Finite Axiomatisability in Nilpotent Varieties

Joshua Thomas Grice

Follow this and additional works at: https://scholarcommons.sc.edu/etd

Part of the Mathematics Commons

Recommended Citation

This Open Access Dissertation is brought to you by Scholar Commons. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Scholar Commons. For more information, please contact dillarda@mailbox.sc.edu.
Finite Axiomatisability in Nilpotent Varieties

by

Joshua Thomas Grice

Bachelor of Science
Virginia Commonwealth University, 2014

Submitted in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy in
Mathematics
College of Arts and Sciences
University of South Carolina
2020

Accepted by:
George F. McNulty, Major Professor
Joshua Cooper, Committee Member
Stephen Fenner, Committee Member
Alex Duncan, Committee Member
Eva Czabarka, Committee Member
Cheryl L. Addy, Vice Provost and Dean of the Graduate School
DEDICATION

For all the students who believe themselves unworthy

and all the mentors who prove them wrong
Acknowledgments

This dissertation was made possible by a great number of people, some who are named on the title page and some who are not. I would like to take a page to thank those people now.

Firstly, I wish to thank my PhD advisor and mentor, George McNulty. Without Dr. McNulty’s support, guidance, and patience, I would certainly have burnt out or given up several times.

I also wish to thank my mentors and professors at the University of South Carolina. Joshua Cooper and Eva Czabarka have my thanks for continuing to be invested in my education and well-being even after I decided not to pursue research in their fields. Thanks to Stephen Fenner and Alex Duncan, as well, for their work as my committee members and in guiding me to this accomplishment.

The department of mathematics at the University of South Carolina has my gratitude as well. Ognian Trifonov, Matt Boylan, Anton Schep and Lincoln Lu have my thanks for their leadership during my time here.

Finally, I wish to personally thank a few friends and family members for their support. I have a number of close, supportive friends, whose encouragement was vital during the last six years. My mother, father, and brother provided another pillar of support that helped me get through the harder parts. I thank Dr. Kevin Beanland for inspiring me to pursue a career in mathematics. And, finally, I wish to thank my wife Kayla for her ceaseless and unconditional support as I pursued this quite challenging goal. As in so many things, she is my inspiration and my foundation, and this work is no exception.
Dr. McNulty
ABSTRACT

Study of general algebraic systems has long been concerned with finite basis results that prove finite axiomatisability of certain classes of general algebras. In the 1970’s, Bjarni Jónsson speculated that a variety generated by a finite algebra might be finitely based provided the variety has a finite residual bound (that is, a finite bound on the cardinality of subdirectly irreducible algebras in the variety). As such, most finite basis results since then have had the hypothesis of a finite residual bound. However, Jónsson also speculated that it might be sufficient to replace the finite residual bound with the weaker hypothesis that the subdirectly irreducible algebras themselves be finitely axiomatisable.

In this dissertation, we give an overview of the concepts and history involving this topic. We also prove that two types of varieties that are already known to be finitely based have the property that their subdirectly irreducible members are finitely axiomatisable.

- Varieties generated by finite nilpotent groups have this property.
- Congruence permutable varieties generated by finite nilpotent algebras of finite signature that are the product of algebras of prime power order have this property.
TABLE OF CONTENTS

DEDICATION .................................................................................................................. iii

ACKNOWLEDGMENTS ........................................................................................................ iv

ABSTRACT ........................................................................................................................ vi

CHAPTER 0 INTRODUCTION ............................................................................................. 1
  0.0 Congruence relations .................................................................................................. 2
  0.1 Subdirectly irreducible algebras ................................................................................. 5
  0.2 Nilpotent algebras ...................................................................................................... 6
  0.3 Finite basis results ..................................................................................................... 9
  0.4 The main results ....................................................................................................... 12

CHAPTER 1 PRELIMINARIES AND EXAMPLES ............................................................. 14
  1.0 Elementary Logic ..................................................................................................... 14
  1.1 Definable Principal Subcongruences ....................................................................... 16
  1.2 Algebraic preliminaries ............................................................................................ 18
  1.3 Congruence permutability ....................................................................................... 22
  1.4 A variety with no finite residual bound but finitely axiomatisable
      subdirectly irreducibles .............................................................................................. 28
  1.5 An example of a nilpotent algebra that is not the product of algebras of prime power order ........................................................................................................... 30

vii
### Chapter 2 The Group Theorem

2.0 Nilpotent groups .................................................. 37
2.1 Conjugate product polynomials ................................. 41
2.2 Definable principal normal subgroups ......................... 42
2.3 Proof of the group theorem .................................... 44

### Chapter 3 The Algebra theorem ................................. 50

3.0 Commutator words ................................................ 50
3.1 Proving Theorem 3.1 ............................................ 52

### Chapter 4 Open problems ........................................ 60

### Bibliography ....................................................... 63
Chapter 0

Introduction

This dissertation is concerned with the study of *general algebraic systems*, which we will henceforth refer to as *algebras*. The study of such objects is sometimes called universal algebra. We define an *algebra* as a nonempty set endowed with some collection of finitary operations, often referred to as the *basic operations* of the algebra. We refer to the collection of operation symbols as the *signature* of the algebra. Many of the mathematical structures studied by abstract algebraists fit this definition, such as groups, rings, vector spaces, lattices, and Boolean algebras. For instance, a group is an algebra whose signature includes \( \cdot \), a symbol representing the binary multiplication operation, \(-1\), a symbol representing the unary inverse operation, and \(1\), a symbol representing the identity, which can be viewed as a 0-ary operation.

Many common definitions from fields such as group theory and ring theory can be naturally defined for algebras in general. For instance, a *homomorphism* between algebras of the same signature is a map that respects the basic operations. A *sub-algebra* of a given algebra is a subset that is closed under the basic operations. The *direct product* of algebras takes its natural meaning as well, with the basic operations defined coordinate-wise on the Cartesian product.

If we have a signature for some algebra or class of algebras, we can talk about the *terms* in that signature, which are expressions built up from variables and basic operations (we give a richer definition in Chapter 1). We can also talk about *equations*, which are statements of equality between terms. For instance, an equation in the
signature of rings with identity might look like

\[ xy + z \approx y + 1 \]

A *variety* of algebras is a class of algebras that is closed with respect to subalgebras, homomorphic images, and arbitrary direct products. According to a paper by Birkhoff (1935), a variety is also a class of algebras that all satisfy some given set of equations; we say that the variety is *axiomatised* by those equations. If the set of equations is finite, we say that \( \mathcal{V} \) is *finitely based*. This two-sided perspective on varieties is what makes the study of them interesting; they can be analysed with an algebraic frame of mind, or with a logical one.

If \( A \) is an algebra, the smallest variety containing it is called the *variety generated by \( A \)*, and will be denoted \( \mathcal{V}(A) \). Much work has gone into finding out what hypotheses need to be satisfied by \( A \) in order for \( \mathcal{V}(A) \) to be axiomatisable by a finite set of equations, and the original results in this dissertation will hopefully add to that body of work. In this introduction, we will define enough algebraic concepts in order to state our main results.

0.0 **Congruence relations**

In group theory and ring theory, much of the structural information of the algebra of interest comes from the study of special subsets: normal subgroups in group theory and two-sided ideals in ring theory. Due to certain closure properties (such as normal subgroups being closed under inner automorphisms), these subsets inform special equivalence relations that underlie the construction of quotient algebras, both determining the quotient algebra itself and also the homomorphism that produces it. For instance, in rings, we can define a congruence relation using some ideal \( I \) where \( a \equiv b \mod I \) if \( a - b \in I \). These relations are powerful, both in groups and rings, since one class of the relation defined by this special subset determines the whole
relation. Unfortunately, there are no such special subsets in algebras in general, so we instead turn our attention to the relations themselves as an acceptable substitute.

If $h: A \to B$ is a homomorphism between two algebras, we define the **relational kernel** of $h$ to be the subalgebra of $A^2$ given by $\{\langle a, b \rangle \mid h(a) = h(b)\}$. This kernel is a special type of equivalence relation called a **congruence relation**. The congruence relations on an algebra $A$ are also precisely the equivalence relations on $A$ that are subalgebras of $A^2$. The congruences of a given algebra $A$ form a complete lattice under set inclusion, denoted $\text{Con}(A)$. Given two congruences $\alpha$ and $\beta$ in this lattice, the greatest lower bound or **meet** of two congruences (which is just their intersection) is denoted by $\alpha \wedge \beta$. Their least upper bound or **join** (the congruence generated by their union) is denoted $\alpha \vee \beta$. The top element in this lattice is $1_A = \{\langle a, b \rangle \mid a, b \in A\}$, and the bottom element is $0_A = \{\langle a, a \rangle \mid a \in A\}$. A congruence on $A$ is called **principal** if it the smallest congruence containing a given pair $\langle a, b \rangle$, in which case it is denoted $\text{Cg}_A(a, b)$.

Congruence relations are an acceptable substitution for normal subgroups in algebras in general. In fact, the lattice of normal subgroups of a given group is isomorphic to its congruence lattice. If $\theta$ is a congruence relation of a group $G$, then the congruence class $1/\theta$ is a normal subgroup of $G$. Every normal subgroup has a corresponding congruence relation. This fact can be seen by examining principal congruences and normal subgroups; if $\theta = \text{Cg}_G(a, b)$ is a congruence in $G$, it can be easily rewritten as $\theta = \text{Cg}_G(ab^{-1}, 1)$ using the closure of the congruence under multiplication. Then, $1/\theta$ is the normal subgroup in $G$ generated by $ab^{-1}$. On the other hand, any normal subgroup generated by $a$ determines the congruence relation $\text{Cg}_G(a, 1)$.

Many characteristics of algebras are determined by certain identities being satisfied by their congruences. One such definition that is a hypothesis for both of our results is that of congruence permutability. Given two equivalence relations $\alpha$ and $\beta$,
their composition is the relation

$$\alpha \circ \beta = \{ \langle a, b \rangle \mid \exists c \text{ such that } \langle a, c \rangle \in \alpha \text{ and } \langle c, b \rangle \in \beta \}$$

An algebra $A$ is said to be congruence permutable if, for any congruences $\alpha$ and $\beta$ of $A$, we have that $\alpha \circ \beta = \beta \circ \alpha$. A variety is congruence permutable if all of its algebras are. This is a stronger property, as there are some congruence permutable algebras that do not generate congruence permutable varieties. This dissertation is concerned with varieties that are congruence permutable.

Congruence distributivity is another potential characteristic of congruences of an algebra. We say that $A$ is congruence distributive if any congruences $\alpha, \beta, \gamma \in \text{Con}(A)$ satisfy the equation

$$\alpha \land (\beta \lor \gamma) = (\alpha \land \beta) \lor (\alpha \land \gamma)$$

or its dual, which is equivalent due to some rudimentary lattice theory. Congruence distributivity is less frequently encountered in the study of the classical types of algebras. Groups, rings, vector spaces, and other types of 19th-century algebras often fail to be congruence distributive. They do, however, satisfy a weakening of the distributive law that was discovered by Dedekind in the late 19th century, which he called the modular law, and is as follows:

$$\alpha \land \beta = \beta \Rightarrow \alpha \land (\beta \lor \gamma) = (\alpha \land \beta) \lor (\alpha \land \gamma)$$

A algebra $A$ is called congruence modular if any congruences $\alpha, \beta, \gamma$ of $A$ satisfy this law. Modularity enables a well-behaved extension of the commutator operation on groups (which we will define below) that can be used to define Abelianness, solvability, and nilpotence in general algebras. A variety is, as in the case of permutability, called congruence distributive if its algebras are all congruence distributive, and congruence modular if its algebras are all congruence modular.
0.1 Subdirectly irreducible algebras

Let $A$ be an algebra, and let $\langle B_i \mid i \in I \rangle$ be a system of algebras. Let $\langle h_i \mid i \in I \rangle$ be a system of homomorphisms so that $h_i : A \to B_i$ is onto for each $i$. This system of homomorphisms is called a subdirect representation of $A$ if it separates points; that is, for $a, b \in A$ so that $a \neq b$, there is some $j \in I$ so that $h_j(a) \neq h_j(b)$. Such a representation is trivial if $h_j$ is one-to-one for some $j \in I$. Given such a subdirect representation, there is a natural embedding of the algebra $A$ into the direct product of the algebras $B_i$ such that the projections onto each factor are surjective. If every subdirect representation of $A$ is trivial, we say that $A$ is subdirectly irreducible.

Subdirect irreducibility has another useful characterisation. We will prove this characterisation in Chapter 1, but it is useful to state now for ease of conceptualisation. An algebra $A$ is subdirectly irreducible if and only if it has a minimal nontrivial congruence, called its monolith. This is equivalent to the presence of a critical pair; that is, a pair $\langle c, d \rangle$ such that $c \neq d$ and $\langle c, d \rangle \in \theta$ for any nontrivial congruence $\theta$. Of course, if $A$ is a group, we could also say that $A$ has a minimal nontrivial normal subgroup, which is the normal closure of a single element.

Given a variety $\mathcal{V}$, we write $\mathcal{V}_{si}$ to denote the class of subdirectly irreducible members of $\mathcal{V}$. According to Birkhoff (1944), two varieties are equal if and only if they share the same subdirectly irreducible members. Given this fact, knowing about $\mathcal{V}_{si}$ can tell us about $\mathcal{V}$ itself, so the study of subdirectly irreducible algebras has been illuminating. Subdirect irreducibility is not maintained under direct products, so $\mathcal{V}_{si}$ isn’t a variety, and as such isn’t axiomatisable by equations. However, it might still in some cases be axiomatisable by a broader range of first-order sentences, which are formed from equations joined together with logical connectives and quantifiers (we give a more rigorous definition in Chapter 1). If a class of algebras is axiomatisable by finitely many sentences, we say it is finitely axiomatisable. Our main results prove finite axiomatisability of $\mathcal{V}_{si}$ for certain varieties $\mathcal{V}$. 
0.2 NILPOTENT ALGEBRAS

Our theorems both take place in varieties of nilpotent algebras. Nilpotence is a group theoretic notion that has been extended to algebras in general. Nilpotence is similar to solvability, but while solvability is a frequently-encountered topic in a standard group theory course, nilpotence may not be as well known. We will therefore define it in full. In order to define nilpotent algebras, we must first define the commutator operation on congruences of algebras.

In group theory, the commutator \([H, K]\) of two normal subgroups \(H\) and \(K\) of a group \(G\) is the normal subgroup

\[ [H, K] = \{hkh^{-1}k^{-1} | h \in H, k \in K \} \]

This notion is difficult to extend to algebras in general whose signatures do not necessarily contain multiplication and inverses, and whose operations may have wildly different arities than those of groups. The extension works, however, and even emulates many of the nice properties of the group commutator as long as the algebras in question are congruence modular. There is an excellent exposition on commutator theory in general algebras, which we will refer to as “the Commutator Book” on the numerous occasions it comes up in this dissertation (Freese and McKenzie 1987). We will use the notation and several results from the Commutator Book in this dissertation.

Let \(A\) be a congruence modular algebra. Let \(\alpha, \beta\) and \(\delta\) be in \(\text{Con}(A)\). We define \(M(\alpha, \beta)\) as the set of all matrices

\[ \begin{bmatrix} t(\bar{a}_1, \bar{b}_1) & t(\bar{a}_1, \bar{b}_2) \\ t(\bar{a}_2, \bar{b}_1) & t(\bar{a}_2, \bar{b}_2) \end{bmatrix} \]

where the \(\bar{a}_i\) are both sequences of \(n\) elements of \(A\), the \(\bar{b}_i\) are both sequences of \(m\) elements of \(A\) for some \(n, m \geq 0\), satisfying \(a_{1k} \alpha a_{2k}\) and \(b_{1j} \beta b_{2j}\) for any \(k\) and \(j\),
and \( t \) is an \( n + m \) variable term on \( A \). This relationship can be summarised by the following diagram.

\[
\begin{array}{c}
t(a_1, b_1) \xrightarrow{\beta} t(a_1, b_2) \\
\alpha \downarrow \qquad \alpha \downarrow \\
t(a_2, b_1) \xrightarrow{\beta} t(a_2, b_2)
\end{array}
\]

We say that \( \alpha \) centralises \( \beta \) modulo \( \delta \), and write \( C(\alpha, \beta; \delta) \), provided that for every \(
\begin{bmatrix}
u_{11} & u_{12} \\
u_{21} & u_{22}
\end{bmatrix}
\) in \( M(\alpha, \beta) \), \( u_{11} \delta u_{12} \) implies \( u_{21} \delta u_{22} \). That is, the solid line in the following picture implies the dashed line.

\[
\begin{array}{c}
t(a_1, b_1) \xrightarrow{\delta} t(a_1, b_2) \\
t(a_2, b_1) \longrightarrow \delta \longrightarrow t(a_2, b_2)
\end{array}
\]

Then, the \textit{commutator} \([\alpha, \beta]\) of two congruences \( \alpha \) and \( \beta \) is the smallest \( \delta \) such that \( C(\alpha, \beta; \delta) \). The commutator operation in modular varieties has many useful properties, all of which are proved in the Commutator Book.

