CENTRALITY

A dissertation
submitted for the degree of
Doctor of Philosophy
at the
University of Cambridge
by
Jonathan Dallas Hayden Smith
of
Queens' College
PREFACE

The work in this dissertation has not been submitted for a degree or diploma at any other university, and is to the best of my knowledge and belief original, except where explicit mention is made to the contrary.

I am most grateful to the Science Research Council for financial support, to my supervisor Dr. J. H. Conway and temporary supervisor Dr. R. Dark for mathematical support, and to the late Dr. H. Popova-Alderson for acquainting me with non-associative algebra in the first place.

J. D. H. Smith

May 1974
TABLE OF CONTENTS

Introduction and section-by-section guide

1. Central congruences 3
2. Nilpotence 9
3. The congruence category and direct decompositions 16
4. Centrality and direct decompositions 23
5. Stable isotopy 31
6. Quasigroups and centrality 38
7. Stabilisers in multiplication groups of finite quasigroups 50
8. Further results on multiplication groups 54
References 68
Index 70
In group theory the concept of centrality owes its fundamental importance to two main areas of application: in the classification of groups by properties such as commutativity or nilpotence, and in the theory of direct products. Since both these areas pertain equally to general algebras, it is natural to ask whether a corresponding notion also arises there. The answer has hitherto been negative except for certain algebras having "zeros", namely those whose direct decompositions were studied by Jónsson and Tarski in 1947 [8]. Indeed in 1966 Jónsson [7] wrote (summarizing his extension of the 1947 results to more general structures still possessing "zeros"):

For other structures many of these results are not even meaningful, since they involve concepts that are not defined for such structures, namely the notions of an inner direct product and of center. The inner direct products of subalgebras can be replaced by (weak) direct products of factor relations, but so far no substitute has been offered for the notion of a center.

The purpose of this dissertation is to propose such a substitute and to demonstrate its uses in the two areas mentioned.

1 CENTRAL CONGRUENCES This presental section introduces the basic idea of centrality. For general algebras one must work with congruences rather than subalgebras, because it is those
that describe the effect of morphisms internally. The substitute proposed for the central subalgebra of group theory or of Jónsson-Tarski is thus the central congruence, essentially a congruence admitting a certain kind of congruence on it. The concept is defined, and shown to have desirable properties both for the algebras studied by Jónsson-Tarski and for algebras whose congruences commute. It is no surprise that things work nicely in the Jónsson-Tarski case; one has merely made the switch from subalgebra language to congruence language. The case of algebras with commuting congruences is much more interesting, and it is the application of centrality to the study of such algebras with which the dissertation is primarily concerned.

2 NILPORENOE The first application of centrality is to the classification of algebras by a property known as nilpotence, a direct generalisation of group-theoretic nilpotence. This section sets up the definition of nilpotence, and uses it in the study of non-generators and Frattini subalgebras.

3 THE CONGRUENCE CATEGORY AND DIRECT DECOMPOSITIONS Direct decompositions of algebras not necessarily possessing zeros, like their centrality, must be studied in terms of congruences. The lattices of congruences on algebras whose congruences commute are modular, and so the first theorem on their direct decompositions is the Birkhoff-Ore unique factorisation theorem [2, VII.7 or 13] for modular lattices of finite length. For a deeper study of direct decompositions more elaborate machinery than the lattice of congruences is necessary. Section 3 introduces such machinery:

4 CENTRALITY AND DIRECT DECOMPOSITIONS With the appropriate machinery set up in the previous section, Section 4 applies centrality to produce "non-classical" versions of the theorems on direct decompositions, culminating in the Unique Factorisation Theorem 4.6 which has weaker hypotheses and stronger conclusions than the Classical Unique Factorisation Theorem. This Unique Factorisation Theorem is probably the best available since it generalises directly the best available theorem of group theory, the Krull-Remak-Schmidt Theorem in its latest form.

5 STABLE ISOTOPY In contrast to Sections 3 and 4 which deal with the direct decompositions of a single algebra, this section studies the behaviour of a whole variety of algebras under the direct product. In particular it gives an internal characterisation, involving centrality, of the relationship between two algebras C and D for which there is a third algebra B such that $B \times C \cong B \times D$. For algebras without zeros this relationship is merely isomorphism; for algebras without zeros it is the more interesting relationship of stable isotopy. Section 5 may thus be regarded as the peculiar territory of general algebras with commuting congruences where things get beyond straight generalizations
of group theory. A useful by-product of the considerations of Section 5 is the Structure Theorem 5.5 for algebras in the variety \( \mathfrak{A} \), nilpotent algebra of class 1, which is the analogue of the variety of abelian groups.

The rest of the dissertation is concerned with applications of centrality and the previous sections to the study of quasigroups. These have long been neglected because it has been thought that they do not have sufficient structure to be interesting. If any work has been done on them, it has consisted of adding additional axioms which are perform so unnatural that nothing of any consequence results. In fact the quasigroup axioms as they stand impose subtle limits on the structure which create intriguing problems. The way to tackle them seems to be to study the group of translations acting on a quasigroup as a permutation group. This is begun in the last two sections. Incidentally it may be worth pointing out that the work of the earlier sections on general algebra with commuting congruences arose first in the study of quasigroups. The concept of centrality appeared in terms of newy pseudo-commutative and pseudo-associative laws, vestiges of which remain in the proof of Theorem 7.7.

6 QUASIGROUPS AND CENTRALITY This is a short introductory section giving basic definitions and the connection between stable isotopy and translation groups of quasigroups. In addition brief mention is made of the way two previously published papers on quasigroups and non-associative algebra fit in to the scheme of things.

7 STABILISERS IN MULTIPLICATION GROUPS OF FINITE QUASIGROUPS Beginning the programme of studying quasigroups in relation to their translation groups acting as permutation groups on them, centrality is used to investigate the implications for the algebraic quasigroup-structure of normality and subnormality of point stabilizers in the translation groups. An interesting corollary is the fact that no Hamiltonian groups may be translation groups of quasigroups. This fact, illustrating the subtlety of the quasigroup axioms, raises the problem of determining precisely what groups can or cannot be translation groups of quasigroups.

8 FURTHER RESULTS ON MULTIPLICATION GROUPS This final section looks at the connection between centrality of quasigroups and normality properties of their translation groups. Its results, which can only be regarded as a first brief glance at the subject, are used to begin the classification of quasigroups of prime order by applying a theorem of Galois. Solubility of the translation group of a quasigroup of prime order is shown to correspond exactly with the quasigroup being in the class \( \mathfrak{A} \). The search for further such connections between algebraic properties of quasigroups and the nature of their translation groups may well prove very fruitful for quasigroup theory and for the theory of permutation groups.
A knowledge of such basics of universal algebra and group theory as may be found in [2] and [6] is assumed throughout. Acquaintance with some non-associative algebra as in [4] would also be useful.

1. CENTRAL CONGRUENCES

The following universal-algebra notations are used throughout. Let $\Omega$ be a given variety of algebra, with operator domain $\Omega$. If $V$ is a congruence relation on a $\Omega$-algebra $A$, then $V$ is an equivalence relation which is also a subalgebra of the direct square $A \times A$ of $A$. At times it will be convenient to write $a \sim b$ rather than $(a,b) \in V$, for elements $a, b \in A$.

If $a \in A$, let $a^V = \{ b \in A | (a,b) \in V \}$, let $A^V$ be the $\Omega$-algebra formed by the set of all these equivalence classes, and let $\pi_V : A \rightarrow A^V$ be the natural projection. Let $A$ denote the image of the diagonal embedding $A : A \rightarrow A \times A ; a \mapsto (a,a)$. The basic concept of centrality is introduced in this section by consideration of the embedding $A : A \rightarrow V$ of the diagonal in a congruence.

1.1 DEFINITIONS If $V$ is a congruence on a $\Omega$-algebra $A$, then a congruence $\overline{V}$ on the $\Omega$-algebra $V$ is said to respect equivalence of $V$ iff the three conditions (RR), (RS), and (RT) are satisfied:

- $(RR)$ $\forall a, b \in A, (a,a) \overline{V} (b,b)$;
- $(RS)$ $\forall (v_1,v_2), (v_1,v_3) \in V, (v_1,v_2) \overline{V} (v_1,v_3)$;
- $(RT)$ $\forall (v_1,v_2), (v_2,v_3), (v_1,v_4), (v_2,v_5) \in V, (v_1,v_2) \overline{V} (v_3,v_4)$ and $(v_2,v_3) \overline{V} (v_5,v_6) \Rightarrow (v_4,v_5) \overline{V} (v_6,v_7)$.

These conditions are called respect of reflexivity, symmetry, and transitivity.
Let $x_A : A \times A \to A$ be the projection onto the $i$-th factor ($i = 1, 2$). If there is a congruence $\mathcal{V}$ on a congruence $\mathcal{W}$ on $A$ such that the two conditions
\[(C1) \quad (v_1, v'_2) \in \mathcal{V}, \quad x_A : (v_1, v'_2) \mathcal{V} \to A \text{ bijects and}
\]
\[(C2) \quad \mathcal{V} \text{ respects equivalence of } \mathcal{W}
\]
are satisfied, then $\mathcal{V}$ is said to centre $\mathcal{W}$ and $\mathcal{V}$ is called a central congruence on $A$.

**1.2 Proposition** If $\mathcal{V}$ is centred by $\mathcal{W}$, then the universal congruence $\mathcal{U}^V \times \mathcal{U}^V$ is central.

**Proof.** Define a relation $\mathcal{W}$ on $\mathcal{U}^V \times \mathcal{U}^V$ by
\[
((v_1, v_2), (v'_1, v'_2)) \mathcal{W} = ((v_1, v_2)'V, (v'_1, v'_2)'V) \iff (v_1, v'_2) \mathcal{V} \iff (v_1, v'_2)'V.
\]
It follows straightforwardly from the properties of $\mathcal{V}$ that $\mathcal{W}$ is a well-defined equivalence-respecting congruence on $\mathcal{U}^V \times \mathcal{U}^V$, and it only remains to verify (C1) for $\mathcal{W}$ in order to show that it centres $\mathcal{U}^V \times \mathcal{U}^V$.

Suppose that $((v_1, v_2), (v'_1, v'_2), (v_1, v'_2)) \in \mathcal{V}$.

By property (C1) of $\mathcal{V}$, with $v = (v_2, v'v) \in A$ and $(v_2, v') \mathcal{V} (v_2, v')$, by transitivity of $\mathcal{V}$, $(v_2, v') \mathcal{V} (v_2, v')$.

Then $((w_1, w_2), (v_1, v'_2)) \mathcal{V} (v_1, v'_2)'V$ surjects.

If $((w_1, w_2), (v_1, v'_2)) \mathcal{V} (v_1, v'_2)'V$ and $(w_1, w_2) \mathcal{V} (v_1, v'_2)'V$, then since $(v_2, v') \mathcal{V} (v_2, v')$ by definition of $\mathcal{V}$, it follows that $(w_1, w_2) \mathcal{V} (v_1, v'_2)'V$.

Hence $x_A$ injects, and (C1) for $\mathcal{V}$ is verified.

Besides its $\mathcal{R}$-algebra structure, $\mathcal{W}$ has an additional operation $+$ given by $(w_1, w_2) + (v_1, v'_2) = (w_1, w'_2) + (v_1, v'_2)$. Proposition (C1) and (C2) of $\mathcal{W}$ imply that $+$ is well-defined, and also that $(\mathcal{W}^V, +)$ is a quasigroup. But $+$ is clearly associative, and so $(\mathcal{W}^V, +)$ is a group, with $\mathcal{V}$ as its identity.

**1.3 Definition** A variety $\mathcal{V}$ of algebras is said to be rectifiable iff for each central congruence $\mathcal{V}$ on each $\mathcal{R}$-algebra $A$, the group $(\mathcal{W}^V, +)$ is abelian.

Rectifiability is an obscure property somehow connected with the good behaviour of direct decompositions. This section will do no more than give two sufficient conditions for rectifiability and an example of non-rectifiability. It is not yet known whether there are any other rectifiable varieties or useful necessary and sufficient conditions.

**1.4 Example** Suppose that $\mathcal{V}$ is empty, so that $\mathcal{R}$-algebras are just sets, and congruences on them are just equivalence relations. Let $(G, .)$ be a non-abelian group. Let $V = G \times G$, and let $\mathcal{W}$ be the equivalence relation on $V$ whose classes are just the right cosets of the subgroup $(G, .)$ of $(G \times G, .)$. Then $\mathcal{V}$ centres $\mathcal{W}$, and $(\mathcal{W}^V, +) \cong (G, .)$. Thus sets are not rectifiable.

In [8] algebras $A$ are considered having a nullary operation $\eta$ and a derived binary operation $*$ such that $\{ \eta \}$ forms a singleton subalgebra and $\forall a \in A$, $a * \eta = a = \eta * a$ is an identity. Such algebras will be referred to as *Higman-Tarski algebras*. 
1.5 PROPOSITION Varieties of Jónsson-Tarski algebras are rectifiable.

Proof. Let \( V \) centre \( V \) on a Jónsson-Tarski algebra \( A \).

Any \( V \)-class has a unique expression as \( (\gamma, x) \mathcal{V} \) for some \( x \in A \).

Then
\[
(\gamma, x) \mathcal{V} + (\gamma, y) \mathcal{V} = (\gamma, x) \mathcal{V} + (\gamma, x'y) \mathcal{V} = (\gamma, x \cdot y) \mathcal{V} = (\gamma, x) \mathcal{V} + (\gamma, y) \mathcal{V}.
\]

Thus \( (\mathcal{V}^{+}, +) = (\mathcal{V}^{*}, \ast) \). How the congruence \( \mathcal{V} \) is produced for the proof of Proposition 1.2 centers the universal congruence on \( (\mathcal{V}^{+}, +) \). Since \( (\mathcal{V}^{+} +, +) = (\mathcal{V}^{*}, \ast) \), \( \mathcal{V} \) defines a central congruence on \( (\mathcal{V}^{+}, +) \). It follows [6, Satz 1.9.14] that \( (\mathcal{V}^{+}, +) \) is abelian.

For Jónsson-Tarski algebras, central congruences \( V \) are precisely the unique minimal congruences having a central subalgebra [8, Definition 2.1] as equivalence class \( \gamma \mathcal{V} \). Since Jónsson-Tarski algebras \( A \) have a unique maximal central subalgebra [8, Theorem 2.11], they also have a unique maximal central congruence called the central congruence \( \mathcal{C}(A) \).

In addition to the Jónsson-Tarski algebras there is another important group of rectifiable algebras, these, to be referred to as Mal'cev algebras, resemble various algebras all of whose congruences commute.

1.6 PROPOSITION Varieties of Mal'cev algebras are rectifiable.

Proof. Mal'cev showed [10] that all congruences on algebras \( A \) of a variety \( \mathcal{V} \) commute if there is a derived operation \( P \) such that \( \mathcal{V}(a, b, c) = P(b, c, a) \) is an identity. Let \( \mathcal{V} \) centre \( V \) on a Mal'cev algebra \( A \). Define a derived operation \( \ast \) on \( \mathcal{V}(A) \) by \( (a, b) \mathcal{V} \ast (c, d) \mathcal{V} = P((a, b) \mathcal{V}, (c, d) \mathcal{V}) \).

For any \( (a, b), (c, d) \in V \). Then
\[
(\mathcal{V}(a, b) \mathcal{V} + (c, d) \mathcal{V}) = P(\mathcal{V}(a, b) \mathcal{V}, (c, d) \mathcal{V}) \mathcal{V} = (\mathcal{V}(a, b) \mathcal{V} + (c, d) \mathcal{V}).
\]

Thus \( (\mathcal{V}^{+}, +) = (\mathcal{V}^{*}, \ast) \), and so by the same reasoning as in the proof of Proposition 1.5, \( (\mathcal{V}^{+}, +) \) is abelian.

Before the publication of Mal'cev's result, Goldie [5] studied direct decompositions of Mal'cev algebras \( A \) having singleton subalgebras \( \{ \eta \} \). However, definition of the derived operation \( \ast \) of \( A \) by \( a \ast b = P(a, b, 0) \) reduces such algebras to the Jónsson-Tarski case. In the general Mal'cev case the absence of singleton subalgebras prevents such a reduction, but it is nevertheless possible to obtain results analogous to those of Jónsson-Tarski. Section 4 contains theorems on direct decompositions of Mal'cev algebras similar to those for Jónsson-Tarski algebras in [8], while the rest of this section is devoted to demonstrating that Mal'cev algebras also have a unique maximal central congruence.

