x, g] \in G_i$ for all $g \in G$, so $[x, g] \in \zeta^i(G)$ for all $g \in G$ by induction. Thus $x \in \zeta^{i+1}(G)$.

Now, I show that $\gamma_i(G) \leq G_{n-i}$ for all i; the proof is again by induction on $i \geq 0$. If $i = 0$, the result is trivial; suppose that it is true for some $i \geq 0$. Let $x \in \gamma_i(G)$. Then $x \in G_{n-i}$ by induction, so $[x, g] \in [G_{n-i}, G] \leq G_{n-i-1}$ since $G_{n-i}/G_{n-i-1} \leq Z(G/G_{n-i-1})$. It follows that $\gamma_{i+1}(G) \leq G_{n-(i+1)}$.

(ii) If G is nilpotent, then $G = \zeta^n(G)$ for some $n \geq 0$ by part (i), and if $G = \zeta^n(G)$ for some $n \geq 0$, then the higher central series of G is a central series, so G is nilpotent.

(iii) If G is nilpotent, then $\{1\} = \gamma_n(G)$ for some $n \geq 0$ by part (i), and if $\{1\} = \gamma_n(G)$ for some $n \geq 0$, then the lower central series of G is a central series, so G is nilpotent.

(iv) Let $H \leq G$. If $\gamma_i(H) \leq \gamma_i(G)$, then $\gamma_{i+1}(H) = [\gamma_i(H), H] \leq [\gamma_i(G), G] = \gamma_{i+1}(G)$. Thus $\gamma_i(H) \leq \gamma_i(G)$ for all $i \geq 0$ by induction. Then if G is nilpotent, H is clearly nilpotent by part (iii).

Similarly, if $\varphi : G \to H$ is an onto homomorphism, then $\gamma_i(G\varphi) \leq \gamma_i(G)\varphi$ for all $i \geq 0$, so for some $n \geq 0$, we have that $\gamma_i(H) = \gamma_i(G\varphi) = \gamma_i(G)\varphi = \{1\}\varphi = \{1\}$. Thus H is nilpotent.

(v) G/H is nilpotent, so we have a central series

$$H/H = G_0/H \trianglelefteq G_1/H \trianglelefteq \cdots \trianglelefteq G_n/H = G/H,$$

so

$$\{1\} \trianglelefteq H = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G.$$

If $x \in G_{i+1}$, then $(G_i/H)(Hx) \in Z((G/H)/(G_i/H))$, so $H[x, g] \in G_i/H$ for all $g \in G$. This implies that $[x, g] \in G_i$ for all $g \in G$, so $G_{i+1}/G_i \leq Z(G/G_i)$ for all $i \geq 0$. But $H \leq Z(G)$, so we have a central series for G.

(vi) By induction on $|G|$. If $G = \{1\}$ the result is trivial. Suppose that $|G| > 1$. Then $Z(G)$ is not trivial by Proposition 1.3.1, so $G/Z(G)$ is nilpotent by induction. By part (v), G is nilpotent.

(vii) By part (ii), $G = \zeta^n(G)$ for some $n \geq 0$. Then $N \leq \zeta^n(G)$, but $N \cap \zeta^0(G) = \{1\}$, so there exists a least positive integer i such that $N \cap \zeta^i(G) \neq \{1\}$. Let $g \in G$ and $1 \neq x \in N \cap \zeta^i(G)$. Then $[x, g] \in N$ since $N \trianglelefteq G$, but $[x, g] \in \zeta^{i-1}(G)$ by definition, so $[x, g] = 1$ since $N \cap \zeta^{i-1}(G) = \{1\}$. Thus $x \in Z(G)$, but $x \in N$, so $N \cap Z(G) \neq \{1\}$.

(viii) Let $H < G = \gamma_0(G)$. Since G is nilpotent, $\gamma_n(G) = \{1\} \leq H$ for some $n \geq 0$, so there is a least positive integer i with $\gamma_{i+1}(G) \leq H$ but $\gamma_i(G) \not\leq H$. Then $[\gamma_i(G), H] \leq [\gamma_i(G), G] = \gamma_{i+1}(G) \leq H$, so if $x \in \gamma_i(G)$, then $[x, h] \in H$ for all $h \in H$. It follows that $\gamma_i(G) \leq N_G(H)$. Thus if $H = N_G(H)$, then $\gamma_i(G) \leq H$, a contradiction, so $H < N_G(H)$.

(ix) If $N_G(P) < G$, then $N_G(P) < N_G(N_G(P))$ by part (vii), but this contradicts Proposition 1.3.6, so $N_G(P) = G$. Thus $P \trianglelefteq G$ and P is the unique Sylow p-subgroup of G. □

Let G be a finite group with $|G| = p^n k$ for some prime p where $p \nmid k$. G is said to be *p-nilpotent* if there exists a normal subgroup N of G with $|N| = k$.

Proposition 1.8.2. *If G is a finite nilpotent group, then G is p-nilpotent for all primes p dividing the order of G.*

Proof. By Proposition 1.8.1(ix), G has a unique Sylow p-subgroup for each prime p dividing the order of G. Fix such a prime and write $|G| = p^n k$ where $p \nmid k$. Let N be the product of all of the Sylow q-subgroups of G such that $q \neq p$. Then $N \trianglelefteq G$ and $|N| = k$. Thus G is p-nilpotent. □

Let P be a finite p-group and let n be the largest order of an elementary abelian p-subgroup of P. The *Thompson subgroup* of P, denoted by $J(P)$, is defined to be the subgroup of P generated by all of the elementary abelian p-subgroups of P of order n. Note that if P is nontrivial, then $J(P)$ is nontrivial. Moreover, $J(P)$ is a characteristic subgroup of P, for if $\alpha \in Aut(P)$ and P' is an elementary abelian p-subgroup of P of order n, then so is $(P')\alpha \leq J(P)$.

Theorem 1.8.3 (Thompson)**.** *Let G be a finite group and let P be a Sylow p-subgroup of G where p is odd. Then G is p-nilpotent if and only if $N_G(J(P))$ and $C_G(Z(P))$ are p-nilpotent.*

Proof. See [19, p. 298]. □

1.9 Fixed-point-free Automorphisms

Let G be a group and let $\alpha \in Aut(G)$. α is said to have a *fixed point* $g \in G$ if $g\alpha = g$. If the identity of G is the only fixed point of α, then α is said to be *fixed-point-free*.

Here are some basic properties of fixed-point-free automorphisms.

Proposition 1.9.1 ([19, p. 305])**.** *Let α be a fixed-point-free automorphism of order n of a finite group G.*

(i) If $gcd(m, n) = 1$, then α^m is fixed-point-free.

(ii) If $\beta : G \to G$ is defined by $g \mapsto g^{-1}(g\alpha)$, then β is a permutation of G.

(iii) If $g \in G$, then g and $g\alpha$ are conjugate in G if and only if $g = 1$.

(iv) $g(g\alpha)\cdots(g\alpha^{n-1}) = 1$ for all $g \in G$.

(v) For each prime p dividing the order of G, there exists a Sylow p-subgroup P of G such that $P\alpha = P$.

Proof. (i) There exist integers s and t with $ms + nt = 1$. Suppose that $g\alpha^m = g$. Then $g\alpha = g\alpha^{ms+nt} = g\alpha^{ms} = g$, so $g = 1$. Thus α^m is fixed-point-free.

(ii) Suppose that $g\beta = h\beta$. Then $g^{-1}(g\alpha) = h^{-1}(h\alpha)$ so $hg^{-1} = (hg^{-1})\alpha$, but α is fixed-point-free, so $h = g$. Thus β is 1-1, but G is finite, so β is also onto.

(iii) Suppose that $g\alpha = h^{-1}gh$ for some $h \in G$. By part (ii), $h = a^{-1}(a\alpha)$ for some $a \in G$. Then

$$g\alpha = h^{-1}gh = (a^{-1}(a\alpha))^{-1}g(a^{-1}(a\alpha)) = (a\alpha)^{-1}aga^{-1}(a\alpha),$$

which implies that $(aga^{-1})\alpha = aga^{-1}$, but α is fixed-point-free, so $aga^{-1} = 1$. Thus $g = 1$. The converse is trivial.

(iv) Let $x := g(g\alpha)\cdots(g\alpha^{n-1})$. Then

$$x\alpha = (g(g\alpha)\cdots(g\alpha^{n-1}))\alpha = (g\alpha)\cdots(g\alpha^{n-1})g = g^{-1}xg,$$

so $x = 1$ by part (iii).

(v) Let Q be a Sylow p-subgroup of G. Then $Q\alpha$ is also a Sylow p-subgroup of G, so $Q\alpha = g^{-1}Qg$ for some $g \in G$. By part (ii), $g = h(h^{-1}\alpha)$ for some $h \in G$. Let $P := h^{-1}Qh$. Then P is a Sylow p-subgroup and

$$\begin{aligned} P\alpha &= (h^{-1}Qh)\alpha \\ &= (h\alpha)^{-1}(Q\alpha)(h\alpha) \\ &= (h\alpha)^{-1}(h(h^{-1}\alpha))^{-1}Q(h(h^{-1}\alpha))h\alpha \\ &= h^{-1}Qh \\ &= P. \end{aligned}$$

□

Lemma 1.9.2. *Let G be a finite group with a fixed-point-free automorphism α of prime order p. If H is a proper normal subgroup of G satisfying $H\alpha = H$, then G/H has a fixed-point-free automorphism of order p.*

Proof. Define $\beta : G/H \to G/H$ by $Hg \mapsto H(g\alpha)$. Then $Hg = Hg' \iff g'g^{-1} \in H \iff (g'g^{-1})\alpha \in H \iff H(g\alpha) = H(g'\alpha)$, so β is well-defined and 1-1. Since α is an onto homomorphism, so is β. Note that if $Hg = H(g\alpha)$ for all $g \in G$, then $g(g\alpha)^{-1} \in H$ for all $g \in G$, or $g^{-1}(g\alpha) \in H$ for all $g \in G$, but then $H = G$ by part (ii) of Proposition 1.9.1, a contradiction. Thus β is not the identity. Then since α has order p, $Hg\beta^p = H(g\alpha^p) = Hg$ for all $g \in G$, so β has order p. Lastly, suppose that $(Hg)\beta = (Hg)$ for some $g \in G$. Then $g(g^{-1}\alpha) \in H$. Since $H\alpha = H$, $\alpha|_H \in Aut(H)$ and is fixed-point-free, so by part (ii) of Proposition 1.9.1, $g \in H$. Thus β is fixed-point-free. □

Lemma 1.9.3 ([19, p. 306])**.** *Suppose that $H \leq Aut(A)$ where A is a finite abelian group. Suppose further that there exist $\sigma \in Aut(A)$ and $M \leq Aut(A)$ such that $\sigma\beta$ is fixed-point-free of prime order p for all $\beta \in M$, $gcd(|A|, |M|) = 1$, and $H = M \rtimes \langle\sigma\rangle$. Then $M = \{1\}$.*

Proof. Let $a \in A$ and $\beta \in M$. Then $a(a\sigma\beta)\cdots(a(\sigma\beta)^{p-1}) = 1$ by Proposition 1.9.1. Since A is abelian,

$$1 = \prod_{\beta\in M}\left(\prod_{i=0}^{p-1} a(\sigma\beta)^i\right) = a^{|M|}\prod_{i=1}^{p-1}\left(\prod_{\beta\in M} a(\sigma\beta)^i\right).$$

Fix $i \in \{1, \ldots, p-1\}$. If $(\sigma\beta)^i = (\sigma\beta')^i$ for some $\beta, \beta' \in M$, then $(\sigma\beta)^i \in \langle\sigma\beta'\rangle$, so $\sigma\beta \in \langle\sigma\beta'\rangle$ since $gcd(i, p) = 1$ and $\sigma\beta$ has order p. Thus for some $j \in \{1, \ldots, p-1\}$,

$$\sigma\beta = (\sigma\beta')^j = \sigma^j((\sigma^{j-1})^{-1}\beta'\sigma^{j-1})\cdots((\sigma^2)^{-1}\beta'\sigma^2)(\sigma^{-1}\beta'\sigma)\beta'.$$

The element $((\sigma^{j-1})^{-1}\beta'\sigma^{j-1})\cdots((\sigma^2)^{-1}\beta'\sigma^2)(\sigma^{-1}\beta'\sigma)\beta' \in M$ since $M \trianglelefteq H$, and $\sigma^j \in \langle\sigma\rangle$; since $M \cap \langle\sigma\rangle = \{1\}$, we must have that $\sigma = \sigma^j$, but σ has order p and $j \in \{1, \ldots, p-1\}$, so $j = 1$. Thus if $(\sigma\beta)^i = (\sigma\beta')^i$, then $\beta = \beta'$. Now, $(\sigma\beta)^i = \sigma^i(\sigma^{i-1})^{-1}\beta\cdots\sigma\beta = \sigma^i\beta^*$ where $\beta^* := (\sigma^{i-1})^{-1}\beta\cdots\sigma\beta \in M$. Since $(\sigma\beta)^i$ is distinct for each $\beta \in M$, so is each β^*. Then

$$\prod_{\beta\in M} a(\sigma\beta)^i = \prod_{\beta\in M} a\sigma^i\beta.$$

It follows that

$$a^{-|M|} = \prod_{i=1}^{p-1}\left(\prod_{\beta\in M} a\sigma^i\beta\right).$$

Let $\gamma \in M$. Then

$$(a^{-|M|})\gamma = \prod_{i=1}^{p-1}\left(\prod_{\beta\in M} a\sigma^i\beta\gamma\right) = \prod_{i=1}^{p-1}\left(\prod_{\beta\in M} a\sigma^i\beta\right) = a^{-|M|}.$$

Let n denote the order of a. Then $gcd(n, |M|) = 1$, so there exist integers s and t with $ns + |M|t = 1$, which implies that $a\gamma = (a^{|M|}\gamma)^t = a^{|M|t} = a$. Since $a \in A$ was arbitrary and $\gamma : A \to A$, $\gamma = 1$. Thus $M = \{1\}$. □

Theorem 1.9.4 (Thompson, [19, p. 306])**.** *Let G be a finite group with a fixed-point-free automorphism α of prime order p. Then G is nilpotent.*

Proof. The proof is by induction on $|G|$. The base case is the cyclic group of order 3 (it has a fixed-point-free automorphism of order 2), which is nilpotent.

First I show that G must be solvable. If G is any q-group, where q is a prime, then G is solvable, so we may assume both that G is not a q-group and that there is an odd prime q dividing $|G|$. By Proposition 1.9.1, there exists a Sylow q-subgroup Q such that $Q\alpha = Q$. Note that the Thompson subgroup of Q, J(Q), is solvable as it is a q-group. Moreover, $J(Q)\alpha = J(Q)$ since $J(Q)$ *char* Q.

If $J(Q) \trianglelefteq G$, then $G/J(Q)$ has a fixed-point-free automorphism of order p by Lemma 1.9.2; $J(Q) \neq \{1\}$ so $|G/J(Q)| < |G|$. Then $G/J(Q)$ is nilpotent by induction, hence solvable, but so is $J(Q)$, so G is solvable by Proposition 1.7.1.

If $J(Q)$ is not normal in G, then $N_G(J(Q)) < G$. I claim that $(N_G(J(Q)))\alpha = N_G(J(Q))$. Suppose $g^{-1}J(Q)g = J(Q)$ where $g \in G$. Then

$$J(Q) = J(Q)\alpha = (g^{-1}J(Q)g)\alpha = (g\alpha)^{-1}J(Q)(g\alpha),$$

so $N_G(J(Q))\alpha \leq N_G(J(Q))$. As they have the same order, $N_G(J(Q))\alpha = N_G(J(Q))$, as desired. Since $\{1\} \neq J(Q) \leq N_G(J(Q))$, $\alpha|_{N_G(J(Q))}$ is fixed-point-free of order p, so $N_G(J(Q))$ is nilpotent by induction.

Now, consider $C_G(Z(Q))$. If $C_G(Z(Q)) = G$, then $Z(Q) \trianglelefteq G$. Since $Z(Q)$ is characteristic in Q, $G/Z(Q)$ has a fixed-point-free automorphism of order p by Lemma 1.9.2. $Z(Q)$ is not trivial since Q is a nontrivial q-group, so $|G/Z(Q)| < |G|$. Thus $G/Z(Q)$ is nilpotent by induction, hence solvable, but $Z(Q)$ is solvable as it is a q-group, so G is solvable.

Suppose now that $C_G(Z(Q)) < G$. Let $g \in C_G(Z(Q))$ and $x \in Z(Q)$. Then $x = y\alpha$ for some $y \in Z(Q)$ since $Z(Q)$ is characteristic in Q. This implies that

$$(g\alpha)^{-1}x(g\alpha) = (g^{-1}yg)\alpha = y\alpha = x,$$

so $C_G(Z(Q))\alpha \leq C_G(Z(Q))$. Thus $C_G(Z(Q))\alpha = C_G(Z(Q))$. If $C_G(Z(Q))$ is trivial, it is nilpotent. If not, then $\alpha|_{C_G(Z(Q))}$ is fixed-point-free of order p, so $C_G(Z(Q))$ is nilpotent by induction.

Thus both $C_G(Z(Q))$ and $N_G(J(Q))$ are q-nilpotent by Proposition 1.8.2, so G is q-nilpotent by Theorem 1.8.3. Then there exists a normal subgroup N of G with $|N| = k$ where $|G| = q^n k$ and $q \nmid k$. Note that $G = QN$ since $|QN| = |G|$. Let $n \in N$. Then

$n\alpha = am$ where $a \in Q$ and $m \in N$, so $a = n\alpha m^{-1} \in Q$. This implies that $n\alpha m^{-1}$ has order q^l for some $l \in \{0, \ldots, n\}$, so

$$1 = (n\alpha m^{-1})^{q^l} = (n\alpha)^{q^l}((n\alpha)^{q^l-1})^{-1}m^{-1} \cdots n\alpha m^{-1}.$$

The element $((n\alpha)^{q^l-1})^{-1}m^{-1} \cdots n\alpha m^{-1} \in N$ since $N \trianglelefteq G$, so $(n\alpha)^{q^l} \in N$. But $gcd(q^l, k) = 1$, so there exist integers s and t with $q^l s + kt = 1$. Then since $n^{kt} = 1$, $n\alpha = (n\alpha)^{q^l s} \in N$, so $N\alpha = N$. Since $N < G$, N is nilpotent by induction, hence solvable. But N is nontrivial as G is not a q-group, so $|G/N| < |G|$. Thus G/N is solvable by induction and Lemma 1.9.2, so G is solvable.

Thus in all cases, G is solvable. Of course, we may assume that G is not abelian, so if $Z(G)$ is nontrivial, then $G/Z(G)$ is nilpotent by induction and Lemma 1.9.2, which implies that G is nilpotent by Proposition 1.8.1. Hence, it suffices to show that $Z(G)$ is nontrivial. Note that if $G' = G$, then $G^{(i)} = G$ for all $i \geq 1$, but G is solvable, so $G^{(n)} = 1$ for some $n \geq 1$ by Proposition 1.7.1, a contradiction. Thus G' is a proper nontrivial characteristic subgroup of G. Let A be a nontrivial normal subgroup of G that is minimal with respect to $A\alpha = A$. Since $G' < G$ and A is minimal, $A < G$. Now, A' *char* A, so $A' \trianglelefteq G$ and $A'\alpha = A'$. Since A is solvable, $A' < A$, so by the minimality of A, $A' = \{1\}$. Thus A is abelian. Let q be a prime dividing $|A|$, and define $A^* := \{a \in A : a^q = 1\} \neq \{1\}$. Then A^* *char* A since $(a\beta)^q = a^q\beta = 1$ for all $\beta \in Aut(A)$, so, by the minimality of A, $A = A^*$. Thus A is an elementary abelian q-group.

If G is a q-group, then $Z(G)$ is nontrivial, so we may assume that there exists a prime $r \mid |G|$ such that $r \neq q$. By Proposition 1.9.1, there exists a Sylow r-subgroup R of G such that $R\alpha = R$. $AR \leq G$ since $A \trianglelefteq G$. If $AR < G$, then since $(AR)\alpha = A\alpha R\alpha = AR$, AR is nilpotent by induction. R is a Sylow r-subgroup of AR, so by Proposition 1.8.1, R is the unique Sylow r-subgroup. Thus $R \trianglelefteq AR$. Clearly $A \cap R = \{1\}$ since $q \neq r$, so $[A, R] \leq A \cap R = \{1\}$, which implies that $R \leq C_G(A)$. Suppose that $AR < G$ for each prime r dividing the order of G such that $r \neq q$ (where R is defined as above). Then $G/C_G(A)$ is a q-group. Define a group action of $G/C_G(A)$ on $Aut(A)$ by $a^{C_G(A)g} := g^{-1}ag$ for all $g \in G$ and $a \in A$. Then $A \rtimes G/C_G(A)$ is a q-group, hence is nilpotent, so we may let $1 \neq a \in A \cap Z(A \rtimes G/C_G(A))$ by part (vii) of Proposition 1.8.1. Then for all $g \in G$,

$$\begin{aligned}(a, C_G(A)g) &= (a, C_G(A))(1, C_G(A)g)\\ &= (1, C_G(A)g)(a, C_G(A))\\ &= (a^{C_G(A)g^{-1}}, C_G(A)g)\\ &= (gag^{-1}, C_G(A)g).\end{aligned}$$

Then $a = gag^{-1}$ for all $g \in G$, so $a \in Z(G)$, and we are done.

So we may assume that there exists a prime $r \neq q$ dividing the order of G and a Sylow r-subgroup R with $R\alpha = R$ and $AR = G$. Let $\varphi_m : A \to A$ be conjugation by $m \in G$. Let $\sigma := \alpha|_A$ and let $M := \{\varphi_m : m \in R\} \leq Aut(A)$.

Let $1 \neq \varphi_m \in M \cap \langle\sigma\rangle$. m must have order $n \neq 1$ for some integer n, so $a\varphi_m^n = (m^n)^{-1}am^n = a$ for all $a \in A$, but $\varphi_m \in \langle\sigma\rangle$ implies that φ_m has order p, so $p \mid n$. Thus R contains an element of order p, but R is an r-group, so $r = p$. Define $\varphi : \langle\alpha\rangle \to Aut(R)$ by $\alpha \mapsto \alpha|_R$. This is a group action. Then $R \rtimes \langle\alpha\rangle$ is nilpotent since it is a p-group, so by Proposition 1.8.1, $R \cap Z(R \rtimes \langle\alpha\rangle)$ is nontrivial; let $1 \neq x$ be in this intersection. Then

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

so $x = x\alpha$, which implies that x is a nontrivial fixed point of α, a contradiction. Thus $M \cap \langle\sigma\rangle = \{1\}$. Now, suppose that $\varphi_m \in M$ and $\sigma^i \in \langle\sigma\rangle$. Then

$$\begin{aligned} a(\sigma^{-i}\varphi_m\sigma^i) &= (m^{-1}(a\sigma^{-i})m)\sigma^i \\ &= (m^{-1}(a\alpha^{-i})m)\alpha^i \\ &= (m\alpha^i)^{-1}a(m\alpha^i) \\ &= a\varphi_{m\alpha^i} \end{aligned}$$

for all $a \in A$, so $\sigma^{-i}\varphi_m\sigma^i = \varphi_{m\alpha^i} \in M$ since $m\alpha^i \in R$. Thus M is normalized by $\langle\sigma\rangle$, so we may define $H := M \rtimes \langle\sigma\rangle \leq Aut(A)$.

If M contains an element of order q, say φ_m, and the order of m is n, then $q \mid n$ as we saw before, but R is an r-group, so $q = r$, a contradiction. Thus $gcd(|A|, |M|) = 1$. Let $\varphi_m \in M$. Suppose that $a\sigma\varphi_m = a$ for some $a \in A$. Then $a\alpha = a\sigma = mam^{-1}$, so $a\alpha$ and a are conjugate in G. By Proposition 1.9.1, $a = 1$, so $\sigma\varphi_m$ is fixed-point-free on A. To show that $\sigma\varphi_m$ has order p, it suffices to show that $\sigma\varphi_m$ is conjugate to σ in $Aut(A)$. α^{-1} is fixed-point-free on R and $m\alpha^{-1} \in R$, so there exists an $s \in R$ with $m\alpha^{-1} = s^{-1}(s\alpha^{-1})$ by Proposition 1.9.1. Then $m = (s^{-1}\alpha)s$, so

$$a\varphi_s^{-1}\sigma\varphi_s = s^{-1}((sas^{-1})\sigma)s = s^{-1}(s\alpha)(a\alpha)(s^{-1}\alpha)s = m^{-1}(a\sigma)m = a\sigma\varphi_m$$

for all $a \in A$, so $\varphi_s^{-1}\sigma\varphi_s = \sigma\varphi_m$, as desired. Thus $\sigma\beta$ is fixed-point-free on A of order p for all $\beta \in M$, so $M = 1$ by Lemma 1.9.3, which implies that $a = m^{-1}am$ for all $m \in R$ and $a \in A$. Then since A is abelian, $A \leq Z(AR) = Z(G)$, and we are done. □

1.10 Finite Simple Groups

My main references for this section are [7], [8] and [12]. Let G be a group. A *composition series* of a group G is a sequence of subgroups

$$\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

where G_{i+1} is a maximal normal subgroup of G_i for each i. As we saw in Section 1.4, G_i/G_{i+1} is simple for all i. The factors G_i/G_{i+1} are called *composition factors*, and n is

the *length* of the series. Moreover, it is easy to see that every finite group has a composition series: G must contain a maximal normal subgroup G_1; if G_1 is trivial, we are done, and if not, then G_1 contains a maximal normal subgroup, and so on. This process must terminate since G is finite. Note that if the factor groups all have prime order, then G is solvable. The Jordan-Hölder Theorem (see [20, p. 100], for example) states that any two composition series of a group G have the same length and also that there exists a 1-1 correspondence between the sets of correspondence factors such that corresponding factor groups are isomorphic. Thus a finite group G determines a unique list of finite simple groups, namely, the factors of any one of its composition series. It is for this reason that finite simple groups are so important.

Here is the classification of the finite simple groups:

Theorem 1.10.1 ([12, p. 6])**.** *A finite simple group is either cyclic of prime order, the alternating group A_n when $n \geq 5$, a group of Lie type, or one of 26 sporadic groups.*

As I mentioned in the introduction, the original proof was based on extensive research by numerous mathematicians; the completion of this immense result was first announced by Gorenstein in [11]. The proof is now being rewritten in a more concise and self-contained fashion; presently, there are six volumes of a projected twelve, of which [12] is the first.

I will very briefly outline the various types of finite simple groups. Of course, if G is simple and abelian, then G is a cyclic group of prime order. Moroever, it is well-known that the alternating group A_n is a nonabelian simple group for $n \geq 5$. The simple groups of *Lie type* can be characterized as groups of fixed points of endomorphisms of linear algebraic groups over an algebraically closed field of characteristic p (see [23]), and they consist of several infinite families of groups. Some of the groups of Lie type involve families of well-known classical groups: linear groups, unitary groups, symplectic groups and orthogonal groups. I give details on the first two classical groups of Lie type as they will be mentioned in Section 3.

Consider the general linear group of $n \times n$ invertible matrices over the finite field $\mathbb{F}_q$, denoted by $GL_n(q)$. The special linear group, denoted by $SL_n(q)$, is the set of all of matrices of determinant one, and is actually a normal subgroup of $GL_n(q)$. The projective special linear group, denoted by $PSL_n(q)$, is simply $SL_n(q)/Z(SL_n(q))$. In fact, $Z(SL_n(q))$ consists of the scalar matrices of $SL_n(q)$. $PSL_n(q)$ is simple if $n \geq 2$ except when $n = 2$ and $q = 2$ or 3; it is called a *linear group* within the world of finite simple groups.

The general unitary group $GU_n(q)$ is the group of matrices $M \in GL_n(q^2)$ such that $M^{-1} = (\bar{M})^t$, where $\bar{M}$ is simply M with every entry raised to the q-th power. The special unitary group $SU_n(q)$ is then the subgroup of $GU_n(q)$ consisting of those matrices with determinant one, and the projective special unitary group $PSU_n(q)$ is $SU_n(q)$ factored out by its scalar matrices. $PSU_n(q)$ is simple if $n \geq 2$ except when $q = 2$ and $n = 2$ or 3 or when $q = 3$ and $n = 2$; it is called a *unitary group* within the world of finite simple groups.

There are also 26 sporadic groups which do not fit into any infinite family of nonabelian simple groups. The first five of these groups were discovered by Mathieu in the 1860's, but most of the remaining sporadic groups were disovered through attempts to prove the classification of the finite simple groups.