- The commutator is commutative.
- The commutator is monotone in both arguments.
- \([\alpha, \beta] \land [\gamma, \beta] = [\alpha \land \gamma, \beta]\); that is, the commutator respects the meet operation.
- \([\alpha, \beta] \leq \alpha \land \beta\).
- This commutator generalises the group commutator.

Using the commutator, we can now define nilpotence in general algebras. Given an algebra \( A \) and a congruence \( \alpha \in \text{Con}(A) \), we write \( (\alpha)^0 = \alpha \) and \( (\alpha)^{i+1} = [\alpha, (\alpha)^i] \). We say that \( \alpha \) is an \textit{Abelian} congruence if \( [\alpha, \alpha] = 0_A \). The algebra \( A \) is \textit{Abelian} if all of its congruences are, or equivalently if \( [1_A, 1_A] = 0_A \). We define \( A \) to be \textit{nilpotent of class} \( k \) if \( (1_A)^k = 0_A \) for some \( k \). The descending sequence \( (1_A)^0 \geq (1_A)^1 \geq \cdots \geq (1_A)^k \) is called the \textit{lower central series} of \( A \). Of course, an algebra is Abelian if and only if it
is nilpotent of class 1. In this way, nilpotence is an extension of Abelianness, in the same way as in groups.

Nilpotence is usually defined in groups in the following way: Let $G$ be a group, define $G_0 = G$, and define $G_{i+1} = [G, G_i]$. Then, $G$ is nilpotent if $G_k = \{1\}$ for some $k$. Of course, since the algebraic commutator generalises the group commutator, these two definitions of nilpotence agree with each other. The sequence of normal subgroups $G_i$ is also called the lower central series.

This commutator-based presentation of nilpotence is often, both in the context of groups and algebras, the default definition. But there is another way of defining nilpotence using the center of a group or an algebra that we will include here, and actually default to, since it is the most useful definition for all of the work that we do.

Let $A$ be an algebra. As we have stated, a congruence $\alpha$ of $A$ is called Abelian if $[\alpha, \alpha] = 0_A$. This is equivalent to saying that for any term $t(\bar{u}, \bar{v})$ and any tuples $\bar{a}_1, \bar{a}_2$ of the same length as $\bar{u}$ and $\bar{b}_1, \bar{b}_2$ of the same length of $\bar{v}$ so that $\langle (a_1)_i, (a_2)_i \rangle \in \alpha$ for each $i$ and $\langle (b_1)_j, (b_2)_j \rangle \in \alpha$ for each $j$, we have that $t(\bar{a}_1, \bar{b}_1) = t(\bar{a}_1, \bar{b}_2) \rightarrow t(\bar{a}_2, \bar{b}_1) = t(\bar{a}_2, \bar{b}_2)$. That is, given the following diagram, the dashed line holds if all of the solid lines hold also:

$$
\begin{array}{c}
t(\bar{a}_1, \bar{b}_1) \\
\downarrow \alpha \\
t(\bar{a}_2, \bar{b}_1)
\end{array}
\quad
\begin{array}{c}
t(\bar{a}_1, \bar{b}_2) \\
\downarrow \alpha \\
t(\bar{a}_2, \bar{b}_2)
\end{array}
$$

Each algebra has at least one Abelian congruence called the center. The center is the binary relation $\zeta_A$ on $A$ defined by

$$
\langle x, y \rangle \in \zeta_A \iff (\forall t)(\forall \bar{u}, \bar{v})(t(\bar{u}, x) = t(\bar{v}, x) \leftrightarrow t(\bar{u}, y) = t(\bar{v}, y))
$$

where the first quantifier is over all term operations on $A$ and the second over all $n$-tuples from $A$, depending on the arity of $t$. It follows from this definition that the center $\zeta_A$ is the largest congruence $\alpha$ on $A$ so that $[\alpha, 1_A] = 0_A$, and so by
monotonicity of the commutator, $\zeta_A$ is always Abelian. The center provides another definition of Abelian algebras that is now more similar to the group definition; an algebra $A$ is Abelian if $\zeta_A = 1_A$.

Equipped as we are now with the definition of a center, the above definition of a group’s upper central series in section 2.0 generalises nicely. We define the *upper central series* of an algebra $A$ to be the sequence of congruences

$$0_A = \zeta_0 \leq \zeta_1 \leq \zeta_2 \leq \ldots$$

so that $\zeta_{i+1}/\zeta_i = \zeta(A/\zeta_i)$ for each $i$, where $\zeta_{i+1}/\zeta_i$ refers to the image of the congruence $\zeta_{i+1}$ under the quotient map that forms $A/\zeta_i$. The Correspondence Theorem familiar to those studying groups and rings generalises to general algebras, permitting this definition.

It is easily shown that this upper central series coincides in length with the lower central series defined in section 0.2. That is, $\zeta_k = 1_A$ if and only if $A$ is nilpotent of class $k$.

We will adapt this definition for groups in Chapter 2. We will also present a third well-known characterisation that only works for groups: That a finite group $G$ is a nilpotent group if and only if it is the direct product of its Sylow subgroups.

### 0.3 Finite basis results

As it is with varieties, if an algebra $A$ is axiomatised by finitely many equations, we say that it is *finitely based*. Of course, the variety generated by a finitely based algebra is itself finitely based as well. Universal algebraists have long been interested in determining which algebras and varieties are and are not finitely based. Tarski wondered, in his finite basis problem, whether there is an algorithm to determine whether a given finite algebra is finitely based. The problem was solved by McKenzie (1996), who proved that no such algorithm exists. And so, many classes of algebras
and varieties have been studied individually to determine whether or not they are finitely based.

Lyndon (1952) proved that any nilpotent group is finitely based. Oates and Powell (1964) proved that any finite group is finitely based. Another proof of their theorem was published by Neumann (1967) in her book on varieties of groups. Kruse (1973) and L’vov (1973) independently extended that result to finite rings. McKenzie (1970) proved in that any finite lattice with finitely many additional basic operations is finitely based. A generalisation of this comes in the form of Baker’s Finite Basis Theorem, which states that if $A$ is a finite algebra with only finitely many basic operations and $\mathcal{V}(A)$ is congruence distributive, then $A$ is finitely based (Baker 1977). Baker’s theorem was reproved a number of times by different researchers and inspired much of the investigation into finite basis problems.

Freese and Vaughan-Lee showed that a congruence modular variety generated by a finite nilpotent algebra is finitely based, provided that the generating algebra is a product of algebras of prime power order. We state this later as Theorem 3.3.

A variety $\mathcal{V}$ is said to have a finite residual bound if there is some natural number $m$ so that every algebra in $\mathcal{V}$ has cardinality at most $m$. In 1974, Bjarni Jónsson made a few speculations about what the connection might be between finite axiomatisability of $\mathcal{V}$ and of $\mathcal{V}$ itself for certain varieties. One such speculation was that any variety with a finite residual bound that is generated by a finite algebra with finitely many basic operations is finitely based. This is still an open problem, and has been the inspiration for many finite basis results from the last several decades. For instance, McKenzie proved that if $A$ is a finite algebra with finitely many basic operations so that $\mathcal{V}(A)$ is congruence modular and has a finite residual bound, then $A$ is finitely based (McKenzie 1987). This result is in some ways orthogonal to Freese and Vaughan-Lee’s result, as it is known that the only nilpotent algebras that generate
a variety with a finite residual bound are the Abelian ones, so the overlap between
those results is quite narrow.

Willard (2000) proved a similar result, where he showed that if $A$ is a finite algebra
with finitely many basic operations so that $\mathcal{V}(A)$ is congruence meet-semidistributive
and has a finite residual bound, then $A$ is finitely based. Meet-semidistributivity is
yet another weakening of the distributive law:

$$\alpha \land \beta = \alpha \land \gamma \Rightarrow \alpha \land (\beta \lor \gamma) = (\alpha \land \beta) \lor (\alpha \land \gamma)$$

Many algebraic properties of varieties depend upon the presence of certain terms
(which are built of compositions of the basic operations of the variety) that satisfy
certain equations. For example, a ternary term $p(x, y, z)$ is called a difference term if
it satisfies the identity $p(x, x, y) \approx y$ and if $p(a, b, b) = a$ whenever $\langle a, b \rangle$
belongs to an Abelian congruence of an algebra in the variety. Varieties with a difference term
generalise both congruence modular varieties and congruence meet semi-distributive
varieties. Kearnes, Szendrei, and Willard (2016) showed that if $\mathcal{V}$ is a variety with
finitely many basic operations, a difference term, and a finite residual bound, then $\mathcal{V}$
is finitely based.

If $\mathcal{V}$ has a finite residual bound, it has finitely many subdirectly irreducible mem-
bers up to isomorphism, and so $\mathcal{V}_{si}$ is finitely axiomatisable. The converse is not
necessarily true, however, as we will show later in Chapter 1. So, it is possible that
for some of the finite basis results that have a finite residual bound as a hypothesis,
that hypothesis could potentially be weakened to the finite axiomatisability of $\mathcal{V}_{si}$. In
fact, Jónsson speculated if perhaps the hypothesis of $\mathcal{V}_{si}$ being finitely axiomatisable
was enough to guarantee that a variety generated by a finite algebra be finitely based.
This speculation is also still open, but has a lot less evidence to support it than the
version invoking a finite residual bound.
0.4 The main results

In 2000, McNulty and Wang circulated a preprint of an ultimately incorrect proof that for any finite group $G$ and variety $\mathcal{V} = \mathcal{V}(G)$, $\mathcal{V}_{si}$ is finitely axiomatisable. The proof has not yet been repaired, but the author has made it partway to McNulty and Wang’s conjecture by proving the theorem with the added hypothesis of nilpotence. This is the first of two main original results of this dissertation. It can also be found in the author’s 2020 paper (Grice 2020).

**Theorem 2.1.**

Let $\mathcal{V}$ be a variety generated by a finite nilpotent group $G$. Then, the class $\mathcal{V}_{si}$ of sub-directly irreducible groups belonging to $\mathcal{V}$ is axiomatisable by a finite set of elementary sentences.

We have also extended the result to congruence permutable algebras, but have to include the extra hypothesis that the generating algebra is a product of algebras of prime power order. While this hypothesis is guaranteed in groups, it is not necessarily true of all nilpotent algebras, which we prove via an example in Chapter 1.

**Theorem 3.1.**

Let $A$ be a finite nilpotent algebra of finite signature that is a product of algebras of prime power order such that $\mathcal{V} = \mathcal{V}(A)$ is a congruence permutable variety. Then, $\mathcal{V}_{si}$ is finitely axiomatisable.

The remainder of this dissertation will be written towards the goal of proving these two results. Chapter 1 will build up some more background and definitions required for the results, and introduce some motivating examples to show the results’ significance in the broader knowledge of finite basis theorems. Chapter 2 will prove the first theorem using group-theoretic concepts. Chapter 3 will then prove the second theorem using a somewhat similar but in many ways different method. We will then
end with Chapter 4, which will state a few open problems relevant to our results and what progress has been made towards them.
In this chapter, we will more rigorously define some notions from the introduction, as well as the concept of definable principal subcongruences, which will be required for the proofs of the main results. We will also present a few motivating examples that illustrate the importance of the results in the grander scope of finite basis problems. The author wishes to make clear that nothing in this chapter is original work, but rather is reproduced either from other authors' work or from folklore.

1.0 Elementary Logic

We will first introduce the concepts of first-order logic, also known as elementary logic, that will be required for our results. First-order logic is concerned with elements of structures, and uses variables along with logical connectives and quantifiers, in addition to the basic operations supplied by the structures in question. The symbols representing the basic operations that come from the structure are called the signature of that structure, and along with variables (that represent elements), logical symbols, and punctuation, form the alphabet that formal statements are made from.

The first-order terms of a structure or class of structures are built up from the variables and the basic operations. Specifically, the set of terms is the smallest set that contains every variable and is closed under all of the basic operations. For instance, the conjugate $xyx^{-1}$ is a term in the language of groups. As a matter of notation, let $t(x_0, \ldots, x_{n-1})$ be a term for some algebra $A$. Then, we denote its evaluation in $A$ at parameters $a_0, \ldots, a_{n-1}$ by writing $t^A(a_0, \ldots, a_{n-1})$. Additionally, it is conventional
in universal algebra and model theory to write the bold-face \( A \) to denote the algebra, and the non-bold \( A \) to talk about the universe of the algebra as a set.

An *equation* is some statement of equality between two terms whose variables are understood to range over the whole group. For instance, the commutative law of Abelian groups can be expressed as an equation:

\[
xy \approx yx
\]

As we stated in the introduction, an *elementary formula* is built up from equations in a systematic way with the help of logical connectives \( \lor, \land, \neg, \rightarrow, \) and \( \leftrightarrow \) (conjunction, disjunction, negation, implication and biconditional, respectively), and the quantifiers \( \exists \) and \( \forall \). We can define formulas rigorously with the following recursive definition:

1. If \( t_1 \) and \( t_2 \) are terms, then the equation \( t_1 \approx t_2 \) is a formula.

2. If \( \phi \) is a formula, its negation \( \neg \phi \) is a formula.

3. If \( \phi \) and \( \psi \) are formulas, their conjunction \( \phi \land \psi \) and their disjunction \( \phi \lor \psi \) are formulas.

4. If \( \phi \) and \( \psi \) are formulas, the implication \( \phi \rightarrow \psi \) and the biconditional \( \phi \leftrightarrow \psi \) are both formulas.

5. If \( \phi \) is a formula and \( x \) is a variable, then the quantified statements \( \exists x \phi \) and \( \forall x \phi \) are formulas.

A formula may look something like:

\[
\forall y \,(xy \approx yx) \land \neg(x \approx 1)
\]

Note that in this formula, the variable \( x \) appears but is not quantified. This makes \( x \) a *free variable*, and illustrates how formulas can be used to define sets of elements. If the above formula is named \( \Phi \), for instance, the set defined by \( \Phi(x) \) would be the
set of all elements \( x \) of a group that satisfy that formula. If this formula is written for a group, for example, \( \Phi(x) \) is the set of nontrivial elements of the group’s center.

If a formula has no free variables, it is called an \textit{elementary sentence}. A sentence might be true or false in a given structure, whereas the truth of a formula depends on the values taken by the variables. Sentences are useful for stating laws obeyed in a structure that cannot be expressed by equations alone. For example, the presence of an inverse for every element of a group:

\[
\forall x \exists y \, (xy \approx 1)
\]

1.1 \textbf{Definable Principal Subcongruences}

A first-order formula \( \Phi(u, v, x, y) \) with four free variables is called a \textit{congruence formula} for a class \( \mathcal{K} \) of algebras provided that for every algebra \( A \in \mathcal{K} \),

if \( A \models \Phi(a, b, c, d) \), then \( \langle a, b \rangle \in Cg^A(c, d) \)

A class \( \mathcal{K} \) of algebras is said to have \textit{definable principal subcongruences} if and only if there are congruence formulas \( \Phi(u, v, x, y) \) and \( \Psi(u, v, x, y) \) so that for every \( A \in \mathcal{K} \) and every \( a, b \in A \) with \( a \neq b \), there exist \( c, d \in A \) with \( c \neq d \) so that

1. \( A \models \Psi(c, d, a, b) \) and
2. \( \Phi(u, v, c, d) \) defines \( Cg^A(c, d) \).

In other words, if a principal congruence on any algebra in \( \mathcal{K} \) is chosen, the first formula \( \Psi \) is capable of finding another principal congruence contained within it that is definable by the second formula \( \Phi \). This definition is introduced by Baker and Wang (2002), where they prove the following finite basis theorem:
Theorem (Baker, Wang). Let $\mathcal{V}$ be a variety of finite signature and suppose that $\mathcal{V}$ has definable principal subcongruences. Then, $\mathcal{V}$ is finitely based if and only if $\mathcal{V}_{si}$ is finitely axiomatisable.

