Residually Small Varieties and Commutator Theory

by

Istine Rodseth Swart

Submitted in fulfilment of the requirements for the degree of Master of Science in the School of Mathematical and Statistical Sciences, University of Natal.

Durban
2000

Acknowledgements

The preparation of this thesis has taken several years during which I have had the help and encouragement of my family, friends, colleagues and fellow students. I thank them for their support, both moral and practical. I have been honoured to have the support, in particular, of two remarkable men:

Gert Swart, my husband, who understands the pursuit of dreams and

James Raftery, my supervisor, who has taught me more than Mathematics. It has been a great privilege to work with James, who has worked tirelessly in spite of difficult circumstances. My long association with him has served to increase my admiration for him as a mathematician, a teacher and a friend. I am grateful to him for his tact and patience and for the glimpse he has given me into the thrilling world of pure Mathematics.

I wish to thank Prof. Johan Swart and the Department of Mathematics and Applied Mathematics of Pietermaritzburg for their role in making this thesis possible. I am especially grateful to John Hearne for the use of his laptop computer and to Petrovius Horton for his gracious assistance with the diagrams. I thank the University of Natal and the National Research Foundation for their financial assistance.

Preface

The work described in this thesis was carried out under the supervision of Prof James G. Raftery, School of Mathematical and Statistical Sciences, University of Natal, Durban.

The thesis represents original work by the author and has not been submitted in any form to another University. Where use was made of the work of others it has been duly acknowledged in the text.

Abstract

Chapter 0

In this introductory chapter, certain notational and terminological conventions are established and a summary given of background results that are needed in subsequent chapters.

Chapter 1

In this chapter, the notion of a "weak conguence formula" [Tay72], [BB75] is introduced and used to characterize both subdirectly irreducible algebras and essential extensions. Special attention is paid to the role they play in varieties with definable principal congruences.

The chapter focuses on residually small varieties; several of its results take their motivation from the so-called "Quackenbush Problem" and the "RS Conjecture". One of the main results presented gives nine equivalent characterizations of a residually small variety; it is largely due to W. Taylor. It is followed by several illustrative examples of residually small varieties.

The connections between residual smallness and several other (mostly categorical) properties are also considered, e.g., absolute retracts, injectivity, congruence extensibility, transferability of injections and the existence of injective hulls. A result of Taylor that establishes a bound on the size of an injective hull is included.

Chapter 2

Beginning with a proof of A. Day's Mal'cev-style characterization of congruence modular varieties [Day69] (incorporating H.-P. Gumm's "Shifting Lemma"), this chapter is a self-contained development of commutator theory in such varieties. We adopt the purely algebraic approach of R. Freese and R. McKenzie [FM87] but show that, in modular varieties, their notion of the commutator $[\alpha, \beta]$ of two congruences α and β of an algebra coincides with that introduced earlier by J. Hagemann and C. Herrmann [HH79] as well as with the geometric approach proposed by Gumm [Gum80a], [Gum83].

Basic properties of the commutator are established, such as that it behaves very well with respect to homomorphisms and sufficiently well in products and subalgebras. Various characterizations of the condition "$(x, y) \in [\alpha, \beta]$" are proved. These results will be applied in the following chapters. We show how the theory manifests itself in groups (where it gives the familiar group theoretic commutator), rings, modules and congruence distributive varieties.

Chapter 3

We define Abelian congruences, and Abelian and affine algebras. Abelian algebras are algebras **A** in which $[A^2, A^2] = id_A$ (where A^2 and id_A are the greatest and least congruences of A). We show that an affine algebra is polynomially equivalent to a module over a ring (and is Abelian). We give a proof that an Abelian algebra in a modular variety is affine; this is Herrmann's Fundamental Theorem of Abelian Algebras [Her79]. Herrmann and Gumm [Gum78], [Gum80a] established that any modular variety has a so-called ternary "difference term" (a key ingredient of the Fundamental Theorem's proof). We derive some properties of such a term, the most significant being that its existence characterizes modular varieties.

Chapter 4

An important result in this chapter (which is due to several authors) is the description of subdirectly irreducible algebras in a congruence modular variety. In the case of congruence distributive varieties, this theorem specializes to Jónsson's Theorem.

We consider some properties of a commutator identity (C1) which is a necessary condition for a modular variety to be residually small. In the main result of the chapter we see that for a finite algebra **A** in a modular variety, the variety $V(\mathbf{A})$ is residually small if and only if the subalgebras of **A** satisfy (C1). This theorem of Freese and McKenzie also proves that a finitely generated congruence modular residually small variety has a finite residual bound, and it describes such a bound. Thus, within modular varieties, it proves the RS Conjecture.

Conclusion

The conclusion is a brief survey of further important results about residually small varieties, and includes mention of the recently disproved (general) RS Conjecture.

Contents

Introduction

G. Birkhoff showed in 1944 that every algebra in a variety V is a subdirect product of subdirectly irreducible algebras in V. Therefore, many properties of a variety can be established merely by establishing the same properties of the subdirectly irreducible algebras in the variety. For example, identities and quasi-identities that are true in the subdirectly irreducible algebras are true throughout the variety since subdirect products preserve identities and quasi-identities.

The fewer subdirectly irreducible algebras there are in V, the easier it is to describe the variety. This makes residually small (RS) varieties desirable since in such varieties V, the subdirectly irreducible algebras form a set; equivalently, there is an upper bound on the sizes of the subdirectly irreducible algebras in V. When this upper bound can be chosen finite, we say the variety has a *finite residual bound.* In this case if V also has only finitely many operations, then V must be finitely generated, i.e., generated as a variety by a single finite algebra. This thesis is a self-contained exposition on residually small varieties. The strength of the main result to be discussed is that it establishes a sufficient condition (with wide application) for the existence of a finite bound on the size of the subdirectly irreducible algebras in a residually small finitely generated variety.

The first part of the thesis is a discussion of various general properties of residually small varieties, based mainly on work done by W. Taylor, J. Baldwin, J. Berman, D. Higgs, B. Banaschewski and E. Nelson (c.1970). The thesis includes several results that are partial answers to the "Quackenbush Conjecture", formulated by R.W. Quackenbush [Qua71]. This conjecture claims that if a variety $V(\mathbf{A})$ generated by a finite algebra $\mathbf{A}$ (with finitely many operations) has arbitrarily large finite subdirectly irreducible algebras, then it must have an infinite subdirectly irreducible algebra.

In the mid-1980's, it was proposed in the so-called "RS Conjecture", that a residually small variety generated by a finite algebra should always have a finite residual bound. (This is a stronger claim than Quackenbush's Conjecture.) In 1996 R. McKenzie showed that, contrary to expectation, the RS Conjecture is false. He also proved a number of important results concerning the size of residual bounds.

This work contrasts with an important earlier result of R. Freese and McKenzie, namely that the RS Conjecture is true for congruence modular varieties (1981). This result is the aforementioned main theorem of the thesis. Thus, a finitely generated residually small and *congruence modular* variety has a finite residual bound, and the theorem includes a description of the bound.

This result was obtained via the development of a general "commutator" theory which includes elements of ring theory. The second part of this thesis examines aspects of this commutator theory that are prerequisite to the main result. The theory of commutators was introduced in the context of congruence permutable varieties by J.D.H. Smith (1976). It was developed for congruence modular varieties by J. Hagemann, C. Herrmann, H.-P. Gumm, Freese, McKenzie and others.

In this thesis we follow Freese and McKenzie's purely algebraic approach to the commutator as expounded in [FM87]. According to this approach, the commutator is a binary operation on the congruences of an algebra. It is a generalization of the commutator of a group and possesses all the corresponding abstract properties of the commutator of normal subgroups. It entails the notion of an "Abelian" algebra and a strong representation theorem (due to Herrmann) linking such algebras to modules over rings (1979). The main result of this thesis is an important application of the commutator theory: it depends on a further result of Freese and McKenzie showing that if a congruence modular variety V is residually small, it must satisfy a certain "commutator identity". Moreover, provided that V is finitely generated, the converse is also true. We present a proof of the main result and conclude the thesis with a summary of further recent advances in the theory of residually small varieties.

Chapter 0

Preliminaries

In this chapter we fix certain notational and terminological conventions and state the background results that will be needed in the chapters that follow. Occasionally, where a result is especially important to the sequel or where it is not easily located in the literature, we include a proof. For the most part, however, we omit proofs from this chapter, giving references instead to standard texts, particularly [BS81] and [Grä79]. We stress that these standard references are not usually the original sources of the results, but they contain directions to original sources.

0.1 Set Theoretic Prerequisites. We assume a basic knowledge of axiomatic set theory (see, e.g., [Men87]) such as the use of Zorn's Lemma and transfinite induction and recursion, as well as rudimentary ordinal and cardinal arithmetic.

We always denote set inclusion by $\subseteq$ and *proper* set inclusion by $\subset$. If A and B are sets then $\mathcal{P}(A)$ denotes the power set (i.e., the set of all subsets) of A, $|A|$ is the cardinality of A, $A \setminus B = \{a \in A : a \notin B\}$ and B^A is the set of all functions from A to B. If $f : X \to Y$ is a function and $Z \subseteq X$ and $W \subseteq Y$ then the *image* of Z and the *inverse image* of W are $f[Z] := \{f(x) : x \in Z\}$ and $f^{-1}[W] := \{x \in X : f(x) \in W\}$. Recall that a *family of sets*, denoted $\{X_i : i \in I\}$ is really a function g whose domain is a set I such that $X_i = g(i)$ is a set for each $i \in I$. This family is called *finite* if the set I is finite.

By ordinals we mean Von Neumann ordinals, i.e., each ordinal is identified with its set of predecessors. The least infinite ordinal is denoted ω; its elements are called the *natural numbers*. The elementhood relation $\in$ between ordinals is also denoted $<$. The relation $\leq$ obtained from $<$ in the usual way therefore coincides with set inclusion $\subseteq$ in every ordinal.

The symbols $\mathsf{m}, \mathsf{n}, \mathsf{k}, \ldots$ denote cardinals but we revert to $m, n, k, \ldots$ if they are known to be finite. We replace ω by $\aleph_0$ when considering it as a cardinal. We use $+$ for both ordinal and cardinal addition, relying on the context to distinguish meaning. Ordinal multiplication and exponentiation never arise in this thesis, so the standard $\mathsf{m}.\mathsf{n}$ (or mn) and m^{n} denote *cardinal* multiplication and exponentiation. The cardinal successor of m is denoted by m^+.

If a sequence of objects is denoted by $a_1, \dots, a_n$ ($n \in \omega$) or by $\langle a_\alpha : \alpha < \beta\rangle$ (β an ordinal), we often abbreviate this sequence by $\mathbf{a}$.

Let $\sim$ be a (binary) relation on a set A (i.e., $\sim \in \mathcal{P}(A \times A)$). For $a, b \in A$, we frequently write $a \sim b$ for $(a, b) \in \sim$. We sometimes write $a \sim b$ as $a \overset{\sim}{\equiv} b$. Recall that on A, $\sim$ is called

reflexive if for all $a \in A$, we have $a \sim a$;
symmetric if whenever $a, b \in A$, and $a \sim b$ then $b \sim a$;
anti-symmetric if whenever $a, b \in A$, and $a \sim b$ and $b \sim a$ then $a = b$;
transitive if whenever $a, b, c \in A$, and $a \sim b$ and $b \sim c$ then $a \sim c$;
connected if whenever $a, b \in A$, then $a \sim b$ or $b \sim a$;
an *equivalence relation* if it is reflexive, symmetric and transitive;
a *partial order* if it is reflexive, anti-symmetric and transitive;
a *linear order* if it is a connected partial order.

If $B \subseteq A$, the restriction $\sim \sqcap (B \times B)$ of $\sim$ to B is denoted by $\sim |_B$ or $\sim_B$. If $\leq$ is a partial [respectively linear] order on A, we call the pair $\langle A; \leq\rangle$ a *partially ordered set* [respectively a *linearly ordered set*] or, briefly, a *poset* [respectively a *chain*]. We then call A the *universe* of the poset $\mathbf{A} = \langle A; \leq\rangle$. Unless we indicate otherwise, the universe of a poset is understood to be a set A if the poset is denoted by $\mathbf{A}$.

0.2 Lattices. Let $\mathbf{P} = \langle P; \leq\rangle$ be a poset and $A \subseteq P$. An element $t \in P$ is called an *upper bound* of A (in $\mathbf{P}$) if $a \leq t$ for every $a \in A$. We call A an *upward directed* subset of $\mathbf{P}$ if for any $b, c \in A$, there exists $a \in A$ such that a is an upper bound (in $\mathbf{P}$) of $\{b, c\}$. An element $t \in P$ is called a *least upper bound* or *supremum* of A if t is an upper bound of A and $t \leq q$ for every upper bound $q \in P$ of A. We write $t = \bigvee_{\mathbf{P}} A$ in this case and we will omit the subscript unless confusion could arise. Lower bounds of A and the *greatest lower bound* or *infimum* of A are defined dually, and we will use $\bigwedge_{\mathbf{P}} A$ or just $\bigwedge A$ for the infimum. We abbreviate $\bigvee\{a, b\}$ and $\bigwedge\{a, b\}$ by $a \vee b$ and $a \wedge b$, respectively.

If $a, b \in P$ we use $a < b$ or $b > a$ to indicate that $a \leq b$ but $a \neq b$. We say that b *covers* a, written $a \prec b$ or $b \succ a$, if $a < b$ and there is no $c \in P$ with $a < c < b$. In this case b is called a *cover* for a.

If $a \vee b$ exists for all $a, b \in P$, we call $\mathbf{P}$ an *upper semilattice*, and if $a \wedge b$ exists for all $a, b \in P$, we call $\mathbf{P}$ a *lower semilattice.* $\mathbf{P}$ is called a *lattice* when it is both an upper and a lower semilattice. In an upper semilattice, the binary operation $\vee$ ("join") is associative so we may abbreviate $\bigvee\{a_1, \dots, a_n\}$ as $a_1 \vee \dots \vee a_n$ without parentheses; similarly for $\wedge$ ("meet") in a lower semilattice.

Let $\mathbf{L} = \langle L; \leq \rangle$ be a lattice and let L' be a nonempty subset of L. If for every $a, b \in L'$, both $\bigvee_{\mathbf{L}}\{a, b\}$ and $\bigwedge_{\mathbf{L}}\{a, b\}$ are elements of L', then $\mathbf{L}' = \langle L'; \leq_{L'} \rangle$ is called a *sublattice* of $\mathbf{L}$.

Two lattices $\mathbf{L}_1$ and $\mathbf{L}_2$ are said to be *isomorphic* if there is a one-to-one, onto function $\alpha : L_1 \to L_2$ such that, for all $a, b \in L_1$,

$$\alpha(a \vee b) = \alpha(a) \vee \alpha(b) \text{ and } \alpha(a \wedge b) = \alpha(a) \wedge \alpha(b).$$

In this case we write $\mathbf{L}_1 \cong \mathbf{L}_2$ or $\alpha : \mathbf{L}_1 \cong \mathbf{L}_2$ and we call α a *lattice isomorphism.*

Let $\mathbf{P}_1$ and $\mathbf{P}_2$ be posets and $\alpha : P_1 \to P_2$ a function. We say that α is *order-preserving* if for any $a, b \in P_1$, $a \leq b$ implies $\alpha(a) \leq \alpha(b)$.

Theorem 0.1. [BS81, Theorem 2.3, p8]

Two lattices $\mathbf{L}_1$ and $\mathbf{L}_2$ are isomorphic if and only if there is a bijection $\alpha : L_1 \to L_2$ such that α and α^{-1} are both order-preserving.

A lattice $\mathbf{L}$ is *distributive* if for all $x, y \in L$ it satisfies either (equivalently, both) of the distributive laws:

$$\begin{aligned} x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z) \\ x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z). \end{aligned}$$

Every lattice satisfies:

$$\begin{aligned} x \wedge (y \vee z) &\geq (x \wedge y) \vee (x \wedge z) \\ x \vee (y \wedge z) &\leq (x \vee y) \wedge (x \vee z). \end{aligned}$$

Also, every lattice satisfies the condition $x \leq y$ implies $x \vee (y \wedge z) \leq y \wedge (x \vee z)$.

A lattice $\mathbf{L}$ is said to be *modular* if the following law, called the *Modular Law* holds in it :

$$x \leq y \text{ implies } x \vee (y \wedge z) = y \wedge (x \vee z).$$

Theorem 0.2. [BS81, Theorem 3.4, p11]

Every distributive lattice is a modular lattice.

For any poset $\mathbf{P} = \langle P; \leq \rangle$ and $x, y \in P$, we define the *interval* $int(x, y)$ as the set of all $c \in P$ such that $x \leq c \leq y$. If in addition, $\mathbf{P}$ is a lattice and $x \leq y$ then $int(x, y)$ is the universe of a sublattice $\mathbf{int}(x, y)$ of $\mathbf{P}$.

Consider $int(x, y)$ and $int(v, w)$ (where $x \leq y$ and $v \leq w$) in a lattice $\mathbf{L}$. We say that $int(x, y)$ *transposes down* onto $int(v, w)$ and write $int(x, y) \searrow int(v, w)$ if $x \wedge w = v$ and $x \vee w = y$. This relationship can also be described by saying $int(v, w)$ *transposes up* onto $int(x, y)$, and is written $int(v, w) \nearrow int(x, y)$.

Theorem 0.3. *Let* $\mathbf{L}$ *be a lattice and let* $a, b, c, d \in L$ *with* $a \leq b$ *and* $c \leq d$ *such that* $int(a, b) \nearrow int(c, d)$. *If* $\mathbf{L}$ *is modular, then the map* $x \mapsto x \vee c$ $(x \in int(a, b))$ *is a lattice isomorphism from* $\mathbf{int}(a, b)$ *onto* $\mathbf{int}(c, d)$ *whose inverse isomorphism is given by* $y \mapsto y \wedge b$ $(y \in int(c, d))$.

(This theorem can fail if $\mathbf{L}$ is nonmodular.)

A poset $\mathbf{P}$ is called a *complete lattice* if for every subset A of P, both $\bigvee_{\mathbf{P}} A$ and $\bigwedge_{\mathbf{P}} A$ exist (in P). Thus, a complete lattice has a greatest and a least element (setting $A = \emptyset$). A nonempty subset L of P is then said to be (the universe of) a *complete sublattice* $\mathbf{L}$ of $\mathbf{P}$ if $\bigvee_{\mathbf{P}} A$, $\bigwedge_{\mathbf{P}} A \in L$ whenever $A \subseteq L$.

Theorem 0.4. [BS81, Theorem 4.2, p14]

Let $\mathbf{P}$ *be a poset such that* $\bigwedge A$ *exists for every subset* A *of* P, *or such that* $\bigvee A$ *exists for every subset of* P. *Then* $\mathbf{P}$ *is a complete lattice.*

For any set A, the poset $\mathbf{P} = \langle \mathcal{P}(A); \subseteq \rangle$ is a complete lattice; if $X \subseteq \mathcal{P}(A)$ then $\bigwedge_{\mathbf{P}} X = \cap X$ and $\bigvee_{\mathbf{P}} X = \cup X$.

An element y of a lattice $\mathbf{L}$ is called *completely meet irreducible* if, for any $Y \subseteq L$, $y = \bigwedge Y$ implies $y \in Y$.

Let $\mathbf{L}$ be a lattice and let $a \in L$. We say that a is *compact* (in $\mathbf{L}$) if the following condition holds: for every subset A of L such that $a \leq \bigvee_{\mathbf{L}} A \in L$, there exists a *finite* subset A' of A such that $a \leq \bigvee_{\mathbf{L}} A' \in L$. $\mathbf{L}$ is said to be *compactly generated* if every element of L is the supremum of some set of compact elements of L. If a lattice is complete and compactly generated, it is said to be *algebraic.*

Given a complete lattice $\mathbf{L} = \langle L; \leq \rangle$, a subset X of L is called a *closure system* in $\mathbf{L}$ if for every $Y \subseteq X$, $\bigwedge_{\mathbf{L}} Y \in X$. (This forces X to contain the greatest element of L, viz. $\bigwedge_{\mathbf{L}} \emptyset$; in particular, $X \neq \emptyset$ and $\langle X; \leq \rangle$ is a complete lattice in its own right.) If in addition, we have $\bigvee_{\mathbf{L}} Y \in X$ for every nonempty upward directed subset Y of $\langle X; \leq \rangle$, then X is called an *algebraic closure system* in $\mathbf{L}$. With a closure system X in a complete lattice $\langle L; \leq \rangle$, we associate a mapping $u = u_X : L \to L$ defined by $u(x) = \bigwedge_{\mathbf{L}} \{z \in X : x \leq z\}$. This map has the following properties:

$$\begin{aligned} &\text{(i)} \quad x \leq u(x) = u(u(x)); \\ &\text{(ii)} \quad x \leq y \text{ implies } u(x) \leq u(y) \end{aligned}$$

for all $x, y \in L$. The range $u[L]$ of this map is just X. If X is an algebraic closure system then we also have

$$\text{(iii)} \quad u(x) = \bigvee_{\mathbf{L}} \{u(y) : y \leq x \text{ and } y \text{ is compact in } \mathbf{L}\} \quad (x \in L).$$

Mappings $u : L \to L$ satisfying (i) and (ii) are called *closure operators* on $\langle L; \leq \rangle$. For such a map u, we always have

$$\bigvee_{u[\mathbf{L}]} u[Y] = u(\bigvee_{\mathbf{L}} Y) \text{ for any } Y \subseteq L \text{ (where } u[\mathbf{L}] = \langle u[L]; \leq \rangle = \langle X; \leq \rangle)$$

[BS81, Theorem 5.2, p18]. A closure operator u on $\langle L; \leq \rangle$ is called an *algebraic closure operator* on $\langle L; \leq \rangle$ if it satisfies (iii) (for all $x \in L$). The elements of the form $u(x)$ (for some $x \in L$) are called *closed (with respect to u)*. Every (algebraic) closure operator u on $\langle L; \leq \rangle$ has the form u_X for some (algebraic) closure system X in $\langle L; \leq \rangle$, viz., for $X = u[L]$, and the correspondence $X \mapsto u_X$ is one-to-one. Also, every (algebraic) closure system X in $\langle L; \leq \rangle$ is the range $u[L]$ of a suitable (algebraic) closure operator u on $\langle L; \leq \rangle$, viz. $u = u_X$, and the correspondence $u \mapsto u[L]$ is one-to-one. The aforementioned two correspondences are mutually inverse bijections between the set of (algebraic) closure systems on $\langle L; \leq \rangle$ and the set of (algebraic) closure operators on $\langle L; \leq \rangle$. The following results are to be found in most introductory lattice theory texts or, e.g., [Grä79, Theorem 5 and Lemma 5, p25].

Proposition 0.5. *The following conditions on a lattice* $\mathbf{L} = \langle L; \leq \rangle$ *are equivalent:*

(i) $\mathbf{L}$ *is an algebraic lattice;*

(ii) *there exists a set* S *and an algebraic closure system* X *in the complete lattice* $\langle \mathcal{P}(S); \subseteq \rangle$ *of all subsets of* S *(ordered by inclusion) such that* $\mathbf{L}$ *is isomorphic to the lattice* $\langle X; \subseteq \rangle$.

Proposition 0.6. *Let* $\mathbf{L} = \langle L; \leq \rangle$ *be an algebraic lattice and* u *an algebraic closure operator on* $\mathbf{L}$. *Then* $y \in L$ *is a compact element of* $\langle u[L]; \leq \rangle$ *if and only if* $y = u(x)$ *for some compact element* x *of* $\langle L; \leq \rangle$.

Corollary 0.7. *Let* S *be a set and* $X \subseteq \mathcal{P}(S)$. *Then* $\langle X; \subseteq \rangle$ *is an algebraic lattice if and only if* X *is closed under arbitrary intersections and* $\bigcup Y \in X$ *for any nonempty upward directed subset* Y *of* $\langle X; \subseteq \rangle$. *In this case, the map* $Z \to u(Z) = \bigcap\{A \in X : A \supseteq Z\}$ $(Z \in \mathcal{P}(S))$ *is the algebraic closure operator on* $\langle \mathcal{P}(S); \subseteq \rangle$ *corresponding to* X *and the compact elements of* $\langle X; \subseteq \rangle$ *are just the elements of the form* $u(Z)$, *where* Z *is any finite subset of* S.

If θ and φ are relations on a set A, we define the *relational product* $\theta \circ \varphi$ by: $\theta \circ \varphi = \{(a, b) \in A \times A :$ there exists $c \in A$ such that $(a, c) \in \theta$ and $(c, b) \in \varphi\}$. The operation $\circ$ is associative so brackets are unnecessary in expressions like $\theta \circ \varphi \circ \eta$.

We define $Eq(A)$ to be the set of all equivalence relations on a set A. For any set A, $Eq(A)$ is an algebraic closure system in $\langle \mathcal{P}(A \times A); \subseteq \rangle$, hence $\mathbf{Eq}(A) := \langle Eq(A); \subseteq \rangle$, the *equivalence lattice* of A, is an algebraic lattice.

Its least element is the *identity relation*, $id_A = \{(a,a) : a \in A\}$ and its greatest is the *total relation*, $A \times A$. For $\Gamma \subseteq Eq(A)$, $\bigwedge\Gamma = \bigcap\Gamma$ and $\bigvee\Gamma = \bigcap\{\sigma \in Eq(A) : \bigcup\Gamma \subseteq \sigma\}$. Thus, for $\theta, \varphi \in Eq(A)$, $\theta \wedge \varphi = \theta \cap \varphi$ and $\theta \vee \varphi = \bigcap\{\sigma : \theta \cup \varphi \subseteq \sigma \in Eq(A)\}$.

Theorem 0.8. [BS81, Theorem 4.7, p16]

Let $\{\theta_i : i \in I\}$ be a nonempty set of equivalence relations on a set A. Then in $\mathbf{Eq}(A)$,

$$\bigvee_{i\in I}\theta_i = \bigcup\{\theta_{i_1} \circ \theta_{i_2} \circ \ldots \circ \theta_{i_n} : \ 0 < n \in \omega \ \textit{and}\ i_1, \ldots, i_n \in I\},$$

i.e., $a(\bigvee_{i\in I}\theta_i)b$ if and only if there exist $i_1, \ldots, i_n \in I$ such that $a(\theta_{i_1} \circ \theta_{i_2} \circ \ldots \circ \theta_{i_n})b$. In particular, when $I = \{1,2\}$, then in $\mathbf{Eq}(A)$,

$$\theta_1 \vee \theta_2 = \theta_1 \cup (\theta_1 \circ \theta_2) \cup (\theta_1 \circ \theta_2 \circ \theta_1) \cup (\theta_1 \circ \theta_2 \circ \theta_1 \circ \theta_2) \cup \ldots .$$

Equivalently, $(a,b) \in \theta_1 \vee \theta_2$ if and only if there is a sequence of elements $c_1, c_2, \ldots, c_n$ from A (with $n \geq 2$) such that $(c_i, c_{i+1}) \in \theta_1$ or $(c_i, c_{i+1}) \in \theta_2$ for $i = 1, \ldots, n-1$, and $a = c_1$, and $b = c_n$.

From this theorem and the definition of the relational product, it is clear that for any set A and for $\theta, \varphi \in Eq(A)$, $\theta \circ \varphi \subseteq \theta \vee \varphi$.

0.3 Universal Algebras. Let A be a nonempty set and $n \in \omega$. If $n > 0$, we identify A^n with $\{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in A\} = \prod_{i=1}^{n} A$; note that $A^0 = \{\emptyset\}$.

For any $n \in \omega$, by an *n-ary operation* on A we mean any function $f : A^n \to A$; n is called the *arity* of f, written $ar(f) = n$. In this case f is a *finitary* operation on A. In particular, f is a nullary (or constant), unary, binary, or ternary operation on A if it is a 0-ary, 1-ary, 2-ary or 3-ary operation on A, respectively.

A *type* or *language* $\mathcal{T}$ is an ordered pair $\langle \mathsf{F}, ar\rangle$ where F is a set whose elements are called *operation symbols* and ar is a function from F to ω, called the *arity* function. The type $\mathcal{T}$ is called *finite* if $|\mathsf{F}|$ is finite. A *universal algebra* of type $\mathcal{T}$ (or a $\mathcal{T}$-*algebra*) is an ordered pair $\mathbf{A} = \langle A; F\rangle$ where A is a nonempty set called the *universe* of A and $F = \{f^{\mathbf{A}} : f \in \mathsf{F}\}$ where for each $f \in \mathsf{F}$ with $ar(f) = n$, $f^{\mathbf{A}}$ is an n-ary operation on A. (If $ar(f) = 0$, we may identify $f^{\mathbf{A}}$ with an element of A.) The $f^{\mathbf{A}}$'s are called the *fundamental operations* of $\mathbf{A}$. If F is finite, say $F = \{f_1, \ldots, f_k\}$, we often write $\langle A; f_1, \ldots, f_k\rangle$ for $\langle A; F\rangle$, usually listing the f_i's in descending order of arity, and say that $\mathbf{A}$ has type $\langle ar(f_1), \ldots, ar(f_k)\rangle$.

Unless we specify otherwise, it is understood that the universe of an algebra $\mathbf{A}$ is always a set denoted by A.

An algebra $\mathbf{A}$ is said to be *finite* if $|A|$ is finite; *trivial* if $|A| = 1$.

0.3.1 Subalgebras. A subset X of A is a *subuniverse* of a $\mathcal{T}$-algebra $\mathbf{A} = \langle A; F\rangle$ if and only if X is closed under each of the operations $f^{\mathbf{A}}$ $(f \in \mathsf{F})$, i.e., for every $f \in \mathsf{F}$ and any $x_1, \dots, x_n \in X$, we have $f^{\mathbf{A}}(x_1, \dots, x_n) \in X$ (where $n = ar(f)$). We will denote the set of all subuniverses of $\mathbf{A}$ by $Sub(\mathbf{A})$. If X is a nonempty subuniverse of $\mathbf{A}$ then the $\mathcal{T}$-algebra $\langle X; \{f^{\mathbf{A}}|_{X^{ar(f)}} : f \in \mathsf{F}\}\rangle$ is called a *subalgebra* of $\mathbf{A}$.

The subuniverse of $\mathbf{A}$ *generated by* $X \subseteq A$, denoted by $Sg^{\mathbf{A}}(X)$, is defined as $\bigcap\{Y \in Sub(\mathbf{A}) : X \subseteq Y\}$. Then $\langle Sg^{\mathbf{A}}(X); \{f^{\mathbf{A}}|_{Sg(X)^{ar(f)}} : f \in \mathsf{F}\}\rangle$ is a subalgebra of $\mathbf{A}$, denoted by $\mathbf{Sg}^{\mathbf{A}}(X)$. We say X *generates* $\mathbf{A}$ (or $\mathbf{A}$ is *generated by* X or X is a *set of generators of* $\mathbf{A}$) if $Sg^{\mathbf{A}}(X) = A$. If X is a finite subset of A [respectively $|X| \leq \mathsf{m}$, a cardinal], we call $Sg^{\mathbf{A}}(X)$ a *finitely generated* [respectively $\mathsf{m}-$*generated*] subuniverse of $\mathbf{A}$, and $\mathbf{Sg}^{\mathbf{A}}(X)$ a *finitely generated* [respectively $\mathsf{m}-$*generated*] subalgebra of $\mathbf{A}$.

We write $\mathbf{A} \leq \mathbf{B}$ to denote that $\mathbf{A}$ is a subalgebra of an algebra $\mathbf{B}$; $\mathbf{A} < \mathbf{B}$ will denote that $\mathbf{A}$ is a *proper* subalgebra of $\mathbf{B}$, i.e., that $\mathbf{A} \leq \mathbf{B}$ and $A \neq B$. In these respective cases we also say that $\mathbf{B}$ is an *extension*, or a *proper extension* of $\mathbf{A}$.

Theorem 0.9. [BS81, Corollary 3.3, p31]

If $\mathbf{A}$ is an algebra, then $Sub(\mathbf{A})$ is an algebraic closure system in $\langle \mathcal{P}(A); \subseteq\rangle$, hence $\langle Sub(\mathbf{A}); \subseteq\rangle$ is an algebraic lattice. The corresponding algebraic closure operator on $\langle \mathcal{P}(A); \subseteq\rangle$ is $Sg^{\mathbf{A}}$.

Note that an upper [respectively lower] semilattice $\mathbf{A} = \langle A; \leq\rangle$ gives rise to an algebra $\langle A; \vee\rangle$ [respectively $\langle A; \wedge\rangle$] of type $\langle 2\rangle$ and a lattice $\mathbf{A} = \langle A; \leq\rangle$ to an algebra $\mathbf{A} = \langle A; \vee, \wedge\rangle$ of type $\langle 2, 2\rangle$. In the latter case, the sublattices of $\mathbf{A}$ are just the subalgebras of $\langle A; \vee, \wedge\rangle$. In all cases, $\leq$ is recoverable from the algebraic language because for $a, b \in A$, we have $a \leq b$ if and only if $b = a \vee b$, if and only if $a = a \wedge b$.

Let $\mathbf{L} = \langle L; F\rangle$ be a lattice with least and greatest elements 0 and 1. An element $a \in L$ is called *complemented* if there exists $a' \in L$ such that $a \wedge a' = 0$ and $a \vee a' = 1$. In this case a' is called a *complement* of a. If L is distributive and $a \in L$ is complemented then a has a *unique* complement in L.

A complemented distributive lattice is called a *Boolean lattice*; in this case the associated algebra $\langle L; \vee, \wedge, ', 0, 1\rangle$ of type $\langle 2, 2, 1, 0, 0\rangle$ is called a *Boolean algebra.*

For any set I, the lattice $\langle \mathcal{P}(I); \subseteq\rangle$ is Boolean; the associated Boolean algebra is $\langle \mathcal{P}(I); \cup, \cap, ', \emptyset, I\rangle$, where $X' = I \setminus X$ for all $X \subseteq I$.

Let $\mathbf{A} = \langle A; F\rangle$ and $\mathbf{B} = \langle B; F^*\rangle$ be a $\mathcal{T}$-algebra and a $\mathcal{T}^*$-algebra, where $\mathcal{T} = \langle \mathsf{F}, ar\rangle$ and $\mathcal{T}^* = \langle \mathsf{F}^*, ar^*\rangle$. If $B = A$ and $\mathsf{F} \subseteq \mathsf{F}^*$ and $f^{\mathbf{A}} = f^{\mathbf{B}}$ for all

$f \in \mathsf{F}$ then we call $\mathbf{A}$ a *reduct* (or the *F-reduct* or the F-*reduct* or the *$\mathcal{T}$-reduct*) of $\mathbf{B}$.

Henceforth all algebras considered are assumed to be of type $\mathcal{T} = \langle \mathsf{F}, ar \rangle$ unless we say otherwise.

A nonempty set C of $\mathcal{T}$-algebras is called a *chain of $\mathcal{T}$-algebras* if for any $\mathbf{A}, \mathbf{B} \in C$, we have $\mathbf{A} \leq \mathbf{B}$ or $\mathbf{B} \leq \mathbf{A}$. In this case, since C is a set, there is an ordinal β and a sequence $\langle \mathbf{A}_\alpha : \alpha < \beta \rangle$ of $\mathcal{T}$-algebras with $\mathbf{A}_\alpha \in C$ for all $\alpha < \beta$ such that $\cup_{\alpha<\beta} A_\alpha = \cup_{\mathbf{A} \in C} A$ and $\mathbf{A}_\alpha \leq \mathbf{A}_\gamma$ whenever $\alpha < \gamma < \beta$. Then there is a $\mathcal{T}$-algebra $\mathbf{D}$ called the *union of C*, such that the universe of $\mathbf{D}$ is $D = \cup_{\mathbf{A} \in C} A$ and for any $f \in F$ with $ar(f) = n$, the fundamental operation $f^{\mathbf{D}}$ may be defined (unambiguously) as follows:

(i) if $n = 0$ then $f^{\mathbf{D}} = f^{\mathbf{A}_0} \in A_0 \subseteq D$;

(ii) if $n > 0$ and $a_1, \ldots, a_n \in D$ then there exist $\gamma_1, \ldots, \gamma_n < \beta$ such that $a_i \in A_{\gamma_i}$ for each $i \in \{1, \ldots, n\}$; choose $\gamma < \beta$ such that $\gamma_1, \ldots, \gamma_n < \gamma$ and define $f^{\mathbf{D}}(a_1, \ldots, a_n) = f^{\mathbf{A}_\gamma}(a_1, \ldots, a_n)$.

We write $\mathbf{D} = \cup_{\mathbf{A} \in C} \mathbf{A}$. Note that $\mathbf{A} \leq \mathbf{D}$ for all $\mathbf{A} \in C$.

0.3.2 Congruence Relations. Let $\mathbf{A} = \langle A; F \rangle$ be an algebra of type $\mathcal{T} = \langle \mathsf{F}, ar \rangle$ and let θ be a relation on A. Let f be an n-ary operation on A. We say θ is *compatible* with f if for all $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$, if $a_i \theta b_i$ for $i = 1, 2, \ldots, n$, then $f(a_1, \ldots, a_n) \theta f(b_1, \ldots, b_n)$. We call θ a *congruence relation* on (or just a *congruence* of) $\mathbf{A}$ if θ is an equivalence relation on A and is compatible with all the fundamental operations of $\mathbf{A}$.

Let θ be a congruence on a $\mathcal{T}$-algebra $\mathbf{A} = \langle A; F \rangle$. If $a \in A$, we denote the equivalence class of a under θ by a/θ, i.e., $a/\theta = \{x \in A : (x, a) \in \theta\}$. We define $A/\theta = \{a/\theta : a \in A\}$. For each $f \in \mathsf{F}$ (with $ar(f) = n$, say), an operation $f^{\mathbf{A}/\theta}$ on A/θ is (well-)defined by

$$f^{\mathbf{A}/\theta}(a_1/\theta, \ldots, a_n/\theta) = f^{\mathbf{A}}(a_1, \ldots, a_n)/\theta \ \ (a_1, \ldots, a_n \in A).$$

We may therefore define a $\mathcal{T}$-algebra $\mathbf{A}/\theta = \langle A/\theta; F/\theta \rangle$ where $F/\theta = \{f^{\mathbf{A}/\theta} : f \in \mathsf{F}\}$. $\mathbf{A}/\theta$ is called the *quotient* algebra (or *factor* algebra) of $\mathbf{A}$ (modulo θ).

The set of congruence relations of an algebra $\mathbf{A}$ is denoted by $Con(\mathbf{A})$.

Theorem 0.10. [BS81, Theorem 5.5, p37]

For any algebra $\mathbf{A}$, $Con(\mathbf{A})$ is an algebraic closure system in $\langle \mathcal{P}(A \times A); \subseteq \rangle$, hence $\mathbf{Con}(\mathbf{A}) := \langle Con(\mathbf{A}); \subseteq \rangle$ is an algebraic lattice. Moreover, $\mathbf{Con}(\mathbf{A})$ is a complete sublattice of $\mathbf{Eq}(A)$.

We call $\mathbf{Con}(\mathbf{A})$ the *congruence lattice* of $\mathbf{A}$. Thus, in $\mathbf{Con}(\mathbf{A})$, meets and joins are calculated in the same way as when working with equivalence relations. The least and greatest elements of $\mathbf{Con}(\mathbf{A})$ are the *identity congruence*, id_A, and the *total congruence*, A^2, respectively. The algebraic closure operator on $\langle \mathcal{P}(A \times A); \subseteq \rangle$ corresponding to $Con(\mathbf{A})$ is denoted by $\Theta^{\mathbf{A}}$. In other words, for $X \subseteq A^2$,

$$\Theta^{\mathbf{A}}(X) = \cap\{\rho \in Con(\mathbf{A}) : X \subseteq \rho\};$$

this is called the congruence on $\mathbf{A}$ *generated by* X. By Proposition 0.6, the compact elements of $\mathbf{Con}(\mathbf{A})$ are just all $\Theta^{\mathbf{A}}(X)$, where X is a finite subset of A^2. We call these the *finitely generated congruences* of $\mathbf{A}$. If $X = \{(a, b)\} \subseteq A^2$, $\Theta^{\mathbf{A}}(X)$ is called a *principal congruence* and will be abbreviated by $\Theta^{\mathbf{A}}(a, b)$.

We say that an algebra $\mathbf{A}$ is *congruence distributive* [respectively *congruence modular*] if the lattice $\mathbf{Con}(\mathbf{A})$ is distributive [respectively modular]. $\mathbf{A}$ is *congruence permutable* if for every pair $\theta_1, \theta_2 \in Con(\mathbf{A})$, $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$ i.e., θ_1 and θ_2 *permute*.

Theorem 0.11. *(Birkhoff)* [BS81, Theorem 5.10, p41]

If an algebra $\mathbf{A}$ *is congruence permutable, then* $\mathbf{A}$ *is congruence modular.*

If $\mathbf{B}$ is a subalgebra of $\mathbf{A}$ and $\theta \in Con(\mathbf{A})$, then $\theta|_B = \theta \cap (B \times B)$ is a congruence of $\mathbf{B}$. We will therefore use $\theta|_{\mathbf{B}}$ to denote $\theta \cap (B \times B)$.

A reflexive, symmetric and compatible relation η on an algebra $\mathbf{A}$ is called a *tolerance* relation on $\mathbf{A}$. Let $\eta^{[n]}$ be defined as follows: $\eta^{[1]} = \eta$ and $\eta^{[k+1]} = \eta^{[k]} \circ \eta$ for $k > 1$. The *transitive closure* of η is $\cup_{n=1}^{\infty} \eta^{[n]}$; it is the least transitive relation on A containing η.

Theorem 0.12. *Let* η *be a tolerance relation on* $\mathbf{A}$. *Then* $\cup_{n=1}^{\infty} \eta^{[n]} = \Theta^{\mathbf{A}}(\eta)$.

0.3.3 Homomorphisms. Let $\mathbf{A}, \mathbf{B}$ and $\mathbf{C}$ be $\mathcal{T}$-algebras and $\alpha : A \to B$ a function. We call α a *homomorphism* from $\mathbf{A}$ to $\mathbf{B}$ if for any $n \in \omega$ and any n-ary fundamental operation $f^{\mathbf{A}}$ on $\mathbf{A}$, and for any $a_1, \ldots, a_n \in A$, we have $\alpha(f^{\mathbf{A}}(a_1, \ldots, a_n)) = f^{\mathbf{B}}(\alpha(a_1), \ldots, \alpha(a_n))$. (Interpret this as $\alpha(f^{\mathbf{A}}) = f^{\mathbf{B}}$ when $ar(f) = 0$). A homomorphism from $\mathbf{A}$ to $\mathbf{A}$ is called an *endomorphism* of $\mathbf{A}$.

If $\alpha : \mathbf{A} \to \mathbf{B}$ and $\beta : \mathbf{B} \to \mathbf{C}$ are homomorphisms then the composition $\beta \circ \alpha$ is a homomorphism from $\mathbf{A}$ to $\mathbf{C}$.[1] We will use $Hom(\mathbf{A}, \mathbf{B})$ to denote the set of all homomorphisms from $\mathbf{A}$ to $\mathbf{B}$.

[1] We have to tolerate notational ambiguity here. This composite function is unfortunately equal to the relational product $\alpha \circ \beta$.

Theorem 0.13. [BS81, Theorem 6.3, p43]

Let $\alpha : \mathbf{A} \to \mathbf{B}$ be a homomorphism. Then the image of a subuniverse X of $\mathbf{A}$ under α is a subuniverse of $\mathbf{B}$, and the inverse image of a subuniverse Y of $\mathbf{B}$ is a subuniverse of $\mathbf{A}$.

We denote the corresponding algebras by $\alpha[\mathbf{X}]$ and $\alpha^{-1}[\mathbf{Y}]$.