The *outer automorphism group* of G, denoted by $Out(G)$, is simply the quotient group $Aut(G)/Inn(G)$. Consider briefly the outer automorphism group of a finite simple group: if G is cyclic of prime order p, it is not hard to see that $Out(G) \simeq Aut(G) \simeq \mathbb{Z}_p^*$, the multiplicative group of units of the ring $\mathbb{Z}_p$, which is abelian. Suppose that $n \geq 5$. Let $\pi \in S_n$, and as usual, let $\varphi_\pi : S_n \to S_n$ be conjuagtion by π. We can easily map S_n into $Aut(A_n)$ by $\pi \mapsto \varphi_\pi|_{A_n}$; this is clearly an embedding since $C_{S_n}(A_n)$ is trivial. Moreover, it can be shown that if $n \neq 6$, then this map is onto (see [24, p. 299]). But A_n is simple and nonabelian, so $A_n \simeq Inn(A_n)$, which gives us that $|Out(A_n)| = [S_n : A_n] = 2$. Thus $Out(A_n) \simeq \mathbb{Z}_2$ when $n \neq 6$. In [24, p. 300], it is proved that $Aut(A_6) = Aut(S_6)$ and $[Aut(S_6) : Inn(S_6)] = 2$. Since we also have that $S_6 \simeq Inn(S_6)$, it follows that $|Out(A_6)| = 4$ (in fact, $Out(A_6) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$). Hence for $n \geq 5$, $Out(A_n)$ is abelian. I will not go into details when G is of Lie type, but it turns out that $Out(G)$ is solvable; see [7]. Lastly, if G is one of the 26 sporadic groups, then $Out(G)$ has order at most 2, hence is abelian.

Summarizing, if G is either cyclic of prime order, the alternating group A_n when $n \geq 5$, or one of the 26 sporadic groups, then $Out(G)$ is abelian, and if G is of Lie type, then $Out(G)$ is solvable. The classification of the finite simple groups then implies that we have proven the Schreier Conjecture, stated below. To date, no simpler proof is known. Interestingly, I could not find an original reference for this conjecture.

Theorem 1.10.2 (Schreier Conjecture)**.** *The outer automorphism group of a finite simple group is solvable.*

2 Finite Primitive Permutation Groups

First I define primitivity and look at some of the properties of finite primitive permutation groups; specifically, I examine the highly restrictive structure of the socle of a finite primitive permutation group. I then describe the five isomorphism classes of a finite primitive permutation group as they are outlined in [14]. I finish with the proof of the O'Nan-Scott Theorem. Except where otherwise noted, all of the results in the isomorphism class sections (2.2-2.6) are stated or implied in [14] but not proved; again, my main source for the proof of the O'Nan-Scott Theorem is [14], though I have reorganized their proof somewhat. Both [8] and [19] are general references for this entire section.

2.1 Primitivity

Let Ω be a G-space, and let $\alpha \in \Omega$. A *block* is a nonempty subset Γ of Ω such that for every $g \in G$, either $\Gamma = \Gamma^g$ or $\Gamma \cap \Gamma^g = \emptyset$. Ω and $\{\alpha\}$ are called *trivial blocks* as they are rather uninteresting. Any other block of Ω is called *nontrivial*. A transitive G-space Ω is called *primitive*, or equivalently, G is said to *act primitively* on Ω, if Ω contains no nontrivial block. If the action of a primitive G-space is faithful, then G is said to be a *primitive permutation group*. Note that if G is primitive, then G^Ω is a primitive permutation group (irrespective of the action being faithful).

The definition is only given for transitive G-spaces since if the action of G on Ω is nontrivial and not transitive, then G must have a proper orbit containing at least two elements, which is a nontrivial block.

Before I look at some of the properties of primitive G-spaces, I consider briefly how any group action can be reduced to a primitive one. Let G act on Ω. Then G is transitive on the orbit $\theta_G(\alpha)$ for all $\alpha \in \Omega$. Suppose that $\theta_G(\alpha)$ contains at least two elements, and let $\Gamma \subseteq \theta_G(\alpha)$ be a minimal block of G containing at least two elements. Then I claim that G_Γ acts primitively on Γ. Let $\alpha, \beta \in \Gamma$. Then there exists a $g \in G$ with $\alpha^g = \beta$ since G is transitive on $\theta_G(\alpha)$. Since $\alpha^g = \beta \in \Gamma^g \cap \Gamma$ and Γ is a block of G, $\Gamma^g = \Gamma$. Thus $g \in G_\Gamma$, so G_Γ is transitive on Γ. Now, let $\Delta \subseteq \Gamma$ be a block of G_Γ containing at least two elements. Let $g \in G$. If $g \in G_\Gamma$, then of course $\Delta^g = \Delta$. If $g \notin G_\Gamma$, then $\Gamma^g \cap \Gamma = \emptyset$, so $\Delta^g \cap \Delta = \emptyset$. Hence, Δ is actually a block of G, so $\Delta = \Gamma$ by the minimality of Γ. Thus G_Γ has no nontrivial blocks, so G_Γ is primitive on Γ.

Suppose now that N acts on Ω and contains a subgroup G which is primitive on Ω. Then for every proper subset Γ of Ω containing at least two elements, there exists a $g \in G$ such that $\Gamma \neq \Gamma^g$ and $\Gamma \cap \Gamma^g \neq \emptyset$. Then each such $g \in N$, but G is transitive, so N is transitive, hence primitive. In particular, every subgroup of S^Ω containing a primitive group is itself primitive.

I claim that A^Ω is primitive when Ω contains at least three elements (if Ω is infinite,

then A^Ω is defined to be the subgroup of S^Ω generated by all of the 3-cycles). A^Ω is transitive, for if $\alpha, \beta \in \Omega$, then, choosing $\gamma \in \Omega$ such that $\gamma \neq \alpha$ and $\gamma \neq \beta$, we get that the permutation $\pi := (\alpha\ \beta\ \gamma) \in A^\Omega$ and that $\alpha\pi = \beta$. Let Γ be a proper subset of Ω containing at least two elements. Then there exist $\alpha \in \Omega \setminus \Gamma$ and $\beta, \gamma \in \Gamma$ with $\beta \neq \gamma$. Again, let π be $(\alpha\ \beta\ \gamma)$. Then $\alpha = \gamma\pi \in \Gamma\pi$ so $\Gamma \neq \Gamma\pi$. Similarly, $\gamma \in \Gamma\pi \cap \Gamma$, so $\Gamma\pi \cap \Gamma \neq \emptyset$. Thus A^Ω is primitive. Moreover, it follows that S^Ω is primitive for all nonempty Ω: the result is trivial when Ω contains one or two elements, and if Ω contains at least three elements, then S^Ω is primitive since A^Ω is.

A *G-congruence* on Ω is a G-invariant equivalence relation $\sim$ on Ω; that is, $\alpha \sim \beta \iff \alpha^g \sim \beta^g$ for all $g \in G$. Trivial and nontrivial G-congruences are defined in the obvious way.

This next proposition is from an exercise in [8, p. 13].

Proposition 2.1.1. *Suppose that Ω is a G-space with G^Ω nontrivial. Then it is primitive if and only if the only G-congruences on Ω are trivial.*

Proof. Suppose that $\sim$ is a nontrivial G-congruence on Ω. Let $[\alpha]$ be an equivalence class of $\sim$ which contains at least two elements (and is of course proper). Let $g \in G$ and $\beta \in [\alpha]^g$. Then $\beta = \gamma^g$ where $\gamma \sim \alpha$, so $\beta^{g^{-1}} = \gamma \sim \alpha$, which implies that $\beta \sim \alpha^g$ since $\sim$ is a G-congruence. Thus $\beta \in [\alpha^g]$, so $[\alpha]^g \subseteq [\alpha^g]$. Similarly, $[\alpha^g] \subseteq [\alpha]^g$, so $[\alpha]^g = [\alpha^g]$. Thus $[\alpha]^g$ is an equivalence class for all $g \in G$; it follows that $[\alpha]$ is a nontrivial block, so Ω cannot be primitive.

Suppose now that Ω is not primitive but is transitive. Then there exists a nontrivial block Γ, and every element of Ω is in Γ^g for some $g \in G$. Moreover, if $\Gamma^g \cap \Gamma^h \neq \emptyset$ for some $g, h \in G$, then $\Gamma^{gh^{-1}} \cap \Gamma \neq \emptyset$, so $\Gamma^{gh^{-1}} = \Gamma$ since Γ is a block, which implies that $\Gamma^g = \Gamma^h$. Thus $\{\Gamma^g : g \in G\}$ partitions Ω, which allows us to define an equivalence relation $\sim$ on Ω by $\alpha \sim \beta$ if there exists a $g \in G$ with $\alpha, \beta \in \Gamma^g$. $\sim$ is G-invariant since $\alpha \sim \beta$ implies that $\alpha, \beta \in \Gamma^h$ for some $h \in G$, so $\alpha^g, \beta^g \in \Gamma^{hg}$ and $\alpha^g \sim \beta^g$. Thus $\sim$ is a nontrivial G-congruence.

Lastly, suppose that Ω is not transitive. Define $\sim$ by $\alpha \sim \beta$ if α and β are in the same orbit. This clearly defines a G-congruence whose congruence classes are orbits. Since Ω is not transitive and since the action is not trivial, $\sim$ must be nontrivial. □

The proof of Proposition 2.1.1 shows that this variant must also be true:

Proposition 2.1.2. *Suppose that Ω is a transitive G-space. Then it is primitive if and only if the only G-congruences on Ω are trivial.*

This next property of primitive permutation groups is quite important and will be used without reference.

Proposition 2.1.3 ([19, p. 199])**.** *Let G be a primitive permutation group on Ω. If N is a nontrivial normal subgroup of G, then N is transitive on Ω.*

Proof. N is nontrivial, so N must move some element of Ω; thus there exists an N-orbit Γ containing at least two elements. Let $\alpha \in \Gamma$ and $g \in G$. Then $\alpha gn = \alpha(gng^{-1})g \in \Gamma g$ for all $n \in N$ since N is normal in G, so $\Gamma gn \subseteq \Gamma g$ for all $n \in N$ and $g \in G$. It follows that $\Gamma gn = \Gamma g$ for all $n \in N$ and $g \in G$, so Γg is an N-orbit for all $g \in G$. Then Γ is a block of G since two orbits are either the same or have empty intersection, but G is primitive, so $\Gamma = \Omega$. Thus N is transitive. □

Note that the requirement above that G be a permutation group is necessary: if G does not act faithfully on Ω where Ω contains at least two elements, then the kernel of the action is a nontrivial normal subgroup of G that moves no element of Ω and so cannot be transitive.

Let H, K and L be subgroups of a group G where $H \leq K$. Suppose that we have an action of L on K. Then H is said to be an *L-invariant subgroup* of K if $H^l = H$ for all $l \in L$. For the action to be conjugation, L must normalize K. If so, then H is an L-invariant subgroup of K if and only if $L \leq N_G(H)$. I will assume for the remainder of this thesis that the action is conjugation whenever I refer to invariant subgroups.

In the following, the proof of part (i) comes from [19, p. 198] while part (ii) is an exercise from [8, p. 124].

Theorem 2.1.4. *Let G act on Ω, where Ω contains at least two elements.*

(i) G is primitive if and only if G is transitive and G_α is a maximal subgroup of G for all $\alpha \in \Omega$.

(ii) Let H be a transitive subgroup of G which is normalized by G_β for some $\beta \in \Omega$. Then G is primitive if and only if H_α is a maximal G_α-invariant subgroup of H for all $\alpha \in \Omega$.

Proof. (i) Suppose that G is primitive, and let $\alpha \in \Omega$. G_α is a proper subgroup of G since Ω contains at least two elements. Let $G_\alpha \leq H \leq G$ and define $\Gamma := \{\alpha^h : h \in H\}$. Then Γ is an H-orbit. Let $g \in G$ and suppose that $\beta \in \Gamma^g \cap \Gamma$. Then $\beta = \alpha^{h_1 g} = \alpha^{h_2}$ for some $h_1, h_2 \in H$, which implies that $h_1 g h_2^{-1} \in G_\alpha \leq H$, so $g \in H$. But then $\Gamma^g = \Gamma$, so Γ is a block. G is primitive so either $\Gamma = \{\alpha\}$ or $\Gamma = \Omega$. Suppose that $\Gamma = \{\alpha\}$, and let $h \in H$. Then $\alpha^h = \alpha$ as $\alpha^h \in \Gamma$, so $h \in G_\alpha$. Thus $G_\alpha = H$. Suppose instead that $\Gamma = \Omega$, and let $g \in G$. Then $\alpha^g \in \Omega = \Gamma$, so $\alpha^g = \alpha^h$ for some $h \in H$. It follows that $gh^{-1} \in G_\alpha \leq H$, so $g \in H$ and $H = G$. Thus G_α is a maximal subgroup of G.

Suppose now that G is not primitive but is transitive. Then there exists a nontrivial block Γ; let $\alpha \in \Gamma$. $G_\alpha \leq G_\Gamma$ since if $\alpha^g = \alpha$, then $\Gamma^g \cap \Gamma \neq \emptyset$, which implies that $\Gamma^g = \Gamma$.

Suppose that $G_\alpha = G_\Gamma$, and let $\beta \in \Gamma$. By transitivity, there exists a $g \in G$ such that $\beta = \alpha^g$. Then $\Gamma^g \cap \Gamma \neq \emptyset$, so it follows that $g \in G_\Gamma = G_\alpha$. But then $\beta = \alpha^g = \alpha$, so $\Gamma = \{\alpha\}$, a contradiction. Suppose now that $G = G_\Gamma$, and let $\beta \in \Omega$. Again, there exists a $g \in G$ such that $\beta = \alpha^g$. Then $\beta \in \Gamma^g = \Gamma$, so $\Omega = \Gamma$, a contradiction. Thus $G_\alpha < G_\Gamma < G$, so G_α is not maximal in G.

(ii) Since H is transitive, G is transitive, and since Ω contains at least two elements, H_α is a proper subgroup of H. Moreover, for every $\alpha \in \Omega$ there exists an $h \in H$ with $\beta = \alpha^h$, so $G_\beta = G_{\alpha^h} = h^{-1}G_\alpha h$. Then G_α normalizes H for all $\alpha \in \Omega$ since G_β normalizes H. In particular, H_α is normal in G_α, so H_α is a proper G_α-invariant subgroup of H for all $\alpha \in \Omega$.

Suppose that G is primitive, and let $\alpha \in \Omega$. Suppose further that there exists $M \leq G$ such that $H_\alpha \leq M \leq H$ and $G_\alpha \leq N_G(M)$. If $G_\alpha = N_G(M)$, then $M \leq G_\alpha$, but $M \leq H$ so $M \leq G_\alpha \cap H = H_\alpha$. Thus $M = H_\alpha$. If $G_\alpha < N_G(M)$, then since G is primitive, $N_G(M) = G$ by part (i). Then M is normal in G, so $G_\alpha \leq G_\alpha M \leq G$. Moreover, if M is trivial, then $H_\alpha = \{1\} = M$, so we may assume that M is not trivial. Then since $M \trianglelefteq G$ and G is primitive, M is transitive. If $G_\alpha = G_\alpha M$, then G_α is transitive since M is, a contradiction of Ω containing at least two elements. Thus $G_\alpha M = G$, again by part (i), so $H = H \cap (G_\alpha M) = H_\alpha M = M$. Thus H_α is a maximal G_α-invariant subgroup of H.

Suppose now that G is not primitive; let Γ be a nontrivial block and $\alpha \in \Gamma$. As we saw in the proof of part (i), $G_\alpha < G_\Gamma < G$. Let $M := G_\Gamma \cap H = H_\Gamma$. Then G_α normalizes M since $G_\alpha \leq G_\Gamma$ and G_α normalizes H. Clearly $H_\alpha \leq M \leq H$. If $H = M = H_\Gamma$, then since H is transitive, repeating the proof of part (i) gives us that $\Omega = \Gamma$, a contradiction. If $H_\alpha = M = H_\Gamma$, then again by the proof of (i), we get that $\Gamma = \{\alpha\}$, a contradiction. Thus H_α is not a maximal G_α-invariant subgroup of H. □

Note that when G is a transitive permutation group, given any $\beta \in \Omega$, $G_\beta = G_{\alpha^g} = g^{-1}G_\alpha g$ for some $g \in G$. Thus every stabilizer of a transitive permutation group G is conjugate in G. It follows that if one stabilizer of G is a maximal subgroup of G, then every stabilizer is maximal in G. Thus to show that a transitive group G acts primitively, it suffices to show that one stabilizer is maximal in G. Similarly for part (ii), it suffices to show that H_α is a maximal G_α-invariant subgroup of H for some $\alpha \in \Omega$. On the other hand, if we know that G is primitive, both conditions will be useful in classifying which isomorphism class G belongs to. In particular, since we will see shortly that the socle of a finite primitive permutation group has a very nice structure and since such a socle is transitive by Proposition 2.1.3, the H in part (ii) is often taken to be the socle.

The next result is an exercise in [8, p. 52] that is required to prove Proposition 2.1.6, the first application of Theorem 2.1.4.

Proposition 2.1.5. *Let G be primitive on Ω where Ω contains at least two elements. Then G is not regular if and only if G_α is self-normalizing in G for all $\alpha \in \Omega$.*

Proof. Let $\alpha \in \Omega$. Since G is primitive, G is transitive, so G is regular if and only if G_α is trivial. Note that if G_α is trivial, then $G_\alpha \trianglelefteq G$. On the other hand, if $G_\alpha \trianglelefteq G$ and G_α is not trivial, then G_α is transitive by primitivity, but then Ω can only contain one element, a contradiction. Thus G is regular if and only if $G_\alpha \trianglelefteq G$, or G is not regular if and only if $N_G(G_\alpha) < G$. Since G is primitive, G_α is maximal in G, but $G_\alpha \leq N_G(G_\alpha) \leq G$, so either $G_\alpha = N_G(G_\alpha)$ or $N_G(G_\alpha) = G$. Hence, G is not regular if and only if $G_\alpha = N_G(G_\alpha)$. □

Proposition 2.1.6 ([8, p. 50])**.** *Let G and H be groups acting on sets Δ and Γ respectively, where H is not trivial, and both Δ and Γ contain at least two elements. Then the product action of $W := H\ wr_\Delta\ G$ on $\Omega := \Gamma^\Delta$ is primitive if and only if Δ is finite, G is transitive on Δ, and H is primitive but not regular on Γ.*

Proof. Let B be the base group of W, $B' := \{(b, 1) : b \in B\}$ and $G' := \{(1_B, g) : g \in G\}$, so that $W = B'G'$. Let $\gamma \in \Gamma$ and define $\alpha_\gamma \in \Omega$ by $\delta \mapsto \gamma$. Now

$$\alpha_\gamma = \alpha_\gamma^{(b,g)} \iff \gamma = \delta\alpha_\gamma = \delta\alpha_\gamma^{(b,g)} = (\delta^{g^{-1}}\alpha_\gamma)^{\delta^{g^{-1}}b} = \gamma^{\delta^{g^{-1}}b}$$

for all $\delta \in \Delta$, which is true if and only if $\gamma = \gamma^{\delta b}$ for all $\delta \in \Delta$ (as $\delta^{g^{-1}}$ acts as a bijection on Δ). Thus

$$W_{\alpha_\gamma} = \{(b, g) \in W : \delta b \in H_\gamma \text{ for all } \delta \in \Delta\}.$$

Since Γ contains at least two elements, so does Ω, so by Theorem 2.1.4, W is primitive if and only if W is transitive and W_{α_γ} is maximal in W. First, I prove that if one of the five conditions in the theorem fails, then one of these two conditions on W must fail.

Suppose that H is not transitive on Γ. Let $\gamma, \gamma' \in \Gamma$. If W is transitive on Ω, then for α_γ and $\alpha_{\gamma'}$ defined as above, there exists a $(b, g) \in W$ with

$$\alpha_\gamma^{(b,g)} = \alpha_{\gamma'}.$$

Then for each $\delta \in \Delta$,

$$\gamma' = \delta\alpha_{\gamma'} = \delta\alpha_\gamma^{(b,g)} = (\delta^{g^{-1}}\alpha_\gamma)^{\delta^{g^{-1}}b} = \gamma^{\delta^{g^{-1}}b},$$

and $\delta^{g^{-1}}b \in H$, so H is transitive on Γ, a contradiction. Thus W is not transitive on Ω.

We may assume then that H is transitive. Since $|\Gamma| \geq 2$, H_γ is a proper subgroup of H. If $h \in H$, define $b_h \in B$ by $\delta \mapsto h$. This function will be used repeatedly.

Suppose that H is not primitive. Since H is transitive, there exists a K with $H_\gamma < K < H$. Let $K' := \{(b, g) \in W : \delta b \in K \text{ for all } \delta \in \Delta\}$. Clearly $W_{\alpha_\gamma} \leq K' \leq W$. Let $h \in H \setminus K$. Then $(b_h, 1) \in W \setminus K'$, so $K' < W$. Similarly, let $k \in K \setminus H_\gamma$. Then $(b_k, 1) \in K' \setminus W_{\alpha_\gamma}$, so $W_{\alpha_\gamma} < K'$. Thus W_{α_γ} is not maximal in W.

Suppose that H is regular. Then $W_{\alpha_\gamma} = \{(b, g) \in W : \delta b = 1 \text{ for all } \delta \in \Delta\} = \{(1_B, g) \in W\} = G'$. Let $L := \{(b, 1) \in W : \delta b = \delta' b \text{ for all } \delta, \delta' \in \Delta\}$. Then $L \leq W$.

Moreover, L is normalized by G' since if $(b,1) \in L$ then for all $\delta, \delta' \in \Delta$ and $g \in G$, $\delta b^g = \delta^{g^{-1}} b = \delta'^{g^{-1}} b = \delta' b^g$, which implies that $(1_B, g)^{-1}(b,1)(1_B, g) = (b^g, 1) \in L$. Thus $W_{\alpha_\gamma} = G' \leq LG' \leq W$. If $G' = LG'$, then $L \leq G'$, but $L \leq B'$ so L must be trivial. H is not trivial, so let $1 \neq h \in H$. Then $(1_B, 1) \neq (b_h, 1) \in L$, a contradiction. If $LG' = W$, then clearly $L = B'$, but Δ contains at least two elements so we can define an element of B which separates 1 and $h \neq 1$, a contradiction. Thus $W_{\alpha_\gamma} < LG' < W$.

Suppose that G is not transitive on Δ. Let Σ be an orbit of G in Δ, and let $M := \{(b,1) \in W : \delta b \in H_\gamma \text{ for all } \delta \in \Sigma\} \leq B$. Again, M is normalized by G' since for $(b,1) \in M$ and $g \in G$, $\delta b^g = \delta^{g^{-1}} b \in H_\gamma$ for all $\delta \in \Sigma$ (since $\delta^{g^{-1}} \in \Sigma$ for all $\delta \in \Sigma$), which implies that $(b^g, 1) \in M$. Clearly we then have that $W_{\alpha_\gamma} \leq MG' \leq W$. Let $h \in H \setminus H_\gamma$, and define $b \in B$ by

$$\delta b := \begin{cases} 1 & \text{if } \delta \in \Sigma, \\ h & \text{otherwise.} \end{cases}$$

Then $(b,1) \in MG' \setminus W_{\alpha_\gamma}$. Moreover, $(b_h, 1) \in W \setminus MG'$. Thus $W_{\alpha_\gamma} < MG' < W$.

Lastly, suppose that Δ is infinite, and let

$$N := \{(b,1) \in W : \delta b = 1 \text{ for all but finitely many } \delta \in \Delta\}.$$

Let $(n,1) \in N$. Then for all $(b,g) \in W$,

$$(b,g)^{-1}(n,1)(b,g) = ((b^{-1})^g, g^{-1})(nb, g) = ((b^{-1})^g (nb)^g, 1) = ((b^{-1}nb)^g, 1).$$

g^{-1} permutes the elements of Δ so $\delta^{g^{-1}} n = 1$ almost always, and if $\delta^{g^{-1}} n = 1$, then $\delta(b^{-1}nb)^g = (\delta^{g^{-1}} b)^{-1}(\delta^{g^{-1}} n)(\delta^{g^{-1}} b) = 1$, so $\delta(b^{-1}nb)^g = 1$ almost always. This implies that $((b^{-1}nb)^g, 1) \in N$, so N is a normal subgroup of W. Then $W_{\alpha_\gamma} \leq W_{\alpha_\gamma} N \leq W$. Let $h \in H \setminus H_\gamma$. Choose $\delta_0 \in \Delta$ and define $b_0 \in B$ by

$$\delta b_0 := \begin{cases} h & \text{if } \delta = \delta_0, \\ 1 & \text{otherwise.} \end{cases}$$

Then clearly $(b_0, 1) \in W_{\alpha_\gamma} N \setminus W_{\alpha_\gamma}$. Now consider $(b_h, 1)$. If $(b_h, 1) \in W_{\alpha_\gamma} N$, then $(b_h, 1) = (b, g)(n, 1) = (bn^{g^{-1}}, g)$ for some $(b, g) \in W_{\alpha_\gamma}$ and $(n, 1) \in N$. Then $g = 1$, so $b_h = bn$. $\delta b \in H_\gamma$ for all $\delta \in \Delta$, so $\delta b \neq h$ for all $\delta \in \Delta$. But then $\delta n = \delta b^{-1} b_h = (\delta b)^{-1} h \neq 1$ for all $\delta \in \Delta$, so $(n, 1) \notin N$, a contradiction. Thus $(b_h, 1) \in W \setminus W_{\alpha_\gamma} N$.

Hence, if any of the conditions that Δ be finite, G be transitive on Δ, or H be primitive but not regular on Γ fail, then W is not primitive.

Suppose now that Δ is finite, G is transitive on Δ, and H is primitive but not regular on Γ. Let $\alpha, \beta \in \Omega$. For each $\delta \in \Delta$, we may choose $h_\delta \in H$ such that $(\delta\alpha)^{h_\delta} = \delta\beta$ since H is transitive on Γ. Define $b_{\alpha\beta} \in B$ by $\delta \mapsto h_\delta$. Then

$$\delta\alpha^{(b_{\alpha\beta}, 1)} = (\delta\alpha)^{\delta b_{\alpha\beta}} = (\delta\alpha)^{h_\delta} = \delta\beta$$

for all $\delta \in \Delta$, so $\alpha^{(b_{\alpha\beta},1)} = \beta$. Thus W is transitive on Ω.

Let U be such that $W_{\alpha_\gamma} < U \leq W$. To show that W is primitive, we must show that $U = W$. $W = B'G' = B'W_{\alpha_\gamma}$ since $G' \leq W_{\alpha_\gamma}$. Then $U = U \cap W = U \cap B'W_{\alpha_\gamma} = (U \cap B')W_{\alpha_\gamma}$. It follows that if $U \cap B' = W_{\alpha_\gamma} \cap B'$, then $U = W_{\alpha_\gamma} \cap B'W_{\alpha_\gamma} = W_{\alpha_\gamma}$, a contradiction, so there exists a $(b^*, 1) \in (U \cap B') \setminus (W_{\alpha_\gamma} \cap B')$. Then $(b^*, 1) \notin W_{\alpha_\gamma}$, so there exists a $\delta_0 \in \Delta$ with $\delta_0 b^* \notin H_\gamma$. H is primitive but not regular and Γ contains at least two elements, so by Proposition 2.1.5, H_γ is self-normalizing in H. Then there exists an $h \in H_\gamma$ where $(\delta_0 b^*)^{-1} h^{-1} (\delta_0 b^*) \notin H_\gamma$ (or else $\delta_0 b^*$ normalizes H_γ, which implies that $\delta_0 b^* \in H_\gamma$). Define $b_0 \in B$ by

$$\delta b_0 := \begin{cases} h & \text{if } \delta = \delta_0, \\ 1 & \text{otherwise.} \end{cases}$$

Then clearly $(b_0, 1) \in W_{\alpha_\gamma} \leq U$, so $([b^*, b_0], 1) \in U \cap B'$. $\delta_0[b^*, b_0] = [\delta_0 b^*, \delta_0 b_0] = [\delta_0 b^*, h] \notin H_\gamma$ since $h \in H_\gamma$ and $(\delta_0 b^*)^{-1} h^{-1} (\delta_0 b^*) \notin H_\gamma$. Thus we have that $H_\gamma < \langle \delta_0[b^*, b_0], H_\gamma \rangle \leq H$, but H is primitive, so $\langle \delta_0[b^*, b_0], H_\gamma \rangle = H$.

For each $\delta \in \Delta$, let $B_\delta := \{(b, 1) \in W : \delta' b = 1 \text{ for all } \delta' \neq \delta\} \leq W$. Moreover, I claim that $B_{\delta_0} \leq U$. Let $(b, 1) \in B_{\delta_0}$. $\delta_0 b \in H = \langle \delta_0[b^*, b_0], H_\gamma \rangle$, so $\delta_0 b = h_1(\delta_0[b^*, b_0])^{n_1} \cdots h_k(\delta_0[b^*, b_0])^{n_k}$ where for all $i \in \{1, \ldots, k\}$, $h_i \in H_\gamma$ and n_i is a nonnegative integer. For each $i \in \{1, \ldots, k\}$, define $b_i \in B$ by

$$\delta b_i := \begin{cases} h_i & \text{if } \delta = \delta_0, \\ 1 & \text{otherwise.} \end{cases}$$

Since $\delta[b^*, b_0] = 1$ for all $\delta \neq \delta_0$, $b = b_1[b^*, b_0]^{n_1} \cdots b_k[b^*, b_0]^{n_k}$. Then $(b, 1) \in U$ since $([b^*, b_0], 1) \in U$ and $(b_i, 1) \in W_{\alpha_\gamma} \leq U$ for all i. Hence, $B_{\delta_0} \leq U$, as desired.