Let \( A \) be a Mal'cev algebra, \( 0 \) an element of \( A \), and define a derived operation \( + \) on \( A \) by \( a + b = P(a, 0, b) \) for all \( a, b \in A \). As has been seen, there is no inconsistency in the use of the same symbol + as that for the binary operation of \( (\mathcal{V}^{+} +) \).

1.7 PROPOSITION (i) If \( \mathcal{V} \) centres \( \mathcal{V} \), then \( (0, +) \mathcal{V} \) is an abelian group isomorphic to \( (\mathcal{V}^{+}, +) \).

(ii) If \( x, x' \in A \), \( c, c' \in 0 \mathcal{V} \), then
\[
(x + c) + (x' + c') = (x + c') + (x' + c')
\]

Proof. (i) The map \( (0, +) \mathcal{V} \rightarrow (\mathcal{V}^{+}, +) \); \( c \mapsto (0, c) \mathcal{V} \) yields the isomorphism.

(ii) \( (x, x + c) \mathcal{V} (0, c) \mathcal{V} \) and \( (x', x' + c') \mathcal{V} (0, c') \mathcal{V} \) imply
\[
(x + x'), (x + c)(x' + c') \mathcal{V} (0, c + c').
\]
1.0 PROPOSITION Suppose $V_1$, $V_2$ respectively centre congruences $V_1$, $V_2$ on $A$. Then $V_1$ and $V_2$ agree on $V_1 \cap V_2$.

Proof. Let $x \in A$, $(0,c) \in V_1 \cap V_2$. Then $(0,0) V_1 (x,x)$ and $(0,0) V_2 (0,0) \Rightarrow (0,0) V_1 (x,x+c)$, $(0,0) V_2 (x,x) \Rightarrow (0,0) V_2 (x,x+c)$.

1.10 THEOREM If $A$ is a Mal'cev algebra, then $A$ has a unique maximal central congruence, called the central congruence $\xi(A)$.

Proof. The set of central congruences on $A$ is partially ordered by inclusion. Zorn's Lemma yields the existence of maximal central congruences, and Proposition 1.9 gives the uniqueness.
2. NILPOTENCE

The centre congruence \( \xi(A) \) of a Mal'cev algebra \( A \) plays a role analogous to that of the centre of a group. Its use in the theory of direct decompositions will become apparent later, but this section shows its use in defining certain subvarieties of a variety \( T \) of Mal'cev algebra, namely the nilpotent algebras of specified class. A similar procedure is possible for Jónsson-Tarski algebras (although there are detail differences such as the use of normal subalgebras instead of congruences) and Bruck [4] has already treated the case of loops.

2.1 DEFINITION If \( B \) is a subalgebra of an algebra \( A \), write \( B \subseteq A \). \( B \) is said to be a normal subalgebra of \( A \), written \( B \triangleleft A \), if there is a congruence \( \sim \) on \( A \) such that \( B \) is an equivalence class of \( \sim \). A nat \( V \) will then be denoted by \( A/B \), the congruence \( V \) being implicit in the context.

2.2 PROPOSITION \( A \subseteq V \subseteq A \times A \) if \( V \) is a congruence on \( A \).

Proof. It is sufficient to show that \( A \subseteq V \subseteq A \times A \) implies that \( V \) is an equivalence relation. Since \( A \subseteq V \), \( V \) is reflexive. Suppose \( (x,y) \in V \). Now \( (x,z), (y,z) \in V \). Hence \( (y,z) = \langle P(x,x,y), P(x,y,z) \rangle \in \langle P(V,V,V) \rangle \subseteq V \) : \( V \) is symmetric. Suppose also \( (y,z) \in V \). Then \( (x,y), (y,z), (y,z) \in V \). Thus \( (x,z) = \langle P(x,y,y), P(y,y,z) \rangle \in V \) : \( V \) is transitive. \]

2.3 PROPOSITION A congruence \( V \) on \( A \) is central iff \( \bar{V} < V \).

Proof. If \( V \) is central by \( \bar{V} \), then properties (RR) and (C1) imply that \( \bar{V} = (x,x)^{\bar{V}} \) for any \( x \in A \).

Conversely, suppose that \( \bar{V} \) is an equivalence class of a congruence \( V \) on \( V \). The various conditions of Definition 1.1 must be verified.

(RR): Suppose \( (v_1,v_2) \in V \) and \( (v_1,v_2) \notin (v_1,v_2) \).

Now \( (v_1,v_1) \notin (v_1,v_1) \) by (RR),

\[ (v_1,v_2)^{\bar{V}} = (v_1,v_2) \]

is given, and \( (v_2,v_2)^{\bar{V}} = (v_2,v_2) \) by (RR).

Hence \( (P(v_1,v_1),P(v_1,v_2),P(v_1,v_2)) \notin (P(v_1,v_1),P(v_1,v_2),P(v_1,v_2)) \), i.e. \( (v_2,v_1) \notin (w_2,w_1) \). Thus \( V \) respects symmetry of \( V \).

(RT): Suppose also \( (v_2,v_3), (w_2,w_3) \in V \) and \( (v_2,v_3), (w_2,w_3) \).

Then \( (v_1,v_2) \notin (v_1,v_2) \),

\[ (v_1,v_2)^{\bar{V}} = (v_1,v_2) \]

and \( (v_2,v_2)^{\bar{V}} = (v_2,v_2) \).

Hence \( (P(v_1,v_2),P(v_1,v_3),P(v_1,v_3)) \notin (P(v_1,v_2),P(v_1,v_3),P(v_1,v_3)) \), i.e. \( (v_1,v_2) \notin (w_1,w_2) \). Thus \( V \) respects transitivity of \( V \).

(C1) is verified similarly. Suppose \( (x,y) \in V \), and \( z \in A \).

Then \( (x,z) \notin (x,z) \), and \( (x,z) \notin (x,z) \) since \( V \) is reflexive, while \( (x,y) \notin (z,y) \) by (RR).

Hence \( (P(x,x,y),P(y,x,y),P(y,x,y)) \notin (P(x,x,y),P(y,x,y),P(y,x,y)) \), i.e. \( (x,y) \notin (z,y) \), so that \( \bar{V} = (x,y)^{\bar{V}} \rightarrow A \) surjects.

Suppose \( (z',z') \notin (z',z') \).

Then \( (z,z') \notin (z,z') \), and \( (z',z') \notin (z',z') \) by (RR).

Hence \( (P(z,z,z'),P(z',z),P(z',z')) \notin (P(z,z,z'),P(z',z),P(z',z')) \), i.e. \( (z',z') \notin (z',z') \). So \( (z',z') \notin (z',z') \) for any \( z',z' \) in \( (z',z')^{\bar{V}} = \bar{V} \), i.e. \( z' = z' \).

Thus \( \bar{V} : (x,y)^{\bar{V}} \rightarrow A \) injects. \]
2.4 PROPOSITION (1) If $B \leq A$, then $(B,B) \triangleleft \xi(A) \leq \xi(B)$.

(ii) If $e: A \rightarrow A_0$ is an epimorphism, then $\xi(A)(e,e) \leq \xi(Ae)$.

(iii) If $V$ is a congruence on $A$, define the commutator $[V,A]$ to be the intersection of all congruences $K$ on $A$ such that $(V \cdot X)(\text{mat}_K,\text{mat}_K) \leq \xi(A \text{ mat}_K)$. Then $(V \cdot [V,A])(\text{mat}_A,\text{mat}_A) = \xi(A \text{ mat}_V)$. 

Proof. Let $\bar{V}$ centre $\xi(A)$.

(i) The restriction $\bar{V}|((B,B)\triangleleft \xi(A)) \times ((B,B)\triangleleft \xi(A))$ centres $(B,B)\triangleleft \xi(A)$.

(ii) $\bar{V}|((e,e),(e,e))$ centres $\xi(A)(e,e)$.

(iii) Let $S$ be the set of all congruences $K$ on $A$ such that $(V \cdot X)(\text{mat}_K,\text{mat}_K) < \xi(A \text{ mat}_K)$. If $K \in S$, let $\bar{V}_k$ centre $(V \cdot X)(\text{mat}_K,\text{mat}_K)$. Let $(x_1,y_1), (x_2,y_2)$ be in $V \cdot [V,A]$.

Define $\bar{V}$ on $(V \cdot [V,A])(\text{mat}_A,\text{mat}_A)$ by

$$(x_1 \text{ mat}_V, y_1 \text{ mat}_V) \bar{V} (x_2 \text{ mat}_V, y_2 \text{ mat}_V)$$

for $V \cdot X \in S$, $(x_1 \text{ mat}_K, y_1 \text{ mat}_K) \bar{V}_k (x_2 \text{ mat}_K, y_2 \text{ mat}_K)$.

It is easily checked that $\bar{V}$ is a well-defined congruence on $(V \cdot [V,A])(\text{mat}_V,\text{mat}_V)$ with $\bar{V} \leq \xi(A \text{ mat}_V)$ as an equivalence class. The result then follows by Proposition 2.3.]

A central series in a Mal'cev algebra $A$ is a series

$A = V_0 < V_1 < \ldots < V_n = A x A$ such that $V_i \text{ mat}_{V_{i-1}} \leq \xi(A \text{ mat}_{V_{i-1}})$ for $i = 1, \ldots, n$.

Writing $A_0 = A x A$, $\xi(A) = \bar{A}$, define

$A_{i+1} = [A_i,A]$ and $\xi_{i+1}(A)$ (or more briefly $\xi_{i+1}$) by

$$\xi_{i+1} \triangleleft \text{mat}_{A_{i+1}} = \xi(A \text{ mat}_{A_{i+1}})$$

inductively. If $A_j \leq \xi_1$, then $(A_j,\xi_{i-1} \triangleleft \text{mat}_{A_{i-1}}) \leq \xi_{i-1} \triangleleft \text{mat}_{A_{i-1}} = \xi(A \text{ mat}_{A_{i-1}})$, so $\xi_{i+1} \triangleleft [A_j,A] = A_{j+1}$.

Also $(A_j,\xi_{i+1}) \triangleleft \text{mat}_{A_{i+1}} = \xi(A \text{ mat}_{A_{i+1}}) = \xi_{i+1} \triangleleft \text{mat}_{A_{i+1}}$, so $A_{j+1} \leq \xi_{i+1}$.

Thus $A_0 \leq \xi_0$ iff $A_0 \leq \xi_0$. If $A$ satisfies these conditions,

$c$ being the least such integer for which it does, then $A$ is said to be nilpotent of class $c$. $A_1$ is called the lower central series and $\xi_1$ the upper central series. The variety of all $\mathbb{Z}$-algebras of class at most $c$ will be denoted by $\mathcal{F}_c(\mathbb{Z})$ or just $\mathcal{F}_c$. The class of all nilpotent $\mathbb{Z}$-algebras, of unspecified (nilpotency) class, will be denoted by $\mathcal{F}$. The symbol $\mathbb{Z}$ will be used instead of $\mathbb{Z}_c$. For example, if $\mathbb{F}$ is the variety of groups, loops, Lie algebras, then $\mathcal{F}(\mathbb{Z})$ is the variety of abelian groups, abelian loops, abelian Lie algebras respectively.

2.5 PROPOSITION A variety $\mathcal{Y}$ of $\mathbb{Z}$-algebras is a subvariety of $\mathcal{F}(\mathbb{Z})$ iff every subalgebra $B$ of every $\mathbb{Z}$-algebra $A$ is normal in $A$.

Proof. Suppose the latter condition is satisfied. If $A$ is a $\mathbb{Z}$-algebra, so is $A \times A$. Then the subalgebra $2$ of $A \times A$ is normal. Proposition 2.3 then implies that $A \times A$ is a central congruence, so that $A \in \mathcal{F}(\mathbb{Z})$.

Conversely, if $B$ is a subalgebra of a $\mathcal{F}(\mathbb{Z})$-algebra $A$, and $A \times A$ is centred by $\mathcal{Y}$, then by Proposition 2.2,

$(B \times B) \text{ mat}_\mathcal{Y} = U \{ (b_1,b_2) \mid b_1, b_2 \in B \}$ is a congruence on $A$.

If $(b,x) \in (B \times B) \text{ mat}_\mathcal{Y}$, then $(b,x) \bar{Y} (b_1,b_2)$ for some $b_1, b_2 \in B$, so that $x = P(b,b_1,b_2) \in B$. Clearly also $B \times B \subseteq (B \times B) \text{ mat}_\mathcal{Y}$. Thus $B$ is an equivalence class of $(B \times B) \text{ mat}_\mathcal{Y}$, i.e. $B \leq A$.}
The subvariety \( \bar{\mathcal{V}}(\mathcal{V}) \) of a variety \( \mathcal{V} \) of Mal'cev algebras is an extremely useful object which will reappear continually. In the last part of this section, however, it is the broader concept of nilpotence which is applied to a study of non-generators and Frattini subalgebras of Mal'cev algebras. This generalizes long-standing results of group theory and Bruck's work \([3,4]\) on loops, although relaxation of the demand for singleton subalgebras introduces the new and rather awkward possibility that the maximal subalgebras of an algebra do not intersect.

2.6 DEFINITION If \( \emptyset \not\subseteq S \subseteq A \), let \( \langle S \rangle \) denote the least subalgebra of \( A \) containing \( S \). Then an element \( x \) of \( A \) is said to be a non-generator of \( A \) iff \( \langle x, S \rangle = A \) for any \( \emptyset \not\subseteq S \subseteq A \) implies \( \langle S \rangle = A \).

2.7 EXAMPLE Consider the quasigroup of order three in which every element is idempotent, i.e. with this multiplication table:

<table>
<thead>
<tr>
<th>( \emptyset )</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

Every pair of elements of \( Q \) generates \( Q \), but no singleton does. Thus \( Q \) has no non-generators. Note also that the maximal subquasigroups \( \{1\}, \{2\}, \{3\} \) do not intersect.

(For those unfamiliar with quasigroups, the relevant facts may be found at the beginning of Section 6.)

2.8 PROPOSITION The set of non-generators of an algebra \( A \), if non-empty, forms a subalgebra \( \mathfrak{g}(A) \) of \( A \) called the Frattini subalgebra. If \( A \) has no maximal (proper) subalgebra, then \( \mathfrak{g}(A) = A \). Otherwise \( \mathfrak{g}(A) \) is the intersection of all the maximal subalgebras.

Proof. Let \( \emptyset \) be an \( n \)-ary operation of \( A \), and let \( \emptyset \not\subseteq S \subseteq A \), \( x_1, \ldots, x_n, S \in \mathfrak{g}(A) \). Then \( \langle x_1, \ldots, x_n, S \rangle = A \Rightarrow \langle x_1, \ldots, x_n, S \rangle = A \Rightarrow \ldots \Rightarrow \langle x_n, S \rangle = A \Rightarrow \langle S \rangle = A \). Thus \( \mathfrak{g}(A) \) is a subalgebra of \( A \).

Now let \( x \in A \). If there is a maximal subalgebra \( M \) not containing \( x \), then \( x, M > = A \) but \( M > = H < A \). Thus \( x \) is not a non-generator. So each non-generator is contained in the intersection of all maximal subalgebras.

Conversely, suppose element \( x \) of \( A \) is contained in all maximal subalgebras. Let \( x, S > = A \) for \( \emptyset \not\subseteq S \subseteq A \).

If \( \emptyset \not\subseteq S \subseteq A \), \( x \not\subseteq S \). Using Zorn's Lemma, choose subalgebra \( M > = S \) maximal with respect to the requirement \( x \not\subseteq M \). Now \( x, M > = x, S > = A \); by choice of \( M \) any subalgebra properly containing \( M \) must contain \( x \) as well, and so all of \( A \). Thus \( M \) is a maximal subalgebra not containing \( x \). But \( x \) is in all maximal subalgebras. So \( \langle S \rangle = A \), and \( x \) is a non-generator.

2.9 PROPOSITION If \( M \) is a subalgebra of \( A \), and \( M \) nat(\( A \)) = \( A \) (i.e. every element of \( A \) is in the \( * \)-class of some element of \( M \)), then \( M < A \) and \( A/M \in \bar{\mathcal{V}}(\mathcal{V}) \).