A *surjective* (i.e., an onto) homomorphism is also called an *epimorphism*, while an *injective* (i.e., a one-to-one) homomorphism is called a *monomorphism* or an *embedding*. We say the algebras $\mathbf{A}$ and $\mathbf{B}$ are *isomorphic* (written $\mathbf{A} \cong \mathbf{B}$) if there is a *bijective* homomorphism α from $\mathbf{A}$ to $\mathbf{B}$. We write $\alpha : \mathbf{A} \cong \mathbf{B}$ (or $\mathbf{A} \overset{\alpha}{\cong} \mathbf{B}$) in this case and call α an *isomorphism*.

If $\alpha \in Hom(\mathbf{A}, \mathbf{B})$, then the *kernel* of α, denoted $ker(\alpha)$, is $\{(a,b) \in A^2 : \alpha(a) = \alpha(b)\}$ and is an element of $Con(\mathbf{A})$. The homomorphism α is an embedding if and only if $ker(\alpha) = id_A$. For $\theta \in Con(\mathbf{A})$, the *natural map* λ from $\mathbf{A}$ to $\mathbf{A}/\theta$ is defined by $\lambda(a) = a/\theta$ $(a \in A)$; it is an epimorphism and $ker(\lambda) = \theta$.

Theorem 0.14. *Let $h : \mathbf{A} \to \mathbf{B}$ be an epimorphism and $\varphi \in Con(\mathbf{A})$. Then $h(\varphi) := \{(h(a), h(a')) : (a, a') \in \varphi\}$ is a tolerance relation on $\mathbf{B}$, so $\Theta^{\mathbf{B}}(h(\varphi))$ is the transitive closure of $h(\varphi)$. If $ker(h) \subseteq \varphi$ then $h(\varphi) \in Con(\mathbf{B})$. Also if $\eta \in Con(\mathbf{B})$ then $h^{-1}(\eta) \in Con(\mathbf{A})$, where $h^{-1}(\eta) := \{(a, a') \in A^2 : (h(a), h(a')) \in \eta\}$.*

By the above theorem, if $\theta, \varphi \in Con(\mathbf{A})$ with $\theta \subseteq \varphi$, then there is a congruence relation φ/θ on $\mathbf{A}/\theta$ defined by:

$$\varphi/\theta = \{(a/\theta, b/\theta) \in (A/\theta)^2 : (a,b) \in \varphi\}.$$

We will make frequent use of the following well-known theorems.

Theorem 0.15. (Homomorphism Theorem) [BS81, Theorem 6.12, p46]

Suppose $\alpha : \mathbf{A} \to \mathbf{B}$ is a homomorphism onto $\mathbf{B}$. Then there is an isomorphism β from $\mathbf{A}/ker(\alpha)$ onto $\mathbf{B}$ such that $\alpha = \beta \circ \lambda$, where λ is the natural homomorphism from $\mathbf{A}$ to $\mathbf{A}/ker(\alpha)$.

Theorem 0.16. (Second Isomorphism Theorem) [BS81, Theorem 6.15 , p47]

If $\varphi, \theta \in Con(\mathbf{A})$ and $\theta \subseteq \varphi$, then the map $\alpha : (A/\theta)/(\varphi/\theta) \to A/\varphi$ defined by $\alpha((a/\theta)/(\varphi/\theta)) = a/\varphi$ is an isomorphism from $(\mathbf{A}/\theta)/(\varphi/\theta)$ onto $\mathbf{A}/\varphi$.

For $\theta, \gamma \in Con(\mathbf{A})$, recall that $int(\theta, \gamma) = \{\rho \in Con(\mathbf{A}) : \theta \subseteq \rho \subseteq \gamma\}$ and that this is the universe of a sublattice of $\mathbf{Con}(\mathbf{A})$, denoted by $\mathbf{int}(\theta, \gamma)$.

Theorem 0.17. (Correspondence Theorem) [BS81, Theorem 6.20, p49]

Let $\mathbf{A}$ *be an algebra and let* $\theta \in Con(\mathbf{A})$. *Then the mapping* α *defined on* $int(\theta, A^2)$ *by* $\alpha(\varphi) = \varphi/\theta$ *is a lattice isomorphism from* $\mathbf{int}(\theta, A^2)$ *onto* $\mathbf{Con}(\mathbf{A}/\theta)$ *with inverse isomorphism given by* $\rho \mapsto \alpha^{-1}(\rho)$ $(\rho \in Con(\mathbf{A}/\theta))$.

0.3.4 Products. Let $\mathbf{A}_i = \langle A_i; F_i \rangle$, $i \in I$, be a family of $\mathcal{T}$-algebras. Recall that the *Cartesian product* of the family $\{A_i : i \in I\}$ is defined as the set of all functions $g : I \to \cup_{i \in I} A_i$ such that $g(i) \in A_i$ for each $i \in I$. If $|I| = n \in \omega$, we will identify the elements of $\prod_{i \in I} A_i$ with n-tuples, as usual. Note that if $I = \emptyset$, then $\prod_{i \in I} A_i = \{\emptyset\}$. For each $j \in I$, the j^{th} *projection* is the surjection $\pi_j : \prod_{i \in I} A_i \to A_j$ defined by $\pi_j(x) = x(j)$ $(x \in \prod_{i \in I} A_i)$. Then there is a $\mathcal{T}$-algebra $\mathbf{D}$, with universe $D = \prod_{i \in I} A_i$, called the *direct product* of $\{\mathbf{A}_i : i \in I\}$, whose fundamental operations are defined as follows:

If $f \in \mathsf{F}$, with $ar(f) = n$ and $a_1, \ldots, a_n \in D$ and $j \in I$, then

$$\pi_j(f^{\mathbf{D}}(a_1, \ldots, a_n)) = f^{\mathbf{A}_j}(a_1(j), \ldots, a_n(j)).$$

(If f is nullary, $f^{\mathbf{D}} = c \in D$ where $c(i)$ is $f^{\mathbf{A}_i} \in A_i$ for each $i \in I$.) We write $\mathbf{D} = \prod_{i \in I} \mathbf{A}_i$.

We need the following consequences of the above definitions:

(i) For each $j \in I$, the j^{th} projection map $\pi_j : \prod_{i \in I} \mathbf{A}_i \to \mathbf{A}_j$ is a homomorphism.

(ii) If $\mathbf{A}$ is a $\mathcal{T}$-algebra and for each $i \in I$, $h_i : A \to A_i$ is a function, we define $h : A \to \prod_{i \in I} A_i$ by $\pi_i(h(a)) = h_i(a)$ for all $i \in I$. If for each i, h_i is a homomorphism from $\mathbf{A}$ to $\mathbf{A}_i$, then h is a homomorphism from $\mathbf{A}$ to $\prod_{i \in I} \mathbf{A}_i$.

If $\{\mathbf{A}_i : i \in I\}$ is a finite family of $\mathcal{T}$-algebras with $I = \{1, \ldots, n\}$, the direct product $\prod_{i \in I} \mathbf{A}_i$ is denoted by $\prod_{i=1}^{n} \mathbf{A}_i = \mathbf{A}_1 \times \mathbf{A}_2 \times \ldots \times \mathbf{A}_n$. Notice that the subuniverses of $\mathbf{A}^2 = \mathbf{A} \times \mathbf{A}$ are just the relations on A that are compatible with all the fundamental operations of $\mathbf{A}$.

A $\mathcal{T}$-algebra $\mathbf{A}$ is said to be a *subdirect product* of a family $\{\mathbf{A}_i : i \in I\}$ of $\mathcal{T}$-algebras if

(i) $\mathbf{A}$ is a subalgebra of $\prod_{i \in I} \mathbf{A}_i$, and

(ii) $\pi_j[\mathbf{A}] = \mathbf{A}_j$ for each projection $\pi_j : \prod_{i \in I} \mathbf{A}_i \to \mathbf{A}_j$.

Let $\mathbf{B}$ be a $\mathcal{T}$-algebra. A homomorphism $\alpha : \mathbf{B} \to \prod_{i \in I} \mathbf{A}_i$ is called a *subdirect embedding* if α is one-to-one and $\alpha[\mathbf{B}]$ is a subdirect product of $\{\mathbf{A}_i : i \in I\}$.

Given a family $\{Y_i : i \in I\}$ of sets, a set Y and functions $\alpha_i : Y \to Y_i$ (for each $i \in I$), the family $\{\alpha_i : i \in I\}$ is said to *separate points* of Y if for any $y_1, y_2 \in Y$ with $y_1 \neq y_2$, there is an $i \in I$ such that $\alpha_i(y_1) \neq \alpha_i(y_2)$.

Lemma 0.18. [BS81, Lemma 7.14, p55]

For an indexed family of homomorphisms $\alpha_i : \mathbf{A} \to \mathbf{A}_i$, $i \in I$, the following are equivalent:

(i) *The homomorphisms α_i separate points of A.*

(ii) *The natural homomorphism $\alpha : \mathbf{A} \to \prod_{i \in I} \mathbf{A}_i$ (induced by the maps α_i) is injective.*

(iii) $\bigcap_{i \in I} ker(\alpha_i) = id_A$.

Theorem 0.19. *Let $\mathbf{A}$ be an algebra and let $a, b \in A$, $a \neq b$. The following are equivalent:*

(i) *Whenever f is a homomorphism defined on $\mathbf{A}$ and f is not one-to-one, then $f(a) = f(b)$.*

(ii) *Every nonidentity congruence relation on $\mathbf{A}$ identifies a and b.*

Definition 0.20. We define an algebra $\mathbf{A}$ to be *(a, b)-irreducible* if $a, b \in A$ and $a \neq b$ and the conditions of the above theorem hold.

Theorem 0.21. *The following are equivalent for an algebra $\mathbf{A}$:*

(i) *For every subdirect embedding $\alpha : \mathbf{A} \to \prod_{i \in I} \mathbf{A}_i$ there is an $i \in I$ such that the map $\pi_i \circ \alpha : \mathbf{A} \to \mathbf{A}_i$ is an isomorphism.*

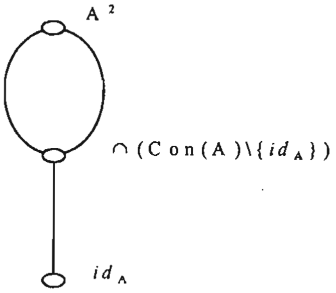
(ii) *Any family of homomorphisms defined on $\mathbf{A}$ which separates points of $\mathbf{A}$ contains a homomorphism which is one-to-one.*

(iii) *In $\mathbf{Con}(\mathbf{A})$, id_A is completely meet irreducible.*

(iv) *Either $\mathbf{A}$ is trivial or there exist $a, b \in A$ such that $\mathbf{A}$ is (a, b)-irreducible.*

Definition 0.22. We define an algebra $\mathbf{A}$ to be *subdirectly irreducible* if it is nontrivial and the conditions of the above theorem hold. (Otherwise $\mathbf{A}$ is said to be *subdirectly reducible.*)

The above theorem gives a useful characterization of subdirectly irreducible algebras, namely, an algebra $\mathbf{A}$ is subdirectly irreducible if and only if $Con(\mathbf{A}) \setminus \{id_A\}$ has a least element. This least element is called the *monolith* of $\mathbf{A}$. It is clearly a principal congruence and equal to $\bigcap(Con(\mathbf{A}) \setminus \{id_A\})$. In this case $\mathbf{Con}(\mathbf{A})$ looks like this:



The following result is due to G. Birkhoff. We will refer to it as *Birkhoff's Subdirect Decomposition Theorem.* As a consequence of this theorem, the study of classes of algebras closed under the taking of homomorphic images is reduced to the study of the subdirectly irreducible algebras in the class.

Theorem 0.23. *(Birkhoff)* [Bir44]

Every $\mathcal{T}$-algebra $\mathbf{A}$ is isomorphic to a subdirect product of subdirectly irreducible $\mathcal{T}$-algebras (which are homomorphic images of $\mathbf{A}$).

Corollary 0.24. [BS81, Corollary 8.7, p59]

Every finite algebra is isomorphic to a subdirect product of a finite family of subdirectly irreducible finite algebras.

0.4 Varieties. If O is a "class operator" mapping classes of $\mathcal{T}$-algebras to other classes of $\mathcal{T}$-algebras, we say a class K of $\mathcal{T}$-algebras is *closed* under O if $O(K) \subseteq K$. The composition of two class operators, O_1 and O_2 (mapping any K to $O_2(O_1(K))$) is written O_2O_1. A class operator is said to be *idempotent* if $O^2 = OO = O$.

We use the letters I, H, S, P and P_S to denote the class operators used to obtain from a class K of $\mathcal{T}$-algebras the class of all *isomorphic images*, *homomorphic images*, *subalgebras*, *direct products* and *subdirect products*, respectively, of members of K. A class of $\mathcal{T}$-algebras is called a *$\mathcal{T}$-variety* (or just a *variety*) if it is closed under the class operators H, S and P. If K is a class of similar algebras (i.e., algebras of the same type), $V(K)$ will denote the *variety V generated by K*, i.e., the intersection of all the varieties containing K.

Theorem 0.25. *(Tarski)* [BS81, Theorem 9.5, p61].

Let K be a class of algebras of the same type $\mathcal{T}$. Then $V(K) = HSP(K)$.

If K has only one member $\mathbf{A}$, we write $V(\mathbf{A})$ for $V(K)$. A variety V is said to be *finitely generated* if $V = V(K)$ for some *finite* set K of *finite* algebras (equivalently, $V = V(\mathbf{A})$ for some finite algebra $\mathbf{A}$). For any class K of $\mathcal{T}$-algebras, we denote the class of all subdirectly irreducible algebras in V by V_{SI}.

The following version of Birkhoff's Subdirect Decomposition Theorem (above) reinforces the comment made previously about the importance of subdirectly irreducible algebras in classes of algebras. It shows that in a variety, these algebras are "building blocks" for all the other algebras.

Theorem 0.26. [BS81, Theorem 9.6, p62]

For any variety V, we have $V = IP_S(V_{SI})$.

A variety V is called *congruence distributive* if for all $\mathbf{A} \in V$, $Con(\mathbf{A})$ is distributive; *congruence modular* if for all $\mathbf{A} \in V$, $Con(\mathbf{A})$ is modular and *congruence permutable* if for all $\mathbf{A} \in V$, $Con(\mathbf{A})$ is permutable. Thus a congruence distributive or congruence permutable variety is congruence modular.

Definition 0.27. The class K of $\mathcal{T}$-algebras has the *congruence extension property (CEP)* if whenever $\mathbf{A} \leq \mathbf{B} \in K$ and θ is a congruence on $\mathbf{A}$ there is a congruence θ_1 on $\mathbf{B}$ with $\theta_1|_{\mathbf{A}} = \theta$.

We say K has the *principal congruence extension property (PCEP)* if whenever $\mathbf{A}, \mathbf{B} \in K$ with $\mathbf{A} \leq \mathbf{B}$ and $a, b \in A$ then $\Theta^{\mathbf{A}}(a, b) = A^2 \cap \Theta^{\mathbf{B}}(a, b)$.

Theorem 0.28. [Day71]

For a variety V, the following are equivalent:

(i) V *has the CEP.*

(ii) V *has the PCEP.*

Corollary 0.29. [Day71]

A variety V satisfies the CEP if and only if for all $\mathbf{A} \in V$ and all $a, b, c, d \in A$, the following is true: $(c, d) \in \Theta^{\mathbf{A}}(a, b)$ if and only if $(c, d) \in \Theta^{\mathbf{S}}(a, b)$ where $\mathbf{S} = \mathbf{Sg}^{\mathbf{A}}(\{a, b, c, d\})$.

If a class K has the CEP then $HS(\mathbf{A}) \subseteq SH(\mathbf{A})$ for all $\mathbf{A} \in K$.

0.4.1 Examples of Varieties. In each case listed below, the class of all algebras named is a variety (of the indicated type).

(1) Semigroups, i.e., algebras $\langle S; \cdot \rangle$ of type $\langle 2 \rangle$, where $\cdot$ is associative on S.

(2) Groups, considered as algebras $\langle G; +, -, 0 \rangle$ (sometimes written $\langle G; \cdot, ^{-1}, e \rangle$) of type $\langle 2, 1, 0 \rangle$. Occasionally we take the liberty of referring to the $\langle +, - \rangle$-reduct of a group as a group.

(3) Abelian groups.

(4) Lattices, considered as algebras $\langle L; \vee, \wedge \rangle$ of type $\langle 2, 2 \rangle$.

(5) Distributive lattices.

(6) Modular lattices.

(7) Boolean algebras, considered as algebras $\langle B; \vee, \wedge, ', 0, 1 \rangle$ of type $\langle 2, 2, 1, 0, 0 \rangle$.

(8) Rings, considered as algebras $\langle R; +, \cdot, -, 0 \rangle$ of type $\langle 2, 2, 1, 0 \rangle$.

(9) Rings with identity, considered as algebras $\langle R; +, \cdot, -, 0, 1 \rangle$, of type $\langle 2, 2, 1, 0, 0 \rangle$, where we do *not* insist that $0 \neq 1$.[2]

[2] The class of rings with identity $\mathbf{R} = \langle R; +, \cdot, -, 0, 1 \rangle$ such that $0 \neq 1$ is *not* a variety; it is obviously not closed under homomorphic images.

(10) Left $\mathbf{R}$-modules $\mathbf{M}$, (where $\mathbf{R}$ is a fixed ring), considered as algebras $\langle M; \{+, -, 0\} \cup \{\tilde{r} : r \in R\}\rangle$, where for each $r \in R$, the operations $+, -, 0, \tilde{r}$ have respective arities $2, 1, 0, 1$. For each $m \in M$ and $r \in R$, $\tilde{r}(m)$ is the "scalar multiple" usually denoted by module theorists as rm.

(11) Unitary left $\mathbf{R}$-modules $\mathbf{M}$, (where $\mathbf{R}$ is a fixed ring with identity, 1); these are as in (10) but, for all $m \in M$, must satisfy $\tilde{1}(m) = m$.

It is well-known that all of the above varieties, except for the variety of semigroups, are congruence modular.[3] The variety of lattices is congruence distributive [FN42] (hence the same for distributive or modular lattices and for Boolean algebras). The variety of groups is congruence permutable; it follows that the same is true for Abelian groups, for rings and for modules (of all kinds described above); but none of these varieties is congruence distributive. The variety of Boolean algebras is also congruence permutable.

In this thesis we assume a rudimentary knowledge of the algebras mentioned above; where more sophisticated facts (e.g., about modules) are required, we give detailed references. Axioms for all of the above varieties may be found in [BS81, pp24 -25].

0.4.2 Ultrafilters and Ultraproducts. Let $\mathbf{S} = \langle S; \leq\rangle$ be a lower semilattice. A nonempty subset $\mathcal{G}$ of S is called a *filter* of $\mathbf{S}$ if and only if for any $a, b \in S$ we have

(i) $a, b \in \mathcal{G}$ implies $a \wedge b \in \mathcal{G}$ and

(ii) $a \in \mathcal{G}$ and $b \geq a$ implies $b \in \mathcal{G}$.

If $\mathbf{B} = \langle B; \vee, \wedge, ', 0, 1\rangle$ is the Boolean algebra arising from a Boolean lattice $\langle B; \leq\rangle$, by a *filter of* $\mathbf{B}$, we simply mean a filter of $\langle B; \leq\rangle$. For any set I, a *filter over* I shall mean a filter of the Boolean lattice $\langle \mathcal{P}(I); \subseteq\rangle$.

Lemma 0.30. *Let* $\mathbf{B} = \langle B; \vee, \wedge, ', 0, 1\rangle$ *be a Boolean algebra and* $\mathcal{G}$ *a filter of* $\mathbf{B}$. *Then* $1 \in \mathcal{G}$. *Also* $\mathcal{G}$ *is proper (i.e.,* $\mathcal{G} \neq B$*) if and only if* $0 \notin \mathcal{G}$.

An *ultrafilter* of a Boolean algebra $\mathbf{B}$ is a *proper* filter of $\mathbf{B}$ that is maximal, with respect to $\subseteq$, among all proper filters of $\mathbf{B}$. The next result is a routine application of Zorn's Lemma.

Theorem 0.31. *Let* $\mathbf{B} = \langle B; \vee, \wedge, ', 0, 1\rangle$ *be a Boolean algebra. If* $\mathcal{F}$ *is a proper filter of* $\mathbf{B}$ *then there exists an ultrafilter* $\mathcal{U}$ *of* $\mathbf{B}$ *such that* $\mathcal{F} \subseteq \mathcal{U}$.

Let $\{\mathbf{A}_i : i \in I\}$ be a family of algebras of the same type and let $a, b \in \prod_{i \in I} A_i$. The *equalizer* $[[a = b]]$ of a and b is defined to be $\{i \in I : a(i) = b(i)\}$. Let $\mathcal{G}$ be a filter over the index set I. We define a binary relation $\theta_{\mathcal{G}}$ on $\prod_{i \in I} A_i$

[3] A slick proof of this appears in Examples 2.4 and 2.5.

as follows: for $a, b \in \prod_{i\in I} A_i$,

$$(a,b) \in \theta_{\mathcal{G}} \text{ if and only if } [[a=b]] \in \mathcal{G}.$$

Then $\theta_{\mathcal{G}}$ is a congruence relation on $\prod_{i\in I} \mathbf{A}_i$; the quotient algebra $(\prod_{i\in I} \mathbf{A}_i)/\theta_{\mathcal{G}}$ is called a *reduced product* and denoted by $\prod_{i\in I} \mathbf{A}_i/\mathcal{G}$. If $\mathcal{G}$ is an *ultrafilter* over I, we call $\prod_{i\in I} \mathbf{A}_i/\mathcal{G}$ an *ultraproduct* of the family $\{\mathbf{A}_i : i \in I\}$. If $a \in \prod_{i\in I} A_i$, we write $a/\mathcal{G}$ for $a/\theta_{\mathcal{G}}$.

Lemma 0.32. *Let $\{\mathbf{B}_i : i \in I\}$ be a family of algebras of the same type and let $\mathcal{U}$ be an ultrafilter over I. Let $\mathbf{C} = \prod_{i\in I} \mathbf{B}_i$ and let $\mathbf{D}$ be the ultraproduct $\mathbf{C}/\theta_{\mathcal{U}} = \prod_{i\in I} \mathbf{B}_i/\mathcal{U}$, where*

$$\theta_{\mathcal{U}} = \{(c_1,c_2) \in C^2 : [[c_1 = c_2]] \in \mathcal{U}\} \ (\in Con(\mathbf{C})).$$

Let $\alpha_i \in Con(\mathbf{B}_i)$ for each $i \in I$ and define

$$\prod_{i\in I} \alpha_i := \{(c_1,c_2) \in C^2 : (c_1(i), c_2(i)) \in \alpha_i \textit{ for all } i \in I\}$$

and

$$\eta = \{(c_1,c_2) \in C^2 : \{i \in I : (c_1(i), c_2(i)) \in \alpha_i\} \in \mathcal{U}\}.$$

Then $\eta, \prod_{i\in I} \alpha_i \in Con(\mathbf{C})$ and $\eta = \theta_{\mathcal{U}} \vee (\prod_{i\in I} \alpha_i)$ in **Con(C)**.

Proof.

The verification that $\eta, \prod_{i\in I} \alpha_i \in Con(\mathbf{C})$ is straightforward and clearly $\theta_{\mathcal{U}} \cup (\prod_{i\in I} \alpha_i) \subseteq \eta$. Let $\theta_{\mathcal{U}} \cup (\prod_{i\in I} \alpha_i) \subseteq \sigma \in Con(\mathbf{C})$. Let $(c_1, c_2) \in \eta$. Then

$$J := \{i \in I : (c_1(i), c_2(i)) \in \alpha_i\} \in \mathcal{U}.$$

Define $a \in C$ by :

$$a(i) = \begin{cases} c_2(i) & \text{if } i \in J \\ c_1(i) & \text{if } i \in I \setminus J. \end{cases}$$

Then $(c_1, a) \in \prod_{i\in I} \alpha_i$ and $(a, c_2) \in \theta_{\mathcal{U}}$, so $(c_1,a), (a,c_2) \in \sigma$, hence $(c_1,c_2) \in \sigma$. Thus $\eta \subseteq \sigma$. It follows that $\eta = \theta_{\mathcal{U}} \vee (\prod_{i\in I} \alpha_i)$.

□

We shall use the following results about ultraproducts:

Lemma 0.33. [BS81, Lemma 6.5, p146]

If $\{\mathbf{A}_i : i \in I\}$ is a finite set of finite algebras, say $\{\mathbf{B}_1, \ldots, \mathbf{B}_k\}$ (where I is not assumed to be finite), and $\mathcal{U}$ is an ultrafilter over I then $\prod_{i\in I} \mathbf{A}_i/\mathcal{U}$ is isomorphic to one of the algebras $\mathbf{B}_1, \ldots, \mathbf{B}_k$, namely to that $\mathbf{B}_j$ such that

$$\{i \in I : \mathbf{A}_i = \mathbf{B}_j\} \in \mathcal{U}.$$

We shall use the symbol P_U to denote the class operator used to obtain ultraproducts.

Theorem 0.34. (Jónsson's Theorem) [Jón67]

Let K be a class of algebras of the same type such that $V(K)$ is a congruence distributive variety. If $\mathbf{A}$ is a subdirectly irreducible algebra in $V(K)$, then

$$\mathbf{A} \in HSP_U(K);$$

hence

$$V(K) = IP_S HSP_U(K).$$

Theorem 0.35. [BS81, Theorem 2.14, p213]

Every algebra $\mathbf{A}$ can be embedded into an ultraproduct of finitely generated subalgebras of $\mathbf{A}$.

0.5 Terms and Polynomials. Let $\mathcal{T} = \langle \mathsf{F}, ar \rangle$ be a fixed type (i.e., language) of algebras and $\mathbf{A} = \langle A; F \rangle$ a $\mathcal{T}$-algebra with $A \cap \mathsf{F} = \emptyset$. Let $A' = \{a' : a \in A\}$ be a "copy" of A disjoint from $A \cup \mathsf{F}$. (By this we imply that $a \mapsto a'$ $(a \in A)$ is one-to-one.) We define $\mathsf{F}[\mathbf{A}] = \mathsf{F} \cup A'$ and a function $ar' : \mathsf{F}[\mathbf{A}] \to \omega$ by $ar' = ar \cup \{(a', 0) : a \in A\}$. Let $\mathcal{T}[\mathbf{A}]$ be the type $\langle \mathsf{F}[\mathbf{A}], ar' \rangle$. $\mathbf{A}$ is the F-reduct of a $\mathcal{T}[\mathbf{A}]$-algebra $\mathbf{A}'$ where $(a')^{\mathbf{A}'} = a$ for all $a \in A$. For simplicity of notation, however, we usually denote each a' by a, unless there is a danger of confusion.

Let X be a set whose elements will be called *variables.*[4] The set $T(X)$ of all $\mathcal{T}$-*terms* over X is defined to be the smallest set such that

(i) $X \subseteq T(X)$;

(ii) if $t_1, \ldots, t_n \in T(X)$ and $f \in \mathsf{F}$ with $ar(f) = n$ then the formal expression $f(t_1, \ldots, t_n)$ is an element of $T(X)$. (We take this to imply that $c \in T(X)$ for every nullary operation symbol $c \in \mathsf{F}$.)

For $t \in T(X)$ and $x_1, \ldots, x_n \in X$, if we write t as $t(x_1, \ldots, x_n)$ we mean that the variables occurring in t are among $x_1, \ldots, x_n$. We call t an *n-ary term* if the number of (distinct) variables that occur in t is at most n.

Let $t(x_1, \ldots, x_n) \in T(X)$ and let $\mathbf{B}$ be a $\mathcal{T}$-algebra. We define a map $t^{\mathbf{B}} : B^n \to B$, called the *term function of t on* $\mathbf{B}$, recursively as follows: for $b_1, \ldots, b_n \in B$,

(i) if t is a variable, x_i (where $1 \leq i \leq n$), then $t^{\mathbf{B}}(b_1, \ldots, b_n) = b_i$;

(ii) if t has the form $f(t_1(x_1, \ldots, x_n), \ldots, t_k(x_1, \ldots, x_n))$, where $f \in \mathsf{F}$ and $ar(f) = k$ and $t_1^{\mathbf{B}}, \ldots, t_k^{\mathbf{B}} : B^n \to B$ have been defined then

$$t^{\mathbf{B}}(b_1, \ldots, b_n) = f^{\mathbf{B}}(t_1^{\mathbf{B}}(b_1, \ldots, b_n), \ldots, t_k^{\mathbf{B}}(b_1, \ldots, b_n)).$$

[4] We can always arrange that X is disjoint from $\mathsf{F} \cup A \cup A' \cup F$ for any single algebra $\mathbf{A}$ under discussion, so we shall assume that this is the case.

We take this to imply that if t is a constant symbol c of $\mathcal{T}$ then $t^{\mathbf{B}} = c^{\mathbf{B}}$.

Replacing $\mathcal{T}$ by $\mathcal{T}[\mathbf{A}]$ in the above definition, for each $n \in \omega$, the n-ary terms t (over X) of the language $\mathcal{T}[\mathbf{A}]$ are now also defined. Their corresponding term functions on the algebra $\mathbf{A}'$ shall be called the *n-ary polynomials* (or *n-ary polynomial functions*) of $\mathbf{A}$.

The following theorem establishes that term functions behave like fundamental operations with respect to congruences and homomorphisms and that they can be employed in a useful description of the algebra generated by a given set. Theorem 0.37 then shows that polynomial functions are similarly useful when it comes to describing principal congruence generation.

Theorem 0.36. [BS81, Theorem 10.3, p63]

(i) *If p is an n-ary $\mathcal{T}$-term (over X) and $\theta \in Con(\mathbf{A})$ and $a_1, \dots, a_n, a_1', \dots, a_n' \in A$ with $(a_i, a_i') \in \theta$ for $i = 1, \dots, n$ then*

$$(p^{\mathbf{A}}(a_1, \dots, a_n), p^{\mathbf{A}}(a_1', \dots, a_n')) \in \theta.$$

(ii) *If p is as in (i) and $\alpha : \mathbf{A} \to \mathbf{B}$ is a homomorphism then*

$$\alpha(p^{\mathbf{A}}(a_1, \dots, a_n)) = p^{\mathbf{B}}(\alpha(a_1), \dots, \alpha(a_n)) \text{ for all } a_1, \dots, a_n \in A.$$

(iii) *If $Y \subseteq A$ then $Sg^{\mathbf{A}}(Y) = \{p^{\mathbf{A}}(a_1, \dots, a_n) : p$ is an n-ary $\mathcal{T}$-term for some $n \in \omega$ and some $a_1, \dots, a_n \in Y\}$.*

In particular, if $\mathbf{B}$ is a subalgebra of $\mathbf{A}$, p is an n-ary $\mathcal{T}$-term and $b_1, \dots, b_n \in B$ then $p^{\mathbf{A}}(b_1, \dots, b_n) = p^{\mathbf{B}}(b_1, \dots, b_n)$.

Theorem 0.37. (Mal'cev's Lemma) [Mal54] [Dud83b] *(See also* [BS81, Lemma 3.1, p221]*)*

For an algebra $\mathbf{A}$ and $a, b, c, d \in A$, the following conditions are equivalent:

(i) $(c, d) \in \Theta^{\mathbf{A}}(a, b)$.

(ii) *There exist $n \in \omega$ ($n > 0$) and binary polynomials $f_1, \dots, f_n$ of $\mathbf{A}$ such that*

$$\begin{aligned} c &= f_1(a, b), \\ f_i(b, a) &= f_{i+1}(a, b) \text{ for all } i \in \{1, \dots, n-1\}, \\ f_n(b, a) &= d. \end{aligned}$$

(iii) *There exist $n \in \omega$ ($n > 0$) and unary polynomials $g_1, \dots, g_n$ of $\mathbf{A}$ and pairs $(u_1, v_1), \dots, (u_n, v_n)$ such that $\{u_i, v_i\} = \{a, b\}$ for all $i \in \{1, \dots, n\}$ and*

$$\begin{aligned} c &= g_1(u_1), \\ g_i(v_i) &= g_{i+1}(u_{i+1}) \textit{ for all } i \in \{1, \dots, n-1\}, \\ g_n(v_n) &= d. \end{aligned}$$

Let $\mathbf{A}$ be an algebra. A binary relation η on A is called a *semicongruence* of $\mathbf{A}$ if it is reflexive and compatible. In this case, for any n-ary polynomial p of $\mathbf{A}$, if $(a_i, b_i) \in \eta$ for all $i \in \{1, \dots, n\}$ then $(p(a_1, \dots, a_n), p(b_1, \dots, b_n)) \in \eta$.

The set $Sc(\mathbf{A})$ of all semicongruences of $\mathbf{A}$ is an algebraic closure system in $\langle \mathcal{P}(A \times A); \subseteq \rangle$, hence it is the universe of an algebraic lattice $\mathbf{Sc(A)}$. For $X \subseteq A^2$, the least semicongruence of $\mathbf{A}$ containing X (i.e., the intersection of all semicongruences of $\mathbf{A}$ containing X) is denoted by $\sigma^{\mathbf{A}}(X)$. We abbreviate $\sigma^{\mathbf{A}}(\{(a,b)\})$ by $\sigma^{\mathbf{A}}(a,b)$.

The following refinement of Mal'cev's Lemma will be labour-saving later.

Lemma 0.38. [Dud83a]

Let $\mathbf{A}$ be an algebra and $a, b \in A$. Let $Y = \{(c,d) \in A^2 :$ there exists a unary polynomial q of $\mathbf{A}$ such that $q(a) = c$ and $q(b) = d\}$. Then $\sigma^{\mathbf{A}}(a,b) = Y$.

0.6 Model Theoretic Algebra. We continue to consider a fixed type $\mathcal{T} = \langle \mathsf{F}, ar \rangle$, a given $\mathcal{T}$-algebra $\mathbf{A} = \langle A; F \rangle$ and a set X (of variables). The set of *(first order) formulas of type $\mathcal{T}$* (or *$\mathcal{T}$-formulas*) over X is the smallest set S of expressions (i.e., finite strings of symbols) that use only symbols from

$$\mathsf{F} \cup X \cup \{(,)\} \cup \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, \approx\} \cup \{,\}\ ^{5}$$

such that (i) all *$\mathcal{T}$-equations* $p \approx q$ $(p, q \in T(X))$ over X are elements of S and (ii) whenever $\Phi, \Phi_1, \Phi_2 \in S$ and $x \in X$ then S also contains each of:

$$\begin{array}{lll} (\Phi_1) \wedge (\Phi_2), & (\Phi_1) \vee (\Phi_2), & \neg(\Phi), \\ (\Phi_1) \rightarrow (\Phi_2), & (\Phi_1) \leftrightarrow (\Phi_2), & \\ \forall x(\Phi), & \exists x(\Phi). & \end{array}$$

We adopt standard bracket-omission conventions. We usually abbreviate $\neg(p \approx q)$ as $p \not\approx q$. Formulas of the form $p \approx q$ and $p \not\approx q$ are called *atomic* and *negated atomic* formulas, respectively. Let Φ_1 and Φ be $\mathcal{T}$-formulas over X and $x \in X$. We call Φ_1 a *subformula* of Φ if it is a consecutive string of symbols occurring in Φ. An occurrence of x in Φ is called *free* if it is not an occurrence of x in any subformula Φ of the form $\forall x(\Psi)$ or $\exists x(\Psi)$; otherwise it is called a *bound* occurrence of x. A *free* variable of Φ means a variable $y \in X$ that has a free occurrence in Φ. A (first order) *$\mathcal{T}$-sentence* is a $\mathcal{T}$-formula with no free variables. If $x_1, \dots, x_n \in X$, we sometimes write Φ as $\Phi(x_1, \dots, x_n)$

[5] This union is assumed disjoint, and disjoint from $A \cup A' \cup F$.

to indicate that the *free* variables of Φ are all among $x_1, \ldots, x_n$. We call Φ *quantifier-free* if the symbols $\forall$ and $\exists$ do not occur in Φ.

Let $\Phi(x_1, \ldots, x_n)$ be a $\mathcal{T}$-formula. If $t_1, \ldots, t_n$ are $\mathcal{T}$-terms then $\Phi[t_1, \ldots, t_n]$ denotes the $\mathcal{T}$-formula resulting from replacing, simultaneously, each free occurrence of x_i in Φ by t_i for all $i \in \{1, \ldots, n\}$. In particular, if $a_1, \ldots, a_n \in A$ then $\Phi[a_1, \ldots, a_n]$ is a $\mathcal{T}[\mathbf{A}]$-sentence. The atomic sentences of $\mathcal{T}[\mathbf{A}]$ all have the form $p[a_1, \ldots, a_n] \approx q[a_1, \ldots, a_n]$ for some $p, q \in T(X)$ and $a_1, \ldots, a_n \in A$. We define $\mathbf{A} \models p[a_1, \ldots, a_n] \approx q[a_1, \ldots, a_n]$ to mean that $p^{\mathbf{A}}(a_1, \ldots, a_n) = q^{\mathbf{A}}(a_1, \ldots, a_n)$. For other (i.e., non-atomic) *sentences* Φ of $\mathcal{T}[\mathbf{A}]$, we define $\mathbf{A} \models \Phi$ (to be read as $\mathbf{A}$ *satisfies* Φ or as Φ *is true in* $\mathbf{A}$ or as Φ *holds in* $\mathbf{A}$) in the obvious recursive way and we use $\not\models$ to mean "does not satisfy". For example, for *sentences* Φ, Φ_1, Φ_2 of $\mathcal{T}[\mathbf{A}]$,

$\mathbf{A} \models \Phi_1 \to \Phi_2$ denotes that $\mathbf{A} \not\models \Phi_1$ or $\mathbf{A} \models \Phi_2$ while

$\mathbf{A} \models \forall x\, \Phi(x)$ denotes that for every $a \in A$, $\mathbf{A} \models \Phi[a]$.

The *diagram* $D(\mathbf{A})$ of $\mathbf{A}$ is defined as the set of all atomic or negated atomic $\mathcal{T}[\mathbf{A}]$-sentences Φ such that $\mathbf{A} \models \Phi$.

For a formula (not necessarily a sentence) Φ of $\mathcal{T}[\mathbf{A}]$ whose free variables, in order of their first occurrence in Φ, read from left to right, are $x_1, x_2, \ldots, x_n$, the *(universal) closure* $\bar{\Phi}$ of Φ is the $\mathcal{T}[\mathbf{A}]$-sentence $\forall x_1 \forall x_2 \ldots \forall x_n \Phi$; we define $\mathbf{A} \models \Phi$ to mean $\mathbf{A} \models \bar{\Phi}$ in this case. For a class K of $\mathcal{T}$-algebras and a set Σ of $\mathcal{T}[\mathbf{A}]$-formulas, we define $\mathbf{A} \models \Sigma$ to mean that $\mathbf{A} \models \Phi$ for all $\Phi \in \Sigma$, while $K \models \Sigma$ means that $\mathbf{B} \models \Sigma$ for all $\mathbf{B} \in K$, and $K \models \Phi$ abbreviates $K \models \{\Phi\}$. If $\mathbf{A} \models \Sigma$ we call $\mathbf{A}$ a *model* of Σ.

For a set $\Sigma \cup \{\Phi\}$ of $\mathcal{T}$*-sentences* over X, we define $\Sigma \vdash_{Th(\mathcal{T})} \Phi$ (or, briefly, $\Sigma \vdash \Phi$ if $\mathcal{T}$ is understood) to mean that for every $\mathcal{T}$-algebra $\mathbf{B}$, if $\mathbf{B} \models \Sigma$ then $\mathbf{B} \models \Phi$.[6]

We abbreviate $\emptyset \vdash_{Th(\mathcal{T})} \Phi$ as $\vdash_{Th(\mathcal{T})} \Phi$ (or $\vdash \Phi$) and call Φ a $\mathcal{T}$*-theorem* if this is the case. If we wish to give $Th(\mathcal{T})$ a concrete meaning we can define it as the set of all $\mathcal{T}$-theorems; we will call this set the *first order theory with equality over the language* $\mathcal{T}$.

For a set Σ of $\mathcal{T}$-sentences and for $\mathcal{T}$-formulas Φ_1, Φ_2, we say that Φ_1 and Φ_2 are *logically equivalent modulo* Σ if $\Sigma \vdash_{Th(\mathcal{T})} \Phi_1 \leftrightarrow \Phi_2$. If, in addition, $\Sigma = \emptyset$, we say that Φ_1 and Φ_2 are *logically equivalent.* [7]

[6] By the Validity and Completeness Theorems of first order logic, $\Sigma \vdash_{Th(\mathcal{T})} \Phi$ may be characterized syntactically by the existence of a first order "proof" of Φ "from" Σ (see, e.g. [Men87]) but such a syntactic perspective will not be required in this thesis.

[7] To avoid ambiguity, if Σ contains $\mathcal{T}$-formulas that are not sentences, we leave the expression $\Sigma \vdash \Phi$ undefined; we never use such expressions in this thesis.

A $\mathcal{T}$-formula Φ (over X) is said to be in *prenex form* if it is of the form $Q_1x_1Q_2x_2\ldots Q_nx_n\Psi$ where $n \in \omega$ and $Q_1, Q_2, \ldots, Q_n \in \{\forall, \exists\}$ and Ψ is a quantifier-free formula.[8]

A formula Φ in prenex form is called *universal* [respectively, *existential*] if the symbol $\exists$ [respectively $\forall$] does not occur in it; it is called *positive* if no symbol from $\{\wedge, \vee, \neg, \rightarrow, \leftrightarrow\}$ other than $\wedge$ and $\vee$ occurs in it.

A formula Φ is a $\forall\exists$*–fomula* if it is in prenex form and all (if any) occurrences of $\forall$ in Φ precede all (if any) occurrences of $\exists$ in Φ.

We abbreviate formulas of the forms $\Phi_1 \wedge \Phi_2 \wedge \ldots \wedge \Phi_n$ and $\Phi_1 \vee \Phi_2 \vee \ldots \Phi_n$ by $\bigwedge_{i=1}^n \Phi_i$ and $\bigvee_{i=1}^n \Phi_i$, respectively. A $\mathcal{T}$*-quasi-equation* (over X) is a formula of the form $(\bigwedge_{i=1}^n \Phi_i) \rightarrow \Psi$, where each of $\Phi_1, \Phi_2, \ldots, \Phi_n, \Psi$ is a $\mathcal{T}$-equation $p \approx q$ $(p, q \in T(X))$. The universal closure $\bar{\Phi}$ of a $\mathcal{T}$-quasi-equation [respectively a $\mathcal{T}$-equation] Φ is called a $\mathcal{T}$*-quasi-identity* [respectively, a $\mathcal{T}$*-identity*].[9]

A class K of $\mathcal{T}$-algebras is said to be *axiomatized* by a set Σ of $\mathcal{T}$-formulas if K is the class of *all* $\mathcal{T}$-algebras $\mathbf{B}$ such that $\mathbf{B} \models \Sigma$.

A class K of $\mathcal{T}$-algebras is called a $\mathcal{T}$*-(quasi-)equational class* if it is axiomatized by a set of $\mathcal{T}$-(quasi-)identities. We often drop the prefix $\mathcal{T}$- when the type is understood.

Theorem 0.39. *(Mal'cev)* [BS81, Theorem 2.23, p218]

The following are equivalent for a class K of $\mathcal{T}$-algebras:

(i) *K is a quasi-equational class.*

(ii) *K is closed under the class operators I, S, P and P_U.*

(iii) *$K = ISPP_U(K')$ for some class K' of $\mathcal{T}$-algebras.*

A quasi-equational class is also called a *quasivariety*. It follows from the above that, for any class K of $\mathcal{T}$-algebras, $ISPP_U(K)$ is the smallest $\mathcal{T}$-quasivariety containing K. We therefore write $Q(K) = ISPP_U(K)$ and call this the quasivariety *generated* by K.