Let $(b, 1) \in B_{\delta_0}$ and $(1, g) \in G'$. Then $(1, g)^{-1}(b, 1)(1, g) = (b^g, 1)$, and if $\delta \neq \delta_0^g$, then $\delta^{g^{-1}} \neq \delta_0$, so $\delta b^g = \delta^{g^{-1}} b = 1$ (as $(b, 1) \in B_{\delta_0}$). Thus $(1, g)^{-1}(b, 1)(1, g) \in B_{\delta_0^g}$. On the other hand, suppose that $(b, 1) \in B_{\delta_0^g}$. If $\delta \neq \delta_0$, then $\delta^g \neq \delta_0^g$, so $\delta b^{g^{-1}} = \delta^g b = 1$ (as $(b, 1) \in B_{\delta_0^g}$), and so $(b^{g^{-1}}, 1) \in B_{\delta_0}$, which implies that $(b, 1) = (1, g)^{-1}(b^{g^{-1}}, 1)(1, g) \in (1, g)^{-1} B_{\delta_0}(1, g)$. Thus $(1, g)^{-1} B_{\delta_0}(1, g) = B_{\delta_0^g}$ for all $g \in G$. But G is transitive on Δ, so for each $\delta \in \Delta$ there exists a $g_\delta \in G$ with $\delta_0^{g_\delta} = \delta$. Hence for all $\delta \in \Delta$,

$$B_\delta = B_{\delta_0^{g_\delta}} = (1, g_\delta)^{-1} B_{\delta_0}(1, g_\delta) \leq U$$

since $G' \leq U$ and $B_{\delta_0} \leq U$. But Δ is finite, so $B' = \prod_{\delta \in \Delta} B_\delta \leq U$, and thus $W = B'W_{\alpha_\gamma} \leq U$, as desired. □

The next set of propositions give a very precise description of the socle of a finite primitive permutation group.

Proposition 2.1.7 ([14]). *Let G be a finite primitive permutation group on Ω. Then G has at most two minimal normal subgroups.*

Proof. If G is trivial, then G has no minimal normal subgroups, and we are done. Let J be a minimal normal subgroup of G. If $C_G(J) = \{1\}$, then J is the unique minimal normal subgroup of G since if K is another minimal normal subgroup of G, then $K \leq C_G(J) = \{1\}$, a contradiction.

Suppose then that $C_G(J)$ is not trivial. Since G is primitive and $C_G(J)$ is normal in G, $C_G(J)$ is transitive, so $C_{S^\Omega}(J)$ is transitive. Then by Proposition 1.2.1, J is semiregular. Similarly, J is transitive, so by Proposition 1.2.1, $C_{S^\Omega}(J)$ is semiregular, which implies that $C_G(J)$ is also semiregular. Thus both J and $C_G(J)$ are regular. Let K be a nontrivial normal subgroup of G contained in $C_G(J)$. Since K is nontrivial and normal in G, it is transitive, but K is contained in a semiregular group, so it is also semiregular, hence regular. Then both K and $C_G(J)$ are isomorphic to Ω, so $K = C_G(J)$, which implies that $C_G(J)$ is a minimal normal subgroup of G. Now, if L is any minimal normal subgroup of G that is different from J, then $L \leq C_G(J)$, but $C_G(J)$ is minimal normal so $L = C_G(J)$. Thus G has minimal normal subgroups J and $C_G(J)$ (where J and $C_G(J)$ may be equal). Hence in all cases, G has at most two minimal normal subgroups. □

Proposition 2.1.8 ([8, p. 114]). *If G is a finite nontrivial primitive permutation group on Ω, then one of the following holds:*

(i) G has exactly one minimal normal subgroup J where J is a regular elementary abelian p-group for some prime p;

(ii) G has exactly one minimal normal subgroup J where $C_G(J) = \{1\}$;

(iii) G has exactly two minimal normal subgroups J and $C_G(J)$, which are permutation isomorphic, nonabelian and regular.

Proof. Following the proof of Proposition 2.1.7, if $C_G(J) = \{1\}$, then we are in case (ii). If $C_G(J) \neq \{1\}$, then we have regular minimal normal subgroups J and $C_G(J)$. Note that $J = C_G(J)$ if and only if J is abelian: if $J = C_G(J)$, then clearly J is abelian; on the other hand, if J is abelian, then $J \leq C_G(J)$, and so $J = C_G(J)$ since $C_G(J)$ is minimal normal. So if $J = C_G(J)$, then we are in case (i) by Proposition 1.7.2 as an abelian group is solvable. If $J \neq C_G(J)$, then J is nonabelian. J is regular, so J is permutation isomorphic to $C_{S^\Omega}(J)$ by Proposition 1.2.6, hence to $C_G(J)$ as $C_G(J) \leq C_{S^\Omega}(J)$ and both are regular. Then $C_G(J)$ is also nonabelian, and we are in case (iii). □

Note that in case (ii), J may or may not be regular.

Theorem 2.1.9 ([14]). *The socle of a finite nontrivial primitive permutation group G on Ω is isomorphic to T^k for some simple group T and some positive integer k.*

Proof. If we are in case (i) or (ii) of Proposition 2.1.8, then the result follows from Corollary 1.5.5. Suppose that we are in case (iii). Then $soc(G) = \langle J, C_G(J)\rangle = J \times C_G(J)$. But J is permutation isomorphic to $C_G(J)$, so the result follows again from Corollary 1.5.5. □

I conclude this section with some useful results about primitive permutation groups.

Proposition 2.1.10. *Let G be a finite primitive permutation group with a nonabelian socle. Then $C_G(soc(G)) = \{1\}$.*

Proof. Let $M := soc(G)$. $M \simeq T^k$ for some $k \geq 1$ and some nonabelian simple group T by Theorem 2.1.9, so $C_G(M) = \{1\}$ by Proposition 1.5.6. □

Proposition 2.1.11 ([8, p. 115])**.** *Let G be a finite nontrivial primitive permutation group on Ω. Then $soc(G)$ is a minimal normal subgroup of $N_{S^\Omega}(soc(G))$.*

Proof. Let $M := soc(G)$. Of course M is normal in $N := N_{S^\Omega}(M)$ and $G \leq N$. First suppose that M is minimal normal in G. Let K be a nontrivial normal subgroup of N contained in M. Then $K \trianglelefteq G$, so $K = M$. Thus M is a minimal normal subgroup of N.

Suppose now that M is not a minimal normal subgroup of G. Then $M = J \times C_G(J)$ where J and $C_G(J)$ are the regular distinct minimal normal subgroups of G by Proposition 2.1.8. Since J is transitive and $J \leq C_G(C_G(J))$, $C_G(C_G(J))$ is transitive. Since $C_G(J)$ is also transitive, it follows from Proposition 1.2.1 that $C_G(C_G(J))$ is semiregular hence regular. Then $C_G(C_G(J)) = J$ since J is also regular. Moreover, we know that J is permutation isomorphic to $C_G(J)$, so by Proposition 1.2.4, $C_G(J) = n^{-1}Jn$ for some $n \in S^\Omega$. It is then routine to verify that $n^{-1}C_G(J)n$ centralizes $n^{-1}Jn$ since $C_G(J)$ centralizes J. Summarizing, we have that $C_G(J) = n^{-1}Jn$ for some $n \in S^\Omega$, $n^{-1}C_G(J)n \leq C_G(n^{-1}Jn)$ and $C_G(C_G(J)) = J$. Then

$$n^{-2}Jn^2 = n^{-1}(n^{-1}Jn)n = n^{-1}C_G(J)n \leq C_G(n^{-1}Jn) = C_G(C_G(J)) = J,$$

but $n^{-2}Jn^2$ and J have the same order, so $n^{-2}Jn^2 = J$. Replacing $n^{-1}Jn$ with $C_G(J)$, we have $n^{-1}C_G(J)n = J$, which implies that $n \in N$ since

$$n^{-1}Mn = n^{-1}Jn \times n^{-1}C_G(J)n = C_G(J) \times J = M.$$

Now, $M \simeq T^k$ for some $k \geq 1$ and some nonabelian simple group T by Theorem 2.1.9, so $J \simeq T^{\frac{k}{2}} \simeq C_G(J)$. By Proposition 1.5.2, G acts transitively on the $k/2$ factors of J and of $C_G(J)$, so N does as well. But then N acts transitively on all k factors of M since $n \in N$. Thus M is a minimal normal subgroup of N, again by Proposition 1.5.2. □

The following is constructed primarily for the proof of the O'Nan-Scott Theorem. Like Lemma 1.4.3, the formulation and proof of the lemma are mine, but its existence is implied by the proof of the O'Nan-Scott Theorem in [14].

Lemma 2.1.12. *Let G be a finite primitive permutation group on Ω, and let M be the socle of G where M is nonabelian. Let $\alpha \in \Omega$. Suppose that there exist groups $X_1, \ldots, X_n$ such that $M = X_1 \times \cdots \times X_n$ and $M_\alpha = (X_1)_\alpha \times \cdots \times (X_n)_\alpha$. Suppose that one of the following holds:*

(i) X_i is simple for all $i \in \{1, \ldots, n\}$;

(ii) $(X_i)_\alpha$ is a full diagonal subgroup of X_i for all $i \in \{1, \ldots, n\}$.

Then G_α acts transitively by conjugation on $\{X_1, \ldots, X_n\}$.

Proof. By Theorem 2.1.9, $M \simeq T^k$ for some nonabelian simple group T and some $k \geq 1$. So we may write $M = T_1 \times \cdots \times T_k$ where $T_i \simeq T$ for all i. Let $N := N_{S^\Omega}(M)$. In Proposition 2.1.11, we saw that M is a minimal normal subgroup of N, so N acts transitively by conjugation on $\{T_1, \ldots, T_k\}$. Moreover, N is primitive since $G \leq N$, so $N = N_\alpha M$. Thus N_α acts transitively on $\{T_1, \ldots, T_k\}$ (since $T_i \trianglelefteq M$ for all i). Both N_α and G_α normalize M and M_α, $M_\alpha = M \cap N_\alpha = M \cap G_\alpha$ and $(X_i)_\alpha = X_i \cap M_\alpha$ for all i, so the conditions of Lemma 1.4.3 with A taken to be N_α or G_α and K taken to be M_α are satisfied. Thus both N_α and G_α act by conjugation on $\{X_1, \ldots, X_n\}$ and $\{(X_1)_\alpha, \ldots, (X_n)_\alpha\}$. Moreover, if $a \in N_\alpha$ and $a^{-1}X_i a = X_j$, then $a^{-1}(X_i)_\alpha a = (X_j)_\alpha$, and if $(X_l)_\alpha$ is full diagonal for all l and $a^{-1}(X_i)_\alpha a = (X_j)_\alpha$, then $a^{-1}X_i a = X_j$. Lastly, note that N_α acts transitively on $\{X_1, \ldots, X_n\}$, hence on $\{(X_1)_\alpha, \ldots, (X_n)_\alpha\}$ since N_α acts transitively on $\{T_1, \ldots, T_k\}$. It follows in either case that if $(X_{i_0})_\alpha = X_{i_0}$ for some i_0, then $(X_i)_\alpha = X_i$ for all i, hence $M_\alpha = M$. However, this is a contradiction since M being a nontrivial transitive permutation group implies that $M_\alpha < M$. Thus $(X_i)_\alpha < X_i$ for all i.

(i) Suppose first that X_i is simple for all i. To show that G_α acts transitively on $\{X_1, \ldots, X_n\}$, it suffices to show that M is a minimal normal subgroup of G by Proposition 1.5.2 since $G = G_\alpha M$ and $X_i \trianglelefteq M$ for all i. Let U be a nontrivial normal subgroup of G contained in M. Then $U \trianglelefteq M = X_1 \times \cdots \times X_n$, so, rearranging the indices as needed, $U = X_1 \times \cdots \times X_s$ where $s \in \{1, \ldots, n\}$. Suppose that $s < n$ for a contradiction. Let $V := X_1 \times \cdots \times X_s \times (X_{s+1})_\alpha \times \cdots \times (X_n)_\alpha$. Then $M_\alpha < V < M$ since $(X_i)_\alpha < X_i$ for all i. Let $a \in G_\alpha$. Then a permutes $\{X_1, \ldots, X_s\}$ since $U \trianglelefteq G$, so a permutes $\{X_{s+1}, \ldots, X_n\}$, hence $\{(X_{s+1})_\alpha, \ldots, (X_n)_\alpha\}$ since $G_\alpha \leq N_\alpha$. But then $G_\alpha \leq N_G(V)$, so M_α is not a maximal G_α-invariant subgroup of M, contradicting the primitivity of G by Theorem 2.1.4. Thus $s = n$, so M is a minimal normal subgroup of G.

(ii) Suppose that $(X_i)_\alpha$ is full diagonal in X_i for all i. If G_α acts transitively by conjugation on $\{(X_1)_\alpha, \ldots, (X_n)_\alpha\}$, then G_α acts transitively on $\{X_1, \ldots, X_n\}$, so it suffices to show that M_α is a minimal normal subgroup of G_α since $(X_i)_\alpha$ is simple and nonabelian for all i. Let U be a nontrivial normal subgroup of G_α contained in M_α. Then $U \trianglelefteq (X_1)_\alpha \times \cdots \times (X_n)_\alpha$, so by Lemma 1.4.1, we have without loss of generality that $U =$

$(X_1)_\alpha \times \cdots \times (X_r)_\alpha$ where $r \in \{1, \ldots, n\}$. Suppose for a contradiction that $r < n$. Let $V := (X_1)_\alpha \times \cdots \times (X_r)_\alpha \times X_{r+1} \times \cdots \times X_n$. Then again $M_\alpha < V < M$ and $G_\alpha \leq N_G(V)$ since for $a \in G_\alpha$, $a^{-1}(X_i)_\alpha a = (X_j)_\alpha$ implies that $a^{-1}X_i a = X_j$. This contradicts the primitivity of G, so we must have that $r = n$ and $U = M_\alpha$, as desired. □

2.2 Affine Type

Let V be a vector space over a field F. Consider $GL(V)$ (the group of all automorphisms of V) as a permutation group on the set V. Let $v \in V$. Define $v^* \in S^V$ by $x \mapsto x + v$. v^* is clearly a bijection and is called a *translation*. Considering V as an additive group, define $\phi : V \to S^V$ by $v \mapsto v^*$. It is routine to verify that ϕ is a 1-1 group homomorphism. The image of ϕ, denoted by V^*, is called the *translation group of* V. Of course $V^* \cap GL(V) = \{1_V\}$ since only the trivial translation can be linear. Let $v^* \in V^*$ and $T \in GL(V)$. For all $x \in V$,

$$x(T^{-1}v^*T) = (xT^{-1} + v)T = xT^{-1}T + vT = x + vT = x(vT)^*,$$

so $T^{-1}v^*T = (vT)^* \in V^*$. Thus $GL(V)$ normalizes V^*, so we may define the *affine group* of V to be $V^* \rtimes GL(V) :=\mathrm{Aff}(V)$. Keep the identity $T^{-1}v^*T = (vT)^*$ in mind.

Let $v^*T \in \mathrm{Aff}(V)_0$. Then $0 = 0(v^*T) = (0 + v)T = vT$, so $v = 0$. Thus $v^*T = 0^*T = T \in GL(V)$. On the other hand, if $T \in GL(V)$, then of course $0T = 0$, so $T \in \mathrm{Aff}(V)_0$. Thus $\mathrm{Aff}(V)_0 = GL(V)$.

Note that V^* is transitive on V, for if $x, y \in V$, then $(y-x)^* \in V^*$ and $x(y-x)^* = x + y - x = y$. The additive group of V is abelian, so V^* is abelian. Thus $V^* \leq C_{S^V}(V^*)$. Since V^* is transitive, $C_{S^V}(V^*)$ is semiregular by Proposition 1.2.1, so V^* is also semiregular. Moreover, $C_{S^V}(V^*)$ is transitive since it contains V^*, so both V^* and $C_{S^V}(V^*)$ are regular. Thus $V^* = C_{S^V}(V^*)$.

Let V be a k-dimensional vector space over $\mathbb{F}_p$ where $k \geq 1$. In this case, we write $\mathrm{Aff}(k, p)$ for $\mathrm{Aff}(V)$; note that $\mathrm{Aff}(k, p) \simeq \mathbb{Z}_p^k \rtimes GL(k, p)$. Of course, if W is a subspace of V, then $W^* \leq V^*$, but it turns out that the opposite true. Let $H \leq V^*$ and define $W := \{v \in V : v^* \in H\}$. Clearly $0 \in W$ and if $v, w \in W$, then $(v + w)^* = v^*w^* \in H$ so $v + w \in W$. If $n \in \mathbb{F}_p$, then $(nv)^* = (v + \cdots + v)^* = v^* \cdots v^* = (v^*)^n \in H$ so $nv \in W$. Thus W is a subspace of V and $H = W^*$, so every subgroup of V^* has the form W^* for some subspace W of V when V is k-dimensional over $\mathbb{F}_p$.

A group G is said to be of *affine type* if $V^* \leq G \leq \mathrm{Aff}(k, p)$ and G is primitive for some k-dimensional vector space V over $\mathbb{F}_p$.

Let $U \leq GL(V)$ and W be a subspace of V. W is a *U-invariant* subspace of V if $(W)T = W$ for all $T \in GL(V)$. Of course V and $\{0\}$ are always U-invariant. U is an *irreducible* subgroup of $GL(V)$ if the only U-invariant subspaces of V are V and $\{0\}$.

Proposition 2.2.1. *Let $V^* \leq G \leq Aff(k, p)$ where $k \geq 1$. Then G is primitive if and only if $G \cap GL(V)$ is an irreducible subgroup of $GL(V)$.*

Proof. Since $\mathrm{Aff}(k,p)_0 = GL(V)$, $G_0 = G \cap GL(V)$. V^* is normal in G and transitive, so by Theorem 2.1.4, G is primitive if and only if $\{1_V\} = V_0^*$ (read as $(V^*)_0$) is a maximal G_0-invariant subgroup of V^*.

Suppose that $V_0^* = \{1_V\}$ is a maximal G_0-invariant subgroup of V^*. Let W be a nontrivial G_0-invariant subspace of V. Then W^* is a nontrivial subgroup of V^*. Let $T \in G_0$ and $w \in W$. Then $T^{-1}w^*T = (wT)^* \in W^*$ since W is G_0-invariant, so $G_0 \leq N_G(W^*)$. It follows that $W^* = V^*$, so $W = V$. Thus G_0 is an irreducible subgroup of $GL(V)$.

On the other hand, suppose that G_0 is an irreducible subgroup of $GL(V)$. Let H be a nontrivial G_0-invariant subgroup of V^*. Then $H = W^*$ where W is a nontrivial subspace of V. Let $T \in G_0$ and $w \in W$. Then $(wT)^* = T^{-1}w^*T \in H$ as $w^* \in H$ and H is G_0-invariant. Thus $wT \in W$, so W is a G_0-invariant subspace of V. Since G_0 is an irreducible subgroup of $GL(V)$, $W = V$. Thus $H = W^* = V^*$, so $V_0^* = \{1_V\}$ is a maximal G_0-invariant subgroup of V^*. □

Proposition 2.2.2. *Let G be of affine type. Then V^* is the unique minimal normal subgroup of G.*

Proof. Let N be a minimal normal subgroup of G. If $N \cap V^* = \{1_V\}$, then $N \leq C_G(V^*) = V^*$, a contradiction. Thus $N \cap V^*$ is not trivial, but it is a normal subgroup of G contained in N, so $N \cap V^* = N$, or $N \leq V^*$. Since G is primitive, N is transitive, but then N is regular since V^* is; it follows that $N = V^*$. Since V^* is then an abelian minimal normal subgroup of G, we are done by Proposition 2.1.8. □

Thus if G is of affine type, then G has regular socle $V^* \simeq V \simeq \mathbb{Z}_p^k$ where V^* is the unique minimal normal subgroup of G.

2.3 Twisted Wreath Type

Let P be a transitive permutation group on $\{1, \ldots, k\}$ where $k \geq 2$ and Q be the stabilizer of 1 in P. Suppose that we have a homomorphism $\varphi : Q \to Aut(T)$ for some simple nonabelian group T where $Inn(T) \leq Q\varphi$. Then φ is a group action of Q on T, so we may define $G := T\ twr_Q\ P = {}_QB \rtimes P$ where ${}_QB$ denotes the base group of the twisted wreath product. $P\backslash Q \simeq \{1, \ldots, k\}$ since P is transitive, so there are k cosets of Q in P. Let $\{1 = g_1, g_2, \ldots, g_k\}$ be a left transversal for Q in P.

Proposition 2.3.1. *In the notation given above, ${}_QB \simeq T^k$ and is the unique minimal normal subgroup of G.*

Proof. Recall from the end of Section 1.6 that ${}_QB = T_1 \times \cdots \times T_k$ where $T_i := \{b \in {}_QB : g_jb = 1 \text{ for all } j \neq i\} \simeq T$. ${}_QB \trianglelefteq G$, so G permutes $\{T_1, \ldots, T_k\}$. Let i and j be given,

and let $p := g_i g_j^{-1} \in P$. Let $b \in T_i$, and suppose that $l \neq j$. Note that if $g_i g_j^{-1} g_l \in g_i Q$, then $g_j^{-1} g_l \in Q$, so $l = j$. Thus $g_i g_j^{-1} g_l \notin g_i Q$, so

$$1 = (g_i g_j^{-1} g_l) b = (p g_l) b = g_l b^p.$$

Then $b^p \in T_j$, and since $(1,p)^{-1}(b,1)(1,p) = (b^p, 1)$, we get that $(1,p)^{-1} T_i (1,p) = T_j$. Thus G acts transitively by conjugation on $\{T_1, \ldots, T_k\}$, so ${}_Q B$ is a minimal normal subgroup of G by Proposition 1.5.2.

It suffices now to show that $C_G({}_Q B)$ is trivial. Let $(b,p) \in C_G({}_Q B)$. Fix $i \in \{1, \ldots, k\}$. Then $(b,p) \in C_G(T_i)$, so if $b_i \in T_i$, then

$$(b_i, 1) = (b,p)^{-1}(b_i, 1)(b,p) = ((b^{-1} b_i b)^p, 1),$$

which implies that if $j \neq i$, then

$$1 = g_j b_i = g_j (b^{-1} b_i b)^p = ((p g_j) b)^{-1} (g_j) b_i^p (p g_j) b.$$

Hence, $b_i^p \in T_i$. Then $(1,p)^{-1} T_i (1,p) = T_i^p \leq T_i$, so it follows that $T_i^p = T_i$; in particular, we may assume that there exists a $b_i \in T_i$ such that $b_i^p \neq 1_B$. But $b_i^p \in T_i$, so

$$1 \neq g_i b_i^p = (p g_i) b_i = (\overline{p g_i} b_i)^{q_{p g_i}}.$$

Then $1 \neq \overline{p g_i} b_i$, so $p g_i Q = g_i Q$. As i was arbitrary,

$$p \in \bigcap_{i=1}^{k} g_i Q g_i^{-1}.$$

Since P is transitive, every point stabilizer of P has the form $g_i Q g_i^{-1}$ for some i, but P is a permutation group and $k \geq 2$, so

$$\bigcap_{i=1}^{k} g_i Q g_i^{-1} = \{1\}.$$

Thus $p = 1$. Moreover, if $i \in \{1, \ldots, k\}$, then $b^{-1} b_i b = b_i$ for all $b_i \in T_i$. Let $t \in T$. Define $b_i \in T_i$ by $g_i b_i := t$ and $g_j b_i := 1$ for all $j \neq i$ (this is sufficient to define an element of ${}_Q B$ since $x b_i = (\overline{x} b_i)^{q_x}$ for all $x \in P$). Then $(g_i b)^{-1} t (g_i b) = t$ for all $t \in T$, so $g_i b \in Z(T) = \{1\}$. As i was arbitrary, b must also be the identity, and we are done. $\square$

Let $\Omega := G \backslash P$. Then G acts transitively on Ω. Define $\alpha := P \in \Omega$. Then $G_\alpha = P$. Let U be a normal subgroup of G contained in G_α. If U is not trivial, then it must contain ${}_Q B$ as ${}_Q B$ is the unique minimal normal subgroup of G, but then ${}_Q B \leq G_\alpha = P$, a contradiction. Thus G_α is a core-free subgroup of W, so the action is faithful.

G is said to be of *twisted wreath type* if G acts primitively on Ω. Since ${}_Q B_\alpha = {}_Q B \cap P = \{1\}$, the socle of a group of twisted wreath type is a regular unique minimal normal subgroup. Moreover, $|\Omega| = [G : P] = |T|^k$. Note that there are no simple conditions for G to be primitive.

2.4 Almost Simple Type

A finite group is *almost simple* if it is isomorphic to a group G for which $Inn(T) \leq G \leq Aut(T)$ for some nonabelian simple group T.

Proposition 2.4.1. *A finite group G is almost simple if and only if G has a simple nonabelian socle.*

Proof. Suppose that G is almost simple. Then $Inn(T) \leq H \leq Aut(T)$ for some group H isomorphic to G. $Inn(T)$ is simple and normal in $Aut(T)$, hence H, so $Inn(T)$ is a minimal normal subgroup of H. Since $C_H(Inn(T)) = \{1\}$ by Proposition 1.1.1, $Inn(T)$ is the socle of H by Proposition 1.5.6, so the socle of H is simple and nonabelian. Thus the socle of G is also simple and nonabelian.

On the other hand, suppose that G has a simple nonabelian socle, say T. Let $g \in G$ and define $\varphi_g \in Aut(T)$ to be conjugation by g. Define $\varphi : G \to Aut(T)$ by $g \mapsto \varphi_g$. If $g \in ker(\varphi)$, then $t = g^{-1}tg$ for all $t \in T$, so $g \in C_G(T) = \{1\}$ by Proposition 1.5.6. Thus φ is 1-1. Since φ is clearly a homomorphism and $Inn(T) = T\varphi$, we are done. □

A group G is said to be of *almost simple type* if G is a finite almost simple primitive permutation group. This is the only isomorphism class of the finite primitive permutation groups for which no group action will be identified.

This next result appears as part of the proof of the O'Nan-Scott Theorem in [14]. It requires the Schreier Conjecture (Theorem 1.10.2).

Proposition 2.4.2 ([14])**.** *If G is of almost simple type, then the socle of G is not regular.*

Proof. Suppose that G is of almost simple type. Then $soc(G) = T$ for some simple nonabelian group T, and by the proof of Proposition 2.4.1 we have an embedding φ of G into $Aut(T)$ where $T\varphi = Inn(T)$. Suppose that $\alpha \in \Omega$ where $G \leq S^\Omega$. Then T_α is normal in G_α since T is normal in G, so we can define $\psi : G_\alpha/T_\alpha \to Out(T)$ by $gT_\alpha \mapsto g\varphi Inn(T)$. Then for $g, h \in G_\alpha$, $gT_\alpha = hT_\alpha \iff g^{-1}h \in T \iff (g^{-1}h)\varphi \in Inn(T) \iff g\varphi Inn(T) = h\varphi Inn(T)$, so ψ is well-defined and 1-1. It is also clearly a homomorphism. But T is simple, so by the Schreier Conjecture, $Out(T)$ is solvable. Hence, G_α/T_α is solvable.

Suppose for a contradiction that $T_\alpha = \{1\}$. Then G_α is solvable. Let N be a minimal normal subgroup of G_α. Then by Proposition 1.7.2, N is an elementary abelian p-group for some prime p. $T_\alpha = \{1\} \leq C_T(N) < T$ since if $C_T(N) = T$, then $tn = nt$ for all $n \in N$ and $t \in T$, so $N \leq C_G(T) = \{1\}$ by Proposition 1.5.6, a contradiction. Moreover, G_α normalizes $C_T(N)$ since if $a \in G_\alpha$, $n \in N$ and $c \in C_T(N)$, then $ana^{-1} \in N$, so

$$(a^{-1}ca)^{-1}n(a^{-1}ca) = a^{-1}c^{-1}(ana^{-1})ca = a^{-1}(ana^{-1})a = n,$$

which implies that $a^{-1}ca \in C_G(N) \cap T = C_T(N)$ (as $T \trianglelefteq G$). But G is primitive, so by Theorem 2.1.4, $C_T(N) = T_\alpha = \{1\}$.

N acts on T by conjugation since $T \trianglelefteq G$. Let $t \in T$. Since N is a p-group and $|N| = |\theta_N(t)||N_t|$, either $|\theta_N(t)| = 1$ or $p \mid |\theta_N(t)|$. If $|\theta_N(t)| = 1$, then $n^{-1}tn = t$ for all $n \in N$, so $t \in C_T(N) = \{1\}$. Thus if $t \neq 1$, then $|\theta_N(t)| > 1$, which implies that $p \mid |\theta_N(t)|$ for all $t \neq 1$. It follows that $p \mid (|T| - 1)$, so $p \nmid |T|$. Suppose that $q \mid |T|$ where q is a prime. N acts by conjugation on the set of Sylow q-subgroups of T. If $|\theta_N(S)| > 1$ for every Sylow q-subgroup S, then $p \mid |\theta_N(S)|$ for every Sylow q-subgroup S, so $p \mid n_q$, but $n_q \mid |T|$, a contradiction. Thus there exists a Sylow q-subgroup S of T for which $n^{-1}Sn = S$ for all $n \in N$; that is, N normalizes S.