This theorem is significant in comparison with most of the other finite basis results that we have mentioned. The hypothesis of a finite residual bound is either implicitly or explicitly needed for many of the finite basis theorems from the past fifty years. Baker and Wang’s result, however, weakens that hypothesis to the finite axiomatisability of $\mathcal{V}_{si}$ in the presence of definable principal subcongruences. A finite residual bound implies finite axiomatisability of $\mathcal{V}_{si}$, since there can be only finitely many subdirectly irreducible algebras in $\mathcal{V}$ up to isomorphism, all of which can be axiomatised by finitely many sentences. The implication does not go the other way, however; there are varieties $\mathcal{V}$ with arbitrarily large subdirectly irreducibles for whom $\mathcal{V}_{si}$ is finitely axiomatisable, as we will show below.

A variation on the proof of Baker and Wang’s theorem yields the following result, whose proof we reproduce from McNulty and Wang’s unpublished work.

**Theorem 1.1.** If $\mathcal{V}$ is a variety and $\mathcal{V}_{si}$ has definable principal subcongruences, then $\mathcal{V}_{si}$ is finitely axiomatisable relative to $\mathcal{V}$. In particular, if $\mathcal{V}$ is finitely based, then $\mathcal{V}_{si}$ is finitely axiomatisable.

**Proof.** Let $\Sigma$ be a finite set of elementary sentences which axiomatises $\mathcal{V}$, and let $\Phi(u, v, x, y)$ and $\Psi(u, v, x, y)$ be the formulas witnessing that $\mathcal{V}_{si}$ has definable principal subcongruences. Let $\Theta$ be the following set of sentences:

$$\Sigma \cup \{\exists u, v, [u \neq v \land \forall z, w(z \neq w \Rightarrow \exists x, y(\Phi(u, v, x, y) \land \Psi(x, y, z, w)))\}$$

We claim that $\Theta$ axiomatises $\mathcal{V}_{si}$.

On one hand, suppose $S \in \mathcal{V}_{si}$. Let $\langle c, d \rangle$ be a critical pair for $S$. So, $c \neq d$ and $\langle c, d \rangle$ belongs to every nontrivial congruence. Now, let $e, f \in S$ with $e \neq f$. Because
\[ V_\text{bi} \text{ has definable principal subcongruences, there are } a, b \in S \text{ where } a \neq b \text{ so that } S \models \Psi(a, b, e, f), \text{ and } \Phi(x, y, a, b) \text{ defines } Cg^S(a, b). \text{ Since } a \neq b \text{ and } \langle c, d \rangle \text{ is a critical pair, } \langle c, d \rangle \in Cg^S(a, b), \text{ so } S \models \Phi(c, d, a, b). \text{ So, }\\\\S \models \{ \exists u, v, [u \neq v \land \forall z, w(z \neq w \Rightarrow \exists x, y(\Phi(u, v, x, y) \land \Psi(x, y, z, w)))]\}\]

Since \( S \) is in \( V \), \( S \models \Sigma \) also. Therefore, \( S \models \Theta \).

Now, suppose \( S \models \Theta \). Then, \( S \in V \) since \( \Sigma \) axiomatises \( V \). But also, since \( S \) believes the second part of \( \Theta \) and \( \Phi \) and \( \Psi \) are congruence formulas, there exist \( c, d \in S \) so that \( c \neq d \) and \( \langle c, d \rangle \) is contained within any other principal congruence. So, \( \langle c, d \rangle \) is a critical pair for \( S \) and \( S \) is subdirectly irreducible. \( \square \)

### 1.2 Algebraic preliminaries

In this section, we list a few definitions and theorems that did were not done full justice in the introduction. The results in this section are either folkloric or from the excellent book by McKenzie, McNulty, and Taylor (2018).

Firstly, we should discuss local finiteness of varieties and free algebras. A class \( K \) of algebras is called \textit{locally finite} if all of its finitely generated algebras are finite. If \( A \) is a finite algebra, then \( \mathcal{V}(A) \) is always locally finite. A few details about algebras and varieties go into proving this fact.

Let \( A \) be an algebra and \( n \) be a non-negative integer. We define the \textit{clone of }\( n \)-ary \textit{term operations on }\( A \) to be the smallest set of \( n \)-ary operations on \( A \) that contains the projection functions and the basic operations of \( A \), and is closed under composition. We denote it \( \text{Clo}_n(A) \). It is easy to see that \( \text{Clo}_n(A) \) is an algebra, and is in fact a subalgebra of \( A^{A^n} \). In light of that, we obtain the following lemma:

\textbf{Lemma 1.2.} \textit{Suppose that }\( A \) \textit{is an algebra, }\( B \in \mathcal{V}(A) \), \textit{and }\( B \) \textit{is generated by }\( n \) \textit{or fewer elements for some positive integer }\( n \). \textit{Then, }\( B \) \textit{is a homomorphic image of }\( \text{Clo}_n(A) \).
Proof. Since $B$ belongs to $\mathcal{V}(A)$, $B$ is a homomorphic image of a subalgebra of a direct product of $A$, say $A^X$ for some set $X$. Choose a set $v_0, \ldots, v_{n-1} \in A^X$ that map onto a set of generators for $B$. Then, $B$ is a homomorphic image of the subalgebra $C$ generated by these elements, so it suffices to show that $C$ is a homomorphic image of $\text{Clo}_n(A)$. Consider the following mapping of the set of all $n$-ary operations on $A$ into $A^X$:

$$F(g) = (g(v_0(x), \ldots, v_{n-1}(x)) : x \in X)$$

It is easy to verify that $F$ is a homomorphism of $A^n$ into $A^X$, and that if $p^n_i$ is the $i + 1$st $n$-ary projection on $A$ then we have $F(p^n_i) = v_i$. From this, we can conclude that $F$ restricted to $\text{Clo}_n(A)$ maps onto $C$. 

Corollary 1.3. If $A$ is a finite algebra, then $\mathcal{V}(A)$ is locally finite.

The idea in this proof of the algebra $B$ being a homomorphic image of some generating set is highly useful if carried to its natural conclusion. Let $\mathcal{K}$ be a set of algebras with the same signature, and let $U$ be an algebra with that signature. Let $X$ be any subset of $U$. We say that $U$ has the universal mapping property for $\mathcal{K}$ over $X$ if for every $A \in \mathcal{K}$ and for every mapping $f : X \to A$, there is a homomorphism $h : U \to A$ that extends $f$. We say that $U$ is free for $\mathcal{K}$ over $X$ if $U$ is generated by $X$ and has the universal mapping property for $\mathcal{K}$ over $X$. If $U \in \mathcal{K}$ in this case, we say that $U$ is free in $\mathcal{K}$ over $X$.

This dissertation will use this concept by referring to the free algebra in $\mathcal{V}$ on $n$ generators for a particular variety. This refers specifically to the algebra in $\mathcal{V}$ generated by the set of variables $X = \{x_0, x_1, \ldots, x_{n-1}\}$ (sometimes we will rename some of these variables). We denote it as we denote $F^{\mathcal{V}}(X)$, or as $F^n_\mathcal{V}$ if the names of the $n$ distinct variables are irrelevant. This algebra can be viewed as the algebra of $n$-ary term operations in the signature of $\mathcal{V}$ modded out by the equivalence class defined by the equations that are true in $\mathcal{V}$. The universal mapping property guarantees that
equations that are true of the elements of $F_V(X)$ are also true in the variety $V$. For instance, if $V$ is a variety of groups and the equation $x^m \approx 1$ is true in the free algebra on one generator, then that equation is true in the whole variety.

We now prove two folkloric theorems which were mentioned in the introduction. The first is an alternate way of classifying congruence relations.

**Theorem 1.4.** The congruences of an algebra $A$ are precisely the subalgebras of $A^2$ which are also equivalence relations.

**Proof.** Recall from the introduction that a congruence $\theta$ on an algebra $A$ is the kernel of some homomorphism $h$;

$$\theta = \{ (a, b) \mid h(a) = h(b) \}$$

These relations are all clearly congruences. A kernel is also a subalgebra; suppose $Q(x_0, \ldots, x_{n-1})$ is an $n$-ary basic operation on $A$, and that $(a_0, b_0), \ldots, (a_{n-1}, b_{n-1})$ are all pairs from $\theta$. Then, since homomorphisms respect all of the basic operations, we have that

$$h(Q^A(a_0, \ldots, a_{n-1})) = Q^A(h(a_0), \ldots, h(a_{n-1}))$$

$$= Q^A(h(b_0), \ldots, h(b_{n-1}))$$

$$= h(Q^A(b_0, \ldots, b_{n-1}))$$

So we have that

$$\langle Q^A(a_0, \ldots, a_{n-1}), Q^A(b_0, \ldots, b_{n-1}) \rangle \in \theta$$

Therefore, any congruence is indeed an equivalence class and a subalgebra of $A^2$. To see the converse, simply observe that if $\theta$ is an equivalence class and a subalgebra of $A^2$, then the map that takes any $a \in A$ to its equivalence class $a/\theta$ is a homomorphism onto $A/\theta$ with $\theta$ as its kernel. \qed
The second theorem is one that provides an easier way to classify subdirectly irreducible algebras. Recall the original definition of subdirect irreducibility; that any subdirect representation \( \langle h_i \mid i \in I \rangle \) of an algebra is trivial.

**Theorem 1.5.** Let \( A \) be an algebra. The following are equivalent.

1. \( A \) is subdirectly irreducible.

2. \( A \) has a smallest nontrivial congruence called the monolith.

3. \( A \) has a critical pair: that is, a pair \( \langle c, d \rangle \) with \( c \neq d \) that is contained within every nontrivial congruence on \( A \).

**Proof.** 1 \( \Rightarrow \) 2) Suppose that \( A \) is subdirectly irreducible. Let \( \Sigma \) be the set of all nonzero congruences of \( A \), and let \( \theta = \cap \Sigma \). If \( \theta \neq 0_A \), then \( \theta \) is the smallest nontrivial congruence of \( A \), so suppose that \( \theta = 0_A \). For each congruence \( \sigma \in \Sigma \), let \( h_\sigma \) be the homomorphism whose kernel is \( \sigma \). We claim that \( \langle h_\sigma \mid \sigma \in \Sigma \rangle \) is a subdirect representation of \( A \). Indeed, this system of homomorphisms separates points, since if it didn’t, there would be some nontrivial pair in \( \theta \). This representation is not trivial, since if it were, the offending one-to-one \( h_\sigma \) would have \( 0_A \) as its associated congruence, violating the definition of \( \Sigma \). However, this contradicts the assumption that \( A \) was subdirectly irreducible.

2 \( \Rightarrow \) 3) Suppose that \( A \) has a monolith \( \mu \). Suppose that there is no pair \( \langle c, d \rangle \) that generates the monolith. Then, the congruence \( \text{Cg}^A(c, d) \) is a nontrivial congruence properly contained within the monolith, which is impossible. So, there is such a pair \( \langle c, d \rangle \) (in fact, any nontrivial pair in \( \mu \) suffices). Since \( \mu \) is contained within every nontrivial congruence on \( A \), so is \( \langle c, d \rangle \).

3 \( \Rightarrow \) 1) Let \( \langle c, d \rangle \) be a critical pair for \( A \), and let \( \langle h_i \mid i \in I \rangle \) be a subdirect representation of \( A \). Then, \( \langle h_i \mid i \in I \rangle \) separates points. So, there is some \( j \in I \)
so that $h_j(c) \neq h_j(d)$. Now, the kernel $\theta$ of $h_j$ does not contain the pair $\langle c, d \rangle$, and therefore must be $0_A$. Thus, $h_j$ is in fact one-to-one, and the representation is trivial. \hfill \square

1.3 Congruence permutability

Groups carry the useful property that if $H$ and $K$ are normal subgroups of $G$, their products commute; that is, $HK = KH$. This property generalises to congruences of algebras. Recall that an algebra $A$ is called congruence permutable if, for any two congruences $\alpha$ and $\beta$ of $A$, we have $\alpha \circ \beta = \beta \circ \alpha$. Groups are an example of congruence permutable algebras. We call a variety $\mathcal{V}$ congruence permutable if every algebra contained in $\mathcal{V}$ is congruence permutable. One can also define congruence permutability using the join, since the join of two congruences (which is the same as the join in the lattice of equivalence relations) is its transitive closure. That is,

$$\alpha \vee \beta = (\alpha \circ \beta) \cup (\alpha \circ \beta \circ \alpha) \cup (\alpha \circ \beta \circ \alpha \circ \beta) \cup \ldots$$

Congruence permutability trivialises most of the right-hand side of this equation, so an algebra $A$ is congruence permutable if and only if, for any congruences $\alpha$ and $\beta$ of $A$, we have $\alpha \vee \beta \subseteq \alpha \circ \beta$.

In 1954, Anatoli Mal’tsev proved that a variety $\mathcal{V}$ is congruence permutable if and only if it has a ternary term $m(x, y, z)$ so that

$$m(x, y, y) = x = m(y, y, x)$$

We call such a term a Mal’tsev term (Mal’tsev 1954). First, for purposes of demonstration in a more familiar setting, we will argue that the Mal’tsev term in groups is tied to the fact that any group is congruence permutable. Recall that in groups, normal subgroups are in direct correspondence with congruence relations, in the way that the normal subgroups of a group are precisely the classes of its congruences

22
that contain the identity. We claim that, due to this correspondence, the congruence
permutability of groups is equivalent to the fact that $HK = KH$ whenever $H$ and
$K$ are normal subgroups of a group $G$. This fact is already known, but we prove its
equivalence to congruence permutability for purposes of elucidation.

Let $G$ be a group and let $\alpha$ and $\beta$ be congruence relations on $G$, with associated
normal subgroups $1/\alpha = H$ and $1/\beta = K$. Suppose firstly that $G$ is congruence
permutable, so that $\alpha \circ \beta = \beta \circ \alpha$. Choose some element $ab \in HK$ where $a \in H$
and $b \in K$, and so therefore $b^{-1} \in K$. Then, we have that $a \alpha 1 \beta b^{-1}$. So, $\langle a, b^{-1} \rangle \in
\alpha \circ \beta = \beta \circ \alpha$. So that means that there is some element $c \in G$ so that $a \beta c$ and $c \alpha b^{-1}$. It follows that $\langle ac^{-1}, 1 \rangle \in \beta$ and so $ac^{-1} \in K$, and similarly $cb \in H$. Then,$ac^{-1}cb = ab \in KH$. This argument can be reversed to show that $KH \subseteq HK$, proving
that $HK = KH$.

Now, with $\alpha, \beta, H$ and $K$ defined as above, we use the fact that $HK = KH$ to
prove that $G$ is congruence permutable. Let $\langle a, b \rangle \in \alpha \circ \beta$. So, there is some $c \in G$
so that $a \alpha c$ and $c \beta b$. This means that $ac^{-1} \in H$ and $cb^{-1} \in K$. So, we have
that $ac^{-1}cb^{-1} = ab^{-1} \in HK = KH$. So, there is some $k \in K$ and $h \in H$ so that
$ab^{-1} = kh$. Then, $ab^{-1}h^{-1} = a(hb)^{-1} = k \in K$. So, that means that $a \beta hb$. Also note
that $b(hb)^{-1} = h \in H$, so that means $b \alpha hb$. So, $\langle a, b \rangle \in \beta \circ \alpha$. A symmetric argument
completes the proof that $G$ is congruence permutable.

Now, we will show that the permutability is equivalent to the presence of a
Mal’tsev term. The term in question is the term $m(x, y, z) = xy^{-1}z$. This term
is a Mal’tsev term already, simply by group axioms, so we will just use it to prove
that $HK = KH$, which in turn is equivalent to permutability.

Let $a \in H$ and $b \in K$, so that $ab \in HK$. We will show that $ab \in KH$. Indeed,$ab = a \ast m(b, a, a) = aba^{-1}a$. Since $b \in K$ and $K$ is normal, $aba^{-1} \in K$. So,$aba^{-1}a = (aba^{-1})a \in KH$. The proof can be reversed to show the other inclusion.
Now, of course, it is a well-known fact that $HK = KH$ for groups. The previous argument was merely to show the Mal’stev term performing its role. The following proof is Mal’tsev’s proof that the term is equivalent to congruence permutability in any algebra.

**Theorem 1.6.** Let $\mathcal{V}$ be a variety. Then, $\mathcal{V}$ is congruence permutable if and only if it has a Mal’tsev term $m(x, y, z)$.