Proof. Suppose \( \emptyset \) centres \( \mathcal{V} \). Now \( M \) nat(\( A \)), so if \( g \in A \), then \( j = g \in M \), \( (g, e) \in \mathcal{V} \).
Define a relation \( \mu \) on \( A \) by \( (e_1, e_2) \in \mu \iff \nexists a_1, a_2 \in M: (e_1, a_1), (e_2, a_2) \in \zeta \) and \( (e_1, a_1) \not\in (e_2, a_2) \).

It follows immediately from Proposition 2.2 that \( \mu \) is a congruence on \( A \). If \( a_1, a_2 \in H \), then \((a_1, a_1), (a_2, a_2) \in \zeta \) and \((a_1, a_1) \not\in (a_2, a_2) \) by \((HK)\), so that \( a_1 \mu a_2 \).

Conversely, suppose \( x \mu y \in K \), say with \((x, x_1) \not\in (y, y_2) \).

Then \( x = \frac{P_{12}m_1, m_2} \in H \). Thus \( K \) is an equivalence class of \( \mu \).

Since \( H \text{nat}_{\zeta} = A \), \( \mu \cdot \zeta = A \cdot A \). Thus \( \zeta \text{nat}(\text{nat}_{\zeta}, \text{nat}_{\mu}) = A/H \times A/H \).

But by Proposition 2.4(ii), \( \zeta \text{nat}(\text{nat}_{\zeta}, \text{nat}_{\mu}) \subseteq \zeta(L/H) \). Thus \( A/H \in \frac{E}{E} \). ]

2.10 THEOREM If \( A \) is nilpotent and has non-generators, then \( \phi(A) \subseteq A \) and \( A/\phi(A) \in \frac{E}{E} \).

Proof. Suppose \( A \in \frac{E}{E} \). Then \( \text{nat}_{\zeta}(A) = A \cdot A \). Let \( M \) be a maximal subalgebra of \( A \). Then \( H \text{nat}_{\zeta}(A) = A \).

Let \( n \) be minimal with respect to the requirement \( H \text{nat}_{\zeta}^n(A) = \emptyset \).

Note that \( n > 0 \), since \( H \text{nat}_{\zeta}^0 = A \).

Also \( 1 < n \Rightarrow H \text{nat}_{\zeta}^n(A) \not\subseteq A \), since \( H \text{nat}_{\zeta}^n(A) \not\subseteq A \).

Now \((H \text{nat}_{\zeta}^n(A)) \text{nat}(\text{nat}_{\zeta}^{n-1}, \text{nat}_{\zeta}^{n-1}) = A \text{ nat}_{\zeta}^{n-1} \).

Thus by Proposition 2.9, \( H \text{ nat}_{\zeta}^{n-1} < \text{ nat}_{\zeta}^{n-1} \) and \( (A \text{ nat}_{\zeta}^{n-1})/(H \text{ nat}_{\zeta}^{n-1}) \in \frac{E}{E} \). Hence \( H \vartriangleleft A \) and \( A/H \in \frac{E}{E} \).

Then by Proposition 2.8, \( \phi(A) \vartriangleleft A \) and \( A/\phi(A) \in \frac{E}{E} \). ]

3. THE CONGRUENCE CATEGORY AND DIRECT DECOMPOSITIONS

One of the main applications of the concept of centrality is to the study of direct decompositions of Mal'cev algebras. In the possible absence of singleton subalgebras such decompositions have to be studied in terms of congruences rather than subalgebras. The correct setting for this is the category of congruences on a Mal'cev algebra, a strengthening of the lattice of congruences.

Now the lattice of congruences on a Mal'cev algebra is modular [2, VII.3, Theorem 4], and so one may apply the Birkhoff-Ore Theorem [2, VII.7 or 13] on direct decompositions in modular lattices of finite length to get a "Classical" Unique Factorisation Theorem on direct decompositions of Mal'cev algebras satisfying certain finiteness conditions (viz. maximal and minimal conditions on chains of congruences). For groups with operators (which are Mal'cev algebras) this Classical Unique Factorisation Theorem is none other than the Krull-Remak-Schmidt Theorem [6, Sats 1.12,3].

The usual group-theoretic proof of the Krull-Remak-Schmidt Theorem involves the use of Fitting's Lemma [6, Sats 1.1.0,6], and differs from the lattice-theoretic proof of the Birkhoff-Ore Theorem. The purpose of the current section is to introduce the category of congruences on a Mal'cev algebra, and to show how it may be used to prove the Classical Unique Factorisation Theorem for a Mal'cev algebra by the Fitting's Lemma techniques used for the Krull-Remak-Schmidt Theorem in group theory. Centrality does not appear at all here: it is held over until Section 4 ready to weaken the hypotheses and strengthen the conclusion of the Unique Factorisation Theorem.
The category of congruences \( \mathcal{G}(A) \) on an algebra \( A \) in a variety \( \mathcal{V} \) of Mal'tsev algebras has the congruences on \( A \) as objects, and if \( U \) and \( V \) are two such, a morphism of congruences (or "\( \equiv \)-morphism") \( \varphi : U \to V \) is a \( \mathcal{V} \)-algebra morphism such that

(i) \( \Delta \varphi = \Delta : U \to V \) and

(ii) \( \varphi_1 = \pi_U \), i.e. such that this diagram commutes:

\[
\begin{array}{ccc}
U & \xrightarrow{\varphi} & V \\
\downarrow \varphi_1 & & \downarrow \pi_V \\
A & & A
\end{array}
\]

The kernel \( \text{Ker}_\varphi \) of \( \varphi \) is defined to be the congruence \( \{(x,y) \in U \mid (x,y)\varphi = (x,x)\} \), the embedding \( \text{Ker}_\varphi \to U \) having the usual universality property for kernels [9]. Note that the image \( U\varphi \) of \( \varphi \) is also a congruence. (Proposition 2.2 verifies that the kernel and image are congruences.) The lattice of congruences on \( A \) is a subcategory of the category \( \mathcal{G}(A) \).

If \( \alpha \), \( \beta \), \( \gamma \) are congruences on \( A \), \( \alpha \) is said to be the direct product \( \beta \times \gamma \) of \( \beta \) and \( \gamma \) iff \( \alpha = \beta \times \gamma \) and \( \beta \cap \gamma = \hat{\Lambda} \). Since \( A \) is a Mal'tsev algebra the partial operation \( \alpha \) on \( \mathcal{G}(A) \) is associative. If \( \alpha = \beta \times \gamma \) there is a \( \equiv \)-morphism \( \phi : \alpha \to \beta \times \gamma = (x,y) \mapsto (x,z) \), where if \( (x,y) \in \alpha = \beta \times \gamma \), \( x \beta \gamma y \), \( x \) being uniquely defined since \( \beta \cap \gamma = \hat{\Lambda} \).

If \( \hat{\alpha} \leq \hat{\delta} \leq \alpha = \beta \times \gamma \), the congruence \( \delta \phi \) will be written as \( \beta \delta \), the projection of \( \delta \) onto \( \beta \) along \( \gamma \). If \( \gamma \) is implicit in the context, it will be suppressed as a suffix in \( \beta \delta \).

Note that \( \delta \leq \beta \delta \leq \gamma \delta \).

3.1 FITTING'S LEMMA If \( \varphi : U \to U \) is an endomorphism of congruences, and \( U \) has both the maximal and minimal conditions on subcongruences, then there is a positive integer \( n \) such that \( U = U^n \cap \text{Ker}_\varphi^n \).

Proof. \( U \triangleright U \triangleright U^n \triangleright \ldots \) and \( \text{Ker}_\varphi \leq \text{Ker}_\varphi^2 \leq \text{Ker}_\varphi^3 \leq \ldots \).

The maximal and minimal conditions yield the existence of a positive integer \( n \) such that \( U^n = U^{n+1} \) and \( \text{Ker}_\varphi^n = \text{Ker}_\varphi^{n+1} \). Suppose \( (x,y) \) \( \in U^n \cap \text{Ker}_\varphi^n \). Then \( (x,y)\varphi^n = (x,x) \) and also \( (x,z) \in U , (x,z)\varphi^n = (x,y) \).

\[ \Rightarrow (x,z)\varphi^{2n} = (x,y)\varphi^n = (x,z) \Rightarrow (x,z) \in \text{Ker}_\varphi^{2n} = \text{Ker}_\varphi^n \]

\[ \Rightarrow (x,z)\varphi^n = (x,y) = (x,x) \] Hence \( U^n \cap \text{Ker}_\varphi^n = \hat{\Lambda} \).

Let \( (x,y) \in U \). Let \( (x,z) = (x,y)\varphi^n \in U^n \cap \text{Ker}_\varphi^n \).

Then \( (x,z) \in U \). \( (x,z) = (x,y)\varphi^n \). Let \( (x,z)\varphi^n = (x,t) \).

Then \( (x,z)\varphi^n = (x,x) \)

\( (x,t)\varphi^n = (x,z) \)

\( (x,y)\varphi^n = (x,z) \)

\[ \Rightarrow (x,P(x,t,y))\varphi^n = (x,t) \] Thus \( (x,P(x,t,y)) \in U^n \).

Also \( (x,s)\varphi^n = (x,t) \)

\( (t,t)\varphi^n = (t,t) \)

\( (y,y)\varphi^n = (y,y) \)

\[ \Rightarrow (P(x,t,y),P(s,t,y))\varphi^n = (P(x,t,y),y) \] Thus \( (P(x,t,y),y) \in U^n \). Let \( x \in \text{Ker}_\varphi P(x,t,y) U^n \).

Hence \( U = \text{Ker}_\varphi^n \cap U^n \).

3.2 PROPOSITION Under the hypotheses of Fitting's Lemma 3.1, if \( U = U \), then \( \varphi \) is an automorphism of congruences.

Proof. \( U = U \triangleright U = U^n \) for all positive integers \( n \).

Thus by Fitting's Lemma 3.1, \( \text{Ker}_\varphi^n = \hat{\Lambda} \). But \( \text{Ker}_\varphi \leq \text{Ker}_\varphi^n \) and so \( \text{Ker}_\varphi = \hat{\Lambda} \). Thus \( \varphi \) injects. Clearly it also surjects.
A congruence $\beta$ is said to be indecomposable if $\hat{\beta} = \beta$ and if $\beta = \gamma \cap \delta$ implies that either $\gamma$ or $\delta$ is in $\hat{\beta}$.

Suppose that $\beta$ is indecomposable, and has the maximal and minimal conditions on subcongruences. Suppose $\beta \cap Y = \delta_1 \cap \delta_2$.

Define $\varphi_1 : \beta \rightarrow (x,y) \mapsto (x,y)$, where $x \delta_1 y$, $x \delta_2 y$, and $x \beta y_1 y_2 = y_1 \delta y_2$.

Define $\varphi_2$ similarly, but with $\delta_1$ and $\delta_2$ interchanged. Now $\varphi_1$ and $\varphi_2$ commute, for one has the following setup (in which two points lie on a straight line labelled by a certain congruence iff they are related by that congruence): 

By Pitting's Lemma 3.1, there is a positive integer $n$ such that $\beta = \varphi_1^n \cap \text{Ker} \varphi_1^n = \varphi_2^n \cap \text{Ker} \varphi_2^n$. Since $\varphi_1$ is indecomposable, one of the pairs of factors is just $\hat{\beta}$. Suppose that neither $\varphi_1$ nor $\varphi_2$ is an automorphism of congruences. Then by Proposition 3.2 $\varphi_1 < \beta$ and $\varphi_2 < \beta$. Hence $\varphi_1^n = \hat{\beta}$ and $\varphi_2^n = \hat{\beta}$.

Now in the notation of the previous diagram, $y = \varphi_1^n(x,2)$, since $y = \varphi_1^n(x,2)$ and $y = \varphi_2^n(x,2)$.

In other words, $(x,y) = \varphi_1^n(x,y)$.

Thus $\beta < \varphi_1^n \varphi_2^n$. Suppose as an induction hypothesis on $m$ that $\beta < \varphi_1^{n+1} \varphi_2^{n+1}$ implies $\beta < \varphi_1^n \varphi_2^n$.

Then $\beta \varphi_1^n \varphi_2^n < \varphi_1^n \varphi_2^n \varphi_1^n \varphi_2^n$.

Thus $\beta < \varphi_1^{n+2} \varphi_2^{n+2}$.

The result is true for all $m$, and in particular for $m = 2n$.

Hence $\beta = \hat{\beta}$. But $\beta$ is indecomposable, so this is impossible.

Thus either $\varphi_1$ or $\varphi_2$ is an automorphism of congruences.

Suppose then without loss of generality that $\varphi_1$ is an automorphism of congruences.

Since it is clear from the context that projections onto $\delta_1$ must be along $\delta_2$, the suffix in the projection notation will be dropped. Now $\delta_1 \cap Y = \hat{\beta}$, for if $x \delta_1 \cap Y$, say with $x \beta y \delta_2 y \delta_1 x$, then $(x,s) = (x,s)$, so that $s = x = y$.

As $\beta = \varphi_1^n \delta_1 \cap Y$, it follows that $\delta_1 \cap \beta = \delta_1 \cap \gamma$. By the modular law in the lattice of congruences, $\delta_1 = (\delta_1 \cap \gamma) \cap \delta_1 = \delta_1 \cap (\gamma \cap \delta_1)$. If $(x,y) \in \beta \cap (\gamma \cap \delta_1) \cap \delta_2$, then $(x,y) \varphi_1 = (x,y)$, so that $y = x$. Thus $\beta \cap (\gamma \cap \delta_1) \cap \delta_2 = \hat{\beta}$.

Now $\beta \subseteq \delta_1 \cap \beta \delta_1 \cap \delta_2$, and so $\beta \cap \delta_2 \subseteq \delta_2 \cap \beta \delta_1$.

Suppose $(x,y) \in \beta \cap \delta_1 \cap \delta_2$, say $y = x \delta_1 \cap \delta_2 \cap \gamma$. Since $\beta \cap \delta_2 \cap \beta x$.

$\Rightarrow (x,y) \in \beta \cap \delta_2 \cap \beta$.

Hence $\beta \cap \delta_2 \cap \beta = \delta_2 \cap \beta$.
3.4 PROPOSITION (Cf. [1,(VI,4,6),Theorème 2].)
If $A \times A$ has the minimal condition on subcongruences, it can be expressed as a direct product of indecomposables.

Proof. If $A \times A$ is indecomposable, there is nothing to prove. Otherwise, $A \times A$ is indecomposable, there is nothing to prove. If $a_1$ is indecomposable, it is the first sought factor found. If not, $a_1 = a_1' \cap a_1''$, and $A \times A = a_1' \cap a_1'' \cap a_2$, with $A \times A > a_1'$. Continue thus. The descending chain $A \times A > a_1 > a_1' > ...$ stops, at the first indecomposable direct factor. Call it $a_1'$. Then $A \times A = a_1 \cap a_1'$. Now $a_1'$ has the minimal condition on subcongruences, and so can be expressed as $a_1' = a_2' \cap a_2''$, $a_2'$ being indecomposable.

Then $A \times A = a_1 \cap a_2' \cap a_2''$. Continue thus. The descending chain $A \times A > a_2' > a_2'' > ...$ stops. Thus the whole process does, and the required expression is found.

3.5 CLASSICAL UNIQUE FACTORIZATION THEOREM If $A \times A$ has both the maximal and minimal conditions on subcongruences, then the factorisation of $A \times A$ as a direct product of indecomposables obtained by Proposition 3.4 is unique up to isomorphisms of congruences. More precisely, if $A \times A = a_1 \cap a_2 \cap ... \cap a_n = \beta_1 \cap \beta_2 \cap ... \cap \beta_n$ with the $a_i$ and $\beta_i$ indecomposable, then $n = n$ and there is a permutation $\sigma$ of $\{1,...,n\}$ such that $A \times A = \beta_{\sigma(1)} \cap ... \cap \beta_{\sigma(n)} \cap a_{\sigma(1)} \cap ... \cap a_{\sigma(n)} ... \cap a_n$ for $r = 0,...,n$.

Further, $a_1$ is isomorphic with $\beta_{\sigma(1)}$ for $1 = 1,...,n$. 

---

3.3 CLASSICAL EXCHANGE THEOREM If indecomposable $\beta$ has the maximal and minimal conditions on subcongruences, and $\beta \cap Y = \delta_1 \cap ... \cap \delta_n$, then $\frac{1}{2} \leq \delta_1 \leq n$ and $\beta \cap Y = \delta_1 \cap ... \cap \delta_n$.