Suppose that N also normalizes S', another Sylow q-subgroup of T. We know that $S = t^{-1}S't$ for some $t \in T$. Since N is abelian, $N \leq C_G(N)$, but $C_G(N) \cap T = C_T(N) = \{1\}$, so $N \cap T = \{1\}$. Thus $|TN| = |T||N|$. Now, $N \leq TN \cap N_G(S) \leq TN$ and $p \nmid |T|$, so N is a Sylow p-subgroup of TN, hence of $TN \cap N_G(S) = N_{TN}(S)$. But $t^{-1}Nt \leq N_{TN}(S)$ since for all $n \in N$, $t^{-1}nt \in TN$ and $(t^{-1}nt)^{-1}S(t^{-1}nt) = t^{-1}n^{-1}(tSt^{-1})nt = t^{-1}(n^{-1}S'n)t = t^{-1}S't = S$; thus $t^{-1}Nt$ is also a Sylow p-subgroup of $N_{TN}(S)$, so there exists a $t' \in N_T(S)$ with $N = t'^{-1}(t^{-1}Nt)t'$. Then since $T \trianglelefteq G$, $[tt', N] \leq N \cap T = \{1\}$, which implies that $tt' \in C_T(N) = \{1\}$. Since $t' \in N_T(S)$, $t \in N_T(S)$, but then $t^{-1}St = S = t^{-1}S't$, so $S = S'$. Thus S is the only Sylow q-subgroup of T that is normalized by N.

Now I claim that $N_G(N) \leq N_G(S)$. Let $g \in N_G(N)$. If $n \in N$, then since $gng^{-1} \in N$ and N normalizes S,

$$g^{-1}Sg = g^{-1}(gng^{-1})^{-1}S(gng^{-1})g = n^{-1}(g^{-1}Sg)n.$$

Then N normalizes $g^{-1}Sg$, but $g^{-1}Sg$ is a Sylow q-subgroup of T (as $T \trianglelefteq G$ implies that $g^{-1}Sg \leq T$), so we must have that $S = g^{-1}Sg$ as S is the unique such Sylow q-subgroup. Thus $g \in N_G(S)$, as desired. Since N is normal in G_α, it follows that G_α normalizes S, so $G_\alpha \leq G_\alpha S \leq G$.

If $G_\alpha = G_\alpha S$, then $S \leq G_\alpha$, but $S \leq T$, so $S \leq T_\alpha = \{1\}$, a contradiction. If $G_\alpha S = G$, then

$$T = T \cap G = T \cap (G_\alpha S) = (T \cap G_\alpha)S = T_\alpha S = S,$$

so T is a q-group. This is a contradiction since $Z(T) = \{1\}$. Thus $G_\alpha < G_\alpha S < G$, contradicting the primitivity of G, so T must be regular. □

Thus if G is of almost simple type, then G has a nonregular simple nonabelian socle.

2.5 Diagonal Type

Let T be a nonabelian simple group and $k \geq 2$ an integer. Let

$$A := \{(a_1, \ldots, a_k) \in (Aut(T))^k : Inn(T)a_i = Inn(T)a_j \text{ for all } i, j \in \{1, \ldots, k\}\}.$$

Then $A \leq (Aut(T))^k$ since if $(a_1, \ldots, a_k), (b_1, \ldots, b_k) \in A$, then it is easy to see that $Inn(T)a_ib_i^{-1} = Inn(T)a_jb_j^{-1}$ for all $i, j \in \{1, \ldots, k\}$.

Let $W := A \rtimes S_k$ where $\pi \in S_k$ acts on $(a_1, \ldots, a_k) \in A$ by moving a_i to the $i\pi$-th coordinate. It is routine to verify that this defines an action on A. Notationally, we have that $(a_1, \ldots, a_k)^\pi = (a_{1\pi^{-1}}, \ldots, a_{k\pi^{-1}})$ since $a_{i\pi^{-1}}$ gets moved to the i-th coordinate. For notational ease, denote the elements of W by $(a_1, \ldots, a_k)\pi$ instead of $((a_1, \ldots, a_k), \pi)$.

Let $M := (Inn(T))^k \leq W$. Then $M \trianglelefteq W$ since $Inn(T) \trianglelefteq Aut(T)$. Let

$$T_i := \{(1, \ldots, a_i, \ldots, 1) \in W : a_i \in Inn(T)\}.$$

Then $T_i \simeq T$ for each $i \in \{1, \ldots, k\}$, and clearly $M = T_1 \times \cdots \times T_k$. Let $(a_1, \ldots, a_k)\pi \in W$. Then $((a_1, \ldots, a_k)\pi)^{-1}T_i(a_1, \ldots, a_k)\pi = T_{i\pi}$ for all $i \in \{1, \ldots, k\}$:

$$\begin{aligned}
& ((a_1, \ldots, a_k)\pi)^{-1}T_i(a_1, \ldots, a_k)\pi \\
= \; & (a_{1\pi^{-1}}^{-1}, \ldots, a_{k\pi^{-1}}^{-1})(a_1, \ldots, Inn(T)a_i, \ldots a_k)^\pi\pi^{-1}\pi \\
= \; & (1, \ldots, a_i^{-1}Inn(T)a_i, \ldots, 1) \qquad \text{(in } i\pi\text{-th spot)} \\
= \; & T_{i\pi}.
\end{aligned}$$

Let i and j be given. There exists a $\pi \in S_k \leq W$ with $i\pi = j$, so $\pi^{-1}T_i\pi = T_{i\pi}$. Then W acts transitively by conjugation on $\{T_1, \ldots, T_k\}$, so M is a minimal normal subgroup of W by Proposition 1.5.2. Moreover, let $g := (a_1, \ldots, a_k)\pi \in C_W(M)$. Then $g \in \bigcap_{i=1}^k C_W(T_i)$, so, in particular, $T_{i\pi} = g^{-1}T_ig = T_i$. Thus π is the identity, but then $a_i^{-1}aa_i = a$ for all $a \in Inn(T)$, so $a_i \in C_{Aut(T)}(Inn(T)) = \{1\}$ for all i. Hence, $C_W(M) = \{1\}$, so M is the unique minimal normal subgroup of W.

Let Ω be the right coset space $W\backslash D$ where $D := \{(a, \ldots, a)\pi \in W\} \simeq Aut(T) \times S_k$. Note that $|\Omega| \geq 2$, for if $D = W$, then $ab^{-1} \in Inn(T)$ implies that $a = b$, so if we take $a = 1_T$ and any $1_T \neq b \in Inn(T)$, then we get a contradiction. Of course W acts transitively on Ω. Let $\alpha := D \in \Omega$ so that $W_\alpha = D$. Since $M \trianglelefteq W$, $MW_\alpha \leq W$. Let $(a_1, \ldots, a_k)\pi \in W$. Then

$$(a_1, \ldots, a_k)\pi = (a_1a_1^{-1}, \ldots, a_ka_1^{-1})(a_1, \ldots, a_1)\pi \in MW_\alpha$$

since $a_ia_1^{-1} \in Inn(T)$ for all $i \in \{1, \ldots, k\}$. Thus $W = MW_\alpha$, so M is also transitive on Ω. Note that $M_\alpha = \{(a, \ldots, a) \in W : a \in Inn(T)\} \simeq T$, and let U be a normal subgroup of W contained in W_α. If U is not trivial, then it must contain M as M is the unique minimal normal subgroup of W, but then $M \leq W_\alpha$, so $M = M_\alpha$, which is a contradiction since $k \geq 2$. Thus W_α is a core-free subgroup of W, so the action is faithful.

A group G is said to be of *diagonal type* if $M \leq G \leq W$ and G is primitive. The term diagonal is used since M_α is a full diagonal subgroup of M and $\Omega \simeq M/M_\alpha$.

For $G \leq W$, let $P_G := \{\pi \in S_k : (a_1, \ldots, a_k)\pi \in G \text{ for some } (a_1, \ldots, a_k) \in A\} \leq S_k$.

Proposition 2.5.1 ([8, p. 123]). *Let G be a subgroup of W containing M. G is primitive on Ω if and only if P_G is primitive on $\{1,\dots,k\}$ or $P_G = \{1\}$ and $k = 2$.*

Proof. Suppose that $P := P_G$ is not primitive. If $P \neq \{1\}$, then $k \geq 3$ since if $k = 2$, then $P = S_2$, which is primitive, a contradiction. If we assume instead that $k \geq 3$, but $P = \{1\}$, then it is routine to verify that $T_1,\dots,T_k$ are all minimal normal subgroups of $A = G$, which implies that G is not primitive as a primitive G can have at most two minimal normal subgroups. Thus we may assume that $k \geq 3$ and $P \neq \{1\}$. Recall that $M \trianglelefteq G$ and M is transitive.

Since P is not primitive and is nontrivial, there exists a nontrivial P-congruence $\sim$ by Proposition 2.1.1. Let $L := \{(a_1,\dots,a_k) \in M : i \sim j \Rightarrow a_i = a_j\} \leq M$. Since $\sim$ is nontrivial there exist i and j such that $i \neq j$ but $i \sim j$. Let $a, b \in Inn(T)$ with $a \neq b$, and let $a_i := a$ and $a_l := b$ for $l \neq i$. Then $(a_1,\dots,a_k) \in M \setminus L$ since $i \sim j$ but $a_i = a \neq b = a_j$. Thus $L < M$. Again since $\sim$ is nontrivial, there exist i and j with $i \neq j$ and $i \nsim j$. If $[i]_\sim$ denotes the equivalence class of i, then $[i]_\sim < \Omega$. Let $a_l := a$ if $l \in [i]_\sim$ and $a_l := b$ if $l \notin [i]_\sim$. Then $(a_1,\dots,a_k) \in L \setminus M_\alpha$. Thus $M_\alpha < L$.

Let $(a_1,\dots,a_k) \in L$ and $(c,\dots,c)\pi \in G_\alpha$. Then

$$((c,\dots,c)\pi)^{-1}(a_1,\dots,a_k)(c,\dots,c)\pi = (c^{-1}a_{1\pi^{-1}}c,\dots,c^{-1}a_{k\pi^{-1}}c).$$

Suppose that $i \sim j$. Then $i\pi^{-1} \sim j\pi^{-1}$ since $\sim$ is a P-congruence, so $a_{i\pi^{-1}} = a_{j\pi^{-1}}$. Thus $(c^{-1}a_{1\pi^{-1}}c,\dots,c^{-1}a_{k\pi^{-1}}c) \in L$, so $G_\alpha \leq N_G(L)$. But $M_\alpha < L < M$, so by Theorem 2.1.4, G is not primitive.

Suppose on the other hand that G is not primitive. Then by Theorem 2.1.4, there exists an $L \leq G$ such that $M_\alpha < L < M$ and $G_\alpha \leq N_G(L)$. Let ρ_i be the i-th projection map from L to $Inn(T)$ for each $i \in \{1,\dots,k\}$, and let $L_i := ker(\rho_i)$ for each $i \in \{1,\dots,k\}$. Define $\sim$ on $\{1,\dots,k\}$ by $i \sim j$ if and only if $L_i = L_j$. Then $\sim$ is clearly an equivalence relation.

Let $\pi \in P$. Then there exists a k-tuple $(a_1,\dots,a_k) \in A$ with $(a_1,\dots,a_k)\pi^{-1} \in G$. The element $(a_1a_1^{-1},\dots,a_ka_1^{-1}) \in M \leq G$ and

$$(a_1,\dots,a_k)\pi^{-1} = (a_1a_1^{-1},\dots,a_ka_1^{-1})(a_1,\dots,a_1)\pi^{-1},$$

so letting $a := a_1$, we get that $g := (a,\dots,a)\pi^{-1} \in G_\alpha \leq N_G(L)$. Thus if $l := (l_1,\dots,l_k) \in L$, then $(a^{-1}l_{1\pi}a,\dots,a^{-1}l_{k\pi}a) = g^{-1}lg \in L$. It follows that $l \in L_{i\pi} \iff l_{i\pi} = 1 \iff a^{-1}l_{i\pi}a = 1 \iff g^{-1}lg \in L_i$. Now, if $L_i = L_j$, then $l \in L_{i\pi} \iff g^{-1}lg \in L_i = L_j \iff l \in L_{j\pi}$, so $L_{i\pi} = L_{j\pi}$. Conversely, if $L_{i\pi} = L_{j\pi}$, then $l \in L_i \iff glg^{-1} \in L_{i\pi} = L_{j\pi} \iff l \in L_j$, so $L_i = L_j$. Thus $L_i = L_j$ if and only if $L_{i\pi} = L_{j\pi}$. That is, $i \sim j$ if and only if $i\pi \sim j\pi$, so $\sim$ is a P-congruence.

If $a \in Inn(T)$, then $(a,\dots,a) \in M_\alpha < L$ and $(a,\dots,a)\rho_i = a$, so ρ_i is onto $Inn(T)$ for all i. Then $L/L_i \simeq Inn(T)$, so L/L_i is simple for all i. Clearly $\bigcap_{i=1}^k L_i = \{1\}$,

so if the L_i are all distinct, then by Lemma 1.4.4, $L \simeq (Inn(T))^k = M$, contradicting $L < M$. Moreover, if the L_i are all the same group, then $L_1 = \bigcap_{i=1}^k L_i = \{1\}$. But then $M_\alpha \simeq Inn(T) \simeq L/L_1 \simeq L$, contradicting $M_\alpha < L$. Thus $\sim$ must be nontrivial.

Hence, $\sim$ is a nontrivial P-congruence on $\{1, \ldots, k\}$. If $k = 2$, then every P-congruence is trivial, so $k \geq 3$. If P is not transitive, then P is not primitive. If P is transitive, then since we have a nontrivial P-congruence, P is not primitive by Proposition 2.1.2. Thus in either case, $k \geq 3$ and P is not primitive. □

Note that since $P_W = S_k$ and S_k is primitive for all $k \geq 2$, W itself is of diagonal type.

Proposition 2.5.2. *Let G be a group of diagonal type. Then G has socle M. Moreover, if P_G is primitive on $\{1, \ldots, k\}$, then M is the unique minimal normal subgroup of G, and if $P_G = \{1\}$ and $k = 2$, then G has two minimal normal subgroups.*

Proof. $C_G(M) \leq C_W(M) = \{1\}$, so M is the socle of G. Suppose that P_G is primitive on $\{1, \ldots, k\}$. Let i and j be given. Since P_G is primitive, P_G is transitive, so there exists a $\pi \in P_G$ with $i\pi = j$. Then $(a_1, \ldots, a_k)\pi \in G$ for some $(a_1, \ldots, a_k) \in A$, and

$$((a_1, \ldots, a_k)\pi)^{-1} T_i (a_1, \ldots, a_k)\pi = T_{i\pi} = T_j.$$

Thus G acts transitively by conjugation on $\{T_1, \ldots, T_k\}$, so $M = T_1 \times \cdots \times T_k$ is a minimal normal subgroup of G, hence is the only one. Suppose then that $P_G = \{1\}$ and $k = 2$. In this case, it is easy to see that T_1 and T_2 are both minimal normal subgroups of $A = G$. □

Thus G has nonregular nonabelian socle $Inn(T)^k$, which is either a minimal normal subgroup of G or consists of two regular minimal normal subgroups T_1 and T_2. Also, $|\Omega| = [M : M_\alpha] = |T|^{k-1}$.

The following is not really needed but is interesting.

Proposition 2.5.3. *W is an extension of M by $Out(T) \times S_k$.*

Proof. Define $\psi : W \to Out(T) \times S_k$ by $(a_1, \ldots, a_k)\pi \mapsto (Inn(T)a_1, \pi)$. Then for all $(a_1, \ldots, a_k)\pi, (a'_1, \ldots, a'_k)\pi' \in W$,

$$\begin{aligned}
(a_1, \ldots, a_k)\pi\psi(a'_1, \ldots, a'_k)\pi'\psi &= (Inn(T)a_1a'_1, \pi\pi') \\
&= (Inn(T)a_1a'_{1\pi}, \pi\pi') \\
&= (a_1a'_{1\pi}, \ldots, a_ka'_{k\pi})\pi\pi'\psi \\
&= ((a_1, \ldots, a_k)\pi(a'_1, \ldots, a'_k)\pi')\psi,
\end{aligned}$$

so ψ is a homomorphism. To see that ψ is onto, let $(Inn(T)a, \pi) \in Out(T) \times S_k$. Then $(a, \ldots, a)\pi \in W$ and $(a, \ldots, a)\pi\psi = (Inn(T)a, \pi)$. Lastly, let $(a_1, \ldots, a_k)\pi \in ker(\psi)$. Then π is the identity of S_k, and $a_1 \in Inn(T)$. But then $a_i \in Inn(T)$ for all $i \in \{1, \ldots, k\}$, so $(a_1, \ldots, a_k)\pi \in M$. Conversely, if $(a_1, \ldots, a_k) \in M$, then clearly $(a_1, \ldots, a_k) \in ker(\psi)$. Thus $ker(\psi) = M$, so $W/M \simeq Out(T) \times S_k$. □

It follows that if G is of diagonal type, then G is an extension of M by a subgroup of $Out(T) \times P_G$ and G_α is isomorphic to a subgroup of $Aut(T) \times P_G$.

Last of all, I prove that we essentially cannot make W any larger. This result is taken from [8, p. 122], but the proof is somewhat different because [8] constructs groups of diagonal type differently (although analogously).

Proposition 2.5.4. $W^\Omega = N_{S^\Omega}(M^\Omega)$.

Proof. Identify W with W^Ω for simplicity. Since $M \trianglelefteq W$, $W \leq N_{S^\Omega}(M) =: N$. Let $n \in N$. Define $\theta_n \in Aut(M)$ by $m \mapsto n^{-1}mn$. Note that $M_\alpha\theta_n = n^{-1}M_\alpha n = M_{\alpha n}$. But M is transitive on Ω, so there exists an $m \in M$ with $\alpha n = \alpha m$. Then $M_\alpha\theta_n = m^{-1}M_\alpha m$. Define $\theta : N \to Aut(M)$ by $n \mapsto \theta_n$. Then N is clearly a homomorphism with kernel $C_{S^\Omega}(M)$. Suppose that $C_{S^\Omega}(M) \neq \{1\}$. $C_{S^\Omega}(M) \trianglelefteq N_{S^\Omega}(M)$, which is primitive since it contains W, so $C_{S^\Omega}(M)$ is transitive. Then M is semiregular by Proposition 1.2.1, a contradiction. Thus $C_{S^\Omega}(M) = \{1\}$, so N is embedded into $Aut(M)$. Now, $Inn(T)^k \simeq T^k$, so $Aut(M) \simeq Aut(T^k)$. In the proof of Proposition 1.6.1, we saw that every element of $Aut(T^k)$ has the form $\psi_{(a_1,\ldots,a_k)\pi}$ for some $(a_1,\ldots,a_k)\pi \in Aut(T)^k \rtimes S_k$. Let $\psi_{(a_1,\ldots,a_k)\pi}$ be the image of θ_n and let $U := \{(t,\ldots,t) : t \in T\}$. Then $U\psi_{(a_1,\ldots,a_k)\pi} = (t_1,\ldots,t_k)^{-1}U(t_1,\ldots,t_k)$ for some $(t_1,\ldots,t_k) \in T^k$ since $M_\alpha\theta_n = m^{-1}M_\alpha m$.

Let $t \in T$. Since $(t,\ldots,t) \in U$, there exists a k-tuple $(t',\ldots,t') \in U$ such that

$$\begin{aligned}(t_1,\ldots,t_k)^{-1}(t',\ldots,t')(t_1,\ldots,t_k) &= (t,\ldots,t)\psi_{(a_1,\ldots,a_k)\pi} \\ &= (ta_{1\pi^{-1}},\ldots,ta_{k\pi^{-1}}).\end{aligned}$$

Then $ta_i = t_{i\pi}^{-1}t't_{i\pi}$ for all i, so $t_{i\pi}(ta_i)t_{i\pi}^{-1} = t' = t_{j\pi}(ta_j)t_{j\pi}^{-1}$ for all i and j. Rewriting, we get that $ta_i = t_{i\pi}^{-1}t_{j\pi}(ta_j)t_{j\pi}^{-1}t_{i\pi}$. Since a_j is an isomorphism,

$$ta_ia_j^{-1} = ((t_{j\pi}^{-1}t_{i\pi})a_j^{-1})^{-1}t((t_{j\pi}^{-1}t_{i\pi})a_j^{-1}),$$

but $(t_{j\pi}^{-1}t_{i\pi})a_j^{-1} \in T$ and t was arbitrary, so $a_ia_j^{-1} \in Inn(T)$. Then since $Aut(T^k) \simeq Aut(T)^k \rtimes S_k$, we can embed N into $Aut(T)^k \rtimes S_k$ where the image of $n \in N$ is some $(a_1,\ldots,a_k)\pi$ for which $a_ia_j^{-1} \in Inn(T)$ for all i and j. That is, the image of N in $Aut(T)^k \rtimes S_k$ is contained in W. Thus $W = N_{S^\Omega}(M)$. □

2.6 Product Type

Let $\Delta := \{1,\ldots,n\}$ where $n > 1$, and let H be a primitive permutation group on Γ where H is of almost simple type or diagonal type. Define $W := H\ wr_\Delta\ S_n$. Since $W \simeq H^n \rtimes S_n$, we may write the elements of W as $(h_1,\ldots,h_n)\pi$ where $h_i \in H$ for all $i \in \{1,\ldots,n\}$ and $\pi \in S_n$. Then the product action of W on $\Omega = \Gamma^n$ (instead of Γ^Δ) becomes

$$(\gamma_1,\ldots,\gamma_n)^{(h_1,\ldots,h_n)\pi} = (\gamma_{1\pi^{-1}}^{h_{1\pi^{-1}}},\ldots,\gamma_{n\pi^{-1}}^{h_{n\pi^{-1}}}).$$

This action is faithful by Proposition 1.6.2 since Γ must contain at least two elements (or else $H = \{1\}$, which cannot be) and since S_n and H are both permutation groups on Δ and Γ respectively.

Let $\gamma \in \Gamma$, and let $\alpha := (\gamma, \ldots, \gamma) \in \Omega$. Suppose that $(h_1, \ldots, h_n)\pi \in W_\alpha$. Then

$$(\gamma, \ldots, \gamma) = (\gamma, \ldots, \gamma)^{(h_1, \ldots, h_n)\pi} = (\gamma^{h_{1\pi^{-1}}}, \ldots, \gamma^{h_{n\pi^{-1}}}),$$

so $h_i \in H_\gamma$ for all i; that is, $(h_1, \ldots, h_n)\pi \in H_\gamma^n \rtimes S_n = H_\gamma \; wr_\Delta \; S_n$. It is not hard to see then that $W_\alpha = H_\gamma \; wr_\Delta \; S_n$.

Suppose that H has socle K. Let $M := K^n$. Then

$$M_\alpha = W_\alpha \cap K^n = (H_\gamma^n \rtimes S_n) \cap K^n = H_\gamma^n \cap K^n = K_\gamma^n.$$

Note that since H is of almost simple type or diagonal type, K is not regular (see Proposition 2.4.2), so H is not regular in either case. Then since Δ is finite, S_n is transitive on Δ, and H is primitive but not regular on Γ, W is a primitive permutation group by Proposition 2.1.6. Since $K \trianglelefteq H$, $M \trianglelefteq W$. Thus M is transitive on Ω.

For each $i \in \{1, \ldots, n\}$, let $K_i := \{(1, \ldots, k, \ldots, 1) \in W : k \in K\}$, where each $k \in K$ is in the i-th coordinate. As we saw for groups of diagonal type, if $(h_1, \ldots, h_n)\pi \in W$, then $((h_1, \ldots, h_n)\pi)^{-1} K_i (h_1, \ldots, h_n)\pi = K_{i\pi}$. Thus W acts on $\{K_1, \ldots, K_n\}$ by conjugation.

Proposition 2.6.1. *If $M \leq G \leq W$, then M is the socle of G.*

Proof. Let $g := (h_1, \ldots, h_n)\pi \in C_G(M)$. Then $g \in \bigcap_{i=1}^n C_G(K_i)$, so $K_{i\pi} = g^{-1} K_i g = K_i$ for all $i \in \{1, \ldots, n\}$. Thus π is the identity. But then $g = (h_1, \ldots, h_n) \in \bigcap_{i=1}^n C_G(K_i)$, so for all $i \in \{1, \ldots, n\}$, $h_i \in C_H(K)$, which is trivial by Proposition 2.1.10 as K is the nonabelian socle of primitive H. Then g is the identity, so $C_G(M) = \{1\}$. Thus M is the socle of G by Proposition 1.5.6. □

A group G is said to be of *product type* if $M \leq G \leq W$ and G is primitive. When H is of almost simple type or diagonal type, G is said to be of *almost simple product type* or *diagonal product type* respectively.

Proposition 2.6.2. *If G is of product type, then G acts transitively on $\{K_1, \ldots, K_n\}$ by conjugation.*

Proof. Suppose that G is of product type. Note that $M = K_1 \times \cdots \times K_n$ and $M_\alpha = K_\gamma \times \cdots \times K_\gamma = (M_\alpha \cap K_1) \times \cdots \times (M_\alpha \cap K_n) = (K_1)_\alpha \times \cdots \times (K_n)_\alpha$. Moreover, either K_i is simple for all i or $(K_i)_\alpha$ is a full diagonal subgroup of K_i for all i, so by Lemma 2.1.12, G acts transitively on $\{K_1, \ldots, K_n\}$ by conjugation. □

According to [14, p. 391], the converse of Proposition 2.6.2 is also true for a group G such that $M \leq G \leq W$, but I was unable to prove it. Fortunately, it has no bearing on the proof of the O'Nan-Scott Theorem.

The next result tells us when a group of product type has one or two minimal normal subgroups. I was unable to prove (iii), but again, this result has no bearing on the proof of O'Nan-Scott and is included here because it is interesting. Recall that when H is of diagonal type, either $P_H = \{1\}$ or P_H is primitive.

Proposition 2.6.3 ([14, p. 391])**.** *Let G be a group of product type.*

(i) If H is of almost simple type, then M is the unique minimal normal subgroup of G.

(ii) If H is of diagonal type and $P_H = \{1\}$, then G has two minimal normal subgroups.

(iii) If H is of diagonal type and P_H is primitive, then M is the unique minimal normal subgroup of G.

Proof. (i) Suppose that H is of almost simple type. Then K is a nonabelian simple group. Since G acts transitively on $\{K_1, \ldots, K_n\}$, all of which are nonabelian and simple, $M = K_1 \times \ldots \times K_n$ is a minimal normal subgroup of G by Proposition 1.5.2, and we are done.

(ii) Suppose that H is of diagonal type where $P_H = \{1\}$. Then $H \leq \{(a_1, a_2) \in Aut(T) \times Aut(T) : Inn(T)a_1 = Inn(T)a_2\}$ for some simple nonabelian group T, so $K = Inn(T) \times Inn(T)$. Let

$$N_1 := \{((a_1, 1), \ldots, (a_n, 1)) : a_i \in Inn(T) \text{ for all } i\}.$$

Define N_2 similarly, so that $M = N_1 \times N_2$. It is routine to verify that N_1 and N_2 are normal subgroups of G. For $i \in \{1, \ldots, n\}$ and $j \in \{1, 2\}$, let $T_{i,j}$ be the set of all elements of K_i of the form $((1, 1), \ldots, (a_1, a_2), \ldots, (1, 1))$ where $a_l = 1$ if $l \neq j$. Then $K_i = T_{i,1} \times T_{i,2}$ and $N_j = T_{1,j} \times \cdots \times T_{n,j}$. Since G is transitive on $\{K_1, \ldots, K_n\}$, given $i, l \in \{1, \ldots, n\}$, there exists a $g \in G$ with $g^{-1}K_i g = K_l$. But then $g^{-1}T_{i,j}g = T_{l,j}$ for $j = 1, 2$ (as $P_H = \{1\}$), so G acts transitively on the simple factors of N_1 and N_2; that is, N_1 and N_2 are both minimal normal subgroups of G. □

Thus if G is of product type, then G has a nonabelian nonregular socle K^n where K is the socle of H. K^n is either a nonregular unique minimal normal subgroup of G or is the direct product of two regular minimal normal subgroups of G. Also, $|\Omega| = |\Gamma|^n$.

2.7 The O'Nan-Scott Theorem

Note that the five types described above are all pairwise disjoint: groups of affine type are the only ones with an abelian socle, groups of twisted wreath type are the only ones with

a regular nonabelian unique minimal normal subgroup, and groups of almost simple type are the only ones with a simple nonabelian socle. It remains to show that a group cannot be of diagonal and product type.

Suppose that G is of diagonal and product type, where G has socle T^k ($k \geq 2$) for some nonabelian simple group T. Then, using the notation from the diagonal and product types, $G \leq A \rtimes S_k$ and $G \leq H \ wr_\Delta \ S_n$ for some $n \geq 2$. Since the socle of G is also K^n, where K is the socle of H, H has socle $T^{\frac{k}{n}}$. If H is of almost simple type, then $K \simeq T$, so $k = n$. Also $H \leq Aut(T)$. Then T^k has point stabilizers $\{(a, \ldots, a) : a \in Inn(T)\}$ and $\{(h_1, \ldots, h_k) : h_i \in Inn(T)_\gamma\}$, which must be permutation isomorphic in S^Ω, hence conjugate in S^Ω by Proposition 1.2.4. Then there exists a $\sigma \in S^\Omega$ with $(\sigma^{-1}a\sigma, \ldots, \sigma^{-1}a\sigma) = \sigma^{-1}(a, \ldots, a)\sigma = (h_1, \ldots, h_k)$ for all $a \in Inn(T)$ and $h_i \in Inn(T)_\gamma$, which is clearly not so. If H is of diagonal type (acting on Γ), then $|\Gamma| = |T|^{\frac{k}{n}-1}$. But then $(|T|^{\frac{k}{n}-1})^n = |\Gamma|^n = |\Omega| = |T|^{k-1}$ since G is of diagonal type, so $k - n = k - 1$, or $n = 1$, a contradiction.