Theorem 0.40. (Birkhoff's Theorem) [BS81, Theorem 11.9, p75]

Let K be a class of $\mathcal{T}$-algebras. Then K is an equational class if and only if K is a variety.

Let Φ be a $\mathcal{T}$-formula over X with free variables $x_1, \ldots, x_n \in X$ and let Σ be a set of $\mathcal{T}$-sentences over X. We say that Φ *persists* (modulo Σ) *under*

(i) *extensions* (ii) *subalgebras* (iii) *homomorphisms* (iv) *unions of chains*

[8] The case $n = 0$ is allowed, so every quantifier-free $\mathcal{T}$-formula is in prenex form.

[9] From the point of view of satisfaction, however, it is harmless to blur the distinction between "identity" and "equation".

(respectively) provided that for any $\mathcal{T}$-algebras $\mathbf{A}, \mathbf{B}$ such that $\mathbf{A}, \mathbf{B} \models \Sigma$ and for any $a_1, \ldots, a_n \in A$, the following (respective) conditions are met:

(i) if $\mathbf{A} \leq \mathbf{B}$ and $\mathbf{A} \models \Phi[a_1, \ldots, a_n]$ then $\mathbf{B} \models \Phi[a_1, \ldots, a_n]$;

(ii) if $\mathbf{A} \leq \mathbf{B}$ and $\mathbf{B} \models \Phi[a_1, \ldots, a_n]$ then $\mathbf{A} \models \Phi[a_1, \ldots, a_n]$;

(iii) if $f : \mathbf{A} \to \mathbf{B}$ is a homomorphism and $\mathbf{A} \models \Phi[a_1, \ldots, a_n]$ then $\mathbf{B} \models \Phi[f(a_1), \ldots, f(a_n)]$;

(iv) if $\mathbf{B} = \cup_{\alpha<\beta}\mathbf{A}_\alpha$ is the union of a chain $\langle \mathbf{A}_\alpha : \alpha < \beta \rangle$ of $\mathcal{T}$-algebras satisfying Σ and $\mathbf{A} = \mathbf{A}_0$ and $\mathbf{A}_\alpha \models \Phi[a_1, \ldots, a_n]$ for all $\alpha < \beta$ then $\mathbf{B} \models \Phi[a_1, \ldots, a_n]$.

Of course if $\Sigma \subseteq Th(\mathcal{T})$ (e.g. if $\Sigma = \emptyset$) then all the above references to Σ may be omitted. Parts (i) and (ii) of the next result are consequences of the *Loś-Tarski Theorem* (see [Hod97, Theorem 5.4.4, Corollary 5.4.5]), (iii) is a specialization of *Lyndon's Theorem* (see [Hod97, Corollary 8.3.5]) while (iv) is called the *Chang-Łoś-Suszko Theorem* (see [Hod97, Theorem 5.4.9]).

Theorem 0.41. *Let Φ be a $\mathcal{T}$-formula and Σ be a set of $\mathcal{T}$-sentences (over X). Then Φ persists (modulo Σ) under*

(i) extensions (ii) subalgebras (iii) homomorphisms (iv) union of chains

(respectively) if and only if Φ is logically equivalent (modulo Σ) to a

(i) existential (ii) universal (iii) positive (iv) $\forall\exists$

$\mathcal{T}$-formula (respectively).

A property P that $\mathcal{T}$-algebras either do or do not possess is said to be *(first order) definable* (modulo a set Σ of $\mathcal{T}$-sentences) if there is a $\mathcal{T}$-formula (equivalently, a $\mathcal{T}$-sentence) Φ such that the $\mathcal{T}$-algebras satisfying Σ that have property P are just the $\mathcal{T}$-algebras satisfying $\Sigma \cup \{\Phi\}$.

If $0 < k < \omega$ then the property of having at least k elements is definable by a formula Φ_k; e.g., we may take Φ_3 to be

$$\exists x \exists y \exists z ((x \not\approx y) \wedge (x \not\approx z) \wedge (y \not\approx z)).$$

If Ψ_k is $\Phi_k \wedge (\neg\Phi_{k+1})$ then Ψ_k defines having exactly k elements. Having at most k elements is definable by $\Psi_1 \vee \Psi_2 \vee \ldots \vee \Psi_k$.

The following theorem accounts for the importance of ultraproducts.

Theorem 0.42. (Łoś' Theorem) [BS81, Theorem 2.9, p210]

Given $\mathcal{T}$-algebras $\mathbf{A}_i$, $i \in I$, an ultrafilter $\mathcal{U}$ over I, any (first order) $\mathcal{T}$-formula $\Phi(x_1, \ldots, x_n)$ and any $a_1, \ldots, a_n \in \prod_{i\in I} A_i$, we have

$$\prod_{i\in I} \mathbf{A}_i/\mathcal{U} \models \Phi[a_1/\mathcal{U}, \ldots, a_n/\mathcal{U}] \text{ iff } \{i \in I : \mathbf{A}_i \models \Phi[a_1(i), \ldots, a_n(i)]\} \in \mathcal{U}.$$

Thus, if a first order formula holds in all members of a class K of $\mathcal{T}$-algebras then it holds in any ultraproduct of members of K. In particular:

(i) *First order definable properties are preserved by ultraproducts.*

(ii) *If $|A_i| < k \in \omega$ for all $i \in I$ then $|\prod_{i \in I} A_i/\mathcal{U}| < k$, regardless of $|I|$ and of $|\mathsf{F}|$ (where $\mathcal{T} = \langle \mathsf{F}, ar \rangle$). Similarly for $\leq, =, >, \geq k$.*

A set Σ of $\mathcal{T}$-formulas over X is said to be *satisfiable* if there is a $\mathcal{T}$- algebra $\mathbf{B}$ and a function $f : X \to B$ such that for any $\Phi = \Phi(x_1, \ldots, x_n) \in \Sigma$, we have $\mathbf{B} \models \Phi[f(x_1), \ldots, f(x_n)]$. (In this case we also say that Σ is satisfiable in $\mathbf{B}$.) The following strong form of the *Compactness Theorem* of first order logic will be needed. Since most texts on logic state less general forms of the theorem, we sketch the proof here.

Theorem 0.43. *Let Γ be any set of $\mathcal{T}$-formulas over X such that every finite subset of Γ is satisfiable. Then Γ is satisfiable.*

Proof.

Let $\mathcal{P}_\omega(\Gamma)$ be the set of all finite subsets of Γ. For each $\Delta \in \mathcal{P}_\omega(\Gamma)$, choose a $\mathcal{T}$-algebra $\mathbf{A}_\Delta$ and a function $f_\Delta : X \to A_\Delta$ such that whenever $\Phi \in \Delta$ has free variables $x_1, \ldots, x_n$, then $\mathbf{A}_\Delta \models \Phi[f_\Delta(x_1), \ldots, f_\Delta(x_n)]$ and define $J_\Delta = \{\Delta' \in \mathcal{P}_\omega(\Gamma) : \Delta' \supseteq \Delta\}$.

Let $\mathcal{F} = \{J \subseteq \mathcal{P}_\omega(\Gamma) : J \supseteq J_\Delta$ for some $\Delta \in \mathcal{P}_\omega(\Gamma)\}$. Then $\mathcal{F}$ is a proper filter over $\mathcal{P}_\omega(\Gamma)$ and is contained in an ultrafilter $\mathcal{U}$ over $\mathcal{P}_\omega(\Gamma)$ (by Theorem 0.31).

Let $\mathbf{C} = \prod_{\Delta \in \mathcal{P}_\omega(\Gamma)} \mathbf{A}_\Delta$ and let $\mathbf{C}/\mathcal{U}$ be the corresponding ultraproduct. Define $f : X \to C$ and $g : X \to C/\mathcal{U}$ by

$$(f(x))(\Delta) = f_\Delta(x) \text{ and } g(x) = f(x)/\mathcal{U} \quad (x \in X \text{ and } \Delta \in \mathcal{P}_\omega(\Gamma)).$$

For each $\Phi \in \Gamma$ with free variables $x_1, \ldots, x_n$, say,

$$\{\Delta \in \mathcal{P}_\omega(\Gamma) : \mathbf{A}_\Delta \models \Phi[(f(x_1))(\Delta), \ldots, (f(x_n))(\Delta)]\} \supseteq J_{\{\Phi\}} \in \mathcal{F} \subseteq \mathcal{U}$$

so by Łoś' Theorem, $\mathbf{C}/\mathcal{U} \models \Phi[g(x_1), \ldots, g(x_n)]$.

□

The Compactness Theorem is usually stated with the added assumption that Γ consists of $\mathcal{T}$-*sentences*, in which case the function f in the definition of "satisfiability" plays no role and the notion of satisfiability reduces to that of possessing a model. From this one derives the next corollary easily; it is also known as the *Compactness Theorem.*

Corollary 0.44. [BS81, Corollary 2.13, p212]

Let $\Sigma \cup \{\Phi\}$ be a set of $\mathcal{T}$-sentences (over X) such that $\Sigma \vdash_{Th(\mathcal{T})} \Phi$. Then there exists a finite subset Σ' of Σ such that $\Sigma' \vdash_{Th(\mathcal{T})} \Phi$.

Theorem 0.45. (Downward Löwenheim-Skolem Theorem) [Hod97, Corollary 3.1.4]

Let $\mathbf{B}$ be a $\mathcal{T}$-algebra (recall that $\mathcal{T} = \langle \mathsf{F}, ar\rangle$) and $Y \subseteq B$ and let m be an infinite cardinal such that $|\mathsf{F}| + |Y| \leq \mathsf{m} \leq |B|$. Then there is a subalgebra $\mathbf{C}$ of $\mathbf{B}$ with $Y \subseteq C$ and $|C| = \mathsf{m}$ such that $\mathbf{C}$ and $\mathbf{B}$ satisfy exactly the same (first order) $\mathcal{T}$-sentences.

0.7 Free Algebras. We continue to assume that all algebras have type $\mathcal{T} = \langle \mathsf{F}, ar\rangle$; for each $n \in \omega$, let $\mathsf{F}_n = \{f \in \mathsf{F} : ar(f) = n\}$. We also continue to assume that a fixed set (of variables) X is given.

Recall that $T(X)$ is the set of all $\mathcal{T}$-terms over X. If $T(X) \neq \emptyset$ then we define the *term algebra of type $\mathcal{T}$ over X* to be the $\mathcal{T}$-algebra $\mathbf{T}(X) = \langle T(X); G\rangle$, with $G = \{f^{\mathbf{T}(X)} : f \in \mathsf{F}\}$, where, if $f \in \mathsf{F}_n$, the n-ary operation $f^{\mathbf{T}(X)} : (T(X))^n \to T(X)$ is defined by

$$f^{\mathbf{T}(X)}(p_1, \dots, p_n) = f(p_1, \dots, p_n) \quad (p_1, \dots, p_n \in T(X)).$$

If $f \in \mathsf{F}_0$, interpret this as $f^{\mathbf{T}(X)} = f$.

Note that $\mathbf{T}(X)$ exists if and only if $T(X) \neq \emptyset$ if and only if $X \neq \emptyset$ or $\mathsf{F}_0 \neq \emptyset$. Note also that $\mathbf{T}(X)$ is generated by X.

Let K be a class of $\mathcal{T}$-algebras and $\mathbf{U} = \langle U; G\rangle$ a $\mathcal{T}$-algebra. Let $Y \subseteq U$ be a generating set for $\mathbf{U}$. We say that $\mathbf{U}$ has the *universal mapping property (U.M.P.)* for K over Y if the following condition holds: for every $\mathbf{A} = \langle A; G_A\rangle \in K$ and every function $\alpha : Y \to A$, there exists a homomorphism $\beta : \mathbf{U} \to \mathbf{A}$ which extends α, i.e., $\beta(y) = \alpha(y)$ for all $y \in Y$. In this case the homomorphism β is unique, Y is called a *set of free generators* of $\mathbf{U}$ and $\mathbf{U}$ is said to be *freely generated* by Y (with respect to K).

Theorem 0.46. [BS81, Theorem 10.8, p66]

If $X \neq \emptyset$ or $\mathsf{F}_0 \neq \emptyset$, the term algebra $\mathbf{T}(X)$ has the universal mapping property for the class of all $\mathcal{T}$-algebras over X.

Let K be a class of $\mathcal{T}$-algebras and suppose $\mathbf{T}(X)$ exists. Define $\theta_K(X) = \bigcap\{\varphi \in Con(\mathbf{T}(X)) : \mathbf{T}(X)/\varphi \in IS(K)\} \in Con(\mathbf{T}(X))$. For each $x \in X$, define $\bar{x} = x/\theta_K(X)$ and $\bar{X} = \{\bar{x} : x \in X\}$, which we write as $X/\theta_K(X)$. We define the *K-free $\mathcal{T}$-algebra over $\bar{X}$* (denoted $\mathbf{F}_K(\bar{X})$) to be the $\mathcal{T}$-algebra $\mathbf{T}(X)/\theta_K(X)$. If K contains a nontrivial algebra then the map from $x \mapsto \bar{x}$ defines a bijection from X onto $\bar{X}$.

Note that $\mathbf{F}_K(\bar{X})$ exists if and only if $\mathbf{T}(X)$ exists. If $p = p(x_1, \ldots, x_n) \in T(X)$, we write $\bar{p}$ for $p^{\mathbf{F}_K(\bar{X})}(\bar{x}_1, \ldots, \bar{x}_n)$ where $p^{\mathbf{F}_K(\bar{X})}$ is the n-ary term function on $\mathbf{F}_K(\bar{X})$ associated with p. If $\mathbf{F}_K(\bar{X})$ exists, then it is generated by $\bar{X}$ since $\mathbf{T}(X)$ is generated by X. If X is finite, say $X = \{x_1, \ldots, x_n\}$, we often write $\mathbf{F}_K(\bar{x}_1, \ldots, \bar{x}_n)$ for $\mathbf{F}_K(\bar{X})$ and call this the *K-free $\mathcal{T}$-algebra on n free generators.*

Theorem 0.47. *(Birkhoff)* [BS81, Theorem 10.10, p67]

Suppose $\mathbf{T}(X)$ *exists, and let K be a class of $\mathcal{T}$-algebras. Then* $\mathbf{F}_K(\bar{X})$ *has the U.M.P. for K over $\bar{X}$. If* $\mathbf{U} \in V(K)$ *is a $\mathcal{T}$-algebra having the U.M.P. for K over a set Y and there is a bijection $\alpha : Y \to \bar{X}$ then there is a (unique) isomorphism* $\beta : \mathbf{U} \cong \mathbf{F}_K(\bar{X})$ *such that $\beta|_Y = \alpha$.*

Corollary 0.48. [BS81, Corollary 10.11, p68]

If K is a class of $\mathcal{T}$-algebras and $\mathbf{A} \in K$ *then for sufficiently large X,* $\mathbf{A} \in H(\mathbf{F}_K(\bar{X}))$. *More precisely, if* $\mathbf{A}$ *is* n*−generated (where* n *is any cardinal) and* $|X| = \mathsf{n}$ *then* $\mathbf{A} \in H(\mathbf{F}_K(\bar{X}))$.

In general, $\mathbf{F}_K(\bar{X})$ is not a member of K. The following theorem asserts, however, that $\mathbf{F}_K(\bar{X})$ is embeddable into a direct product of elements of K.

Theorem 0.49. *(Birkhoff)* [BS81, Theorem 10.12, p68]

Suppose $\mathbf{T}(X)$ *exists, and let K be a class of $\mathcal{T}$-algebras. Then* $\mathbf{F}_K(\bar{X}) \in ISP(K)$. *Thus, if K is closed under I, S and P, in particular if K is a variety or quasivariety, then* $\mathbf{F}_K(\bar{X}) \in K$.

Theorem 0.50. [BS81, Theorem 11.4, p73]

Let K be a class of $\mathcal{T}$-algebras and let $p, q \in T(X)$. Then the following conditions are equivalent:

(i) $K \models p \approx q$.

(ii) $\mathbf{F}_K(\bar{X}) \models p \approx q$.

(iii) $\bar{p} = \bar{q}$ *in* $\mathbf{F}_K(\bar{X})$.

(iv) $(p, q) \in \theta_K(X)$.

An algebra is said to be *locally finite* if every finitely generated subalgebra of $\mathbf{A}$ is finite (i.e., has a finite universe). A class K of algebras is said to be *locally finite* if every member of K is locally finite.

Lemma 0.51. *Let* $\mathbf{A}$ *be an algebra, let* $K = V(\mathbf{A}) = HSP(\mathbf{A})$, *and let* $\mathbf{F} = \mathbf{F}_K(\bar{x}_1, \ldots, \bar{x}_n)$. *Then* $|F| \leq |A|^{(|A|^n)}$. *Thus, if* $\mathbf{B} \in K$ *is generated by at most n elements of B then* $|B| \leq |A|^{(|A|^n)}$.

Proof.

Define $\rho : F \to A^{(A^n)}$ by $\rho(\bar{t}) = t^{\mathbf{A}}$. (Recall that $\bar{t}$ abbreviates $t^{\mathbf{F}}(\bar{x}_1, \dots, \bar{x}_n) \in F$ for any $t(x_1, \dots, x_n) \in T(X)$.) Let $t(x_1, \dots, x_n), s(x_1, \dots, x_n) \in T(X)$. If $\bar{t} = \bar{s}$ then $V \models t(x_1, \dots, x_n) \approx s(x_1, \dots, x_n)$ by Theorem 0.50 and $\mathbf{A} \in V$ so for all $a_1, \dots, a_n \in A$, $t^{\mathbf{A}}(a_1, \dots, a_n) = s^{\mathbf{A}}(a_1, \dots, a_n)$, i.e., $t^{\mathbf{A}} = s^{\mathbf{A}}$, so ρ is well-defined.

If $t^{\mathbf{A}} = s^{\mathbf{A}}$ then $\mathbf{A} \models t(x_1, \dots, x_n) \approx s(x_1, \dots, x_n)$ so $V(\mathbf{A}) \models t(x_1, \dots, x_n) \approx s(x_1, \dots, x_n)$ so $\bar{t} = \bar{s}$. Thus ρ is one-to-one. Therefore $|F| \leq |A^{(A^n)}| = |A|^{|A^n|} = |A|^{(|A|^n)}$. If $\mathbf{B} \in K$ is $n-$generated, then by Corollary 0.48, $\mathbf{B} \in H(F)$, so $|B| \leq |F|$. □

If $|A|$ is finite in the above lemma then for every $n \in \omega$ and every $n-$generated $\mathbf{B} \in K$, $|B|$ is finite. Thus we have:

Corollary 0.52. [BS81, Theorem 10.16, p70]

A finitely generated variety is locally finite.

Results esablishing so-called "Mal'cev conditions" for classes of varieties (as exemplified by Theorem 0.54 for congruence permutable varieties) usually make crucial use of properties of free algebras. In particular, the following strong variant of Theorem 0.50 will be needed in Chapter 2, where we treat congruence modularity.

Theorem 0.53. [BS81, Theorem 12.1, p77]

Let V be a variety, and r, s, r_i, s_i $(i = 1, \dots, n \in \omega)$. Let $\mathbf{F} = \mathbf{F}_V(\bar{X})$. The following conditions are equivalent:

(i) $(\bar{r}, \bar{s}) \in \Theta^{\mathbf{F}}(\{(\bar{r}_i, \bar{s}_i) : 1 \leq i \leq n\})$;

(ii) $V \models (\bigwedge_{i=1}^{n} r_i \approx s_i) \to r \approx s$.

Theorem 0.54. *(Mal'cev)* [BS81, Theorem 12.2, p78]

A $\mathcal{T}$-variety is congruence permutable if and only if there is a $\mathcal{T}$-term $p(x, y, z)$ such that

$$V \models p(x, x, y) \approx y \text{ and } V \models p(x, y, y) \approx x.$$

A term p as described in the above theorem is called a *Mal'cev term.*

Theorem 0.55. [BS81, Theorem 12.3, p79]

Let V be a $\mathcal{T}$-variety for which there is a ternary $\mathcal{T}$-term $m(x, y, z)$ such that

$$V \models m(x, x, y) \approx m(x, y, x) \approx m(y, x, x) \approx x.$$

Then V is congruence distributive.

A term m as described in the above theorem is known as a *majority* term.

We have mentioned that the variety of groups is congruence permutable. One can verify this by setting $p(x,y,z) = x - y + z$ in Theorem 0.54. Similarly, the congruence distributivity of the variety of lattices follows from Theorem 0.55 using the term $m(x,y,z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$. A detailed proof of an analogue of Theorem 0.54 will be given in Chapter 2 for congruence modular varieties.

Chapter 1

Residually Small Varieties: Categorical Properties

By Birkhoff's Subdirect Decomposition Theorem, the difficulty in analyzing a variety V can be expected to be proportional to its "residual size", by which, roughly speaking, we mean the sizes of the subdirectly irreducible algebras in V and the number of such algebras. The condition "V is residually small" (Definition 1.20) below will amount to the requirement that, up to isomorphism, these algebras form a set (rather than a proper class).

The main result of this thesis is a theorem due to R. Freese and R. McKenzie [FM81] which we present in Chapter 4. It establishes a sufficient condition for the existence of a finite bound on the size of subdirectly irreducible algebras in residually small finitely generated varieties and describes such a bound.

Our main aim in this first chapter is to become familiar with residually small varieties. We largely follow the approach of W. Taylor in [Tay72] and J. Baldwin and J. Berman in [BB75]. We first consider Taylor's characterization of subdirectly irreducible algebras in terms of the existence of first order formulas (called "weak congruence formulas") with specific properties. Such formulas are used in Baldwin and Berman's discussion of varieties with definable principal congruences. We show that a residually small variety with definable principal congruences has a finite residual bound and that a variety of finite type with definable principal congruences has subdirectly irreducible algebras of every infinite cardinality if it has infinitely many nonisomorphic finite subdirectly irreducible algebras. These two theorems may be regarded as responses to Quackenbush's Theorem [Qua71], which states that a locally finite variety with only finitely many finite subdirectly irreducible algebras has no infinite subdirectly irreducible algebra, and to the so-called "Quackenbush Problem" and the related "RS Conjecture" to be discussed later.

This chapter includes a theorem that gives nine equivalent conditions for residual smallness of a variety as well as a number of examples of residually small varieties.

Taylor's weak congruence formulas also provide a characterization of essential extensions of an algebra. In the first part of this chapter we consider this characterization as well as other results involving essential extensions. These results are used in the final section of this chapter which deals with transferable injections and injective hulls of algebras.

In what follows, we continue to deal with a fixed type (i.e. language) $\mathcal{T} = \langle \mathsf{F}, ar \rangle$, unless we specify otherwise. Recall that $Th(\mathcal{T})$ is the first order theory with equality whose set of operation symbols is F and whose models are just all $\mathcal{T}$-algebras and that, given any $\mathcal{T}$-algebra $\mathbf{A} = \langle A; F \rangle$ we may consider the extended type $\mathcal{T}[\mathbf{A}]$ and the extended theory $Th(\mathcal{T}[\mathbf{A}])$ in which new constant symbols are available corresponding to the elements of A. (See Sections 0.5 and 0.6 for details)

1.1 Essential Extensions. The first two theorems extend Mal'cev's Lemma by showing that principal congruences on $\mathbf{A}$ and (a, b)-irreducibility can be characterized by the existence of $\mathcal{T}$-formulas with specific properties.

Proposition 1.1. [Tay72, Proposition 0.3]

Let $\mathbf{A}$ be a $\mathcal{T}$-algebra, $a, b, c, d \in A$ and let $\theta = \Theta^{\mathbf{A}}(c, d)$. The following are equivalent:

(1) $(a, b) \in \theta = \Theta^{\mathbf{A}}(c, d)$.

(2) *There exists a $\mathcal{T}$-formula Φ with four free variables, say $\Phi(x_0, x_1, x_2, x_3)$, such that the following are true:*

- *(i)* *Φ is positive.*
- *(ii)* $\vdash_{Th(\mathcal{T})} \forall y \forall z[(\exists x\, \Phi(x, x, y, z)) \to y \approx z]$.
- *(iii)* $\mathbf{A} \models \Phi[c, d, a, b]$.

Proof.

(1)⇒(2): Let $(a, b) \in \Theta^{\mathbf{A}}(c, d)$. Then by Mal'cev's Lemma (Lemma 0.37), there are $\mathcal{T}$-terms $t_i(x_0, x_1, y_2, \dots, y_m)$, $0 \le i \le n$ and elements $a, b, e_2, \dots, e_m$ of A such that

$$\begin{aligned} a &= t_0^{\mathbf{A}}(c, d, e_2, \dots, e_m) \\ t_i^{\mathbf{A}}(d, c, e_2, \dots, e_m) &= t_{i+1}^{\mathbf{A}}(c, d, e_2, \dots, e_m) \ (0 \le i < n) \\ t_n^{\mathbf{A}}(d, c, e_2, \dots, e_m) &= b. \end{aligned}$$

Define $\Phi(x_0, x_1, x_2, x_3)$ as

$$\exists z_0 \exists z_n \exists y_2 \dots \exists y_m [z_0 \approx x_2 \wedge z_n \approx x_3 \wedge (z_0 \approx t_0(x_0, x_1, y_2, \dots, y_m) \wedge$$
$$t_0(x_1, x_0, y_2, \dots, y_m) \approx t_1(x_0, x_1, y_2, \dots, y_m) \wedge$$
$$t_1(x_1, x_0, y_2, \dots, y_m) \approx t_2(x_0, x_1, y_2, \dots, y_m) \wedge \dots$$

$$\ldots$$

$$\ldots \wedge t_n(x_1, x_0, y_2, \ldots, y_m) \approx z_n)].$$

Note that Φ is positive (and existential) and $\mathbf{A} \models \Phi[c, d, a, b]$.

Let Ψ be $\forall y \forall z[(\exists x\ \Phi(x, x, y, z)) \to y \approx z]$. Note that Ψ is logically equivalent to $\forall y \forall z \forall x[\Phi(x, x, y, z) \to y \approx z]$. Choose an arbitrary $\mathcal{T}$-algebra $\mathbf{B}$. We show Ψ is true in $\mathbf{B}$. This will show that $\vdash_{Th(\mathcal{T})} \Psi$.

Let $a', b', c' \in B$ and suppose $\Phi[c', c', a', b']$ is true in $\mathbf{B}$. Then there exist $e_2, \ldots, e_m \in B$ such that

$$a' = t_0^{\mathbf{B}}(c', c', e_2, \ldots, e_m) = \ldots = t_n^{\mathbf{B}}(c', c', e_2, \ldots, e_m) = b',$$

so $\mathbf{B} \models \Psi$.

(2)$\Rightarrow$(1): Suppose there is a first order formula Φ that satisfies (i) - (iii). Observe that in $\mathbf{A}/\theta$ we have $c/\theta = d/\theta$. By (ii), since $\mathbf{A}/\theta$ is a $\mathcal{T}$-algebra, $\forall y \forall z[(\exists x\ \Phi(x, x, y, z)) \to y \approx z]$ is true in $\mathbf{A}/\theta$. Thus,

$(\exists x\ \Phi(x, x, a/\theta, b/\theta)) \to a/\theta \approx b/\theta$ is true in $\mathbf{A}/\theta$. .... (*)

Now by (iii), $\Phi[c, d, a, b]$ is true in $\mathbf{A}$ and the onto map $\lambda : \mathbf{A} \to \mathbf{A}/\theta$ defined by $u \mapsto u/\theta$ is a homomorphism so by Theorem 0.41, since Φ is positive, $\mathbf{A}/\theta \models \Phi[c/\theta, d/\theta, a/\theta, b/\theta]$. Since c/θ is d/θ, $\exists x\ \Phi(x, x, a/\theta, b/\theta)$ is true in $\mathbf{A}/\theta$. By (*), $a/\theta \approx b/\theta$ is true in $\mathbf{A}/\theta$, i.e., $(a, b) \in \theta$. □

Note that in (2)(i) above we could require Φ to be existential, without affecting the proof. This motivates the following definitions.

Definition 1.2. A *congruence formula* is a $\mathcal{T}$-formula $\Psi(x_0, x_1, x_2, x_3)$ of the form

$$\exists z_0 \ldots \exists z_n([z_0 \approx x_2 \wedge z_n \approx x_3] \wedge \textstyle\bigwedge_{i=0}^{n-1} \exists x_2 \ldots \exists x_m(z_i \approx t_i \wedge z_{i+1} \approx t_i(\sigma)))$$

where each t_i is a $\mathcal{T}$-term $t_i(x_0, x_1, x_2, \ldots, x_m)$ and $t_i(\sigma)$ abbreviates $t_i(x_1, x_0, x_2, \ldots, x_m)$.

Note that any congruence formula Ψ is logically equivalent to an existential $\mathcal{T}$-formula and satisfies the first two conditions of Proposition 1.1, namely

(i) Ψ is positive and

(ii) $\vdash_{Th(\mathcal{T})} \forall y \forall z[(\exists x\ \Psi(x, x, y, z)) \to y \approx z]$.

Definition 1.3. A positive existential formula Ψ with four free variables is a *weak congruence formula* if it satisfies condition (ii) above.

Thus, any conjunction or disjunction of congruence formulas is logically equivalent to a weak congruence formula.

In summary: Given a $\mathcal{T}$-algebra $\mathbf{A}$ and $a, b, c, d \in A$, Mal'cev's Lemma says that $(a, b) \in \Theta^{\mathbf{A}}(c, d)$ if and only if $\mathbf{A} \models \Phi[c, d, a, b]$ for some congruence ($\mathcal{T}$-)formula Φ, while Proposition 1.1 says that "congruence formula" can be replaced by "weak congruence formula" in this statement.

Corollary 1.4. [Tay72, Corollary 0.4]

A $\mathcal{T}$-algebra $\mathbf{A}$ with distinct elements a, b is (a, b)-irreducible if and only if for all $c, d \in A$ with $c \neq d$, there exists a weak congruence $\mathcal{T}$-formula Φ such that $\mathbf{A} \models \Phi[c, d, a, b]$.

Proof.

This follows directly from Theorem 0.19 (ii) and Proposition 1.1. □

Lemma 1.5. [Tay72]

The following are equivalent for $\mathcal{T}$-algebras $\mathbf{B}$ and $\mathbf{A}$ with $\mathbf{A} \leq \mathbf{B}$:

(i) For any $\mathcal{T}$-algebra $\mathbf{C}$, every homomorphism $h : \mathbf{B} \to \mathbf{C}$ whose restriction $h|_{\mathbf{A}}$ to $\mathbf{A}$ is a monomorphism, is itself a monomorphism.

(ii) For any $\theta \in Con(\mathbf{B})$ with $\theta \neq id_B$, we have $\theta|_{\mathbf{A}} \neq id_A$.

Proof.

(i)$\Rightarrow$(ii): Assume (i). Let $\psi \in Con(\mathbf{B})$ such that $\psi|_{\mathbf{A}} = id_A$. The natural map $\lambda : \mathbf{B} \to \mathbf{B}/\psi$ is a homomorphism with $ker(\lambda) = \psi$. Therefore $ker(\lambda)|_{\mathbf{A}} = \psi|_{\mathbf{A}} = id_A$, so $\lambda|_{\mathbf{A}}$ is one-to-one and by the assumption, λ is one-to-one. Thus, $ker(\lambda) = id_B$, i.e., ψ is id_B.

(ii)$\Rightarrow$(i): Assume (ii). Let f be any homomorphism from $\mathbf{B}$ to a $\mathcal{T}$-algebra $\mathbf{C}$ such that $f|_{\mathbf{A}}$ is one-to-one. Then $ker(f)|_{\mathbf{A}}$ is id_A, so by the assumption, $ker(f)$ is id_B, i.e., f is itself one-to-one.

□

Definition 1.6. Suppose $\mathbf{A}$ is a subalgebra of an algebra $\mathbf{B}$. We call $\mathbf{B}$ an *essential extension* of $\mathbf{A}$ if the conditions of the above lemma hold.

Evidently, if $\mathbf{C}$ is an essential extension of $\mathbf{B}$ and $\mathbf{B}$ is an essential extension of $\mathbf{A}$, then $\mathbf{C}$ is an essential extension of $\mathbf{A}$.

In this section the weak congruence formulas described in Proposition 1.1 are used to establish the existence of essential extensions of an algebra $\mathbf{A}$ and some of their properties, that are to be applied later in the chapter.

Lemma 1.7. [Tay72]

If $\mathbf{B}$ *is an* (a,b)*-irreducible algebra then* $\mathbf{B}$ *is an essential extension of* $\mathbf{A} = \mathbf{Sg}^{\mathbf{B}}(\{a,b\}) \leq \mathbf{B}$ *(hence* $\mathbf{B}$ *is an essential extension of* $\mathbf{C}$ *whenever* $a, b \in C$ *and* $\mathbf{C} \leq \mathbf{B}$*).*

Proof.

Let $\mathbf{B}$ be (a,b)-irreducible (where $a, b \in B, a \neq b$). Take any $\theta \in Con(\mathbf{B})$ with $\theta \neq id_B$. Then there exist $c, d \in B$ such that $(c,d) \in \theta$ and $c \neq d$, so $\Theta^{\mathbf{B}}(c,d) \neq id_B$. Therefore $(a,b) \in \Theta^{\mathbf{B}}(c,d)$, by (a,b)-irreducibility of $\mathbf{B}$.

Now if $\mathbf{A} = \mathbf{Sg}^{\mathbf{B}}(\{a,b\})$ then $(a,b) \in \theta|_{\mathbf{A}}$ so $\theta|_{\mathbf{A}} \neq id_A$. Therefore $\mathbf{B}$ is an essential extension of $\mathbf{A}$. □

Lemma 1.8. [Tay72]

If $\mathbf{A} \leq \mathbf{B}$, $\mathbf{A}$ *is* (a,b)*-irreducible and* $\mathbf{B}$ *is an essential extension of* $\mathbf{A}$*, then* $\mathbf{B}$ *is* (a,b)*-irreducible.*

Proof.

Let $id_B \neq \theta \in Con(\mathbf{B})$. Since $\mathbf{B}$ is an essential extension of $\mathbf{A}$, $id_A \neq \theta|_{\mathbf{A}} \in Con(\mathbf{A})$. Since $\mathbf{A}$ is (a,b)-irreducible, $(a,b) \in \theta|_{\mathbf{A}} \subseteq \theta$. Thus, $\mathbf{B}$ is (a,b)-irreducible. □

Corollary 1.9. [Tay72, Corollary 0.5]

An algebra $\mathbf{B}$ *is an essential extension of an algebra* $\mathbf{A}$ *if and only if* $\mathbf{A} \leq \mathbf{B}$ *and for each* $c, d \in B$ *with* $c \neq d$ *there exist* $a, b \in A$ *with* $a \neq b$ *and a weak congruence* $\mathcal{T}$*-formula* Φ *such that* $\mathbf{B} \models \Phi[c,d,a,b]$.

Proof.

$(\Rightarrow)$ Suppose $\mathbf{B}$ is an essential extension of $\mathbf{A}$. Then for any $(c,d) \in B \times B$ with $c \neq d$, $id_B \neq \Theta^{\mathbf{B}}(c,d) \in Con(\mathbf{B})$. Since $\mathbf{B}$ is an essential extension of $\mathbf{A}$, there exist $(a,b) \in \Theta^{\mathbf{B}}(c,d)|_{\mathbf{A}}$ such that $a \neq b$. Since $(a,b) \in \Theta^{\mathbf{B}}(c,d)$ there is a weak congruence formula Φ such that $\mathbf{B} \models \Phi[c,d,a,b]$.

$(\Leftarrow)$ Suppose $\mathbf{A} \leq \mathbf{B}$ and for each $c, d \in B$ with $c \neq d$ there exist $a, b \in A$ with $a \neq b$ and a weak congruence formula Φ such that $\mathbf{B} \models \Phi[c,d,a,b]$.

Take any $\theta \in Con(\mathbf{B})$ with $\theta \neq id_B$. Then there exist $c, d \in B$ such that $(c,d) \in \theta$ and $c \neq d$. By the assumption, there exist $a, b \in A$ with $a \neq b$ and a formula Φ as in Proposition 1.1. Then $(a,b) \in \Theta^{\mathbf{B}}(c,d)$ by Proposition 1.1. Now $\Theta^{\mathbf{B}}(c,d) \subseteq \theta$, so $(a,b) \in \theta$ but $(a,b) \in A \times A$ and $a \neq b$, therefore $\theta|_{\mathbf{A}} \neq id_A$. Thus $\mathbf{B}$ is an essential extension of $\mathbf{A}$.

□

The following result, called the *Erdös-Rado Theorem* [ER56], will be needed in subsequent theorems. It is stated without proof since the techniques required to prove it are combinatorial and beyond the scope of this thesis. For any set A, let $A^{(2)}$ denote the set of pairs $\{a, b\} \subseteq A$ such that $a \neq b$.

Theorem 1.10. (Erdös-Rado Theorem) [ER56]

For an infinite cardinal m, *if* A *is a set such that* $|A| > 2^{\mathsf{m}}$ *and* $A^{(2)} = \cup\mathcal{D}$ *where* $\mathcal{D}$ *is a set of sets such that* $|\mathcal{D}| \leq \mathsf{m}$, *then there exist* $D \in \mathcal{D}$ *and* $B \subseteq A$ *with* $|B| > \mathsf{m}$ *such that* $B^{(2)} \subseteq D$.

Recall that $\mathcal{T} = \langle \mathsf{F}, ar\rangle$. For $\mathcal{T}$-algebras $\mathbf{A}$ and $\mathbf{B}$, let $Id(\mathbf{B})$ be the set of $\mathcal{T}$-identities holding in $\mathbf{B}$ and recall that $D(\mathbf{A})$ is the set of atomic $\mathcal{T}[\mathbf{A}]$-sentences and negations of atomic $\mathcal{T}[\mathbf{A}]$-sentences which hold in $\mathbf{A}$.

Corollary 1.11. [Tay72, Corollary 0.7]

Let $\mathbf{B}$ *be an essential extension of* $\mathbf{A}$, *with* $|B| > 2^{\mathsf{m}}$, *where* $\mathsf{m} = \aleph_0 + |A| + |\mathsf{F}|$. *Then there exist* $a, b \in A, a \neq b$, *and a weak congruence* $\mathcal{T}$*-formula* Φ *such that*

$$D(\mathbf{A}) \cup Id(\mathbf{B}) \cup \{\Phi(x_i, x_j, a, b) : i < j < \omega\}$$

is satisfiable.

Proof.

Let Λ be the set of all $\lambda = (\Phi, a, b)$ where Φ is a weak congruence formula, $a, b \in A$ and $a \neq b$. Let $\preceq$ be a linear order of B (then for every $a, b \in B, a \prec b$ or $a \succ b$ or $a = b$).

For each $\lambda = (\Phi, a, b) \in \Lambda$ we define

$$C_\lambda = \{\{c, d\} \in B^{(2)} : c \prec d \text{ and } \mathbf{B} \models \Phi[c, d, a, b]\}.$$

We show $B^{(2)} = \cup\{C_\lambda : \lambda \in \Lambda\}$.

For every $\{e, f\} \in B^{(2)}$, $e \neq f$ and since $\mathbf{B}$ is an essential extension of $\mathbf{A}$, by Corollary 1.9, there exist $a, b \in A$ with $a \neq b$ and a weak congruence formula Φ with $\mathbf{B} \models \Phi[e, f, a, b]$. Since $e \neq f$ we have $e \prec f$, say. (If $f \prec e$, define $\Psi(x, y, z, w)$ to be $\Phi(y, x, z, w)$ and use Ψ instead of Φ). Thus, $\{e, f\} \in C_\lambda$, where $\lambda = (\Phi, a, b)$, therefore $\{e, f\} \in \cup\{C_\lambda : \lambda \in \Lambda\}$, therefore $B^{(2)} \subseteq \cup\{C_\lambda : \lambda \in \Lambda\}$. Clearly, equality follows.

Since $|\Lambda| = \mathsf{m}, |\{C_\lambda : \lambda \in \Lambda\}| \leq \mathsf{m}$ so since $|B| > 2^{\mathsf{m}}$ and $B^{(2)} = \cup\{C_\lambda : \lambda \in \Lambda\}$, by Theorem 1.10, there exists $\lambda \in \Lambda$ and $C \subseteq B$ with $|C| > \mathsf{m}$ such that $C^{(2)} \subseteq C_\lambda$ for this $\lambda = (\Phi, a, b) \in \Lambda$. Since $|C| > \mathsf{m}, C$ is infinite.

We show $D(\mathbf{A}) \cup Id(\mathbf{B}) \cup \{\Phi(x_i, x_j, a, b) : i < j < \omega\}$ is satisfiable. Since C is infinite, C has a denumerable subset, say $\{c_0, c_1, c_2, \ldots\}$ with $c_0 \prec c_1 \prec c_2 \prec \ldots$. Let X be the set of variables $\{x_\alpha : \alpha < \omega\}$. We must show there is a function $f : X \to B$ such that for each $\Psi \in D(\mathbf{A}) \cup Id(\mathbf{B}) \cup \{\Phi(x_i, x_j, a, b) : i < j < \omega\}$ with free variables $x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n}$, we have $\mathbf{B} \models \Psi[f(x_{\alpha_1}), f(x_{\alpha_2}), \dots, f(x_{\alpha_n})]$.

Define $f : X \to B$ by $f(x_i) = c_i$ $(i \in \omega)$. Since $A \cup C \subseteq B$, $a, b, c_0, c_1, \dots \in B$.

(i) Sentences from $D(\mathbf{A})$ have no free or bound variables and hold in $\mathbf{A}$ (hence in $\mathbf{B}$) regardless of the above substitutions.

(ii) Sentences in $Id(\mathbf{B})$ have no free variables and hold in $\mathbf{B}$, by definition of $Id(\mathbf{B})$.

(iii) For any $i < j < \omega$, for our fixed a, b and for $\lambda = (\Phi, a, b)$ we have $\{c_i, c_j\} \in C^{(2)} \subseteq C_\lambda$ so $\mathbf{B} \models \Phi[c_i, c_j, a, b]$, i.e., $\mathbf{B} \models \Psi[f(x_i), f(x_j), a, b]$.

□

Definition 1.12. An algebra $\mathbf{A}$ is an *absolute retract in* a variety V if $\mathbf{A} \in V$ and whenever $\mathbf{A} \leq \mathbf{T} \in V$, there exists a homomorphism f retracting $\mathbf{T}$ onto $\mathbf{A}$, i.e., $f : \mathbf{T} \to \mathbf{A}$ and the restriction of f to $\mathbf{A}$ is the identity map on $\mathbf{A}$.

Lemma 1.13. [Tay72, Lemma 0.8]

Let V be a variety, $\mathbf{A}$, $\mathbf{B} \in V$ and let $\mathbf{B}$ be an essential extension of $\mathbf{A}$. Then $\mathbf{B}$ is an absolute retract in V if and only if no proper extension of $\mathbf{B}$ in V is an essential extension of $\mathbf{A}$.

Proof.

($\Rightarrow$) Let $\mathbf{B}$ be an absolute retract in V. Let $\mathbf{T}$ be any proper extension of $\mathbf{B}$ in V, i.e., $\mathbf{B} < \mathbf{T}$. We show $\mathbf{T}$ is not an essential extension of $\mathbf{A}$, i.e., we show for some $\theta_{\mathbf{T}} \in Con(\mathbf{T})$ with $\theta_{\mathbf{T}} \neq id_T$ we have $(\theta_{\mathbf{T}})|_{\mathbf{A}} = id_A$.

Since $\mathbf{B}$ is an absolute retract in V, there exists an onto homomorphism $f : \mathbf{T} \to \mathbf{B}$ such that $f|_{\mathbf{B}}$ is the identity map on $\mathbf{B}$. Define $\theta_f = ker(f)$, so $\theta_f \in Con(\mathbf{T})$. We show $\theta_f \neq id_T$. Now $\mathbf{B} < \mathbf{T}$ so for any $c \in T \setminus B$, let $b = f(c) \in B$, so $c \neq b$. Then $f(c) = f(b) = b$ so $(c, b) \in \theta_f$ but $c \neq b$, so $\theta_f \neq id_T$.