**Proof.** Suppose, firstly, that a variety $\mathcal{V}$ has a Mal’tsev term $m$. Let $A$ be some algebra in $\mathcal{V}$, and let $\alpha$ and $\beta$ be congruences on $A$. We will prove that $\alpha \circ \beta \subseteq \beta \circ \alpha$. Suppose $\langle a, b \rangle \in \alpha \circ \beta$. This means that there exists some $c$ so that $a \alpha c$ and $c \beta b$. Now, consider $m(a, c, b)$. Since $m$ is a Mal’tsev term, $m(a, c, b) / \alpha = m(c, c, b) / \alpha = b / \alpha$, and $m(a, c, b) / \beta = m(a, b, b) / \beta = a / \beta$. So, since $\alpha \circ \beta m(a, c, b) \alpha b$, we have that $\langle a, b \rangle \in \beta \circ \alpha$, as desired. Now, we have that

$$\alpha \lor \beta = \alpha \circ \beta \cup \alpha \circ \beta \circ \alpha \cup \alpha \circ \beta \circ \alpha \circ \beta \cup \ldots$$

$$= \alpha \circ \beta \cup \alpha \circ \beta \cup \ldots$$

$$= \alpha \circ \beta \cup \alpha \circ \beta \cup \ldots$$

$$= \alpha \circ \beta$$

and so $\mathcal{V}$ is congruence permutable, as desired.

Now, suppose $\mathcal{V}$ is congruence permutable. Then, in particular, the free algebra $\mathcal{F} = \mathcal{F}^\mathcal{V}(x, y, z)$ on three generators is congruence permutable. Set $\alpha = Cg^\mathcal{F}(x, y)$ and $\beta = Cg^\mathcal{F}(y, z)$. Since $\mathcal{F}$ is congruence permutable, $(x, z) \in \alpha \circ \beta = \beta \circ \alpha$. So, there exists some term $t(x, y, z)$ in $\mathcal{F}$ so that $x \beta t(x, y, z) \alpha z$.

Now, if we take the quotient of $\mathcal{F}$ by $\alpha$, we are effectively collapsing $x$ with $y$ and the resulting algebra will be isomorphic to the free algebra in $\mathcal{V}$ on two generators. In $\mathcal{F}/\alpha$, we have that $t(x, y, z)/\alpha = t(x, x, z)/\alpha = z/\alpha$, so since the free algebra on two generators satsifies the equation $t(x, x, z) \approx z$, so does all of $\mathcal{V}$. Modding out by
\( \beta \) in the same way gives us that \( t(x, y, y) \approx x \), and so \( t \) is a Mal'tsev term for all of \( V \).

We define a *unary polynomial* in some algebra \( A \) as a function made from taking a term \( t(x, y_1, \ldots, y_{n-1}) \) and replacing each \( y_i \) with some parameter \( b_i \in A \), and leaving \( x \) as an argument. Unary polynomials can be used in congruence permutable varieties to define any principal congruences, as the following folklore theorem shows.

**Theorem 1.7.** Suppose \( V \) is a congruence permutable variety with Mal'tsev term \( m(x, y, z) \). Then, for any \( A \in V \) and any elements \( c, d \in A \), we have that \( (c, d) \) belongs to \( Cg^A(a, b) \) iff there exists a unary polynomial \( p(x) \) so that \( \{p(a), p(b)\} = \{c, d\} \).

**Proof.** Let \( C = \{\langle p(a), p(b) \rangle \mid p \text{ is some unary polynomial in } A\} \). The identity function is a unary polynomial, so \( \langle a, b \rangle \in C \) and therefore \( Cg^A(a, b) \subseteq C \). Also, \( C \in Cg^A(a, b) \), since \( Cg^A(a, b) \) is a subalgebra of \( A^2 \). So, we need only prove that \( C \) is a congruence. \( C \) is a subalgebra of \( A^2 \) since applying some basic operation to a tuple of unary polynomials will produce another unary polynomial. So, we only need to show that \( C \) is an equivalence relation.

To see that \( C \) is reflexive, let \( c \in A \) and let \( p(x) = m(x, x, c) \). Then, \( \langle p(a), p(b) \rangle = \langle c, c \rangle \).

To see that \( C \) is symmetric, suppose that \( \langle p(a), p(b) \rangle \in C \) for some polynomial \( p \). Let \( q(x) = m(p(a), p(x), p(b)) \). Then, \( \langle q(a), q(b) \rangle = \langle p(b), p(a) \rangle \).

To see that \( C \) is transitive, suppose that \( \langle p(a), p(b) \rangle \) and \( \langle q(a), q(b) \rangle \) are elements of \( C \) where \( p \) and \( q \) are unary polynomials and \( p(b) = q(a) \). Then, set \( r(x) = m(p(x), p(b), q(x)) \). Then, \( \langle r(a), r(b) \rangle = \langle p(a), q(b) \rangle \).

Freese and McKenzie in their Commutator Book prove a number of results relating nilpotence and congruence permutability (Freese and McKenzie 1987). We will reproduce a number of their results here, including proofs where convenient. The first theorem appears in the Commutator Book as Lemma 7.6.
Theorem 1.8. If $\mathcal{V}$ is a congruence permutable variety with Mal’tsev term $m(x, y, z)$, $A \in \mathcal{V}$ is a nilpotent algebra, and $a, b, c \in A$, then
\[
Cg^A(a, b) = Cg^A(m(a, b, c), c)
\]

The proof of this theorem is contingent on another useful property of nilpotent algebras; namely, the presence of a sort of inverse to the Mal’tsev term. If $m(x, y, z)$ is the Mal’tsev term of the variety $\mathcal{V}$, define the terms $f_n(y, u, v)$ inductively by
\[
f_0(y, u, v) := y \text{ and } f_{n+1}(y, u, v) = m(u, m(u, y, m(f_n(y, u, v), u, v)), f_n(y, u, v))
\]

The following lemma (which appears in the Commutator Book as Lemma 7.3) shows us that for any $A \in \mathcal{V}$ and $b, c \in A$, the function $x \mapsto f_n(x, b, c)$ is the inverse of the function $x \mapsto m(x, b, c)$ provided $A$ is nilpotent. We do not prove the lemma, as its proof involves several layers of technical results from the Commutator Book.

Lemma 1.9. If $A \in \mathcal{V}$ as above and $x, y, b, c \in A$, then for every $n$, we have
\[
f_n(m(x, b, c), b, c) \ (1)_n x \text{ and } m(f_n(y, b, c), b, c) \ (1)_n y
\]

Corollary 1.10. If $A \in \mathcal{V}$ is nilpotent and $b, c \in A$, then the function $x \mapsto m(x, b, c)$ is bijective. Moreover, if $\phi \in \text{Con}(A)$, then this function, restricted to $b/\phi$, is a bijection from $b/\phi$ to $c/\phi$.

Proof. The bijectivity of the function is clear from Lemma 1.9. Let $f$ denote the function restricted to $b/\phi$. If $f(x) = f(y)$ for $x, y \in b/\phi$, then $x = f_n(f(x), b, c) = f_n(f(y), b, c) = y$, so $f$ is injective. Now, since $A/\phi$ is also nilpotent, the function $x \mapsto m(x, b/\phi, c/\phi)$ is bijective as well, and therefore induces a permutation of the $\phi$-blocks. Hence, the inverse images of every element of $c/\phi$ under $f$ belong to $b/\phi$. Now, surjectivity of $f$ is a consequence of the surjectivity of the nonrestricted function. □
Corollary 1.11. If $A$ is nilpotent, then $A$ has uniform congruences (that is, all the blocks of a given congruence have the same size). \qed

Now, armed with the inverse, we can prove Theorem 1.8.

**Proof.** Suppose $(1)_k = 0$ in $A$. Then, $p(f_n(c, b, c), b, c) = c = p(b, b, c)$. So, $f_n(c, b, c) = b$, by Corollary 1.10. Now, let $\phi = Cg^A(m(a, b, c), c)$. The unary polynomial $p(a, b, c)$ maps $a$ to $m(a, b, c)$ and $b$ to $c$, so $\langle m(a, b, c), c \rangle \in Cg^A(a, b)$ and so $\phi \leq Cg^A(a, b)$.

But also, $m(a, b, c) \phi c$. So, $a = f_n(m(a, b, c), b, c) \phi f_n(c, b, c) = b$

Thus, since $\langle a, b \rangle \in \phi$, we have that $Cg^A(a, b) \leq \phi$. \qed

The next theorem, which appears in the Commutator Book as Theorem 14.2, establishes that nilpotence persists throughout the whole variety. We omit the proof.

**Theorem 1.12.** Let $\mathcal{V} = \mathcal{V}(A)$ be a congruence modular variety. If $A$ is nilpotent of class $k$, then every other algebra in $\mathcal{V}$ is nilpotent of class at most $k$.

We take a moment to note here that the main result of Chapter 3, Theorem 3.1, is in fact generalisable in two different directions. Firstly, according to Freese and McKenzie (1987), the hypothesis of congruence permutability can be weakened to congruence modularity. We state without proof a fact from Theorem 5.5 in the Commutator Book, that any congruence modular variety has a *difference term*; that is, a ternary term $d(x, y, z)$ so that $\mathcal{V} \models d(x, x, y) \approx y$ and if $\langle x, y \rangle \in \theta \in \text{Con}(A)$ for some $A \in \mathcal{V}$, then $d^A(x, y, y)[\theta, \theta] x$. Using this fact, we obtain the following theorem (Theorem 6.2 in the Commutator Book), reproducing Freese and McKenzie’s proof:

**Theorem 1.13.** If $A$ is congruence modular, then for all $\alpha, \beta \in \text{Con}(A)$, $k < \omega$, we have

$$\alpha \circ \beta \subseteq (\alpha)_k \circ \beta \circ \alpha$$

Therefore, if $A$ is nilpotent, it is congruence permutable.
Proof. We use induction on $k$. The inclusion is trivial for $k = 0$. For $k > 0$, suppose that $x \alpha y \beta z$. Then, by induction, there exist elements $u, v \in A$ where $x (\alpha_k u \beta v \alpha z$. Let $d(x, y, z)$ be a difference term in $\mathcal{V}$. Since $(\alpha)_k \leq \alpha$, we have

$$x (\alpha)_{k+1} d(x, u, u) \beta d(x, u, v) \alpha d(u, u, z) = z$$

Now, if $A$ is nilpotent, there is some $k$ so that $(\alpha)_k = 0_A$. Then,

$$\alpha \circ \beta \subseteq 0_A \circ \beta \circ \alpha = \beta \circ \alpha$$

The second possible generalisation is due to the work of Faulkner (2015) in his PhD dissertation. A weak difference term for a variety $\mathcal{V}$ is a term $p(x, y, z)$ that satisfies the Mal’tsev equations $p(a, a, b) = b = p(b, a, a)$ whenever $a$ and $b$ both belong to a block of some Abelian congruence of a member of $\mathcal{V}$. According to Faulkner’s dissertation, if $A$ is a nilpotent algebra that is the product of algebras of prime power order, and $\mathcal{V}(A)$ is a variety with a weak difference term, then every algebra in $\mathcal{V}$ is congruence permutable (and, by consequence, congruence modular). So, in fact, the hypothesis of congruence permutability in Theorem 3.1 can also be weakened to the presence of a weak difference term. Weak difference terms have been studied by Hobby and McKenzie (1988), Lipparini (1994), Mamedov (2007), and Kearnes, Szendrei, and Willard (2017). Since the hypotheses of Theorem 3.1 can be weakened in two different ways, we leave the statement of the theorem as it is, as the hypothesis of permutability unites these two generalisations.

1.4 A variety with no finite residual bound but finitely axiomatisable subdirectly irreducibles

In this section, we motivate our result’s place in the broader family of finite basis results by showing that having finitely axiomatisable subdirectly irreducible members is a strictly weaker hypothesis for a variety than a finite residual bound.
Consider the 8-element quaternion group, $Q_8$. This finite group is nilpotent. Indeed,

$$[Q_8, Q_8] = \{aba^{-1}b^{-1} \mid a, b \in Q_8\} = \{1, -1\}$$

And then,

$$[\{1, -1\}, \{1, -1\}] = \{1\}$$

So $Q_8$ is nilpotent of class 2. Theorem 2.1 posits that the variety $\mathcal{V} = \mathcal{V}(Q_8)$ has finitely axiomatisable subdirectly irreducibles, which we prove in Chapter 2. Here, we will show that $\mathcal{V}$ does not have a finite residual bound. That is, that there are infinitely large subdirectly irreducibles in $\mathcal{V}$. In fact, we will show the stronger fact that for any cardinal $\kappa$, there is a subdirectly irreducible algebra in $\mathcal{V}$ that has cardinality $\kappa$. The following argument is a modified version of the proof of Theorem 24 in Anthony Bonato’s master’s thesis (Bonato 1994).

It is easy to see that $Q_8$ is subdirectly irreducible, with monolith $M = \{1, -1\}$. In the case of $Q_8$, the monolith $M$ is actually also the center of the group. Now, let $K$ be the normal subgroup of $Q_8 \times Q_8$ generated by $\{(x, x^{-1}) \mid x \in Q_8\}$. Clearly, $M \times \{1\} \subseteq K$ since -1 is its own inverse.

Now, let $\lambda$ be an infinite cardinal, and let

$$B = \{f \in Q_8^\lambda \mid f(i) = 1 \text{ for all but finitely many } i < \lambda\}$$

$B$ is a subgroup of $Q_8^\lambda$, since having finitely many nonidentity coordinates is a property conserved under multiplication and inverse. Now, for each $i < j < \lambda$, define

$$K_{ij} = \{f \in B \mid (f(i), f(j)) \in K \text{ and } f(k) = 1 \text{ for all } k \neq i, j\}$$

and define

$$N = \{f \in B \mid f(i) \in M \text{ for each } i < \lambda \text{ and } \prod_{i<\lambda} f(i) = 1\}$$

Now, we have that $K_{ij} \triangleleft B$ for all $i < j$, since $bab^{-1}$ is the inverse of $ba^{-1}b^{-1}$. We also have $N \triangleleft B$, since $M$ is the center of $Q_8$ and so every coordinate in any element of $N$. 

29
commutes with the rest of $Q_8$. Now, for any $c \in Q_8$ and $i < j$, we define $f_i^c \in B$ by:

$$f_i^c(j) = \begin{cases} c & \text{if } j = i \\ 1 & \text{otherwise} \end{cases}$$

Now, fix some $a \in M$ where $a \neq 1$. Since $M \times \{1\} \subseteq K$, we have that $f_i^a \in K_{ij}$ for all $i < j < \lambda$. For any $i < j < \lambda$, we have $f_i^a \equiv f_j^a \mod N$, and therefore $f_0^a \in N \cap K_{ij}$ for all $i < j < \lambda$. We also know that $f_0^a \notin N$, since the product of all of its coordinates is $a$ which is not 1.

Now, let $S$ be any normal subgroup of $B$ maximal with respect to the property that $N \subseteq S$ and $f_0^a \notin S$. Then, $B/S$ is subdirectly irreducible. $B/S$ will be our arbitrarily large subdirectly irreducible algebra. We claim that for any infinite cardinal $\kappa$, if we choose $\lambda = (2^\kappa)^+$, then $|B/S| \geq \kappa^+$.

Fix $i < j < \lambda$. Then, $K_{ij}$ is the smallest normal subgroup of $B$ containing the set

$$\{ f_i^x(f_j^x)^{-1} \mid x \in Q_8 \}$$

Since $f_0^a \in N \cap K_{ij}$ and $N \subseteq S$, but $f_0^a \notin S$, we know that $K_{ij} \not\subseteq S$. So,

$$\{ f_i^x(f_j^x)^{-1} \mid x \in Q_8 \} \not\subseteq S$$

Therefore, for all $i < j < \lambda$, there exists some $x \in Q_8$ so that $f_i^x(f_j^x)^{-1} \notin S$. Now, by the Erdős-Rado theorem, there exists $X \subseteq \lambda$ such that $|X| = \kappa^+$ and some $c \in Q_8$ such that

$$(i, j \in X \text{ and } i < j) \rightarrow f_i^c(f_j^c)^{-1} \notin S$$

Here, $f_i^c$ has coordinates that are pairwise inequivalent modulo $S$. So, $|B/S| \geq |X| \geq \kappa^+$. Therefore, $V$ is residually large.

### 1.5 An example of a nilpotent algebra that is not the product of algebras of prime power order

In this section, we illustrate the necessity of one of our theorem’s hypotheses by proving the existence of a nilpotent algebra that is not the product of algebras of prime power order.
prime power order. We present an example of a 12-element algebra from Michael Vaughan-Lee’s paper on nilpotence in congruence permutable varieties (Vaughan-Lee 1983).