Proof. This follows by induction on $n$ using the above.

Suppose $\beta \cap Y = \delta_0 \cap ... \cap \delta_n$. Then $\beta \cap Y = \delta_0 \cap ... \cap \delta_n$. In an obvious extension of the above notation, either $\delta_0$ or $\delta_n$ is an automorphism of congruences.

If $\sigma_n$ is an automorphism of congruences, take $1 = n$; then $\sigma_n$ follows by the above. If not, $\delta_0$ is an automorphism.

Then by the above, $\beta \cap Y = \delta_0 \cap Y$, so that $\sigma : \beta \mapsto \delta_0$;

$(x,y) \mapsto (s,\tau)$ where $x \mapsto y \mapsto \delta_0 x$ is an isomorphism of congruences. In particular, $\delta_0$ is indecomposable.

Also $\delta_0 \cap (Y \cap \delta_0) = \delta_1 \cap ... \cap \delta_{n-1}$, and so by induction $\frac{1}{2} \leq \delta_1 \leq n-1$. Thus $\delta_0$ is isomorphic with $\delta_1$.

Composing the isomorphisms, $\beta$ is isomorphic with $\delta_1$.

Now $\beta \cap Y = \delta_1 \cap ... \cap \delta_{n-1} \cap \delta_{n-1} \cap ... \cap \delta_1$, and again using an extension of the above notation, $\delta_1$ is an automorphism of congruences. The result follows by applying the above to this setup.
Proof. Suppose \( \sigma : \{1, \ldots, s\} \to \{1, \ldots, n\} \) has been defined so that (*) holds for \( r \leq s \). In particular,
\[
\sigma_{s+1} \cap (\beta_{\sigma(1)} \cap \cdots \cap \beta_{\sigma(s)} \cap \beta_{s+2} \cap \cdots \cap \beta_n) = \beta_1 \cap \cdots \cap \beta_n.
\]
By the Classical Exchange Theorem 3.3, \( \xi \leq \eta \), \( \beta_1 = \xi \cap \eta \), and \( \eta = \hat{\eta} \). Define \( \sigma(s+1) = 1 \). Then
\[
\lambda \times \lambda = \beta_{\sigma(1)} \cap \cdots \cap \beta_{\sigma(s+1)} \cap \beta_{s+2} \cap \cdots \cap \beta_n.
\]
The result follows by induction.

4. CENTRALITY AND DIRECT DECOMPOSITIONS

In Section 3 the Classical Unique Factorisation Theorem for a Mal'cev algebra \( A \) was proved from Fitting's Lemma using the category of congruences on \( A \). Centrality was not used at all. In this section it is brought in to make two improvements on the "classical" situation. Firstly the isomorphism of congruences used in passing in the proof of the Classical Exchange Theorem 3.3 is examined in more detail by the Central Isomorphism Theorem 4.3. This allows a preciser conclusion to the unique factorisation theorem. Secondly the hypothesis of the Classical Unique Factorisation Theorem 3.5, viz. that \( A \times A \) has both the maximal and minimal conditions on subcongruences, is relaxed to the requirement of those conditions only on the centre congruence \( \zeta(A) \). The result of these two improvements in the Unique Factorisation Theorem 4.6, which is the best available theorem of its kind for Mal'cev algebras since it generalises directly the best available theorem for groups, the Krull-Remak-Schmidt Theorem in its latest form.

The proof of the Central Isomorphism Theorem 4.3 to be given here, via Propositions 4.1 and 4.2, is slightly more complicated than it need be. It is done thus this because Proposition 4.1 is required later anyway, to prove Propositions 4.4 and 5.4.
If $\beta$, $\gamma$ are congruences on $A$, then $\gamma$ is said to centralise $\beta$ iff there is a centralising congruence $((\gamma|\beta)$ on $\beta$, satisfying the two conditions

(C1) $X(x,y) \subseteq \beta$, $X((\gamma|\beta)) \to x \gamma y$ bijects $x$ onto $y$.

(C2) $(\gamma|\beta)$ respects equivalence of $\beta$.

Comparing with Definition 1.1, a congruence $V$ is central iff $A \times A$ centralises $V$, $(A \times A|V)$ being the centralising congruence.

If $\beta \cap \gamma = \delta = A$, then $\gamma$ centralises $\beta$, the congruence $(\gamma|\beta)$ being defined on $\beta$ by

$$(x,y) (\gamma|\beta) (x',y') \iff x \gamma y \iff x' \gamma y'.$$

4.1 Proposition

Suppose $\beta \cap \delta = A$.

(i) If $a \leq \beta \cap \delta$, then it also centralises $\delta^\beta$.

(ii) If $\beta$ centralises $\beta'$, and $\beta' \subseteq \beta$, then $\beta \cap \delta$ centralises $\beta'$.

Proof. (i) Since $\beta$ centralises $a$, there is a congruence $(\beta|a)$ on $a$ satisfying (C1) and (C2). Define a relation $(\beta|\beta')$ on $\delta^\beta$ by

$$(x,y) (\beta|\beta') (x',y') \iff x \beta y \delta a x', x' \beta y' \delta a x',$$

and $(x,a) (\beta|\beta) (x',a')$. Then $(\beta|\beta')$ is a congruence satisfying (C1) and (C2).

(ii) Since $\beta$ centralises $\beta'$, there is a congruence $(\beta|\beta')$ on $\beta'$ satisfying (C1) and (C2). But $\beta' \subseteq \beta \Rightarrow \beta \cap \delta = A$.

Then $(\beta|\beta') \cap (\delta|\beta') = (\beta \cap \delta|\beta')$ centralises $\beta'$.]

4.2 Proposition

Suppose $\beta \cap \gamma = \delta \cap \epsilon$.

Then $\beta$ centralises $\delta^\gamma \cap \epsilon^\beta$.

Proof. Define a relation $(\beta|\epsilon^\beta)$ on $\delta^\gamma$ by

$$(x,y) (\beta|\epsilon^\beta) (x',y') \iff x \beta x', y \beta y',$$

and $\frac{x}{\delta} \in \epsilon \iff \frac{y}{\delta} \in \epsilon$, where $x, y, x', y' \in y \delta x'$. Then $(\beta|\epsilon^\beta)$ is a congruence on $\delta^\gamma$ satisfying (C1) and (C2). Now define a relation $(\beta|\delta^\gamma \cap \epsilon^\beta)$ on $\delta^\gamma \cap \epsilon^\beta$ by

$$(x,y) (\beta|\delta^\gamma \cap \epsilon^\beta) (x',y') \iff x \beta x', y \beta y',$$

and $\frac{x}{\delta} \in \epsilon \iff \frac{y}{\delta} \in \epsilon$, where $x, y, x', y' \in y \delta x'$. Then $(\beta|\delta^\gamma \cap \epsilon^\beta)$ is a congruence satisfying (C1) and (C2).]

An isomorphism of congruences $\phi : U \to V$ on $A$ is said to be central iff $U \cap \phi(A) \subseteq V \cap \phi(U)$. If $U$ and $V$ are centrally isomorphic congruences on $A$, write $U \sim V$.

4.3 Central Isomorphism Theorem

$A \equiv A = \beta \equiv \gamma = \beta \cap \delta = \gamma \cap \delta$.

Proof. Define $\phi : \gamma \to \delta ; (x,y) \mapsto (x,a)$, where $x \gamma y \beta \delta x$.

Clearly $\phi$ is an isomorphism of congruences, and it merely remains to show that each $(y,z) \in \phi(A)$. Let $a = \beta^\gamma \cap \delta^\beta$.

By Proposition 4.2, $\beta$ centralises $a$.

By Proposition 4.1(i), $\beta$ centralises $\beta^\beta$.

By Proposition 4.1(ii), $\beta^\beta \subseteq \phi(A)$.

Now $a \leq \phi = \phi^\beta \cap \phi^\gamma$, and so $\phi^\beta = \phi^\gamma$.

But since $y \gamma \delta \beta \beta \gamma y$, $(y,z) \in \phi^\gamma$.]


Now for the "non-classical" versions of the theorems of the previous section.

4.4 PROPOSITION Suppose \( \zeta = \zeta(a) \) has the maximal and minimal conditions on subcongruences, and \( A \times A = \beta \cap \gamma = \delta_1 \cap \cdots \cap \delta_n \).

Then for each \( i = 1, \ldots, n \), there are subcongruences \( \delta_i \) of \( \delta_1 \) such that \( \beta \cap \gamma = \beta \cap \delta_1 \cap \cdots \cap \delta_i \).

Proof. For each \( i \), let \( \delta_i = \delta_1 \cap \cdots \cap \delta_{i-1} \cap \delta_{i+1} \cap \cdots \cap \delta_n \). Let \( \gamma = \delta_i \gamma_i \). By Proposition 4.1, \( \beta \) centralises \( \beta \gamma_i \), and so \( \beta \gamma_i \leq \beta \cap \zeta \).

But \( \gamma_i \leq \beta \gamma_i \cap \gamma = (\beta \cap \zeta) \cap \gamma \).

Since \( \gamma \leq \gamma_1 \cap \cdots \cap \gamma_n \), it follows that

\[
\gamma \leq \cap \delta_i \cap (\beta \cap \zeta) \cap \delta_1 \cap \cdots \cap \delta_n (1).
\]

Thus \( \beta \cap \gamma \leq \delta_1 \cap \cdots \cap \delta_n \).

Since \( A \times A \) centralises \( \beta \cap \zeta \), \( \delta_1 \) centralises \( \delta_i \).

Thus for each \( i \), \( \delta_i \leq \zeta \).

Since \( \beta \times \beta \) centralises \( \delta_i \), \( \beta \) centralises \( \delta_i \).

Thus \( \delta_1 \cap \beta \gamma_i \cap \gamma \leq (\beta \cap \zeta) \cap \delta_1 \cap \delta_i \). Hence

\[
\beta \cap \zeta \leq \cap \delta_i \cap (\beta \cap \zeta) \cap \delta_1 \cap \delta_i (2).
\]

From (1) and (2),

\[
(\beta \cap \zeta) \cap \gamma = \cap \delta_i \cap (\beta \cap \zeta) \cap \delta_1 \cap \delta_i (3).
\]

Since \( \zeta \) has the minimal condition on subcongruences, Proposition 3.4 yields \( \beta \cap \zeta = \beta_1 \cap \cdots \cap \beta_p \) for some finite number \( p \) of indecomposable \( \beta_p \). It will be shown by induction on \( p \) that

\[
\cap \delta_i \cap (\beta \cap \zeta) \cap \gamma = \cap \delta_i \cap (\beta \cap \zeta) \cap \delta_1 \cap \cdots \cap \delta_n (4).
\]

This is sufficient to give the result, for, letting \( a = \delta_1 \cap \cdots \cap \delta_n \), \( (\beta \cap \zeta) \cap \gamma = (\beta \cap \zeta) \cap a \). Suppose \( (x, y) \in \beta \cap \gamma \). Then \( \cap \delta_i \cap \beta \cap \gamma \cap \delta_1 \cap \delta_i \cap \delta_1 \). Hence \( \beta \cap \gamma = A \times A \).

Suppose \( (x, y) \in \beta \cap \gamma \). In particular, \( (x, y) \in \cap \beta \cap \zeta \cap \gamma \). So \( \cap \delta_i \cap \beta \cap \gamma \cap \delta_1 \cap \delta_i \cap \delta_1 \). Hence \( \beta \cap \gamma = A \times A \).

It thus remains to prove (4) by induction on \( p \).

If \( p = 0 \), \( \beta \cap \zeta = A \). Equation (4) is then just (3) with \( \delta_1 \cap (\beta \cap \zeta) \cap \gamma = \delta_1 \cap \gamma \).

Suppose (4) holds for all \( p < m \).

If \( p = m \), then \( (\beta \cap \zeta) \cap \gamma = \delta_m \cap \gamma \).

By induction, \( \cap \delta_i \cap \beta \cap \gamma \cap \delta_1 \cap \delta_i \cap \delta_1 \delta_i \cap \gamma \).

Note that \( \beta \cap \gamma \) is indecomposable and, being central, has the maximal and minimal conditions on subcongruences. The Classical Exchange Theorem 3.3 then shows \( \cap \delta_i \cap (\beta \cap \zeta) \cap \gamma = \delta_i \cap \gamma \).

Note that \( \delta_i \cap \gamma \cap \delta_1 \cap \delta_i \cap \delta_1 \).

Set \( \delta_i = \gamma \), and \( \delta_1 \cap \gamma \cap \delta_1 \).

Then \( (\beta \cap \zeta) \cap \gamma = (\beta \cap \zeta) \cap \delta_1 \cap \cdots \cap \delta_n \).

(4) thus holds for all \( p < m+1 \).
4.5 [EXCHANGE THEOREM] If \( \beta \) is indecomposable, \( \zeta(A) \) has the maximal and minimal conditions on subcongruences, and \( \beta \cap \gamma = \delta_1 \cap \ldots \cap \delta_n = A \times A \),
then \( \delta_1 \leq \ldots \leq \delta_n \) and
\[ \beta \cap \gamma = \delta_1 \cap \ldots \cap \delta_n = A \times A, \]

**Proof.** If \( \beta \leq \zeta(A) \), then the result follows by the Classical Exchange Theorem 3.3. So assume \( \beta \nleq \zeta(A) \). By Proposition 4.4,
\[ \delta_1 \leq \delta_2 \leq \ldots \leq \delta_n. \]
By the modularity of the lattice of congruences, there are direct complements \( \delta_i^* \) such that \( \delta_i = \delta_i \cap \delta_i^* \), \( i = 1, \ldots, n \), and then
\[ \beta \cap \gamma = \delta_1^* \cap \ldots \cap \delta_n = \delta_n. \]
By the Central Isomorphism Theorem 4.3, \( \beta \cap \gamma = \delta_n \). But \( \beta \) is indecomposable, and so there is just one \( i \), say \( i = 1 \), with \( \delta_1^* > \delta_1 \).

Hence \( \delta_1 = \delta_2 \) for \( 1 \leq i = 1, \ldots, n \).
Putting \( \xi = \delta_1 \) and \( \eta = \delta_1^* \),
\[ A \times A = \beta \cap \gamma = \beta \cap \eta = \beta \cap \xi = A \times A. \]
Proposition 4.4 then yields \( \beta' \leq \beta, \gamma' \leq \gamma \) such that
\[ \beta \cap \gamma = \xi \beta' \cap \eta \gamma'. \]
By modularity, \( \beta' \leq \beta, \gamma' \leq \gamma \) if \( \beta' \cap \gamma' \). Then
\[ \beta \cap \gamma = \xi \beta' \cap \eta \gamma' = \beta' \cap \gamma' \cap \xi \beta' \cap \eta \gamma'. \]
By the Central Isomorphism Theorem 4.3, \( \beta \leq \beta \cap \gamma \).

But \( \beta \) is indecomposable, and so \( \beta' \cap \gamma' = \xi \beta' \cap \eta \gamma' \).
If \( \beta' = \xi \beta \), then there is a central isomorphism \( \gamma' \leq \gamma' \).
Now \( \beta \cap \gamma = \xi \beta \), and so \( \beta \) centres \( \gamma \) by congruence \( (\beta, \gamma) \).
Define a relation \( (\beta, \gamma) \) on \( (x, y) \) by \( (x, y) (\beta, \gamma) (x', y') \) iff \( (x, y)(\beta, \gamma)(x', y') \).
Then \( (\beta, \gamma) \) is a centreing congruence. Thus \( \beta \) and hence \( \beta \cap \gamma = A \times A \) by Proposition 4.1(iii), hence \( \beta \) is a contradiction to the assumption that \( \beta \) is indecomposable. The alternative remaining is that \( \gamma' = \xi \beta' \cap \gamma' \).
Hence \( \beta' = \beta' \cap \gamma' \).

4.6 [UNIQUE FACTORIZATION THEOREM] If \( \zeta(A) \) has the maximal and minimal conditions on subcongruences, then \( A \times A \) has the unique decomposition \( A \times A = a_1 \cap \ldots \cap a_m \) into indecomposable factors. More precisely, if
\[ A \times A = a_1 \cap \ldots \cap a_m \cap \ldots \cap a_m \]
with the \( a_i \) and \( a_i \) indecomposable, then \( n = m \) and
there is a permutation \( \sigma \) of \( \{1, \ldots, m\} \) such that
\[ A \times A = \beta_{\sigma(1)} \cap \ldots \cap \beta_{\sigma(n)} \cap \ldots \cap \beta_{\sigma(m)} \]
for \( r = 0, \ldots, m \).