Now $\theta_f|_{\mathbf{B}} = id_B$ so $\theta_f|_{\mathbf{A}} = (\theta_f|_{\mathbf{B}})|_{\mathbf{A}} = id_A$.

($\Leftarrow$) Assume no proper extension of $\mathbf{B}$ in V is an essential extension of $\mathbf{A}$. Pick $\mathbf{T} \in V$ such that $\mathbf{B} \leq \mathbf{T}$. If $\mathbf{T} = \mathbf{B}$ then the identity map from $\mathbf{T}(= \mathbf{B})$ to $\mathbf{B}$ fulfils the required conditions. Suppose $\mathbf{T}$ is a proper extension of $\mathbf{B}$. Then $\mathbf{T}$ is not an essential extension of $\mathbf{A}$ (by the assumption) so there exists $\theta_{\mathbf{T}} \in Con(\mathbf{T})$, $\theta_{\mathbf{T}} \neq id_T$, such that $(\theta_{\mathbf{T}})|_{\mathbf{A}} = id_A$.

Let $S = \{\theta \in Con(\mathbf{T}) : \theta \neq id_T$ and $\theta|_{\mathbf{A}} = id_A\}$. S is nonempty since $\theta_{\mathbf{T}} \in S$ and $\subseteq$ partially orders S. Let $\langle C; \subseteq \rangle$ be a chain in S, i.e., $C \subseteq S$ and

$\subseteq$ linearly orders C. We claim that C has an upper bound in S. (We can assume $C \neq \emptyset$, since any element of S is an upper bound of $\emptyset$ in S).

(i) $\cup C \in Con(\mathbf{T})$ since $\mathbf{Con}(\mathbf{T})$ is an algebraic lattice and C is a chain (see Theorem 0.10).

(ii) For each $\theta \in C$, $\theta \neq id_T$. Moreover, $C \neq \emptyset$ so we can choose such a θ. Since $\theta \subseteq \cup C$, we have $\cup C \neq id_T$.

(iii) For each $(a,b) \in \cup C|_{\mathbf{A}}, (a,b) \in \theta$ for some $\theta \in C$ and $(a,b) \in A \times A$ so $(a,b) \in \theta|_{\mathbf{A}} = id_A$, and so $\cup C|_{\mathbf{A}} = id_A$.

From (i), (ii) and (iii), $\cup C \in S$, so $\cup C$ is an upper bound of C in S. By Zorn's Lemma, S has a maximal element, say θ_m, i.e., θ_m is maximal such that $\theta_m \in Con(\mathbf{T})$, $\theta_m \neq id_T$ and $\theta_m|_{\mathbf{A}} = id_A$. Note that $\mathbf{T}/\theta_m \in V$, since V is a variety.

By the Correspondence Theorem (Theorem 0.17), any congruence relation φ on $\mathbf{T}/\theta_m$ is of the form η/θ_m where $\theta_m \subseteq \eta \in Con(\mathbf{T})$. For any $\eta \in Con(\mathbf{T})$ such that $\theta_m \subset \eta$, $\eta/\theta_m \neq id_{T/\theta_m}$ and $\eta|_{\mathbf{A}} \neq id_A$ (by the maximality of θ_m).

Define $g : \mathbf{B} \to \mathbf{T}/\theta_m$ by $g(b) = b/\theta_m$ for all $b \in B$. Then g is a homomorphism. Also, since $\theta_m|_{\mathbf{A}} = id_A$ and $\mathbf{B}$ is an essential extension of $\mathbf{A}$, $\theta_m|_{\mathbf{B}} = id_B$, so g is one-to-one. Therefore $\mathbf{B} \cong g[\mathbf{B}] \leq \mathbf{T}/\theta_m$ (and $\mathbf{A} \cong g[\mathbf{A}] \leq \mathbf{T}/\theta_m$).

We show $\mathbf{T}/\theta_m$ is an essential extension of $g[\mathbf{A}](\cong \mathbf{A})$. Let $\varphi \in Con(\mathbf{T}/\theta_m)$, $\varphi \neq id_{T/\theta_m}$. Then $\varphi = \eta/\theta_m$ where $\eta \in Con(\mathbf{T})$, $\theta_m \subset \eta$ and

$$\begin{aligned}\varphi|_{g[\mathbf{A}]} &= \{(a/\theta_m, b/\theta_m) : (a,b) \in \eta \text{ and } a/\theta_m, b/\theta_m \in g[A]\}\\ &= \{(a/\theta_m, b/\theta_m) : (a,b) \in \eta|_{\mathbf{A}}\}.\end{aligned}$$

Further, since $\eta|_{\mathbf{A}} \neq id_A$, there exists $(x,y) \in \eta|_{\mathbf{A}}$ such that $x \neq y$ and $x/\theta_m \neq y/\theta_m$, since $\theta_m|_{\mathbf{A}} = id_A$. Now $(x/\theta_m, y/\theta_m) \in \varphi|_{g[\mathbf{A}]}$, so $\varphi|_{g[\mathbf{A}]} \neq id_{g[A]}$.

Thus $\mathbf{T}/\theta_m$ is an essential extension of $g[\mathbf{A}]$ and $g[\mathbf{B}] \leq \mathbf{T}/\theta_m$ but no proper extension of $g[\mathbf{B}]$ in V is an essential extension of $g[\mathbf{A}]$ (because $g[\mathbf{B}] \cong \mathbf{B}$) so $g[\mathbf{B}] = \mathbf{T}/\theta_m$, i.e., g is onto, so g is an isomorphism.

Let λ be the natural homomorphism $\lambda : \mathbf{T} \to \mathbf{T}/\theta_m$ defined by $\lambda(t) = t/\theta_m$, $t \in T$. Then $g^{-1} \circ \lambda$ is a homomorphism from $\mathbf{T}$ to $\mathbf{B}$ and for every $b \in B, (g^{-1} \circ \lambda)(b) = g^{-1}(b/\theta_m) = b$, so $(g^{-1} \circ \lambda)|_{\mathbf{B}} = id_B$.

□

Corollary 1.14. [Tay72, Corollary 0.9]

Let V be a variety such that each $\mathbf{A} \in V$ has, up to isomorphism, only a set of essential extensions that are in V. Then for each $\mathbf{A} \in V$, some essential extension of $\mathbf{A}$ is an absolute retract in V.

Proof.

For each $\mathbf{D} \in V$, let $S_{\mathbf{D}}$ be a subset of V consisting of essential extensions of $\mathbf{D}$, such that every essential extension $\mathbf{E}$ of $\mathbf{D}$ in V is isomorphic to just one algebra in $S_{\mathbf{D}}$; call this algebra $S_{\mathbf{D}}(\mathbf{E})$. Let $\mathbf{A} \in V$.

Claim 1: If C is a nonempty chain (ordered by subalgebrahood) of essential extensions of $\mathbf{A}$ in V and $\mathbf{U}$ is the union of C, as defined in Section 0.3 then $\mathbf{U}$ is an essential extension of $\mathbf{A}$ in V.

Since V is a variety it is axiomatizable by identities. Now identities are $\forall\exists$ sentences, so $\mathbf{U} \in V$, by Theorem 0.41, and $\mathbf{A}$ is a subalgebra of $\mathbf{U}$. Let $id_U \neq \theta \in Con(\mathbf{U})$ and choose $(x, y) \in \theta$ with $x \neq y$. Since $x, y \in U$ there exist $\mathbf{B}_1, \mathbf{B}_2 \in C$ such that $x \in B_1, y \in B_2$ and, without loss of generality, $B_1 \subseteq B_2$ (since C is a chain), so $x, y \in B_2$, and $(x, y) \in \theta|_{\mathbf{B}_2}$. Thus, $id_{B_2} \neq \theta|_{\mathbf{B}_2} \in Con(\mathbf{B}_2)$ so $id_A \neq (\theta|_{\mathbf{B}_2})|_{\mathbf{A}} = \theta|_{\mathbf{A}}$, since $\mathbf{B}_2$ is an essential extension of $\mathbf{A}$. This shows that $\mathbf{U}$ is an essential extension of $\mathbf{A}$, and Claim 1 is proved.

For each $\mathbf{D} \in V$, since $S_{\mathbf{D}}$ is a set, there exists a cardinal $\mathsf{m}(\mathbf{D})$ such that for every essential extension $\mathbf{E}$ of $\mathbf{D}$ in V, $|E| \leq \mathsf{m}(\mathbf{D})$. .... (*)

Define, by transfinite recursion, a sequence $\langle \mathbf{A}_\alpha : \alpha \in On \rangle$ (where On is the class of all ordinals) as follows:

$\mathbf{A}_0 = \mathbf{A}$;

for $\alpha \in On$, let $\mathbf{A}_{\alpha+1} = S_{\mathbf{A}_\alpha}(\mathbf{D})$, where $\mathbf{D}$ is a proper essential extension of $\mathbf{A}_\alpha$ in V, if such a $\mathbf{D}$ exists; otherwise, set $\mathbf{A}_{\alpha+1} = \mathbf{A}_\alpha$;

for a limit ordinal α, let $\mathbf{A}_\alpha$ be the union of the chain of algebras $\langle A_\gamma : \gamma < \alpha \rangle$.

Note that $\mathbf{A}_\alpha$ is a subalgebra of $\mathbf{A}_\beta$ and an essential extension of $\mathbf{A}$ in V, whenever $\alpha < \beta \in On$, by Claim 1.

Claim 2: For some $\beta \in On$, we have $\mathbf{A}_\beta = \mathbf{A}_\gamma$ whenever $\beta < \gamma \in On$.

Suppose not. Then the function $F : \alpha \mapsto \mathbf{A}_\alpha$ ($\alpha \in On$) is one-to-one and $\mathbf{A}_\gamma$ is a proper subalgebra of $\mathbf{A}_\alpha$ whenever $\gamma < \alpha \in On$.

Let $\mathsf{m} = \mathsf{m}(\mathbf{A})$ and let T be the set of all successor ordinals less than m^+, so $|T| = \mathsf{m}^+$. Using the Axiom of Choice, we can pick, for each $\alpha < \mathsf{m}^+$, an element $g(\alpha + 1) \in A_{\alpha+1} \setminus A_\alpha$. Then the function $g : T \to A_{\mathsf{m}^+}$ is one-to-one, so $|A_{\mathsf{m}^+}| \geq |T| = \mathsf{m}^+ > \mathsf{m}$, contradicting (*), so the claim is true.

Let β be the least ordinal as in Claim (2). Then by our construction, $\mathbf{A}_\beta$ has no proper essential extension in V and is therefore an absolute retract in V (by Lemma 1.13).[10]

[10] In [Tay72] this result is proved by applying Zorn's Lemma to the class of essential extensions of $\mathbf{A}$ in V. This class is a proper class; its isomorpism classes form a set, but

□

1.2 Definable Principal Congruences. We now specialize the characterization of principal congruences by (weak) congruence formulas (Proposition 1.1) to the notion of varieties with definable principal congruences. Conditions under which varieties have definable principal congruences as well as some properties of such varieties are explored. We continue to consider varieties V of $\mathcal{T}$-algebras, $\mathcal{T} = \langle \mathsf{F}, ar \rangle$. For any algebra $\mathbf{A} \in V$, and $a, b \in A$, let

$$\Phi[a, b, x_2, x_3](\mathbf{A}) \text{ denote } \{(a_2, a_3) \in A^2 : \mathbf{A} \models \Phi[a, b, a_2, a_3]\}.$$

Definition 1.15. A variety V has *definable principal congruences* if there is a (first order) $\mathcal{T}$-formula $\Phi(x_0, x_1, x_2, x_3)$ such that for each $\mathbf{A} \in V$, and each $a, b \in A$, $\Phi[a, b, x_2, x_3](\mathbf{A}) = \Theta^{\mathbf{A}}(a, b)$. In this case we say that Φ *defines* the principal congruences of V.

Theorem 1.16. [BB75, Theorem 1]

(i) *A variety V of type $\mathcal{T}$ has definable principal congruences if there are only finitely many congruence formulas which are pairwise inequivalent and satisfiable in V.*

(ii) *If V has definable principal congruences the defining formula Ψ is equivalent in V to a weak congruence formula and persists under extensions.*

Proof.

(i) Let Σ' be a set of $\mathcal{T}$-equations that axiomatizes V. Let Σ be the set of sentences that are the (universal) closures of the equations in Σ'. Suppose that up to logical equivalence modulo Σ, $\Phi_1, \ldots, \Phi_n$ are the only congruence formulas satisfiable in V.

Take any $\mathbf{A} \in V$ and any $a, b, c, d \in A$. Now $(c, d) \in \Theta^{\mathbf{A}}(a, b)$ if and only if there is a congruence formula Ψ such that $\mathbf{A} \models \Psi[a, b, c, d]$ (by Mal'cev's Lemma (Lemma 0.37)); if and only if $\mathbf{A} \models \bigvee_{i=1}^{n} \Phi_i[a, b, c, d]$ (because $\Phi_1, \ldots, \Phi_n$ are the only congruence formulas satisfiable in V); if and only if $(c, d) \in (\bigvee_{i=1}^{n} \Phi_i[a, b, x_2, x_3])(\mathbf{A})$.

Since $c, d \in A$ were arbitrary, $\Theta^{\mathbf{A}}(a, b) = (\bigvee_{i=1}^{n} \Phi_i[a, b, x_2, x_3])(\mathbf{A})$ so V has definable principal congruences.

that set is not generally partially ordered by the embeddability relation (since anti-symmetry may fail). Even if it is so ordered, Zorn's Lemma yields an essential extension of $\mathbf{A}$ that may have proper essential extensions (isomorphic to it), which makes Lemma 1.13 difficult to apply. For these reasons, the above (different) proof has been given.

(ii) If Ψ defines principal congruences in V but Ψ is not a congruence formula, let $\langle \Phi_i : i \in \beta \rangle$ be a well-ordering of the inequivalent congruence formulas in V that are satisfiable in V (where β is an ordinal).

First, if there are only finitely many such formulas, say n of them, then by (i), $\Phi = \bigvee_{i=1}^{n} \Phi_i$ is a defining formula and is a weak congruence formula since it is a disjunction of congruence formulas.

For any $\mathbf{A} \in V$ and $a, b \in A$, by definition of Ψ and by (i), $\Psi[a, b, x_2, x_3](\mathbf{A}) = \Theta^{\mathbf{A}}(a, b) = (\bigvee_{i=1}^{n} \Phi_i[a, b, x_2, x_3])(\mathbf{A})$, so for all $c, d \in A$, $\mathbf{A} \models \Psi[a, b, c, d]$ if and only if $\mathbf{A} \models \bigvee_{i=1}^{n} \Phi_i[a, b, c, d]$. Since a, b, c, d were arbitrary, $\mathbf{A} \models \Psi(x_0, x_1, x_2, x_3) \leftrightarrow (\bigvee_{i=1}^{n} \Phi_i(x_0, x_1, x_2, x_3))$.

Thus, $V \models \Psi(x_0, x_1, x_2, x_3) \leftrightarrow (\bigvee_{i=1}^{n} \Phi_i(x_0, x_1, x_2, x_3))$ (because $\mathbf{A}$ was arbitrary in V), i.e., $\Sigma \vdash_{Th(\mathcal{T})} \Psi \leftrightarrow (\bigvee_{i=1}^{n} \Phi_i)$.

Secondly, suppose there are infinitely many Φ_i. Add distinct new constant symbols a, b, c_1, c_2 to $\mathcal{T}$; let $\mathcal{T}'$ be the resulting type. Let

$$\Gamma = \Sigma \cup \{\Psi[c_1, c_2, a, b]\} \cup \{\neg \Phi_i[c_1, c_2, a, b] : i \in \beta\}.$$

Note that Γ is a set of $\mathcal{T}'$*-sentences.*

Suppose that every finite subset of Γ has a model. Then by the Compactness Theorem (see the remarks following Theorem 0.43), Γ has a model. Let $\mathbf{A}'$ be a model of Γ and $\mathbf{A}$ the $\mathcal{T}$-reduct of $\mathbf{A}'$, so $\mathbf{A} \in V$ (since Σ axiomatizes V). We write a, b, c_1, c_2 for the elements of A that interpret the symbols a, b, c_1, c_2 in $\mathbf{A}'$, respectively.

Since $\mathbf{A} \models \Psi[c_1, c_2, a, b]$, we have $(a, b) \in \Theta^{\mathbf{A}}(c_1, c_2)$, while for all $i < \beta$, $\mathbf{A} \models \neg \Phi_i[c_1, c_2, a, b]$, contradicting Mal'cev's Lemma. Thus there is a finite subset Γ' of Γ such that Γ' has no model. We may assume without loss of generality that

$$\Gamma' = \Sigma'' \cup \{\Psi[c_1, c_2, a, b]\} \cup \{\neg \Phi_{i_j}[c_1, c_2, a, b] : j \in \{1, \ldots, n\}\}$$

for some finite $\Sigma'' \subseteq \Sigma$, some positive $n \in \omega$ and some $i_1, \ldots, i_n \in \beta$.

Thus, there is no $\mathbf{A} \in V$, and $a, b, c_1, c_2 \in A$ such that $\Psi[c_1, c_2, a, b]$ and all $\neg \Phi_i[c_1, c_2, a, b], i \in \{1, \ldots, n\}$ are true in $\mathbf{A}$. It follows that

$$V \models \Psi(x_0, x_1, x_2, x_3) \to \bigvee_{j=1}^{n} \Phi_{i_j}(x_0, x_1, x_2, x_3).$$

On the other hand, by Mal'cev's Lemma and the definition of Ψ,
$V \models (\bigvee_{j=1}^{n} \Phi_{i_j}(x_0, x_1, x_2, x_3)) \to \Psi(x_0, x_1, x_2, x_3)$.

Thus, $\Sigma \vdash_{Th(\mathcal{T})} (\bigvee_{j=1}^{n} \Phi_{i_j}(x_0, x_1, x_2, x_3)) \leftrightarrow \Psi(x_0, x_1, x_2, x_3)$.

Since $\bigvee_{n}^{j=1} \Phi_{i_j}(x_0, x_1, x_2, x_3)$ is logically equivalent to an existential formula, Ψ persists under extensions, by Theorem 0.41.

□

Theorem 1.17. [BB75, Theorem 2]

Let the variety V have definable principal congruences with defining formula $\Phi(x_0, x_1, x_2, x_3)$. Then Φ persists in subalgebras if and only if V has the congruence extension property.

Proof.

By Theorem 0.28, V has the congruence extension property if and only if V has the principal congruence extension property; if and only if for any $\mathbf{A} \leq \mathbf{B} \in V$ and $a_0, a_1 \in A$, we have $\Theta^{\mathbf{B}}(a_0, a_1)|_{\mathbf{A}} = \Theta^{\mathbf{A}}(a_0, a_1)$ (i.e., $\Phi[a_0, a_1, x_2, x_3](\mathbf{B}) \cap A^2 \subseteq \Phi[a_0, a_1, x_2, x_3](\mathbf{A})$); if and only if for any $\mathbf{A} \leq \mathbf{B} \in V$ and $a_0, a_1, a_2, a_3 \in A$, $\mathbf{A} \models \Phi[a_0, a_1, a_2, a_3]$ whenever $\mathbf{B} \models \Phi[a_0, a_1, a_2, a_3]$ (i.e., Φ persists under subalgebras in V). □

According to [BB75], the conditions of the above theorem hold exactly when there is a quantifier free formula $\Psi(x_0, x_1, x_2, x_3)$ such that $V \models \Psi \leftrightarrow \Phi$.

Theorem 1.18. [BB75, Theorem 3]

If a variety V is locally finite and has the congruence extension property, then V has definable principal congruence relations.

Proof.

For each $h \in \omega$, let $m(h) = |F|$, where $\mathbf{F}$ is the V-free algebra on h free generators. Note that $m(h) \in \omega$, because V is locally finite. Also, every h-generated algebra $\mathbf{C} \in V$ is a homomorphic image of $\mathbf{F}$ by Corollary 0.48, so $|C| \leq m(h)$.

Let $\mathbf{T} = \mathbf{T}(x, y, z, u, v, w)$ and $\mathbf{F} = \mathbf{F}_V(\bar{x}, \bar{y}, \bar{z}, \bar{u}, \bar{v}, \bar{w})$ be the term algebra and the V-free algebra on six free generators (respectively), so $|F| = m(6) \in \omega$. Since $\mathbf{F} = \mathbf{T}/\theta$ where, for $s, t \in T$, $s\theta t$ if and only if $V \models s \approx t$, if and only if $\bar{s} = s^{\mathbf{F}}(\bar{x}, \bar{y}, \bar{z}, \bar{u}, \bar{v}, \bar{w}) = t^{\mathbf{F}}(\bar{x}, \bar{y}, \bar{z}, \bar{u}, \bar{v}, \bar{w}) = \bar{t}$, there exists a finite sequence $t_1, \ldots, t_{m(6)}$ of distinct terms $t_i = t_i(x, y, z, u, v, w) \in T$ such that for every $t \in T$, there is an $i \in \{1, \ldots, m(6)\}$ with

$$V \models t(x, y, z, u, v, w) \approx t_i(x, y, z, u, v, w)$$

(hence $F = \{\bar{t}_1, \ldots, \bar{t}_{m(6)}\}$).

Let $\mathbf{B} = \mathbf{Sg}^{\mathbf{B}}(b_2, b_3, b_4, b_5)$ be a 4-generated algebra in V. For any binary polynomial $f : B^2 \to B$ of $\mathbf{B}$, there exists a term $p(x_0, \ldots, x_m)$ and $\mathbf{e} = e_2, \ldots, e_m \in B$ such that for all $b_0, b_1 \in B$, $f(b_0, b_1) = p^{\mathbf{B}}(b_0, b_1, \mathrm{e})$. But each e_i is $r_i^{\mathbf{B}}(b_2, b_3, b_4, b_5)$ for some term $r_i(z, u, v, w)$ in four variables, by Theorem 0.36 (iii).

Therefore, for all $b_0, b_1 \in B$,

$f(b_0,b_1) = p^{\mathbf{B}}(b_0,b_1,r_2^{\mathbf{B}}(b_2,\dots,b_5),\dots,r_m^{\mathbf{B}}(b_2,\dots,b_5)) = q^{\mathbf{B}}(b_0,b_1,b_2,b_3,b_4,b_5)$ where $q(x,y,z,u,v,w) := p(x,y,r_2(z,u,v,w),\dots,r_m(z,u,v,w)) \in T$. Thus, for some $j \in \{1,\dots,m(6)\}$, $V \models q \approx t_j$. Since $\mathbf{B} \in V$, we have $f(b_0,b_1) = t_j^{\mathbf{B}}(b_0,b_1,b_2,b_3,b_4,b_5)$, for all $b_0,b_1 \in B$.

Now for any $a,b,c,d \in B$, by Mal'cev's Lemma, and the above fact about binary polynomials, $(c,d) \in \Theta^{\mathbf{B}}(a,b)$ if and only if there exists $n \leq |B| \leq m(4) \in \omega$ and there exist distinct $g_0,\dots,g_n \in B$ and a finite $n-$sequence $\sigma = s_0,\dots,s_{n-1}$ of terms from $\{t_1,\dots,t_{m(6)}\}$ such that $g_0 = c, g_n = d$ and for all $i \in \{0,\dots,n-1\}$,

$$g_i = s_i^{\mathbf{B}}(a,b,b_2,\dots,b_5) \text{ and } g_{i+1} = s_i^{\mathbf{B}}(b,a,b_2,\dots,b_5).$$

Now there are only finitely many finite sequences of length $\leq m(4)$ that can be chosen from $\{t_1,\dots,t_{m(6)}\}$. Let these be $\sigma_0,\dots,\sigma_M$, where $M \in \omega$. Let $\Sigma = \{\sigma_0,\dots,\sigma_M\}$. For each $\sigma = s_0,\dots,s_{n-1} \in \Sigma$, let $\Psi_\sigma = \Psi_\sigma(x_0,x_1,x_2,x_3)$ be the following first order formula, where $\mathbf{x}$ abbreviates x_0,x_1,x_2,x_3:

$$\exists z_0 \exists z_n [z_0 \approx x_2 \wedge z_n \approx x_3 \wedge$$
$$z_0 \approx s_0(x_0,x_1,\mathbf{x}) \wedge s_0(x_1,x_0,\mathbf{x}) \approx s_1(x_0,x_1,\mathbf{x}) \wedge s_1(x_1,x_0,\mathbf{x}) \approx s_2(x_0,x_1,\mathbf{x})$$
$$\wedge \dots \wedge s_{n-2}(x_1,x_0,\mathbf{x}) \approx s_{n-1}(x_0,x_1,\mathbf{x}) \wedge s_{n-1}(x_1,x_0,\mathbf{x}) \approx z_n]$$

and let Ψ be the first order formula $\Psi_{\sigma_0} \vee \dots \vee \Psi_{\sigma_M}$.

We have shown that for any 4-generated $\mathbf{B} \in V$ and $a,b,c,d \in B$, $(c,d) \in \Theta^{\mathbf{B}}(a,b)$ if and only if for some $\sigma \in \Sigma$, $\mathbf{B} \models \Psi_\sigma[a,b,c,d]$ if and only if $\mathbf{B} \models \Psi[a,b,c,d]$. Let $\mathbf{A} \in V$ and $a,b,c,d \in A$ and $\mathbf{S} = \mathbf{Sg}^{\mathbf{A}}(a,b,c,d)$. Then by Corollary 0.29, $(c,d) \in \Theta^{\mathbf{A}}(a,b)$ if and only if $(c,d) \in \Theta^{\mathbf{S}}(a,b)$ (since V has the congruence extension property), if and only if $\mathbf{S} \models \Psi[a,b,c,d]$, in which case $\mathbf{A} \models \Psi[a,b,c,d]$.

Conversely, if $\mathbf{A} \models \Psi[a,b,c,d]$ then for some $\sigma \in \Sigma$, $\mathbf{A} \models \Psi_\sigma[a,b,c,d]$ so by Mal'cev's Lemma, $(c,d) \in \Theta^{\mathbf{A}}(a,b)$.

Thus $(c,d) \in \Theta^{\mathbf{A}}(a,b)$ if and only if $\mathbf{A} \models \Psi[a,b,c,d]$. Since $\mathbf{A} \in V$ and $a,b,c,d \in A$ were arbitrary and Ψ is independent of them, V has definable principal congruences.

□

The following definition will be needed in the next section.

Definition 1.19. For fixed elements a,b of an algebra $\mathbf{A}$ and a weak congruence formula Φ, let

$$C_\Phi = C_\Phi(\mathbf{A},a,b) := \{\{c,d\} \in A^{(2)} : \mathbf{A} \models \Phi[c,d,a,b,] \vee \Phi[d,c,a,b]\}.$$

If $\Phi(x_0, x_1, x_2, x_3)$ is any conjunction or disjunction of congruence formulas, then $\mathbf{A} \models \forall x_0 \forall x_1 \forall x_2 \forall x_3 [\Phi(x_0, x_1, x_2, x_3) \leftrightarrow \Phi(x_1, x_0, x_2, x_3)]$, so $C_\Phi = \{\{c, d\} \in A^{(2)} : \mathbf{A} \models \Phi[c, d, a, b]\}$.

1.3 Residually Small Varieties.

Definition 1.20. A variety V is *residually small* if there is some cardinal m strictly greater than the cardinalities of all the subdirectly irreducible algebras in the variety. In this case, the smallest cardinal m for which this is true will be called the *residual bound* of V. We say a variety is *residually* $< \mathsf{m}$ if every subdirectly irreducible algebra in the variety has cardinality $< \mathsf{m}$. We call V *residually countable* if it is residually $< \aleph_1$, *residually finite* if it is residually $< \aleph_0$ and *residually finitely bounded* if it is residually $< n$ for some $n \in \omega$ (i.e., if it has a finite residual bound). We call V *residually large* if it is not residually small.

Lemma 1.21. *Let V be a variety and m a cardinal. V has, up to isomorphism, only a set of m-generated algebras, i.e., there exists a set T of m-generated algebras in V such that every m-generated algebra in $V$is isomorphic to an algebra in T.*

Proof.

Let $\mathbf{F}$ be the V-free algebra on m free generators (i.e. $\mathbf{F} = \mathbf{F}_V(\bar{X})$ where $|\bar{X}| = \mathsf{m}$). Define $T = \{\mathbf{F}/\theta : \theta \in Con(\mathbf{F})\}$. T is a set (because F and $Con(\mathbf{F})$ are sets). Now if $\mathbf{A} \in V$ is m-generated then there is a surjective homomorphism $h : \mathbf{F} \to \mathbf{A}$ (Corollary 0.48) so $\mathbf{A} \cong \mathbf{F}/ker(h) \in T$. □

The following theorem is an adaptation of [Tay72, Theorem 1.2, p37] and [BB75, Theorem 5, p385] and states nine equivalent characterizations of residual smallness. The proof proceeds via (i)⇒(ii)⇒(iii)⇒(iv)⇒(v)⇒
(vi)⇒ (vii)⇒(i) then (ii)⇒(viii)⇒(ix)⇒(vii).

Theorem 1.22. [Tay72, Theorem 1.2]

Let V be a variety of algebras of the type $\mathcal{T} = \langle \mathsf{F}, ar \rangle$ defined by a set Σ' of equations, let Σ be the set of sentences that are the universal closures of the equations in Σ', and let $\mathsf{n} = \aleph_0 + |\mathsf{F}|$. Then the following conditions are equivalent:

(i) *There exists a cardinal m such that every subdirectly irreducible algebra in V has cardinality $\leq \mathsf{m}$ (i.e., V is residually small).*

(ii) *For every weak congruence $\mathcal{T}$-formula Φ, there exists a finite number $n = n(\Phi)$ such that*

$$\Sigma \vdash_{Th(\mathcal{T})} \forall y \forall z [(\exists x_1 \ldots \exists x_n \bigwedge_{1 \leq i < j \leq n} \Phi(x_i, x_j, y, z)) \to y \approx z].$$

(iii) *For each weak congruence $\mathcal{T}$-formula Φ there is an integer $n = n(\Phi)$ such that whenever* $\mathbf{A}$ *is an (a, b)-irreducible algebra in V then there is no set $X \subseteq A$ with $X^{(2)} \subseteq C_\Phi$ and $|X| > n$.*

(iv) *If* $\mathbf{A}$ *is an (a, b)-irreducible algebra in V then for each congruence $\mathcal{T}$-formula Φ, there is an integer n such that the conclusion of (iii) holds.*

(v) *Every subdirectly irreducible algebra in V has cardinality $\leq 2^{\mathsf{n}}$.*

(vi) *There are $\leq 2^{(2^{\mathsf{n}})}$ nonisomorphic subdirectly irreducible algebras in V.*

(vii) *There exists a* set *K such that $V \subseteq ISP(K)$.*

(viii) *If* $\mathbf{B} \in V$ *is an essential extension of* $\mathbf{A}$ *then $|B| \leq 2^{\mathsf{n}+|A|}$.*

(ix) *Each* $\mathbf{A} \in V$ *has, up to isomorphism, only a set of essential extensions in V.*

Moreover, if the above conditions hold then every $\mathbf{A} \in V$ *is a subalgebra of an absolute retract in V.*[11]

Proof.

(i)$\Rightarrow$(ii): Suppose (ii) fails and that m is as in (i). Let U be a set of variables such that $|U| = \mathsf{m}^+$ (the cardinal successor of m) with $y \notin U$ and $z \notin U$ and let $\preceq$ be a linear order on U. The failure of (ii) implies that there is a positive $\mathcal{T}$-formula $\Phi(\cdot, \cdot, \cdot, \cdot)$ such that

$\vdash_{Th(\mathcal{T})} \forall y \forall x[(\exists x\, \Phi(x, x, y, z)) \to y \approx z]$, but for any finite n,

$\Sigma \nvdash_{Th(\mathcal{T})} \forall y \forall z[(\exists x_1 \ldots \exists x_n \bigwedge_{1 \leq i < j \leq n} \Phi(x_i, x_j, y, z)) \to y \approx z]$, i.e., there is an algebra in V in which
$\forall y \forall z[(\exists x_1 \ldots \exists x_n \bigvee_{1 \leq i < j \leq n} \Phi(x_i, x_j, y, z)) \to y \approx z]$ is not true. This means that for any finite n, the set of $\mathcal{T}$-formulas $\Sigma \cup \{\Phi(x_i, x_j, y, z) : 1 \leq i < j \leq n\} \cup \{y \not\approx z\}$ is satisfiable.

Let $\Gamma = \Sigma \cup \{\Phi(u, v, y, z) : u, v \in U, u \prec v\} \cup \{y \not\approx z\}$. Take any finite subset Δ of Γ. Then $\Delta = \Sigma'' \cup \{\Phi(u^i, v^i, y, z) : i = 1, \ldots, r\} \cup \Omega$ where Σ'' is a finite subset of Σ, $r \in \omega, u^i, v^i \in U$ with $u^i \prec v^i$ for $i = 1, \ldots, r$ and Ω is either $\emptyset$ or $\{y \not\approx z\}$. Rename $u^1, v^1, u^2, v^2, \ldots, u^r, v^r$ as $x_1, x_2, x_3, x_4, \ldots, x_{2r}$.

Now $\Delta \subseteq \Sigma \cup \{\Phi(x_i, x_j, y, z) : 1 \leq i < j \leq 2r\} \cup \{y \not\approx z\}$ which is satisfiable. Thus Δ is satisfiable. Since Δ was an arbitrary finite subset of Γ, it follows from the Compactness Theorem (Theorem 0.43) that Γ is satisfiable. Thus there exists an algebra $\mathbf{A} \in V$ and an assignment $f : U \cup \{y, z\} \to A$ under which the formulas of Γ are true in $\mathbf{A}$.

[11] The converse is also true [Tay72], but its (nontrivial) proof requires an excursion into the theory of equationally compact algebras and will not be needed in this thesis.

Let $\theta \in Con(\mathbf{A})$ be maximal in $\{\rho \in Con(\mathbf{A}) : (f(y), f(z)) \notin \rho\}$. Such a θ exists by a routine application of Zorn's Lemma. We show that $\mathbf{A}/\theta$ is subdirectly irreducible.

For any $\eta \in Con(\mathbf{A})$, if $\theta \subset \eta$ then $(f(y), f(z)) \in \eta$ (by maximality of θ). Using the Correspondence Theorem, we may rephrase this as follows: any nonidentity congruence of $\mathbf{A}/\theta$ contains $(f(y)/\theta, f(z)/\theta)$. Thus, $id_{A/\theta} \neq \Theta^{\mathbf{A}/\theta}(f(x)/\theta, f(y)/\theta) = \bigcap(Con(\mathbf{A}/\theta) \setminus \{id_{A/\theta}\})$, and so $\mathbf{A}/\theta$ is subdirectly irreducible (with $\Theta^{\mathbf{A}/\theta}(f(x)/\theta, f(y)/\theta)$ as its monolith).
By (i), $|A/\theta| \leq \mathsf{m}$. .... (1)

Now let $u, v \in U$, with $u \prec v$. The natural map $\lambda : \mathbf{A} \to \mathbf{A}/\theta$ defined by $a \mapsto a/\theta$ is a surjective homomorphism, Φ is positive and $\mathbf{A} \models \Phi[f(u), f(v), f(y), f(z)]$, so since homomorphisms preserve positive sentences (by Theorem 0.41), $\mathbf{A}/\theta \models \Phi[f(u)/\theta, f(v)/\theta, f(y)/\theta, f(z)/\theta]$.

Now $f(y)/\theta \neq f(z)/\theta$ so it follows that $f(u)/\theta \neq f(v)/\theta$ (since $\vdash_{Th(T)} \forall y \forall z[(\exists x\, \Phi(x, x, y, z)) \to y \approx z]$). Thus, the map $u \mapsto f(u)/\theta$ from U to A/θ is one-to-one, so $|A/\theta| \geq |U| = \mathsf{m}^+ > \mathsf{m}$, which contradicts (1).

(ii)$\Rightarrow$(iii): Assume (ii). Let Φ be weak congruence formula and $n(\Phi)$ as in (ii). Let $\mathbf{A}$ be an (a,b)-irreducible algebra in V (so $a \neq b$). Suppose there exists $X \subseteq A$ such that $X^{(2)} \subseteq C_\Phi$ and such that $|X| > n(\Phi)$. Let $a_1, a_2, \ldots$ be a sequence of *distinct* elements of X of length greater than $n(\Phi)$. By (ii), $\Sigma \vdash_{Th(T)} \forall y \forall z[(\exists x_1 \ldots \exists x_n \bigwedge_{1 \leq i < j \leq n(\Phi)} \Phi(x_i, x_j, y, z)) \to y \approx z]$.

Whenever $1 \leq i < j \leq n(\Phi)$, we have $\{a_i, a_j\} \in X^{(2)} \subseteq C_\Phi$, so $\mathbf{A} \models \Phi[a_i, a_j, a, b]$. Then by (ii), we must have $a = b$, a contradiction.

(iii)$\Rightarrow$(iv): Every congruence formula is a weak congruence formula.

(iv)$\Rightarrow$(v): Let $\mathbf{A} \in V$ be subdirectly irreducible. Then $\mathbf{A}$ is (a,b)-irreducible for some $a, b \in A$ with $a \neq b$. Suppose $|A| > 2^{\mathsf{n}}$. For any congruence formula Φ and for fixed $e, f \in A$, recall that $C_\Phi = \{\{c,d\} \in A^{(2)} : \mathbf{A} \models \Phi[c, d, e, f]\}$. Let $\{c,d\} \in A^{(2)}$. Then $c \neq d$ so $\Theta^{\mathbf{A}}(c,d) \neq id_A$, so $(a,b) \in \Theta^{\mathbf{A}}(c,d)$ (since $\mathbf{A}$ is (a,b)-irreducible), so $\mathbf{A} \models \Phi[c, d, a, b]$ for some congruence formula Φ of V, by Mal'cev's Lemma, so $\{c,d\} \in C_\Phi$. Thus, $A^{(2)} \subseteq \bigcup\{C_\Phi : \Phi \text{ is a congruence formula}\}$, whence $\bigcup\{C_\Phi : \Phi \text{ is a congruence formula}\} = A^{(2)}$.

Now there are at most n congruence formulas, so $|\{C_\Phi : \Phi \text{ is a congruence formula}\}| \leq \mathsf{n}$ so by Theorem 1.10, there exist a congruence formula Ψ and a set $X \subseteq A$ with $|X| > \mathsf{n}$ such that $X^{(2)} \subseteq C_\Psi$, contradicting (iv). Consequently, $|A| \leq 2^{\mathsf{n}}$.

(v)⇒(vi): Let C be a set such that $|C| = 2^{\mathsf{n}}$. Let S be the class of all $\mathcal{T}$-algebras $\mathbf{D}$, such that $D \subseteq C$ and $\mathbf{D}$ is subdirectly irreducible.

We first show that S is a set. Suppose $f \in \mathsf{F}$ with $ar(f) = r \in \omega$. For each $\mathbf{D} \in S$, $f^{\mathbf{D}}$ is a function from D^r to D, therefore $f^{\mathbf{D}} \subseteq D^r \times D \subseteq C^r \times C \subseteq \bigcup_{r \in \omega}(C^r \times C)$, i.e., $f^{\mathbf{D}} \in \mathcal{P}(\bigcup_{r\in\omega}(C^r \times C))$ (a set). Now define $G : S \to \mathcal{P}(C) \times \prod_{f \in \mathsf{F}} \mathcal{P}(\bigcup_{r\in\omega}(C^r \times C))$ as follows: if $\mathbf{D} \in S$, let $G(\mathbf{D}) = \langle D; \langle f^{\mathbf{D}} \rangle_{f\in\mathsf{F}} \rangle$. G is one-to-one so S is equivalent to a subclass of a set, so S is a set.

Now let T be the class of all subdirectly irreducible algebras $\mathbf{A}$ in V. Let $\sim$ be the equivalence relation on T defined by $\mathbf{A} \sim \mathbf{B}$ if and only if $\mathbf{A} \cong \mathbf{B}$. By (v), each equivalence class has a representative $\mathbf{D} \in S$, and of course, distinct classes have distinct representatives. It is therefore enough to show that $|S| \leq 2^{(2^{\mathsf{n}})}$. For this it suffices to show $|\mathcal{P}(C) \times \prod_{f\in\mathsf{F}} \mathcal{P}(\bigcup_{r\in\omega}(C^r \times C))| \leq 2^{(2^{\mathsf{n}})}$.

Since $\aleph_0$, $|\mathsf{F}| \leq \mathsf{n} < 2^{\mathsf{n}}$, $|\mathcal{P}(C) \times \prod_{f\in\mathsf{F}} \mathcal{P}(\bigcup_{r\in\omega}(C^r \times C))| =$
$2^{|C|}.\prod_{f\in\mathsf{F}} 2^{(\sum_{r\in\omega}|C|^r.|C|)} = 2^{(2^{\mathsf{n}})}.\prod_{f\in\mathsf{F}} 2^{(2^{\mathsf{n}})} = 2^{(2^{\mathsf{n}})}.2^{(2^{\mathsf{n}})} = 2^{(2^{\mathsf{n}})}$.

(vi)⇒(vii): Recall that V_{SI} denotes the class of subdirectly irreducible members of V. By (vi) there exists a set $K \subseteq V_{SI}$ (with $|K| \leq 2^{(2^{\mathsf{n}})}$) such that every subdirectly irreducible algebra in V is isomorphic to an algebra in K. By Birkhoff's Subdirect Decomposition Theorem (Theorem 0.26), every algebra in V is in $IP_S(V_{SI})$, hence in $IP_S(K) \subseteq ISP(K)$. Thus, $V \subseteq ISP(K)$.

(vii)⇒(i): Let K be a set with $V \subseteq ISP(K)$. Then $L = \{|A| : \mathbf{A} \in K\}$ is a set of cardinals, so there exists a cardinal m with $\mathsf{d} \leq \mathsf{m}$ for all $\mathsf{d} \in L$.

Now take $\mathbf{B} \in V_{SI}$. Then $\mathbf{B} \in ISP(K)$, say $\mathbf{B}$ is isomorphic to a subalgebra $\mathbf{C}$ of $\prod_{i\in I} \mathbf{A}_i$ where $\mathbf{A}_i \in K$ for all $i \in I$. Now $\mathbf{C}$ is a subdirect product of the algebras $\pi_i[\mathbf{C}]$ $(i \in I)$, where each $\pi_j : \prod_{i\in I} \mathbf{A}_i \to \mathbf{A}_j$ is the j^{th} projection homomorphism. Since each $\pi_i[\mathbf{C}]$ is a subalgebra of $\mathbf{A}_i \in K$, $\mathbf{B}$ is isomorphic to a member of $P_S S(K)$. But $\mathbf{B}$ is subdirectly irreducible so $\mathbf{B}$ is isomorphic to a member of $S(K)$.

Now there exists $\mathbf{A} \in K$ with $\mathbf{B}$ isomorphic to a subalgebra of $\mathbf{A}$. Thus $|B| \leq |A| \leq \mathsf{m}$. Since $\mathbf{B} \in V_{SI}$ was arbitrary, the result follows.

(ii)⇒(viii): Let $\mathbf{B} \in V$ be an essential extension of $\mathbf{A}$. Let $X = \{x_\alpha : \alpha < \omega\}$ be a set of variables with $y, z \notin X$. Let $\mathsf{m} = \mathsf{n} + |A| = \aleph_0 + |\mathsf{F}| + |A|$. We show that $|B| \leq 2^{\mathsf{n}+|A|} = 2^{\mathsf{m}}$.