A loop is an algebra \( \langle A, 1, *, \backslash, / \rangle \) satisfying the equations

\[
\begin{align*}
x \ast 1 & \approx x \approx 1 \ast x \\
y & \approx x \ast (x \backslash y) & y & \approx x \langle x \ast y \rangle \\
y & \approx (y/x) \ast x & y & \approx (y \ast x)/x
\end{align*}
\]

The operations \( \backslash \) and / can be viewed as a left division and a right division, respectively. Associative loops are simply groups, where \( x \backslash y \) is \( x^{-1}y \) and \( x/y \) is \( xy^{-1} \).

Loops are always congruence permutable, by the following Mal’tsev term:

\[ m(x, y, z) \approx x \ast (y \backslash z) \]

Vaughan-Lee’s example is the loop \( A \) given by the following multiplication table:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>a</th>
<th>a^2</th>
<th>a^3</th>
<th>c</th>
<th>ac</th>
<th>a^2c</th>
<th>a^3c</th>
<th>c^2</th>
<th>ac^2</th>
<th>a^2c^2</th>
<th>a^3c^2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>a</td>
<td>a^2</td>
<td>a^3</td>
<td>c</td>
<td>ac</td>
<td>a^2c</td>
<td>a^3c</td>
<td>c^2</td>
<td>ac^2</td>
<td>a^2c^2</td>
<td>a^3c^2</td>
</tr>
</tbody>
</table>
| a     | a   | a^2 | a^3  | c    | ac   | a^2c | a^3c  | c^2   | ac^2 | a^2c^2 | a^3c^2 | 1      
| a^2   | a^2 | a^3 | 1    | a    | a^2c | a^3c | c    | ac    | a^2c^2 | a^3c^2 | c^2    | ac^2   |
| a^3   | a^3 | c   | a    | a^2  | a^3c | c^2  | ac   | a^2c  | a^3c^2 | 1     | ac^2   | a^2c^2 |
| c     | c   | ac  | a^2c | a^3c | c^2  | ac^2 | a^2c^2 | a^3c^2 | 1    | a     | a^2    | a^3    |
| ac    | ac  | a^2c| a^3c | c^2  | ac   | a^2c^2 | a^3c^2 | c    | ac^2 | a^2c   | a^2c^2 | a^3   |
| a^2c  | a^2c| a^3c | c   | ac   | a^2c^2 | a^3c^2 | c^2  | ac^2 | a^2c  | a^2  | a^3    | 1      | a      |
| a^3c  | a^3c| c^2 | ac   | a^2c | a^3c^2 | 1    | ac^2 | a^2c^2 | a^3c  | c    | a      | a^2    |
| c^2   | c^2 | ac  | a^2c | a^3c^2 | 1    | a    | a^2  | a^3c  | ac   | a^2c  | a^3    | ac     |
| ac^2  | ac^2| a^2c^2 | a^3c^2 | 1    | a    | a^2  | a^3c  | ac   | a^2c  | a^3c  | c      | ac     |
| a^2c^2| a^2c^2 | a^3c^2 | c^2  | ac^2 | a^2c  | a^3  | 1    | a    | a^2c  | a^3c  | c      | ac     |
| a^3c^2| a^3c^2 | 1    | ac^2 | a^2c^2 | a^3c  | c    | a    | a^2c  | a^3c  | c^2   | ac     | a^2c   |

31
A is commutative, which means that its left division and right division are in fact the same operation; we will use / for simplicity. So, in fact, A satisfies all of the axioms of an Abelian group except perhaps for associativity. A is not associative, since 
\[(a^2a)a = a^3a = c,\] 
but 
\[a^2(aa) = a^2a^2 = 1,\] 
so A is not quite a group.

First, we claim that A cannot be the product of algebras of prime power order. Suppose it is. Then, since A has order 12, it must be that 
\[A \cong B \times C,\] 
where B is an algebra of order 3. Let \(\pi\) be the projection of A onto B (which is a homomorphism), and let \(\eta\) be its kernel. So, \(\eta\) is the congruence given by

\[\eta = \{ \langle a, b \rangle \mid \pi(a) = \pi(b) \}\]

Congruences respect the isomorphism theorems familiar to anyone who has take an abstract algebra course, so this must mean that 
\[A/\eta \cong B,\] 
and so A/\(\eta\) has order 3. Now, by Corollary 1.11, that means that A is split into three equal blocks by \(\eta\), so in particular, the congruence class 1/\(\eta\) must have order 4. We contend that this is impossible.

Every element of A except for 1, \(a^2, c, c^2, a^2c\) and \(a^2c^2\) generates all of A. So, if \(\eta\) contains the pair \(\langle 1, x \rangle\) for any \(x\) except for these five elements, \(\eta\) must be \(1^A\) because congruence relations are subalgebras of \(A^2\). In that case, we would have that \(|1/\eta| > 4\). If \(\eta\) contains one of the pairs \(\langle 1, a^2c^2 \rangle\) or \(\langle 1, a^2c \rangle\), then taking powers of this pair produces six nontrivial pairs, each with 1 in the first coordinate, so that \(|1/\eta| > 4\).

We first claim that 1/ Cg\(A\langle 1, a^2 \rangle = \{1, a^2\}\). The following argument is based on trying to take the pair \(\langle 1, a^2 \rangle\) and the pairs \(\langle x, x \rangle\) for every \(x \in A\) that are guaranteed by reflexivity and generating new pairs by combining them with the basic operations of the loop.

Since \(\langle 1, a^2 \rangle^2 = \langle 1, 1 \rangle\), we cannot gain any new pairs from taking powers of \(\langle 1, a^2 \rangle\). If \(x \in A\), we have that \(\langle 1, a^2 \rangle \ast \langle x, x \rangle = \langle x, a^2x \rangle\) which only contributes to the congruence class of 1 if \(a^2x = 1\), in which case \(x = a^2\) and we just gain the pair
\langle a^2, 1 \rangle$, which we already knew we had from symmetry. So, multiplication of \langle 1, a^2 \rangle by other pairs does not add anything to $1/\text{Cg}^A(1, a^2)$.

If $x \in A$, then $\langle 1, a^2 \rangle/\langle x, x \rangle = \langle 1/x, a^2/x \rangle = \langle x^{-1}, a^2/x \rangle$. Again, this only contributes to $1/\text{Cg}^A(1, a^2)$ if either $x^{-1}$ is 1 (in which case $x$ is also 1), or if $a^2/x$ is 1, in which case $x$ is $a^2$. Either way, this division does not add anything to $1/\text{Cg}^A(1, a^2)$, so our claim is accurate.

Similarly, we claim that $1/\text{Cg}^A(1, c) = \{1, c, c^2\}$.

To sum up, if we consider what elements belong to $1/\eta$, we see that this congruence class is either too small or too large, and so the congruence $\eta$ cannot exist in the way that permits $A/\eta$ to have cardinality 3. Therefore, $A$ is not the product of an algebra of order 3 with anything, and so it cannot be the product of algebras of prime power order.

Now, to show that $A$ is nilpotent, we need to calculate one of its central series. We will use the upper central series in this example. So, we first need to calculate the center $\zeta_A$ of $A$. Recall that the center is defined by

$$\langle x, y \rangle \in \zeta_A \iff (\forall t)(\forall \bar{u}, \bar{v})(t(\bar{u}, x) = t(\bar{v}, x) \leftrightarrow t(\bar{u}, y) = t(\bar{v}, y))$$

We claim that $\langle 1, a^2 \rangle$ cannot be in $\zeta$, and provide an example for a term violating the condition above. Let

$$t(z_0, z_1, z_2, z_3, x) = (x * (z_0/z_1)) * (z_2 * (z_3/z_2))$$
And let \( \langle u_0, u_1, u_2, u_3 \rangle = \langle a^2, a^2, a, 1 \rangle \) and \( \langle v_0, v_1, v_2, v_3 \rangle = \langle 1, a, a, a \rangle \). Then, we have

\[
\begin{align*}
t(\bar{u}, 1) &= (1 * (a^2/a^2)) \ast (a * (1/a)) = 1 \ast 1 = 1 \\
t(\bar{v}, 1) &= (1 * (1/a)) \ast (a * (a/a)) = (1/a) \ast a = 1
\end{align*}
\]

however,

\[
\begin{align*}
t(\bar{u}, a^2) &= (a^2 * (a^2/a^2)) \ast (a * (1/a)) = a^2 \ast 1 = a^2 \\
t(\bar{v}, a^2) &= (a^2 * (1/a)) \ast (a * (a/a)) = (a^2 \ast a^3 c^2) \ast (a) = ac^2 \ast a = a^2 c^2
\end{align*}
\]

This fact rules out a number of pairs from being in \( \zeta \). In fact, using the same reasoning as above that discusses which elements generate all of \( A \), it follows from the exclusion of \( \langle 1, a^2 \rangle \) that \( \zeta \) must either collapse 1 with \( c \) and \( c^2 \), or else be the trivial congruence \( 0_A \). We claim that the former is true, and that in fact \( \zeta = Cg^A(1, c) \). Let \( t(\bar{z}, x) \) be a term.

Intimate familiarity with the multiplication table of \( A \) provides the fact that the element \( c \) associates with any other two elements of \( A \). That is, \( x(y c) = (x y)c \), \( x(c y) = (x c)y \) and \( c(x y) = (c x)y \). Therefore, if \( \bar{u} \) is a tuple of parameters from \( A \), every multiplicative occurrence of \( c \) in \( \bar{u} \) can be "factored out" and moved to one side of the equation. In the case of division, we can do the same thing by observing that \( c/x = c * (1/x) \) and \( x/c = (x/1) * c^2 \). All of this means that \( t(\bar{u}, c) = t(\bar{u}, 1) * (c^m) \) where \( m \) is some integer. Therefore, we have

\[
\begin{align*}
t(\bar{u}, c) &= t(\bar{v}, c) \\
\uparrow &
\end{align*}
\]

\[
\begin{align*}
t(\bar{u}, 1) \ast (c^m) &= t(\bar{v}, 1) \ast (c^m) \\
\uparrow &
\end{align*}
\]

\[
\begin{align*}
t(\bar{u}, 1) &= t(\bar{v}, 1)
\end{align*}
\]

To sum up, we know that the pair \( \langle 1, a^2 \rangle \) does not belong to \( \zeta \), but the pair \( \langle 1, c \rangle \) does. So, the only remaining candidate for \( \zeta \) is the congruence \( Cg^A(1, c) \).
Now, observe that $A/\zeta$ is a four-element loop whose congruence classes are $1/\zeta$, $a/\zeta$, $a^2/\zeta$, and $a^3/\zeta$. This four-element loop is actually associative, since $\zeta$ collapses $1$ and $c$. So, it is in fact isomorphic to the four-element cyclic group, which is Abelian. Therefore, $A$ is nilpotent of class 2.

For more information on loops, including a fascinating exploration of the commutator and center in loops, we refer readers to Stanovský and Vojtěchovský (2014). This paper contains, amongst other things, a theorem that the center of a loop is precisely the congruence that collapses the identity with every element that both commutes and associates with the rest of the loop, which aided in our analysis of Vaughan-Lee’s example.
Chapter 2

The Group Theorem

In this section, we will prove the finite axiomatisability theorem for groups. We restate the theorem from the introduction.

**Theorem 2.1.** Let $\mathcal{V}$ be a variety generated by a finite nilpotent group $G$. Then, the class $\mathcal{V}_{si}$ of subdirectly irreducible groups belonging to $\mathcal{V}$ is axiomatisable by a finite set of elementary sentences.

Any group is congruence permutable by the Mal’tsev term $m(x, y, z) = xy^{-1}z$. In addition, every finite nilpotent group is the direct product of its Sylow subgroups, and is therefore the product of groups of prime power order (we will prove this fact below). Hence, Theorem 2.1 is actually contained within the result for general algebras, but we will prove it in a different way using group-theoretic concepts rather than general algebraic concepts. In this section, we will reinterpret many of the definitions from the introduction through the lens of group theory.

The first adjustment to be made is to shift our focus back from congruence relations to normal subgroups. Recall that the two are interchangeable; the classes of congruences of a given group that contain the identity element are in bijection with the normal subgroups of that group, and the lattices are isomorphic. The definition of subdirect irreducibility will now adjust in the natural way: a group is subdirectly irreducible if it has a smallest nontrivial normal subgroup that is contained within every other nontrivial normal subgroup. Recall that an algebra is subdirectly irreducible if it has a critical pair $\langle c, d \rangle$. In groups, this implies that the pair $\langle cd^{-1}, 1 \rangle$ generates
the monolith congruence; so, the element $cd^{-1}$ generates the monolith subgroup as a normal subgroup. In fact, the monolith is the normal closure of any of its nonidentity elements. In groups with nontrivial centers (such as nilpotent groups), the monolith is always contained within the center and therefore is actually a cyclic subgroup.

As an example, the 8-element quaternion group $Q_8$ is subdirectly irreducible. This follows from observing that the normal subgroup \{1, −1\} is contained within every other nontrivial normal subgroup of $Q_8$. In this case, the element −1 generates the monolith.

Next, we will redefine nilpotence in the context of normal subgroups. The following definition agrees with the definition for nilpotent algebras.

2.0 Nilpotent groups

We define the normal closure of a set $X$ of elements of a group $G$ as the smallest normal subgroup containing $X$. We may also call it the normal subgroup generated by $X$. We will denote this subgroup by $\text{Norm}_G(X)$ or $\text{Norm}(X)$ when $G$ is clear from context. If $X$ is a singleton set, say $X = \{a\}$, we call this subgroup a principal normal subgroup and write $\text{Norm}(a)$. Note that in a subdirectly irreducible group, the monolith cannot contain any nontrivial normal subgroup and is therefore always principal.

Given two elements $a, b$ of a given group $G$, their commutator $[a, b]$ is the element $aba^{-1}b^{-1}$. The commutator operation can be extended to normal subgroups; the commutator of two normal subgroups $H$ and $K$ of $G$ is defined as $[H, K] = \{[h, k] : h \in H, k \in K\}$. The commutator of two normal subgroups is again a normal subgroup. Using the commutator operation, one may fabricate a lower central series $G_0 \triangleright G_1 \triangleright G_2 \triangleright \ldots$ where $G_0 = G$ and $G_i = [G, G_i]$. The group $G$ is called nilpotent of class $k$ if there is some $k$ for which $G_k = \{1\}$. 
Recall that for any group $G$, the *center* $Z(G)$ is the subgroup of all elements that commute with every other element of $G$. An equivalent (and, for our purposes, more useful) definition of nilpotence is the presence of an *upper central series* $Z_0 \lhd Z_1 \lhd Z_2 \lhd \ldots$ so that $Z_0 = \{1\}$, $Z_1 = Z(G)$, the center of $G$, and for each $i$, $Z_{i+1}/Z_i = Z(G/Z_i)$. The group $G$ is nilpotent of class $k$ if there is some $k$ for which $Z_k = G$. It is well-known that the length of the upper and lower central series coincides; a proof can be found in Dummit and Foote (2004) as Theorem 8 of section 6.1.

As an example, we turn to our old friend $Q_8$. This group is not Abelian, so it is not nilpotent of class 1. Examining the lower central series, we see that $G_1 = [Q_8, Q_8] = \{1, -1\}$, and so then $G_2 = [Q_8, [Q_8, Q_8]] = \{1\}$.

On the other hand, examining the upper central series, we observe that the center $Z_1 = Z(Q_8) = \{1, -1\}$. Then, $Q_8/Z_1 = \{Q_8, iQ_8, jQ_8, kQ_8\}$ which is isomorphic to the Klein-4 group. This group is Abelian, and so $Z(Q_8/Z_1) = Q_8/Z_1$, therefore $Z_2 = Q_8$. Both central series have length 2, and so $Q_8$ is nilpotent of class 2.

We will now prove that a finite group is nilpotent if and only if it is the direct product of its Sylow subgroups, reproducing this proof also from Dummit and Foote, where it appears in section 6.1 as Theorem 3. Recall that for a subgroup $H$ of a group $G$, the *normaliser* of $H$ in $G$ is the subgroup

$$N_G(H) = \{g \in G \mid gH = Hg\} = \{g \in G \mid \forall h \in H, \ ghg^{-1} \in H\}$$

**Theorem 2.2.** Let $G$ be a finite group, let $p_0, p_1, \ldots, p_{s-1}$ be the distinct primes dividing its order, and let $P_i$ be their corresponding Sylow $p_i$-subgroups. Then, the following are equivalent.