Further, \( a_{\sigma(i)} \cap \beta_{\sigma(i)} \) for \( i = 1, \ldots, m \).

**Proof.** \( (*) \) is proved by induction as for the Classical Unique Factorization Theorem 3.5, but using the Exchange Theorem 4.5 instead of the Classical Exchange Theorem 3.3. Application of the Central Isomorphism Theorem 4.3 to successive \( r \)-values of \( (*) \) yields the central isomorphism. \]

4.7 [COROLLARY] If \( A \times A \) has the minimal condition on subcongruences, and \( \zeta(A) \) the maximal condition, then \( A \times A \) has precisely one direct decomposition into a finite number of indecomposables.

**Proof.** From Proposition 3.4 and the Unique Factorization Theorem 4.6. \]
5. STABLE ISOTOPY

The previous two sections have examined the direct decompositions of a single Mal'cev algebra $A$. By contrast, the topic of this section is the behaviour of a whole variety $\mathcal{T}_A$ of Mal'cev algebras under the direct product. Let $[\xi]$ denote the set of isomorphism classes of finite $\mathcal{T}_A$-algebras. $[\xi]$ is a category with the class $\{1\}$ of the one-element $\mathcal{T}_A$-algebra as identity. Let $[\xi]$ be the Grothendieck group of the monoid $[\xi]$, i.e., a group with monoid-morphism $[\xi] \to [\xi]$ universal among monoid-morphisms from $[\xi]$ to groups. Let $[\xi]$ denote the image of the isomorphism class of $\mathcal{T}_A$-algebra $A$ under this morphism. For two $\mathcal{T}_A$-algebras $C, D$, $[C] = [D]$ if there is a third $\mathcal{T}_A$-algebra $B$ such that $B \times C \cong B \times D$. The goal of the current section is the Cancellation Theorem 5.7 giving an internal characterization of this relationship between $C$ and $D$. A useful by-product of the proof is the Structure Theorem 5.5 for algebras in the subvariety $\mathcal{S}[\xi]$.

It is first necessary to make the universal-algebra notation more precise. Hitherto, if $\omega$ has been an element of the set $|A|$ of the operator domain $A$ having arity $n$, and if $\rho : |A| \to \bigotimes_{i=1}^n A$ is the map describing the action of $|A|$ on a $\mathcal{T}_A$-algebra $(A, \rho)$, then for $a_1, \ldots, a_n \in A$, the result $(a_1, \ldots, a_n)\rho(\omega)$ of the action of $\omega$ has been written laxly as $a_1 \ldots a_n \omega$ (or with the operator in some other position), and also $(A, \rho)$ has been written merely as $A$, the

5.1 DEFINITIONS A $\mathcal{T}_A$-algebra $(B, \circ)$ is said to be a stable isotopy of a $\mathcal{T}_A$-algebra $(A, \rho)$ if there is a bijection $\sigma : B \to A$, called a stable isotopy, such that $\forall \omega \in |A|$, $(a_1, \ldots, a_n) \in \Xi(A)$, $\forall b_1, \ldots, b_n \in B$, $\sigma$ being the arity of $\omega$,

$$((b_1, \ldots, b_n)\circ(\omega_1, \ldots, \omega_n)) \in \Xi(A) \text{ and } (a_1, \ldots, a_n) \in \Xi((b_1, \ldots, b_n)\circ(\omega_1, \ldots, \omega_n)),$$

where $\Xi$ centres $\Xi(A)$. In this case write $(B, \circ) \sim (A, \rho)$.

5.2 PROPOSITION $\sim$ is an equivalence relation.

Further, if $\sigma : (B, \circ) \to (A, \rho)$ is a stable isotopy, and if $\Xi \subseteq B$ respectively centre $\Xi(A)$, $\Xi(B)$, then $\Xi(A) = \Xi(B)(\sigma, \sigma)$, and $\Xi = \Xi((\sigma, \sigma, \sigma))$.

Proof. Since $\sigma$ bijections, $\Xi(A)(\sigma^{-1}, \sigma^{-1})$ is an equivalence relation on $\Xi$. It follows from the definition of stable isotopy and the transitivity of $\Xi(A)$ that $\Xi(A)(\sigma^{-1}, \sigma^{-1})$ is a $\mathcal{T}_A$-algebra, so a congruence on $(B, \circ)$.

Again, since $\sigma$ bijections, $\Xi((\sigma^{-1}, \sigma^{-1}, \sigma^{-1}))$ is an equivalence relation on $\Xi(A)(\sigma^{-1}, \sigma^{-1})$. Let $\omega$ be an $n$-ary operation, and suppose $((b_1, \ldots, b_n)\circ(\omega_1, \ldots, \omega_n)) \in \Xi((\sigma, \sigma, \sigma))$, for $i = 1, \ldots, n$.

Then $((b_1, \ldots, b_n)\circ(\sigma, \sigma, \sigma)) \in \Xi((\sigma, \sigma, \sigma)(\sigma^{-1}, \sigma^{-1}, \sigma^{-1})(\sigma, \sigma, \sigma))$, for $i = 1, \ldots, n$.
Any isomorphism \( \phi : (B, \sigma) \to (A, \rho) \) is a stable isotopy, with \( a_n = \bar{a}_n \) for all \( n \in \Omega \). As a partial converse, if \((A, \rho)\), \((B, \sigma)\) have respective singleton subalgebras \((\{e\}, \rho)\), \((\{f\}, \sigma)\), and if \( \phi : B \to A \) is a stable isotopy with \( fe = e \), then \( \phi \) is an isomorphism of \((A, \rho)\) and \((B, \sigma)\).

If \((A, \rho)\) has singleton subalgebra \((\{e\}, \rho)\), then the mapping \( \zeta(A) \to \zeta(B) \) (the \( \{e\} \)-class) is an isomorphism of \( \mathbb{Z}\)-algebras. The isomorphism induces an operation \( + \) on \( \zeta(A) \) making it an abelian group with \( e \) as identity. (cf. Proposition 1.7(i)). Singleton subalgebras within \( \zeta(A) \) form a subgroup \( G \). Stable isotopies of \((A, \rho)\) to itself permuting singleton subalgebras within a given \( \zeta(A) \)-class then form an abelian group of fixed-point-free automorphisms of \((A, \rho)\) isomorphic with \( G \).

Now to return to the main theme of this section.

Note that if \( A \times A = a_1 \times \cdots \times a_m \), and defining the complements \( a_n = a_1 \times \cdots \times a_{n-1} \times a_{n+1} \times \cdots \times a_m \), then \( A = A \text{ nat}_a \times \cdots \times A \text{ nat}_{a_m} \).

Also, \( A \text{ nat}_{a} \) is indecomposable iff \( a_1 \) is.

Let \( \mathcal{Z}_0 \) denote the class of all \( \mathbb{Z}\)-algebras having singleton subalgebras.

5.3 THEOREM If \((B, \sigma)\) is a stable isotopy of \((A, \sigma)\), then there is an algebra \( \mathcal{Z} \in \mathcal{Z}_0 \) such that \( A \times \mathcal{Z} \cong A \times \mathcal{Z} \).

Proof. Suppose \( \phi : B \to A \) is a stable isotopy with \((b_n, \bar{b}_n) \in (\mathcal{O}_n, \sigma) \sigma(\omega), \sigma(\sigma), \cdots, \sigma(\omega)) \) for each \( n \)-ary \( \omega \in \Omega \), \( \mathcal{Y} \) centring \( \zeta(B) \).

Now by Definition 5.1, \((b_n, \bar{b}_n) \sigma(\omega), \sigma(\sigma), \cdots, \sigma(\omega)) \)
\[ \mathcal{Y} (\mathcal{O}_n, \sigma) \sigma(\omega) \sigma(\sigma), \sigma(\sigma), \cdots, \sigma(\omega)) \]
Since \( \mathcal{Y} \) is a congruence, \((b_n, \bar{b}_n) \sigma(\omega), \sigma(\sigma), \cdots, \sigma(\omega)) \)
\[ \mathcal{Y} (\mathcal{O}_n, \sigma) \sigma(\omega) \sigma(\sigma), \sigma(\sigma), \cdots, \sigma(\omega)) \]
Again by Definition 5.1, \((b_n, \bar{b}_n) \sigma(\omega), \sigma(\sigma), \cdots, \sigma(\omega)) \)
\[ \mathcal{Y} (\mathcal{O}_n, \sigma) \sigma(\omega) \sigma(\sigma), \sigma(\sigma), \cdots, \sigma(\omega)) \]
Thus since \( \mathcal{Y} \) respects transitivity of \( \zeta(A) \),
\[(b_n, \bar{b}_n) \sigma(\omega), \sigma(\sigma), \cdots, \sigma(\omega)) \]
\[ \mathcal{Y} (\mathcal{O}_n, \sigma) \sigma(\omega) \sigma(\sigma), \sigma(\sigma), \cdots, \sigma(\omega)) \]
Hence \( \mathcal{Y}(o^{-1}, o^{-1}, o^{-1}) \) is a congruence on \( \zeta(A)(e^{-1}, o^{-1}) \).
Properties (C1) and (C2) of Definition 1.1 for \( \mathcal{Y}(e^{-1}, o^{-1}, o^{-1}) \) follow immediately since \( \mathcal{Y} \) bijects.
Thus \( \mathcal{Y}(e^{-1}, o^{-1}, o^{-1}) \) centres \( \zeta(A)(e^{-1}, o^{-1}) \).
By Theorem 1.10, \( \zeta(A)(e^{-1}, o^{-1}) \subseteq \zeta(B) \), and by Proposition 1.8,
\[ \mathcal{Y}(e^{-1}, o^{-1}, o^{-1}) = \mathcal{Y}(\zeta(A)(e^{-1}, o^{-1}) \times \zeta(A)(e^{-1}, o^{-1})) \]
In the notation of Definition 5.1, let \( b_0 = \bar{a}_0 \).
Now \( a_0, \cdots, a_n \in A \),
\[ (b_n, \bar{b}_n) \mathcal{Y} (a_0, a_1, \cdots, a_n) \sigma(\omega), (a_0, a_1, \cdots, a_n) \sigma(\omega)) \]
Applying \( e^{-1} \) and using respect of \( \mathcal{Y} \) for symmetry of \( \zeta(A) \), \((b_n, \bar{b}_n) \mathcal{Y}(e^{-1}, o^{-1}, o^{-1}) (((a_0, a_1, \cdots, a_n) \sigma(\omega), (a_0, a_1, \cdots, a_n) \sigma(\omega)) \). From above, this can be written as
\[ (b_0, \bar{b}_0) \mathcal{Y} (a_0, a_1, \cdots, a_n) \sigma(\omega), (a_0, a_1, \cdots, a_n) \sigma(\omega)) \]
Thus \( e^{-1} : A \to B \) is also a stable isotopy. In particular, the relation \( \sim \) is symmetric. Repeating the above procedure for the new stable isotopy \( e^{-1} \), \( \zeta(A)(e^{-1}, o^{-1}) \subseteq \zeta(A) \).
Hence \( \zeta(A) = \zeta(B)(e, o) \) and \( \mathcal{Y}(e, o, o) \mathcal{Y} \). The transitivity of \( \sim \) follows easily, and since \( \zeta(A) \) is a stable isotopy, reflexivity is immediate.
Define an action of \( \mathcal{B} \) on \( \Omega \) by
\[
(b_{n}, b')_{n} \varphi \equiv ((b_{1}, \ldots, b_{n}) b_{n}(\omega), (b_{1}, \ldots, b_{n}) \sigma(\omega))
\]
Then \( (b, c) \sim (b, c) \equiv (c, \sigma) \).

Now \( \zeta(\mathcal{B}) \) is a subset of \( \mathcal{B} \times \mathcal{B} \). Suppose \( \omega \) is an \( n \)-ary operation of \( \mathcal{B} \), and \( (b_{1}, b_{2}) \in \zeta(\mathcal{B}) \) for \( i = 1, \ldots, n \).

Since \( ((\zeta(\mathcal{B}), (\sigma, c)) \) is a subalgebra of \( \mathcal{B} \times \mathcal{B}, (\sigma, c) \),
\[
((b_{1}, \ldots, b_{n}) \sigma(\omega), (b_{1}, \ldots, b_{n}) \sigma(\omega)) \in \zeta(\mathcal{B})
\]
By definition of the action of \( \sigma \) on \( \mathcal{B} \),
\[
((b_{1}, \ldots, b_{n}) \sigma(\omega), (b_{1}, \ldots, b_{n}) \sigma(\omega)) \in \zeta(\mathcal{B})
\]
Then by transitivity of \( \zeta(\mathcal{B}) \),
\[
((b_{1}, \ldots, b_{n}) \sigma(\omega), (b_{1}, \ldots, b_{n}) \sigma(\omega)) \in \zeta(\mathcal{B})
\]
Thus \( (\zeta(\mathcal{B}), (\sigma, c)) \) is a subalgebra of \( \mathcal{B} \times \mathcal{B}, (\sigma, c) \).

Let \( (A, \rho) = (\zeta(\mathcal{B}), (\sigma, c)) \).

The projection \( \pi_{1} : (\mathcal{B} \times \mathcal{B}, (\sigma, c)) \rightarrow (\mathcal{B}, \sigma) \)
yields a congruence \( \text{kern}_{\mathcal{A}} \) on \( (\mathcal{B} \times \mathcal{B}, (\sigma, c)) \),
\[
\text{viz.} \quad (b_{1}, b_{2}) \text{kern}_{\mathcal{A}} (b_{1}', b_{2}') \Leftrightarrow b_{1} = b_{1}'.
\]
Let \( \beta = \text{kern}_{\mathcal{A}} \cap \zeta(\mathcal{B}) \).

Then \( \beta \) is a congruence on \( (A, \rho) \), and \( (A, \rho, \beta) = (A, \sigma, c) \).

Similarly, if \( \gamma = \text{kern}_{\mathcal{A}} \cap \zeta(\mathcal{B}) \), then \( \gamma \) is a congruence on \( A \) with \( (A, \gamma, \gamma) = (A, \sigma, c) \).

Suppose \( \omega \) is an \( n \)-ary operation of \( \mathcal{B} \), and for \( i = 1, \ldots, n \),
\[
(a_{1}, a_{2}) \in \zeta(\mathcal{B}) \text{ with } (a_{1}, a_{2}) \varphi \equiv (a_{1}, a_{2}) \varphi.
\]
Now \( (a_{1}, a_{2}, a_{3}) \sigma(\omega), (a_{1}, a_{2}, a_{3}) \sigma(\omega), (a_{1}, a_{2}, a_{3}) \sigma(\omega)) \equiv \gamma \varphi \equiv (a_{1}, a_{2}, a_{3}) \sigma(\omega)
\]
\[
((b_{1}, \ldots, b_{n}) \sigma(\omega), (b_{1}, \ldots, b_{n}) \sigma(\omega)) \equiv (b_{1}, \ldots, b_{n}) \sigma(\omega)
\]
Since \( \gamma \) respects transitivity of \( \zeta(\mathcal{B}) \),
\[
((a_{1}, a_{2}, a_{3}) \sigma(\omega), (a_{1}, a_{2}, a_{3}) \sigma(\omega), (a_{1}, a_{2}, a_{3}) \sigma(\omega)) \equiv \gamma \varphi \equiv (a_{1}, a_{2}, a_{3}) \sigma(\omega)
\]
Thus \( \gamma \) is a congruence on \( (A, \sigma, c) \).

By proportion (1) and (2) of \( \gamma \), \( A \times A = A = \gamma \sigma \gamma \).

Let \( A^{2} = A \). Then \( x \in [A] \), having singleton subalgebra \( B \).
\[ A \ast A^{2} = A^{2} \ast A^{2} \Rightarrow 2 \times 2 \Rightarrow 2 x 2 \times 2 \times 0 \text{ as required.} \]

Theorem 5.3 goes halfway towards solving the main problem of this section. It shows that if \( B \) is a stable isotope of \( C \), then \([B] = [C] \). What is more, it produces the algebra \( Z \) in the class \( [B] \), such that \( B \times B \Rightarrow 2 \times 2 \times 2 \times 2 \times 0 \).