Typically, questions about finite permutation groups can be reduced via the O'Nan-Scott Theorem to the almost simple case. It is this isomorphism class which is the most difficult to work with. Now that the classification of the finite simple groups is complete, it is hoped that the properties of almost simple groups will become more clear. See [1] for details.

At last we have reached the main result of this thesis.

Theorem 2.7.1 (O'Nan, Scott)**.** *Let G be a nontrivial finite primitive permutation group on Ω. Then G is permutation isomorphic to a group that is either of affine type, twisted wreath type, almost simple type, diagonal type, or product type.*

The proof of the O'Nan-Scott Theorem is broken down into several propositions. So for this section, let G be a nontrivial finite primitive permutation group on Ω, and let M be the socle of G. Then M is isomorphic to T^k for some simple group T and some positive integer k by Theorem 2.1.9. Write $M = T_1 \times \cdots \times T_k$ where $T_i \simeq T$ for all $i \in \{1, \ldots, k\}$. Let $\alpha \in \Omega$. Note that since G is primitive and nontrivial, G_α is a maximal subgroup of G and M_α is a maximal G_α-invariant subgroup of M by Theorem 2.1.4. In particular, $G = MG_\alpha$ since the transitivity of M implies that $G_\alpha < MG_\alpha \leq G$. Also, $M_\alpha < M$ since M is transitive and Ω is nontrivial.

Proposition 2.7.2 ([19, p. 200])**.** *Suppose that T is abelian. Then G is permutation isomorphic to a group of affine type.*

Proof. Since T is abelian, G must have a unique minimal normal subgroup by Proposition 2.1.8, namely, M. Moreover, M is an elementary abelian p-group for some prime p, and M is regular, so if $|M| = p^k$, then $|\Omega| = p^k$. Let V be a vector space of dimension k over the field $\mathbb{F}_p$.

Let $\theta : M \to V$ be a $\mathbb{Z}$-isomorphism (which must exist since $M \simeq \mathbb{Z}_p^k \simeq V$, where we consider the additive group of V). Note that $G = M \rtimes G_\alpha$ since $M \cap G_\alpha = M_\alpha = \{1\}$, so every element of G can be written uniquely in the form ma where $m \in M$ and $a \in G_\alpha$. Define $\phi_a : M \to M$ by $m \mapsto a^{-1}ma$. Then ϕ_a is a bijection.

Define $\psi : G \to \mathrm{Aff}(k,p) = V^* \rtimes GL(k,p)$ by $ma \mapsto (m\theta)^*(\theta^{-1}\phi_a\theta)$. Clearly $\theta^{-1}\phi_a\theta$ is a bijection which maps from V onto V for all $a \in G_\alpha$. Let $x, y \in V$. Then

$$\begin{aligned}
(x+y)\theta^{-1}\phi_a\theta &= (x\theta^{-1}y\theta^{-1})\phi_a\theta && (\theta^{-1} \text{ homomorphism}) \\
&= (a^{-1}x\theta^{-1}aa^{-1}y\theta^{-1}a)\theta \\
&= (a^{-1}x\theta^{-1}a)\theta + (a^{-1}y\theta^{-1}a)\theta && (\theta \text{ homomorphism}) \\
&= x\theta^{-1}\phi_a\theta + y\theta^{-1}\phi_a\theta
\end{aligned}$$

and if $n \in \mathbb{F}_p$, then

$$\begin{aligned}
(nv)\theta^{-1}\phi_a\theta &= (v\theta^{-1})^n\phi_a\theta \\
&= (a^{-1}(v\theta^{-1})^n a)\theta \\
&= (a^{-1}(v\theta^{-1})a)^n\theta \\
&= n((a^{-1}(v\theta^{-1})a)\theta) \\
&= n(v\theta^{-1}\phi_a\theta).
\end{aligned}$$

Thus $\theta^{-1}\phi_a\theta \in GL(k,p)$ for all $a \in G_\alpha$, so ψ is well-defined.

To see that ψ is a homomorphism, let $ma, m'a' \in G$. Then,

$$\begin{aligned}
(ma\psi)(m'a'\psi) &= (m\theta)^*(\theta^{-1}\phi_a\theta)(m'\theta)^*(\theta^{-1}\phi_{a'}\theta) \\
&= (m\theta)^*(\theta^{-1}\phi_a\theta)(m'\theta)^*(\theta^{-1}\phi_a\theta)^{-1}(\theta^{-1}\phi_a\theta)(\theta^{-1}\phi_{a'}\theta) \\
&= (m\theta)^*(m'\theta(\theta^{-1}\phi_a\theta)^{-1})^*(\theta^{-1}\phi_{aa'}\theta) \\
&= (m\theta)^*(m'\phi_{a^{-1}}\theta)^*(\theta^{-1}\phi_{aa'}\theta) \\
&= (m\theta + am'a^{-1}\theta)^*(\theta^{-1}\phi_{aa'}\theta) \\
&= ((mam'a^{-1})\theta)^*(\theta^{-1}\phi_{aa'}\theta) \\
&= ((mam'a^{-1})(aa'))\psi \\
&= (mam'a')\psi,
\end{aligned}$$

as desired.

Suppose that $ma \in ker(\psi)$. Then $(m\theta)^*(\theta^{-1}\phi_a\theta) = 1_V$, so $(m\theta)^* = 0^*$ and $\theta^{-1}\phi_a\theta = 1_V$. Then $m\theta = 0$, but θ is an isomorphism, so $m = 1$. We also have that $\phi_a = \theta 1_V \theta^{-1} = 1_M$, so $a^{-1}ma = m\phi_a = m$ for all $m \in M$. Then $a \in C_G(M) = M$, but $a \in G_\alpha$, so $a = 1$. Thus $ma = 1$ and ψ is 1-1.

Note that $M\psi = V^*$ since θ maps onto V. Then $V^* = M\psi \leq G\psi$, so $G\psi$ is transitive. Of course G is also transitive, so to show that G is permutation isomorphic to $G\psi$, it suffices to show that $G_\alpha\psi = (G\psi)_0$ by Proposition 1.2.3. But $(G\psi)_0 = G\psi \cap \mathrm{Aff}(k,p)_0 = G\psi \cap GL(k,p)$, so we must show that $G_\alpha\psi = G\psi \cap GL(k,p)$. Clearly $G_\alpha\psi \leq G\psi \cap GL(k,p)$ by the construction of ψ. On the other hand, if $x \in G\psi \cap GL(k,p)$, then $x =$

$(ma)\psi = (m\theta)^*(\theta^{-1}\phi_a\theta)$ for some $m \in M$ and $a \in G_\alpha$, but $(m\theta)^* = x(\theta^{-1}\phi_a\theta)^{-1} \in V^* \cap GL(k,p)$, so $(m\theta)^* = 0^*$. Thus $m = 1$, so $x = a\psi \in G_\alpha\psi$, and we are done. Hence, G is permutation isomorphic to $G\psi$, which is a group of affine type since $G\psi$ is primitive and $V^* \leq G\psi \leq \mathrm{Aff}(k,p)$. □

Suppose that T is not abelian and that $k \geq 2$, and suppose further that there exist groups $X_1, \ldots, X_n$ such that $M = X_1 \times \cdots \times X_n$ and $M_\alpha = (X_1)_\alpha \times \cdots \times (X_n)_\alpha$ where X_i is simple for all i or $(X_i)_\alpha$ is a full diagonal subgroup of X_i for all i. I call this the *simple condition* and the *diagonal condition* respectively. Note that in either case, the requirements for Lemma 2.1.12 are satisfied. For the rest of this section, I will write $X := X_1$ and $N := N_G(X)$ whenever one of these conditions occurs.

Lemma 2.7.3. *If the simple condition or the diagonal condition is satisfied, then X_α is a maximal N_α-invariant subgroup of X. Moreover, $X_\alpha \trianglelefteq X$ or $N_\alpha C_G(X) < N$.*

Proof. By Lemma 2.1.12, G_α acts transitively on $\{X_1, \ldots, X_n\}$, so there must exist $1 = g_1, g_2, \ldots, g_n \in G_\alpha$ with $g_i^{-1} X g_i = X_i$ for all i. Define $\gamma_i : X \to X_i$ by $x \mapsto g_i^{-1} x g_i$ for all $i \in \{1, \ldots, n\}$. Then each γ_i is an isomorphism. Recall that if $g \in G_\alpha$ and $g^{-1} X_i g = X_j$, then $g^{-1}(X_i)_\alpha g = (X_j)_\alpha$; in particular, if $a \in N_\alpha$, then $a^{-1} X_\alpha a = X_\alpha$, so N_α normalizes X_α. Moreover, if $X_\alpha = X$, then $M_\alpha = M$, a contradiction. Thus X_α is a proper N_α-invariant subgroup of X.

Suppose that L is an N_α-invariant subgroup of X properly containing X_α. Let $R := L \times L\gamma_2 \times \cdots \times L\gamma_n$. Then $M_\alpha \leq R \leq M$. For $a \in G_\alpha$, define $\pi_a \in S_n$ by $a^{-1} X_i a = X_{i\pi_a}$. Then for each i, $g_{i\pi_a^{-1}} a g_i^{-1} \in N_\alpha$ since

$$g_i a^{-1} g_{i\pi_a^{-1}}^{-1} X g_{i\pi_a^{-1}} a g_i^{-1} = g_i a^{-1} X_{i\pi_a^{-1}} a g_i^{-1} = g_i X_{i\pi_a^{-1}\pi_a} g_i^{-1} = X,$$

but $N_\alpha \leq N_G(L)$, so $g_{i\pi_a^{-1}} a g_i^{-1} \in N_G(L)$. Now let $r := (l_1, l_2\gamma_2, \ldots, l_n\gamma_n) \in R$. Then

$$a^{-1} r a = a^{-1}(l_1, l_2\gamma_2, \ldots, l_n\gamma_n)a = (a^{-1}(l_{1\pi_a^{-1}}\gamma_{1\pi_a^{-1}})a, \ldots, a^{-1}(l_{n\pi_a^{-1}}\gamma_{n\pi_a^{-1}})a),$$

but $a^{-1} r a \in X_1 \times \cdots \times X_n = X \times X\gamma_2 \times \cdots \times X\gamma_n$, so for each i, $a^{-1}(l_{i\pi_a^{-1}}\gamma_{i\pi_a^{-1}})a = x_i\gamma_i$ for some $x_i \in X$. Then

$$x_i = g_i a^{-1}(l_{i\pi_a^{-1}}\gamma_{i\pi_a^{-1}})a g_i^{-1} = (g_{i\pi_a^{-1}} a g_i^{-1})^{-1} l_{i\pi_a^{-1}}(g_{i\pi_a^{-1}} a g_i^{-1}) \in L$$

by the above, so $a^{-1} r a \in R$. Thus $G_\alpha \leq N_G(R)$, so by the primitivity of G, $R = M_\alpha$ or $R = M$. But if $R = M_\alpha$, then $L = X_\alpha$, a contradiction, so $R = M$, which implies that $L = X$. Thus X_α is a maximal N_α-invariant subgroup of X.

Now suppose for a contradiction that X_α is not a normal subgroup of X and that $N_\alpha C_G(X) = N$. Let $S := \langle \{x^{-1} y x : x \in X, y \in X_\alpha\} \rangle$. Then $X_\alpha < S \leq X$ since if $X_\alpha = S$, then $X_\alpha \trianglelefteq X$. Moreover, $N_\alpha \leq N_G(S)$ since if $a \in N_\alpha$, then for all $x \in X$ and $y \in X_\alpha$,

$a^{-1}x^{-1}yxa = (a^{-1}xa)^{-1}(a^{-1}ya)(a^{-1}xa) \in S$ because $a^{-1}xa \in X$ and $a^{-1}ya \in X_\alpha$. Since X_α is a maximal N_α-invariant subgroup of X, $S = X$. Then

$$\begin{aligned} X &= \langle\{x^{-1}yx : x \in X, y \in X_\alpha\}\rangle \\ &\leq \langle\{a^{-1}ya : a \in C_G(X)N_\alpha, y \in X_\alpha\}\rangle \quad (\text{since } X \leq N = N_\alpha C_G(X)) \\ &= \langle\{a^{-1}ya : a \in N_\alpha, y \in X_\alpha\} \quad (\text{since } X_\alpha \leq X) \\ &= X_\alpha. \end{aligned}$$

But then $X = X_\alpha$, a contradiction. □

Note that the Schreier Conjecture (Theorem 1.10.2) is required for the proof of the following proposition.

Proposition 2.7.4. *If the simple condition is satisfied and $N_\alpha C_G(X) = N$, then G is permutation isomorphic to a group of twisted wreath type.*

Proof. We may assume without loss of generality that $X_i = T_i$ for all i. Recall that G_α acts transitively on $\{T_1, \ldots, T_k\}$ by Lemma 2.1.12; in particular, there exist elements $1 = g_1, g_2, \ldots, g_k \in G_\alpha$ such that $g_i^{-1}T_i g_i = T_1$ (note that this is opposite the usual setup). Since $N_\alpha C_G(T_1) = N$, it follows from Lemma 2.7.3 that $(T_1)_\alpha$ is a proper normal subgroup of T_1, but T_1 is simple, so $(T_1)_\alpha = \{1\}$. Hence $M_\alpha = \{1\}$, so M is regular.

Let $n \in N_\alpha$. Define $\varphi_n : T_1 \to T_1$ by $t \mapsto n^{-1}tn$. Define $\varphi : N_\alpha \to Aut(T_1)$ by $n \mapsto \varphi_n$. Then φ is a homomorphism with $ker(\varphi) = C_G(T_1) \cap N_\alpha = C_G(T_1) \cap G_\alpha$. If $\gamma \in Inn(T_1)$, then there exists a $t_1 \in T_1$ such that $t\gamma = t_1^{-1}tt_1$ for all $t \in T_1$. $T_1 \leq N = N_\alpha C_G(T_1)$, so $t_1 = nc$ for some $n \in N_\alpha$ and $c \in C_G(T_1)$. Then for all $t \in T_1$,

$$t\varphi_n = n^{-1}tn = (t_1c^{-1})^{-1}t(t_1c^{-1}) = c(t\gamma)c^{-1} = t\gamma,$$

so $\gamma = \varphi_n \in N_\alpha\varphi$. Thus $Inn(T_1) \leq N_\alpha\varphi$, so we may let $Z \leq N_\alpha$ be the preimage of $Inn(T_1)$ under φ.

Note that $Z/C_{N_\alpha}(T_1)$ is simple and nonabelian: if $z \in Z$, then $z\varphi = \varphi_t$ for some $t \in T_1$. If $z' \in Z$ where $z'\varphi = \varphi_{t'}$ and $z = z'$, then $\varphi_t = \varphi_{t'}$, so $t^{-1}xt = t'^{-1}xt'$ for all $x \in T_1$. Then $t't^{-1} \in Z(T_1) = \{1\}$, so $t = t'$. Thus we may define $\chi : Z \to T_1$ by $z \mapsto t$ where $z\varphi = \varphi_t$. χ is an onto homomorphism since $T_1 \leq Z$ and φ is a homomorphism. Further, $z \in ker(\chi)$ if and only if $z\varphi = \varphi_1$, which is true if and only if $z^{-1}tz = t$ for all $t \in T_1$. Thus $ker(\chi) = C_{N_\alpha}(T_1)$, giving the desired result.

I claim that M is the kernel of the action of G on $\{T_1, \ldots, T_k\}$. Let Y be this kernel. Then $y^{-1}T_iy = T_i$ for all $i \in \{1, \ldots, k\}$ and $y \in Y$. Clearly $M \leq Y$, so $Y = Y \cap (G_\alpha M) = Y_\alpha M$. I will prove that $Y_\alpha = \{1\}$. First, embed $Y_\alpha M/M$ into $Out(T_1) \times \cdots \times Out(T_k)$ as follows: define $\theta : Y \to Out(T_1) \times \cdots \times Out(T_k)$ by $y \mapsto (Inn(T_1)y^{*_1}, \ldots, Inn(T_k)y^{*_k})$ where for all i, $y^{*_i} \in Aut(T_i)$ is defined by $t \mapsto y^{-1}ty$. θ is clearly a homomorphism. Let

$y \in ker(\theta)$. Fix $i \in \{1, \ldots, k\}$. Then $y^{*i} \in Inn(T_i)$, so for all $t \in T_i$, $y^{-1}ty = ty^{*i} = t_i^{-1}tt_i$ for some $t_i \in T_i$. Then $yt_i^{-1} \in C_G(T_i)$. As i was arbitrary, $y \in \bigcap_{i=1}^k C_G(T_i)T_i = (\bigcap_{i=1}^k C_G(T_i))T_1 \cdots T_k$ by Lemma 1.1.3. But $\{1\} = C_G(M) = \bigcap_{i=1}^k C_G(T_i)$ again by Lemma 1.1.3, so $y \in T_1 \cdots T_k = M$. Thus $ker(\theta) \leq M$. On the other hand, let $m \in M$. Write $m = (t_1, \ldots, t_k)$. Then if $t \in T_i$, $tm^{*i} = m^{-1}tm = t_i^{-1}tt_i$, so $m^{*i} \in Inn(T_i)$ for all i. Thus $M = ker(\theta)$, so Y/M is embedded into $Out(T_1) \times \cdots \times Out(T_k)$, as desired. Moreover, by the Schreier Conjecture, $Out(T_i)$ is solvable for all i, so $Out(T_1) \times \cdots \times Out(T_k)$ is also solvable by Proposition 1.7.1. Since $Y_\alpha \cap M = M_\alpha = \{1\}$, $Y_\alpha \simeq Y_\alpha M/M = Y/M$, so Y_α is solvable. Then $Y_\alpha C_{N_\alpha}(T_1)/C_{N_\alpha}(T_1) \simeq Y_\alpha/(Y_\alpha \cap C_{N_\alpha}(T_1))$ is also solvable, again by Proposition 1.7.1. Now $Y \trianglelefteq G$, so $Y_\alpha \trianglelefteq N_\alpha$, as is $C_{N_\alpha}(T_1)$. Thus $Y_\alpha C_{N_\alpha}(T_1) \trianglelefteq N_\alpha$. Moreover, $Z \trianglelefteq N_\alpha$ since $Inn(T) \trianglelefteq N_\alpha\varphi$. Let $C := C_{N_\alpha}(T_1)$. Then

$$[Z/C, Y_\alpha C/C] \leq Z/C \cap Y_\alpha C/C \trianglelefteq Z/C.$$

If $Z/C \cap Y_\alpha C/C = Z/C$, then $Z/C \leq Y_\alpha C/C$, which is solvable, so Z/C is solvable, but Z/C is simple and nonabelian, a contradiction. Thus since Z/C is simple, $Z/C \cap Y_\alpha C/C = C/C$, so $[Z/C, Y_\alpha C/C] = C/C$. It follows that $[Z, Y_\alpha C] = C$. Let $t \in T_1$ and $y \in Y_\alpha$. Then $[t, y] \in [Z, Y_\alpha C] = C \leq C_G(T_1)$, but $[t, y] \in T_1$ since $y^{-1}T_1y = T_1$, so $[t, y] = 1$. As $t \in T_1$ was arbitrary, $y \in C_G(T_1)$. Thus $Y_\alpha \leq C_G(T_1)$. Let $x \in T_i$ and $y \in Y_\alpha$. Note that $g_iyg_i^{-1} \in Y_\alpha$ for all i since $Y_\alpha \trianglelefteq G_\alpha$. Also, $g_i^{-1}xg_i \in T_1$. Then

$$y^{-1}xy = g_i(g_i^{-1}yg_i)^{-1}(g_i^{-1}xg_i)(g_i^{-1}yg_i)g_i^{-1} = g_i(g_i^{-1}xg_i)g_i^{-1} = x,$$

so $y \in \bigcap_{i=1}^k C_G(T_i) = \{1\}$. Thus $Y_\alpha = \{1\}$.

Let $P := G_\alpha$. Then P acts transitively on $\{T_1, \ldots, T_k\}$. For convenience, write $p^{-1}T_ip = T_{ip}$ (abusing the notation somewhat). This action is also faithful, for if $p \in P$ is in the kernel of the action, then $p \in M$, but $P \cap M = M_\alpha = \{1\}$, so $p = 1$. Let $Q := P_1 = N_\alpha$. Then φ is a group action of Q on T_1. I will denote this action by $t^q := q^{-1}tq$. I claim that G is permutation isomorphic to $T_1 \; twr_Q \; P$.

Note that $\{g_1, \ldots, g_k\} \subseteq P$. In fact, $L := \{g_1, \ldots, g_k\}$ is a left transversal for Q in P: suppose that $g_iQ = g_jQ$. Then $g_i^{-1}g_j \in Q = N_\alpha$, so $(g_i^{-1}g_j)^{-1}T_1(g_i^{-1}g_j) = T_1$. Then

$$T_j = g_jT_1g_j^{-1} = g_j(g_i^{-1}g_j)^{-1}T_1(g_i^{-1}g_j)g_j^{-1} = T_i,$$

so $i = j$. If $p \in P$, then $pT_1p^{-1} = T_i$ for some i, which implies that

$$(p^{-1}g_i)^{-1}T_1p^{-1}g_i = g_i^{-1}T_ig_i = T_1.$$

Thus $p^{-1}g_i \in Q$, so $pQ = g_iQ$ and we have our left transversal. Every element p of P can then be written uniquely in the form $\overline{p}q_p$ where $\overline{p} \in L$ and $q_p \in Q$.

Recall that ${}_QB$ is the base group of the twisted wreath product $T_1\ twr_Q\ P$. Let $m := (t_1, \ldots, t_k) \in M$. Define $\psi_m : P \to T_1$ by $p \mapsto p^{-1}t_i p$ when $\overline{p} = g_i$. First I show that $\psi_m \in {}_QB$. Let $p \in P$ and $q \in Q$. Suppose that $\overline{p} = g_i$. Then we also have that $\overline{pq} = g_i$, so

$$(p\psi_m)^q = q^{-1}(p^{-1}t_i p)q = (pq)^{-1}t_i(pq) = (pq)\psi_m,$$

as desired. Note that $\psi_{mm'} = \psi_m\psi_{m'}$ for all $m, m' \in M$. Moreover, I claim that if $m \in M$ and $p \in P$, then $\psi_m^p = \psi_{p^{-1}mp}$. For each i, $x_i := g_{ip^{-1}}^{-1}pg_i \in Q$ since

$$(g_{ip^{-1}}^{-1}pg_i)^{-1}T_1(g_{ip^{-1}}^{-1}pg_i) = g_i^{-1}p^{-1}(T_{ip^{-1}})pg_i = g_i^{-1}T_{ip^{-1}p}g_i = T_1.$$

Let $x \in P$ and suppose that $\overline{x} = g_i$, so that $x = g_i q_x$. Then

$$\begin{aligned}
x\psi_m^p &= (g_{ip^{-1}}x_i q_x)\psi_m \\
&= (x_i q_x)^{-1}(g_{ip^{-1}}\psi_m)(x_i q_x) && \text{(since } x_i q_x \in Q\text{)} \\
&= q_x^{-1}x_i^{-1}g_{ip^{-1}}^{-1}t_{ip^{-1}}g_{ip^{-1}}x_i q_x \\
&= (g_i q_x)^{-1}(p^{-1}t_{ip^{-1}}p)(g_i q_x) && \text{(subbing in for } x_i\text{)} \\
&= x\psi_{p^{-1}mp} && \text{(as } p^{-1}mp = (p^{-1}t_{1p^{-1}}p, \ldots, p^{-1}t_{kp^{-1}}p)\text{)},
\end{aligned}$$

as desired.

Since $G = MG_\alpha = MP$ and $M \cap P = \{1\}$, $G = M \rtimes P$. Define $\psi : G \to T_1\ twr_Q\ P$ by $mp \mapsto (\psi_m, p)$. Let $mp, m'p' \in G$. Then

$$\begin{aligned}
(mp)\psi(m'p')\psi &= (\psi_m, p)(\psi_{m'}, p') \\
&= (\psi_m\psi_{m'}^{p^{-1}}, pp') \\
&= (\psi_m\psi_{pm'p^{-1}}, pp') \\
&= (\psi_{mpm'p^{-1}}, pp') \\
&= (mpm'p^{-1}pp')\psi \\
&= (mpm'p')\psi,
\end{aligned}$$

so ψ is a homomorphism. Let $mp \in ker(\psi)$. Then $\psi_m = 1_B$ and $p = 1$, so $1 = g_i\psi_m = g_i^{-1}t_i g_i$ for all i. Thus $t_i = 1$ for all i, so $mp = 1$. Hence, ψ is 1-1. Let $(b, p) \in T_1\ twr_Q\ P$. Suppose that $xQ = yQ$ where $x, y \in P$. Then since $y^{-1}x \in Q$,

$$xb = (yy^{-1}x)b = (yb)^{y^{-1}x} = (y^{-1}x)^{-1}(yb)(y^{-1}x),$$

so $x(xb)x^{-1} = y(yb)y^{-1}$ for all x and y satisfying $xQ = yQ$. Thus we may define $t_i := x(xb)x^{-1}$ for all $i \in \{1, \ldots, k\}$ where we may take x to be any element with $\overline{x} = g_i$. Moreover, $x(xb)x^{-1} \in xT_1x^{-1} = g_i q_x T_1 q_x^{-1}g_i^{-1} = g_i T_1 g_i^{-1} = T_i$. Thus $m := (t_1, \ldots, t_k) \in M$ and $x\psi_m = x^{-1}t_i x = x^{-1}(x(xb)x^{-1})x = xb$ for all $x \in P$, so $mp\psi = (\psi_m, p) = (b, p)$ and ψ is onto. Thus ψ is an isomorphism. Since $G_\alpha\psi = P\psi = P = (T_1\ twr_Q\ P)_\alpha$, G is permutation isomorphic to $T_1\ twr_Q\ P$, a group of twisted wreath type. $\square$

Proposition 2.7.5. *Suppose that T is not abelian and that $k \geq 2$. If M_α is a full diagonal subgroup of M, then G is permutation isomorphic to a group of diagonal type.*

Proof. Let W be the group of diagonal type that is an extension of $Inn(T_1)^k$ by $Out(T_1) \times S_k$. Then W has socle $Inn(T_1)^k$ and acts transitively and faithfully on $\Omega' := W/W_{\alpha'}$ where $\alpha' := D$ (in the notation of a group of diagonal type). Since M_α is a full diagonal subgroup of M, for $i \in \{2, \ldots, k\}$, there exist isomorphisms $\gamma_i : T_1 \to T_i$ such that $M_\alpha = \{(t, t\gamma_2, \ldots, t\gamma_k) : t \in T_1\}$ (see (1) in the proof of Lemma 1.4.1(i)). Further, every element of M can be written uniquely as $(t_1, t_2\gamma_2, \ldots, t_k\gamma_k)$ for some $t_1, \ldots, t_k \in T_1$. Define $\theta : M \to (Inn(T_1))^k$ by $(t_1, t_2\gamma_2, \ldots, t_k\gamma_k) \mapsto (\theta_{t_1}, \ldots, \theta_{t_k})$ where $\theta_{t_i} : T_1 \to T_1$ is conjugation by t_i. Since γ_i is a homomorphism for all i and $\theta_{tt'} = \theta_t\theta_{t'}$ for all $t, t' \in T_1$, θ is a homomorphism. If $(t_1, t_2\gamma_2, \ldots, t_k\gamma_k) \in ker(\theta)$, then $t = t\theta_{t_i} = t_i^{-1}tt_i$ for all $t \in T_1$, so $t_i \in Z(T_1) = \{1\}$ for all i. Thus θ is 1-1. θ is clearly onto, so θ is an isomorphism. Moreover,

$$M_\alpha\theta = \{(a, \ldots, a) : a \in Inn(T_1)\} = (Inn(T_1)^k)_{\alpha'}.$$

Since both M and $Inn(T_1)^k$ are transitive, M is permutation isomorphic to $Inn(T_1)^k$ by Proposition 1.2.3. Then there exists a permutation isomorphism $\psi : N_{S^\Omega}(M) \to N_{S^{\Omega'}}(Inn(T_1)^k)$ such that $m\psi = m\theta$ for all $m \in M$ by Proposition 1.2.5. Note that $G \leq N_{S^\Omega}(M)$ since $M \trianglelefteq G$. Then

$$Inn(T_1)^k = M\psi \leq G\psi \leq N_{S^\Omega}(M)\psi = N_{S^{\Omega'}}(Inn(T_1)^k) = W$$

by Proposition 2.5.4. $G\psi$ is primitive since G is, so G is permutation isomorphic to $G\psi$, a group of diagonal type. □

Proposition 2.7.6. *If the simple condition is satisfied and $N_\alpha C_G(X) < N$ or if the diagonal condition is satisfied and $n \geq 2$, then G is permutation isomorphic to a group of almost simple product type or diagonal product type respectively.*

Proof. Again there exist $1 = g_1, g_2, \ldots, g_n \in G_\alpha$ with $g_i^{-1}Xg_i = X_i$ for all i since G_α acts transitively on $\{X_1, \ldots, X_n\}$ by Lemma 2.1.12. Rearranging indices as needed, we may write $X = T_1 \times \cdots \times T_m$ for some $m \geq 1$ since $X \trianglelefteq M$.