1. $G$ is nilpotent.
2. Every proper subgroup of $G$ is a proper subgroup of its normaliser in $G$.
3. Every Sylow subgroup of $G$ is normal in $G$.  

38
4. \( G \cong P_0 \times P_1 \times \cdots \times P_{s-1} \)

**Proof.** 1 \( \Rightarrow \) 2) Let \( H \) be a proper subgroup of \( G \). Clearly, \( H \leq N_G(H) \), so it remains to show that \( H \neq N_G(H) \). We will prove this by induction on the nilpotence class of \( G \). Recall that \( Z = Z(G) \) is the center of \( G \). Of course, \( Z \subseteq N_G(H) \). If \( Z \) is not contained in \( H \), then \( H \) cannot equal \( N_G(H) \), so suppose \( Z \subseteq H \). Now, \( G/Z \) is also nilpotent of degree one less than \( G \) itself. Therefore, \( N_{G/Z}(H/Z) \neq N_G(H)/Z \) by induction. But, \( N_{G/Z}(H/Z) = N_G(H)/Z \) and so \( H \neq N_G(H) \).

2 \( \Rightarrow \) 3) Let \( P = P_i \) for some \( i \) and let \( N = N_G(P) \). Since \( P \triangleleft N \), we have that \( P \) is characteristic in \( N \) by a corollary to Sylow’s theorem. Since \( N \triangleleft N_G(N) \), we have that \( P \triangleleft N_G(N) \). So, \( N_G(N) \leq N \) and so \( N_G(N) = N \). By (2), that must mean that \( N \) is \( G \) itself.

3 \( \Rightarrow \) 4) We will use induction on \( t \) to show that for any \( 1 \leq t \leq s \),

\[
P_1P_2\ldots P_t \cong P_1 \times P_2 \times \cdots \times P_t
\]

The case \( t = 1 \) is trivial. Since each \( P_i \) is normal, \( P_1\ldots P_t \) is a subgroup of \( G \). Let \( H = P_1\ldots P_{t-1} \) and let \( K = P_t \). So, by induction, \( H \cong P_1 \times \cdots \times P_{t-1} \). This implies that \( |H| = |P_1|\ldots |P_{t-1}| \). Now, since \( |K| = |P_t| \) and the orders of \( H \) and \( K \) are relatively prime, Lagrange’s theorem tells us that \( H \cap K = 1 \). Then, a known theorem tells us that \( HK \cong H \times K \). So, we have

\[
P_1\ldots P_t = HK \cong H \times K = (P_1 \times \cdots \times P_{t-1}) \times P_t \cong P_1 \times \cdots \times P_t
\]

4 \( \Rightarrow \) 1) We will use induction on \( |G| \). It is true that

\[
Z(P_1 \times \cdots \times P_s) \cong Z(P_1) \times \cdots \times Z(P_s)
\]

and that

\[
G/Z(G) = (P_1/Z(P_1)) \times \cdots \times (P_s/Z(P_s))
\]
So that means that (4) also holds for $G/Z(G)$. Any nontrivial $p$-group has a nontrivial center, so if $G$ is nontrivial, then $|G/Z(G)| < |G|$. By induction, $G/Z(G)$ is nilpotent, so that means that $G$ must be nilpotent also.

By Lyndon’s proof of the main result in his finite basis result, the nilpotence class of a group can be captured with a finite set of equations (Lyndon 1952). Therefore, if $G$ is nilpotent of class $k$, any group $H \in V(G)$ is nilpotent of class at most $k$.

Given a group $G$, the normal subgroups of $G$ form a lattice. If $K < N$ are normal subgroups of $G$ and there exists no normal subgroup $M$ of $G$ so that $K \leq M \leq N$, then $N/K$ is called a chief factor of $G$. The following result is due to Hanna Neumann’s Theorem 51.23 (Neumann 1967).

**Theorem 2.3.** If $G$ is a finite group, then the cardinality of any finite chief factor in the variety generated by $G$ is bounded above by $|G|$.

**Proof.** Let $H$ be a finite group in $V(G)$. Then, $H$ is a homomorphic image of a finite direct product of subalgebras of $G$, say that

$$H = h(G_0 \times G_1 \times \cdots \times G_{n-1})$$

Or, if $h_i$ is the restriction of $h$ to $G_i$,

$$H = h_0(G_0) \times \cdots \times h_{n-1}(G_{n-1})$$

If $N/K$ is a chief factor of $H$, then there is some unrefinable normal series in $H$ where $K$ and $N$ are successive members of that series. That is,

$$\{1\} = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_i \triangleleft K \triangleleft N = N_{i+1} \triangleleft \cdots \triangleleft N_{m-1} = H$$

To find this series, simply look at the normal subgroup lattice of $H$, and find a chain from $\{1\}$ to $H$ that includes $K$ and $N$.

The chief series $(N_i)_{0}^{m-1}$ can be refined in such a way that each factor $N_{i+1}/N_i$ is a chief factor of some $h_i(G_i)$. So, there is some $h_i(G_i)$ in which $N/K$ is the image of
a chief factor. The preimage of $N/K$ is bounded above by the largest size of a chief factor in $h_i(G_i)$, which is in turn bounded above by the largest size of a chief factor in $G_i$, and again in $G$. Of course, the largest a chief factor of $G$ could possibly be is if $G$ is simple and the factor is $G/\{1\}$. Therefore, $|N/K| \leq |G|$. \hfill $\square$

This result was actually extended in Freese and McKenzie’s Commutator Book to the following theorem, where it appears as part of Theorem 10.16. Here, $\alpha \succ \beta$ means that $\alpha \geq \beta$ and that there is no congruence between $\alpha$ and $\beta$.

**Theorem 2.4.** Let $A$ be a finite algebra in a congruence modular variety, and let $B \in \mathcal{V}(A)$. Let $\alpha$ and $\beta$ be congruences of $A$ so that $\alpha \succ \beta$. Then, the supremum over $x \in A$ of the cardinalities of the sets $\{y/\beta \mid y \in x/\alpha\}$ is bounded above by $|A|$. In particular, if $A$ is a group, then the cardinality of any chief factor in $\mathcal{V}$ is bounded above by $|A|$.

We omit the proof of this extension, as it involves a number of concepts not mentioned in this dissertation. Curious readers can find it as Theorem 10.16 in the Commutator Book (Freese and McKenzie 1987).

### 2.1 Conjugate product polynomials

We now introduce some machinery that will let us quantify principal normal subgroup inclusion in a first-order way. The set of *conjugate product terms* in $x$ of a variety of groups is the smallest set $C$ of terms so that

1. $1 \in C$

2. If $t \in C$ and $y$ is a variable, then both $(yxy^{-1})t$ and $(yx^{-1}y^{-1})t$ belong to $C$.

The definition is apt; $C$ is the set of all terms made by taking products of conjugates of $x$ and $x^{-1}$. A sample member of $C$ might be

$$t(x, y_0, y_2, y_7) = y_0x y_0^{-1} y_2 x^{-1} y_2^{-1} y_7 x y_7^{-1}$$
A conjugate product polynomial is a unary polynomial $\pi(x)$ forged from some conjugate product term. We might write $\pi(x, \bar{y})$ if we wish to specify the parameters. So, for instance, in some group $H$, we might choose members $c_0, c_2, c_7 \in H$ and, from our prior example, obtain the following conjugate product polynomial

$$\pi(x) = t(x, c_0, c_2, c_7) = c_0 x c_0^{-1} c_2 x^{-1} c_2^{-1} c_7 x c_7^{-1}$$

Conjugate product polynomials are a powerful tool in groups; they are capable of defining principal normal subgroups. The normal closure of an element $a$, for instance, is the collection of products of conjugates of $a$ and $a^{-1}$, which is precisely the outputs of the set of conjugate product polynomials in $a$. This arms us with a method of defining principal normal subgroups with objects that are easily written in first-order logic.

**Proposition 2.5.** Given an element $a$ of a group $G$, the normal closure $\text{Norm}(a)$ consists precisely of all elements $\pi(a)$ where $\pi$ is some conjugate product polynomial.

We refer to a statement of the form $a \in \text{Norm}(c)$ as a membership condition. Membership conditions are our main object of interest in trying to establish definable principal normal subgroups, and we now have technology in the form of conjugate product polynomials to witness them. Our strategy in the proof will be to show that these conditions can be witnessed with a limited number of variables. This will enable us to quantify the witnessing using a first-order statement. In this paper, the complexity of a conjugate product polynomial refers to the number of conjugates present in the product. Our previous example has complexity 3.

### 2.2 Definable principal normal subgroups

We will now redefine Baker and Wang’s notion of definable principal subcongruences to use normal subgroups instead of congruence relations.
Let $\Phi(x, y)$ be an elementary formula. We will say that $\Phi$ is a *normal closure formula* provided that for any group $G$, if $\Phi(a, b)$ holds in $G$, then $a$ belongs to the normal closure $\text{Norm}_G(b)$. For instance, the formula

$$\exists z \ (x \approx zyz^{-1})$$

is a normal closure formula, since any conjugate of the element $b$ will belong to $\text{Norm}(b)$. These formulas will take the place of congruence formulas in the definition.

We will say that a class $\mathcal{K}$ of groups has *definable principal normal subgroups* if and only if there are normal closure formulas $\Phi(x, y)$ and $\Psi(x, y)$ so that for every $H \in \mathcal{K}$ and every nonidentity $b \in H$, there exists a nonidentity $a \in H$ so that

1. $H \models \Psi(a, b)$ and
2. $\Phi(x, a)$ defines the normal closure of $a$.

In other words, if $b$ is an arbitrary element of $H$, then $\Psi$ can find some nonidentity $a \in \text{Norm}(b)$ so that $\text{Norm}(a)$ is definable by $\Phi$.

We will reprove Theorem 1.1 using these new definitions, but the proof itself is almost identical modulo some technical changes.

**Theorem 2.6.** If $\mathcal{V}$ is a variety of groups and $\mathcal{V}_{si}$ has definable principal normal subgroups, then $\mathcal{V}_{si}$ is finitely axiomatisable relative to $\mathcal{V}$. In particular, if $\mathcal{V}$ is finitely axiomatisable, then $\mathcal{V}_{si}$ is finitely axiomatisable.

**Proof.** Let $\Sigma$ be a finite set of elementary sentences which axiomatises $\mathcal{V}$, and let $\Phi(x, y)$ and $\Psi(x, y)$ be the formulas witnessing that $\mathcal{V}_{si}$ has definable principal normal subgroups. Let $\Theta$ be the following set of sentences:

$$\Sigma \cup \{\exists u [u \neq 1 \land \forall z (z \neq 1 \Rightarrow \exists x (\Phi(u, x) \land \Psi(x, z)))]\}$$

We claim that $\Theta$ axiomatises $\mathcal{V}_{si}$. 
On one hand, suppose $S \in \mathcal{V}_{si}$. Let $c$ be a generator of the monolith of $S$. So, $c \neq 1$ and $c$ belongs to every nontrivial normal subgroup. Now, let $b \in S - \{1\}$. Because $\mathcal{V}_{si}$ has definable principal normal subgroups, there exists some nonidentity $a \in S$ so that $S \models \Psi(a,b)$ and $\Phi(x,a)$ defines the normal closure $\text{Norm}_S(a)$. Since $c$ generates the monolith, however, $c \in \text{Norm}(a)$ also, and so $S \models \Phi(c,a)$. So,

$$S \models \exists u[u \neq 1 \land \forall z(z \neq 1 \Rightarrow \exists x(\Phi(u,x) \land \Psi(x,z)))]}$$

Since $S$ belongs to $\mathcal{V}$, $S \models \Sigma$ also. Therefore, $S \models \Theta$.

Now, suppose $S \models \Theta$. Then, $S \in \mathcal{V}$ since $\Sigma$ axiomatises $\mathcal{V}$. But also, since $S$ believes the second part of $\Theta$ and since $\Phi$ and $\Psi$ are normal closure formulas, there exists $c \in S - \{1\}$ so that $c$ is contained within any other principal normal subgroup. In particular, the principal normal subgroup $\text{Norm}(c)$ is contained within any other principal normal subgroup of $S$ and so $S$ is subdirectly irreducible.

2.3 Proof of the group theorem

In view of Theorem 2.6 and Oates and Powell (1964), to prove our main result we need only prove the following.

**Theorem 2.7.** Let $\mathcal{V}$ be a variety generated by a finite nilpotent group $G$. Then, $\mathcal{V}_{si}$ has definable principal normal subgroups.

In order to show that $\mathcal{V}_{si}$ has definable principal normal subgroups, as desired, we need two different normal closure formulas. The first formula, $\Psi(x,y)$, will seek out some definable principal normal subgroup (in our case, the monolith) of any given principal normal subgroup in $\mathcal{V}_{si}$. The second formula, $\Phi(x,y)$, will actually define the monolith. We will prove the existence of $\Phi$ first, using a proof of McNulty and Wang that appears in their unpublished paper that they have kindly allowed to be presented here. By an *atom* we mean a nontrivial normal subgroup $N$ of $G$ which does not properly contain any other nontrivial normal subgroups of $G$. 44
**Theorem 2.8.** Let \( \mathcal{V} \) be the variety generated by a finite group. Then, there is a normal closure formula \( \Phi(x, y) \) such that for any \( H \in \mathcal{V} \) and every \( c \in H \) such that \( \text{Norm}_H(c) \) is an atom in the lattice of normal subgroups of \( H \), it follows that \( \Phi(x, c) \) defines \( \text{Norm}_H(c) \).

**Proof.** Let \( r \) be a finite upper bound on the size of chief factors in algebras belonging to \( \mathcal{V} \) as given by Theorem 2.4. Then, we claim that if \( \text{Norm}(c) \) is an atom for some \( c \in H \), then any membership condition of the form \( a \in \text{Norm}(c) \) can be witnessed by a conjugate product polynomial of complexity no more than \( r \).

If \( a \in \text{Norm}(c) \), then \( a = g_0g_1 \cdots g_{n-1} \) where each \( g_i \) is some conjugate of either \( c \) or \( c^{-1} \). If \( n \) is chosen to be as small as possible, then the elements

\[
g_0, \ g_0g_1, \ g_0g_1g_2, \ldots, g_0g_1 \cdots g_{n-1}
\]

are \( n \) distinct elements of \( \text{Norm}(c) \). Now, since \( \text{Norm}(c) \) is an atom, \( \text{Norm}(c)/\{1\} \) is a chief factor. Thus, \( |\text{Norm}(c)| = |\text{Norm}(c)/\{1\}| \leq r \), so \( n \leq r \).

Now, let \( T \) be the set of all conjugate product terms in the signature of \( \mathcal{V} \) whose parameters are chosen from the distinct variables \( u_0, \ldots, u_{r-1} \). Since there are only finitely many variables being used and \( \mathcal{V} \) is locally finite, \( T \) is finite. Now, let \( \Phi(x, y) \) be the formula

\[
\exists u_0, \ldots, u_{r-1} \left[ \bigvee_{t \in T} t(y, \bar{u}) \approx x \right]
\]

\( \Phi(x, c) \) now defines \( \text{Norm}(c) \) whenever \( \text{Norm}(c) \) is an atom.

Theorem 2.8 gives us a normal closure formula that can define any atoms in any group belonging to the given \( \mathcal{V} \); in particular, for any group in \( \mathcal{V}_{si} \), this formula will always define the group’s monolith. The second formula that we need, \( \Psi(x, y) \), will come from the following theorem, which is the original work of the author.
Theorem 2.9. Let $\mathcal{V}$ be a variety generated by a nilpotent group $G$ of finite exponent. Let $S \in V_{k_S}$. Then, given any $a \in S$, there is some nonidentity $b$ belonging to the monolith of $S$ so that the membership condition $b \in \text{Norm}(a)$ is witnessed by a conjugate product polynomial of complexity bounded above in terms of the generating group $G$.

Proof. Since $S \in V$, the exponent $m$ of $S$ divides that of $G$, as the equation $x^{\text{exp}(G)} = 1$ holds throughout $\mathcal{V}$. We also know from Lyndon’s work that the nilpotence class $k$ of $S$ is bounded above by that of $G$. Denote the upper central series by $S$ as

$$
\{1\} = Z_0 \triangleleft Z_1 \triangleleft \ldots \triangleleft Z_k = S
$$

Note that $Z_1$ is the center of $S$, which contains the monolith $M$ of $S$. Choose any arbitrary $a \in S$. If $a \in M$, then no more work is needed, so we can assume it is not. Label $a = a_k$; now, we will form a sequence of elements walking down the steps of the central series that form a chain of principal normal subgroups.