The value of this is that \( 
\text{Algebras have a very simple and easily examined structure, as will become apparent from the Structure Theorem 5.5. This arises in the solution of the other half of the main problem. From now on the actions of the operator domain are once more suppressed.} \]

5.4 PROPOSITION Suppose \( A \times A = B \), \( Y = \delta \in A \)

and there is a central isomorphism \( \varphi : B \rightarrow \delta \).

Then \( \delta \) is a stable isotope of \( A^{2} \).

Proof. Define a congruence \( (\beta, \alpha) \) on \( \alpha \) by
\[
(x, y) (\beta, \alpha) (x', y') \Leftrightarrow x \varphi x', y \varphi y', \text{ and}
\]
Then by Proposition 4.1(1), \( \beta \) centralises \( \gamma \) with \( (\beta, \alpha) \).

Thus \( \beta, \gamma \in \zeta(A) \).

Fix \( a \in A \). Let \( \omega \in \{A\} \) be an \( n \)-ary operation.

Suppose \( a \beta, a \in A \), and \( \gamma \beta, a \in A \). Then \( (a, a) \in \beta \gamma \in \zeta(A) \).

Hence \( (a, a, a) \in \zeta(A) \), and so \( (a, a, a) \in \zeta(A) \).
5.5 STRUCTURE THEOREM FOR ALGEBRAS IN $\mathbb{H}$

An algebra in the class $\mathbb{H}$ iff it is a stable isotop of an algebra in the class $\mathbb{E}_0$. The structure of an algebra in the class $\mathbb{E}_0$ is essentially that of a module over a ring.

**Proof.** Recall that a $\mathbb{H}$-algebra in $\mathbb{H}(\mathbb{E})$ iff there is a congruence centering its direct square. Proposition 5.2 then shows that any stable isotop of an algebra in $\mathbb{H}$ is also in $\mathbb{H}$. Conversely suppose that algebra $B$ is in $\mathbb{H}$.

Let $\mathcal{F}$ centre $\mathcal{F}(B) = B \times B$. Let $E_1$, $E_2$ respectively be the congruences $\ker x_1$, $\ker x_2$ as in the proof of Theorem 5.3.

Then $B \times B \times B = E_1 \cap E_2 = E_1 \cap \mathcal{F}$. By Proposition 5.4,

$E_1 \cap E_2 \rightarrow (B \times B)\mathfrak{m}_E \sim (B \times B)\mathfrak{m}_F$.

But $(B \times B)\mathfrak{m}_E = B$ and $(B \times B)\mathfrak{m}_F$ has singleton subalgebra $B$.

Suppose $A$ in $\mathbb{E}_0$ has singleton subalgebra $\{e\}$.

By the remarks after Proposition 5.2, there is an operation $\cdot$ on $A$ making it an abelian group $(A,+,0)$ with 0 as identity.

A binary operation $\cdot$ and a nullary operation "select 0" are induced on every element of the subvariety $\mathbb{A}_n$ of $\mathbb{T}$ generated by $A$. Adjoin them to the operator domain $\Omega$ of $\mathbb{A}_n$ to make a new variety $\mathbb{A}_n$. If $\mathcal{F}$ centres the $\mathbb{A}_n$-algebra $AxA$, then by definition of $\mathcal{F}$ it also centres the $\mathbb{A}_n$-algebra $AxA$. Let $T$ be the set of translations of the $\mathbb{A}_n$-algebra $A$ fixing 0. Then if $c \in T$, $(c, y)(x, y)$ implies $(c, y)(x, (x+y)c)$, so that $(x+y)c = xc + yc$. $T$ becomes a subring of the ring of endomorphisms of the abelian group $(A, +, 0)$.

It follows that if $e \in \Omega$ is an n-ary operation, then $\forall x_1, \ldots, x_n \in A$, $x_1 \ldots x_n \omega = x_1 \ldots x_n \omega + g_{x_1} \ldots g_{x_n} + \ldots + g_{x_1} \ldots x_n \omega$, where the mappings $A = A; z_1 \mapsto 0; \ldots; x_n \omega$ are in $T$.

Thus the structure of $A$ as a $\mathbb{H}$-algebra is determined precisely by its structure as a T-module.

5.6 COROLLARY If two $\mathbb{E}_0$-algebras are stably isotopic, then they are isomorphic.

**Proof.** Suppose $B$ and $C$ are $\mathbb{E}_0$-algebras with a stable isotopy $e : B \mapsto C$. Let $\{e\}, \{f\}$ be singleton subalgebras of $B$, $C$ respectively. By the remarks after Proposition 5.2, there is an operation $\cdot$ on $C$ making $(C, +, 0)$ an abelian group with identity $e$. Suppose $ee = g$. Then from Structure Theorem 5.5, the mappings $B \mapsto C$; $b \mapsto be-g$ is a stable isotopy.

For since $e$ is a stable isotopy, $\forall n$-ary $\omega \in \Omega$, $\{e\} \in \mathbb{C}$. $\forall b_1, \ldots, b_n \in B$, $b_1 \ldots b_n \omega = b_1 \ldots b_n \omega + a_0$. Then $\mathcal{F}$-ally, $e \cdot (b_1 \ldots b_n \omega) = b_1 \ldots b_n \omega + g \cdot e \omega$.

$= b_1 \ldots b_n \omega - (a_0 + \ldots + a_n)$, so that $b \mapsto be-g$ is a stable isotopy, since $ee = e = f$, $b \mapsto be-g$ is an isomorphism, again by the remarks after Proposition 5.2.
Define \( \phi : A^2 \to A^2 \) by \( \phi (a,b) = (a,b) \), where \( a \neq b \). It will be shown that \( \phi \) is the required stable isotopy. Let \( a \neq b \), \( (a,b) \neq (a,b) \), \( 1 = 1, \ldots, n \).

Let \( B = F(a_1, \ldots, a_n, b_1, \ldots, b_n) \), \( (a,b) = (a,b) \), for since \( a \neq a \neq a \neq a \neq a \) \( b_1, \ldots, b_n \), \( b_1, \ldots, b_n \).

\( \psi \) a \( F \)-morphism \( \Rightarrow \psi (a_1, \ldots, a_n, b_1, \ldots, b_n) \) \( = \psi (a_1, \ldots, a_n, b_1, \ldots, b_n) \).

Hence \( b_1^* \ldots b_n^* e = F(a_1^* \ldots a_n^*, b_1^* \ldots b_n^* e) \).

But \( (a_1^* \ldots a_n^*, b_1^* \ldots b_n^* e) = (a_1^*, b_1^*) \) in \( F \).

Thus if \( \psi \) centre \( \psi (a_1^*, b_1^*) \), \( (a_1^*, b_1^*) \) \( \psi (a_1^* \ldots a_n^*, b_1^* \ldots b_n^* e) \), as required.

5.5 STRUCTURE THEOREM FOR ALGEBRAS IN \( \mathcal{G} \).

An algebra is in the class \( \mathcal{G} \) iff it is a stable isotopy of an algebra in the class \( \mathcal{G}_0 \). The structure of an algebra in the class \( \mathcal{G}_0 \) is essentially that of a module over a ring.

Proof. Recall that a \( F \)-algebra is in \( \mathcal{G}(F(\mathcal{G})) \) iff there is a congruence centreing its direct square. Proposition 5.2 then shows that any stable isotopy of an algebra in \( \mathcal{G} \) is also in \( \mathcal{G} \). Conversely suppose that algebra \( B \) is in \( \mathcal{G} \).

Let \( \psi \) centre \( \psi (B) = B \times B \). Let \( K_1, K_2 \) respectively be the congruences \( \ker_1, \ker_2 \) as in the proof of Theorem 5.3. Then \( B \times B \times B = K_1 \times K_2 = K_1 \times \psi \).

By Proposition 5.4, \( K_1 \supset K_1 = (B \times B) \ker_2 = (B \times B) \ker_2 \).

But \( (B \times B) \ker_2 \supset B \) and \( (B \times B) \ker_2 \) has singleton subalgebra \( B \).

Suppose \( A \) in \( \mathcal{G}_0 \) has singleton subalgebra \( \{0\} \).

By the remarks after Proposition 5.2, there is an operation \( + \) on \( A \) making it an abelian group \( (A,+\{0\}) \) with \( 0 \) as identity. A binary operation \( + \) and a nullary operation "select \( 0 \)" are induced on every element of the subvariety \( \mathcal{G}_A \) of \( \mathcal{G} \) generated by \( A \) . Adjoint them to the operator domain \( \Omega \) of \( \mathcal{G}_A \) to make a new variety \( \mathcal{G}_A \). If \( \psi \) centre the \( F \)-algebra \( A \times A \), then by definition of \( + \) it also centre the \( \mathcal{G}_A \)-algebra \( A \times A \).

Let \( T \) be the set of translations of the \( \mathcal{G}_A \)-algebra \( A \) fixing \( 0 \).

If \( \omega \in \Omega \), \( \varphi (x, y) \) \( \psi (x, y) \) implies \( \varphi (x y, \omega) = \varphi (x, y) \psi (x) \), so that \( \psi (x, y) = x y + y \). \( T \) becomes a subring of the ring of endomorphisms of the abelian group \( (A,+\{0\}) \).

It follows that if \( \omega \in \Omega \), \( \psi (B) = B \) is an \( n \)-ary operation, then \( \psi (x_1, \ldots, x_n) = x_1 + x_2 + \cdots + x_n \omega \), where the mappings \( A \to A ; x_1 \mapsto 0 \cdots x_n \omega \) are in \( T \).

Thus the structure of \( A \) as a \( F \)-algebra is determined precisely by its structure as a \( T \)-module.

5.6 COROLLARY If two \( \mathcal{G}_0 \)-algebras are stably isotopic, then they are isomorphic.

Proof. Suppose \( B \) and \( C \) are \( \mathcal{G}_0 \)-algebras with a stable isotopy \( \psi : B \to C \). Let \( \{0\} \), \( \{f\} \) be singleton subalgebras of \( B \), \( C \) respectively. By the remarks after Proposition 5.2, there is an operation \( + \) on \( C \) making \( (0,+f) \) an abelian group with identity \( f \).

Suppose \( ee = g \). Then from Structure Theorem 5.5, the mapping \( B \to C ; b \mapsto b e - g \) is a stable isotopy.

For since \( e \) is a stable isotopy, \( \psi (\omega) \in \Omega \), \( \{0\} \) is a singleton subalgebra \( B \).

\( b_1, b_2 \in B \), \( b_1 \cdots b_n \omega = b_1 \cdots b_n \omega + a_n \).

Then \( (b, e - g) \cdots (b, e - g) \omega = b_1 \cdots b_n \omega - g \cdots \omega \omega = b_1 \cdots b_n \omega - (a_n + \cdots + a_n) \omega \), so that \( b \mapsto b e - g \) is a stable isotopy. Since \( ee = g = f \), \( b \mapsto b e - g \) is an isomorphism, again by the remarks after Proposition 5.2.
Up to this point no finiteness conditions have been placed on the $\mathbb{Z}$-algebras appearing. This was why Theorem 5.3 was stated in a form not involving $[\mathbb{Z}]$, the monoid of isomorphism classes of finite $\mathbb{Z}$-algebras. The Cancellation Theorem 5.7, however, requires some finiteness condition because it uses a unique factorisation theorem in its proof. It is then natural to state it in a form involving $[\mathbb{Z}]$.

5.7 CANCELLATION THEOREM For two finite $\mathbb{Z}$-algebras $B, C$, $[B] = [C]$ if $B \sim C$.

Proof. Theorem 5.3 shows $B \sim C \Rightarrow [B] = [C]$.

The converse follows in three steps (a), (b), (c).

All algebras appearing are finite. Note that in the notation of Theorem 5.3, if $B$ is finite then so are $C$ and $D$.

(a) For $Z_1, Z_2 \in \mathbb{Z}$, $Z_1 \times B \sim Z_2 \times B$ and $Z_1 \sim Z_2 \Rightarrow B \sim D$.

By the Structure Theorem 5.5, $Z_1 \times Z_2 \times \mathbb{Z}_0 \sim Z_1 \times Z_2 \times \mathbb{Z}_0$.

Thus $Z_1 \sim Z_2 \sim \mathbb{Z}_0$.

(b) For $Z_1, Z_2 \in \mathbb{Z}$, $Z_1 \times B \sim Z_2 \times D$ and $B \sim D \Rightarrow B \sim D$.

By Theorem 5.3, $Z_1 \times \mathbb{Z}_0 \sim Z_2 \times \mathbb{Z}_0$.

Thus $Z_1 \sim Z_2 \sim \mathbb{Z}_0$.

Now $Z_0 \sim \text{Anat}^{\mathbb{Z}_0} \times \text{Anat}^{\mathbb{Z}_0} \sim \text{Anat}^{\mathbb{Z}_0} \times \text{Anat}^{\mathbb{Z}_0}$.

Since $Z_0$ is in the class of $\mathbb{Z}_0$, all the factors are.

By Proposition 5.4, $\text{Anat}^{\mathbb{Z}_0} \sim \text{Anat}^{\mathbb{Z}_0}$.

By Corollary 5.6, $\text{Anat}^{\mathbb{Z}_0} \sim \text{Anat}^{\mathbb{Z}_0}$.

Hence $\text{Anat}^{\mathbb{Z}_0} \sim \text{Anat}^{\mathbb{Z}_0}$, from the Structure Theorem 5.5 and the usual cancellation theorem for finite groups with operators [e.g. 8, Theorem 3.11].

Then by Proposition 5.4,

$$\text{Anat}^{\mathbb{Z}_0} \sim \text{Anat}^{\mathbb{Z}_0} \sim \text{Anat}^{\mathbb{Z}_0} \sim \text{Anat}^{\mathbb{Z}_0}$$

Thus $B \sim \text{Anat}^{\mathbb{Z}_0} \sim \text{Anat}^{\mathbb{Z}_0} \sim \text{Anat}^{\mathbb{Z}_0}$.

So to prove (a), it is sufficient to prove (a').

(a') For $Z_1, Z_2 \in \mathbb{Z}$, $Z_0 \sim Z_1 \times Z_2 \times \mathbb{Z}_0$ and $Z_0 \sim Z_2 \times \mathbb{Z}_0$.

Express $B = B_1 \times B_2$, $D = D_1 \times D_2$, where $B_1, D_1 \in \mathbb{Z}$ and $B_2, D_2$ have no indecomposable factors in $\mathbb{Z}$.

(c) Let $Z_0 \sim Z_1, Z_0 \sim Z_2$, $Z_0 \times B \sim Z_1 \times B$, $Z_0 \times D \sim Z_2 \times D$.

Then $B_1 \sim Z_1$, $B_2 \sim Z_2$.

complement notation as before Theorem 5.3.

It follows by decomposing $a, b, c, d$ into indecomposables,
\( \beta_1 \sim \beta_2 \) and \( \delta_1 \sim \delta_2 \) - there are no cross-terms since \( B_n \) and \( D_n \) have no factors in \( \mathbb{Z} \).

Thus \( Z_B \sim Z_D \), by Proposition 5.4.

Now \( B_n \times Z_B \times Z_1 \equiv D_n \times Z_2 \times Z_2 \cong A_n \), say,

where \( A \times A = B_n \times Z_B \times Z_1 \sim \delta_n \times \xi_1 \), \( \xi_1 \times \xi_2 \), \( \eta \sim E \sim B_n \), \( \eta \sim E \sim D_n \), \( \eta \sim E \sim Z_2 \), \( \eta \sim E \sim Z_2 \).

Again applying the Unique Factorisation Theorem 4.6,

\[ \begin{align*}
\tilde{\beta} &= \tilde{\beta} \sim \tilde{E} \sim B_n, \\
\tilde{\delta} &= \tilde{\delta} \sim \tilde{E} \sim D_n, \\
\tilde{\xi_1} &= \tilde{\xi_1} \sim \tilde{E} \sim \eta_1, \\
\tilde{\xi_2} &= \tilde{\xi_2} \sim \tilde{E} \sim \eta_2, \\
\tilde{\gamma_1} &= \tilde{\gamma_1} \sim \tilde{E} \sim \gamma_1, \\
\tilde{\gamma_2} &= \tilde{\gamma_2} \sim \tilde{E} \sim \gamma_2,
\end{align*} \]

with \( \tilde{\beta} \sim \tilde{\delta} \sim \tilde{E} \sim \xi_1 \), \( \tilde{\beta} \sim \tilde{\delta} \sim \tilde{E} \sim \xi_2 \), \( \tilde{\gamma_1} \sim \tilde{\gamma_2} \sim \tilde{E} \sim \gamma_1 \), \( \tilde{\gamma_1} \sim \tilde{\gamma_2} \sim \tilde{E} \sim \gamma_2 \), and \( \beta_n \sim \tilde{\beta} \sim \delta_n \).

there are again no cross-terms in \( \beta_n \) or \( \delta_n \).