Note that $N = N_\alpha XC_G(X)$: $X_2 \times \cdots \times X_n$ clearly centralizes X, so $M \leq XC_G(X)$. Moreover, X is a normal subgroup of M, so $M \leq N$ (in fact it is a normal subgroup). Then $N = N \cap G = N \cap (G_\alpha M) = N_\alpha M$, which implies that $N = N_\alpha M \leq N_\alpha XC_G(X) \leq N$ as $XC_G(X) \trianglelefteq N$. Thus $N = N_\alpha XC_G(X)$.

Moreover, note that if the diagonal condition is satisfied, then since X_α is a full diagonal subgroup of X, X_α is self-normalizing in X by Lemma 1.4.1, which implies that if $X_\alpha \trianglelefteq X$, then $X_\alpha = X$, a contradiction of Lemma 2.7.3. Thus $N_\alpha C_G(X) < N$ by Lemma 2.7.3.

For $L \leq N$, let $L^* := LC_G(X)/C_G(X)$. Let $U \leq N^*$. Then $U = V/C_G(X)$ for some $C_G(X) \leq V \leq N$ and

$$V = V \cap N = V \cap (N_\alpha X C_G(X)) = (V \cap N_\alpha X)C_G(X),$$

so $U = (V \cap N_\alpha X)^*$. Thus if $U \leq N^*$, we may assume that $U = V^*$ for some $V \leq N$.

I claim that N_α^* is a maximal subgroup of N^*. In either case, $N_\alpha^* < N^*$ since $N_\alpha C_G(X) < N$. Now, let $N_\alpha C_G(X) \leq Y \leq N$. $X_\alpha \leq N_\alpha \leq Y$, so $X_\alpha \leq Y \cap X \leq X$. N_α clearly normalizes $Y \cap X$, but X_α is a maximal N_α-invariant subgroup of X by Lemma 2.7.3, so either $X_\alpha = Y \cap X$ or $Y \cap X = X$. But $Y = Y \cap (XN_\alpha C_G(X)) = (Y \cap X)N_\alpha C_G(X)$, so $Y = X_\alpha N_\alpha C_G(X) = N_\alpha C_G(X)$ or $Y = XN_\alpha C_G(X) = N$. It follows that N_α^* is a maximal subgroup of N^*.

Let $H := N^*$, and let Γ be the right coset space $H \backslash N_\alpha^*$ (note that $|\Gamma| \geq 2$). Then H is transitive on Γ. Let $\gamma := N_\alpha^*$. Then $H_\gamma = N_\alpha^*$, so H_γ is a maximal subgroup of H. Thus H acts primitively on Γ.

Note that if $*_L : L \to L^*$ is defined by $l \mapsto C_G(X)l$ where $L \leq N$, then $*_L$ is an onto homomorphism. Moreover, $ker(*_L) = C_G(X) \cap L$, so $*_L$ is 1-1 if and only if $C_G(X) \cap L = \{1\}$. Now suppose that $L \leq X$, and let $l \in C_G(X) \cap L$. Write $l = (l_1, \ldots, l_m)$ where $l_i \in T_i$, and let $t_i \in T_i$. Then $x := (t_1, \ldots, t_m) \in X$, so $lx = xl$ which implies that $l_i t_i = t_i l_i$ for all i. Thus $l_i \in Z(T_i) = \{1\}$ for all i, so $C_G(X) \cap L = \{1\}$. Hence for all $L \leq X$, $L \simeq L^*$. In particular, $X \simeq X^*$ and $T_i \simeq T_i^*$ for all i, so T_i^* is simple and nonabelian for all i.

Since $T_1^* \cdots T_m^* = X^*$, $T_i^* \cap (T_1^* \cdots T_{i-1}^* T_{i+1}^* \cdots T_m^*) = C_G(X)/C_G(X)$ and $T_i C_G(X)$ is a normal subgroup of $XC_G(X)$ for all $i \in \{1, \ldots, m\}$, $X^* = T_1^* \times \cdots \times T_m^*$. I claim that X^* is the socle of H. Of course $X^* \trianglelefteq H$, so it suffices to show that $C_H(X^*) = \{C_G(X)\}$ by Proposition 1.5.6. Let $C_G(X)g \in C_H(X^*)$. Then for all $x \in X$, $C_G(X)gx = C_G(X)xg$, so $gxg^{-1}x^{-1} \in C_G(X)$. But $gxg^{-1}x^{-1} \in X$ and $X \cap C_G(X) = \{1\}$, so $gx = xg$ for all $x \in X$. Thus $g \in C_G(X)$, so $C_G(X)g = C_G(X)$, as desired.

Suppose that X_α is a full diagonal subgroup of X. Note that $m \geq 2$, or else X is simple, which implies that $X_\alpha = X$, a contradiction of Lemma 2.7.3. Of course, $X_\alpha^* \leq T_1^* \times \cdots \times T_m^*$. Fix $i \in \{1, \ldots, m\}$, let $\rho_i^* : X_\alpha^* \to T_i^*$ be the i-th projection map and let $x^* \in X_\alpha^* \cap ker(\rho_i^*)$. We may write $x^* = (t_1^*, \ldots, t_k^*)$ where $t_j \in T_j$ for all j, so $t_i^* = C_G(X)$. Then $t_i \in C_G(X) \leq C_G(T_i)$, so $t_i \in Z(T_i) = \{1\}$. But $(t_1, \ldots, t_k) \in X_\alpha$, X_α is full diagonal in X, and $t_i = 1$, so $t_j = 1$ for all $j \in \{1, \ldots, m\}$. Thus $x^* = 1$, so $\rho_i^*|_{X_\alpha^*}$ is 1-1 for all i. Then $T_i^* \simeq T_i \simeq X_\alpha \simeq X_\alpha^* \simeq X_\alpha^* \rho_i^* \leq T_i^*$ for all i, so X_α^* is a full diagonal subgroup of X^*.

To see that the action of H on Γ is faithful, the proof is divided into two cases, depending on whether X is simple or X_α is a full diagonal subgroup of X.

Case 1: Suppose that X is simple. Then X^* is simple and is the socle of H, so X^* is the unique minimal normal subgroup of H. Let U be a normal subgroup of H contained in N_α^*. If U is not trivial, then $X^* \leq U \leq N_\alpha^*$, but this implies that $N_\alpha^* = N_\alpha^* X^* = N^*$, a contradiction. Thus N_α^* is core-free, so the action is faithful.

Case 2: Suppose that X_α is a full diagonal subgroup of X. Then X_α^* is a full diagonal subgroup of X^*. Let $U \trianglelefteq H$ with $U \leq N_\alpha^*$ where U is the minimal nontrivial such group. Then U is a minimal normal subgroup of H, so $U \leq X^*$, which implies that $U \leq N_\alpha^* \cap X^* = X_\alpha^*$. But X_α^* is simple, $U \trianglelefteq X_\alpha^*$ and U is nontrivial, so $U = X_\alpha^*$. Then $X_\alpha^* \trianglelefteq X^*$, but X_α^* is full diagonal in X^*, hence is self-normalizing in X^* by Lemma 1.4.1, so $X_\alpha \simeq X_\alpha^* = X^* \simeq X$. Then $X_\alpha = X$, a contradiction by Lemma 2.7.3. Thus N_α^* is core-free, so the action of H on Γ is faithful.

Summarizing, H is a primitive permutation group on Γ with socle X^*. If X is simple, then the socle of H is simple and nonabelian, so H is of almost simple type. If X_α is a full diagonal subgroup of X, then $(X^*)_\gamma = X_\alpha^*$ is a full diagonal subgroup of $X^* = T_1^* \times \cdots \times T_m^*$ with $m \geq 2$, so H is of diagonal type by Proposition 2.7.5.

I claim that G is permutation isomorphic to a subgroup of $H \ wr_\Delta \ S_n$ where $\Delta = \{1, \ldots, n\}$ and $H \ wr_\Delta \ S_n$ acts on Γ^n with the product action. Write the elements of $H \ wr_\Delta \ S_n$ in the form $(h_1, \ldots, h_n)\pi$ where $h_i \in H$ for all i and $\pi \in S_n$. Note that $T^m \simeq X \simeq X_i$ and $X_\alpha \simeq (X_i)_\alpha$ for all i, so

$$|\Gamma|^n = [X^* : X_\alpha^*]^n = [X : X_\alpha]^n = |T|^{mn}/|X_\alpha|^n = [M : M_\alpha] = |\Omega|.$$

I claim that $R := \{g_1, \ldots, g_n\}$ is a right transversal for N in G: first suppose that $Ng_i = Ng_j$. Then $g_i g_j^{-1} \in N$, so $g_j g_i^{-1} X g_i g_j^{-1} = X$. But then

$$X_j = g_j^{-1} X g_j = g_j^{-1} g_j g_i^{-1} X g_i g_j^{-1} g_j = X_i,$$

so $i = j$. Thus $i = j$ if and only if $Ng_i = Ng_j$. Let $g \in G$. Then $g = ma$ for some $m \in M$ and $a \in G_\alpha$, so $g^{-1} X g = a^{-1}(m^{-1} X m)a = a^{-1} X a = X_i$ for some i. Then

$$(g_i g^{-1})^{-1} X (g_i g^{-1}) = g X_i g^{-1} = X,$$

so $g_i g^{-1} \in N$ and $Ng_i = Ng$. Thus R is a right transversal for N in G, so every element g of G can be written uniquely in the form $n_g \overline{g}$ where $n_g \in N$ and $\overline{g} \in R$. For all $g \in G$, define $\pi_g \in S_n$ by $g^{-1} X_i g = X_{i\pi_g}$. Define $\psi : G \to H \ wr_\Delta \ S_n$ by $g \mapsto (n_{g_1 g}^*, \ldots, n_{g_n g}^*)\pi_g$.

Let $g, h \in G$. Note that $\pi_g \pi_h = \pi_{gh}$ since

$$X_{i\pi_g\pi_h} = h^{-1} X_{i\pi_g} h = h^{-1} g^{-1} X_i g h = (gh)^{-1} X_i (gh) = X_{i\pi_{gh}}.$$

Moreover, $g_i g g_{i\pi_g}^{-1} \in N$ for all i since

$$g_{i\pi_g} g^{-1} g_i^{-1} X g_i g g_{i\pi_g}^{-1} = g_{i\pi_g} g^{-1} X_i g g_{i\pi_g}^{-1} = g_{i\pi_g} X_{i\pi_g} g_{i\pi_g}^{-1} = X.$$

Hence, $Ng_ig = Ng_{i\pi_g}$, so $\overline{g_ig} = g_{i\pi_g}$ and $\overline{g_igh} = \overline{g_{i\pi_g}h}$ for all i. Then

$$\begin{aligned}
(g\psi)(h\psi) &= (n^*_{g_1g}, \ldots, n^*_{g_ng})\pi_g(n^*_{g_1h}, \ldots, n^*_{g_nh})\pi_h \\
&= (n^*_{g_1g}n^*_{g_{1\pi_g}h}, \ldots, n^*_{g_ng}n^*_{g_{n\pi_g}h})\pi_g\pi_h \\
&= ((n_{g_1g}n_{g_{1\pi_g}h})^*, \ldots, (n_{g_ng}n_{g_{n\pi_g}h})^*)\pi_{gh} \\
&= ((g_1g\overline{g_1g}^{-1}(g_{1\pi_g}h)\overline{g_{1\pi_g}h}^{-1})^*, \ldots, (g_ng\overline{g_ng}^{-1}(g_{n\pi_g}h)\overline{g_{n\pi_g}h}^{-1})^*)\pi_{gh} \\
&= ((g_1gg_{1\pi_g}^{-1}g_{1\pi_g}h\overline{g_1gh}^{-1})^*, \ldots, (g_ngg_{n\pi_g}^{-1}g_{n\pi_g}h\overline{g_ngh}^{-1})^*)\pi_{gh} \\
&= (n^*_{g_1gh}, \ldots, n^*_{g_ngh})\pi_{gh} \\
&= (gh)\psi.
\end{aligned}$$

Thus ψ is a homomorphism.

Let $g \in ker(\psi)$. Then $(n^*_{g_1g}, \ldots, n^*_{g_ng})\pi_g$ is the identity, so $(g_ig)\overline{g_ig}^{-1} \in C_G(X)$ and $g^{-1}X_ig = X_i$ for all i. In particular, $g \in N$, so $Ng_ig = Ng_i$. Then $\overline{g_ig} = g_i$, so $g \in g_i^{-1}C_G(X)g_i$ for all i. I claim that $g_i^{-1}C_G(X)g_i = C_G(X_i)$ for all i. Let $a \in C_G(X)$ and $b \in X_i$. Then

$$\begin{aligned}
(g_i^{-1}ag_i)^{-1}b(g_i^{-1}ag_i) &= g_i^{-1}a^{-1}(g_ibg_i^{-1})ag_i \\
&= g_i^{-1}(g_ibg_i^{-1})g_i \qquad \text{(since } g_ibg_i^{-1} \in X\text{)} \\
&= b,
\end{aligned}$$

so $g_i^{-1}C_G(X)g_i \leq C_G(X_i)$. Similarly, $g_iC_G(X_i)g_i^{-1} \leq C_G(X)$, so $g_i^{-1}C_G(X)g_i = C_G(X_i)$. Then $g \in \bigcap_{i=1}^n C_G(X_i) = C_G(M)$ by Lemma 1.1.3, but $C_G(M)$ is trivial, so ψ is 1-1.

To show that G is permutation isomorphic to $G\psi$, it suffices to show by Proposition 1.2.3 that $G\psi$ acts transitively on Γ^n and that $G_\alpha\psi = (G\psi)_{\alpha'}$ where $\alpha' := (\gamma, \ldots, \gamma)$. Let $m \in M$. Then $Ng_im = Ng_i$, so $\overline{g_im} = g_i$ for all i. Then $n^*_{g_im} = C_G(X)g_img_i^{-1} \in M^*$ for all i since $M \trianglelefteq G$. But π_m is the identity and

$$M^* = MC_G(X)/C_G(X) \leq XC_G(X)/C_G(X) = X^*,$$

so $m\psi \in (X^*)^n$. Thus $M\psi \leq (X^*)^n$. But $|M\psi| = |M| = |X|^n = |(X^*)^n|$ since $X \simeq X^*$, so $M\psi = (X^*)^n$. Hence, $G\psi$ contains the socle of $H\ wr_\Delta\ S_n$, so $G\psi$ acts transitively on Γ^n. Now, let $a \in G_\alpha$. Then $n_{g_ia} = (g_ia)\overline{g_ia}^{-1} \in G_\alpha \cap N = N_\alpha$ for all i, so $a\psi \in (N^*_\alpha)^n \rtimes S_n = H_\gamma\ wr_\Delta\ S_n = (H\ wr_\Delta\ S_n)_{\alpha'}$. Thus $G_\alpha\psi \leq (G\psi)_{\alpha'}$. Moreover,

$$|\Gamma|^n = [G\psi : (G\psi)_{\alpha'}] = \frac{|G|}{|(G\psi)_{\alpha'}|} = \frac{|\Omega||G_\alpha|}{|(G\psi)_{\alpha'}|} = \frac{|\Gamma|^n|G_\alpha|}{|(G\psi)_{\alpha'}|},$$

so $|G_\alpha\psi| = |G_\alpha| = |(G\psi)_{\alpha'}|$. Thus $G_\alpha\psi = (G\psi)_{\alpha'}$, as desired.

Note that if H is of almost simple type, then $n = k \geq 2$ by assumption, and if H is of diagonal type, then $n \geq 2$ by assumption, so $G\psi$ is a group of product type as it is a primitive subgroup of $H\ wr_\Delta\ S_n$ containing the socle of $H\ wr_\Delta\ S_n$. Thus G is permutation isomorphic to a group of almost simple product type or diagonal product type. □

Now we are able to prove the O'Nan-Scott Theorem. Here it is:

Proof of 2.7.1. If T is abelian, then G is permutation isomorphic to a group of affine type by Proposition 2.7.2. Thus we may assume that T is nonabelian. If $k = 1$, then G has a simple nonabelian socle, so G is of almost simple type and we are done. Suppose now that $k \geq 2$. Since T_i is nonabelian and simple for all i, G acts on $\{T_1, \ldots, T_k\}$ by conjugation. Let $\rho_i : M \to T_i$ be the i-th projection map, and define $R_i := M_\alpha \rho_i$. Note that if $a \in G_\alpha$ and $a^{-1} T_i a = T_j$, then

$$a^{-1} R_i a = a^{-1}(M_\alpha \rho_i) a = (a^{-1} M_\alpha a)\rho_j = M_\alpha \rho_j = R_j$$

since $M_\alpha \trianglelefteq G_\alpha$. Thus G_α permutes $\{R_1, \ldots, R_k\}$, so $G_\alpha \leq N_G(R_1 \times \cdots \times R_k)$. But $M_\alpha \leq R_1 \times \cdots \times R_k \leq M$, so by the primitivity of G, $M_\alpha = R_1 \times \cdots \times R_k$ or $M = R_1 \times \cdots \times R_k$.

Suppose that $M_\alpha = R_1 \times \cdots \times R_k$. Then $R_i = T_i \cap M_\alpha = (T_i)_\alpha$ for all i, so taking X_i to be T_i and n to be k, the simple condition is satisfied. Thus if $N_\alpha C_G(T_1) = N$, then G is permutation isomorphic to a group of twisted wreath type by Proposition 2.7.4, and if $N_\alpha C_G(T_1) < N$, then G is permutation isomorphic to a group of almost simple product type by Proposition 2.7.6.

Suppose now that $M = R_1 \times \cdots \times R_k$. Then $R_i = T_i$ for all i, so M_α is a subdirect subgroup of M. By Lemma 1.4.1, $M_\alpha = D_1 \times \cdots \times D_n$ where for each $i \in \{1, \ldots, n\}$, D_i is a full diagonal subgroup of $X_i := \prod_{j \in I_i} T_j$ for some $I_i \subseteq \{1, \ldots, k\}$ (where the I_i partition $\{1, \ldots, k\}$). If $n = 1$, then M_α is a full diagonal subgroup of M, so G is permutation isomorphic to a group of diagonal type by Proposition 2.7.5. Thus we may assume that $n \geq 2$. Note that $D_i = X_i \cap M_\alpha = (X_i)_\alpha$ for all i. Thus the diagonal condition is satisfied, so G is permutation isomorphic to a group of diagonal product type by Proposition 2.7.6, completing the proof. □

3 Finitely Representing M_n

The Grätzer-Schmidt Theorem states that every algebraic lattice is isomorphic to the congruence lattice of some algebra (see [10]). A finite lattice is said to be *finitely representable* if it is isomorphic to the congruence lattice of some finite algebra. The question can then be asked whether every finite lattice is finitely representable. This is an open problem which is generally believed to have a negative answer.

Pálfy and Pudlák prove in [18] that every finite lattice is finitely representable if and only if every finite lattice can be embedded as an interval into the subgroup lattice of a finite group, where if L is a lattice and $a, b \in L$, then the *interval* of a and b is $\{c \in L : a \leq c \leq b\} := [a, b]$. Moreover, their proof reveals that if a finite lattice satisfies three conditions and is finitely representable, then this lattice can be embedded as an interval into the subgroup lattice of a finite group, and conversely, if a lattice can be embedded as an interval into the subgroup lattice of a finite group, then this lattice is finitely representable. This restricts the problem considerably for certain classes of lattices but by no means makes it trivial, as we shall see.

One lattice which satisfies Pálfy and Pudlák's three conditions is M_n, the lattice of length 2 with n atoms (when $n \geq 4$). It follows that for $n \geq 4$, M_n is finitely representable if and only if there exists a finite group G containing a subgroup H such that there are exactly n proper subgroups of G properly containing H, all of which are maximal subgroups of G. Much work has been done on this lattice over the last thirty years, and I will take the remainder of this thesis to describe the progress that has been made, as outlined in the introduction.

3.1 $n - 1 = p^k$

Here is the first most basic reduction for the problem of finitely representing M_n. It comes from an exercise in [21, p. 10].

Proposition 3.1.1. *If $n = p^k + 1$ for some prime p and positive integer k, then M_n is finitely representable.*

Proof. Let V be a vector space of dimension 2 over $F := \mathbb{F}_{p^k}$. Any nontrivial element of V generates a 1-dimensional subspace of V, and there are $p^{2k} - 1$ such elements. Moreover, any 1-dimensional subspace has $p^k - 1$ nontrivial elements, all of which generate the same subspace, so there are $(p^{2k} - 1)/(p^k - 1) = p^k + 1$ subspaces of V. Since any proper nontrivial subspace of V has dimension 1, V has exactly $p^k + 1 = n$ proper nontrivial subspaces; denote these n proper nontrivial subspaces of V by $V_1, \ldots, V_n$.

For $v \in V$ and $0 \neq a \in F$, let $v_a^* : V \to V$ be defined by $x \mapsto ax + v$. Let $G := \{v_a^* : 0 \neq a \in F, v \in V\}$, $K_i := \{v_a^* : 0 \neq a \in F, v \in V_i\}$ and $H := \{0_a^* : 0 \neq a \in F\}$.

It is easily verified that G, H and $K_1, \ldots, K_n$ are all groups and that $H < K_i < G$ for all $i \in \{1, \ldots, n\}$. Moreover, if $v_a^* \in K_i \cap K_j$ where $i \neq j$, then $v \in V_i \cap V_j = \{0\}$, so $K_i \cap K_j = H$ for all $i \neq j$.

Let $H < K < G$. A typical element of K has the form v_b^* for some $0 \neq b \in F$ and $v \in V$. Then $v_{ba}^* = 0_a^* v_b^* \in K$ for all $a \in F$, so $v_a^* \in K$ for all $a \in F$. Define $W := \{v \in V : v_1^* \in K\}$. Clearly $0 \in W$. Let $v, w \in W$. Then $x(v+w)_1^* = x + v + w = (x+v)w_1^* = xv_1^* w_1^*$ for all $x \in V$, so $(v+w)_1^* = v_1^* w_1^* \in K$. Thus $v + w \in W$. Let $0 \neq a \in F$. Then $x(av)_1^* = x + av = a(a^{-1}x + v) + 0 = (a^{-1}x + v)0_a^* = xv_{a^{-1}}^* 0_a^*$ for all $x \in V$, so $(av)_1^* = v_{a^{-1}}^* 0_a^* \in K$. Thus W is a subspace of V, and clearly $K = \{v_a^* \in G : 0 \neq a \in F, v \in W\}$. But then W must be a proper nontrivial subspace of V since $H < K < G$, so $W = V_i$ for some $i \in \{1, \ldots, n\}$. Thus $K = K_i$, which implies that $[H, G] \simeq M_n$, and we are done. □

It was thought for some time that if M_n were finitely representable, then $n-1$ did have to be a power of a prime, as the next result suggests.

Proposition 3.1.2. *Let G be a finite group whose subgroup lattice is isomorphic to M_n where $n \geq 3$. Then $n-1$ is a prime.*

Proof. Let H be a proper nontrivial subgroup of G. Then H has only trivial subgroups. If $p \mid |H|$ and $q \mid |H|$ where p and q are primes, then H contains subgroups of order p and q, a contradiction. Thus H is a p_H-group for some prime p_H. If H has order p_H^m for some $m \geq 2$, then H has a subgroup of order p_H, a contradiction. Thus every proper nontrivial subgroup of G is a cyclic group of prime order.

To start, suppose that G is a p-group for some prime p. Clearly $|G| \neq p$. Suppose that $|G| = p^m$ for some $m \geq 3$. Then G has a subgroup of order p, say H. By Proposition 1.8.1, G is nilpotent, so $H < N_G(H)$, which implies that $H \trianglelefteq G$. Then G/H has order p^{m-1}, so it contains a subgroup K/H of order p. Since $|G/H|$ is at least p^2, $H/H < K/H < G/H$, so $H < K < G$, a contradiction. Thus $|G| = p^2$, so G is abelian by Proposition 1.3.2. Then $G \simeq \mathbb{Z}_{p^2}$ or $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. $\mathbb{Z}_{p^2}$ is cyclic, so it contains exactly one subgroup of order p, but $n \geq 3$, so G is not isomorphic to $\mathbb{Z}_{p^2}$. Thus $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Since G is not cyclic, every nontrivial element of G generates a proper nontrivial subgroup of order p. Since each pair of nontrivial proper subgroups intersects trivially and every nontrivial element is contained in some proper subgroup of G, the number of nontrivial elements of G must equal the number of proper nontrivial subgroups times the number of nontrivial elements in each subgroup. Then $p^2 - 1 = n(p-1)$, so $n = p + 1$. Thus $n - 1$ is a prime, and we are done.

Hence, we may assume that G is not a p-group for any prime p. Note that since every proper nontrivial subgroup of G has prime order and is maximal in G, every proper nontrivial subgroup of G must be a Sylow subgroup of G. It follows that G is square-free. Suppose that G has a Sylow p-subgroup P which is normal in G. Let $q \neq p$ be a prime

dividing the order of G, and let Q be a Sylow q-subgroup where $p \neq q$. Then $P < PQ \leq G$, so $PQ = G$. Since $P \cap Q = \{1\}$, $|G| = pq$. Then $n_q \mid p$ and $n_p \mid q$. If $n_p = q$ and $n_q = p$, then $q \mid (p-1)$ and $p \mid (q-1)$, so $q < p$ and $p < q$, a contradiction. Moreover, if $n_q = 1$ and $n_p = 1$, then $n = n_p + n_q = 2$, a contradiction. Thus $n = n_p + n_q = 1 + q$ or $1 + p$. In either case, $n - 1$ is a prime, and we are done.

Suppose now for a contradiction that no Sylow p-subgroup of G is normal in G. Let $p < q$ be primes dividing the order of G. Let P be a Sylow p-subgroup of G. Then $N_G(P) < G$, but $P \leq N_G(P)$, so we must have that $P = N_G(P)$. Since P is a proper nontrivial subgroup of G, P is cyclic of order p, so $P = \langle a \rangle$ for some $a \in G$. Let $m := [G : P]$. Choose $g_1, \ldots, g_m$ to be right coset representatives of P in G. Let

$$S_P := \{g_i^{-1} a^j g_i : 1 \leq i \leq m \text{ and } 1 \leq j \leq p-1\}.$$

Suppose that $g^{-1}a^i g = h^{-1}a^j h$ for some $g, h \in G$ and $i, j \in \{1, \ldots, p-1\}$. Then $a^i = gh^{-1}a^j hg^{-1}$. Since $gcd(i, p) = 1$ and a has order p, there exists an integer l for which $a = a^{il}$. Then $a = gh^{-1}a^{jl}hg^{-1}$, so $P = \langle a \rangle \leq gh^{-1}Phg^{-1}$. Thus $P = gh^{-1}Phg^{-1}$, so $hg^{-1} \in N_G(P) = P$, and $Pg = Ph$. It follows that $|S_p| = (p-1)[G : P]$. This argument can be repeated for a Sylow q-subgroup Q of G, so $|S_Q| = (q-1)[G : Q]$ as well. Clearly $S_Q \cap S_P = \emptyset$, so G contains at least $|S_P| + |S_Q| + 1$ elements. Now $p \geq 2$, so $p/(p-1) \leq 2$. Since $q > p \geq 2$, $q > p/(p-1)$, so $pq - p - q \geq 1$. Then $|G|pq - |G|p - |G|q \geq |G| > -pq$, so dividing by pq we get that $|G| - |G|/q - |G|/p > -1$. Thus

$$|S_P| + |S_Q| + 1 = 2|G| - |G|/p - |G|/q + 1 > |G|,$$

a contradiction. □

3.2 Nonsolvable Case

The next proposition gives more information about the case when $n - 1$ is not a power of a prime.

Theorem 3.2.1 (Pálfy and Pudlák, [18])**.** *Let G be a finite group. Suppose that H is a proper subgroup of G containing no nontrivial normal subgroup of G such that the interval $[H, G]$ in the subgroup lattice of G is isomorphic to M_n for some $n \geq 3$. If G has a nontrivial normal abelian subgroup, then $n - 1$ is a prime power.*

Proof. Let $\{K_1, K_2, \ldots, K_n\}$ be the n atoms of $[G, H]$. Let A be a minimal abelian normal subgroup of G. By assumption, $A \not\leq H$, so $H < AH \leq G$. Suppose that $AH = G$, for a contradiction. Since A is abelian, $A \cap K_1$ is abelian and $A \cap K_1 \trianglelefteq A$, but $A \cap K_1 \trianglelefteq K_1$ since $A \trianglelefteq G$, so $A \cap K_1 \trianglelefteq AK_1 = G$ since $G = AH \leq AK_1$. Moreover, if $A \cap K_1$ is trivial, then $H = (K_1 \cap A)H = K_1 \cap (AH) = K_1$, a contradiction, so by the minimality of A,

$A \cap K_1 = A$. But then $G = AH = (A \cap K_1)H \leq K_1$, a contradiction. Thus $H < AH < G$, so we may assume without loss of generality that $AH = K_1$. For $j \in \{2, \ldots, n\}$, we have that $K_1 < K_1K_j = (AH)K_j = AK_j \leq G$, so $K_1K_j = AK_j = G$. Then

$$[A : A \cap K_j] = [G : K_j] = [K_1 : K_1 \cap K_j] = [AH : H] = [A : A \cap H],$$

so $A \cap K_j = A \cap H$. $A \cap K_j \trianglelefteq A$ and $A \cap K_j \trianglelefteq K_j$, so $A \cap K_j \trianglelefteq AK_j = G$. If $A \cap K_j = A$, then $H = H \cap (AK_j) = (H \cap A)K_j = (A \cap K_j)K_j = AK_j = G$, a contradiction, so $A \cap K_j = \{1\}$ by the minimality of A. Thus $G = A \rtimes K_j$ for all $j \in \{2, \ldots, n\}$.