Given $a_{i+1} \in Z_{i+1}$, we will seek out $a_i$ so that the following hold:

1. $a_i \in Z_i$
2. $a_i \neq 1$
3. $a_i \in \text{Norm}(a_{i+1})$ and this fact is witnessed by a conjugate product polynomial of complexity at most $m$.

We can certainly find $a_i \in Z_i$ so that $a_i \in \text{Norm}(a_{i+1})$; since $S$ is subdirectly irreducible, any element of the monolith $M$ will suffice. We choose $a_i$ from all such possible nonidentity candidates in $Z_i$ so that the conjugate product polynomial $\pi_i$ that witnesses $\pi_i(a_{i+1}, \bar{c}) = a_i$ has minimal possible complexity, and claim that this satisfies our above three requirements. The first two are already satisfied, so we need only worry about the complexity of $\pi_i$. 

46
\( \pi_i \) takes the form \( \pi_i(x, \bar{c}) = c_0x^{\pm 1}c_0^{-1}c_1x^{\pm 1}c_1^{-1}, \ldots c_nx^{\pm 1}c_n^{-1} \) for some \( n \). The structure of this polynomial breaks down into two cases.

Case 1) There are both positive and negative conjugates present in \( \pi_i \). So, \( \pi_i \) contains, somewhere, a product of the form

\[
c_jx_j^{-1}c_{j+1}x^{-1}c_{j+1}^{-1}
\]

(or perhaps the same product with the negative conjugate on the left). We claim that these two conjugates are the whole of \( \pi_i \), and that the element \( c_ja_{i+1}c_j^{-1}c_{j+1}a_{i+1}c_{j+1}^{-1} \), which we will temporarily call \( a_i^* \), is in fact \( a_i \) itself. Indeed, \( a_i^* \) cannot be 1; if it were, these two conjugates could be removed from \( \pi_i \) to preserve the given membership condition with a shorter polynomial, contradicting \( \pi_i \)'s minimality. Clearly, \( a_i^* \in \text{Norm}(a_{i+1}) \). So all we need to do is show that \( a_i^* \in Z_i \), and then the minimal complexity of \( \pi_i \) will do the rest of the work for us.

Now, \( Z_{i+1}/Z_i \) is the center of \( S/Z_i \), so \( a_{i+1}/Z_i \) commutes with every member of \( S/Z_i \). So, we have

\[
a_i^*/Z_i = (c_ja_{i+1}c_j^{-1}c_{j+1}a_{i+1}c_{j+1}^{-1})/Z_i
\]

\[
= (c_j/Z_i)(a_{i+1}/Z_i)(c_j^{-1}/Z_i)(c_{j+1}/Z_i)(a_{i+1}^{-1}/Z_i)(c_{j+1}^{-1}/Z_i)
\]

\[
= (a_{i+1}/Z_i)(a_{i+1}^{-1}/Z_i)
\]

\[
= 1/Z_i
\]

So, \( a_i^* \in Z_i \). So, \( a_i^* = a_i \), and the complexity of the polynomial needed to witness the membership \( a_i \in \text{Norm}(a_{i+1}) \) is 2, which is certainly less than the exponent \( m \) of \( G \) unless the variety is trivial.

Case 2) The conjugates present in \( \pi_i \) are either all positive or all negative. We assume that the conjugates are all positive; if they are all negative, the proof is
almost identical. In this case, we claim that the complexity of \( \pi_i \) is at most \( m \). The argument is similar to the first case. Suppose the complexity is at least \( m \); then, look at \( a_i^* = c_0a_{i+1}c_0^{-1}c_1a_{i+1}c_1^{-1}\ldots c_{m-1}a_{i+1}c_{m-1}^{-1} \). We claim that \( a_i^* \) is, again, \( a_i \). As in the first case, \( a_i^* \) satisfies criteria 2 and 3, so it only remains to show \( a_i^* \in Z_i \). Again, we have

\[
a_i^*/Z_i = (c_0a_{i+1}c_0^{-1}c_1a_{i+1}c_1^{-1}\ldots c_{m-1}a_{i+1}c_{m-1}^{-1})/Z_i
\]

\[
= (c_0/Z_i)(a_{i+1}/Z_i)(c_0^{-1}/Z_i)\ldots (c_{m-1}/Z_i)(a_{i+1}/Z_i)(c_{m-1}^{-1}/Z_i)
\]

\[
= (a_{i+1}/Z_i)^m
\]

\[
= 1/Z_i
\]

since the exponent of any algebra in \( \mathcal{V} \) divides \( m \). So, again by minimality of \( \pi_i \), we have that \( a_i^* = a_i \), and so our polynomial has complexity at most \( m \).

So, we have a sequence \((a_i)_{i=1}^k\) that walks down through the upper central series of \( S \), all the way down to \( a_1 \) which belongs to the center of \( S \). We can also walk \( a_1 \) down to some \( a_0 \) in the monolith via a polynomial \( \pi_0 \); the same proof suffices, as \( Z_1 \) is Abelian, so in particular its elements commute with every element of \( M \). \( a_0 \in \text{Norm}(a) \), as witnessed by the composition of each of the conjugate product polynomials \( \pi_i \), which is itself a conjugate product polynomial. The complexity of the composition is bounded above by \( m^k \). This completes the proof. \( \square \)

Now, we can complete the proof of Theorem 2.7. Let \( T \) be the set of all conjugate product terms in the signature of \( \mathcal{V} \) whose parameters are chosen from the distinct variables \( u_0,\ldots,u_{m^k-1} \). Since the list of variables is finite and \( \mathcal{V} \) is locally finite, there are finitely many such terms. Now, let \( \Psi(x,y) \) be the formula

\[
\exists u_0,\ldots,u_{m^k-1} \left[ \bigvee_{t \in T} t(y,\bar{u}) \approx x \right]
\]
Let $\Phi(x, y)$ be the normal closure formula from Theorem 2.8 that defines all atoms of congruence lattices of algebras in $\mathcal{V}$. Together, $\Phi(x, y)$ and $\Psi(x, y)$ witness that $\mathcal{V}_{si}$ has definable principal normal subgroups.

By McNulty and Wang’s theorem, this secures us our desired result. So, in any variety $\mathcal{V}$ generated by a finite group, $\mathcal{V}_{si}$ is finitely axiomatisable, adding to the pool of varieties with this property that are known to be finitely based. In the next chapter, we will extend this result to more general nilpotent algebras that have a few of the nice properties that groups enjoy. The result is a direct extension, but the methods used by the proof differ. There are a few reasons for this, chief among them that there is no suitable extension of conjugate product polynomials in general algebras. As such, we must take a different route in the proof.
We restate the main theorem of this section.

**Theorem 3.1.** Let $A$ be a finite nilpotent algebra of finite signature that is a product of algebras of prime power order such that $\mathcal{V} = \mathcal{V}(A)$ is a congruence permutable variety. Then, $\mathcal{V}_{si}$ is finitely axiomatisable.

We need to do a bit of work before we can dive into the proof of this theorem. Specifically, we must develop the notion of commutator words, which are inexorably tied to Freese and McKenzie’s finite basis theorem for nilpotent algebras. We note that commutator words have only a tenuous connection with the commutator of congruences, which is an unfortunate side effect of the collision of various disciplines that birthed this terminology. However, since we are using the definition of nilpotence that uses the center congruence and not the commutator, the potential for confusion should be minimal.

### 3.0 Commutator words

In order to prove Theorem 3.1, we need a bit more heavy machinery from the commutator book. The following definition is motivated by similar concepts from the study of varieties of groups. The proof of the Oates-Powell theorem that any finite group is finitely based that appears in Chapter 5 of Neumann (1967) makes use of a result by Higman (1952), referred to in the literature as Higman’s Lemma. The lemma uses what Neumann, Higman and others call commutator words, presumably
for their connection to the commutator operation on two elements in groups. It is a
source of some regret to the author that the commutator operation on congruences
in an algebra and the concept of commutator words have little to do with each other.
Fortunately, at this point in this dissertation, we no longer need the commutator
operation, replaced as it has been with the center. Hopefully this will limit confusion
going forwards.

Suppose \( V \) is a nilpotent congruence permutable variety. Consider \( F = \mathcal{F}_V(X \cup z) \)
for some set \( X \) of variables. Define \( u + v = m(u, z, v) \) where \( m \) is the Mal’tsev term
in \( V \). This addition generates a group structure on \( F \). For \( x \in X \) define \( \delta_x \in \text{End}(F) \)
as the map where \( \delta_x(x) = z, \delta_x(z) = z, \) and \( \delta_x(y) = y \) for any \( y \in X - \{x\} \). In
other words, \( \delta_x \) fixes every element of \( X \cup z \) except for \( x \) itself, which it maps to
\( z \). Then, given a term \( w(x_1, \ldots, x_n, z) \in F \), we say that \( w \) is a commutator word if
\( \delta_x(w) = z \) for any \( x \in X \). That is to say, if any of \( x_1, \ldots, x_n \) are replaced with \( z \),
\( w(\bar{x}, z) \approx z \) in the variety \( V \). Commutator words provide a sort of decomposition
for general terms in \( V \), as shown by the following theorem, which is Lemma 14.6 in
Freese and McKenzie’s Commutator Book.

**Theorem 3.2.** If \( V \) is a congruence permutable variety and \( w(\bar{x}, z) \) is a term in the
free algebra on \( X \cup z \), then there exist commutator words \( c_i \) so that

\[
w(\bar{x}, z) \approx w(\bar{z}) + c_1(\bar{x}, z) + c_2(\bar{x}, z) + \cdots + c_m(\bar{x}, z)
\]

Here, \( u + v \) is defined as \( m(u, z, v) \), and associates to the right.

As it turns out, commutator words with enough variables always trivialise in a
nilpotent congruence modular variety generated by a finite algebra. This fact enables
another finite basis result. The following is Theorem 14.16 in the Commutator Book.

**Theorem 3.3.** Let \( A \) be a finite nilpotent algebra of finite signature that is a product
of algebras of prime power order such that \( V = V(A) \) is a congruence modular (and
hence congruence permutable) variety. Then, $\mathcal{V}$ is finitely based. Moreover, there is an integer $M$ such that if $w(\vec{x}, z)$ is a commutator word in more than $M$ variables, then $\mathcal{V} \models w(\vec{x}, z) \approx z$.

This result is a partial analogue to the Oates-Powell theorem. Its contribution to the proof of Theorem 3.1 will mirror the Oates-Powell theorem’s contribution to 2.1. Specifically, it enables us to focus on proving that in the variety $\mathcal{V}$ of interest, $\mathcal{V}_{\text{si}}$ has definable principal subcongruences.

3.1 Proving Theorem 3.1

In light of Theorem 1.1 and of Theorem 3.3, in order to prove Theorem 3.1, it suffices to prove the following:

**Theorem 3.4.** Let $A$ be a finite nilpotent algebra of finite signature that is a product of algebras of prime power order such that $\mathcal{V} = \mathcal{V}(A)$ is a congruence permutable variety. Then, $\mathcal{V}_{\text{si}}$ has definable principal subcongruences.

To recall the definition, we require two congruence formulas $\Phi(u, v, x, y)$ and $\Psi(u, v, x, y)$. The formula $\Psi$ should, if given a principal congruence in $\mathcal{V}_{\text{si}}$, find a second principal congruence that is definable by $\Phi$. We will do this by using Theorem 1.7. Recall that the membership condition $\langle c, d \rangle \in Cg^A(a, b)$ is equivalent to the presence of some unary polynomial $p(x)$ so that $\{p(a), p(b)\} = \{c, d\}$. In this section, we define the complexity of $p(x)$ as the number of parameters used in $p$. So, if we can limit the complexity of $p$ in some way that is determined entirely by the variety, we can find a first-order sentence equivalent to the membership condition in question. This will be our strategy going forward.

We begin with the following handy lemma, which follows directly from the definition of the center congruence.
Lemma 3.5. Let $\mathcal{V}$ be any variety. Let $A \in \mathcal{V}$, and let $\alpha \in \text{Con}(A)$ be an Abelian congruence. Suppose $\langle a, b \rangle \in \alpha$, and let $r(u, v, \bar{y})$ be a term so that $r^A(b, b, \bar{d}) = b$ for any sequence $\bar{d}$ of parameters. Then, it is also the case that $r^A(a, b, \bar{d}) = r^A(a, b, \bar{e})$ for any sequences of parameters $\bar{d}$ and $\bar{e}$. In other words, $r$ only depends on the first two coordinates, if those coordinates are related by an Abelian congruence.

Proof. Let $a, b$ and $r$ be as above and let $\bar{d}$ and $\bar{e}$ be any sequence of parameters of appropriate length. Then, since $\langle a, b \rangle \in \alpha$ and since $r^A(b, b, \bar{d}) = r^A(b, b, \bar{e}) = b$, the following diagram holds:

\[
\begin{array}{ccc}
r^A(b, b, \bar{d}) = b & \alpha & b = r^A(b, b, \bar{e}) \\
\downarrow & & \downarrow \\
r^A(a, b, \bar{d}) & \alpha & = r^A(b, b, \bar{e}) \alpha r^A(a, b, \bar{e})
\end{array}
\]

So, by the definition of the center and since $r(b, b, \bar{d}) = r(b, b, \bar{e})$, we have $r(a, b, \bar{d}) = r(a, b, \bar{e})$ also. $\square$

This lemma has a useful corollary pertaining to commutator words.

Corollary 3.6. Let $w(x, \bar{y}, z)$ be a commutator word in $\mathcal{V}$ with $z$ as its neutral element. Let $\alpha \in \text{Con}(A)$ be an Abelian congruence. Then, for any $\langle a, b \rangle \in \alpha$ and any parameters $\bar{d}$, we have that $w(a, \bar{d}, b) = b$.

Proof. Suppose $w(x, \bar{y}, z)$ is a commutator word as above. Set $r(u, v, \bar{y}) = w(u, \bar{y}, v)$, and let $\langle a, b \rangle \in \alpha$ and $\bar{d}$ be any sequence of parameters. Since $w$ is a commutator word, $w(z, \bar{y}, z) \approx z$, so $r^A(b, b, \bar{d}) = b$. So Lemma 3.6 applies to $r$ and thus to $w$. So, $w(a, \bar{d}, b) = w(a, b, \ldots, b, b) = b$ since $w$ is a commutator word. $\square$

Now, we prove the existence of our desired $\Phi$.

Theorem 3.7. Let $\mathcal{V}$ be a locally finite congruence permutable variety. Then, there exists a congruence formula $\Phi(u, v, x, y)$ so that for any $A \in \mathcal{V}$ and Abelian principal congruence $\alpha = Cg^A(a, b)$, $\alpha$ is defined by $\Phi(u, v, a, b)$. 

53
Proof. Let \( \mathcal{V}, \mathbf{A} \) and \( \alpha \) be as stated. First, we observe that since \( \mathcal{V} \) is congruence permutable with Mal’tsev term \( m \), by Theorem 1.8,

\[
\langle c, d \rangle \in \mathrm{Cg}^\mathbf{A}(a, b) \iff \mathrm{Cg}^\mathbf{A}(c, d) \subseteq \mathrm{Cg}^\mathbf{A}(a, b)
\]

\[
\iff \mathrm{Cg}^\mathbf{A}(m(c, d, b), b) \subseteq \mathrm{Cg}^\mathbf{A}(a, b)
\]

\[
\iff \langle m(c, d, b), b \rangle \in \mathrm{Cg}^\mathbf{A}(a, b)
\]

So, we only have to worry about characterising membership conditions of the form \( \langle c, b \rangle \in \mathrm{Cg}^\mathbf{A}(a, b) \). We claim that such a membership can be witnessed by a binary term.

Suppose, indeed, that \( \langle c, b \rangle \in \mathrm{Cg}^\mathbf{A}(a, b) \). Then, there is a unary polynomial \( p = s(x, \bar{d}) \) witnessing the membership. Suppose without loss of generality that \( p(a) = c \) and \( p(b) = b \). Now, set

\[
r(u, v, \bar{y}) = m(s(u, \bar{y}), s(v, \bar{y}), v)
\]

Now, for any parameters \( \bar{e} \), we have that \( r(b, b, \bar{e}) = m(s(b, \bar{e}), s(b, \bar{e}), b) = b \). So, by Lemma 3.5, \( r(a, b, \bar{d}) = r(a, b, \bar{b}) = c \) and \( r(b, b, \bar{d}) = r(b, b, \bar{b}) = b \) where \( \bar{b} \) is the sequence of the same length as \( \bar{d} \) with \( b \) in every coordinate. Define \( t(x, y) := r(x, y, y, \ldots, y) \). Then, \( t(a, b) = c \) and \( t(b, b) = b \). So the polynomial \( t(x, b) \) witnesses the membership condition. We note that if in fact \( p(a) = b \) and \( p(b) = c \), then defining \( r \) instead as \( m(s(v, \bar{y}), s(u, \bar{y}), v) \) gets the job done in the same way.