Suppose $|B| > 2^{\mathsf{m}}$. Then by Corollary 1.11, there exist $a, b \in A$ with $a \neq b$, and a weak congruence formula $\Phi(\cdot, \cdot, \cdot, \cdot)$ and an algebra $\mathbf{C}$ of type $\mathcal{T}[\mathbf{A}]$ and an assignment $f : X \to C$ such that (1) $\mathbf{C}$ satisfies all atomic or negated atomic $\mathcal{T}[\mathbf{A}]$-sentences that hold in $\mathbf{A}$ (hence, we may assume harmlessly that $\mathbf{A} \leq \mathbf{C}$); and (2) for every $\mathcal{T}$-identity $s \approx t$ such that $\mathbf{B} \models s \approx t$, we have that $\mathbf{C} \models s \approx t$; in particular, this is true for each $s \approx t \in \Sigma'$, since $\mathbf{B} \in V$, so $\mathbf{C} \models \Sigma$; and (3) whenever $i < j < \omega$, $\mathbf{C} \models \Phi[f(x_i), f(x_j), a, b]$.

Since Φ is a weak congruence formula, it follows from (ii) that there exists $n \in \omega$ such that $\Sigma \vdash_{Th(\mathcal{T})} \forall y \forall z[(\exists x_1 \ldots \exists x_n \bigwedge_{1 \leq i < j \leq n} \Phi(x_i, x_j, y, z)) \to y \approx z]$.

Using the assignment $f' : X \cup \{y, z\} \to C$ defined by $f' = f \cup \{(y, a), (z, b)\}$, we deduce from (2) and (3) that $a = b$, a contradiction. Therefore $|B| \leq 2^{\mathsf{m}}$.

(viii)⇒(ix): Let $\mathbf{A} \in V$. Let C be a set such that $A \subseteq C$ and $|C| = 2^{\mathsf{n}+|A|}$ (for example, we could take $C = A \cup (2^{\mathsf{n}+|A|} \times \{u\})$, where u is a set that is not in the range of A). Let S be the class of all $\mathcal{T}$-algebras $\mathbf{D}$ such that $D \subseteq C$ and $\mathbf{A} \leq \mathbf{D}$ and $\mathbf{D}$ is an essential extension of $\mathbf{A}$ in V. Exactly as in the proof of (v)⇒(vi), it follows that S is a set.

Now let T be the class of all essential extensions of $\mathbf{A}$ in V. Let $\sim$ be the equivalence relation on T defined by $\mathbf{B}_1 \sim \mathbf{B}_2$ if and only if there exists an isomorphism $\psi : \mathbf{B}_1 \to \mathbf{B}_2$ with $\psi|_{\mathbf{A}} = id_A$. We shall show that for each equivalence class X of $\sim$ there exists a $\mathbf{D} \in S$ such that $X = \mathbf{D}/\sim$. Then it will follow that the collection of equivalence classes of $\sim$ may be identified with a subclass of S, hence with a set (under the one-to-one assignment $X \mapsto \mathbf{D}$).

Let X be an equivalence class of $\sim$. Then there exists $\mathbf{B} \in T$ with $X = \mathbf{B}/\sim$. By (viii), $|A| \leq |B| \leq 2^{\mathsf{n}+|A|} = |C|$. We claim that there exists a bijection $\sigma : B \to D$ for some D such that $A \subseteq D \subseteq C$, with the property that $\sigma|_{\mathbf{A}} = id_A$. Now

$$|A| + |C \setminus A| = |C| = 2^{\mathsf{n}+|A|} \geq max\{2^{|A|}, 2^{\aleph_0}\} \text{ (because } \mathsf{n} \geq \aleph_0)$$

$$> max\{|A|, \aleph_0\} \text{ (by Cantor's Theorem)}$$

$$\geq |A|, \aleph_0.$$

This implies $|C \setminus A| \geq \aleph_0$ and also implies $|C \setminus A| = 2^{\mathsf{n}+|A|}$, otherwise $|A|, |C \setminus A| < 2^{\mathsf{n}+|A|}$ therefore $|A| + |C \setminus A| = max\{|A|, |C \setminus A|\} < 2^{\mathsf{n}+|A|} = |C|$, a contradiction. Now $|B \setminus A| \leq |B| \leq |C| = |C \setminus A|$, so there exist a subset E of $C \setminus A$ and a bijection $l : B \setminus A \to E$. Now $id_A \cup l$ is a bijection from B to $A \cup E$ and $A \subseteq A \cup E \subseteq C$. This establishes the claim.

Let σ and D be as in the claim. Define a $\mathcal{T}$-algebra $\mathbf{D}$ with universe D as follows: For each $f \in \mathsf{F}$ with $ar(f) = r \in \omega$, say, let

$$f^{\mathbf{D}}(d_1, \ldots, d_r) = \sigma[f^{\mathbf{B}}(\sigma^{-1}(d_1), \ldots, \sigma^{-1}(d_r))]$$

for any $d_1, \dots, d_r \in D$.

Now $\mathbf{D} \in S$ and $\sigma : \mathbf{B} \to \mathbf{D}$ is an isomorphism, so $\mathbf{D} \sim \mathbf{B}$, i.e., $X = \mathbf{D}/\sim$.

(ix)⇒(vii): We give an argument that is due to D. Higgs [Hig71], which is more direct than that of [Tay72].

Assume (ix), so for each $\mathbf{C} \in V$ there is a set $T(\mathbf{C})$ of essential extensions of $\mathbf{C}$ in V such that every essential extension of $\mathbf{C}$ in V is isomorphic to an algebra in $T(\mathbf{C})$. Also, by Lemma 1.21, there exists a set T of 2-generated algebras in V such that every 2-generated algebra in V is isomorphic to an algebra in T. Let $T' = \cup_{\mathbf{A} \in T}(T(\mathbf{A}))$. Note that T' is a set (because T and each $T(\mathbf{A}), \mathbf{A} \in T$, are sets).

Now let $\mathbf{B} \in V_{SI}$. Then there exist $a, b \in B$ (with $a \neq b$) such that $\mathbf{B}$ is (a,b)-irreducible. Let $\mathbf{S} = \mathbf{Sg}^{\mathbf{B}}(\{a,b\})$. Then S is 2-generated so there exists $\mathbf{S}' \in T$ with $\mathbf{S} \cong \mathbf{S}'$. Also, $\mathbf{B}$ is an essential extension of $\mathbf{S}$ (by (a,b)-irreducibility), so $\mathbf{B}$ is isomorphic to some essential extension of $\mathbf{S}'$. Now there exists $\mathbf{B}'$ such that $\mathbf{B} \cong \mathbf{B}' \in T(\mathbf{S}') \subseteq T'$.

Let $K = T'_{SI}$ (i.e. K is the class of all subdirectly irreducible algebras in T'). Then $K \subseteq T'$, so K is a set, and every subdirectly irreducible algebra in V is isomorphic to an element of K. (Thus, V has, up to isomorphism, only a set of subdirectly irreducible members).

By Birkhoff's Subdirect Decomposition Theorem (Theorem 0.26), every algebra in V is in $IP_S(V_{SI})$, hence in $IP_S(K) \subseteq ISP(K)$. Therefore $V \subseteq ISP(K)$.

The last assertion of the theorem follows from (ix) and Corollary 1.14 .

□

Consider the condition:

(ii)$'$: For each congruence $\mathcal{T}$-formula Φ, the conclusion of (ii) holds.

Obviously (ii) ⇒(ii)$'$, while (ii)$'$ ⇒ (iv) follows as a special case of the proof of (ii) ⇒ (iii). Thus, (ii)$'$ is a further characterization of a residually small variety.

Quackenbush's Problem [Qua71] is the following conjecture: if a finitely generated variety V of finite type has arbitrarily large *finite* subdirectly irreducible members then it must have an infinite one. In other words, no finitely generated variety of finite type has $\aleph_0$ as its residual bound. In the mid-1980's a stronger conjecture, called the *RS Conjecture* emerged: if a finitely generated variety is residually small then it has a finite residual bound. (The RS Conjecture does not impose the requirement of finite type.) These problems profoundly influenced research on residually small varieties. (See the Conclusion for details of their present status.)

We now consider residual smallness in relation to varieties with definable principal congruences, locally finite varieties and, as a special case, congruence distributive varieties. Corollary 1.24 below provides a partial answer to Quackenbush's question. It shows that varieties of finite type with definable principal congruences and infinitely many finite subdirectly irreducible algebras will have infinite subdirectly irreducible algebras.

Theorem 1.23. [BB75, Theorem 4]

If a variety V has definable principal congruences and is residually small, then V has a finite residual bound.

Proof.

We need to show there exists a finite cardinal n such that each subdirectly irreducible algebra in V has at most n elements. Suppose the principal congruences in the variety V are defined by the formula Ψ. By the proof of Theorem 1.16 (ii), Ψ is equivalent to a weak congruence formula (in fact, to a disjunction of congruence formulas). By Theorem 1.22 (iii) there is an integer $n(\Psi)$ such that whenever $\mathbf{A}$ is an (a,b)-irreducible algebra in V then there is no set $X \subseteq A$ with $X^{(2)} \subseteq C_\Psi$ and $|X| > n(\Psi)$. (Recall that $C_\Psi = \{\{c,d\} \in A^{(2)} : \mathbf{A} \models \Psi[c,d,a,b]\}$.)

Let $\mathbf{A}$ be any subdirectly irreducible algebra in V. Then for some $a, b \in A$, with $a \neq b$, $\mathbf{A}$ is (a,b)-irreducible (by Theorem 0.21). Let $\{c,d\} \in A^{(2)}$. Then $c \neq d$ so $\Theta^{\mathbf{A}}(c,d) \neq id_A$, so $(a,b) \in \Theta^{\mathbf{A}}(c,d)$ by (a,b)-irreducibility. Now $\mathbf{A} \models \Psi[c,d,a,b]$ so $\{c,d\} \in C_\Psi$. Therefore $A^{(2)} \subseteq C_\Psi$, so $|A| \leq n(\Psi)$ (which is independent of $\mathbf{A}$). Thus $n(\Psi)$ is the n we seek.

□

Corollary 1.24. [BB75]

Let V be a variety of finite type with definable principal congruences. If V has infinitely many nonisomorphic finite subdirectly irreducible algebras, V has subdirectly irreducible algebras of every infinite cardinality.

Proof.

Let the type of V be $\mathcal{T} = \langle\{m_1, \ldots, m_k\}, ar\rangle$ and let $0 < n \in \omega$. Let A be an n-element set. For each $i \in \{1, \ldots, k\}$, there are $|A|^{|A^{m_i}|} = n^{(n^{m_i})}$ different m_i-ary operations on A.

Therefore there are at most $n^{(n^{m_1})} \ldots n^{(n^{m_k})} = n^{(\Sigma_{i=1}^{k} n^{m_i})} = \mathrm{c}(n) \in \omega$ different ways of making A an algebra of type $\langle\{m_1, \ldots, m_k\}, ar\rangle$, so there are

$\leq \mathsf{c}(n)$ nonisomorphic $\mathcal{T}$-algebras of size n. Thus the number of nonisomorphic algebras in V of size n is finite.

Now given that V has infinitely many nonisomorphic finite subdirectly irreducible algebras, it follows that V is not residually $< n$ for any $n \in \omega$ (otherwise it would have at most $\Sigma_{r=2}^{n-1}\mathsf{c}(r) \in \omega$ such algebras). By Theorem 1.23, V is not residually small. Let m be an infinite cardinal, so there is a subdirectly irreducible algebra $\mathbf{B} \in V$ with $|B| > \mathsf{m}$. Choose $X \subseteq B$ with $|X| = \mathsf{m}$, so $|\{m_1, \dots, m_k\}| + |X| = \mathsf{m} < |B|$.

By the Downward Löwenheim-Skolem Theorem (Theorem 0.45), there exists a subalgebra $\mathbf{C}$ of $\mathbf{B}$ with $X \subseteq C$ and $|C| = \mathsf{m}$ such that $\mathbf{B}$ and $\mathbf{C}$ satisfy exactly the same first order $\mathcal{T}$-sentences. Let $\Phi(x_0, x_1, x_2, x_3)$ be a first order $\mathcal{T}$-formula defining the principal congruences of algebras in V, i.e., whenever $\mathbf{D} \in V$ and $a, b, c, d \in D$ we have

$$(c, d) \in \Theta^{\mathbf{D}}(a, b) \text{ if and only if } \mathbf{D} \models \Phi[a, b, c, d].$$

Let Ψ be the first order $\mathcal{T}$-sentence

$$\exists x \exists\, y((x \not\approx y) \wedge \forall z \forall w\ ((z \not\approx w) \to \Phi[z, w, x, y])).$$

Notice that an algebra in V satisfies Ψ if and only if it is "(x, y)-irreducible for some x, y", i.e., subdirectly irreducible. Thus, $V_{SI} = \{\mathbf{E} \in V : \mathbf{E} \models \Psi\}$. Now $\mathbf{B} \in V_{SI}$, so $\mathbf{B} \models \Psi$, therefore $\mathbf{C} \models \Psi$. Also, $\mathbf{C} \in V$ (since $\mathbf{C} \leq \mathbf{B}$), so $\mathbf{C} \in V_{SI}$. Since $|C| = \mathsf{m}$, this completes the proof.

□

Proposition 1.25. [BB75]

If the variety V is congruence distributive and is generated by a set K_0 of algebras all with cardinality less than n, where $n \in \omega$, then V is residually $< n$.

Proof.

Let $V = V(K_0)$ where for each $\mathbf{B} \in K_0$, $|B| < n$. By Jónsson's Theorem (Theorem 0.34), if $\mathbf{A} \in V_{SI}$, then $\mathbf{A} \in HSP_U(K_0)$. By Łoś's Theorem (Theorem 0.42), algebras in $P_U(K_0)$ have fewer than n elements since having fewer than n elements is a first order property (because n is finite).

Thus for each $\mathbf{A} \in V_{SI}$, $|A| < n$ since homomorphic images of subalgebras of algebras $\mathbf{C} \in P_U(K_0)$ will have cardinality $\leq |C|$. Thus, V is residually $< n$.

□

We include here a result known as *Quackenbush's Theorem*, because it contrasts interestingly with Corollary 1.24 and because it will be needed in Chapter 4.

Proposition 1.26. (Quackenbush's Theorem) [Qua71]

If V is a locally finite variety with, up to isomorphism, only finitely many finite subdirectly irreducible algebras, then V has no infinite subdirectly irreducible member, hence V is residually $< n$, for some $n \in \omega$.

Proof.

Let V^* be the class of all finite subdirectly irreducible members of V. If $\mathbf{A} \in V$, let K be the set of all finitely generated subalgebras of $\mathbf{A}$. By Theorem 0.35, $\mathbf{A} \in ISP_U(K)$, and since V is a locally finite variety, K consists of finite algebras. It follows from Birkhoff's Subdirect Representation Theorem (Theorem 0.26) that $K \subseteq IP_S(V^*) \subseteq ISP(V^*)$, hence $\mathbf{A} \in ISP_USP(V^*)$.

Thus $\mathbf{A}$ belongs to the quasivariety $ISPP_U(V^*)$ generated by V^* (see Theorem 0.39). But an ultraproduct of finitely many finite algebras is isomorphic to one of those algebras, by Lemma 0.33, so $\mathbf{A} \in ISP(V^*)$. Thus $\mathbf{A}$ is isomorphic to a subalgebra $\mathbf{B}$ of a product $\prod_{i \in I} \mathbf{C}_i$ of algebras $\mathbf{C}_i \in V^*$.

If $\alpha : \mathbf{A} \to \mathbf{B}$ is this isomorphism and $\pi_j : \prod_{i \in I} \mathbf{C}_i \to \mathbf{C}_j$ is the j^{th} projection homomorphism for each $j \in I$, then $(\pi_j \circ \alpha)[\mathbf{A}]$ is a subalgebra of $\mathbf{C}_j$, for each j, and $\mathbf{A}$ is isomorphic to a subdirect product of the algebras $(\pi_i \circ \alpha)[\mathbf{A}], i \in I$. Thus, $\mathbf{A} \in IP_SS(V^*)$.

Now suppose $\mathbf{A}$ is subdirectly irreducible. Then $\mathbf{A} \in S(V^*)$ so $\mathbf{A}$ is finite. Hence V has no infinite subdirectly irreducible algebras.

□

In [Tay72] Taylor poses the question: For which residually small varieties will there be a uniform $n \in \omega$ such that for *this* n , and for *all* weak congruence formulas Φ, the conclusion of Theorem 1.22 (ii) holds? The following theorem shows that in the varieties that qualify, we may choose n to be just the residual bound of V.

Theorem 1.27. [BB75, Theorem 6]

Let V be a variety of type $\mathcal{T}$ defined by a set Σ' of equations and let Σ be the set of sentences that are the universal closures of the equations in Σ'. For every positive integer n the following are equivalent:

(i) *V is residually $< n$.*

(ii) *For every weak congruence $\mathcal{T}$-formula Φ,*

$$\Sigma \vdash_{Th(\mathcal{T})} \forall y \forall z [(\exists x_1 \ldots \exists x_n \bigwedge_{1 \leq i < j \leq n} \Phi(x_i, x_j, y, z)) \to y \approx z].$$

(iii) *If* $\mathbf{A} \in V$ *is* (a,b)*-irreducible and* $X^{(2)} \subseteq C_\Phi$ *for some weak congruence formula* Φ *then* $|X| \leq n$.

Proof.

Let $0 < n \in \omega$.

(i)$\Rightarrow$(ii): Suppose (ii) fails for some weak congruence formula Φ. Then there is an algebra $\mathbf{A} \in V$ such that $\mathbf{A} \models \exists y \exists z \exists x_1 \ldots \exists x_n (\bigwedge_{1 \leq i < j \leq n} \Phi(x_i, x_j, y, z) \wedge y \not\approx z)$. Choose $a, b, c_1, \ldots, c_n \in A$ such that $\mathbf{A} \models \bigwedge_{1 \leq i < j \leq n} \Phi[c_i, c_j, a, b]$ and $a \neq b$.

By a routine application of Zorn's Lemma there is a maximal congruence on $\mathbf{A}$ that separates a and b, i.e., the set $S = \{\gamma \in Con(\mathbf{A}) : (a,b) \notin \gamma\}$ has a $\subseteq$-maximal element, say θ.

By the maximality of θ in S and the Correspondence Theorem, $\mathbf{A}/\theta$ is $(a/\theta, b/\theta)$-irreducible and so $\mathbf{A}/\theta$ is subdirectly irreducible by Proposition 0.21.

Let h be the natural homomorphism from $\mathbf{A}$ to $\mathbf{A}/\theta$ and let $1 \leq i < j \leq n$. Since Φ is positive, $\mathbf{A}/\theta \models \Phi[h(c_i), h(c_j), h(a), h(b)]$, since $\mathbf{A} \models \Phi[c_i, c_j, a, b]$. Φ is a weak congruence formula so $\mathbf{A} \models \forall y \forall z[(\exists x\, \Phi(x, x, y, z)) \rightarrow y \approx z]$ but $h(a) \neq h(b)$ so we must have $h(c_i) \neq h(c_j)$, so $c_i/\theta \neq c_j/\theta$. Thus, $|A/\theta| \geq n$, contradicting (i).

(ii)$\Rightarrow$(iii): Assume (ii). Then by the proof of Theorem 1.22 ((ii)$\Rightarrow$(iii)), with $n(\Phi) = n$, (iii) follows.

(iii)$\Rightarrow$(i): Let $\mathbf{A}$ be any subdirectly irreducible algebra in V. Then $\mathbf{A}$ is (a,b)-irreducible for some $a, b \in A$ with $a \neq b$, by Proposition 0.21 (i). Suppose $|A| \geq n$. Then we can choose $Y = \{y_1, \ldots, y_n\}$, a set of n distinct elements of $\mathbf{A}$. Since the elements of Y are distinct, for each i, j with $i \neq j, \Theta^{\mathbf{A}}(y_i, y_j) \neq id_A$ so $(a,b) \in \Theta^{\mathbf{A}}(y_i, y_j)$.

Now by Mal'cev's Lemma, for each i, j with $i \neq j$ there is a congruence formula Φ_{ij} such that $\mathbf{A} \models \Phi_{ij}[y_i, y_j, a, b]$. Let $\Psi = \bigvee_{1 \leq i < j \leq n} \Phi_{ij}$. Then Ψ is a weak congruence formula so by (iii), if $X \subseteq C_\Psi$, then $|X| \leq n$.

For each $\{y_i, y_j\} \in Y^{(2)}$, we have $\mathbf{A} \models \Phi_{ij}[y_i, y_j, a, b]$ so $\{y_i, y_j\} \in C_\Psi$, therefore $Y^{(2)} \subseteq C_\Psi$. However $|Y| > n$, contradicting (iii), so we must have $|A| < n$. Since $\mathbf{A}$ was an arbitrary subdirectly irreducible algebra in V, (i) holds. □

1.3.1 Illustrative Examples. We give some examples of residually small varieties and, following [Tay72], show that the upper bounds stated in Theorem 1.22 are the best possible.

Example 1.28.

(i) We shall show in Section 1.4.2 that the class of subdirectly irreducible Abelian groups is (up to isomorphism) the set $\{\mathbb{Z}_{p^n} : p \text{ prime}, n \in \mathbb{N} \cup \{\infty\}\}$ (with cardinality $\aleph_0$), so the variety of Abelian groups is residually small by Theorem 1.22 (vi). Indeed, since $|\mathbb{Z}_{p^\infty}| = \aleph_0$, this variety is residually $< \aleph_1$ (and $\aleph_1$ is its residual bound).

More generally, we shall show that the variety of (unital) modules over any ring with identity is residually small.

(ii) For a finite set of finite algebras K and for a congruence distributive variety V such that $V = V(K)$, V will be residually small, by Proposition 1.25.

Since lattices and Boolean algebras are congruence distributive [FN42], the variety generated by a finite set of finite lattices [respectively Boolean algebras] is residually small. In fact the 2-element distributive lattice [respectively Boolean algebra] is the only subdirectly irreducible distributive lattice [respectively Boolean algebra] and therefore generates the variety DL [respectively BA] of all distributive lattices [respectively Boolean algebras]. These varieties are therefore residually small, with residual bound 3.

An algebra $\mathbf{A}$ (on a variety V) of type $\mathcal{T} = \langle \mathsf{F}, ar \rangle$ is called *unary* if $ar(f) \leq 1$ for all $f \in \mathsf{F}$.

Theorem 1.29. [Hig71]

Any variety V of unary algebras is residually small.

Proof.

Let V be a variety of unary algebras of type $\mathcal{T} = \langle \mathsf{F}, ar \rangle$. If $\mathbf{A} \in V$ and $f : A \to A$ is a nonconstant unary polynomial function of $\mathbf{A}$ then, since $\mathbf{A}$ is unary, there exists a *unary $\mathcal{T}$-term* t such that for all $a \in A$, $f(a) = t^{\mathbf{A}}(a)$. Let T_1 be the set of all unary terms (in the variable x, say), of V.

Let $\mathbf{A} \in V$ be subdirectly irreducible, so there exist distinct $a, b \in A$ such that $\mathbf{A}$ is (a, b)-irreducible. Then for any $c, d \in A$ with $c \neq d$, we have $(a, b) \in \Theta^{\mathbf{A}}(c, d)$. By Mal'cev's Lemma, there exist unary polynomial functions $p_1, \ldots, p_n : A \to A$ of $\mathbf{A}$ and pairs $(u_1, v_1), \ldots, (u_n, v_n) \in \{(c, d), (d, c)\}$ such that

$$\begin{aligned} a &= p_1(u_1) \\ p_i(v_i) &= p_{i+1}(u_i) \text{ for } 1 \leq i < n \\ p_n(v_n) &= b, \end{aligned}$$

and such that the above scheme involves as few equations as possible. For each i, $p_i(u_i) \neq p_i(v_i)$ (hence each p_i is a nonconstant function), otherwise two of the above equations could be replaced by a single equation. Thus, we can assume, without loss of generality, that each p_i is a unary *term* function $p_i^{\mathbf{A}}$, where $p_i \in T_1$.

It follows that the function $A \to \mathcal{P}(T_1)$ defined by $e \mapsto \{p \in T_1 : p^{\mathbf{A}}(e) = a\}$ is one-to-one. Thus, $|A| \leq |\mathcal{P}(T_1)| = 2^{|T_1|}$ (which is independent of A).

□

In fact, the above proof shows that the residual bound of a unary variety is at most $(2^{\mathsf{n}})^+$, where n is the cardinality of the V-free algebra on one free generator.

Example 1.30. [Tay72]

Recall that $\mathcal{T} = \langle \mathsf{F}, ar\rangle$ and let $\mathsf{n} = \aleph_0 + |\mathsf{F}|$. We show that the upper bound 2^{n} in Theorem 1.22 (v) is the best possible.

Let A be the Cantor set 2^{ω} of countable sequences of 0's and 1's and let $\mathbf{A}$ be the unary algebra $\langle A; f, g\rangle$ where

$$f(\langle a_0, a_1, a_2, \ldots\rangle) = \langle a_1, a_2, a_3, \ldots\rangle \text{ and } g(\langle a_0, a_1, a_2, \ldots\rangle) = \langle a_0, a_0, a_0, \ldots\rangle.$$

Of course, $|A| = 2^{\aleph_0}$. Let V be the variety of all algebras with just two unary (and no other) operations, so for V, the value of n in Theorem 1.22 is $\aleph_0 + 2 = \aleph_0$; also, $\mathbf{A} \in V$. We show that $\mathbf{A}$ is subdirectly irreducible, so the residual bound of V is $(2^{\aleph_0})^+ = (2^{\mathsf{n}})^+$, and Theorem 1.22 (v) can't be improved.

Let $a = \langle 1, 1, \ldots\rangle$ (constant sequence of 1's), and $b = \langle 0, 0, \ldots\rangle$ (constant sequence of 0's).

Consider $\Theta^{\mathbf{A}}(a, b) \in Con(\mathbf{A})$. Suppose $id_A \neq \psi \in Con(\mathbf{A})$. Then there exist $c = \langle c_0, c_1, c_2, \ldots\rangle$ and $d = \langle d_0, d_1, d_2, \ldots\rangle$ such that $c \neq d$ and $c\psi d$. Since $c \neq d$, they must differ in at least one entry, say $c_i \neq d_i$.

Now $f(f(\ldots(f(c))\ldots))$ (i applications) $= \langle c_i, c_{i+1}, \ldots\rangle$,
$f(f(\ldots(f(d))\ldots))$ (i applications) $= \langle d_i, d_{i+1}, \ldots\rangle$ and $c_i \neq d_i$, say $c_i = 0$ and $d_i = 1$.

Since ψ is a congruence relation,

$\langle c_i, c_{i+1}, \ldots\rangle \psi \langle d_i, d_{i+1}, \ldots\rangle$ and $g(\langle c_i, c_{i+1}, \ldots\rangle)\psi g(\langle d_i, d_{i+1}, \ldots\rangle)$,
i.e., $\langle 0, 0, 0, \ldots\rangle \psi \langle 1, 1, 1, \ldots\rangle$, i.e., $a\psi b$.

Since ψ was arbitrary, $(a, b) \in \psi$ whenever $id_A \neq \psi \in Con(\mathbf{A})$. Thus, $\Theta^{\mathbf{A}}(a, b)$ is the monolith of $\mathbf{A}$. Therefore $\mathbf{A}$ is subdirectly irreducible, as required.

From Theorem 1.22 ((i)⇒(v)), we deduce:

Corollary 1.31. [Tay72]

Let V be a $\mathcal{T}$-variety, where $\mathcal{T} = \langle \mathsf{F}, ar\rangle$ and $\mathsf{n} = \aleph_0 + |\mathsf{F}|$. If V contains a subdirectly irreducible algebra of cardinality greater than 2^{n} (i.e., $\geq (2^{\mathsf{n}})^+$) then V is residually large, i.e., it contains arbitrarily large subdirectly irreducible algebras.[12]

Example 1.32. [Tay72]

Again, let $\mathsf{n} = \aleph_0 + |\mathsf{F}|$ where $\mathcal{T} = \langle \mathsf{F}, ar\rangle$. By Theorem 1.22 ((i)⇒(vi)), if V is residually small there are $\leq 2^{(2^{\mathsf{n}})}$ nonisomorphic subdirectly irreducible algebras in V. We show this upper bound is the best possible.

Let S be any subset of the Cantor set 2^ω (as in Example 1.30). Define the unary algebra $\mathbf{A}_S = \langle A; f, g, O, h_S\rangle$ where A, f, g are as in Example 1.30 (note $A = 2^\omega$) and

$$\begin{aligned} O(a) &= \langle 0,0,0,\dots\rangle, \\ h_S(a) &= \begin{cases} \langle 1,1,1,\dots\rangle & \text{if } a \in S \\ \langle 0,0,0,\dots\rangle & \text{otherwise.} \end{cases} \end{aligned}$$

Exactly as in Example 1.30, $\mathbf{A}_S$ is subdirectly irreducible for each $S \subseteq 2^\omega$.

We show that distinct subsets S yield nonisomorphic algebras $\mathbf{A}_S$. Take arbitrary $S_1, S_2 \subseteq 2^\omega$, and suppose there exists an isomorphism $k : \mathbf{A}_{S_1} \cong \mathbf{A}_{S_2}$.

We claim that k must be the identity map on A. For suppose there exists $y \in A = 2^\omega$ such that $k(y) \neq y$, i.e., $k(y)$ and y differ in at least one co-ordinate, say $(k(y))(i) = 0,\ y(i) = 1$. Then $k(g(f^i(y))) = k(g(f^i(\langle a_0, a_1, \dots, 1, \dots\rangle))) = k(g(\langle 1, \dots\rangle)) = k(\langle 1, 1, \dots\rangle)$

and $g(f^i(k(y))) = g(f^i(\langle b_0, b_1, \dots, 0, \dots\rangle)) = g(\langle 0, \dots\rangle) = \langle 0, 0, \dots\rangle$.

Since k is a homomorphism we must have $k(g(f^i(y))) = g(f^i(k(y)))$, i.e., $k(\langle 1, 1, \dots\rangle) = \langle 0, 0, \dots\rangle$. .... (*)

But, for all $\langle a_0, a_1, \dots\rangle \in A$, $\langle 0, 0, \dots\rangle = O_{S_2}(k(\langle a_0, a_1, \dots\rangle))$

$= k(O_{S_2}(\langle a_0, a_1, a_2, \dots\rangle))$

$= k(\langle 0, 0, \dots\rangle)$ so by (*), $k(\langle 1, 1, \dots\rangle) = k(\langle 0, 0, \dots\rangle)$ but k is one-to-one, therefore $\langle 1, 1, \dots\rangle = \langle 0, 0, \dots\rangle$, a contradiction. Therefore k must be the identity map on $\mathbf{A}$.

Suppose $c \in S_1$ but $c \notin S_2$. Then $k(h_{S_1}(c)) = k(\langle 1, 1, \dots\rangle) = \langle 1, 1, \dots\rangle$ and $h_{S_2}(k(c)) = h_{S_2}(c) = \langle 0, 0, \dots\rangle$. Thus $k(h_{S_1}(c)) \neq h_{S_2}(k(c))$, contradicting the fact that k is a homomorphism. This shows that $S_1 \subseteq S_2$.

[12] This is sometimes expressed as follows: $(2^{\mathsf{n}})^+$ is the *Hanf number* for subdirect irreducibility in varieties of type $\langle \mathsf{F}, ar\rangle$ with $\mathsf{n} = \aleph_0 + |\mathsf{F}|$.

By symmetry, $S_2 \subseteq S_1$, hence $S_1 = S_2$, as required. Therefore distinct subsets of 2^ω must give rise to distinct algebras $\mathbf{A}_S = \langle A; f, g, O, h_S \rangle$.

Now $\mathsf{n} = \aleph_0 + 4 = \aleph_0$ and the number of subsets of 2^ω is $2^{(2^{\aleph_0})}$ therefore there are $2^{(2^{\mathsf{n}})}$ nonisomorphic subdirectly irreducible algebras $\mathbf{A}_S$ in the variety of all unary algebras $\langle A; f, g, O, h_s \rangle$ (which is residually small, by Theorem 1.29).

Example 1.33. [Tay72]

Following [Tay72] we show that when $\mathsf{n} = \aleph_0$, the upper bound $2^{\mathsf{n}+|A|}$ of Theorem 1.22 (viii) is the best possible.

By Example 1.28 (ii), the variety V of Boolean algebras $\langle C; \vee, \wedge, ', 0, 1 \rangle$ is residually small, with $\mathsf{n} = \aleph_0 + 5 = \aleph_0$.

Assume X is an infinite set with $|X| = \mathsf{m}$. Let $\mathbf{B}$ be the Boolean algebra of all subsets of X so $|B| = |\mathcal{P}(X)| = 2^{|X|} = 2^{\mathsf{m}}$. Let $\mathbf{A}$ be the Boolean algebra of finite and cofinite subsets of X. Recall that the number of finite subsets of X is m. There is a one-to-one correspondence between the finite and the cofinite subsets of X, so $|A| = \mathsf{m} + \mathsf{m} = \mathsf{m}$.

We show $\mathbf{B}$ is an essential extension of $\mathbf{A}$. Let $\theta \in Con(\mathbf{B})$ with $\theta \neq id_B$, so there exists $(c, d) \in \theta$ such that $c \neq d$, say $c \not\subseteq d$. Now there exists $x \in X$ such that $x \in c, x \notin d$. θ is a congruence relation so we have $(\{x\} \cap c)\theta(\{x\} \cap d)$, i.e., $(\{x\}, \emptyset) \in \theta$. But $\{x\}, \emptyset \in A$, and $\{x\} \neq \emptyset$ so $\theta|_{\mathbf{A}} \neq id_A$, as required.

Now $|B| = 2^{\mathsf{m}}$ and $\mathsf{n} + |A| = \aleph_0 + \mathsf{m} = \mathsf{m}$ (since $\mathsf{m} \geq \aleph_0$) in this example, so $|B| = 2^{\mathsf{n}+|A|}$.

1.4 Categorical Properties : Injectivity. We now consider the connections between (a, b)-irreducible algebras, essential extensions and absolute retracts in a variety V. The next few results are largely folklore, the main references being [Ban70], [GL71], [Bac72], [BN72] and [Tay72].

We define V-maximal irreducible algebras and give some properties and examples of these. The results will be applied when we consider the notion of the injective hull of an algebra. In the last theorem of this chapter, we describe a bound on the size of the injective hull of an algebra.

Proposition 1.34. [Tay72]

An (a, b)-irreducible algebra $\mathbf{B} \in V$ is an absolute retract in a variety V if and only if $\mathbf{B}$ is $\leq$-maximal among (a, b)-irreducible algebras in V.

Proof.

Let $\mathbf{B} \in V$ be (a, b)-irreducible and an absolute retract in V . By Lemma 1.7, if there exists some $\mathbf{T} \in V$ such that $\mathbf{B} < \mathbf{T}$ and $\mathbf{T}$ is (a, b)-irreducible, then both $\mathbf{B}$ and $\mathbf{T}$ are essential extensions of $\mathbf{A} = \mathbf{Sg}^{\mathbf{A}}(\{a, b\})$, but this contradicts Lemma 1.13. Thus $\mathbf{B}$ is maximal among (a, b)-irreducible algebras in V.

Conversely, let $\mathbf{B}$ be maximal among (a, b)-irreducible algebras in V. By Lemma 1.7, since $\mathbf{B}$ is (a, b)-irreducible, $\mathbf{B}$ is an essential extension of $\mathbf{A} = \mathbf{Sg}^{\mathbf{A}}(\{a, b\})$. .... (*)

For any $\mathbf{T} \in V$ such that $\mathbf{B} < \mathbf{T}$, $\mathbf{T}$ is not (a, b)-irreducible since $\mathbf{B}$ is maximal with respect to the property of being (a, b)-irreducible. Therefore by Lemma 1.8, $\mathbf{T}$ is not an essential extension of $\mathbf{B}$, so no proper extension of $\mathbf{B} \in V$ is an essential extension of $\mathbf{B}$. By Lemma 1.13, $\mathbf{B}$ is an absolute retract in V . □

Definition 1.35. Let $\mathbf{A}$ be an algebra in a variety V. We call $\mathbf{A}$ a *V-maximal irreducible* algebra if for some $a, b \in A$ with $a \neq b$, $\mathbf{A}$ is (a, b)-irreducible and $\mathbf{A}$ is not a proper subalgebra of any (a, b)-irreducible algebra in V.

Proposition 1.36. [Tay72]

If V is a residually small variety, every subdirectly irreducible algebra in V has a V-maximal irreducible extension.

Proof.

Let $\mathbf{A} \in V$ be subdirectly irreducible algebra and choose $a, b \in A$ such that $\mathbf{A}$ is (a, b)-irreducible. Since V is residually small, $\mathbf{A}$ has (up to isomorphism) only a set of essential extensions in V (by Theorem 1.22 (ix)) and by Corollary 1.14, some essential extension $\mathbf{B}$ of $\mathbf{A}$ is an absolute retract in V. By Lemma 1.8 this $\mathbf{B}$ is (a, b)-irreducible.

By Proposition 1.34, since $\mathbf{B}$ is (a, b)-irreducible and $\mathbf{B}$ is an absolute retract, $\mathbf{B}$ is maximal among (a, b)-irreducible algebras in V, i.e., $\mathbf{B}$ is V-maximal irreducible. □

Remark 1.37. [Tay72]

(i) By Example 1.28 (ii), the two-element Boolean algebra [respectively distributive lattice] is, up to isomorphism, the only V-maximal irreducible algebra where V is the variety of all Boolean algebras [respectively distributive lattices].

(ii) We shall see in Section 1.4.2 that if V is the variety of all Abelian groups then the V-maximal irreducible algebras are, up to isomorphism, just the groups $\mathbb{Z}_{p^\infty}$, where p is prime.

Lemma 1.38. [Tay72, Lemma 1.20]

Suppose that $\mathbf{B}$ is a subalgebra of a product of algebras each of cardinality $\leq \mathsf{m}$ and that $\mathbf{B}$ is an essential extension of an algebra $\mathbf{A}$. Then $|B| \leq \mathsf{m}^{(|A|^2)}$.

Proof.

There exist algebras $\mathbf{C}_i, i \in I$ such that $\mathbf{B} \leq \prod_{i \in I} \mathbf{C}_i$, where $|C_i| \leq \mathsf{m}$ for each $i \in I$. We show that $\mathbf{B}$ is isomorphic to a subalgebra of $\prod_{i \in J} \mathbf{C}_i$, for some $J \subseteq I$ such that $|J| \leq |A|^2$. Then $|B| \leq |\prod_{i \in J} C_i| \leq \mathsf{m}^{(|A|^2)}$.

Now $\mathbf{A} \leq \prod_{i \in I} \mathbf{C}_i$. For any $a, b \in A$ such that $a \neq b$, there exists $j \in I$ such that $a(j) \neq b(j)$. Select (by the Axiom of Choice) such a j for each pair $(a, b) \in A \times A$ such that $a \neq b$; let J be the set of these indices j, so $|J| \leq |A|^2$. Define $g : \mathbf{B} \to \prod_{i \in J} \mathbf{C}_i$ by $(g(b))(i) = b(i)$ for each $i \in J$. Then g is a homomorphism.

By construction, $g|_{\mathbf{A}}$ is one-to-one. Since $\mathbf{B}$ is an essential extension of $\mathbf{A}$, g is one-to-one.

□

1.4.1 Injectivity. For a variety V, we define V-injective algebras and the notion of transferable injections in V and establish when injections are transferable in V. We present a characterization of residually small varieties with transferable injections in terms of V-injective algebras. This leads to the concept of the injective hull of an algebra and finally to a result showing that the size of the injective hull of an algebra $\mathbf{A}$ is bounded by the cardinal $2^{\mathsf{n}+|A|}$ mentioned in Theorem 1.22 (viii) (even if V is not residually small).

Definition 1.39. An algebra $\mathbf{A}$ in a variety V is called *V-injective* if whenever $\mathbf{B} \leq \mathbf{T} \in V$ and $h : \mathbf{B} \to \mathbf{A}$ is a homomorphism, there exists a homomorphism $f : \mathbf{T} \to \mathbf{A}$ extending h. We say the variety V has *enough injectives* if every algebra in V can be embedded in some V-injective algebra.

Definition 1.40. We say that *injections are transferable* in a variety V if for any $\mathbf{A}, \mathbf{B}, \mathbf{C} \in V$, for any homomorphism $f : \mathbf{A} \to \mathbf{C}$ and any embedding $u : \mathbf{A} \to \mathbf{B}$, there exist $\mathbf{D} \in V$, a homomorphism $g : \mathbf{B} \to \mathbf{D}$ and an embedding $v : \mathbf{C} \to \mathbf{D}$ such that $v \circ f = g \circ u$ (as in the diagram).

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "u"'] & C \arrow[d, "v"] \\
B \arrow[r, "g"'] & D
\end{tikzcd}$$

Proposition 1.41. [Tay72, Proposition 2.1]

If injections are transferable in the variety V then V has the congruence extension property.

Proof.

Suppose injections are transferable in V. Let $\mathbf{A} \leq \mathbf{B} \in V$, therefore $\mathbf{A} \in V$, and let $\theta \in Con(\mathbf{A})$. Consider the natural homomorphism $\lambda : \mathbf{A} \to \mathbf{A}/\theta$ and the inclusion map $i : \mathbf{A} \to \mathbf{B}$. Because injections are transferable in V, there exist $\mathbf{D} \in V$, a homomorphism g and an embedding ν such that $\nu \circ \lambda = g \circ i$ (as in the diagram).

$$\begin{tikzcd}
\mathbf{A} \arrow[r, "i"] \arrow[d, "\lambda"'] & \mathbf{B} \arrow[d, "g"] \\
\mathbf{A}/\theta \arrow[r, "\nu"'] & \mathbf{D}
\end{tikzcd}$$

Consider $\theta_g = ker(g) \in Con(\mathbf{B})$. We show $\theta = \theta_g|_{\mathbf{A}}$.

For any a_1, a_2, since ν is one-to-one, we have: $(a_1, a_2) \in \theta$ if and only if $a_1, a_2 \in A$ and $\lambda(a_1) = \lambda(a_2)$; if and only if $(a_1, a_2) \in A^2$ and $\nu(\lambda(a_1)) = \nu(\lambda(a_2))$; if and only if $(a_1, a_2) \in A^2$ and $g(a_1) = g(i(a_1)) = g(i(a_2)) = g(a_2)$; if and only if $(a_1, a_2) \in \theta_g|_{\mathbf{A}}$, as required. This shows that V has the congruence extension property.

□

Lemma 1.42. [Tay72]

Every V-injective algebra $\mathbf{B}$ in a variety V is an absolute retract in V.

Proof.

Choose $\mathbf{T} \in V$ such that $\mathbf{B} \leq \mathbf{T}$. Then the identity map $i : \mathbf{B} \to \mathbf{B}$ is a homomorphism and since $\mathbf{B}$ is V-injective, there exists a homomorphism $f : \mathbf{T} \to \mathbf{B}$ extending i, i.e., $f|_{\mathbf{B}} = i$ so $\mathbf{B}$ is an absolute retract in V. □

Lemma 1.43. [Tay72, Lemma 2.2]

Let V be a variety in which injections are transferable. Then $\mathbf{A} \in V$ is V-injective if and only if A is an absolute retract in V.

Proof.

($\Rightarrow$) follows from the previous lemma.