Let $x \in K_2$, and fix $j \in \{2, \ldots, n\}$. $x \in A \rtimes K_j$, so there exist unique elements $k_x \in K_j$ and $a_x \in A$ with $x = k_x a_x$. Then $x^{-1}k_x \in A$. Define $\varphi_j : K_2 \to A$ by $x \mapsto x^{-1}k_x$. Then φ_j is well-defined and $K_j = \{x(x\varphi_j) : x \in K_2\}$ since $x(x\varphi_j) = xx^{-1}k_x = k_x \in K_j$ and if $k \in K_j$, then $k = xa$ for some $x \in K_2$ and $a \in A$, so $k = k_x = xx^{-1}k_x = x(x\varphi_j)$. Let $x, y \in K_2$. Then

$$k_{xy}a_{xy} = xy = k_x a_x k_y a_y = (k_x k_y)(k_y^{-1} a_x k_y)a_y$$

and $(k_y^{-1}a_x k_y)a_y \in A$, so $k_{xy} = k_x k_y$. Then

$$(xy)\varphi_j = (xy)^{-1}k_{xy} = y^{-1}x^{-1}k_x k_y = y^{-1}(x\varphi_j)yy^{-1}k_y = y^{-1}(x\varphi_j)y(y\varphi_j)$$

for all $x, y \in K_2$. Also, if $h \in H$, then $h \in K_j$, so $a_h = 1$ and $h = k_h$. Thus $h\varphi_j = 1$ for all $h \in H$. Clearly $\varphi_2, \ldots, \varphi_n$ are all different since $K_2, \ldots, K_n$ are all different.

Now, suppose that we have a function $\varphi : K_2 \to A$ satisfying $h\varphi = 1$ for all $h \in H$ and $(xy)\varphi = y^{-1}(x\varphi)y(y\varphi)$ for all $x, y \in K_2$, which I will refer to as $(*)$. Let $B := \{x(x\varphi) : x \in K_2\}$. Clearly $1 \in B$. If $x(x\varphi), y(y\varphi) \in B$, then by $(*)$, $x(x\varphi)y(y\varphi) = xy(xy)\varphi \in B$. Taking $y = x^{-1}$ in $(*)$, we see that $1 = 1\varphi = x(x\varphi)x^{-1}(x^{-1}\varphi)$, so $(x(x\varphi))^{-1} = x^{-1}(x^{-1}\varphi) \in B$. Thus $B \leq G$. Of course $AB \leq G$. Let $xa \in A \rtimes K_2$ (where $x \in K_2$ and $a \in A$). Then $xa = x(x\varphi)(x\varphi)^{-1}a \in BA$, so $G = K_2A \leq BA$. Thus $AB = G$. Suppose that $B = G$. Then $A \leq B$, so if $a \in A$, then $a = x(x\varphi)$ for some $x \in K_2$, so $x \in A \cap K_2 = \{1\}$, which implies that $a = 1$, a contradiction. Thus $B < G$. Moreover, $H \leq B$ since if $h \in H$, then $h = h1 = h(h\varphi) \in B$. If $B = H$, then given $x \in K_2$, $x(x\varphi) \in B = H$, so $x\varphi \in A \cap K_2 = \{1\}$, so $x \in H$, a contradiction. Thus $H < B$. Since $H < B < G$, $B = K_i$ for some i. Let $x \in A \cap B$. Then $x = a = y(y\varphi)$ for some $a \in A$ and $y \in K_2$, which implies that $a(y\varphi)^{-1} = y \in K_2 \cap A = \{1\}$, so $x = 1$. Thus $A \cap B = \{1\}$. Note that if $A \cap K_1 = \{1\}$, then $H = (K_1 \cap A)H = K_1 \cap (AH) = K_1$, a contradiction, so $A \cap K_1$ is not trivial. Then $B \neq K_1$, so $B = K_j$ for some $j \in \{2, \ldots, n\}$. Let $x \in K_2$. Then $x(x\varphi_j) \in K_j$, so $x(x\varphi_j) = y(y\varphi)$ for some $y \in K_2$. But $y^{-1}x = (y\varphi)(x\varphi_j)^{-1} \in K_2 \cap A = \{1\}$, so $x = y$ and $x\varphi_j = x\varphi$. Thus $\varphi = \varphi_j$, so there are exactly $n - 1$ functions $\varphi : K_2 \to A$ satisfying $h\varphi = 1$ for all $h \in H$ and $(xy)\varphi = y^{-1}(x\varphi)y(y\varphi)$ for all $x, y \in K_2$, namely, $\varphi_2, \ldots, \varphi_n$.

Let $K := \{\varphi_j : 2 \leq j \leq n\}$. If $\varphi, \psi \in K$, let $x\varphi\psi := (x\varphi)(x\psi)$ for all $x \in K_2$. Let $x, y \in K_2$. Then

$$\begin{aligned}
xy(xy)\varphi\psi &= (xy(xy\varphi))(xy\psi) \\
&= x(x\varphi)y(y\varphi)(xy\psi) && \text{(by } (*)\text{)} \\
&= x(x\varphi)(y(xy\psi))(y\varphi) && \text{(since A is abelian)} \\
&= x(x\varphi)((x\psi)y(y\psi))(y\varphi) && \text{(by } (*)\text{)} \\
&= x(x\varphi)(x\psi)y(y\psi\varphi) \\
&= x(x\varphi\psi)y(y\varphi\psi) && \text{(since A is abelian)}
\end{aligned}$$

and if $h \in H$, then $h\varphi\psi = h\varphi h\psi = 1$. Thus $\varphi\psi \in K$, so we have a binary operation on K. Clearly $x\varphi_2 = 1$ for all $x \in K_2$. It follows that φ_2 is the identity of K. Note that A is abelian, hence solvable, but it is minimal normal in G, so by Proposition 1.7.2, A is an elementary abelian p-group for some prime p. Thus every element of A has order p. Then $x\varphi^p = (x\varphi)^p = 1$ for all $x \in K_2$ and $\varphi \in K$, so if $\varphi \neq \varphi_2$, then $\varphi^{-1} = \varphi^{p-1} \in K$. Thus K is an abelian group (since A is abelian). Moreover, every nontrivial element of K has order p, so K is an elementary abelian p-group. But $|K| = n - 1$, so $n - 1$ is a power of a prime, as desired. □

Let G be a finite group, and suppose that the interval $[H, G]$ in the subgroup lattice of G is isomorphic to M_n where $n-1$ is not a power of a prime. Let N be the core of H in G. Then the interval $[H/N, G/N]$ in the subgroup lattice of G/N is also isomorphic to M_n. Moreover, H/N contains no nontrivial normal subgroup of G/N, so by Theorem 3.2.1, G/N contains no nontrivial abelian subgroup, which implies that G/N is not solvable. Thus G is not solvable. It follows that for $n - 1$ not a power of a prime, M_n is finitely representable if and only if M_n can be embedded as an interval into the subgroup lattice of a finite nonsolvable group.

3.3 Subdirectly Irreducible Case

A nontrivial group G is subdirectly irreducible if and only if G has a unique minimal normal subgroup (see [5, p. 63] for the definition of a subdirectly irreducible algebra). The smallest n for which $n - 1$ is not a power of a prime is of course 7. Köhler proved in [13] that a finite group minimal with respect to the property of its subgroup lattice containing an interval isomorphic to M_7 must be subdirectly irreducible, hoping that this would lead to a proof that M_7 is not finitely representable. Meanwhile, Feit showed in [9] that M_7 is actually finitely representable by embedding M_7 as an interval into the subgroup lattice of the alternating group on 31 letters (a nonsolvable group, of course). Thus the set of integers n for which $n-1$ is a power of a prime does not completely determine when M_n is finitely representable. Fortunately, Köhler's theorem generalizes quite easily, as he points

out in [13]. Here is the general version of Köhler's result; it differs only slightly from his proof of the case $n = 7$. We start with a lemma.

Lemma 3.3.1 (Köhler, [13])**.** *Let N_1 and N_2 be distinct minimal normal subgroups of a group G. Let $H \leq G$. Then the set of subgroups U of N_1N_2 satisfying*

(i) $U \cap N_1 = U \cap N_2 = \{1\}$,

(ii) $UN_1 = UN_2 = N_1N_2$, *and*

(iii) $H \leq N_G(U)$

is in 1-1 correspondence with the set of isomorphisms $\varphi : N_1 \to N_2$ satisfying $(h^{-1}xh)\varphi = h^{-1}(x\varphi)h$ for all $h \in H$ and $x \in N_1$.

Proof. Note that N_1 and N_2 centralize each other by Proposition 1.5.1. Let $U \leq N_1N_2$ for which (i), (ii) and (iii) hold. Define $\varphi_U : N_1 \to N_2$ by $n_1 \mapsto n_2$ where $n_1n_2 \in U$. If $x = y \in N_1$, then $x(x\varphi_U) \in U$ and $y(y\varphi_U) \in U$, so $(y\varphi_U)^{-1}y^{-1}x(x\varphi_U) = (y\varphi_U)^{-1}(x\varphi_U) \in U \cap N_2 = \{1\}$. Thus $y\varphi_U = x\varphi_U$, so φ_U is well-defined. Let $x, y \in N_1$. $x(x\varphi_U)$, $y(y\varphi_U)$ and $xy(xy\varphi_U) \in U$, so

$$\begin{array}{rl} & (y\varphi_U)^{-1}y^{-1}(x\varphi_U)^{-1}x^{-1}xy(xy\varphi_U) \\ = & (y\varphi_U)^{-1}y^{-1}(x\varphi_U)^{-1}y(xy\varphi_U) \\ = & (y\varphi_U)^{-1}(x\varphi_U)^{-1}y^{-1}y(xy\varphi_U) \\ = & (y\varphi_U)^{-1}(x\varphi_U)^{-1}(xy\varphi_U) \\ \in & U \cap N_2 \\ = & \{1\} \end{array}$$

Thus $(xy)\varphi_U = (x\varphi_U)(y\varphi_U)$, so φ_U is a homomorphism. Suppose that $x \in ker(\varphi_U)$. Then $x\varphi_U = 1$, so $x(x\varphi_U) = x \in U \cap N_1 = \{1\}$. Thus $x = 1$, so φ_U is 1-1. Let $n_2 \in N_2$. Then $n_2 \in N_1N_2 = UN_1$, so $n_2 = n_1^{-1}u$ for some $n_1 \in N_1$ and $u \in U$. Rearranging, we get that $n_1n_2 = u \in U$, so $n_1\varphi_U = n_2$, which implies that φ_U is onto. Thus φ_U is an isomorphism. Further, $(h^{-1}xh)\varphi_U = h^{-1}(x\varphi_U)h$ for all $h \in H$ and $x \in N_1$: $x(x\varphi_U) \in U$, so $h^{-1}x(x\varphi_U)h \in U$ by (iii), but $(h^{-1}xh)(h^{-1}xh\varphi_U) \in U$, so

$$(h^{-1}x(x\varphi_U)h)^{-1}(h^{-1}xh)(h^{-1}xh\varphi_U) = h^{-1}(x\varphi_U)^{-1}h(h^{-1}xh\varphi_U) \in U \cap N_2 = \{1\},$$

giving the desired result.

On the other hand, let $\varphi : N_1 \to N_2$ be an isomorphism that satisfies $(h^{-1}xh)\varphi = h^{-1}(x\varphi)h$ for all $h \in H$ and $x \in N_1$. I claim that $U_\varphi := \{x(x\varphi) : x \in N_1\}$ is a subgroup of N_1N_2 satisfying (i), (ii) and (iii). Clearly $1 \in U_\varphi$. Let $x(x\varphi), y(y\varphi) \in U_\varphi$. Then because N_1 and N_2 centralize each other and because φ is a homomorphism, $x(x\varphi)y(y\varphi) =$

$xy(x\varphi)(y\varphi) = xy(xy\varphi) \in U_\varphi$. Moreover, $(x(x\varphi))^{-1} = (x\varphi)^{-1}x^{-1} = x^{-1}(x^{-1}\varphi) \in U_\varphi$, so $U_\varphi \leq N_1N_2$. Now, let $y = x(x\varphi) \in N_1 \cap U_\varphi$. Then $x^{-1}y = x\varphi \in N_1 \cap N_2 = \{1\}$, so $x = 1$ since φ is 1-1, which implies that $y = 1$. Thus $N_1 \cap U_\varphi = \{1\}$. Let $y = x(x\varphi) \in N_2 \cap U_\varphi$. Then $y(x\varphi)^{-1} = x \in N_2 \cap N_1 = \{1\}$, so $x = 1$. Thus $N_2 \cap U_\varphi = \{1\}$ as well, so (i) is satisfied. Let $n_1n_2 \in N_1N_2$. $n_2 = x\varphi$ for some $x \in N_1$, so $xn_2 = x(x\varphi) \in U_\varphi$, but $n_1n_2 = (n_1x^{-1})(xn_2) \in N_1U_\varphi$, so $N_1N_2 \leq N_1U_\varphi \leq N_1N_2$. Thus $N_1U_\varphi = N_1N_2$. Further, $N_2U_\varphi = N_1N_2$ since if $n_1n_2 \in N_1N_2$, then $n_1n_2 = (n_1(n_1\varphi))((n_1\varphi)^{-1}n_2) \in U_\varphi N_2$, so (ii) is true. Let $h \in H$ and $x(x\varphi) \in U_\varphi$. Then $h^{-1}x(x\varphi)h = h^{-1}xh(h^{-1}xh\varphi) \in U_\varphi$ since $h^{-1}xh \in N_1$, satisfying (iii).

Lastly, I show that $\varphi_{U_\varphi} = \varphi$ and $U_{\varphi_U} = U$, which gives us the desired 1-1 correspondence. Let $x \in N_1$. $x(x\varphi_{U_\varphi}) \in U_\varphi$, so $x(x\varphi_{U_\varphi}) = y(y\varphi)$ for some $y \in N_1$. Then $y^{-1}x = (y\varphi)(x\varphi_{U_\varphi})^{-1} \in N_1 \cap N_2 = \{1\}$, so $y = x$, which implies that $x\varphi_{U_\varphi} = x\varphi$. Thus $\varphi_{U_\varphi} = \varphi$. Now, let $x(x\varphi_U) \in U_{\varphi_U}$. Then $x(x\varphi_U) \in U$, so $U_{\varphi_U} \leq U$. On the other hand, let $u \in U$. Then $u = n_1n_2$ for some $n_1 \in N_1$ and $n_2 \in N_2$. Since $n_1n_2 \in U$, $n_1\varphi_U = n_2$, so $u = n_1(n_1\varphi_U) \in U_{\varphi_U}$. Thus $U_{\varphi_U} = U$. □

Theorem 3.3.2 (Köhler, [13]). *Let G be a finite group. Suppose that the subgroup lattice of G contains an interval that is isomorphic to M_n ($n \geq 3$) where G is minimal with respect to this property. If $n-1$ is not a power of a prime, then G is subdirectly irreducible.*

Proof. Write the interval as $[H, K]$ where $H, K \leq G$. Then by the minimality of G, $K = G$. Let $K_1, \ldots, K_n$ denote the n atoms. Let N be a normal subgroup of G contained in H. Then the interval $[H/N : G/N]$ is isomorphic to M_n and $|G/N| \leq |G|$, so by the minimality of G, $N = \{1\}$. Thus H contains no nontrivial normal subgroup of G. Note that $n \geq 7$ since $n-1$ is not a power of a prime.

Suppose for a contradiction that G is not subdirectly irreducible. Then G does not have a unique minimal normal subgroup. Let N_1 and N_2 be distinct minimal normal subgroups of G. First I show that we may assume that for all $i \in \{1, 2\}$ and $j \in \{3, \ldots, n\}$, $G = N_i \rtimes K_j$, $HN_i = K_i$ and $H \cap N_1N_2 = \{1\}$.

If $N_i \leq K_j$ and $N_i \leq K_l$ for some $j \neq l$, then $N_i \leq K_j \cap K_l = H$, a contradiction as H contains no nontrivial normal subgroup of G. Thus both N_1 and N_2 can be contained in at most one of the groups $K_1, \ldots, K_n$. So we may assume without loss of generality that for $i \in \{1, 2\}$, $N_i \nleq K_j$ for all $j \in \{3, \ldots, n\}$. Then $N_iK_j = G$ for all $i \in \{1, 2\}$ and $j \in \{3, \ldots, n\}$ since $K_j < N_iK_j$. Fix $j \in \{3, \ldots, n\}$. $K_j \cap N_1 \trianglelefteq K_j$. Moreover, $K_j \cap N_1$ is normalized by N_2 since N_1 and N_2 centralize each other. Thus $K_j \cap N_1 \trianglelefteq K_jN_2 = G$. By our choice of j, $K_j \cap N_1 < N_1$, so by the minimality of N_1, $K_j \cap N_1 = \{1\}$. By symmetry, $K_j \cap N_2 = \{1\}$. Thus $G = N_i \rtimes K_j$ for all $i \in \{1, 2\}$ and $j \in \{3, \ldots, n\}$.

Of course $H < HN_i \leq G$ for $i \in \{1, 2\}$. Suppose that $HN_i = G$ for some i. Then $K_j = K_j \cap G = K_j \cap (N_iH) = (K_j \cap N_i)H = H$, a contradiction. Thus $HN_i = K_j$ for some

$j \in \{1,2\}$ since $N_i \not\leq K_j$ when $j \in \{3,\ldots,n\}$, so we may assume without loss of generality that $HN_1 = K_1$. Suppose for a contradiction that $HN_2 = K_1$. Then $N_1N_2 \leq K_1$, which implies that

$$K_j \cap N_1N_2 = K_j \cap K_1 \cap N_1N_2 = H \cap N_1N_2$$

for all $j \in \{2,\ldots,n\}$. $N_1N_2 \trianglelefteq G$, so $K_j \cap N_1N_2 \trianglelefteq K_j$. It follows that $H \cap N_1N_2 \trianglelefteq \langle K_2, K_3\rangle = G$, but $H \cap N_1N_2 \leq H$, so we must have that $H \cap N_1N_2 = \{1\}$. But then $N_1 = (N_1N_2 \cap K_3)N_1 = (N_1N_2) \cap (K_3N_1) = N_1N_2 \cap G = N_1N_2$, so $N_2 \leq N_1$, which cannot happen. Thus $HN_1 = K_1$ and $HN_2 = K_2$.

Note that $H \cap N_2 \leq K_3 \cap N_2 = \{1\}$. Moreover, since $HN_2 = K_2$ and $N_1 \leq K_1$,

$$HN_2 \cap N_1 = K_2 \cap N_1 = K_2 \cap K_1 \cap N_1 = H \cap N_1 \leq K_3 \cap N_1 = \{1\}.$$

Then

$$|HN_1N_2| = |HN_2||N_1| = |H||N_2||N_1| = |H||N_1N_2|$$

since $N_1 \cap N_2 = \{1\}$, so $H \cap N_1N_2 = \{1\}$, as desired.

Let $U_j := K_j \cap N_1N_2$ for all $j \in \{3,\ldots,n\}$. Then U_j is a subgroup of N_1N_2 satisfying (i), (ii) and (iii) of Lemma 3.3.1 for all j: fix $j \in \{3,\ldots,n\}$ and $i \in \{1,2\}$. Then $U_j \cap N_i = K_j \cap (N_1N_2 \cap N_i) = K_j \cap N_i = \{1\}$; $U_jN_i = (K_j \cap N_1N_2)N_i = N_1N_2 \cap (K_jN_i) = N_1N_2 \cap G = N_1N_2$; and since $N_1N_2 \trianglelefteq G$ and $H \leq K_j$, $H \leq N_G(U_j)$.

Moreover, if U is any subgroup of N_1N_2 satisfying (i), (ii) and (iii) of Lemma 3.3.1, then I claim that $U = U_j$ for some $j \in \{3,\ldots,n\}$. Note that $N_1N_2 \cap (HU) = (N_1N_2 \cap H)U = \{1\}U = U$. It then suffices to show that $HU = U_j$ for some $j \in \{3,\ldots,n\}$, for $U = HU \cap N_1N_2 = U_j \cap N_1N_2 = U_j$. Note that $H \leq HU \leq G$ since H normalizes U by (iii). If $H = HU$, then $U \leq H \cap N_1N_2 = \{1\}$, so $N_1 = UN_1 = UN_2 = N_2$ by (ii), a contradiction. If $HU = G$, then $N_1N_2 = U$, which implies that $N_1 \leq U$, but $U \cap N_1 = \{1\}$ by (i), a contradiction. Lastly, if $HU = K_i$ for some $i \in \{1,2\}$, then since $HN_i = K_i$, $N_i \leq K_i \cap N_1N_2 = HU \cap N_1N_2 = U$, contradicting $U \cap N_i = \{1\}$. Thus $HU = U_j$ for some $j \in \{3,\ldots,n\}$.

We conclude that there are exactly $n-2$ subgroups of N_1N_2 satisfying (i), (ii) and (iii) of Lemma 3.3.1, namely, $U_3,\ldots,U_n$. But then there are exactly $n-2$ isomorphisms $\varphi : N_1 \to N_2$ satisfying $(h^{-1}xh)\varphi = h^{-1}(x\varphi)h$ for all $h \in H$ and $x \in N_1$ by Lemma 3.3.1. Moreover, as defined in the proof of Lemma 3.3.1, these isomorphisms are $\varphi_{U_3},\ldots,\varphi_{U_n}$. Let $Y := \{\varphi_{U_3},\ldots,\varphi_{U_n}\}$ and

$$Z := \{\alpha \in Aut(N_1) : (h^{-1}xh)\alpha = h^{-1}(x\alpha)h \text{ for all } h \in H, x \in N_1\}.$$

Then $Z \leq Aut(N_1)$ since if $\alpha,\beta \in Z$, then $(h^{-1}(x\beta^{-1})h)\beta = h^{-1}xh$, so $(h^{-1}xh)\alpha\beta^{-1} = (h^{-1}(x\alpha)h)\beta^{-1} = h^{-1}(x\alpha\beta^{-1})h$. I claim that $Y = \{\alpha\varphi : \alpha \in Z\}$ for any $\varphi \in Y$. Let $\varphi \in Y$ be fixed, and let $\alpha \in Z$. Then $\alpha\varphi$ is an isomorphism from N_1 onto N_2 satisfying

$(h^{-1}xh)\alpha\varphi = h^{-1}(x\alpha\varphi)h$, so $\alpha\varphi \in Y$. Let $\psi \in Y$. Then $\psi\varphi^{-1} \in Aut(N_1)$ satisfying $(h^{-1}xh)\psi\varphi^{-1} = h^{-1}(x\psi\varphi^{-1})h$, so $\psi\varphi^{-1} \in Z$, proving the claim. Z is not trivial since $|Z| = |Y| = n-2 \geq 5$, so Z contains an element of prime order, say α, and $\alpha = \varphi_{U_j}\varphi_{U_3}^{-1}$ for some $j \neq 3$ since $Y = \{\alpha\varphi_{U_3} : \alpha \in Z\}$. Let $x \in N_1$ be a fixed point of α. Then $x = x\varphi_{U_j}\varphi_{U_3}^{-1}$, so $x\varphi_{U_3} = x\varphi_{U_j}$. Then $x(x\varphi_{U_3}) = x(x\varphi_{U_j}) \in U_3 \cap U_j = K_3 \cap K_j \cap N_1N_2 = H \cap N_1N_2 = \{1\}$, so $x\varphi_{U_3} = x^{-1} \in N_2 \cap N_1 = \{1\}$. Thus $x = 1$, so α is a fixed-point-free automorphism of prime order. Then by Thompson's Theorem (1.9.4), N_1 is nilpotent, hence solvable. But N_1 is a minimal normal subgroup of G, so N_1 is abelian by Proposition 1.7.2. Then by Theorem 3.2.1, $n-1$ is a power of a prime, a contradiction. □

Thus for $n-1$ not a power of a prime, M_n is finitely representable if and only if M_n can be embedded as an interval into the subgroup lattice of a finite nonsolvable group with a unique minimal normal subgroup.

3.4 Using the Proof of the O'Nan-Scott Theorem

Suppose that $n-1$ is not a power of a prime, and suppose that M_n is embedded as the interval $[H, G]$ into the subgroup lattice of a finite group G, where G is taken to be the smallest such group. By Theorem 3.3.2, G has a unique minimal normal subgroup, say M, and M is nonabelian by Theorem 3.2.1 since the minimality of G implies that H contains no nontrivial normal subgroup of G. Then $M \simeq T^k$ for some finite simple nonabelian group T and some positive integer k by Corollary 1.5.5 and is of course the socle of G. Thus the socle of G has the same structure as the socle of a finite primitive permutation group, which suggests, as previously discussed, that some of the methods used in the proof of the O'Nan-Scott Theorem might be applicable to this problem; indeed, Lemma 1.4.3 and part of the proof of Lemma 2.7.3 turn out to be fundamental in the next reduction of the problem of finitely representing M_n.

In addition to the assumptions already made, suppose that G is not almost simple, $M \cap H \neq \{1\}$ and $n > 50$. Lucchini then proves in [16] that we must have

$$n = q + 2 \text{ or } n = \frac{q^t + 1}{q + 1} + 1$$

where q is a prime power and t is an odd prime, which is good since he also proves in [15] that for such n, M_n is finitely representable. Note that the case $n = 7$ is included. Let us examine Lucchini's reduction in more detail.

First, make note of the following: since M is the socle of G and T is nonabelian, $C_G(M) = \{1\}$ by Proposition 1.5.6. Let $g \in G$, and define $\varphi_g \in Aut(M)$ to be conjugation by g. Define $\varphi : G \to Aut(M)$ by $g \mapsto \varphi_g$. φ is clearly a homomorphism, and if $g \in ker(\varphi)$, then $g^{-1}mg = m$ for all $m \in M$, so $g \in C_G(M) = \{1\}$, which implies that φ is 1-1. Thus G is embedded in $Aut(M) = Aut(T^k) \simeq (Aut(T))^k \rtimes S_k$ by Proposition 1.6.1.

Lucchini's reduction has three steps. First, he proves that there exists a proper nontrivial subgroup R of T that is self-normalizing in T such that $M \cap H = \{(t, \ldots, t) : t \in R\}$ and that in this case, there are exactly $n-1$ H-invariant full diagonal subgroups of M containing $M \cap H$. Second, $R \leq T \simeq Inn(T)$, so R can be embedded into $Aut(T)$. Then $R \trianglelefteq N_{Aut(T)}(R)$ and $R \leq Inn(T)$, so $R \trianglelefteq N_{Aut(T)}(R) \cap Inn(T) \leq Inn(T)$, but R is self-normalizing in $Inn(T)$, so $R = N_{Aut(T)}(R) \cap Inn(T)$. Then

$$N_{Aut(T)}(R)/R = N_{Aut(T)}(R)Inn(T)/Inn(T) \leq Out(T),$$

so if $Out(T)$ is abelian, then $N_{Aut(T)}(R)/R$ is abelian. He uses the fact that any full diagonal subgroup of M has the form

$$\{(t\gamma_1, t\gamma_2, \ldots, t\gamma_k) : t \in T, \text{ for some } \gamma_i \in Aut(T)\}$$

(see (1) in the proof of Lemma 1.4.1(i)) and that $G \leq (Aut(T))^k \rtimes S_k$ to show that if $N_{Aut(T)}(R)/R$ is abelian, then $[H, G] \simeq M_{q+1}$ where q is a prime power, a contradiction. Lucchini thus assumes that $Out(T)$ is not abelian so that T must be of Lie type. He finishes the second step in his reduction by proving that if T is not $PSL_n(q)$ or $PSU_n(q)$, then we again have that $n-1$ is a power of a prime (this is where the assumption that $n > 50$ is required). Lastly, if T is $PSL_n(q)$ or $PSU_n(q)$, Lucchini proves that n falls into one of the two categories stated above. I will examine the details of the first step of Lucchini's reduction as it is this step that shares many similarities with the proof of the O'Nan-Scott Theorem.

Theorem 3.4.1 (Lucchini, [16])**.** *Let G be a finite group, and suppose that G contains a subgroup H such that the interval $[H, G]$ is isomorphic to M_n ($n \geq 3$) where G is minimal with respect to this property. Let M be the socle of G. If $n-1$ is not a power of a prime, G is not almost simple and $M \cap H \neq \{1\}$, then $M \cap H = \{(t, \ldots, t) : t \in R\}$ for some $1 < R < T$ such that R is self-normalizing in T. Moreover, there are exactly $n-1$ H-invariant full diagonal subgroups of M containing $M \cap H$.*

Before I begin the proof, note the following. Let Ω be the right coset space $G\backslash H$, and let $\alpha := H$, so that $G_\alpha = H$ and $M_\alpha = M \cap H$. This is a transitive faithful action as H containing no nontrivial normal subgroups of G implies that H is core-free in G. Of course, it is not a primitive action since G_α is not a maximal subgroup of G, but this is of no consequence, as we shall see. Keep this construction in mind throughout the following proof.

Proof of 3.4.1. We have seen already that G is not solvable and that M is the nonabelian unique minimal normal subgroup of G. Then $M \simeq T^k$ for some simple nonabelian group T and some integer $k \geq 2$ (as G is not almost simple), so we may write $M = T_1 \times \cdots \times T_k$

where $T_i \simeq T$ for all i. Let $K_1, \ldots, K_n$ be the n atoms of $[H, G]$. As we saw in the proof of Theorem 3.3.2, H contains no nontrivial normal subgroup of G since G is minimal. Thus $H < HM$. If $HM < G$, then $HM = K_i$ for some i, so choosing $j \neq i$ we get that $M \cap H = M \cap (K_i \cap K_j) = M \cap K_j \trianglelefteq K_j$. It follows that if $j \neq i$ and $l \neq i$, then $M \cap H \trianglelefteq \langle K_j, K_l \rangle = G$, but $M \cap H \leq H$, so $M \cap H = \{1\}$, a contradiction. Thus $HM = G$.