Now, let \( T \) be a set of representatives for all congruence classes of terms in the free algebra in \( \mathcal{V} \) on two generators. This free algebra is finite, since \( \mathcal{V} \) is locally finite. So, we can set \( \Phi(u, v, x, y) \) to be the formula

\[
\bigvee_{t \in T} (t(x, y) \approx m(u, v, y) \land t(y, y) \approx y)
\]
The monolith of a nilpotent algebra is always Abelian and principal, so Theorem 3.7 gets us halfway to definable principal congruences in $V_{si}$. Now, we must find the formula $\Psi$ that can link any given principal congruence to the monolith.

**Theorem 3.8.** Let $A$ be a finite nilpotent algebra of finite signature that is the product of algebras of prime power order such that $\mathcal{V} = \mathcal{V}(A)$ is a congruence permutable variety. Then, there exists a congruence formula $\Psi(u,v,x,y)$ so that for any $a \neq b \in S$ where $S \in V_{si}$, there is a critical pair $\langle c, d \rangle$ of $S$ so that $\Psi(c, d, a, b)$ is satisfied in $S$.

This theorem is a direct result of the following:

**Theorem 3.9.** Let $A$ be a finite nilpotent algebra of finite signature that is the product of algebras of prime power order such that $\mathcal{V} = \mathcal{V}(A)$ is a congruence permutable variety. Suppose $S \in V_{si}$. Then, for any $a \neq b \in S$, there exists some $c$ so that $\langle c, b \rangle$ is a critical pair; and the membership $\langle c, b \rangle \in Cg^S(a, b)$ can be witnessed by a unary polynomial whose complexity is bounded by some integer $N$ that is entirely in terms of $\mathcal{V}$.

**Proof.** Let $V$ and $S$ be as stated above. Let

$$0_S = \zeta_0 \leq \zeta_1 \leq \cdots \leq \zeta_k = 1_S$$

be the upper central series of $S$. Since $S$ belongs to $V$, the nilpotence degree $k$ of $S$ is bounded by the nilpotence degree of $A$. Recall that $\zeta_{i+1}/\zeta_i = \zeta(S/\zeta_i)$ for each $i < k$.

**Claim 1)** For $i > 0$, given $a \neq b$ so that $\langle a, b \rangle \in \zeta_{i+1}$, there is some $c' \neq b$ so that $\langle c', b \rangle \in \zeta_i \cap Cg^S(a, b)$ and the membership $\langle c', b \rangle \in Cg^S(a, b)$ can be witnessed by a unary polynomial based on a commutator word.

Certainly, there exists some $c$ so that $\langle c, b \rangle \in \zeta_i \cap Cg^S(a, b)$. Indeed, since the monolith $\mu$ is contained in both $\zeta_i$ and $Cg^S(a, b)$, we can pick $c$ from $b/\mu$. We know
that there is $c \neq b$ in this congruence class, since nilpotent algebras are congruence uniform. So, if no such $c$ existed, $S$ would be a trivial algebra.

So, $\langle c, b \rangle \in C_\mathbf{g}^S(a, b)$. Therefore, we can pick a unary polynomial and parameters $p(x) = s(x, \bar{d})$ so that either $p(a) = c$ and $p(b) = b$, or the other way around. In the first case, define $r(x, \bar{y}, z) := m(s(x, \bar{y}), s(z, \bar{y}), z)$. In the second case, define $r(x, \bar{y}, z) := m(s(z, \bar{y}), s(x, \bar{y}), z)$. Either way, $r$ now satisfies the following three criteria:

1. $r(a, \bar{d}, b) \zeta_i r(b, \bar{d}, b)$
2. $r(b, \bar{d}, b) = b$
3. $r(a, \bar{d}, b) \neq b$

We claim that (1-3) can be satisfied by a commutator word, also. By 3.2, there exist commutator words $w_1, \ldots, w_m$ with neutral element $z$ so that

$$r(x, \bar{y}, z) \equiv r(z, \ldots, z) + w_1(x, \bar{y}, z) + \cdots + w_m(x, \bar{y}, z)$$

We claim that each $w_j$ satisfies (1) and (2). The latter is clear, since each $w_j$ is a commutator word and therefore satisfies $w_j(z, \bar{y}, z) \equiv z$. For the former, recall that by construction, $\zeta_{i+1}/\zeta_i$ is an Abelian congruence in $S/\zeta_i$. So, we can apply Corollary 3.6 to $\langle a/\zeta_i, b/\zeta_i \rangle \in \zeta_{i+1}/\zeta_i$ and see that for each $j$,

$$w_j(a, \bar{d}, b)/\zeta_i = w_j(a/\zeta_i, \bar{d}/\zeta_i, b/\zeta_i) = b/\zeta_i = w_j(b, \bar{d}, b)/\zeta_i$$

We also claim that there is at least one $w_j$ for which $w_j(a, \bar{d}, b) \neq b$. Suppose not. Then, using $x +_b y$ as shorthand for $m(x, b, y)$,

$$r(a, \bar{d}, b) = r(b, \ldots, b) +_b w_1(a, \bar{d}, b) +_b \cdots +_b w_m(a, \bar{d}, b)$$

$$= r(b, \ldots, b) +_b b +_b b +_b \ldots, +_b b$$

$$= r(b, \ldots, b)$$
But, \( r(b, \ldots, b) = r(b, \bar{d}, b) = b \). So, \( r(a, \bar{d}, b) = b \), contradicting item (3) from above. So, \( w_j \) does indeed satisfy (1-3). Now, we can set \( c' \) to be \( w_j(a, \bar{d}, b) \), and the claim is satisfied.

**Claim 2)** Given \( a \neq b \) so that \( \langle a, b \rangle \in \zeta_1 \), there is some \( c \) so that \( \langle c, b \rangle \) is a critical pair, and the membership condition \( \langle c, b \rangle \in Cg^S(a, b) \) can be witnessed by a unary polynomial built from some binary term.

Let \( \langle a, b \rangle \in \zeta_1 \) as above. Pick some \( c \) so that \( \langle c, b \rangle \) is a critical pair. Similar to the proof in claim 1, choose a unary polynomial \( p(x) = s(x, \bar{d}) \) so that \( p(a) = c \) and \( p(b) = b \). Now, set \( r(u, v, \bar{y}) = m(p(u, \bar{y}), p(v, \bar{y}), v) \). Then, \( r(b, b, \bar{e}) = b \) for any sequence \( \bar{e} \) of parameters (as before, if \( p(b) = c \) and \( p(a) = b \) we can tweak \( r \) slightly to have the same effect). So, since \( \langle a, b \rangle \in \zeta_1 \) and \( \zeta_1 \) is Abelian, Lemma 3.5 applies and \( c = r(a, b, \bar{d}) = r(a, b, \bar{e}) \) for any parameters \( \bar{e} \). So, set \( t(x, y) = r(x, y, y, \ldots, y) \). Then, \( t(a, b) = c \) and \( t(b, b) = b \), so the unary polynomial \( q(x) = t(x, b) \) witnesses the membership condition.

With these two claims, we can prove the theorem. Let \( a \neq b \in S \). Trivially, \( \langle a, b \rangle \in \zeta_k \). Apply claim 1 to obtain \( c_1 \) so that \( \langle c_1, b \rangle \in \zeta_{k-1} \cap Cg^S(a, b) \), as witnessed by a unary polynomial based on a commutator word. Then, iterate claim 1 on \( c_1 \) and its descendants to obtain a sequence \( c_1, \ldots, c_{k-1} \) so that for each \( i \), \( \langle c_i, b \rangle \in \zeta_{k-i} \cap Cg^S(a, b) \), and each of these membership conditions for \( Cg^S(a, b) \) is realised by a unary polynomial \( q_i(x) \) based on a commutator word. None of these commutator words are trivial, so by Theorem 3.3, they all use no more than \( M \) parameters.

Then, apply claim 2 to \( c_{k-1} \) to get \( c \) so that \( \langle c, b \rangle \) is a critical pair, and this membership condition is realised by a unary polynomial \( q_k(x) \) built from a binary term.

The composition of a two unary polynomials is again a unary polynomial, so composing each \( q_i \) together, we now have a unary polynomial \( q(x) \) so that \( q(a) = c \) and \( q(b) = b \), realising the condition \( \langle c, b \rangle \in Cg^S(a, b) \). This polynomial is a composition.
of at most \( k \) many polynomials of complexity no more than \( M \), and one polynomial with complexity 2. Since \( k \) and \( M \) both depend on the variety \( \mathcal{V} \), not on \( S \), this proves the theorem.

Now, we can prove Theorem 3.8.

**Proof.** Let \( N \) be the bound on complexity from Theorem 3.9. Let \( T \) be a set of representative terms from the free algebra in \( \mathcal{V} \) on \( N + 1 \) variables. Let \( \Psi(u, v, x, y) \) be the formula

\[
\exists z_0, \ldots, z_{N-1} \bigvee_{t \in T} (t(x, \bar{z}) \approx u, t(y, \bar{z}) \approx v)
\]

\( \Psi(u, v, x, y) \) is clearly a congruence formula. Now, let \( S \in \mathcal{V}_{si} \) and \( a \neq b \in S \). By Theorem 3.9, there is some \( c \in S \) so that \( \langle c, b \rangle \) is a critical pair and \( \Psi(c, b, a, b) \) holds in \( S \), as desired.

Now, we can tie things up and prove Theorem 3.4, which will in turn imply Theorem 3.1.

**Proof.** Let \( A \) be a finite nilpotent algebra that is a product of algebras of prime power order such that \( \mathcal{V} = \mathcal{V}(A) \) is a congruence permutable variety. Let \( \Psi(u, v, x, y) \) and \( \Phi(u, v, x, y) \) be the congruence formulas defined by Theorems 3.8 and 3.7, respectively. Let \( S \in \mathcal{V}_{si} \), and let \( a, b \in S \) so that \( a \neq b \). Then, by Theorem 3.8, there is a critical pair \( \langle c, d \rangle \) of \( S \) so that \( \Psi(c, d, a, b) \) is satisfied in \( S \). Now, since \( S \) is nilpotent and therefore has a nontrivial center \( \zeta \), its monolith \( \mu \), which is contained in \( \zeta \), must be Abelian. So, by Theorem 3.7, the congruence formula \( \Phi(u, v, c, d) \) defines \( Cg^S(c, d) \). Thus, \( \mathcal{V}_{si} \) has definable principal subcongruences.

Thus, we have proved our main result: that if \( A \) is a finite nilpotent algebra of finite signature that is the product of algebras of prime power order such that \( \mathcal{V} = \mathcal{V}(A) \) is a congruence permutable variety, then \( \mathcal{V}_{si} \) is finitely axiomatisable. This extends the group theorem, as finite nilpotent groups have all of those properties.
Theorem 10.14 in the Commutator Book implies that any variety generated by an algebra that is nilpotent but not Abelian cannot have a finite residual bound. So, in the grander context of things, this dissertation’s result gives us a potentially useful example of a kind of variety $\mathcal{V}$ so that

- $\mathcal{V}$ is finitely based.

- $\mathcal{V}_{si}$ is finitely axiomatisable, but

- $\mathcal{V}$ does not have a finite residual bound.

This could be interesting food for thought in future work on Birkhoff’s speculations regarding the connections between finitely based varieties and finitely axiomatisable subdirectly irredcibles.
Chapter 4

Open Problems

A number of natural extensions of our result beg investigation. Firstly, the hypothesis of Theorem 3.1 that the generating algebra must be a product of algebras of prime power order is somewhat of an irritation. In groups, any finite nilpotent group is the direct product of its Sylow subgroups. So in groups, a nilpotent group is always a product of groups of prime power order.

In algebras in general, however, there is no Sylow theorem guaranteeing the existence of such subalgebras, and so an analogue to this alternative characterisation for nilpotence does not exist. So, there are in fact nilpotent algebras that are not products of algebras of prime power order (such as the example given in Section 1.5). These algebras should be studied to hopefully find an extension of this paper’s main theorem. Perhaps some characterisation of these strange non-groupish nilpotent algebras exists that can help.

Problem 4.1. Let \( \mathcal{V} \) be a congruence permutable variety generated by a finite nilpotent algebra \( A \). Then, is it always true that \( \mathcal{V}_{si} \) is finitely axiomatisable?

This question can be generalised; what hypotheses can nilpotence be replaced by to still preserve the result?

Problem 4.2. Let \( \mathcal{V} \) be a variety generated by a finite algebra \( A \). What properties does \( \mathcal{V} \) need to have in order for \( \mathcal{V}_{si} \) to be finitely axiomatisable?

By Theorem 1.1, we know that if a variety \( \mathcal{V} \) is finitely based and \( \mathcal{V}_{si} \) has definable principal subcongruences, then \( \mathcal{V}_{si} \) is finitely axiomatisable. However, there is not
much available in the literature to tell us when the converse might be true. This begs investigation as well. Probing in this direction would give some insight into the potential validity of one of Jónsson’s speculations.

**Problem 4.3.** Let $\mathcal{V}$ be a variety so that $\mathcal{V}_{si}$ is finitely axiomatisable. What properties does $\mathcal{V}$ need to have so that $\mathcal{V}$ is finitely based?

As we showed in Section 1.4, the hypothesis of $\mathcal{V}_{si}$ being finitely axiomatisable is weaker than the hypothesis of having a finite residual bound. Since that is a hypothesis of many finite basis results in the past few decades, we wonder whether it can be weakened.

**Problem 4.4.** Of the extant finite basis theorems, how many can be strengthened by replacing the hypothesis of a finite residual bound with the hypothesis that $\mathcal{V}_{si}$ be finitely axiomatisable?

The author has done some work towards weakening the hypotheses of one of these finite basis theorems. Progress was not significant enough to reference in the main body of this dissertation, but it is perhaps worthy of discussion as an open problem.

A critical algebra is an algebra that is not contained in the variety generated by its proper factors (that is, the homomorphic images of subalgebras that are not equal to the original algebra). We can refer to a variety having a finite critical bound in the same way as a finite residual bound; that is, $\mathcal{V}$ has a finite critical bound if there is some natural number bounding the cardinalities of all of the critical algebras in $\mathcal{V}$. A critical algebra must be subdirectly irreducible, but the reverse is not necessarily true. So, a finite critical bound is a slightly weaker hypothesis than a finite residual bound.

The proof of the Oates-Powell theorem present in Neumann (1967) uses critical algebras in its formation. In fact, it shows that the variety generated by a finite group has a finite critical bound, and that this, in turn, implies that the group is
finitely based. The author attempted to follow the same reasoning in order to reprove McKenzie’s work in (McKenzie 1987) in slightly more generality. The objective was to answer the following problem:

**Problem 4.5.** If $\mathcal{V}$ is a congruence modular variety with finitely many basic operations and a finite critical bound, then is $\mathcal{V}$ finitely based?

McKenzie’s original proof answered this problem in the affirmative in the presence of a finite residual bound, rather than a finite critical bound. The author discovered that, under the finite critical bound, the first half of McKenzie’s proof still all works out. If $\mathcal{V}$ is a variety, we denote by $\mathcal{V}(n)$ the variety generated by every equation true in $\mathcal{V}$ that uses at most $n$ variables. The punchline of the half-proof in question is that, given the above hypotheses, $\mathcal{V}(n)$ is locally finite for any $n$.

However, the second half of the proof did not hold together. The original proof in McKenzie’s work assumes that $\mathcal{V}$ has a finite residual bound and shows that $\mathcal{V}(n)$ also has finite residual bound for every $n$. However, the author was unable to show that the same applies to a finite critical bound. McKenzie’s proof uses a congruence identity that is equivalent to a finite residual bound. No such identity has been discovered for a finite critical bound. The author attempted to mimic the proof of the Oates-Powell theorem, which used a special subgroup called the Frattini subgroup. This subgroup has an analogue in congruences of algebras, but it did not seem useful in the same way. This avenue of thought may yet bear fruit, however, and the author has not quite given up on it yet.

**Problem 4.6.** If $\mathcal{V}$ is a congruence modular variety with finitely many basic operations and finite critical bound, is it true that $\mathcal{V}(n)$ also has a finite critical bound for any $n$?