Thus \( Z_B \times Z_1 \sim Z_2 \times Z_2 \). Since \( Z_B \sim Z_2 \), \( Z_1 \sim Z_2 \) follows by (a).

(b) is proved.

(c) \( B \times C \equiv D \times E \) and \( B \equiv D \equiv C \equiv E \).

(c) clearly completes the proof of the theorem.

It is proved by induction on the number of indecomposable non-\( \mathbb{Z} \) factors in \( B \times C \times D \times E \). If \( 0 \), \( E \in \mathbb{Z} \), it follows by (b).

Otherwise, let \( A \equiv B \times C \equiv D \times E \), \( A \times A = \beta \equiv \delta \equiv \xi \), \( \beta \equiv \delta \equiv \xi \equiv \eta \equiv \gamma \).

From the Unique Factorisation Theorem 4.6,

\[ \begin{align*}
\beta &= \beta \sim \beta \sim \beta \sim \beta, \\
\delta &= \delta \sim \delta \sim \delta \sim \delta, \\
\gamma &= \gamma \sim \gamma \sim \gamma \sim \gamma, \\
\xi &= \xi \sim \xi \sim \xi \sim \xi.
\end{align*} \]

By Proposition 5.4, \( \beta \sim \beta \sim \beta \sim \beta \).

By Theorem 5.3, \( Z \in \mathbb{Z} \). \( Z \times \beta \beta \beta \beta \equiv Z \times \beta \beta \beta \beta \equiv Z \times \beta \beta \beta \beta \).

Now \( Z \times \beta \beta \beta \beta \times \beta \beta \beta \beta \equiv Z \times \beta \beta \beta \beta \equiv Z \times \beta \beta \beta \beta \).

Since \( Z \times B \times Z \times D \) has fewer non-\( \mathbb{Z} \) factors than \( B \times C \times D \times E \), it follows by induction that \( \beta \beta \beta \beta \sim \beta \beta \beta \beta \).

Then \( \beta \beta \beta \beta \sim \beta \beta \beta \beta \sim \beta \beta \beta \beta \) and \( \beta \beta \beta \beta \sim \beta \beta \beta \beta \).

imply \( C \equiv \beta \beta \beta \beta \) and \( \beta \beta \beta \beta \sim \beta \beta \beta \beta \sim \beta \beta \beta \beta \sim \beta \beta \beta \beta \sim \beta \beta \beta \beta \equiv E \), as required. \]
6. QUASIGROUPS AND CENTRALITY

A **quasigroup** \((Q, \cdot)\) is a set \(Q\) with a binary operation \(\cdot\) called **multiplication** such that in the equation \(x \cdot y = z\) any two elements determine the third uniquely. It follows that the mappings \(R(x) : Q \to Q; q \mapsto q \cdot x\) and \(L(x) : Q \to Q; q \mapsto x \cdot q\) are permutations of the set \(Q\).

The subgroup \(\langle R(x), L(x) \mid x \in Q \rangle\) of the group of permutations of \(Q\) generated by all these mappings is called the **multiplication group** \(\text{Mit} Q\) of \(Q\). In universal-algebra terms, if \(x/y = xk(y)^{-1}\) and \(x \cdot y = yL(x)^{-1}\), then \(\text{Mit} Q\) is just the group of translations of \((Q, \cdot, /, \setminus)\). \(\text{Mit} \) is not functorial, but epimorphisms \(e : Q_1 \to Q_2\) of quasigroups do induce epimorphisms \(\text{Mit} e : \text{Mit} Q_1 \to \text{Mit} Q_2\) of groups [cf. 4, Lemma IV.1.3].

Quasigroups are Mal’cev algebras by virtue of the derived operation \(F(x, y, z) = ((x/y)\setminus(x/z))\). This enables one to apply the work of Sections 1 to 5 to the study of quasigroups. (Indeed that work arose first in the quasigroup context.) In Sections 7 and 8 centrality is used to begin a study of the relationship between a finite quasigroup and its multiplication group. This section treats three isolated topics linking centrality and quasigroup theory. The first, which is useful later, is the connection between multiplication groups and stable isotopy.

6.1 PROPOSITION If \((P, +)\) is a quasigroup with a singleton subalgebra (idempotent), and \((Q, \cdot)\) is any stable isotope of \(P\), then \(\text{Mit} P \cong \text{Mit} Q\).

**Proof.** Let the idempotent of \(P\) be \(e\).

Let \(R_p(x) : P \to P ; p \mapsto p + x, L_p(y) : Q \to Q; q \mapsto y \cdot q\), etc. Suppose without loss of generality that \(P = Q\) and the stable isotopy is just the identity mapping. Define a derived operation \(+\) on \(P\) by \(p_1 + p_2 = (p_1R_p(e)^{-1}) \cdot (p_2L_p(e)^{-1})\). \((P, +, e)\) is a loop known as the **corresponding loop or gleam** of \(P\).

From the definition of stable isotopes, there is a member \(p\) of \(e^S(P)\) such that \(x \cdot y = p \cdot (x+y)\). Then \(xR_p(y) = p + (x+y) = (e+pR_p(e)^{-1}) \cdot (x+y) = (e+x) \cdot (pL_p(e)^{-1} + y) = xR_p(pL_p(e)^{-1} + y)\).

Thus \(R_p(y) = R_p(pL_p(e)^{-1} + y)\); similarly \(L_p(y) = L_p(pR_p(e)^{-1} + y)\).

Since \(pR_p(e)^{-1}, pL_p(e)^{-1} \in e^S(P)\), the mappings \(y \mapsto pL_p(e)^{-1} + y\) and \(y \mapsto pR_p(e)^{-1} + y\) are invertible.

The result follows.}

Among non-associative algebras the variety \(\mathfrak{g}\) of quasigroups plays the fundamental role played by the variety \(\mathfrak{g}\) of groups among associative algebras. The counterpart of the variety \(\mathfrak{g}\) of abelian groups is then the variety \(\mathfrak{g}(\mathfrak{g})\). The next result, paraphrasing a theorem of Mine [11], gives an example of this analogy.
6.2 THEOREM Let $Q$ be the free $\mathbb{Z}(g)$-algebra on one generator. By the Structure Theorem 5.5, $Q$ is stably isotopic to $F = Q \times Q / Q$. Let $H$ be the subgroupoid of $F$ generated by a non-idealotent element under the multiplication of $F$. Then $H$ indexes non-associative powers.

If $g$ is replaced by $\mathbb{Z}$, $H$ is replaced by the natural numbers $N$, which index associative powers.

Proof. By [11, Theorem 7.2] and the second half of the Structure Theorem 5.5.

Finally, the topic of this section is finite entropic quasigroups. These were introduced by Murdoch [12] under the confusing name of "abelian quasi-groups". An entropic quasigroup is a quasigroup satisfying the entropic law
\[(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d).
\] Let $E$ denote the variety of entropic quasigroups. A finite quasigroup $Q$ is in $E$ iff the multiplication $G: Q \times Q \to Q$ is a quasigroup morphism.

Murdoch gave three structure theorems in [12] for finite entropic quasigroups. Two of these theorems follow directly from the work of Sections 1 to 5.

Murdoch's Second Structure Theorem showed how an entropic quasigroup having an idealotent could be obtained by tampering with an abelian group. Now every subquasigroup $H$ of an entropic quasigroup $Q$ is normal in $Q$, since $(H \cdot x), (H \cdot y) = (H \cdot x), (y) = H \cdot (x, y)$, so that (right) cosets of $H$ form a quasigroup. Proposition 2.5 then shows that

$H$ is a subvariety of $E(Q)$. The Structure Theorem 5.5 may thus be used to describe a quasigroup $Q$ in $E$ having idempotent $Q$ in terms of the abelian group $(Q, +, 0)$ and its endomorphisms. This description is that given by Murdoch's Second Structure Theorem.

Murdoch's First Structure Theorem decomposed a finite entropic quasigroup $Q$ into a direct product of two quasigroups. Define quasigroup morphism $\rho : Q \to Q; x \mapsto x^Q$ where $x \cdot x^Q = x$. $x^Q$ is called the right unit of $x$.

Murdoch's decomposition produced one factor in which every element was a right unit and a direct complement of that factor having a unique idempotent. His proof considered extensions of the limit of the series $Q \to Q \to Q^2 \to \ldots$.

The theorem may be proved more directly by applying Pitting's Lemma 3.1 to the morphism of congruences $\psi : Q \times Q \to Q \times Q; (x, y) \mapsto (x, x^Q \cdot y)$. Finally, the automorphisms of abelian groups and of quasigroups appearing in [12, Theorem 10] and [12, Section 10] respectively are examples of those mentioned in the remarks after Proposition 5.2.
7. STABILISERS IN MULTIPLICATION GROUPS OF FINITE QUASIGROUPS

The multiplication group \( G = \text{MltQ} \) of a finite quasigroup \( Q \) is a permutation group on the set \( Q \). In this section normality properties of the stabilizer \( \text{Stab}_h \) of an element \( h \) of \( Q \) are examined in relation to the algebraic structure of the quasigroup \( Q \).

7.1 DEFINITION A quasigroup is said to be abelian, or in the class \( \mathbf{A} \), iff it satisfies both the commutative and associative laws, and is thus an abelian group.

7.2 THEOREM \( \forall h \in Q \). \( \text{Stab}_h \triangleleft G \) iff \( Q \in \mathbf{A} \).

PROOF. By Cayley’s Theorem, an abelian quasigroup is isomorphic to its multiplication group. Thus if \( Q \in \mathbf{A} \), \( \text{Stab}_h \triangleleft G \), and so \( \text{Stab}_h \triangleleft G \) for all \( h \) in \( Q \).

Conversely, suppose \( \forall h \in Q \). \( \text{Stab}_h \triangleleft G \).

From the definition of a quasigroup, \( G \) is transitive on \( Q \), so that all the stabilizers are conjugate, and \( \forall x \in Q \), \( \text{Stab}_x = \{1\} \). Then \( |Q| = |\text{Stab}_x| = |G| \).

The mapping \( R : Q \to G \); \( x \mapsto R(x) \) injects.

Since \( Q \) is finite, it bijects; let \( R(e) = 1 \).

Then \( e \text{R}(e) = ee = eR(e) = e \), so that \( \text{Stab}_e \cong \{1\} \).

\( \forall x, y \in Q \), \( eR(x)R(y) = (ex)y = xy = eR(xy) \).

Thus \( R(x)R(y)R(xy)^{-1} \in \text{Stab}_e = \{1\} \). Hence \( R(x)R(y) = R(xy) \).

\( R \) is an isomorphism of \( G \) with the group \( Q \).

\( \forall x \in Q \), \( xR(x)L(x)^{-1} = x \), \( R(x)R(x)^{-1} \in \text{Stab}_x = \{1\} \). \( \Rightarrow Q \in \mathbf{A} \).}

7.3 COROLLARY \( Q \in \mathbf{A} \) iff \( \text{MltQ} \in \mathbf{A} \).

7.4 COROLLARY No Hamiltonian group can be the multiplication group of a quasigroup.

PROOF. If \( Q \) were Hamiltonian, then \( \text{Stab}_h \triangleleft G \) for all \( h \in Q \).

By Theorem 7.2, \( Q \) would be abelian, and then by Corollary 7.3, \( G \) would also be abelian. But Hamiltonian groups are not abelian.

Corollary 7.4 is rather interesting. It might be thought that the concept of quasigroup is so weak that any group could be the multiplication group of some quasigroup (just as, for example, any group can be the automorphism group of a graph).

Corollary 7.4 shows that this is not so. It opens up the problem of finding precisely what groups can be multiplication groups of quasigroups. At the time of writing no groups other than Hamiltonian groups have been denied this possibility.

Theorem 7.2 admits a generalization to the case \( \text{Stab}_h \) subnormal in \( G \) (notation: \( \text{Stab}_h \triangleleft G \) ), giving a result analogous to that obtained by Bruk [3, Section 1.6] for loops. This is Theorem 7.7. Some preliminaries are necessary.

A quasigroup \( Q \) is said to be ultramsoluble if it has a central series \( \widetilde{G} = \{1\} \leq \tilde{V}_1 \leq \tilde{V}_2 \leq \ldots \leq \tilde{V}_n = Q \times Q \) such that \( \tilde{V}_i / \tilde{V}_{i+1} \in \mathbf{A} \) for \( i = 1, \ldots, n \). The class \( \mathbf{U} \) of ultramsoluble quasigroups forms a variety.
7.5 PROPOSITION. An unsolvable quasigroup \( Q \) has a unique idempotent.

**Proof.** This follows by induction on \(|Q|\). Let \( Q \in \mathcal{U} \) have central series \( Q = Q_0 < Q_1 < \ldots < Q_n = Q \) with \( Q_{i+1}/Q_i \) nilpotent for \( i = 1, \ldots, n \).

Suppose the proposition is true for unsolvable quasigroups of smaller order than \( Q \). Then it is true for \( Q_{i+1}/Q_i \), so that \( V_i \) has unique class \( q^V \) such that \( q^V \) is a subalgebra of \( Q \).

By Proposition 2.4(i), \( q^{V_i} = q^V \cdot q^V \).

Now \( V_i/Q \cong (q^V \times q^V)/q^V \in \mathcal{U} \).

By Corollary 7.3, \( NIL(q^V \times q^V)/q^V \in \mathcal{U} \).

Then by Proposition 5.5, Proposition 6.1, and Corollary 7.3, it follows that \( q^V \) is abelian, and thus contains a unique idempotent. But if \( x \) is any idempotent of \( Q \), \( x^V \) is a subalgebra of \( Q \), so \( V_1 \) is \( q \) and \( x \) is the unique idempotent.

7.6 PROPOSITION. \( x, y \in Q \), \( H_y(x) = \bigcup_{t \in \langle y \rangle} g_x p(x, t) \).

**Proof.** \( \{p(x, t) | t \in \langle y \rangle \} \) is a transversal to \( G_x \) in \( G \).

Let \( T \) be the subtransversal to \( G_x \) in \( H_y(x) \).

Then \( t \in T \iff x p(x, t) G_x = x p(x, t) \iff t G_x = t \).

Now for the generalisation of Theorem 7.2.

7.7 THEOREM. \( \exists h \in Q \), \( q_h \Rightarrow 0 \) \( \iff \) \( Q \in \mathcal{U} \).

**Proof.** It will first be shown by induction on the order of \( Q \) that \( \exists h \in Q \), \( q_h \Rightarrow 0 \) \( \Rightarrow \) \( Q \in \mathcal{U} \).

Suppose the result true for all quasigroups of order less than \(|Q|\), and suppose \( h \in Q \), \( q_h \Rightarrow 0 \).

Since \( G \) is transitive on \( Q \) all stabilisers are subnormal.

Let \( V = \{(x, y) \in Q \times Q | y q_h x = y \} \).

By Proposition 7.6 and the subnormality of stabilisers, \( Q \subseteq V \).

(a) \( V \subseteq Q \times Q \):

Fix \( h \in Q \).

Let \( (x_1, x_2) \in V \), i.e. \( y_1 q_{x_1} x_1 = y_1 \), \( i = 1, 2 \).

It is required to show that \( (y_1, y_2) q_{x_1} x_2 = y_1 y_2 \).

Now \( q_{x_1} = \rho(h, x_1)^{-1} \cdot q_h \cdot \rho(h, x_1) \).

so \( y_1 q_{x_1} x_1 = y_1 \), say, with \( y_1 \in \langle q_h \rangle \).

Then \( y_1 = x_1 q_{x_1} L(h)^{-1} \cdot x_1 L(h) \).

Thus \( y_1 y_2 = (x_1 q_{x_1} L(h)^{-1}, x_1 q_{x_1} L(h)^{-1}) \).

Since \( x_1 \in \langle q_h \rangle \), \( L(h) \) is \( H_q(h) \). But also \( q_x \in \langle q_h \rangle \).

so \( x q_{x_1} L(h) \) is \( x_1 q_{x_1} L(h) \).