($\Leftarrow$) Let $\mathbf{A}$ be an absolute retract in V. Suppose $\mathbf{B} \leq \mathbf{E} \in V$ and $h : \mathbf{B} \to \mathbf{A}$ is a homomorphism. The inclusion map $i : \mathbf{B} \to \mathbf{E}$ is an embedding, so since injections are transferable in V, there exist $\mathbf{D} \in V$, a homomorphism $g : \mathbf{E} \to \mathbf{D}$ and an embedding $j : \mathbf{A} \to \mathbf{D}$ such that $g \circ i = j \circ h$ (as in diagram).

$$\begin{tikzcd}
\mathbf{B} \arrow[r, "i"] \arrow[d, "h"'] & \mathbf{E} \arrow[d, "g"] \\
\mathbf{A} \arrow[r, "j"'] & \mathbf{D}
\end{tikzcd}$$

Now $\mathbf{A} \cong j[\mathbf{A}] \leq \mathbf{D}$ and $j[\mathbf{A}]$ is an absolute retract in V, since $\mathbf{A}$ is, so there exists a homomorphism $k : \mathbf{D} \to j[\mathbf{A}]$ such that $k|_{j[\mathbf{A}]} = id_{j[A]}$, i.e., $j^{-1} \circ k \circ j = id_A$. Now $f = j^{-1} \circ k \circ g$ is a homomorphism from $\mathbf{E}$ to $\mathbf{A}$. We show $f|_{\mathbf{B}} = h$.

For each $b \in B$, $f(b) = (j^{-1} \circ k \circ g)(b) = (j^{-1} \circ k \circ g \circ i)(b) = (j^{-1} \circ k \circ j \circ h)(b) = (id_A \circ h)(b) = h(b)$, as required. This shows that $\mathbf{A}$ is V-injective.

□

Theorem 1.44. [Tay72, Theorem 2.3]

For any variety V, the following conditions are equivalent:

(i) $\quad$ *V has enough injectives.*

(ii) $\quad$ *V is residually small and injections are transferable in V.*

Proof.

(i)⇒(ii): Suppose V has enough injectives and let $\mathbf{A} \in V$. By assumption, there is a V-injective algebra $\mathbf{E} \in V$ such that $\mathbf{A} \leq \mathbf{E}$. Let $\mathbf{B} \in V$ be an essential extension of $\mathbf{A}$. Since $\mathbf{E}$ is V-injective and the inclusion map $i : \mathbf{A} \to \mathbf{E}$ is a homomorphism and $\mathbf{B} \in V$, there is a homomorphism $h : \mathbf{B} \to \mathbf{E}$ such that $h|_{\mathbf{A}} = i$. Since i is one-to-one and $\mathbf{A}$ is essential in $\mathbf{B}$, it follows that h is one-to-one (by Lemma 1.5). Thus $\mathbf{B} \cong h[\mathbf{B}] \leq \mathbf{E}$. Up to isomorphism, therefore, the class of all essential extensions of $\mathbf{A}$ in V is a set, because it is a subclass of the set of all subalgebras of $\mathbf{E}$. Since $\mathbf{A} \in V$ was arbitrary, it follows from Theorem 1.22 ((ix)⇒(i)) that V is residually small.

Let $\mathbf{B}, \mathbf{C}, \mathbf{T} \in V$ and h a homomorphism from $\mathbf{B}$ to $\mathbf{C}$ and j an embedding from $\mathbf{B}$ to $\mathbf{T}$. $\mathbf{C} \in V$ so, since V has enough injectives, there exists a V-injective algebra $\mathbf{A} \in V$ and an embedding $k : \mathbf{C} \to \mathbf{A}$.

Now $(k \circ h \circ j^{-1}) : j[\mathbf{B}] \to \mathbf{A}$ is a homomorphism and since $\mathbf{A}$ is V-injective, and $j[\mathbf{B}] \leq \mathbf{T}$, there exists a homomorphism $f : \mathbf{T} \to \mathbf{A}$ extending $k \circ h \circ j^{-1}$, i.e., $f|_{j[\mathbf{B}]} = k \circ h \circ j^{-1}$.

Now $f \circ j = f|_{j[\mathbf{B}]} \circ j = k \circ h \circ j^{-1} \circ j = k \circ h$, so

$$\begin{tikzcd}
\mathbf{B} \arrow[r, "j"] \arrow[d, "h"'] & j[\mathbf{B}] \leq \mathbf{T} \arrow[l, bend left, "j^{-1}"] \arrow[d, "f"] \\
\mathbf{C} \arrow[r, "k"'] & \mathbf{A}
\end{tikzcd}$$

injections are transferable in V.

(ii)⇒(i): Suppose V is residually small and injections are transferable in V. By Theorem 1.22, every algebra in V is a subalgebra of some absolute retract in V. By Lemma 1.43, every absolute retract in V is V-injective, so every algebra in V is a subalgebra of some V-injective algebra in V.

□

The condition in (ii) that injections are transferable in V cannot be dropped: see the last example of this chapter.

Definition 1.45. Let V be a variety and $\mathbf{A} \leq \mathbf{B} \in V$. We call $\mathbf{B}$ a *V-injective hull* of $\mathbf{A}$ if $\mathbf{B}$ is both V-injective and an essential extension of $\mathbf{A}$.

Note that if $\mathbf{A} \in V$ has a V-injective hull $\mathbf{B} \in V$ then $\mathbf{B}$ is unique in the sense that whenever $\mathbf{C} \in V$ is an injective hull of $\mathbf{A}$, there is an isomorphism $k : \mathbf{B} \to \mathbf{C}$ such that $k|_{\mathbf{A}} = id_A$. Indeed, by the V-injectivity of $\mathbf{C}$, the inclusion map $i : \mathbf{A} \to \mathbf{C}$ may be extended to a homomorphism $k : \mathbf{B} \to \mathbf{C}$, which must be one-to-one, because $\mathbf{B}$ is an essential extension in $\mathbf{A}$ and $k|_{\mathbf{A}} = i$ is one-to-one.

Theorem 1.46. *Let V be a variety that has enough injectives. Let $\mathbf{A} \leq \mathbf{B} \in V$. The following conditions are equivalent:*

(i) $\mathbf{B}$ *is a V-injective hull of* $\mathbf{A}$.

(ii) $\mathbf{B}$ *is an essential extension of* $\mathbf{A}$ *and no proper extension of* $\mathbf{B}$ *in V is an essential extension of* $\mathbf{A}$.

(iii) $\mathbf{B}$ *is V-injective and no proper subalgebra of* $\mathbf{B}$ *is both V-injective and an extension of* $\mathbf{A}$.

Proof.

(i)$\Rightarrow$(ii): Since $\mathbf{B}$ is V-injective, it is an absolute retract in V (by Lemma 1.42). Since $\mathbf{B}$ is an essential extension of $\mathbf{A}$, (ii) follows from Lemma 1.13.

(ii)$\Rightarrow$(iii): By Lemma 1.13, $\mathbf{B}$ is an absolute retract in V. Since injections are transferable in V (by Theorem 1.44), $\mathbf{B}$ is V-injective (by Lemma 1.43) and V has the congruence extension property (by Proposition 1.41). Suppose $\mathbf{A} \leq \mathbf{C} \leq \mathbf{B}$ and $\mathbf{C}$ is V-injective. If $id_C \neq \theta \in Con(\mathbf{C})$ then there exists $\varphi \in Con(\mathbf{B})$ such that $\theta = \varphi|_{\mathbf{C}}$, so $\varphi \neq id_B$. Since $\mathbf{A}$ is essential in $\mathbf{B}$, $id_A \neq \varphi|_{\mathbf{A}} \subseteq (\varphi|_{\mathbf{C}})|_{\mathbf{A}} = \theta|_{\mathbf{A}}$, so $\mathbf{C}$ is an essential extension of $\mathbf{A}$. Then by Lemma 1.13, $\mathbf{C} = \mathbf{B}$.

(iii)$\Rightarrow$(i): By Theorem 1.44, V is residually small, so by Theorem 1.22 (ix), $\mathbf{A}$ has, up to isomorphism, only a set of essential extensions in V. By Corollary 1.14, some essential extension $\mathbf{D} \in V$ of $\mathbf{A}$ is an absolute retract in V. By Lemma 1.43, $\mathbf{D}$ is V-injective. Since $\mathbf{B}$ is V-injective, the inclusion map $i : \mathbf{A} \to \mathbf{B}$ may be extended to a homomorphism $f : \mathbf{D} \to \mathbf{B}$. Now f is one-to-one, because $\mathbf{A}$ is essential in $\mathbf{D}$ and $f|_{\mathbf{A}} = i$ is one-to-one. Thus $\mathbf{A} = f[\mathbf{A}] \leq f[\mathbf{D}] \leq \mathbf{B}$ and $\mathbf{D} \cong f[\mathbf{D}]$, so $f[\mathbf{D}]$ is V-injective. By assumption, therefore, $\mathbf{B} = f[\mathbf{D}]$, which is an essential extension of $f[\mathbf{A}] = \mathbf{A}$.

□

Theorem 1.47. *Let V be a variety that has enough injectives. Then every algebra in V has an injective hull in V.*

Proof.

Let $\mathbf{A} \in V$. Exactly as in the proof of (iii)$\Rightarrow$(i) above, some essential extension $\mathbf{D}$ of $\mathbf{A}$ in V is V-injective, i.e., $\mathbf{D}$ is a V-injective hull of $\mathbf{A}$. □

Corollary 1.48. *Let $\mathbf{A} \leq \mathbf{B} \in V$, where V is a variety and $\mathbf{A}$ is subdirectly irreducible. If $\mathbf{B}$ is a V-injective hull of $\mathbf{A}$ then $\mathbf{B}$ is a V-maximal irreducible algebra. If V has enough injectives, and $a, b \in A$ and $\mathbf{B}$ is maximal among the (a, b)-irreducible algebras in V then $\mathbf{B}$ is an injective hull of $\mathbf{A}$.*

Proof.

There exist distinct $a, b \in A$ such that $\mathbf{A}$ is (a, b)-irreducible. If $\mathbf{B}$ is an injective hull of $\mathbf{A}$ then $\mathbf{A}$ is essential in $\mathbf{B}$, so $\mathbf{B}$ is also (a, b)-irreducible, by Lemma 1.8, and $\mathbf{B}$ is an absolute retract in V (since it is V-injective). By Proposition 1.34, $\mathbf{B}$ is a V-maximal irreducible algebra.

Now suppose that V has enough injectives and that $\mathbf{B}$ is maximal among (a, b)-irreducible algebras in V, where $a, b \in A$. Let $\mathbf{E} \in V$ be a V-injective hull of $\mathbf{B}$. Then $\mathbf{E}$ is (a,b)-irreducible (by Lemma 1.8), so $\mathbf{B} = \mathbf{E}$, by assumption, and $\mathbf{B}$ is an essential extension of $\mathbf{A}$, by Lemma 1.7.

□

Theorem 1.49. [Tay72, Theorem 2.10]

Let V be a variety of algebras of type $\mathcal{T} = \langle \mathsf{F}, ar \rangle$. If $\mathbf{B}$ is the V-injective hull of $\mathbf{A} \in V$, then $|B| \leq 2^{\mathsf{n}+|A|}$ where $\mathsf{n} = \aleph_0 + |\mathsf{F}|$.

Proof.

Suppose $|B| > 2^{\mathsf{n}+|A|}$. Since $\mathbf{B}$ is an essential extension of $\mathbf{A}$, it follows from Corollary 1.11 that there exist distinct $a, b \in A$ and a positive formula $\Phi(\cdot,\cdot,\cdot,\cdot)$ such that $\vdash_{Th(\mathcal{T})} \forall y \forall z[(\exists x\, \Phi(x,x,y,z)) \rightarrow y \approx z]$. ....(†)

and $D(\mathbf{A}) \cup Id(\mathbf{B}) \cup \{\Phi(x_i, x_i, a, b) : i < j < \omega\}$ is satisfiable, where $D(\mathbf{A})$ and $Id(\mathbf{B})$ are as for Corollary 1.11.

Therefore every finite subset of $D(\mathbf{A}) \cup Id(\mathbf{B}) \cup \{\Phi(x_\alpha, x_\beta, a, b) : \alpha < \beta < |B|^+\}$ is satisfiable. By the Compactness Theorem (Theorem 0.43),
$D(\mathbf{A}) \cup Id(\mathbf{B}) \cup \{\Phi(x_\alpha, x_\beta, a, b) : \alpha < \beta < |B|^+\}$ is satisfiable.

Let $\mathbf{C}$ be a $\mathcal{T}$-algebra in which $D(\mathbf{A}) \cup Id(\mathbf{B}) \cup \{\Phi(x_\alpha, x_\beta, a, b) : \alpha < \beta < |B|^+\}$ is satisfiable. Then $\mathbf{A}$ is embeddable in $\mathbf{C}$ (because $D(\mathbf{A})$ includes the definition of $f^{\mathbf{A}}(a_1, \ldots, a_{ar(f)})$ for all operation symbols f of the language and all $a_1, \ldots, a_{ar(f)} \in A$). We assume without loss of generality that $\mathbf{A} \leq \mathbf{C}$. In addition there is a set $\{c_\alpha : \alpha < |B|^+\}$ of elements of C such that $\mathbf{C} \models \Phi[c_\alpha, c_\beta, a, b]$ for all $\alpha, \beta < |B|^+$ with $\alpha < \beta$.

By Zorn's Lemma there exists a congruence θ on $\mathbf{C}$ that is $\subseteq$-maximal such that $\theta|_{\mathbf{A}} = id_A$.

Consider the map $\lambda : \mathbf{A} \rightarrow \mathbf{C}/\theta$ defined by $a \mapsto a/\theta$. Since λ is a homomorphism, and $ker(\lambda) = \theta|_{\mathbf{A}} = id_A$, λ is one-to-one. Therefore λ is an embedding of $\mathbf{A}$ into $\mathbf{C}/\theta$. We show $\mathbf{C}/\theta$ is an essential extension of $\lambda[\mathbf{A}]$ (the range of λ). Let $id_{C/\theta} \neq \eta \in Con(\mathbf{C}/\theta)$. We show $\eta|_{\lambda[\mathbf{A}]} \neq id_{\lambda[A]}$.

Suppose $\eta|_{\lambda[\mathbf{A}]} = id_{\lambda[A]}$. η has the form φ/θ where $\theta \subset \varphi$, $\varphi \in Con(\mathbf{C})$. Clearly, $\varphi|_{\mathbf{A}} = id_A$, contradicting the maximality of θ, so $\eta|_{\lambda[\mathbf{A}]} \neq id_{\lambda[A]}$.

Since each $\Phi[c_\alpha, c_\beta, a, b]$ is a positive sentence, $\mathbf{C}/\theta \models \Phi[c_\alpha/\theta, c_\beta/\theta, a/\theta, b/\theta]$. Since $a/\theta \neq b/\theta$ it follows from (†) that $c_\alpha/\theta \neq c_\beta/\theta$ for all $\alpha < \beta$. Thus $|\{c_\alpha/\theta : \alpha < |B|^+\}| = |B|^+$, so $|C/\theta| > |B|$.

Since $\mathbf{B}$ is injective, the inclusion map $i : \mathbf{A} \rightarrow \mathbf{B}$ extends to some homomorphism $\psi : \mathbf{C}/\theta \rightarrow \mathbf{B}$. (See the following diagram.) Since $\mathbf{C}/\theta$ is an essential extension of $\mathbf{A}$, and $\psi|_{\mathbf{A}} = i$ is one-to-one, ψ is one-to-one. Then $|C/\theta| \leq |B|$, a contradiction. Thus, $|B| \leq 2^{\mathsf{n}+|A|}$.

$$\begin{tikzcd}
\mathbf{A} \arrow[r, "\lambda"] \arrow[dr, "i"'] & \mathbf{C}/\theta \arrow[d, "\psi"] \\
& \mathbf{B}
\end{tikzcd}$$

□

Note that in the above result, V is not assumed to be residually small. (For residually small V, the result follows from Theorem 1.22 ((i)⇒(viii)).)

1.4.2 Classical Examples We conclude by interpreting the above results in a classical setting. Recall that an algebra $\mathbf{A}$ is called *simple* if $|Con(\mathbf{A})| = 2$.

R-modules.

Let $\mathbf{R}$ be a ring with identity and V the variety of all unital right $\mathbf{R}-$modules. By a well-known construction of module theory, every $\mathbf{M} \in V$ has an injective hull $E(\mathbf{M})$ ([Lam66, Propositions 9, 10, pp91-92]). By Theorem 1.44 and Proposition 1.41, V has the CEP (which is also easy to verify directly).

By Theorem 1.22, V is also residually small. Here is a more direct explanation of this fact. The map $\theta \mapsto 0/\theta$ from $\mathbf{Con}(\mathbf{M})$ to the subalgebra (i.e., submodule) lattice of $\mathbf{M}$ is a lattice isomorphism, whose inverse is $N \mapsto \{(m_1, m_2) \in M \times M : m_1 - m_2 \in N\}$, for any $\mathbf{M} \in V$. Consequently a module $\mathbf{M} \in V$ is subdirectly irreducible if and only if it has a smallest nonzero submodule $\mathbf{K}$. In this case, by the CEP, $\mathbf{K}$ is itself a simple module, so $K = xR$ for some $x \in K$ and $\mathbf{K} \cong \mathbf{R}/A$ where $A = \{x \in R : xr = 0\}$ is a maximal right ideal of $\mathbf{R}$. Now $\mathbf{M}$ is an essential extension of $\mathbf{K}$, so $\mathbf{M}$ embeds into $E(\mathbf{K})$. Since $\mathbf{R}$ has only a set of (maximal) right ideals $\mathbf{A}$ and for each such $\mathbf{A}$, $E(\mathbf{R}/A)$ has only a set of submodules, it follows that, up to isomorphism, there is only a *set*, namely, $\{\mathrm{N} : \mathbf{R}/A \leq \mathrm{N} \leq E(\mathbf{R}/A)$ for some maximal right ideal $\mathbf{A}$ of $\mathbf{R}\}$ of subdirectly irreducible $\mathbf{R}-$modules $\mathbf{M}$, i.e. V is residually small. In fact, by Theorem 1.49, V is residually $< (2^{\mathsf{k}})^+$ where $\mathsf{k} = max\{\aleph_0, |R|\}$.

Abelian Groups.

It is well known that an Abelian group $\mathbf{G}$ is *simple* if and only if $\mathbf{G} \cong \mathbb{Z}_p$ for some prime p. (Indeed, such a $\mathbf{G}$ must be cyclic, and the group $\mathbb{Z}$ is not simple and neither is $\mathbb{Z}_m$, unless m is prime.)

An Abelian group is essentially the same thing as (more precisely, it is *"termwise equivalent"* to) a $\mathbb{Z}$-module. By the preceding discussion, therefore, the variety of Abelian groups is residually small and an Abelian group is subdirectly irreducible if and only if it has a smallest nonzero subgroup, which shows that the groups $\mathbb{Z}_{p^n}$, p prime, $n \in \mathbb{N} \cup \{\infty\}$ are subdirectly irreducible: in each of these cases, the smallest nonzero subgroup is isomorphic to $\mathbb{Z}_p$.

It is also well known that a $\mathbb{Z}$-module $\mathbf{A}$ is injective exactly when it is *divisible* (by [Lam66, Proposition3, p89]), i.e., for each $a \in A$ and each $n \in \mathbb{Z}$, there exists $x \in A$ such that $nx = a$. This makes it easier to see that $\mathbb{Z}_{p^\infty}$ is injective, for any prime p. It is also an essential extension of its smallest subgroup $K = \{0, 1/p, 2/p, \dots, p-1/p\} (\cong \mathbb{Z}_p)$. Therefore $\mathbb{Z}_{p^\infty} \cong E(\mathbf{K})$ and any nonzero $\mathbb{Z}$-submodule (i.e., subgroup) of $\mathbb{Z}_{p^\infty}$ is isomorphic to $\mathbb{Z}_{p^n}$ for some $n \in \mathbb{N}$.

Thus, by the discussion on modules above, the subdirectly irreducible Abelian groups are, up to isomorphism, just the groups $\mathbb{Z}_{p^n}$, where p is prime and $n \in \mathbb{N} \cup \{\infty\}$, so the variety of Abelian groups is residually small, in fact, residually $< \aleph_1$.

Example 1.50.

We show that a residually small (in fact, a residually finitely bounded) variety need not have enough injectives, so the condition that injections be transferable cannot be dropped from Theorem 1.44. The example is due to Banaschewski [Ban70].

Recall first that a finite field must have just p^n elements for some $p, n \in \mathbb{N}$ with p prime, and that, up to isomorphism, there is exactly one such field, $\mathbf{GF}(p^n)$, for each prime p and $n \in \mathbb{N}$. Recall also that if $\mathbf{F}$ is a finite field then $\mathbf{F}^* = \langle F \setminus \{0\}; \cdot, ^{-1}, 1\rangle$ is a cyclic group.

Let V be the variety of all the commutative rings with identity $\mathbf{R} = \langle R; +, -, \cdot, 0, 1\rangle$ satisfying $x^{22} \approx x$. Every ring $\mathbf{R} \in V$ is "strongly regular" (i.e., for each $x \in R$, there exists $y \in R$ with $x^2 y = x$) so, by a classical result of ring theory ([Lam66, Corollary 1, p30] and [Lam66, Proposition 4, p33]) $\mathbf{R}$ is a subdirect product of fields, i.e., the subdirectly irreducible algebras in V are exactly the fields in V.

Let $\mathbf{F} \in V$ be a field. Since every element of F is a zero of the polynomial $x^{22} - x \in F[x]$, $|F| \leq 22$ and $\mathbf{F}^* \models x^{21} \approx 1$. Since $\mathbf{F}^*$ is cyclic, the order of any generator a of $\mathbf{F}^*$ divides 21 (by Lagrange's Theorem), i.e., a has order 1 or 3 or 7. Thus, $\mathbf{F}$ is isomorphic to $\mathbf{GF}(2)$ or $\mathbf{GF}(4)$ or $\mathbf{GF}(8)$, so these three fields are, up to isomorphism, the subdirectly irreducible members of V, and so V is residually small, indeed, its residual bound is 9. Recall that $\mathbf{GF}(2)$ is a subfield both of $\mathbf{GF}(4)$ and of $\mathbf{GF}(8)$ but that $\mathbf{GF}(8)$ has no subfield $\mathbf{F}$ of order 4 (otherwise $\mathbf{F}^*$ is a subgroup of $\mathbf{GF}(8)^*$, but their respective orders are 3 and 7, contradicting Lagrange's theorem). In particular, there is no ring embedding of $\mathbf{GF}(4)$ into $\mathbf{GF}(8)$.

Now $\mathbf{GF}(8)$ is a V-maximal irreducible algebra; it is an absolute retract in V by Proposition 1.34. If injections were transferable in V, it would follow from Lemma 1.43 that $\mathbf{GF}(8)$ is V-injective. In this case the inclusion map $\mathbf{GF}(2) \to \mathbf{GF}(8)$ would extend to a ring homomorphism from $\mathbf{GF}(4)$ to $\mathbf{GF}(8)$, which is one-to-one because, as a ring, $\mathbf{GF}(4)$ has no nontrivial congruence relations. From this contradiction, we infer that injections are not transferable in V and, by Theorem 1.44, V does not have enough injectives.

Chapter 2

Commutator Theory in Modular Varieties

The general commutator theory was first developed for congruence permutable varieties by J.D.H. Smith [Smi76]. It was fully developed for congruence modular varieties by J. Hagemann and C. Herrmann [HH79] and was extended by several authors, including H.-P. Gumm, R. Freese, R. McKenzie and W. Taylor [Tay82]. In this chapter we trace aspects of the development of the commutator theory (as expounded by Freese and McKenzie in [FM87]) that are relevant to the main result of the thesis, Theorem 4.11. This theorem, which is due to Freese and McKenzie [FM81] says that if a finitely generated congruence modular variety is residually small, then it has a finite residual bound. The first section of this chapter includes a definition and some important properties of the commutator.[13] The first results discussed say that a congruence modular variety is characterized by the existence of *"Day terms"*, i.e., terms (discovered by A. Day [Day69]) satisfying the conditions of Theorem 2.1, and by the conditions of the *"Shifting Lemma"* of Gumm [Gum80a]. The proofs of these results are combined in the proof of Theorem 2.3. These results will be applied when we consider the properties of the commutator in congruence modular varieties. In the rest of the thesis, we will abbreviate *congruence modular* to *modular.*

[13] Regarding references: the book [FM87] grew out of a set of notes by Freese and McKenzie called "The commutator: an overview", which was widely circulated by 1982 but is no longer an accessible source. Usually, where results are attributed here to [FM87], it should be understood that they were proved considerably earlier in the given form, by Freese and McKenzie. Other forms of several of these results, proceeding from different definitions, would have been known to many of the aforementioned other researchers also but, since the equivalence of definitions is not obvious, we have usually accredited [FM87] in this situation. We have stuck largely to the approach of Freese and McKenzie here because it is more purely algebraic than any of the others.

2.1 Congruence Modular Varieties.

Theorem 2.1. [Day69]

A variety V is modular if and only if for some $n \in \omega$ there are terms (called "Day terms"), $m_0(x,y,z,u), \ldots, m_n(x,y,z,u)$ such that V satisfies:

(i) $m_0(x,y,z,u) \approx x,\ m_n(x,y,z,u) \approx u;$

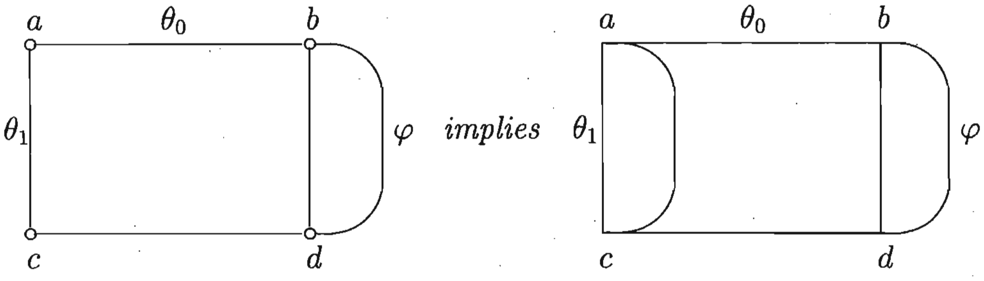
(ii) $m_i(x,y,y,x) \approx x,\ i \leq n;$

(iii) $m_i(x,x,y,y) \approx m_{i+1}(x,x,y,y)$ *for all even* $i < n;$

(iv) $m_i(x,y,y,z) \approx m_{i+1}(x,y,y,z)$ *for all odd* $i < n.$

Lemma 2.2. (The Shifting Lemma). [Gum80a]

Let V be a modular variety and let $\mathbf{A} \in V$ and $\varphi, \theta_0, \theta_1 \in Con(\mathbf{A})$. Suppose that $a,b,c,d \in A$, $(a,b),(c,d) \in \theta_0$, $(a,c),(b,d) \in \theta_1$ and $\theta_0 \cap \theta_1 \subseteq \varphi$. Then $(b,d) \in \varphi$ implies $(a,c) \in \varphi$. Diagramatically,



Note that the diagram above is interpreted in the following manner: whenever the line (or curve) joining the elements a and c (for example) is parallel to the line (or curve) joining the elements b and d, and one of the lines is labelled φ (in this case), then $(a,c),(b,d) \in \varphi$.

Theorem 2.3. *For a variety V the following are equivalent:*

(i) *V is modular.*

(ii) *V has Day terms satisfying (i) to (iv) of Theorem 2.1.*

(iii) *V has terms $m_i(x,y,z,u)$, $i = 0,\ldots,n$, satisfying $m_i(x,y,y,x) \approx x$ ($i \leq n$), such that if $\mathbf{A} \in V$, $\gamma \in Con(\mathbf{A})$, $a,b,c,d \in A$ with $(b,d) \in \gamma$, then $(a,c) \in \gamma$ if and only if for all $i \leq n$, $m_i(a,a,c,c)\gamma\, m_i(a,b,d,c)$.*

(iv) *V satisfies the conditions of the Shifting Lemma, i.e., if $\mathbf{A} \in V$, $a,b,c,d \in A$, and $\varphi, \theta_0, \theta_1 \in Con(\mathbf{A})$ with $\theta_0 \cap \theta_1 \subseteq \varphi$, $(a,b),(c,d) \in \theta_0$, $(a,c),(b,d) \in \theta_1$ then $(b,d) \in \varphi$ implies $(a,c) \in \varphi$.*

Proof.

First, we replace (iv) with (iv)$'$, a statement identical to (iv), except that in (iv)$'$, θ_0 is merely a semicongruence, i.e., a reflexive, compatible relation. The proof proceeds as follows:

(i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv)$'$ $\Rightarrow$ (i).

Clearly, (iv)$'$ implies (iv) since congruences are semicongruences. We end the proof by showing that (iv) implies modularity, and is therefore equivalent to the other conditions.

(i)$\Rightarrow$(ii): Assume V is modular. Let $\mathbf{F} = \mathbf{F}_V(\bar{x}, \bar{y}, \bar{z}, \bar{u})$ be the V-free algebra on four free generators. Define:

$$\begin{aligned} \alpha &= \Theta^{\mathbf{F}}(\bar{x}, \bar{u}) \vee \Theta^{\mathbf{F}}(\bar{y}, \bar{z}), \\ \beta &= \Theta^{\mathbf{F}}(\bar{x}, \bar{y}) \vee \Theta^{\mathbf{F}}(\bar{z}, \bar{u}), \\ \gamma &= \Theta^{\mathbf{F}}(\bar{y}, \bar{z}). \end{aligned}$$

We show, firstly, that $(\bar{x}, \bar{u}) \in \alpha \cap (\beta \vee \gamma)$.

$(\bar{x}, \bar{u}) \in \Theta^{\mathbf{F}}(\bar{x}, \bar{u})$ so $(\bar{x}, \bar{u}) \in \Theta^{\mathbf{F}}(\bar{x}, \bar{u}) \vee \Theta^{\mathbf{F}}(\bar{y}, \bar{z}) = \alpha$. $(\bar{y}, \bar{z}) \in \gamma$ and $(\bar{z}, \bar{u}) \in \beta$ so $(\bar{y}, \bar{u}) \in \beta \circ \gamma \subseteq \beta \vee \gamma$. Also $(\bar{x}, \bar{y}) \in \beta$ so $(\bar{x}, \bar{y}) \in \beta \vee \gamma$ so we have $(\bar{x}, \bar{y})$, $(\bar{y}, \bar{u}) \in \beta \vee \gamma$, therefore $(\bar{x}, \bar{u}) \in \beta \vee \gamma$, by transitivity, so $(\bar{x}, \bar{u}) \in \alpha \cap (\beta \vee \gamma)$.

Since V is a variety, $\mathbf{F} \in V$ so $\mathbf{F}$ is modular and $\gamma \subseteq \alpha$ so $(\bar{x}, \bar{u}) \in \gamma \vee (\alpha \cap \beta)$ by the Modular Law. This means for some $n \in \omega$ there are elements $\bar{x} = \bar{w}_0, \bar{w}_1, \ldots, \bar{w}_n = \bar{u}$ of $F_V(\bar{x}, \bar{y}, \bar{z}, \bar{u})$ such that $(\bar{w}_i, \bar{w}_{i+1}) \in \alpha \cap \beta$ if i is even and $(\bar{w}_i, \bar{w}_{i+1}) \in \gamma$ if i is odd, $i \leq n$. By Theorem 0.8, this implies $(\bar{w}_0, \bar{w}_1) \in \alpha$, and $(\bar{w}_1, \bar{w}_2) \in \gamma \subseteq \alpha$ so $(\bar{w}_0, \bar{w}_2) \in \alpha$ by transitivity. Continuing in this way we have $(\bar{w}_0, \bar{w}_i) \in \alpha$ for each $i \leq n$. ....(1)

Consider $\bar{x} = m_0^{\mathbf{F}}(\bar{x}, \bar{y}, \bar{z}, \bar{u}), m_1^{\mathbf{F}}(\bar{x}, \bar{y}, \bar{z}, \bar{u}), \ldots, m_n^{\mathbf{F}}(\bar{x}, \bar{y}, \bar{z}, \bar{u}) = \bar{u}$, where $m_0, m_1, \ldots, m_n$ are terms in the term algebra $\mathbf{T}(x, y, z, u)$ representing $\bar{w}_0, \bar{w}_1, \ldots, \bar{w}_n$. Then by Theorem 0.50 ((iii)$\Rightarrow$(i)), we have $V \models m_0(x, y, z, u) \approx x$ and $V \models m_n(x, y, z, u) \approx u$. By (1), $(m_0^{\mathbf{F}}(\bar{x}, \bar{y}, \bar{z}, \bar{u}), m_i^{\mathbf{F}}(\bar{x}, \bar{y}, \bar{z}, \bar{u})) \in \alpha = \Theta^{\mathbf{F}}(\bar{x}, \bar{u}) \vee \Theta^{\mathbf{F}}(\bar{y}, \bar{z})$ for $i \leq n$, so $V \models x \approx m_i(x, y, y, x)$ by Theorem 0.53 (since α identifies $\bar{x}$ with $\bar{u}$ and $\bar{y}$ with $\bar{z}$).

We show V satisfies $m_i(x, x, y, y) \approx m_{i+1}(x, x, y, y)$ for all even $i < n$ and $m_i(x, y, y, z) \approx m_{i+1}(x, y, y, z)$ for all odd $i < n$.

Now $(\bar{w}_i, \bar{w}_{i+1}) \in \alpha \cap \beta$ if i is even, i.e., $(m_i^{\mathbf{F}}(\bar{x}, \bar{y}, \bar{z}, \bar{u}), m_{i+1}^{\mathbf{F}}(\bar{x}, \bar{y}, \bar{z}, \bar{u})) \in (\Theta^{\mathbf{F}}(\bar{x}, \bar{u}) \vee \Theta^{\mathbf{F}}(\bar{y}, \bar{z})) \cap (\Theta^{\mathbf{F}}(\bar{x}, \bar{y}) \vee \Theta^{\mathbf{F}}(\bar{z}, \bar{u}))$. Therefore $V \models m_i(x, x, y, y) \approx m_{i+1}(x, x, y, y)$ for all even $i < n$ by Theorem 0.53 (since $\alpha \cap \beta$ identifies $\bar{x}$ with $\bar{y}$ and $\bar{z}$ and $\bar{u}$). Also $(\bar{w}_i, \bar{w}_{i+1}) \in \gamma$ if i is odd, i.e., $(m_i^{\mathbf{F}}(\bar{x}, \bar{y}, \bar{z}, \bar{u}), m_{i+1}^{\mathbf{F}}(\bar{x}, \bar{y}, \bar{z}, \bar{u})) \in \Theta^{\mathbf{F}}(\bar{y}, \bar{z})$ so by Theorem 0.53, $V \models m_i(x, y, y, z) \approx m_{i+1}(x, y, y, z)$ for all odd

$i < n$ (since γ identifies $\bar{y}$ and $\bar{z}$ and we can rename u).

(ii)$\Rightarrow$(iii): Suppose V has Day terms $m_0(x,y,z,u),\ldots,m_n(x,y,z,u)$ as in Theorem 2.1 and let $\mathbf{A} \in V$, $\gamma \in Con(\mathbf{A})$ and $a,b,c,d \in A$ with $b\gamma d$.

Assume $a\gamma c$. Then $(a,a),(c,a) \in \gamma$ so $m_i^{\mathbf{A}}(a,a,c,c)\gamma m_i^{\mathbf{A}}(a,a,a,a) = a$ for all $i \leq n$ and $(a,a),(b,b),(d,b),(c,a) \in \gamma$ so $m_i^{\mathbf{A}}(a,b,d,c)\gamma m_i^{\mathbf{A}}(a,b,b,a) = a$ for all $i \leq n$. Thus, by symmetry and transitivity $m_i^{\mathbf{A}}(a,a,c,c)\gamma m_i^{\mathbf{A}}(a,b,d,c)$ for all $i \leq n$.

Conversely, assume $m_i^{\mathbf{A}}(a,a,c,c)\gamma m_i^{\mathbf{A}}(a,b,d,c)$ for all $i \leq n$. We show $a\gamma c$. Let $u_i = m_i^{\mathbf{A}}(a,b,d,c), v_i = m_i^{\mathbf{A}}(a,a,c,c)$, so $u_i\gamma v_i$ for all $i \leq n$. .... (2)

Now $m_i^{\mathbf{A}}(a,b,d,c)\gamma m_i^{\mathbf{A}}(a,a,c,c) = m_{i+1}^{\mathbf{A}}(a,a,c,c)$ for all even $i < n$ by Theorem 2.1 (iii). Also $m_{i+1}^{\mathbf{A}}(a,b,d,c)\gamma m_{i+1}^{\mathbf{A}}(a,a,c,c)$ for all $i \leq n$, by (2), so $m_i^{\mathbf{A}}(a,b,d,c)\gamma m_{i+1}^{\mathbf{A}}(a,b,d,c)$ for all even $i < n$ by transitivity, i.e., $u_i\gamma u_{i+1}$ for all even $i < n$. .... (3)

We have $(a,a),(b,b),(d,b),(c,c) \in \gamma$ so $m_i^{\mathbf{A}}(a,b,d,c)\gamma m_i^{\mathbf{A}}(a,b,b,c)$ for all $i \leq n$ .... (4)

and $m_i^{\mathbf{A}}(a,b,b,c) = m_{i+1}^{\mathbf{A}}(a,b,b,c)$ for all odd $i < n$, by Theorem 2.1 (iv). Also $m_{i+1}^{\mathbf{A}}(a,b,b,c)\gamma m_{i+1}^{\mathbf{A}}(a,b,d,c)$ for all $i < n$ by (4) so $m_i^{\mathbf{A}}(a,b,d,c)\gamma m_{i+1}^{\mathbf{A}}(a,b,d,c)$ for all odd $i < n$, by transitivity, i.e., $u_i\gamma u_{i+1}$ for all odd $i < n$ .... (5)

From (3) and (5), $u_i\gamma u_{i+1}$ for all $i < n$ so, by transitivity, $u_0\gamma u_n$, i.e., $m_0^{\mathbf{A}}(a,b,d,c)\gamma m_n^{\mathbf{A}}(a,b,d,c)$ but $m_0^{\mathbf{A}}(a,b,d,c) = a$ and $m_n^{\mathbf{A}}(a,b,d,c) = c$ by Theorem 2.1 (i), so $a\gamma c$.

(iii)$\Rightarrow$(iv)$'$: Assume V is a variety satisfying (iii) and that the conditions implied by the left hand side diagram of Lemma 2.2 hold in an algebra $\mathbf{A} \in V$ where θ_1 and φ are congruences on $\mathbf{A}$ and θ_0 is a semicongruence, and $\theta_0 \cap \theta_1 \subseteq \varphi$. We show $(a,c) \in \varphi$.

We have $(a,a),(a,b),(c,d),(c,c) \in \theta_0$ and so $m_i^{\mathbf{A}}(a,a,c,c)\theta_0 m_i^{\mathbf{A}}(a,b,d,c)$ for any $i \leq n$, by reflexivity and compatibility of θ_0. .... (6)

We have $(a,c) \in \theta_1$ so $(a,a),(c,a) \in \theta_1$ so $m_i^{\mathbf{A}}(a,a,c,c)\theta_1 m_i^{\mathbf{A}}(a,a,a,a) = a$ for all $i \leq n$ by Theorem 2.1 (ii). .... (7)

Also $(b,d) \in \theta_1$ so $(a,a),(b,b),(b,d),(a,c) \in \theta_1$ so $a = m_i^{\mathbf{A}}(a,b,b,a)\theta_1 m_i^{\mathbf{A}}(a,b,d,c)$ for all $i \leq n$. .... (8)

By (7), (8) and transitivity, $m_i^{\mathbf{A}}(a,a,c,c)\theta_1 m_i^{\mathbf{A}}(a,b,d,c)$ for all $i \leq n$. ... (9)

From (6) and (9), $m_i^{\mathbf{A}}(a,a,c,c)(\theta_0 \cap \theta_1) m_i^{\mathbf{A}}(a,b,d,c)$ for all $i \leq n$. Now $\theta_0 \cap \theta_1 \subseteq \varphi$ so $m_i^{\mathbf{A}}(a,a,c,c)\varphi m_i^{\mathbf{A}}(a,b,d,c)$ for all $i \leq n$ and $(b,d) \in \varphi$ so

$(a, c) \in \varphi$, by (iii) (with $\gamma = \varphi$).

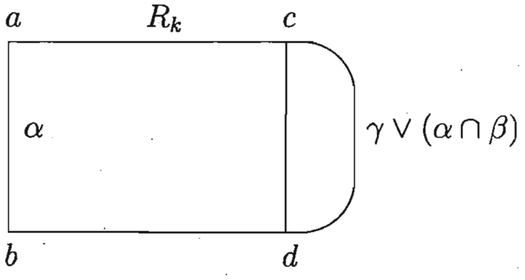
(iv)$'$ $\Rightarrow$ (i): Suppose V satisfies (iv)$'$ and that $\mathbf{A} \in V$ and $\alpha, \beta, \gamma \in Con(\mathbf{A})$ with $\gamma \subseteq \alpha$. We need to show that $\alpha \cap (\beta \vee \gamma) = \gamma \vee (\alpha \cap \beta)$.

We first show $\alpha \cap (\beta \vee \gamma) \subseteq \bigcup_{n<\omega}(\alpha \cap R_n)$ where $R_0 = \beta$, $R_{k+1} = R_k \circ \gamma \circ \beta$ for $k \in \omega$. Note that each R_k is a semicongruence. Let $(a, b) \in \alpha \cap (\beta \vee \gamma)$. Then $(a, b) \in \alpha$ and there exist $c_1, \ldots, c_m$ with $c_1 = a, c_m = b$ and $c_i \beta c_{i+1}$ or $c_i \gamma c_{i+1}$ for all $i < m$. For some k large enough, $(a, b) \in R_{k+1}$, therefore $(a, b) \in \alpha \cap R_{k+1}$, so $(a, b) \in \bigcup_{n<\omega}(\alpha \cap R_n)$.

We show (by induction) that $\bigcup_{n<\omega}(\alpha \cap R_n) \subseteq \gamma \vee (\alpha \cap \beta)$, since then $\alpha \cap (\beta \vee \gamma) \subseteq \gamma \vee (\alpha \cap \beta)$, and equality will follow since $\gamma \subseteq \alpha$ implies $\gamma \vee (\alpha \cap \beta) \subseteq \alpha \cap (\beta \vee \gamma)$ (in every lattice, therefore in $\mathbf{Con(A)}$).

Now $\alpha \cap R_0 = (\alpha \cap \beta) \subseteq \gamma \vee (\alpha \cap \beta)$, so the statement is true for $n = 0$. Assume $\alpha \cap R_k \subseteq \gamma \vee (\alpha \cap \beta)$, where $k \in \omega$. Let $(a, b) \in \alpha \cap R_{k+1} = \alpha \cap (R_k \circ \gamma \circ \beta)$. Then $(a, b) \in \alpha$ and $(a, b) \in R_k \circ \gamma \circ \beta$ which means there exist $c, d \in A$ with $(a, c) \in R_k, (c, d) \in \gamma$ and $(d, b) \in \beta$. Therefore $(b, d) \in \beta$ but $\beta \subseteq R_k$ and so $(b, d) \in R_k$ and $(c, d) \in \gamma \vee (\alpha \cap \beta)$ since $\gamma \subseteq \gamma \vee (\alpha \cap \beta)$.

Diagramatically:

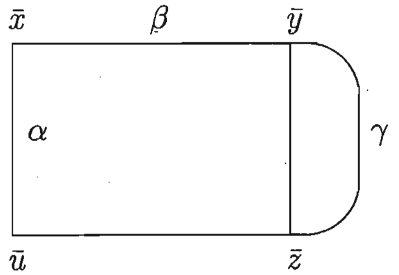


By (iv)$'$ with $\theta_0 = R_k, \theta_1 = \alpha$ and $\varphi = \gamma \vee (\alpha \cap \beta)$, since $\alpha \cap R_k \subseteq \gamma \vee (\alpha \cap \beta)$ (by the induction hypothesis) we have $(a, b) \in \gamma \vee (\alpha \cap \beta)$, as required.