When dealing with primitive permutation groups G, we often focus on the G_α-invariant subgroups of the socle containing the stabilizer of the socle instead of the entire group G. We can do the same thing here because it turns out that the interval $[H, G]$ is isomorphic to the lattice of all H-invariant subgroups of M containing $H \cap M$, which is denoted by $[H \cap M, M]_H$. To see this, let $H \leq K \leq G$. Then $K \cap M$ is an H-invariant subgroup of M containing $H \cap M$. Let L be another subgroup of G containing H. Clearly, if $K \leq L$, then $K \cap M \leq L \cap M$. Conversely, if $K \cap M \leq L \cap M$, then $K = K \cap MH = (K \cap M)H \leq (L \cap M)H = L$. Moreover, if $K \cap M = L \cap M$, then $K = L$. Now, let K be an H-invariant subgroup of M containing $H \cap M$. Then $H \leq HK \leq G$ and $HK \cap M = K(H \cap M) = K$. Hence, $[H \cap M, M]_H \simeq [H, G] \simeq M_n$.

Since $G = HM$ and M is a minimal normal subgroup of G, H acts transitively by conjugation on $\{T_1, \ldots, T_k\}$, so there exist $1 = h_1, h_2 \ldots, h_k \in H$ such that $T_i = h_i^{-1} T_1 h_i$ for all i. As usual, let $\rho_i : M \to T_i$ denote the i-th projection map.

Let K be an H-invariant subgroup of M. If $h \in H$ and $h^{-1} T_i h = T_j$, then as we saw in the proof of the O'Nan-Scott Theorem, $h^{-1}(K\rho_i)h = (h^{-1}Kh)\rho_j = K\rho_j$; in particular, $h_i^{-1}(K\rho_1)h = K\rho_i$. It follows from this and from the transitivity of the action of H on $\{T_1, \ldots, T_k\}$ that if $K\rho_j = T_j$ for some $j \in \{1, \ldots, k\}$, then $K\rho_i = T_i$ for all $i \in \{1, \ldots, k\}$. Hence in this case, K is a subdirect subgroup of M and we know the structure of K by Lemma 1.4.1. On the other hand, suppose that $K\rho_i < T_i$ for all i. Since H is transitive on $\{T_1, \ldots, T_k\}$ and $h^{-1} T_i h = T_j$ implies that $h^{-1} K \rho_i h = K\rho_j$ (where $h \in H$), the proof of Lemma 2.7.3 with X_i taken to be T_i and X_α taken to be $K\rho_i$ carries through; that is, $K\rho_1$ is normalized by $N_H(T_1)$, and if $K\rho_1 \leq S \leq T_1$ where S is $N_H(T_1)$-invariant, then $S^{h_1} \times \cdots \times S^{h_k}$ is an H-invariant subgroup of M containing K (since $K \leq K\rho_1 \times \cdots \times K\rho_k$). Moreover, suppose that $H \cap M < K$, and let S be a proper $N_H(T_1)$-invariant subgroup of T_1 containing $K\rho_1$. Then since $[H \cap M, M]_H \simeq M_n$ and $K \leq (K\rho_1)^{h_1} \times \cdots \times (K\rho_1)^{h_k} \leq S^{h_1} \times \cdots \times S^{h_k} < M$, $K = S^{h_1} \times \cdots \times S^{h_k}$ and $S = K\rho_1$. Thus any maximal H-invariant subgroup of M is either a subdirect subgroup of M or has the form $S^{h_1} \times \cdots \times S^{h_k}$ where S is a maximal $N_H(T_1)$-invariant subgroup of T_1 (namely, the projection of the H-invariant maximal subgroup on T_1).

Now, we consider the structure of $H \cap M$. Suppose for a contradiction of the minimality of G that $H \cap M$ is a subdirect subgroup of M. Then $H \cap M = D_1 \times \cdots \times D_m$ for some $m \geq 1$ where D_i is a full diagonal subgroup of some subproduct $X_i := \prod_{j \in I_i} T_j$ such that $\{1, \ldots, k\}$ is partitioned by the I_i. Without loss of generality, we may assume that $x\rho_r = x\rho_s$ for all

$x \in D_i$, $r, s \in I_i$ and $i \in \{1, \ldots, m\}$. Note that $D_i = (H \cap M) \cap X_i = H \cap X_i$ for all i. Then by Lemma 1.4.3 with A taken to be H, H permutes $\{X_1, \ldots, X_m\}$ by conjugation, and this action is transitive since H acts transitively on $\{T_1, \ldots, T_k\}$. We may of course define an action of H on $\{1, \ldots, k\}$ by $i^h := j$ if $h^{-1}T_i h = T_j$. It follows that H acts transitively on $\{I_1, \ldots, I_m\}$. In particular, $\mathcal{D} := \{I_1, \ldots, I_m\}$ forms a system of blocks on $\{1, \ldots, k\}$ (by which I mean a partition of $\{1, \ldots, k\}$ made up of blocks under the action of H on $\{1, \ldots, k\}$), and if I is the block containing 1, then $\mathcal{D} = \{I^h : h \in H\}$.

Let J be a block on $\{1, \ldots, k\}$ containing 1 that is contained in I, and note the following two facts. If $\emptyset \neq J' \subseteq J$, then $H_{J'} \leq H_J$: let $h \in H_{J'}$. Then $J'^h = J' \subseteq J$, but $J'^h \subseteq J^h$, so $J \cap J^h \neq \emptyset$. Thus $J^h = J$ and $h \in H_J$, as desired. Second, $J = \{1^h : h \in H_J\}$: $1 \in J$, so if $h \in H_J$, then $J^h = J$, which implies that $1^h \in J$. Conversely, if $j \in J$, then there exists an $h \in H$ with $j = 1^h \in J^h$, so $j \in J \cap J^h$, which implies that $J = J^h$; that is, $h \in H_J$.

Let K be an H-invariant subgroup of M containing $H \cap M$. Then $T_i = (H \cap M)\rho_i \leq K\rho_i$, so K is also a subdirect subgroup of M, which implies that $K = E_1 \times \cdots \times E_l$ for some $l \geq 1$ where E_i is a full diagonal subgroup of some subproduct $\prod_{j \in J_i} T_j$ such that $\{1, \ldots, k\}$ is partitioned by the J_i. Let $\pi_j : K \to E_j$ be the projection map, and let $\pi_{i,j} := \pi_j|_{D_i}$. Now, $ker(\pi_{i,j}) = D_i$ or $\{1\}$ since D_i is simple. Clearly if $ker(\pi_{i,j}) = D_i$, then $I_i \cap J_j = \emptyset$. Suppose then that $ker(\pi_{i,j}) = \{1\}$; since $D_i \simeq T \simeq E_j$, $\pi_{i,j}$ must be an isomorphism. Then if $(t_1, \ldots, t_r) \in E_j$, there exists a $(t, \ldots, t) \in D_i$ with $(t, \ldots, t)\pi_{i,j} = (t_1, \ldots, t_r)$, so $t_i = t$ for all i and $J_j \subseteq I_i$. Hence, either $I_i \cap J_j = \emptyset$ or $J_j \subseteq I_i$. Note as well that $x\rho_r = x\rho_s$ for all $x \in E_j$, $r, s \in J_j$ and $j \in \{1, \ldots, l\}$, which I will refer to as $(*)$. Let $Y_i := \prod_{j \in J_i} T_j$ and $\mathcal{E} := \{J_1, \ldots, J_l\}$. Since $E_i = Y_i \cap K$ and K is an H-invariant subgroup of M containing $H \cap M$, H acts by conjugation on $\{E_1, \ldots, E_l\}$ and $\{Y_1, \ldots, Y_l\}$ by Lemma 1.4.3 with A taken to be H. Thus $\mathcal{E}$ is a system of blocks which refines $\mathcal{D}$. Let J be the block in $\mathcal{E}$ containing 1. Then $\mathcal{E} = \{J^h : h \in H\}$ and $J \cap I \neq \emptyset$, so $J \subseteq I$. It follows that $H_1 \leq H_J \leq H_I$.

Let K' be another H-invariant subgroup of M containing $H \cap M$, and let $\mathcal{E}'$ be the system of blocks associated with K', so that $\mathcal{E}' = \{J'^h : h \in H\}$ where J' is the block in $\mathcal{E}'$ containing 1. Suppose first that $K \leq K'$. Then, by the same argument which proved that $\mathcal{E}$ refines $\mathcal{D}$, we have that $\mathcal{E}'$ refines $\mathcal{E}$; in particular, $J' \subseteq J$, so $H_{J'} \leq H_J$. Conversely, suppose that $H_{J'} \leq H_J$. Then $J' = \{1^h : h \in H_{J'}\} \leq \{1^h : h \in H_J\} = J$, so $\mathcal{E}'$ refines $\mathcal{E}$, which implies that $K \leq K'$ by $(*)$. Moreover, if $H_J = H_{J'}$, then $K = K'$. Thus we have defined a 1-1 order-reversing map from the set of H-invariant subgroups of M containing $H \cap M$ to the set of subgroups of H_I containing H_1; now I prove that this map is onto.

Let L be a subgroup of H_I containing H_1. Then I claim that $L = H_J$ where $J := \{1^h : h \in L\}$. If $j \in J$ and $h \in L$, then clearly $j^h \in J$, so $J^h \subseteq J$. Note that if $i^h = j^h$ where $i, j \in J$, then $h^{-1}T_i h = h^{-1}T_j h$, which implies that $i = j$. Since we then get that $|J| \leq |J^h|$, $J^h = J$. Hence, $L \leq H_J$. On the other hand, let $h \in H_J$. Then $J^h = J$, so

$1^h \in J$. This implies that $1^h = 1^{h'}$ for some $h' \in L$, but then $1^{h'h^{-1}} = 1$, so $h'h^{-1} \in H_1 \leq L$. Hence, $h \in L$ and $L = H_J$. Moreover, suppose that $h \in H$ and $J^h \cap J \neq \emptyset$. Then there exist $h', h'' \in L$ such that $1^{h'h} = 1^{h''}$ or $1^{h'hh''^{-1}} = 1$, which implies that $h'hh''^{-1} \in H_1 \leq L$, hence that $h \in L$ and $J^h = J$. Thus J is a block, which implies that J^h is a block for every $h \in H$. It follows from the transitivity of H on $\{1, \ldots, k\}$ that $\mathcal{E} := \{J^h : h \in H\}$ is a system of blocks on $\{1, \ldots, k\}$. Since $J \subseteq I$ and $\mathcal{D} = \{I^h : h \in H\}$, $\mathcal{E}$ refines $\mathcal{D}$. Write $\mathcal{E}$ as $\{J_1, \ldots, J_l\}$ where $\{1, \ldots, k\}$ is a disjoint union of the J_i. Let $Y_i := \prod_{j \in J_i} T_j$ and

$$E_i := \{x \in M : x\rho_r = x\rho_s \text{ for all } r, s \in J_i \text{ and } x\rho_r = 1 \text{ if } r \notin J_i\}.$$

Then E_i is a full diagonal subgroup of Y_i for all i. Let $K := E_1 \times \cdots \times E_l$. Then $H \cap M \leq K \leq M$ since $\mathcal{E}$ refines $\mathcal{D}$, and K is H-invariant since H permutes $\{J_1, \ldots, J_l\}$. Hence, the lattice $[H \cap M, M]_H$ is isomorphic to the dual of the lattice $[H_1, H_I]$, but M_n is self dual, so $[H_1, H_I]$ itself is isomorphic to M_n. This is a contradiction of the minimality of G since $H_I \leq H < G$.

We may assume, therefore, that $R_i := (H \cap M)\rho_i < T_i$ for all i. Note that $\{1\} < R_1 < T_1$ (as $H \cap M$ is nontrivial). Suppose now that every proper H-invariant subgroup of M is not a subdirect subgroup of M, again for a contradiction of the minimality of G. Let L_1 and L_2 be two maximal H-invariant subgroups of M. Then for $i \in \{1, 2\}$, $L_i = S_i^{h_1} \times \cdots \times S_i^{h_k}$ where $S_i = L_i\rho_1$ is a maximal $N_H(T_1)$-invariant subgroup of T_1 (see earlier in the proof). Then $R_1 \leq S_1 \cap S_2$, which gives us the following:

$$\begin{aligned} R_1^{h_1} \times \cdots \times R_1^{h_k} &\leq (S_1 \cap S_2)^{h_1} \times \cdots \times (S_1 \cap S_2)^{h_k} \\ &= L_1 \cap L_2 \\ &= H \cap M \\ &\leq R_1^{h_1} \times \cdots \times R_1^{h_k}. \end{aligned}$$

Thus $H \cap M = R_1^{h_1} \times \cdots \times R_1^{h_k}$.

Now, let K be an H invariant subgroup of M containing $H \cap M$. Then $K = S^{h_1} \times \cdots \times S^{h_k}$ where $R_1 \leq S \leq T_1$ and S is $N_H(T_1)$-invariant. On the other hand, let S be an $N_H(T_1)$-invariant subgroup of T_1 containing R_1. Then $K := S^{h_1} \times \cdots \times S^{h_k}$ is an H-invariant subgroup of M containing $H \cap M$ as we saw near the beginning of this proof (with K taken to be $H \cap M$). It is then routine to verify that the lattice $[H \cap M, M]_H$ must be isomorphic to the lattice $[R_1, T_1]_{N_H(T_1)}$.

Much like in the proof of the O'Nan-Scott Theorem, define $G^* := N_G(T_1)/C_G(T_1)$ and $H^* := N_H(T_1)C_G(T_1)/C_G(T_1)$. Note the following:

$$N_G(T_1) = N_G(T_1) \cap HM = N_H(T_1)M \leq N_H(T_1)T_1C_G(T_1) \leq N_G(T_1),$$

so $N_G(T_1) = N_H(T_1)T_1C_G(T_1)$. Moreover, we have the following:

$$\begin{aligned}
& N_H(T_1)C_G(T_1) \cap T_1 \\
= \;& [(N_G(T_1) \cap H)C_G(T_1)] \cap T_1 \\
= \;& N_G(T_1) \cap HC_G(T_1) \cap T_1 \\
= \;& HC_G(T_1) \cap T_1 \\
= \;& R_1 \times \cdots \times R_k C_G(T_1) \cap T_1 \\
= \;& R_1 C_G(T_1) \cap T_1 \qquad\qquad (R_2 \times \cdots \times R_k \leq C_G(T_1)) \\
= \;& R_1(C_G(T_1) \cap T_1) \\
= \;& R_1\{1\} \\
= \;& R_1.
\end{aligned}$$

Let $U/C_G(T_1)$ be a subgroup of G^* containing H^*. Then

$$R_1 = N_H(T_1)C_G(T_1) \cap T_1 \leq U \cap T_1 \leq T_1,$$

and $U \cap T_1$ is $N_H(T_1)$-invariant since $N_H(T_1) \leq U$ and $N_H(T_1) \leq N_G(T_1)$. Let $V/C_G(T_1)$ be another subgroup of G^* containing H^*. If $U/C_G(T_1) \leq V/C_G(T_1)$, then of course $U \cap T_1 \leq V \cap T_1$. Conversely, suppose that $U \cap T_1 \leq V \cap T_1$. Then

$$\begin{aligned}
U \;& = U \cap N_G(T_1) \\
& = U \cap (T_1 C_G(T_1) N_H(T_1)) \\
& = (U \cap T_1) C_G(T_1) N_H(T_1) \\
& \leq (V \cap T_1) C_G(T_1) N_H(T_1) \\
& = V.
\end{aligned}$$

Moreover, if $U \cap T_1 = V \cap T_1$, then $U = V$. Now, suppose that U is an $N_H(T_1)$-invariant subgroup of T_1 containing R_1. Then $H^* \leq UN_H(T_1)C_G(T_1)/C_G(T_1) \leq G^*$ and

$$UN_H(T_1)C_G(T_1) \cap T_1 = U(N_H(T_1)C_G(T_1) \cap T_1) = UR_1 = U.$$

Thus $[H^*, G^*] \simeq [R_1, T_1]_{N_H(T_1)} \simeq M_n$. If $T_1 \trianglelefteq G$, then G is almost simple; hence, $N_G(T_1) < G$, which implies that $|G^*| < |G|$, giving us our desired contradiction.

Thus there is at least one H-invariant maximal subgroup of M that is a subdirect subgroup of M, call it C. Then $C = D_1 \times \cdots \times D_m$ for some $m \geq 1$ where D_i is a full diagonal subgroup of some subproduct $X_i := \prod_{j \in I_i} T_j$ such that $\{1, \ldots, k\}$ is partitioned by the I_i. Without loss of generality, we may assume that $x\rho_r = x\rho_s$ for all $x \in D_i$, $r, s \in I_i$ and $i \in \{1, \ldots, m\}$. Since C is H-invariant, we have again that H permutes $\{D_1, \ldots, D_m\}$ and $\{X_1, \ldots, X_m\}$ by conjugation by Lemma 1.4.3. This action is transitive since H acts transitively on $\{T_1, \ldots, T_k\}$. Note that since C is a maximal H-invariant subgroup of M, $\mathcal{D} := \{I_1, \ldots, I_m\}$ is a system of blocks which cannot be refined to a smaller nontrivial

system (as we saw earlier in the proof). Also, by the transitivity of the action of H, there exist $1 = y_1, y_2, \ldots, y_m \in H$ with $D_i = D_1^{y_i}$.

$R_1 \times \cdots \times R_k$ is a proper H-invariant subgroup of M containing $H \cap M$. Suppose for a contradiction that $H \cap M = R_1 \times \cdots \times R_k$. Then $R_1 \times \cdots \times R_k \leq C$, so $\prod_{i \in I_1} R_i \leq D_1$. Since any R_i is nontrivial, it follows that I_1 can only contain 1 element, but then $D_1 = T_1$, which implies that $C = M$ by transitivity, a contradiction. Thus $R_1 \times \cdots \times R_k$ is a maximal H-invariant subgroup of M. Now, let U be a maximal H-invariant subgroup of M satisfying $U\rho_i < T_i$ for all i. Then $U\rho_1 \times \cdots \times U\rho_k$ is a proper H-invariant subgroup of M containing $R_1 \times \cdots \times R_k$ and U, both of which are maximal H-invariant subgroups of M, so $U = R_1 \times \cdots \times R_k$. Thus $R_1 \times \cdots \times R_k$ is the unique maximal H-invariant subgroup of M containing $H \cap M$ that is not a subdirect subgroup of M. Moreover, it follows that there are exactly $n - 1$ H-invariant subdirect subgroups of M containing $H \cap M$.

Fix $i \in \{1, \ldots, m\}$, and let $s, t \in I_i$. If $x \in R_s$, then $x = y\rho_s$ for some $y \in H \cap M$. But $H \cap M \leq D_1 \times \cdots \times D_m$, so $y\rho_s = y\rho_t$, which implies that $x \in R_t$. By symmetry, we get that $R_s = R_t$. Choose $r_i \in I_i$. Let $\mathcal{R}_i$ denote the full diagonal subgroup of $R_{r_i}^{|I_i|}$. Then $H \cap M = R_1 \times \cdots \times R_k \cap D_1 \times \cdots \times D_m \leq \mathcal{R}_1 \times \cdots \times \mathcal{R}_m < R_1 \times \cdots \times R_k$ since I_i must contain at least two elements (or else we again get that $C = M$). Moreover, $\mathcal{R}_1 \times \cdots \times \mathcal{R}_m$ is H-invariant. Thus $H \cap M = \mathcal{R}_1 \times \cdots \times \mathcal{R}_m$.

Now for our final reduction! Let $X := X_1$. Note that $\mathcal{R}_1$ is an $N_H(X)$-invariant subgroup of X. Moreover, $\prod_{i \in I_1} R_i$ is an $N_H(X)$-invariant subgroup of X containing $\mathcal{R}_1$. Let K be a proper H-invariant subgroup of M containing $H \cap M$ such that $K \neq H \cap M$ and $K \neq R_1 \times \cdots \times R_k$. Then K is a subdirect subgroup of M, so as usual we have that $K = E_1 \times \cdots \times E_l$ for some $l \geq 1$ where E_i is a full diagonal subgroup of some subproduct $\prod_{j \in J_i} T_j$ such that $\{1, \ldots, k\}$ is partitioned by the J_i. Let $Y_i := \prod_{j \in J_i} T_j$ and $\mathcal{E} := \{J_1, \ldots, J_l\}$. As before, $\mathcal{E}$ forms a system of blocks for the action of H on $\{1, \ldots, k\}$. But $\mathcal{R}_1 \times \cdots \times \mathcal{R}_m = H \cap M \leq K = E_1 \times \cdots \times E_l$, so $\mathcal{E}$ refines $\mathcal{D}$. Thus $\mathcal{E} = \mathcal{D}$ as $\mathcal{D}$ cannot be refined. It follows that E_1 is an $N_H(X)$-invariant subgroup of X containing $\mathcal{R}_1$ and $E_i = E_1^{y_i}$. If $E_1 = F_1$ where $L = F_1 \times \cdots \times F_m$ is another such H-invariant subgroup of M, then $K = L$ since $E_i = E_1^{y_i} = F_1^{y_i} = F_i$ for all i. Let U be an $N_H(X)$-invariant subgroup of X containing $\mathcal{R}_1$. Then $U^{y_1} \times \cdots \times U^{y_m}$ is an H-invariant subgroup of M containing $H \cap M$. This isomorphism is clearly order preserving, so we have proved that the lattice $[H \cap M]_H$ is isomorphic to the lattice $[\mathcal{R}_1, X]_{N_H(X)}$.

Define $G^* := N_G(X)/C_G(X)$ and $H^* := N_H(X)C_G(X)/C_G(X)$. Then, repeating the proof we saw earlier with T_1 replaced by X, we get that

$$[H^*, G^*] \simeq [\mathcal{R}_1, X]_{N_H(X)} \simeq M_n.$$

If $n > 1$, then $I_1 < \{1, \ldots, k\}$, which implies that X is not a normal subgroup of G. Then $N_G(X) < G$, so $|G^*| < |G|$, contradicting the minimality of G. Thus we may assume

that $m = 1$ (in which case $X = M$, so $N_G(X) = G$ and $C_G(X) = \{1\}$, which implies that $G^* \simeq G$). Note here another similarity to the proof of the O'Nan-Scott Theorem: in one case, the definition of G^* involves one simple factor of M (namely, T_1), and in the other case, a product of at least two simple factors of M (namely, X), and both cases use essentially the same proof to arrive at essentially the same contradiction.

Let $R := R_{r_1}$. Then $1 < R < T$ and $M \cap H = \{(t, \ldots, t) : t \in R\}$. Moreover, the $n-1$ H-invariant subdirect subgroups of M containing $M \cap H$ must also be full diagonal subgroups of M, and the remaining H-invariant subgroup of M containing $H \cap M$ is $R_1 \times \cdots \times R_k = R^k$ since $R_i = R$ for all $i \in I_1 = \{1, \ldots, k\}$. It remains to show that R is self-normalizing in T. Since $1 < R < T$ and T is simple, $N_T(R) < T$. Then $R^k \leq (N_T(R))^k < M$. $(N_T(R))^k$ is H-invariant since R is H-invariant (if $h \in H$, then for some j, $h^{-1}Rh = R_j = R$). Thus $R^k = (N_T(R))^k$, so R is self-normalizing in T, as desired. □

3.5 $n \leq 50$

Thus the problem of finitely representing M_n has been reduced to the cases when G is almost simple, $H \cap M = \{1\}$ or $n \leq 50$ (along with the set of assumptions made at the beginning of Section 3.4). What about this last case? If $n = 1$, then M_n is isomorphic to the subgroup lattice of $\mathbb{Z}_4$, and if $n = 2$, then M_n is isomorphic to the subgroup lattice of $\mathbb{Z}_2 \times \mathbb{Z}_3$. It is easy to verify that either $n-1$ or $n-2$ is a power of a prime, hence finitely representable, for all integers n between 3 and 50 with the exception of the integers 16, 22, 23, 35, 36, 40, 41, 46 and 47. Moreover,

$$22 = \frac{5^3 + 1}{5 + 1} + 1,$$

so M_{22} is finitely representable. However, suppose, for example, that

$$16 = \frac{q^t + 1}{q + 1} + 1$$

for some q a prime power and t an odd prime. Then $14 = q(q^{t-1} - 15)$, so $q \mid 14$, which implies that $q = 2$ or $q = 7$. Then $44 = 2^t$ or $119 = 7^t$, both contradictions. Similarly, it can be verified that, besides 22, none of the other integers listed above satisfy this equation. Thus it is unknown whether M_n is finitely representable for $n = 16$, 23, 35, 36, 40, 41, 46 and 47.

3.6 Almost Simple Case and Beyond

We are left with the cases when G is almost simple or $M \cap H = \{1\}$. When $M \cap H = \{1\}$, Baddeley and Lucchini have reduced the set of integers n for which M_n is finitely

representable to a subset of the natural numbers that is associated with questions about almost simple groups. Their proof and their results, even, are quite technical; see [2].

Hence, besides the eight cases under fifty in Section 3.5, the problem of finitely representing M_n has been completely reduced to problems that concern almost simple groups. Baddeley and Lucchini are optimistic that the classification of the finite simple groups will answer these questions about almost simple groups in such a way that leads to a negative answer for finite representability. Just like with finite primitive permutation groups, we must focus on the almost simple case. Hopefully, such a focus will not only lead to a solution to the problem of finite representability but will also answer other open problems in finite group theory.

Bibliography

[1] M. Aschbacher, *The subgroup structure of finite alternating and symmetric groups*, users.dimi.uniud.it/∼mario.mainardis/scuolaestiv2008/venotes.pdf, October 2008.

[2] R. Baddeley and A. Lucchini, 'On representing finite lattices as intervals in subgroup lattices of finite groups ', *J. Algebra* **196** (1997), 1-100.

[3] J. Bamberg, *Permutation Group Theory*, homepages.vub.ac.be/∼pcara/Teaching/PermGrps/PermGroups.pdf, December 2008.

[4] J. Bamberg and C. E. Praeger, 'Finite permutation groups with a transitive minimal normal subgroup', *Proc. London Math. Soc.* (3) **89** (2004), 71-103.

[5] S. Burris and H. P. Sankappanavar, *A course in universal algebra* (Springer, New York-Berlin-Heidelberg, 1981).

[6] P. J. Cameron, *Permutation Groups* (Cambridge University Press, Cambridge, 1999).

[7] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups* (Oxford University Press, Eynsham, 1985).

[8] J. D. Dixon and B. Mortimer, *Permutation groups* (Springer, New York-Berlin-Heidelberg, 1996).

[9] W. Feit, 'An interval in the subgroup lattice of a finite group which is isomorphic to M_7', *Algebra Universalis* **17** (1983), 220-221.

[10] G. Grätzer and E. T. Schmidt, 'Characterizations of congruence lattices of abstract algebra', *Acta Sci. Math (Szeged)* **24** (1963), 34-59.

[11] D. Gorenstein, 'The classification of finite simple groups. I. Simple groups and local analysis', *Bull. Amer. Math. Soc.* **1** (1979), 43-199.

[12] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups*, Math. Surveys and Monographs 40.1 (American Mathematical Society, Providence-Rhode Island, 1994).

[13] P. Köhler, 'M_7 as an interval in a subgroup lattice', *Algebra Universalis* **17** (1983), 263-266.

[14] M. W. Liebeck, C. E. Praeger and J. Saxl, 'On the O'Nan-Scott theorem for finite primitive permutation groups', *J. Austral. Math. Soc. (A)* **44** (1988), 389-396.

[15] A. Lucchini, 'Representation of certain lattices as intervals in subgroup lattices', *J. Algebra* **164** (1994), 85-90.

[16] A. Lucchini, 'Intervals in subgroup lattices of finite groups', *Comm. Algebra* **22** (1994), 529-549.

[17] B. H. Neumann, 'Twisted wreath products of groups', *Arch. Math.* **14** (1963), 1-6.

[18] P. P. Pálfy and P. Pudlák, 'Congruence lattices of finite algebras and intervals in subgroup lattices', *Algebra Universalis* **11** (1980), 22-27.

[19] D. J. S. Robinson, *A course in the theory of groups* (Springer, New York-Berlin-Heidelberg, 1996).

[20] J. Rotman, *An introduction to the theory of groups* (Springer, New York-Berlin-Heidelberg, 1995).

[21] R. Schmidt, *Subgroup lattices of groups* (Walter de Gruyter, Berlin-New York, 1994).

[22] L. L. Scott, 'Representations in characteristic p', *Santa Cruz conference on finite groups*, pp. 318-331, Proc. Sympos. Pure Math., vol 37, Amer. Math. Soc., Providence, R.I., 1980.

[23] R. Steinberg, 'Endomorphisms of linear algebraic groups', *Memoirs Amer. Math. Soc.* **80** (1968).

[24] M. Suzuki, *Group theory I* (Springer, Berlin-Heidelberg-New York, 1982).

[25] T. Tsuzuku, *Finite groups and finite geometries* (Cambridge University Press, Cambridge, 1982).