Thus \( y_1 y_2 = x_1 q_{x_1} x_1 L(h)^{-1} \).

so that \( (y_1, y_2) q_{x_1} x_2 = y_1 y_2 \), as required.

(b) \( V \subseteq \langle q \rangle \):
Suppose \((x_1,y_1), (x_2,y_2) \in V\).

Let \((x_3,y_3) = (x_1,y_1)R((x_2,y_2))^{-1} \cdot (x_2,y_2)\).

By \((a), (x_3,y_3) \in V\). Let \(q, r \in Q\).

Then \(qR(x_1)^{-1}x_1, qR(x_1)^{-1}y_1) = qR(x_2)^{-1}x_2, qR(x_2)^{-1}y_2\),

so that \(Q(x_1,y_1), Q(x_2,y_2) = Q(x_3,y_3)\). It follows that

\[(x,y) \rightarrow (x',y') \rightarrow Q(x,y) \rightarrow Q_{nat}V_{i-1}\] defines a congruence \(\sim V\) on \(V\).

By Proposition 2.2, \(V\) is a congruence on \(Q\).

By Proposition 2.3, \(V\) centres \(V\).

\(c) \sim V \in A:\)

By Proposition 1.2, \(\sim V \in A\).

Let \(L(xR(x^{-1})) \in G\). 

Then if \((x,y) \in V\), \(Q(x,y) = (xR(x^{-1})L(xR(x^{-1})))\).

\[(x,y)^{\sim V} = (xL(xR(x^{-1})))\] 

\[=(x,y)^{\sim V}.

\(a, b \in Q, \ (a)R(b)R((a,b)L(xR(x^{-1})))^{-1} \in G\).

Thus if \((a,b), (b,d) \in V\),

\[[(x,y)^{\sim V}]((a,b)^{\sim V}) = (x,y)^{\sim V}[(x,a)\overline{y}, (b,d)^{\sim V}]\]

\[=(x,y)^{\sim V}[(a,b)^{\sim V}]\].

\(\sim V\), being an associative quasigroup, is a group.

Being in \(A\), it is abelian.

The hypothesis "\(\exists h \in Q, G \times G\) is preserved under epimorphisms. Thus \(Q_{nat}V\) is ultrarisible, by induction.

\(\) It follows that \(Q\) is ultrarisible.
In this section the study of the relationship between a finite quasigroup \( Q \) and its multiplication group \( G \) is continued by correlating centrality of the quasigroup and simplicity of the multiplication group. This leads to Theorem 8.5 which begins a classification of the quasigroups of prime order. Stabilisers once again play an important part, and the first result is a description of the elements of the stabiliser \( G_h \) of \( h \) in \( Q \) analogous to that obtained by Bruck [4, Lemma IV.1.2] for loops.

The natural setting for this description is the groupoid (in the sense of "category with all arrows invertible" and not "set with binary operation" as in the statement of Theorem 6.2) consisting of vertices corresponding to elements of \( Q \) together with arrows \( \sigma \) labelled by \( \sigma \in G \) from vertex \( x \) to vertex \( y \) where \( x\sigma = y \). From the definition of quasigroup, there are unique arrows labelled \( R(\cdot) \) and \( L(\cdot) \) between any two (possibly identical) vertices. The stabiliser \( G_h \) of a vertex \( h \) then consists of the labels of the arrows in the vertex group of the groupoid at the vertex \( h \).

For any \( x, y \) in \( Q \), define
\[
T_h(x) = R(xR(h)L(h)^{-1})L(x)^{-1} ;
\]
\[
R_h(x, y) = R(x)R(y)L((xR(h), y)L(h)^{-1})^{-1} ;
\]
and symmetrically \( L_h(x, y) = L(x)L(y)L((y, xR(h))R(h)^{-1})^{-1} \).
8.1 PROPOSITION \( \varrho_h = \langle \varrho_h(x), \varrho_h(x), \lambda_h(x, y) \mid x, y \in Q > \).

**Proof.** Let \( \varrho_h = \langle \varrho_h(x), \varrho_h(x, y), \lambda_h(x, y) \mid x, y \in Q > \).

Clearly \( \varrho_h \subseteq \varrho_h \).

Conversely, suppose \( a \in \varrho_h \). Then \( a = a_1 \ldots a_n \), where \( a_j \) is of the form \( R(q_j)^{-1} \) or \( L(q_j)^{-1} \), \( q_j \in Q \).

It will be shown by induction on \( n \) that any \( a \) can be expressed as \( a = \nu R(q) \), with \( \nu \in \varrho_h \), \( q \in Q \).

For \( R(x)R(y) = R_h(x, y)R((xL(h)y)H(h)^{-1}) : \)

\[
R(x)R(y)^{-1} = R_h((hx)R(y)^{-1}H(h)^{-1}, y)^{-1}R((hx)R(y)^{-1}L(h)^{-1}) :
\]

For \( R(x)L(y) = \)

\[
T_h((y, (hx)R(y)^{-1}H(h)^{-1}))R_h((hx)R(y)^{-1}H(h)^{-1), y)^{-1}R_h((hx)R(y)^{-1}R(h)^{-1})^{-1} \cdot R((hx)R(y)^{-1}L(h)^{-1}) ;
\]

For \( R(x)L(y)^{-1} = \)

\[
T_h((y, (hx)R(y)^{-1}H(h)^{-1}))R_h((hx)R(y)^{-1}H(h)^{-1), y)^{-1}R_h((hx)R(y)^{-1}R(h)^{-1})^{-1} \cdot R((hx)R(y)^{-1}L(h)^{-1}) ;
\]
In particular $1 = R_h(hL(h)^{-1},x)^{-1}R(hL(h)^{-1})$ is expressed in the required form, and the general case follows by induction using the formulas. The expression $a = cR(q)$ is unique, for $q$ is specified uniquely by $ha = bq$, and then $c = cR(q)^{-1}$.

If $a \in G_h$, then $a = cR(hL(h)^{-1})$ with $c \in G_h$.

But $R(hL(h)^{-1}) = R_h(hL(h)^{-1},y)$ for any $y$, and no $a \in G_h$.

Thus $G_h \subseteq G_h$.

8.2 DEFINITION The derived congruence $K$ of a quasigroup $Q$ is the intersection of all congruences $\psi$ on $Q$ such that $\text{Nat}\psi \in K$.

Proposition 8.1 enables an explicit description of the derived congruence to be given in terms of stabilisers in $G = \text{Nat}Q$.

8.3 PROPOSITION $K = \langle Q(\cup Q \times \cup Q) \rangle$.

Proof. By Proposition 8.1, any element of $G_h$ can be expressed as a product of $R_h(x_1,x_2)$, $L_h(x_1,x_3)$, or their inverses. Write such products generically as $R_h(x_1,\ldots,x_m)$, $L_h(y_1,\ldots,y_n)$.

Suppose $V$ is a congruence on $Q$, and $\text{Nat}V \in K$.

Let $a = \text{Nat}V$. Then $a \in Q$, $(\text{Nat}V)_a = \{1\}$.

So for all $a$ in $Q$ and stabilisers $R_h(x_1,\ldots,x_m)$, $L_h(y_1,\ldots,y_n)$,

$q \alpha_{x_0}(x_1,\ldots,x_n) = a \quad q \alpha_{y_0}(y_1,\ldots,y_n) = a$.

Thus $\langle q \alpha_{x_1}(x_1,\ldots,x_m) \rangle = \langle q \alpha_{y_1}(y_1,\ldots,y_n) \rangle$.

Now $\langle q \alpha \rangle(1,\ldots,\alpha_{y_0}(y_1,\ldots,y_n)) = \langle q \alpha \rangle(1,\ldots,\alpha_{x_0}(x_1,\ldots,x_n))$ and $\langle q \alpha \rangle(1,\ldots,\alpha_{y_0}(y_1,\ldots,y_n)) = \langle q \alpha \rangle(1,\ldots,\alpha_{x_0}(x_1,\ldots,x_n))$.

Thus $\langle q \alpha \rangle(1,\ldots,\alpha_{x_0}(x_1,\ldots,x_m)) = \langle q \alpha \rangle(1,\ldots,\alpha_{y_0}(y_1,\ldots,y_n))$.

Conversely, let $U = \langle Q(\cup Q \times \cup Q) \rangle$.

By Proposition 2.2, $U$ is in a congruence on $Q$. Let $\psi = \text{Nat}U$.

Let $q, y \in Q \uparrow, \alpha \phi(y_1,\ldots,y_n) \in Q \downarrow y$.

Now $\langle q \alpha \phi(y_1,\ldots,y_n) \rangle(1,\ldots,\alpha_{y_0}(y_1,\ldots,y_n)) \in \langle Q(\cup Q \times \cup Q) \rangle$.

Thus $\psi \phi(y_1,\ldots,y_n) = \psi q \alpha \phi(y_1,\ldots,y_n)$.

Hence $\langle q \alpha \phi(y_1,\ldots,y_n) \rangle \subseteq U$.

Thus $\psi \phi(y_1,\ldots,y_n) = \psi q \alpha \phi(y_1,\ldots,y_n)$.

Hence $K \subseteq U$, and thus equality as required.

With these preliminaries done, it is now possible to give the basic relationship between centrality of quasigroups and simplicity of multiplication groups.

8.4 THEOREM If $Q$ is a quasigroup in $K$, then neither $\text{Nat}Q$ nor $(\text{Nat}Q)^{-1}$ can be simple non-abelian.

Proof. In view of the Structure Theorem 5.5 and Proposition 6.1, it is sufficient to consider a quasigroup $Q$ in $K$ having idempotent $e$. Let $(\text{Nat}Q,+,e)$, or just $B$, denote the loop of $Q$ as defined in the proof of Proposition 6.1.

By the Structure Theorem 5.5, $B$ is a $(\text{Nat}Q)_e$-module.

Now $\text{Nat}Q$ certainly cannot be simple non-abelian, for it has the abelian normal subgroup $\text{Nat}B$.

Let $K$ be the derived congruence of $Q$. Let $Q' = e^K$.

By Proposition 8.3, $K = \langle Q(\cup Q \times \cup Q) \rangle$.

Thus $Q' = \langle p(1-e) \mid p \in Q \rangle$.

Hence $Q' = e^K$.
p_1(1-a_1) \cdot p_2(1-a_2) = p_1(1-a_1)R + p_2(1-a_2)B = p_1R(1-a_1^2) + p_2B(1-a_1^2), 
Q' = B - (M_{l/2})_0.

Thus if q \in Q', j \in Q, a \in (M_{l/2})_0, q = p(1-a).

Let \( R_g(q) : B \to B; b \to b \circ q \).

If \( x \in Q, x(a, R_g(p)) = (x^2 - p) a + p = xR_g(q) \).

Hence \( R_g(q) \in (M_{l/2})' \).

Thus \( M_{l/2}(Q') \subseteq (M_{l/2})' \), indeed \( M_{l/2}(Q') \subseteq (M_{l/2})' \).

If \((M_{l/2})'\) is simple, then \( M_{l/2}(Q') \subseteq \{1\} \) or \((M_{l/2})'\).

Now \( M_{l/2}(Q') = \{1\} \to Q' = \{e\} \to Q \subseteq \frac{1}{2} \to M_{l/2} \subseteq \{1\} \to (M_{l/2})' = \{1\} \).

Again \( M_{l/2}(Q') = (M_{l/2})' \to (M_{l/2})' \subseteq \{1\} \). 

For quasigroups \( Q \) of prime order, the mutually exclusive possibilities "\( Q \subseteq \frac{1}{2} \)" and "\((M_{l/2})'\) single non-abelian" are the only ones, as the following application of a theorem of Galois shows.

**6.5 Theorem** If \( Q \) is a quasigroup of prime order \( p \), then either \( Q \subseteq \frac{1}{2} \) or \((M_{l/2})'\) is a simple non-abelian transitive permutation group on \( Q \).

**Proof.** First assume that \( Q \) has an idempotent \( e \).

The notations of Theorem 6.4 will be used.

Let \( C_n \) denote the cyclic group of order \( n \).

If \( Q' = \{e\} \), \( Q \subseteq \frac{1}{2} \), so \( Q \subseteq \frac{1}{2} \). Otherwise, \( Q' = Q \), \([M_{l/2}] > p \), and by primitivity \((M_{l/2})'\) is transitive on \( Q \).

If \((M_{l/2})'\) is not abelian, it is simple [6, Satz V.21.1].

If \((M_{l/2})'\) is abelian, then by Galois' Theorem [6, Satz II,5.6] \((M_{l/2})' \not\subseteq \{1\}, M_{l/2} = (M_{l/2})'\). \((M_{l/2})'\), \((M_{l/2})' \subseteq \{1\} \), and \( M_{l/2} \) on \( Q \) is similar to a group of affine transformations on \( Q' \).

Let the loop of \( Q \) be \( B \).

If \( B \subset Q \), then \( M_{l/2} \subseteq M_{l/2}(Q') = M_{l/2} \), and \((M_{l/2})_0 = \{R, B\} \), \( R \) and \( B \) being automorphisms of \( (B, +, e) \). Thus \( Q \subseteq \frac{1}{2} \).

Suppose then that \( B \not\subseteq Q \). Again, since \( M_{l/2} \subseteq M_{l/2}(Q') \), \( M_{l/2} \) on \( B \) must be of the form above given by Galois' Theorem. If there is a non- \( e \) \( x \) in \( B \) such that \( R_g(x) \in (M_{l/2})'\), then \( R_g(x) \) is of order \( p \), and so a \( p \)-cycle.

Hence \( B \subset Q \), a contradiction to the assumption.

Otherwise for all non- \( e \) \( x \) in \( B \), \( R_g(x) \not\subseteq (M_{l/2})' \).

Then \( R_g(x) \) for any \( x \) must fix some point, say \( y \).

Thus \( yx = y \), but \( ye = y \). Hence \( x = e \), another contradiction. The result is thus true for quasigroups with idempotents.

Now suppose \((Q, \cdot)\) is a general quasigroup of order \( p \).

If \((M_{l/2})'\) is not simple non-abelian, it must be shown that \( Q \subseteq \frac{1}{2} \). Fix \( a \in Q \). If \( a \) is an idempotent, the result follows as above. Otherwise, Galois' Theorem shows that \( M_{l/2} \) contains a cycle \( \alpha \) of length \( p \).

Without loss of generality, \( (a, ab) = a \), for if not, \( \alpha \) may be replaced by an appropriate power.

Define \((Q, \cdot)\) by \( x \cdot y = (x, y)^{\alpha} \).

Then \((Q, \cdot)\) has the idempotent \( a \).

Now \( x \in M_{l/2}(Q, \cdot) \), and so \( M_{l/2}(Q, \cdot) \subseteq M_{l/2}(Q, \cdot) \).

Thus \( M_{l/2}(Q, \cdot) \) is soluble, and from the above \((Q, \cdot) \subseteq \frac{1}{2} \).

Let \( A = (Q, \cdot) \), \( A \subseteq Q, \), and \( \beta \circ A \subseteq A \), \( \beta(b) = \beta^{-1} \).

Then \( A \) is the addition in \( A \), \( x \cdot y = (x, y)^{\beta^{-1}} = \beta(x, y) \).

\((Q, \cdot)\) is thus a stable isotope of \((Q, \cdot)\). By the Structure Theorem 5.5, \((Q, \cdot) \subseteq \frac{1}{2} \), as required. ]
REFERENCES


index

abelian - 54

Cancellation Theorem - 46
category of congruences - 24
central congruence - 10
central isomorphism - 33
Central Isomorphism Theorem - 33
central series - 18
centralise - 32
centre - 10,
centre congruence - 12, 15
centreing congruence - 32
Classical Exchange Theorem - 28
Classical Unique Factorisation Theorem - 29
cloop - 51
commutator - 18
corresponding loop - 51
derived congruence - 64
diagonal embedding - 9
direct product - 24
entropy law - 52
entropic quasigroup - 52
Exchange Theorem - 36

Fitting's Lemma - 25
Frattini subalgebra - 21
Grothendieck group - 30
Hamiltonian groups - 55
image - 24
indecomposable - 26
Jónsson-Tarski algebra - 11
kernel - 24
L( ) - 50
lower central series - 19
Mal'cev algebra - 12
morphism of congruences - 24
multiplication - 50
multiplication group - 50
nilpotent - 19
non-generator - 20
normal subalgebra - 16
P( , , ) - 12
projection - 24
Attention is drawn to the fact that the copyright of this thesis rests with its author. This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without the author's prior written consent.