Finally, we show (iv) implies modularity. Assume (iv) holds in the variety V. Let $\mathbf{F}_V(\bar{x}, \bar{y}, \bar{z}, \bar{u})$ be the free V-algebra on four generators and let

$$\begin{aligned} \alpha &= \Theta^{\mathbf{F}}(\bar{x}, \bar{u}) \vee \Theta^{\mathbf{F}}(\bar{y}, \bar{z}), \\ \beta &= \Theta^{\mathbf{F}}(\bar{x}, \bar{y}) \vee \Theta^{\mathbf{F}}(\bar{z}, \bar{u}), \\ \gamma &= \Theta^{\mathbf{F}}(\bar{y}, \bar{z}). \end{aligned}$$

Now $(\bar{x}, \bar{u}) \in \alpha \cap (\beta \vee \gamma)$ as in the proof of (i)$\Rightarrow$(ii). We also have $\bar{x} \alpha \bar{u}, \bar{y} \alpha \bar{z}, \bar{x} \beta \bar{y}$, $\bar{z} \beta \bar{u}$ and $\bar{y} \gamma \bar{z}$ so $(\bar{y}, \bar{z}) \in \gamma \vee (\alpha \cap \beta)$ and the diagram below holds:



By (iv), with $\alpha = \theta_0, \beta = \theta_1, \varphi = \gamma \vee (\alpha \cap \beta)$ (and $\gamma \vee (\alpha \cap \beta) \supseteq (\alpha \cap \beta)$), we have $(\bar{x}, \bar{u}) \in \gamma \vee (\alpha \cap \beta)$. Therefore $\alpha \cap (\beta \vee \gamma) \subseteq \gamma \vee (\alpha \cap \beta)$. We have $\gamma \subseteq \alpha$, so the reverse inclusion holds (for any lattice). Thus V is modular.

□

Example 2.4.

The variety V of all *groups* $\mathbf{G} = \langle G; +, -, 0\rangle$ is congruence permutable, hence congruence modular. (Recall that a variety V is congruence permutable if and only if there is a *"Malcev" term* $t(x, y, z)$ such that $V \models t(x, y, y) \approx x \approx t(y, y, x)$ (Theorem 0.54); for groups, we may take $t(x, y, z) = (x - y) + z$.) For any congruence permutable variety V with Mal'cev term t, the following are *Day terms* for V (and therefore corroborate the modularity of V):

$$\begin{aligned} m_0(x, y, z, u) &= x \\ m_1(x, y, z, u) &= t(y, z, u) \;\; (= (y - z) + u \text{ for groups}) \\ m_2(x, y, z, u) &= u. \end{aligned}$$

Example 2.5.

The variety V of all *lattices* is congruence distributive (hence modular), and also has a *majority term*, viz. a term $t(x, y, z)$ such that

$$V \models t(x, x, y) \approx t(x, y, x) \approx t(y, x, x) \approx x.[14]$$

For lattices, taking $t(x, y, z) := (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$ works. For any variety V with a majority term t, the following are *Day terms* for V:

$$\begin{aligned} m_0(x, y, z, u) &= x \\ m_1(x, y, z, u) &= t(x, y, u) \;\; (= (x \vee y) \wedge (x \vee u) \wedge (y \vee u) \text{ for lattices}) \\ m_2(x, y, z, u) &= t(x, z, u) \;\; (= (x \vee z) \wedge (x \vee u) \wedge (z \vee u) \text{ for lattices}) \\ m_3(x, y, z, u) &= u. \end{aligned}$$

[14] Any variety with a majority term is congruence distributive: see Theorem 0.55.

2.2 The Commutator. For any variety V, $\mathbf{A} \in V$ and $\alpha, \beta \in Con(\mathbf{A})$, following [FM87], we define a set of matrices, $M(\alpha,\beta)$, of which each element satisfies a row and a column demand. We show that $\mathbf{M}(\alpha,\beta)$ is a subalgebra of $\mathbf{A}^4$. The commutator of the congruence relations α and β, namely $[\alpha,\beta]$, is defined as the smallest congruence relation on $\mathbf{A}$ that satisfies both the row and the column demands. This definition of the commutator depends on $\mathbf{A}$ but is independent of V.

We prove certain facts about $\mathbf{M}(\alpha,\beta)$ as well as $[\alpha,\beta]$ and other related congruences featuring in the definition. Later in the chapter we will extend these properties for modular varieties. Until further notice, let V be any variety of type $\mathcal{T} = \langle \mathsf{F}, ar \rangle$.

Definition 2.6. [FM87, Definition 3.2]

Let α, β, δ be in $Con(\mathbf{A})$, $\mathbf{A} \in V$.

(i) $M(\alpha,\beta)$ is the set of all matrices

$$\begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1,\mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^1,\mathbf{b}^2) \\ t^{\mathbf{A}}(\mathbf{a}^2,\mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^2,\mathbf{b}^2) \end{bmatrix}$$

where $\mathbf{a}^i = a^i_1,\dots,a^i_n$, $i = 1,2$, is any sequence of n elements of A, $\mathbf{b}^i = b^i_1,\dots,b^i_n$, $i = 1,2$, is any sequence of m elements of A $(m,n > 0)$, satisfying $a^1_k \alpha a^2_k$ and $b^1_j \beta b^2_j$ for $k \leq n$ and $j \leq m$, and t is any $(n+m)$-ary $\mathcal{T}$-term. Note that if

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(\alpha,\beta),$$

then $(a,c),(b,d) \in \alpha$ and $(a,b),(c,d) \in \beta$ but the converse need not hold.

(ii) We say α *centralizes* β *modulo* δ, and write $C(\alpha,\beta;\delta)$, if for every

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \in M(\alpha,\beta),$$

$u_{11} \delta u_{12}$ implies $u_{21} \delta u_{22}$.

(iii) $C(\alpha,\beta)$ is the smallest $\delta \in Con(\mathbf{A})$ for which $C(\alpha,\beta;\delta)$ holds.

(iv) $[\alpha,\beta]$ is the smallest $\delta \in Con(\mathbf{A})$ for which both $C(\alpha,\beta;\delta)$ and $C(\beta,\alpha;\delta)$ hold. We call $[\alpha,\beta]$ the *commutator* of α and β.

Remark 2.7.

$C(\alpha,\beta;\alpha\cap\beta)$ holds (see the proof of Proposition 2.9 (i)) and if $C(\alpha,\beta;\delta_i)$, $\delta_i \in Con(\mathbf{A})(i \in I)$ holds, $C(\alpha,\beta;\bigwedge_{i\in I}\delta_i)$ holds. Thus, the definitions (iii) and (iv) make sense.

This definition of the commutator is motivated by the following consequence that it has for groups (proved at the end of the chapter): for normal subgroups M, N of a group $\mathbf{G}$, $[M,N]$ is the least normal subgroup of $\mathbf{G}$ such that in $\mathbf{G}/[M,N]$ every element of $M/[M,N]$ commutes with every element of $N/[M,N]$.[15]

Proposition 2.8. [FM87, Proposition 3.3]

Let $\alpha, \beta \in Con(\mathbf{A}), \mathbf{A} \in V$.

(i) $\mathbf{M}(\alpha,\beta)$ *is the subalgebra of* $\mathbf{A}^4$ *generated by all the matrices of the forms*

$$\begin{bmatrix} a & a \\ a' & a' \end{bmatrix} \text{ and } \begin{bmatrix} b & b' \\ b & b' \end{bmatrix} \text{ where } (a,a') \in \alpha \text{ and } (b,b') \in \beta.$$

(ii)

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(\alpha,\beta) \text{ if and only if } \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in M(\beta,\alpha).$$

Proof.

(i) If we represent

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \in M(\alpha,\beta)$$

as $(u_{11}, u_{12}, u_{21}, u_{22})$ then $M(\alpha,\beta) \subseteq A^4$.

Let $Y = \{(a,a,a',a') : (a,a') \in \alpha\} \cup \{(b,b',b,b') : (b,b') \in \beta\}$. Let $v = (v_{11}, v_{12}, v_{21}, v_{22})$. By Theorem 0.36 (iii), $v \in Sg^{\mathbf{A}^4}(Y)$ if and only if there exist $n, m \in \omega$, an $(n+m)$-ary term t and for each $i \leq n$ and each $j \leq m$, tuples $a_i^* = (a_i^1, a_i^1, a_i^2, a_i^2)$ and $b_i^* = (b_i^1, b_i^2, b_i^1, b_i^2)$ with $(a_i^1, a_i^2) \in \alpha$ and $(b_j^1, b_j^2) \in \beta$ such that

$v = t^{\mathbf{A}^4}(a_1^*, \ldots, a_n^*, b_1^*, \ldots, b_m^*)$
$= (t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2))$,

where $\mathbf{a}^k = (a_1^k, \ldots, a_n^k)$ and $\mathbf{b}^k = (b_1^k, \ldots, b_m^k)$ for $k \in \{1,2\}$. In other words, $v \in Sg^{\mathbf{A}^4}(Y)$ if and only if $v \in M(\alpha,\beta)$, so $M(\alpha,\beta) = Sg^{\mathbf{A}^4}(Y)$.

(ii) Let

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(\alpha,\beta).$$

[15] Here we are identifying the congruences θ of groups $\langle G; +, -, 0\rangle$ with the normal subgroups $0/\theta$, as usual.

Then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2) \\ t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2) \end{bmatrix}$$

where $t, \mathbf{a}^i, \mathbf{b}^i, i = 1, 2$, are as in Definition 2.6 (i).

We have $a_k^1 \alpha a_k^2$ for $k \leq n$ (column condition) and $b_j^1 \beta b_j^2$ for $j \leq m$ (row condition) so

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1) \\ t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2) & t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2) \end{bmatrix}$$

where $b_j^1 \beta b_j^2$ for $j \leq m$ (column condition) and $a_k^1 \alpha a_k^2$ for $k \leq n$ (row condition), so

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} s^{\mathbf{A}}(\mathbf{b}^1, \mathbf{a}^1) & s^{\mathbf{A}}(\mathbf{b}^1, \mathbf{a}^2) \\ s^{\mathbf{A}}(\mathbf{b}^2, \mathbf{a}^1) & s^{\mathbf{A}}(\mathbf{b}^2, \mathbf{a}^2) \end{bmatrix}$$

where we define $s(\mathbf{x}, \mathbf{y}) = t(\mathbf{y}, \mathbf{x})$. Thus,

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \in M(\beta, \alpha).$$

The reverse implication is similar.

□

Proposition 2.9. *For $\alpha, \beta \in Con(\mathbf{A}), \mathbf{A} \in V$,*

(i) $C(\alpha, \beta) \subseteq [\alpha, \beta] = [\beta, \alpha] \subseteq \alpha \cap \beta$*;*

(ii) C *and* $[,]$ *are order-preserving.*

Proof.

(i) Let $\alpha, \beta \in Con(\mathbf{A})$, $\mathbf{A} \in V$. $[\alpha, \beta]$ is the smallest congruence δ for which both $C(\alpha, \beta; \delta)$ and $C(\beta, \alpha; \delta)$ hold, so it will contain the smallest δ' for which $C(\alpha, \beta; \delta')$ holds so $C(\alpha, \beta) \subseteq [\alpha, \beta]$. By the symmetry of its definition, $[\alpha, \beta] = [\beta, \alpha]$.

We show $[\beta, \alpha] \subseteq \alpha \cap \beta$. Firstly we show $C(\alpha, \beta; \alpha \cap \beta)$ holds. Let

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \in M(\alpha, \beta)$$

with $u_{11}(\alpha \cap \beta)u_{12}$. Then

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} = \begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2) \\ t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2) \end{bmatrix}$$

where $t, \mathbf{a}^i, \mathbf{b}^i$ $(i = 1, 2)$ are as in Definition 2.6 (i).

Since $a_k^1 \alpha a_k^2$ for $k \leq n$ and $b_j^i \alpha b_j^i$ for $j \leq m, i \in \{1, 2\}$, we have $u_{21} \alpha u_{11}$ and $u_{12} \alpha u_{22}$. By assumption, $u_{11} \alpha u_{12}$ so by transitivity $u_{21} \alpha u_{22}$. We also have $a_k^i \beta a_k^i$ for $k \leq n, i \in \{1,2\}$ and $b_j^1 \beta b_j^2$ for $j \leq m$ so $u_{11}\beta u_{12}$ and $u_{21}\beta u_{22}$. Therefore, $u_{11}(\alpha \cap \beta)u_{12}$ implies $u_{21}(\alpha \cap \beta)u_{22}$, so $C(\alpha, \beta; \alpha \cap \beta)$ holds.

By symmetry, $C(\beta, \alpha; \alpha \cap \beta)$ holds also. Since $C(\alpha, \beta; \alpha \cap \beta)$ and $C(\beta, \alpha; \alpha \cap \beta)$ hold, $\alpha \cap \beta$ must contain the smallest congruence δ such that $C(\alpha, \beta; \delta)$ and $C(\beta, \alpha; \delta)$ hold, i.e., $[\alpha, \beta] = [\beta, \alpha] \subseteq \alpha \cap \beta$.

(ii) Let $\theta, \theta', \varphi, \varphi' \in Con(\mathbf{A})$ with $\theta \subseteq \theta'$ and $\varphi \subseteq \varphi'$. We show $C(\theta, \varphi) \subseteq C(\theta', \varphi')$.

Let

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \in M(\theta, \varphi).$$

Then

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} = \begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2) \\ t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2) \end{bmatrix}$$

where $t, \mathbf{a}^i, \mathbf{b}^i$ $(i = 1, 2)$ are as in Definition 2.6 (i) but with $a_k^1 \theta a_k^2$ for $k \leq n$ and $b_j^1 \varphi b_j^2$ for $j \leq m$.

Since $\theta \subseteq \theta'$and $\varphi \subseteq \varphi'$ we have $a_k^1 \theta' a_k^2$ for $k \leq n$ and $b_j^1 \varphi' b_j^2$ for $j \leq m$ so

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \in M(\theta', \varphi').$$

If δ' is any congruence relation for which $C(\theta', \varphi'; \delta')$ holds and if $u_{11}\delta' u_{12}$ then $u_{21}\delta' u_{22}$. Thus, δ' is a congruence relation for which $C(\theta, \varphi; \delta')$ holds, so it will contain $C(\theta, \varphi)$. In particular, $C(\theta, \varphi) \subseteq C(\theta', \varphi')$.

Similarly, $C(\varphi, \theta) \subseteq C(\varphi', \theta')$ and $[\theta', \varphi'] \supseteq [\theta, \varphi]$.

□

2.3 The Commutator in Modular Varieties. In this section we will focus on a modular variety V with Day terms (described in Theorem 2.1). For $\mathbf{A} \in V$, with $\alpha, \beta \in Con(\mathbf{A}), \mathbf{M}(\alpha, \beta), C(\alpha, \beta)$ and $[\alpha, \beta]$ have been defined in the preceding section. We define a set of ordered pairs $X(\alpha, \beta) \subseteq A^2$ using Day terms, and in Proposition 2.11, we examine the relationship between $\mathbf{M}(\alpha, \beta), C(\alpha, \beta), [\alpha, \beta]$ and $X(\alpha, \beta)$. In the second part of this theorem we see that $[\alpha, \beta]$ is generated by $X(\alpha, \beta)$.

Definition 2.10.

Let $\mathbf{A} \in V$, where V is modular and has Day terms $m_0(x, y, z, u), \ldots,$ $m_n(x, y, z, u)$. For $\alpha, \beta \in Con(\mathbf{A})$, let $X(\alpha, \beta)$ be the set of ordered pairs

$(m_i^{\mathbf{A}}(a,b,d,c), m_i^{\mathbf{A}}(a,a,c,c))$ where

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(\alpha,\beta) \text{ and } i \leq n.$$

Note that $X(\alpha,\beta)$ is a reflexive relation on $\mathbf{A}$, because $m_i^{\mathbf{A}}(a,a,a,a) = a$ and

$$\begin{bmatrix} a & a \\ a & a \end{bmatrix} \in M(\alpha,\beta)$$

for all $a \in A$ and all $i \leq n$.

Proposition 2.11. [FM87, Proposition 4.2]

Let $\alpha,\beta,\delta \in Con(\mathbf{A})$, $\mathbf{A} \in V$, where V is modular and has Day terms $m_0(x,y,z,u),\ldots,m_n(x,y,z,u)$.

(1) The following are equivalent:

(i) $X(\alpha,\beta) \subseteq \delta$.

(ii) $X(\beta,\alpha) \subseteq \delta$.

(iii) $C(\alpha,\beta;\delta)$ holds.

(iv) $C(\beta,\alpha;\delta)$ holds.

(v) $[\alpha,\beta] \subseteq \delta$.

(2) $C(\alpha,\beta) = [\alpha,\beta] = \Theta^{\mathbf{A}}(X(\alpha,\beta))$. (Thus, $\Theta^{\mathbf{A}}(X(\alpha,\beta))$ does not depend on the particular choice of Day terms for V.)

Proof.

(1) We show (iii) $\Rightarrow$ (i) $\Rightarrow$ (iv), i.e., we show $C(\alpha,\beta;\delta)$ implies $X(\alpha,\beta) \subseteq \delta$ which in turn implies $C(\beta,\alpha;\delta)$. Then by interchanging α and β we have $C(\beta,\alpha;\delta)$ implies $X(\beta,\alpha) \subseteq \delta$ which in turn implies $C(\alpha,\beta;\delta)$, i.e., (iv) $\Rightarrow$ (ii) $\Rightarrow$ (iii). Finally, $[\alpha,\beta]$ is the smallest congruence relation for which $C(\alpha,\beta;\delta)$ and $C(\beta,\alpha;\delta)$ hold so (v) is equivalent to the conjunction of (iii) and (iv), hence to all the other conditions.

(iii)$\Rightarrow$(i): Let t be a $(n+k)$-ary term, with $\mathbf{a}^i \in A^n, \mathbf{b}^i \in A^k, i = 1,2; (\mathbf{a}^1,\mathbf{a}^2) \in \alpha, (\mathbf{b}^1,\mathbf{b}^2) \in \beta$ (co-ordinatewise, as in Definition 2.6 (i)).

$$\text{For} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1,\mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^1,\mathbf{b}^2) \\ t^{\mathbf{A}}(\mathbf{a}^2,\mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^2,\mathbf{b}^2) \end{bmatrix} \in M(\alpha,\beta),$$

and for each $i \leq n$, we show $u\delta v$ where $u = m_i^{\mathbf{A}}(a,a,c,c)$ and $v = m_i^{\mathbf{A}}(a,b,d,c)$.

We do this by showing that

$$\begin{bmatrix} u \\ v \end{bmatrix}.$$

is the right hand column of a matrix of the form

$$\begin{bmatrix} w & u \\ w & v \end{bmatrix} \in M(\beta, \alpha). \text{ Then } \begin{bmatrix} w & w \\ u & v \end{bmatrix} \in M(\alpha, \beta)$$

and because $C(\alpha, \beta; \delta)$, and $(w, w) \in \delta$, we have $(u, v) \in \delta$, i.e., for each $i \leq n, (m_i^{\mathbf{A}}(a, a, c, c), m_i^{\mathbf{A}}(a, b, d, c)) \in \delta$. Then $X(\alpha, \beta) \subseteq \delta$, proving (i).

For $j \in \{1, 2\}$, let $\mathbf{x}^j = x_1^j, \ldots, x_n^j$ and for $l = 1, \ldots, 6$ let $\mathbf{y}^l = y_1^l, \ldots, y_k^l$. Define $s(\mathbf{x}^1, \mathbf{x}^2, \mathbf{y}^1, \mathbf{y}^2, \mathbf{y}^3, \mathbf{y}^4, \mathbf{y}^5, \mathbf{y}^6) = m_i(t(\mathbf{y}^1, \mathbf{y}^2), t(\mathbf{x}^1, \mathbf{y}^3), t(\mathbf{y}^4, \mathbf{y}^5), t(\mathbf{x}^2, \mathbf{y}^6))$. Then $N =$

$$\begin{bmatrix} s^{\mathbf{A}}(\mathbf{a}^2, \mathbf{a}^1, \mathbf{a}^1, \mathbf{b}^1, \mathbf{b}^1, \mathbf{a}^2, \mathbf{b}^1, \mathbf{b}^1) & s^{\mathbf{A}}(\mathbf{a}^1, \mathbf{a}^2, \mathbf{a}^1, \mathbf{b}^1, \mathbf{b}^1, \mathbf{a}^2, \mathbf{b}^1, \mathbf{b}^1) \\ s^{\mathbf{A}}(\mathbf{a}^2, \mathbf{a}^1, \mathbf{a}^1, \mathbf{b}^1, \mathbf{b}^2, \mathbf{a}^2, \mathbf{b}^2, \mathbf{b}^1) & s^{\mathbf{A}}(\mathbf{a}^1, \mathbf{a}^2, \mathbf{a}^1, \mathbf{b}^1, \mathbf{b}^2, \mathbf{a}^2, \mathbf{b}^2, \mathbf{b}^1) \end{bmatrix} \in M(\beta, \alpha)$$

since $(\mathbf{a}^1, \mathbf{a}^2) \in \alpha, (\mathbf{b}^1, \mathbf{b}^2) \in \beta$. Now $s^{\mathbf{A}}(\mathbf{a}^2, \mathbf{a}^1, \mathbf{a}^1, \mathbf{b}^1, \mathbf{b}^1, \mathbf{a}^2, \mathbf{b}^1, \mathbf{b}^1) = m_i^{\mathbf{A}}(t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1))$ and $s^{\mathbf{A}}(\mathbf{a}^2, \mathbf{a}^1, \mathbf{a}^1, \mathbf{b}^1, \mathbf{b}^2, \mathbf{a}^2, \mathbf{b}^2, \mathbf{b}^1) = m_i^{\mathbf{A}}(t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2), t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1))$. This gives

$$N = \begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1) & m_i^{\mathbf{A}}(t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1)) \\ t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1) & m_i^{\mathbf{A}}(t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1)) \end{bmatrix} = \begin{bmatrix} w & u \\ w & v \end{bmatrix}$$

where $w = t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1), u = m_i^{\mathbf{A}}(t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1))$, and $v = m_i^{\mathbf{A}}(t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1))$ so

$$\begin{bmatrix} w & u \\ w & v \end{bmatrix} \in M(\beta, \alpha).$$

(i)⇒(iv): We show if $X(\alpha, \beta) \subseteq \delta$, then for any

$$\begin{bmatrix} b & d \\ a & c \end{bmatrix} \in M(\beta, \alpha),$$

if $(b, d) \in \delta$, then $(a, c) \in \delta$. First,

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \in M(\alpha, \beta) \text{ if and only if } \begin{bmatrix} u_{12} & u_{11} \\ u_{22} & u_{21} \end{bmatrix} \in M(\alpha, \beta)$$

by the symmetry of $\mathbf{b}^1$ and $\mathbf{b}^2$ in the definition of $\mathbf{M}(\alpha, \beta)$.

Now for

$$\begin{bmatrix} b & d \\ a & c \end{bmatrix} \in M(\beta, \alpha), \text{ we have } \begin{bmatrix} b & a \\ d & c \end{bmatrix} \in M(\alpha, \beta)$$

by Proposition 2.8 (ii) and by the above,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(\alpha,\beta).$$

Suppose $(b,d) \in \delta$. Since $X(\alpha,\beta) \subseteq \delta$ we have $(m_i^{\mathbf{A}}(a,b,d,c), m_i^{\mathbf{A}}(a,a,c,c)) \in \delta$ for all $i \leq n$. V is modular and has Day terms m_i, so by Theorem 2.3 ((ii)$\Rightarrow$(iii)), since $(b,d) \in \delta$, we have $(a,c) \in \delta$. Thus $X(\alpha,\beta) \subseteq \delta$ implies $C(\beta,\alpha;\delta)$.

(2) $C(\alpha,\beta) = \gamma$ is the smallest congruence relation on $\mathbf{A}$ for which $C(\alpha,\beta;\gamma)$ holds. By (1), (iii) is equivalent to (v), so $[\alpha,\beta] \subseteq \gamma$. Also since $[\alpha,\beta]$ is a congruence relation for which $C(\alpha,\beta;[\alpha,\beta])$ holds, $\gamma \subseteq [\alpha,\beta]$. Therefore $C(\alpha,\beta) = [\alpha,\beta]$.

$X(\alpha,\beta) \subseteq \Theta^{\mathbf{A}}(X(\alpha,\beta))$, so $[\alpha,\beta] \subseteq \Theta^{\mathbf{A}}(X(\alpha,\beta))$ by (1) ((i) $\Leftrightarrow$ (v)). Let $[\alpha,\beta] = \delta'$. Certainly, $C(\alpha,\beta;\delta')$ and $C(\beta,\alpha;\delta')$ hold so $X(\alpha,\beta) \subseteq \delta'$ by (1) ((iii) (or (iv)) $\Leftrightarrow$ (i)). Thus, $\Theta^{\mathbf{A}}(X(\alpha,\beta)) \subseteq \delta' = [\alpha,\beta]$, and so $[\alpha,\beta] = \Theta^{\mathbf{A}}(X(\alpha,\beta))$.

□

The next results describe some general properties of the commutator $[\alpha,\beta]$ ($\alpha,\beta \in Con(\mathbf{A})$, $\mathbf{A} \in V$). Proposition 2.9 showed that the commutator is symmetric and "sub-multiplicative', i.e., $[\alpha,\beta] = [\beta,\alpha]$ and $[\alpha,\beta] \subseteq \alpha \cap \beta$. Proposition 2.12 shows that it is also join-distributive ("additive"), i.e., $[\alpha, \bigvee_{i\in I}\gamma_i] = \bigvee_{i\in I}[\alpha,\gamma_i]$, provided that V is modular.

We shall see how the commutator behaves with respect to homomorphisms, subalgebras (Proposition 2.14) and direct products (Proposition 2.17). In the last section of this chapter we see that this behaviour generalizes properties in groups and rings.

Proposition 2.12. [HH79]

Let V be a modular variety and let θ,ψ,γ_i $(i \in I)$ be congruences on $\mathbf{A} \in V$. Then we have $[\theta, \bigvee_{i\in I}\gamma_i] = \bigvee_{i\in I}[\theta,\gamma_i]$.

Proof.

For each $i \in I$, $\gamma_i \subseteq \bigvee_{i\in I}\gamma_i$ so for each $i \in I, [\theta,\gamma_i] \subseteq [\theta, \bigvee_{i\in I}\gamma_i]$ since by Proposition 2.9 (ii), $[,]$ is order-preserving. Thus $\bigvee_{i\in I}[\theta,\gamma_i] \subseteq [\theta, \bigvee_{i\in I}\gamma_i]$. Let $\alpha = \bigvee_{i\in I}[\theta,\gamma_i]$. For each $i \in I, [\theta,\gamma_i] \subseteq \bigvee_{j\in I}[\theta,\gamma_j] = \alpha$. By the equivalence of (v) and (iii) in Proposition 2.11, for each $i \in I$, $C(\theta,\gamma_i;\alpha)$ holds. .... (*)

Now let

$$\begin{bmatrix} u & v \\ r & s \end{bmatrix} \in M(\theta,\gamma)$$

where $\gamma = \bigvee_{i \in I} \gamma_i$, and let $(u, r) \in \alpha$.

Then

$$\begin{bmatrix} u & v \\ r & s \end{bmatrix} = \begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2) \\ t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2) \end{bmatrix}$$

$$= \begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1, b_1^1, b_2^1, \dots, b_m^1) & t^{\mathbf{A}}(\mathbf{a}^1, b_1^2, b_2^2, \dots, b_m^2) \\ t^{\mathbf{A}}(\mathbf{a}^2, b_1^1, b_2^1, \dots, b_m^1) & t^{\mathbf{A}}(\mathbf{a}^2, b_1^2, b_2^2, \dots, b_m^2) \end{bmatrix}$$

where $\mathbf{a}^i = (a_1^i, \dots, a_n^i) \in A^n$, $\mathbf{b}^i = (b_1^i, \dots, b_m^i) \in A^m$, $i = 1, 2$; t is a $(n+m)$-ary term with $a_l^1 \theta a_l^2$ for $l \leq n$ and $b_p^1 \gamma b_p^2$ for $p \leq m$, i.e., $b_p^1 (\bigvee_{i \in I} \gamma_i)\, b_p^2$ for $p \leq m$. Thus, for $p \leq m$, by Theorem 0.8, there are $i_1, \dots, i_k \in I$ such that $b_p^1 (\gamma_{i1} \circ \gamma_{i2} \circ \dots \circ \gamma_{ik}) b_p^2$, so there are $y_{p0}, y_{p1}, \dots, y_{pk}$ such that $b_p^1 = y_{p0}, b_p^2 = y_{pk}$ and $y_{p0} (\gamma_{i1})\, y_{p1} (\gamma_{i2})\, y_{p2} \cdots y_{p(k-1)} (\gamma_{ik})\, y_{pk}$.

For

$$\begin{aligned} p = 1 &: \quad b_1^1 (\gamma_{i1})\, y_{11} (\gamma_{i2})\, y_{12} \cdots y_{1(k-1)} (\gamma_{ik})\, b_1^2 \\ p = 2 &: \quad b_2^1 (\gamma_{i1})\, y_{21} (\gamma_{i2})\, y_{22} \cdots y_{2(k-1)} (\gamma_{ik})\, b_2^2 \\ &\quad \dots \\ p = m &: \quad b_m^1 (\gamma_{i1})\, y_{m1} (\gamma_{i2})\, y_{m2} \cdots y_{m(k-1)} (\gamma_{ik})\, b_m^2). \end{aligned}$$

We then get

$$\begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1, b_1^1, b_2^1, \dots, b_m^1) & t^{\mathbf{A}}(\mathbf{a}^1, y_{11}, y_{21}, \dots, y_{m1}) \\ t^{\mathbf{A}}(\mathbf{a}^2, b_1^1, b_2^1, \dots, b_m^1) & t^{\mathbf{A}}(\mathbf{a}^2, y_{11}, y_{21}, \dots, y_{m1}) \end{bmatrix} = \begin{bmatrix} x_0 & x_1 \\ z_0 & z_1 \end{bmatrix} \in M(\theta, \gamma_{i1}),$$

say, since $\mathbf{a}^1 \theta\, \mathbf{a}^2$ (co-ordinatewise) and $b_p^1 (\gamma_{i1})\, y_{p1}$ for all $p \leq m$ and

$$\begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1, y_{11}, y_{21}, \dots, y_{m1}) & t^{\mathbf{A}}(\mathbf{a}^1, y_{12}, y_{22}, \dots, y_{m2}) \\ t^{\mathbf{A}}(\mathbf{a}^2, y_{11}, y_{21}, \dots, y_{m1}) & t^{\mathbf{A}}(\mathbf{a}^2, y_{12}, y_{22}, \dots, y_{m2}) \end{bmatrix} = \begin{bmatrix} x_1 & x_2 \\ z_1 & z_2 \end{bmatrix} \in M(\theta, \gamma_{i2}),$$

say, since $y_{p1} (\gamma_{i2})\, y_{p2}$ for all $p \leq m$.

Continuing thus, we have finite sequences $x_0, x_1, \dots, x_k, z_0, z_1, \dots, z_k$ such that

$$\begin{bmatrix} x_j & x_{j+1} \\ z_j & z_{j+1} \end{bmatrix} = \begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1, y_{1j}, y_{2j}, \dots, y_{mj}) & t^{\mathbf{A}}(\mathbf{a}^1, y_{1(j+1)}, y_{2(j+1)}, \dots, y_{m(j+1)}) \\ t^{\mathbf{A}}(\mathbf{a}^2, y_{1j}, y_{2j}, \dots, y_{mj}) & t^{\mathbf{A}}(\mathbf{a}^2, y_{1(j+1)}, y_{2(j+1)}, \dots, y_{m(j+1)}) \end{bmatrix}$$

$\in M(\theta, \gamma_{i(j+1)})$ for $1 \leq j < k$ since $\mathbf{a}^1 \theta\, \mathbf{a}^2$ (co-ordinatewise), $y_{pj} (\gamma_{i(j+1)})\, y_{p(j+1)}$ for $p \leq m$ and for $j < k$ and such that

$$\begin{bmatrix} x_0 & x_k \\ z_0 & z_k \end{bmatrix} = \begin{bmatrix} u & v \\ r & s \end{bmatrix}.$$

For each $i \in I$, we have $C(\theta, \gamma_i; \alpha)$ (by (*)), so by Proposition 2.11 (1) ((iii) $\Leftrightarrow$ (iv)), $C(\gamma_i, \theta; \alpha)$.

Consider

$$\begin{bmatrix} x_0 & x_1 \\ z_0 & z_1 \end{bmatrix} \in M(\theta, \gamma_{i1}).$$

By Proposition 2.8 (ii),

$$\begin{bmatrix} x_0 & z_0 \\ x_1 & z_1 \end{bmatrix} \in M(\gamma_{i1}, \theta).$$

Since $(u, r) = (x_0, z_0) \in \alpha$ and since $C(\gamma_{i1}, \theta; \alpha)$ holds, we have $(x_1, z_1) \in \alpha$.

Now

$$\begin{bmatrix} x_1 & x_2 \\ z_1 & z_2 \end{bmatrix} \in M(\theta, \gamma_{i2}) \text{ so } \begin{bmatrix} x_1 & z_1 \\ x_2 & z_2 \end{bmatrix} \in M(\gamma_{i2}, \theta)$$

by Proposition 2.8 (ii) and since $C(\gamma_{i2}, \theta; \alpha)$ holds and $(x_1, z_1) \in \alpha$, we have $(x_2, z_2) \in \alpha$. Continuing in this way we get $(x_j, z_j) \in \alpha$ for all $j \leq k$ so $(x_k, z_k) \in \alpha$, i.e., $(v, s) \in \alpha$.

We have shown that $C(\bigvee_{i\in I} \gamma_i, \theta; \alpha)$ holds, so $C(\theta, \bigvee_{i\in I} \gamma_i; \alpha)$ holds by Proposition 2.11 (1) ((iii)⇔(iv)). Thus, we have $[\theta, \bigvee_{i\in I} \gamma_i] \subseteq \bigvee_{i\in I}[\theta, \gamma_i]$.

□

Lemma 2.13. *Let $f : \mathbf{A} \to \mathbf{B}$ be a surjective homomorphism of algebras and $Y \subseteq A^2$ such that $ker(f) \subseteq Y$. Then $f(\Theta^{\mathbf{A}}(Y)) = \Theta^{\mathbf{B}}(f(Y))$.*

Proof.

$f(Y) \subseteq \Theta^{\mathbf{B}}(f(Y))$, so $Y \subseteq f^{-1}(\Theta^{\mathbf{B}}(f(Y))) \in Con(\mathbf{A})$, so $\Theta^{\mathbf{A}}(Y) \subseteq f^{-1}(\Theta^{\mathbf{B}}(f(Y)))$, i.e., $f(\Theta^{\mathbf{A}}(Y)) \subseteq \Theta^{\mathbf{B}}(f(Y))$. Also $f(Y) \subseteq f(\Theta^{\mathbf{A}}(Y))$ and $f(\Theta^{\mathbf{A}}(Y)) \in Con(\mathbf{B})$ (because $ker(f) \subseteq Y \subseteq \Theta^{\mathbf{A}}(Y)$ and $\Theta^{\mathbf{A}}(Y) \in Con(\mathbf{A})$) so $\Theta^{\mathbf{B}}(f(Y)) \subseteq f(\Theta^{\mathbf{A}}(Y))$.

□

Proposition 2.14. [FM87, Proposition 4.4]

Let $\mathbf{A}, \mathbf{B} \in V$, where V is a modular variety with Day terms $m_1, \ldots, m_n$.

(i) If $f \in Hom(\mathbf{A}, \mathbf{B})$ is surjective, with kernel π, and $\theta, \varphi \in Con(\mathbf{A})$, then

$$[\theta, \varphi] \vee \pi = f^{-1}([f(\theta \vee \pi), f(\varphi \vee \pi)]).$$

(ii) If $\mathbf{B}$ is a subalgebra of $\mathbf{A}$ and $\theta, \varphi \in Con(\mathbf{A})$, then the restrictions to $\mathbf{B}$ satisfy

$$[\theta|_{\mathbf{B}}, \varphi|_{\mathbf{B}}] \subseteq [\theta, \varphi]|_{\mathbf{B}}.$$

Proof.

(i) Let $\mathbf{A}, \mathbf{B} \in V$. Let $f \in Hom(\mathbf{A}, \mathbf{B})$ (the set of homomorphisms from $\mathbf{A}$ to $\mathbf{B}$) be surjective, with kernel π, and let $\theta, \varphi \in Con(\mathbf{A})$. We first show

$[\theta,\varphi]\vee\pi = [\theta\vee\pi,\varphi\vee\pi]\vee\pi$. By Proposition 2.12, $[\theta\vee\pi,\varphi\vee\pi] = [\theta\vee\pi,\varphi]\vee[\theta\vee\pi,\pi] = [\theta,\varphi]\vee[\pi,\varphi]\vee[\theta,\pi]\vee[\pi,\pi]$. Now $[\pi,\pi]\subseteq\pi$ and $[\theta,\pi]\subseteq\theta\cap\pi$ and $[\pi,\varphi]\subseteq\pi\cap\varphi$ by Proposition 2.9 (i). Since $\theta\cap\pi\subseteq\pi$ and $\pi\cap\varphi\subseteq\pi$ we have $[\theta\vee\pi,\varphi\vee\pi]\subseteq[\theta,\varphi]\vee\pi$, therefore $[\theta\vee\pi,\varphi\vee\pi]\vee\pi\subseteq[\theta,\varphi]\vee\pi$.

Conversely, $[\theta,\varphi]\vee\pi\subseteq[\theta\vee\pi,\varphi\vee\pi]\vee\pi$ by Proposition 2.9 (ii) because $\theta\subseteq\theta\vee\pi$ and $\varphi\subseteq\varphi\vee\pi$. It follows that $[\theta,\varphi]\vee\pi = [\theta\vee\pi,\varphi\vee\pi]\vee\pi$, so without loss of generality, we may assume $\pi\subseteq\theta,\pi\subseteq\varphi$ and so $f(\theta), f(\varphi)\in Con(\mathbf{B})$ (by Theorem 0.14).

Since $[\theta,\varphi] = \Theta^{\mathbf{A}}(X(\theta,\varphi))$ by Proposition 2.11 (2),

$[\theta,\varphi]\vee\pi = \Theta^{\mathbf{A}}(X(\theta,\varphi)\cup\pi)$. .... (1)

By Proposition 2.11 (2), $[f(\theta),f(\varphi)] = \Theta^{\mathbf{B}}(X(f(\theta),f(\varphi)))$. .... (2)

We show first that $f(X(\theta,\varphi)\cup\pi)\subseteq X(f(\theta),f(\varphi))$. Let $(x,y)\in f(X(\theta,\varphi)\cup\pi)$. Then there exists $(x_1,y_1)\in X(\theta,\varphi)\cup\pi$ with $(f(x_1),f(y_1)) = (x,y)$.

If $(x_1,y_1)\in\pi$ then $f(x_1) = f(y_1)$ so $(x,y) = (x,x)\in X(f(\theta),f(\varphi))$, by reflexiveness of $X(f(\theta),f(\varphi))$. Otherwise, $(x_1,y_1)\in X(\theta,\varphi)$, so $(x_1,y_1) = (m_i^{\mathbf{A}}(a,b,d,c), m_i^{\mathbf{A}}(a,a,c,c))$ for some $i\leq n$, where $a,b,c,d\in A$ and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1,\mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^1,\mathbf{b}^2) \\ t^{\mathbf{A}}(\mathbf{a}^2,\mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^2,\mathbf{b}^2) \end{bmatrix} \in M(\theta,\varphi)$$

for some $\mathbf{a}^i = (a_1^i,\ldots,a_k)\in A^k$ and $\mathbf{b}^i = (b_1^i,\ldots,b_l)\in A^l$ (i = 1,2) and some $(k+l)$-ary term t, where $\mathbf{a}^1\theta\mathbf{a}^2$ and $\mathbf{b}^1\varphi\mathbf{b}^2$ (co-ordinatewise).

Since f is a homomorphism,

$$\begin{bmatrix} f(a) & f(b) \\ f(c) & f(d) \end{bmatrix} = \begin{bmatrix} t^{\mathbf{B}}(\mathbf{c}^1,\mathbf{d}^1) & t^{\mathbf{B}}(\mathbf{c}^1,\mathbf{d}^2) \\ t^{\mathbf{B}}(\mathbf{c}^2,\mathbf{d}^1) & t^{\mathbf{B}}(\mathbf{c}^2,\mathbf{d}^2) \end{bmatrix}$$

where $\mathbf{c}^i = f(a_1^i),\ldots,f(a_k^i)$ and $\mathbf{d}^i = f(b_1^i),\ldots,f(b_l^i)$ $(i = 1,2)$, hence $\mathbf{c}^1 f(\theta)\mathbf{c}^2$ and $\mathbf{d}^1 f(\varphi)\mathbf{d}^2$ (co-ordinatewise).

Thus,

$$\begin{bmatrix} f(a) & f(b) \\ f(c) & f(d) \end{bmatrix} \in M(f(\theta),f(\varphi)), \text{ so}$$

$(x,y) = (f(x_1),f(y_1)) = (m_i^{\mathbf{B}}(f(a),f(b),f(d),f(c)), m_i^{\mathbf{B}}(f(a),f(a),f(c),f(c)))\in X(f(\theta),f(\varphi))$.

Now, we show that $X(f(\theta),f(\varphi))\subseteq f(X(\theta,\varphi)\cup\pi)$. Let $(x,y)\in X(f(\theta),f(\varphi))$. We show $(x,y)\in f(X(\theta,\varphi))$.

Now $(x,y) = (m_i^{\mathbf{A}}(a,b,d,c), m_i^{\mathbf{A}}(a,a,c,c))$ for some $i \leq n$ and some $a,b,c,d \in B$ such that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} t^{\mathbf{B}}(\mathbf{a}^1,\mathbf{b}^1) & t^{\mathbf{B}}(\mathbf{a}^1,\mathbf{b}^2) \\ t^{\mathbf{B}}(\mathbf{a}^2,\mathbf{b}^1) & t^{\mathbf{B}}(\mathbf{a}^2,\mathbf{b}^2) \end{bmatrix} \in M(f(\theta), f(\varphi))$$

for some term t where $\mathbf{a}^1 f(\theta)\mathbf{a}^2$ and $\mathbf{b}^1 f(\varphi)\mathbf{b}^2$ (co-ordinatewise). Thus there exist $\mathbf{c}^j, \mathbf{d}^j$ $(j = 1,2)$ such that $\mathbf{c}^1\theta\mathbf{c}^2$ and $\mathbf{d}^1\varphi\mathbf{d}^2$ (co-ordinatewise) and $(a_k^1, a_k^2) = (f(c_k^1), f(c_k^2))$ and $(b_l^1, b_l^2) = (f(d_l^1), f(d_l^2))$ for each k, l.

Let

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} = \begin{bmatrix} t^{\mathbf{A}}(\mathbf{c}^1,\mathbf{d}^1) & t^{\mathbf{A}}(\mathbf{c}^1,\mathbf{d}^2) \\ t^{\mathbf{A}}(\mathbf{c}^2,\mathbf{d}^1) & t^{\mathbf{A}}(\mathbf{c}^2,\mathbf{d}^2) \end{bmatrix} \in M(\theta,\varphi).$$

Then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} f(u_{11}) & f(u_{12}) \\ f(u_{21}) & f(u_{22}) \end{bmatrix}$$

so $(x,y) = (f(m_i^{\mathbf{A}}(u_{11},u_{12},u_{22},u_{21})), f(m_i^{\mathbf{A}}(u_{11},u_{11},u_{21},u_{21}))) \in f(X(\theta,\varphi))$, as required.

We therefore have $X(f(\theta),f(\varphi)) = f(X(\theta,\varphi)) = f(X(\theta,\varphi)\cup\pi)$. $\ldots\ldots$(3)
Since $ker(f) = \pi \subseteq X(\theta,\varphi)\cup\pi$, it follows from Lemma 2.13 that
$f(\Theta^{\mathbf{A}}(X(\theta,\varphi)\cup\pi)) = \Theta^{\mathbf{B}}(f(X(\theta,\varphi)\cup\pi))$. $\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$(4)
Now $f([\theta,\varphi]\vee\pi) = f(\Theta^{\mathbf{A}}(X(\theta,\varphi)\cup\pi))$ (by (1))
$= \Theta^{\mathbf{B}}(f(X(\theta,\varphi)\cup\pi))$ (by (4))
$= \Theta^{\mathbf{B}}(X(f(\theta),f(\varphi)))$ (by (3))
$= [f(\theta),f(\varphi)]$ (by (2)).

Since $ker(f) \subseteq [\theta,\varphi]\vee\pi \in Con(\mathbf{A})$, it follows from the Correspondence Theorem (Theorem 0.17), that $[\theta,\varphi]\vee\pi = f^{-1}([f(\theta),f(\varphi)]) = f^{-1}([f(\theta\vee\pi), f(\varphi\vee\pi)])$.

(ii) Let $\mathbf{B}$ be a subalgebra of $\mathbf{A}$ and $\theta,\varphi \in Con(\mathbf{A})$. We show $\theta|_{\mathbf{B}}$ centralizes $\varphi|_{\mathbf{B}}$ modulo $[\theta,\varphi]|_{\mathbf{B}}$, i.e., $C(\theta|_{\mathbf{B}}, \varphi|_{\mathbf{B}}; [\theta,\varphi]|_{\mathbf{B}})$, since then by Proposition 2.11 ((iii) $\Rightarrow$ (v)) we will have $[\theta|_{\mathbf{B}}, \varphi|_{\mathbf{B}}] \subseteq [\theta,\varphi]|_{\mathbf{B}}$.

$$\text{Let} \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \in M(\theta|_{\mathbf{B}}, \varphi|_{\mathbf{B}}) \text{ with } (u_{11},u_{12}) \in [\theta,\varphi]|_{\mathbf{B}}.$$

We must show that $(u_{21},u_{22}) \in [\theta,\varphi]|_{\mathbf{B}}$. Here $[\theta,\varphi]|_{\mathbf{B}}$ is the restriction to $B\times B$ of $[\theta,\varphi]$, i.e., of the smallest $\delta \in Con(\mathbf{A})$ for which $C(\theta,\varphi;\delta)$ and $C(\varphi,\theta;\delta)$ hold.

Now

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \text{has the form} \begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1,\mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^1,\mathbf{b}^2) \\ t^{\mathbf{A}}(\mathbf{a}^2,\mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^2,\mathbf{b}^2) \end{bmatrix}$$

where $\mathbf{a}^i \in A^n, \mathbf{b}^i \in A^m, i = 1,2$, with $a_l^1 \theta|_{\mathbf{B}} a_l^2$ for $l \leq n$ and $b_p^1 \varphi|_{\mathbf{B}} b_p^2$ for $p \leq m$, and t is an $(n+m)$-ary term. Now $a_l^i, b_p^i \in B$ for all i, l, p so $u_{11}, u_{12}, u_{21}, u_{22} \in B$.

Since $\theta|_{\mathbf{B}} \subseteq \theta$ and $\varphi|_{\mathbf{B}} \subseteq \varphi$, we have $a_l^1 \theta\, a_l^2$ for $l \leq n$ and $b_p^1 \varphi\, b_p^2$ for $p \leq m$ so

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \in M(\theta, \varphi).$$

Therefore $M(\theta|_{\mathbf{B}}, \varphi|_{\mathbf{B}}) \subseteq M(\theta, \varphi)$. Since $(u_{11}, u_{12}) \in [\theta, \varphi]|_{\mathbf{B}}$, we have $(u_{11}, u_{12}) \in [\theta, \varphi]$. Then since θ centralizes φ modulo $[\theta, \varphi]$, we have $(u_{21}, u_{22}) \in [\theta, \varphi]$. We also have $(u_{21}, u_{22}) \in B \times B$ so $(u_{21}, u_{22}) \in [\theta, \varphi]|_{\mathbf{B}}$, as required.

□

Remark 2.15.

Let $\mathbf{A} \in V$, where $\mathbf{A}$ is a modular variety. Let $f : \mathbf{A} \to \mathbf{B}$ be a surjective homomorphism and let $ker(f) = \pi$. Then $\mathbf{A}/\pi \cong \mathbf{B}$ by the Homomorphism Theorem so $\mathbf{Con}(\mathbf{A}/\pi) \cong \mathbf{Con}(\mathbf{B})$. By the Correspondence Theorem, $\mathbf{int}(\pi, A^2) \cong \mathbf{Con}(\mathbf{A}/\pi)$ (where $int(\pi, A^2) = \{\gamma \in Con(\mathbf{A}) : \pi \subseteq \gamma \subseteq A^2\}$) so we have $\mathbf{int}(\pi, A^2) \overset{\hat{f}}{\cong} \mathbf{Con}(\mathbf{B})$ where $\hat{f} : \mathbf{int}(\pi, A^2) \to \mathbf{Con}(\mathbf{B})$ is defined by $\theta \mapsto f(\theta)$ for all $\theta \in int(\pi, A^2)$.

For $\theta, \varphi \in int(\pi, A^2)$, since $\pi \subseteq \theta, \varphi$, $[\hat{f}(\theta), \hat{f}(\varphi)] = [\hat{f}(\theta \vee \pi), \hat{f}(\varphi \vee \pi)] = [f(\theta \vee \pi), f(\varphi \vee \pi)]$ in $Con(\mathbf{B})$ by definition of $\hat{f}$. By Proposition 2.14 (i), $f^{-1}([f(\theta), f(\varphi)]) = [\theta, \varphi] \vee \pi \in Con(\mathbf{A})$ (which means that for all $a, b \in A$, $(f(a), f(b)) \in [f(\theta), f(\varphi)]$ if and only if $(a, b) \in [\theta, \varphi] \vee \pi$).

As a result, if $f : \mathbf{A} \to \mathbf{B}$ is a surjective homomorphism with $ker(f) = \pi$ then we can calculate $[f(\theta), f(\varphi)]$ by calculating $[\theta, \varphi] \vee \pi$ in $Con(\mathbf{A})$; then $\{(f(a), f(b)) : (a, b) \in [\theta, \varphi] \vee \pi\}$ gives us $[f(\theta), f(\varphi)]$. The operation $[\theta, \varphi] \vee \pi$, denoted by $[\theta, \varphi]_\pi$, is called the *relative commutator.*

This result gives us a description of the commutator of congruences of a quotient algebra $\mathbf{A}/\gamma$, where $\gamma \in Con(\mathbf{A})$, for if f is the natural homomorphism, we will have $[\theta/\gamma, \varphi/\gamma] = \{(a/\gamma, b/\gamma) : (a, b) \in [\theta, \varphi] \vee \gamma\} = ([\theta, \varphi] \vee \gamma)/\gamma$.

Remark 2.16.

Let V be a modular variety. Let $\mathbf{A} \in V$ with $\alpha, \beta, \delta, \gamma \in Con(\mathbf{A})$. Let $int(\beta, \alpha) \nearrow int(\delta, \gamma)$. Since $Con(\mathbf{A})$ is modular, we have a lattice isomorphism $f : \mathbf{int}(\beta, \alpha) \cong \mathbf{int}(\delta, \gamma)$ defined by $f : \theta \mapsto \theta \vee \delta$ $(\theta \in int(\beta, \alpha))$ (Theorem 0.3). We show that f and its inverse h preserve the relative commutator.

Now $int(\beta,\alpha) \nearrow int(\delta,\gamma)$ implies $int(\delta,\gamma) \searrow int(\beta,\alpha)$, so $\alpha \cap \delta = \beta$ and $\alpha \vee \delta = \gamma$. Recall that $h = f^{-1} : \varphi' \mapsto \varphi' \cap \alpha$ ($\varphi' \in int(\delta,\gamma)$). Let $\theta, \varphi \in Con(\mathbf{A})$. We show that $f([\theta,\varphi]_\beta) = [f(\theta), f(\varphi)]_\delta$, i.e., that $[\theta,\varphi]_\beta \vee \delta = [\theta \vee \delta, \varphi \vee \delta]_\delta$.

$[\theta \vee \delta, \varphi \vee \delta]_\delta = [\theta \vee \delta, \varphi \vee \delta] \vee \delta = [\theta,\varphi] \vee [\delta,\varphi] \vee [\theta,\delta] \vee [\delta,\delta] \vee \delta$ by additivity (Proposition 2.12). Now $[\delta,\delta] \subseteq \delta \cap \delta = \delta$ by Proposition 2.9 (i) so $[\delta,\delta] \vee \delta = \delta$, therefore $[\theta \vee \delta, \varphi \vee \delta]_\delta$ is $[\theta,\varphi] \vee [\delta,\varphi] \vee [\theta,\delta] \vee \delta$.

By (Proposition 2.9) (i), $[\delta,\varphi] \vee [\theta,\delta] \subseteq (\varphi \vee \theta) \cap \delta \subseteq \alpha \cap \delta = \beta$, and so $[f(\theta), f(\varphi)]_\delta \subseteq [\theta,\varphi] \vee \beta \vee \delta = [\theta,\varphi]_\beta \vee \delta = f([\theta,\varphi] \vee \beta)$. But $f([\theta,\varphi] \vee \beta) = [\theta,\varphi] \vee \beta \vee \delta = [\theta,\varphi] \vee \delta$ since $\beta \subseteq \delta$. By order-preservation, $[\theta,\varphi] \subseteq [\theta \vee \delta, \varphi \vee \delta]$ so $f([\theta,\varphi] \vee \beta) \subseteq [\theta \vee \delta, \varphi \vee \delta] \vee \delta = [\theta \vee \delta, \varphi \vee \delta]_\delta = [f(\theta), f(\varphi)]_\delta$.

Let $\theta', \varphi' \in Con(\mathbf{A})$. Since f is a lattice isomorphism and $h = f^{-1}$, it follows that $h([\theta', \varphi']_\delta) = [h(\theta'), h(\varphi')]_\beta$, i.e., that $[\theta', \varphi']_\delta \cap \alpha = [\theta' \cap \alpha, \varphi' \cap \alpha]_\beta$.

Proposition 2.17. [FM87, Proposition 4.5]

Let V be a modular variety. Suppose $\mathbf{A}_i \in V$, let $\mathbf{A} = \prod_{i\in I} \mathbf{A}_i$ and $\theta_i \in Con(\mathbf{A}), i \in I$. Then

(i) the map $(\theta_i)_{i\in I} \mapsto \{(a,b) \in A \times A : (a_i,b_i) \in \theta_i$ for all $i \in I$ and $a_i = b_i$ for all but finitely many $i \in I\}$

is a lattice isomorphism from $\prod_{i\in I} \mathbf{Con}(\mathbf{A}_i)$ into $\mathbf{Con}(\mathbf{A})$. Furthermore, this isomorphism preserves the commutator operation. In particular, if $\mathbf{A} = \mathbf{A}_0 \times \mathbf{A}_1$, and $\theta_i, \varphi_i \in Con(\mathbf{A}_i), i = 0, 1$, then

$$[\theta_0 \times \theta_1, \varphi_0 \times \varphi_1] = [\theta_0, \varphi_0] \times [\theta_1, \varphi_1].$$

Moreover if $\prod_{i\in I} \theta_i = \{(a,b) \in A \times A : (a_i,b_i) \in \theta_i$ for all $i \in I\}$, then

(ii) $[\prod_{i\in I} \theta_i, \prod_{i\in I} \varphi_i] \subseteq \prod_{i\in I} [\theta_i, \varphi_i]$.

Proof.

Let g be the map defined in (i) above. Clearly, g is order-preserving. It follows that $g((\theta_i)_{i\in I}) \vee g((\varphi_i)_{i\in I}) \subseteq g((\theta_i)_{i\in I} \vee (\varphi_i)_{i\in I}) = g((\theta_i \vee \varphi_i)_{i\in I})$, for any $(\varphi_i)_{i\in I} \in \prod_{i\in I} Con(\mathbf{A}_i)$.

We show g is a lattice homomorphism.

Clearly, for $(\theta_i)_{i\in I}, (\varphi_i)_{i\in I} \in \prod_{i\in I} Con(\mathbf{A}_i)$, $g((\theta_i)_{i\in I} \wedge (\varphi_i)_{i\in I}) = g((\theta_i \cap \varphi_i)_{i\in I}) = g((\theta_i)_{i\in I}) \cap g((\varphi_i)_{i\in I})$. We show for $(\theta_i)_{i\in I}, (\varphi_i)_{i\in I} \in \prod_{i\in I} Con(\mathbf{A}_i)$, $g((\theta_i \vee \varphi_i)_{i\in I}) = g((\theta_i)_{i\in I}) \vee g((\varphi_i)_{i\in I})$. For this it suffices (by the above) to show $g((\theta_i \vee \varphi_i)_{i\in I}) \subseteq g((\theta_i)_{i\in I}) \vee g((\varphi_i)_{i\in I})$. Let $(x,y) \in g((\theta_i \vee \varphi_i)_{i\in I})$. Then $(x(i), y(i)) \in \theta_i \vee \varphi_i$ for all $i \in I$, and $x(i) = y(i)$ for all but finitely many $i \in I$.

Let $i_1, \ldots, i_n \in I$ be such that $x(i) = y(i)$ if $i \notin \{i_1, \ldots, i_n\}$. Then for all $i \notin \{i_1, \ldots, i_n\}, (x(i), y(i)) \in \theta_i, \varphi_i$. For all $i \in \{i_1, \ldots, i_n\}, (x(i), y(i)) \in$

$\theta_i \vee \varphi_i$ so for each $(x(i_j), y(i_j)), j \in \{1, \ldots, n\}$ there exist $c_{j,0}, c_{j,1}, \ldots, c_{j,k_j}$ such that $c_{j,0} = x(i_j), c_{j,k} = y(i_j)$ and for odd $m, (c_{j,m-1}, c_{j,m}) \in \theta_{i_j}$; for even $m, (c_{j,m-1}, c_{j,m}) \in \varphi_{i_j},\ m \in \{0, 1, \ldots, k_j\}$.

Let $m' = \max\{k_1, \ldots, k_n\}$ and for all $j \in \{1, \ldots, n\}$, define $c_{j,l} = c_{j,k_j}$ whenever $k_j < l \leq m'$. For $l = 0, 1, \ldots, m'$, define $d_l \in A$ by

$$d_l(j) = \begin{cases} c_{j,l} & \text{for } j \in \{i_1, \ldots, i_n\} \\ x(j) & \text{for } j \notin \{i_1, \ldots, i_n\}. \end{cases}$$

Then for odd $l \in \{1, \ldots, m'\}, (d_{l-1}(i), d_l(i)) \in \theta_i$ for all $i \in I$, while for $i \notin \{i_1, \ldots, i_n\}, d_{l-1}(i) = d_l(i)$. For even $l \in \{1, \ldots, m'\}, (d_{l-1}(i), d_l(i)) \in \varphi_i$ for all $i \in I$, while for all $i \notin \{i_1, \ldots, i_n\}, d_{l-1}(i) = d_l(i)$. Now $d_0 = x, d_{m'} = y$ and for odd $l \in \{1, \ldots, m'\}, (d_{l-1}, d_l) \in g((\theta_i)_{i\in I})$ and for even $l \in \{1, \ldots, m'\}, (d_{l-1}, d_l) \in g((\varphi_i)_{i\in I})$. Therefore $(x, y) \in g((\theta_i)_{i\in I}) \vee g((\varphi_i)_{i\in I})$. We now have $g((\theta_i \vee \varphi_i)_{i\in I}) \subseteq g((\theta_i)_{i\in I}) \vee g((\varphi_i)_{i\in I})$, so equality follows.

We show g is one-to-one.

Suppose $(\theta_i)_{i\in I} \neq (\varphi_i)_{i\in I}$. Then there exists some $j \in J$ such that $\theta_j \neq \varphi_j$, say there exists some $(a_j, b_j) \in \theta_j$ such that $(a_j, b_j) \notin \varphi_j$. Define $a, b \in A$ by

$$\begin{aligned} a(i) &= a_j \text{ for all } i \in I, \\ b(i) &= \begin{cases} a_j & \text{for } i \neq j \\ b_j & \text{for } i = j. \end{cases} \end{aligned}$$

Then $(a, b) \in g((\theta_i)_{i\in I})$ but $(a, b) \notin g((\varphi_i)_{i\in I})$, since $(a_j, b_j) \notin \varphi_j$ so $g((\theta_i)_{i\in I}) \neq g((\varphi_i)_{i\in I})$. The map g is therefore a lattice isomorphism from $\prod_{i\in I} Con(\mathbf{A}_i)$ into $Con(\mathbf{A})$.

Let $\lambda = \{(a, b) \in A \times A : a(i) = b(i)$ for all but finitely many $i \in I\}$. Let p_i be the i^{th} projection homomorphism from $\mathbf{A} = \prod_{i\in I} \mathbf{A}_i$ to $\mathbf{A}_i$ and let η_i be its kernel. (Therefore for all $i \in I$, if $\theta_i \in Con(\mathbf{A}_i)$ then $p_i^{-1}(\theta_i) \in Con(\mathbf{A})$.)

For $\theta_i \in Con(\mathbf{A}_i)$ let $\bar{\theta}_i = p_i^{-1}(\theta_i) = \{(a, b) \in A \times A : (p_i(a), p_i(b)) \in \theta_i\}$. g (as defined in (i)) sends $(\theta_i)_{i\in I}$ to $\{(a, b) \in A \times A : (a(i), b(i)) \in \theta_i$ for all $i \in I$ and $a_i = b_i$ for all but finitely many $i \in I\}$, i.e., g sends $(\theta_i)_{i\in I}$ to $\lambda \cap (\cap_{i\in I} p_i^{-1}(\theta_i)) = \lambda \cap (\cap_{i\in I} \bar{\theta}_i)$.

We show $[g((\theta_i)_{i\in I}), g((\varphi_i)_{i\in I})] = g(([\theta_i, \varphi_i])_{i\in I})$.

Let $\alpha = [g((\theta_i)_{i\in I}), g((\varphi_i)_{i\in I})] = [\lambda \cap (\cap_{i\in I} \bar{\theta}_i), \lambda \cap (\cap_{i\in I} \bar{\varphi}_i)]$ by the above argument. Let $\beta = g(([\theta_i, \varphi_i])_{i\in I}) = \lambda \cap (\cap_{i\in I} \overline{[\theta_i, \varphi_i]})$. Clearly $p_i(p_i^{-1}(\theta_i)) = \theta_i$, since p_i is onto. Now for all $i \in I, \eta_i = ker(p_i) \subseteq p_i^{-1}(\theta_i)$. .... (1)

By Proposition 2.14 (i), $[\bar{\theta}_i, \bar{\varphi}_i] \vee \eta_i = p_i^{-1}([p_i(\bar{\theta}_i \vee \eta_i), p_i(\bar{\varphi}_i \vee \eta_i)])$

$= p_i^{-1}([p_i(p_i^{-1}(\theta_i) \vee \eta_i), p_i(p_i^{-1}(\varphi_i) \vee \eta_i)])$

$= p_i^{-1}([p_i(p_i^{-1}(\theta_i)), p_i(p_i^{-1}(\varphi_i))])$ (by (1))
$= p_i^{-1}([\theta_i, \varphi_i])$
$= \overline{[\theta_i, \varphi_i]}$ so $\beta = \lambda \cap (\cap_{i\in I}([\bar{\theta}_i, \bar{\varphi}_i] \vee \eta_i))$.

We show $\alpha \subseteq \beta$.

$\alpha = [\lambda\cap(\cap_{i\in I}\bar{\theta}_i), \lambda\cap(\cap_{i\in I}\bar{\varphi}_i)] \subseteq (\lambda\cap(\cap_{i\in I}\bar{\theta}_i))\cap(\lambda\cap(\cap_{i\in I}\bar{\varphi}_i))$ by Proposition 2.9 (i), so $\alpha \subseteq \lambda$. Now $\cap_{i\in I}\bar{\theta}_i \subseteq \bar{\theta}_i$ for each $i \in I$ so $\lambda \cap (\cap_{i\in I}\bar{\theta}_i) \subseteq \bar{\theta}_i$ for all $i \in I$. Similarly, $\lambda\cap(\cap_{i\in I}\bar{\varphi}_i) \subseteq \bar{\varphi}_i$ for all $i \in I$. By order-preservation (Proposition 2.9 (ii)), $\alpha \subseteq [\bar{\theta}_i, \bar{\varphi}_i]$ for all $i \in I$, therefore $\alpha \subseteq \lambda \cap (\cap_{i\in I}([\bar{\theta}_i, \bar{\varphi}_i] \vee \eta_i)) = \beta$.

We show $\beta \subseteq \alpha$.

For each $i \in I$, let $\eta_i^{'} = \{(a, b) \in A \times A : a(j) = b(j) \text{ for all } j \neq i\}$. We first show $\lambda \cap (\cap_{i\in I}\bar{\theta}_i) = \bigvee_{i\in I}(\bar{\theta}_i \cap \eta_i^{'})$. Clearly, $\bigvee_{i\in I}(\bar{\theta}_i \cap \eta_i^{'}) \subseteq \lambda \cap (\cap_{i\in I}\bar{\theta}_i)$.

Let $(a, b) \in \lambda \cap (\cap_{i\in I}\bar{\theta}_i)$. Since $(a, b) \in \lambda$, there are distinct $i_1, \ldots, i_n \in I$ such that $a(i) = b(i)$ if $i \notin \{i_1, \ldots, i_n\}$. Define $a^0, a^1, \ldots, a^n \in A$ by

$$\begin{aligned}
a^0 &= a, \\
a^1(i) &= \left\{ \begin{array}{ll} a(i) & \text{if } i \neq i_1 \\ b(i) & \text{if } i = i_1 \end{array} \right\}, \\
a^2(i) &= \left\{ \begin{array}{ll} a^1(i) & \text{if } i \neq i_2 \\ b(i) & \text{if } i = i_2 \end{array} \right\}, \ldots, \\
a^{n-1}(i) &= \left\{ \begin{array}{ll} a^{(n-2)}(i) & \text{if } i \neq i_{n-1} \\ b(i) & \text{if } i = i_{n-1} \end{array} \right\}, \\
a^n(i) &= \left\{ \begin{array}{ll} a^{(n-1)}(i) & \text{if } i \neq i_n \\ b(i) & \text{if } i = i_n \end{array} \right\}. \quad \text{Then } a^n = b.
\end{aligned}$$

For $j = 1, 2, \ldots, n$, by the above definition, $(a^{j-1}(i_j), a^j(i_j)) = (a(i_j), b(i_j)) \in \theta_{i_j}$ since $(a(i), b(i)) \in \theta_i$ for all $i \in I$, therefore $(a^{j-1}, a^j) \in \bar{\theta}_{i_j}$. Also $p_i(a^{j-1}) = p_i(a^j)$ for all $i \neq i_j$, therefore $(a^{j-1}, a^j) \in \eta_{i_j}^{'}$.

We now have $(a, b) \in (\bar{\theta}_{i_1} \cap \eta_{i_1}^{'}) \circ \ldots \circ (\bar{\theta}_{i_n} \cap \eta_{i_n}^{'}) \subseteq (\bar{\theta}_{i_1} \cap \eta_{i_1}^{'}) \vee \ldots \vee (\bar{\theta}_{i_n} \cap \eta_{i_n}^{'})$. Thus $\lambda \cap (\cap_{i\in I}\bar{\theta}_i) \subseteq \bigvee_{i\in I}(\bar{\theta}_i \cap \eta_i^{'})$. Since $\lambda \cap (\cap_{i\in I}\bar{\theta}_i) = \bigvee_{i\in I}(\bar{\theta}_i \cap \eta_i^{'})$, for any $(\theta_i)_{i\in I}$, it follows that $\beta = \lambda\cap(\cap_{i\in I}\overline{[\theta_i, \varphi_i]}) = \bigvee_{i\in I}(\overline{[\theta_i, \varphi_i]}\cap\eta_i^{'}) = \bigvee_{i\in I}(([\bar{\theta}_i, \bar{\varphi}_i] \vee \eta_i)\cap\eta_i^{'})$. Now because $\eta_i \subseteq \bar{\theta}_i$ we have $(\bar{\theta}_i\cap\eta_i^{'})\vee\eta_i = \bar{\theta}_i\cap(\eta_i^{'}\vee\eta_i)$ by modularity. Let $(c, d) \in \bar{\theta}_i$. Then $(c(i), d(i)) \in \theta_i$.

Define $a \in A$ as follows: $a(j) = d(j)$ for all $j \neq i$ and $a(i) = c(i)$. Then $(c, a) \in \eta_i$ and $(a, d) \in \eta_i^{'}$ so $(c, d) \in \eta_i \vee \eta_i^{'}$. Therefore $\bar{\theta}_i \subseteq \eta_i \vee \eta_i^{'}$ and $\bar{\theta}_i \cap (\eta_i \vee \eta_i^{'}) = \bar{\theta}_i$, so $\bar{\theta}_i = (\bar{\theta}_i \cap \eta_i^{'}) \vee \eta_i$. This means

$[\bar{\theta}_i, \bar{\varphi}_i] \vee \eta_i = [(\bar{\theta}_i \cap \eta_i^{'}) \vee \eta_i, (\bar{\varphi}_i \cap \eta_i^{'}) \vee \eta_i] \vee \eta_i$

$= [\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i'] \vee [\eta_i, \bar{\varphi}_i \cap \eta_i'] \vee [\bar{\theta}_i \cap \eta_i', \eta_i] \vee [\eta_i, \eta_i] \vee \eta_i$ ....(2)

by additivity (Proposition 2.12).

Now $[\eta_i', \eta_i] \subseteq \eta_i' \cap \eta_i = id_A$ so $[\eta_i', \eta_i] = id_A$. $[\bar{\theta}_i \cap \eta_i', \eta_i] \subseteq \bar{\theta}_i \cap \eta_i' \cap \eta_i = \bar{\theta}_i \cap id_A = id_A$ so $[\bar{\theta}_i \cap \eta_i', \eta_i] = id_A$. Similarly, $[\eta_i, \bar{\varphi}_i \cap \eta_i'] = id_A$. By Proposition 2.9 (i), $[\eta_i, \eta_i] \subseteq \eta_i \cap \eta_i = \eta_i$ so the right hand side of (2) becomes $[\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i'] \vee \eta_i$. We therefore have $\beta = \bigvee_{i \in I}(([\bar{\theta}_i, \bar{\varphi}_i] \vee \eta_i) \cap \eta_i') = \bigvee_{i \in I}(([\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i'] \vee \eta_i) \cap \eta_i')$. By Proposition 2.9 (i), $[\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i'] \subseteq \bar{\theta}_i \cap \eta_i' \cap \bar{\varphi}_i \cap \eta_i' = \bar{\theta}_i \cap \bar{\varphi}_i \cap \eta_i' \subseteq \eta_i'$.

We show $([\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i'] \vee \eta_i) \cap \eta_i' = [\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i']$.
$([\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i'] \vee \eta_i) \cap \eta_i' = [\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i'] \vee (\eta_i \cap \eta_i')$ by modularity since $[\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i'] \subseteq \eta_i'$, so $([\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i'] \vee \eta_i) \cap \eta_i' = [\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i']$ since $(\eta_i \cap \eta_i') = id_A$, and so $\beta = \bigvee_{i \in I}[\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i']$.

We have previously noted for all $i \in I, \bar{\theta}_i \cap \eta_i' \subseteq \lambda \cap (\cap_{i \in I}\bar{\theta}_i)$ so for all $i \in I, [\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i'] \subseteq [\lambda \cap (\cap_{i \in I}\bar{\theta}_i), \lambda \cap (\cap_{i \in I}\bar{\varphi}_i)]$ by order-preservation. Therefore $\bigvee_{i \in I}[\bar{\theta}_i \cap \eta_i', \bar{\varphi}_i \cap \eta_i'] \subseteq [\lambda \cap (\cap_{i \in I}\bar{\theta}_i), \lambda \cap (\cap_{i \in I}\bar{\varphi}_i)]$, i.e., $\beta \subseteq \alpha$, whence $\beta = \alpha$.

Now suppose $\mathbf{A} = \mathbf{A}_0 \times \mathbf{A}_1$. Let $\theta_i, \varphi_i \in Con(\mathbf{A}_i), i = 0, 1$. As a special case of the above (with $I = \{0, 1\}$), we get $g(([\theta_i, \varphi_i])_{i \in \{0,1\}}) = [\theta_0, \varphi_0] \times [\theta_1, \varphi_1]$.

(ii) Let $\mathbf{A}_i \in V$, let $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$ and $\theta_i \in Con(\mathbf{A}), i \in I$.

Now $\prod_{i \in I} \theta_i = \{(a, b) \in A^2 : (a(i), b(i)) \in \theta_i \text{ for all } i \in I\} = \cap_{i \in I}\bar{\theta}_i$ and by Proposition 2.14 (i), $\overline{[\theta_i, \varphi_i]} = p_i^{-1}[\theta_i, \varphi_i] = [\bar{\theta}_i, \bar{\varphi}_i] \vee \eta_i$. $\prod_{i \in I}[\theta_i, \varphi_i] = \cap_{i \in I}\overline{[\theta_i, \varphi_i]} = \cap_{i \in I}([\bar{\theta}_i, \bar{\varphi}_i] \vee \eta_i)$ and $[\prod_{i \in I} \theta_i, \prod_{i \in I} \varphi_i] = [\cap_{i \in I}\bar{\theta}_i, \cap_{i \in I}\bar{\varphi}_i]$. For each $i \in I, \cap_{i \in I}\bar{\theta}_i \subseteq \bar{\theta}_i$ and $\cap_{i \in I}\bar{\varphi}_i \subseteq \bar{\varphi}_i$ so $[\cap_{i \in I}\bar{\theta}_i, \cap_{i \in I}\bar{\varphi}_i] \subseteq [\bar{\theta}_i, \bar{\varphi}_i]$. By order-preservation $[\cap_{i \in I}\bar{\theta}_i, \cap_{i \in I}\bar{\varphi}_i] \subseteq \cap_{i \in I}([\bar{\theta}_i, \bar{\varphi}_i] \vee \eta_i)$.

□

2.4 Equivalence of Commutator Definitions. In the next section, for an algebra $\mathbf{A}$ in a modular variety V and for fixed $\theta, \varphi \in Con(\mathbf{A})$, we regard θ and φ as subalgebras of $\mathbf{A}^2$ and denote them by $\mathbf{A}(\theta)$ and $\mathbf{A}(\varphi)$ respectively. We denote elements $(x, y) \in A(\theta)$ as

$$\begin{bmatrix} x \\ y \end{bmatrix},$$

i.e., as column vectors, while the elements of $A(\varphi)$ are considered to be row vectors.

We shall define congruence relations $\Delta_{\theta,\varphi}$ and $\Delta^{\theta,\varphi}$. We show $\Delta_{\theta,\varphi}$ to be the least transitive relation containing $M(\theta, \varphi)$ (as defined in the previous section) and that, in a suitable sense, $\Delta_{\theta,\varphi} = \Delta^{\theta,\varphi}$. Using these congruences, we show, following [FM87], that $[\theta, \varphi]$ (as defined here) coincides with the commutator originally defined by Hagemann and Herrmann [HH79] for modular varieties. (Condition (iv) of Theorem 2.25 defines the Hagemann - Herrmann commutator.)

Definition 2.18.

(i) Let $\mathbf{A}$ be an algebra and let $\theta, \varphi \in Con(\mathbf{A})$. $\mathbf{A}(\theta, \varphi)$ is the subalgebra of $\mathbf{A}^4$ whose universe is

$$\{(a,b,c,d) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in A^4 : \begin{bmatrix} a \\ c \end{bmatrix}, \begin{bmatrix} b \\ d \end{bmatrix} \in \theta,\ (a,b),(c,d) \in \varphi\},$$

i.e., its elements are those of A^4 whose columns are in θ and whose rows are in φ.

(ii) $\Delta_{\theta,\varphi}$ is the congruence relation on $\mathbf{A}(\theta)$ generated by the set

$$\{\left(\begin{bmatrix} u \\ u \end{bmatrix}, \begin{bmatrix} v \\ v \end{bmatrix}\right) : \begin{bmatrix} u & v \\ u & v \end{bmatrix} \in A(\theta, \varphi)\}.$$

(iii) $\Delta^{\theta,\varphi}$ is the congruence relation on $\mathbf{A}(\varphi)$ generated by

$$\{((x,x),(y,y)) : \begin{bmatrix} x & x \\ y & y \end{bmatrix} \in A(\theta, \varphi)\}.$$

From this definition we see that $\mathbf{A}(\theta, \varphi)$ can be regarded as a subalgebra of $\mathbf{A}(\theta) \times \mathbf{A}(\theta)$, a set of pairs of columns, or of $\mathbf{A}(\varphi) \times \mathbf{A}(\varphi)$, a set of pairs of rows. We use

$$\begin{bmatrix} x & r \\ y & s \end{bmatrix} \in \Delta_{\theta,\varphi} \text{ to abbreviate } \left(\begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} r \\ s \end{bmatrix}\right) \in \Delta_{\theta,\varphi}.$$

We also use

$$\begin{bmatrix} x & r \\ y & s \end{bmatrix} \in \Delta^{\theta,\varphi} \text{ to abbreviate } ((x,r),(y,s)) \in \Delta^{\theta,\varphi}.$$

Remark 2.19.

Consider $M(\theta, \varphi)$ as a relation on $\mathbf{A}(\theta)$, i.e.,
$M(\theta, \varphi) = \{((t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1)), (t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2))) : \mathbf{a}^i, i = 1, 2,$ is a sequence of n elements of $A, \mathbf{b}^i, i = 1, 2,$ is a sequence of m elements of A, $m, n > 0$, where $a^1_k \theta a^2_k$ and $b^1_j \varphi b^2_j$ for $k \leq n$ and $j \leq m$, and t is a $(n+m)$-ary term$\}$.

This means $M(\theta, \varphi) \subseteq \theta \times \theta = A(\theta) \times A(\theta)$, which is a subuniverse of $\mathbf{A}^4$. By Proposition 2.8 (i), $M(\theta, \varphi)$ is a subuniverse of $\mathbf{A}^4$, so it is also a subuniverse of $\mathbf{A}(\theta) \times \mathbf{A}(\theta)$. Clearly, $M(\theta, \varphi)$ is also a reflexive and symmetric relation on $\mathbf{A}(\theta)$, so, as a set of pairs of columns, $M(\theta, \varphi)$ is a tolerance on $\mathbf{A}(\theta)$. Similarly, when considered as a set of pairs of rows, $M(\theta, \varphi)$ is a tolerance on $\mathbf{A}(\varphi)$.

Lemma 2.20. *Let θ, φ be congruence relations on $\mathbf{A} \in V$ where V is a modular variety. Then $\Delta^{\theta,\varphi}$ (regarded as a set of pairs of rows) is the least transitive relation on $\mathbf{A}(\varphi)$ containing $M(\theta, \varphi)$.*

Proof.

Consider $M(\theta, \varphi)$ as a relation on $\mathbf{A}(\varphi)$, i.e., $M(\theta, \varphi) = \{((t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2)), (t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1), t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2)))$: $\mathbf{a}^i, i = 1, 2$, is a sequence of n elements of A, $\mathbf{b}^i, i = 1, 2$ is a sequence of m elements of A, $m, n > 0$, where $a_k^1 \theta a_k^2$ and $b_j^1 \varphi b_j^2$ for $k \leq n$ and $j \leq m$, and t is a $(n+m)$-ary term$\}$. Then $M(\theta, \varphi) \subseteq \varphi \times \varphi = A(\varphi) \times A(\varphi)$. Since $M(\theta, \varphi)$ is a tolerance on $\mathbf{A}(\varphi)$ its transitive closure is $\Theta^{\mathbf{A}(\varphi)}(M(\theta, \varphi))$ by Theorem 0.12.

Let a be an element of the form

$$((x, x), (y, y)) = \begin{bmatrix} x & x \\ y & y \end{bmatrix} \text{ with } (x, y) \in \theta.$$

$$\begin{bmatrix} x & x \\ y & y \end{bmatrix} = ((x, x), (y, y)) \in M(\theta, \varphi)$$

by Proposition 2.8 (i) so $M(\theta, \varphi)$ contains a generating set of $\Delta^{\theta,\varphi}$ therefore $\Theta^{\mathbf{A}(\varphi)}(M(\theta, \varphi))$ contains a generating set of $\Delta^{\theta,\varphi}$, therefore $\Delta^{\theta,\varphi} \subseteq \Theta^{\mathbf{A}(\varphi)}(M(\theta, \varphi))$.

$$\text{If } x = ((b, b'), (b, b')) = \begin{bmatrix} b & b' \\ b & b' \end{bmatrix} \text{with } (b, b') \in \varphi$$

or

$$x = ((a, a), (a', a')) = \begin{bmatrix} a & a \\ a' & a' \end{bmatrix} \text{with } (a, a') \in \theta$$

then, by Definition 2.18, $x \in \Delta^{\theta,\varphi}$ so as a subuniverse of $\mathbf{A}(\varphi) \times \mathbf{A}(\varphi)$, $\Delta^{\theta,\varphi}$ contains a generating set of $M(\theta, \varphi)$, so $\Delta^{\theta,\varphi} \supseteq M(\theta, \varphi)$, hence $\Delta^{\theta,\varphi} \supseteq \Theta^{\mathbf{A}(\varphi)}(M(\theta, \varphi))$.

□

Lemma 2.21. [FM87, Lemma 4.8]

Let θ, φ be congruence relations on $\mathbf{A} \in V$ where V is a modular variety. Then $\Delta_{\theta,\varphi}$ (regarded as a set of pairs of columns) is the least transitive relation on $\mathbf{A}(\theta)$ containing $M(\theta, \varphi)$.

The proof of this lemma will not be included as it is the dual of the proof of the previous lemma.

Proposition 2.22. [FM87, Exercise 4.3]

Let V be a modular variety and let θ, φ be congruence relations on $\mathbf{A} \in V$. If Δ is either $\Delta_{\theta,\varphi}$ or $\Delta^{\theta,\varphi}$ then

(i)

$$\begin{bmatrix} x & y \\ x & y \end{bmatrix} \in \Delta \textit{ if and only if } (x, y) \in \varphi,$$

(ii)

$$\begin{bmatrix} x & x \\ u & u \end{bmatrix} \in \Delta \textit{ if and only if } (x, u) \in \theta,$$

(iii)

$$\begin{bmatrix} x & y \\ u & v \end{bmatrix} \in \Delta \textit{ implies} \begin{bmatrix} x & y \\ x & y \end{bmatrix}, \begin{bmatrix} x & x \\ u & u \end{bmatrix}, \begin{bmatrix} u & v \\ x & y \end{bmatrix}, \begin{bmatrix} y & x \\ v & u \end{bmatrix} \in \Delta.$$

Proof.

(i) Let

$$\begin{bmatrix} x & y \\ x & y \end{bmatrix} \in \Delta_{\theta,\varphi}$$

which is the transitive closure of $M(\theta, \varphi)$, (regarded as a set of pairs of columns), in $\mathbf{A}(\theta)$ by Lemma 2.21. Then there are $(z_0, w_0), \ldots, (z_m, w_m) \in \theta$ such that

$$\begin{bmatrix} x \\ x \end{bmatrix} = \begin{bmatrix} z_0 \\ w_0 \end{bmatrix} \overset{M(\theta,\varphi)}{\equiv} \begin{bmatrix} z_1 \\ w_1 \end{bmatrix} \overset{M(\theta,\varphi)}{\equiv} \cdots \overset{M(\theta,\varphi)}{\equiv} \begin{bmatrix} z_m \\ w_m \end{bmatrix} = \begin{bmatrix} y \\ y \end{bmatrix}$$

so $x = z_0 \varphi z_1 \varphi \ldots \varphi z_m = y$ so $(x, y) \in \varphi$ by transitivity of φ.

Conversely, $(x, y) \in \varphi$ implies

$$\begin{bmatrix} x & y \\ x & y \end{bmatrix} \in M(\theta, \varphi) \subseteq \Delta_{\theta,\varphi}.$$

$$\begin{bmatrix} x & y \\ x & y \end{bmatrix} \in \Delta^{\theta,\varphi}$$

means $((x,y),(x,y)) \in \Delta^{\theta,\varphi} \subseteq \varphi \times \varphi$ which implies $(x,y) \in \varphi$.

Conversely, $(x,y) \in \varphi$ implies $((x,y),(x,y)) \in R$ for any reflexive relation R on $\mathbf{A}(\varphi)$ so $((x,y),(x,y)) \in \Delta^{\theta,\varphi}$, i.e.,

$$\begin{bmatrix} x & y \\ x & y \end{bmatrix} \in \Delta^{\theta,\varphi}.$$

(ii) is proved similarly; reverse the roles played by rows and columns in (i).

(iii) Let

$$\begin{bmatrix} x & y \\ u & v \end{bmatrix} \in \Delta_{\theta,\varphi},$$

which is the transitive closure of $M(\theta,\varphi)$ (a set of pairs of columns), in $\mathbf{A}(\theta)$ by Lemma 2.21, so as above, $(x,y) \in \varphi$. Then by (i),

$$\begin{bmatrix} x & y \\ x & y \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

Since $\Delta_{\theta,\varphi} \subseteq \theta \times \theta$, we also have $(x,u) \in \theta$ so by (ii),

$$\begin{bmatrix} x & x \\ u & u \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

Now $\Delta_{\theta,\varphi}$ is symmetric, so

$$\begin{bmatrix} x & y \\ u & v \end{bmatrix} \in \Delta_{\theta,\varphi} \text{ implies } \begin{bmatrix} y & x \\ v & u \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

Now

$$\begin{bmatrix} x & y \\ u & v \end{bmatrix} \in \Delta_{\theta,\varphi}$$

implies that there are $(z_0,w_0),\ldots,(z_m,w_m) \in \theta$ such that

$$\begin{bmatrix} x \\ u \end{bmatrix} = \begin{bmatrix} z_0 \\ w_0 \end{bmatrix} \overset{M(\theta,\varphi)}{\equiv} \begin{bmatrix} z_1 \\ w_1 \end{bmatrix} \overset{M(\theta,\varphi)}{\equiv} \cdots \overset{M(\theta,\varphi)}{\equiv} \begin{bmatrix} z_m \\ w_m \end{bmatrix} = \begin{bmatrix} y \\ v \end{bmatrix}$$

i.e.,

$$\begin{bmatrix} z_i & z_{i+1} \\ w_i & w_{i+1} \end{bmatrix} \in M(\theta,\varphi),\ i = 0,1,\ldots,m-1. \text{ Therefore}$$

$$\begin{bmatrix} w_i & w_{i+1} \\ z_i & z_{i+1} \end{bmatrix} \in M(\theta,\varphi),\ i = 0,1,\ldots,m-1 \text{ by definition of } M(\theta,\varphi)$$

so
$$\begin{bmatrix} u \\ x \end{bmatrix} = \begin{bmatrix} w_0 \\ z_0 \end{bmatrix} \overset{M(\theta,\varphi)}{\equiv} \begin{bmatrix} w_1 \\ z_1 \end{bmatrix} \overset{M(\theta,\varphi)}{\equiv} \cdots \overset{M(\theta,\varphi)}{\equiv} \begin{bmatrix} w_m \\ z_m \end{bmatrix} = \begin{bmatrix} v \\ y \end{bmatrix}$$
so
$$\left(\begin{bmatrix} u \\ x \end{bmatrix}, \begin{bmatrix} v \\ y \end{bmatrix} \right)$$
is an element of the transitive closure of $M(\theta, \varphi)$, i.e.,
$$\begin{bmatrix} u & v \\ x & y \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

The corresponding claims for $\Delta^{\theta,\varphi}$ are proved in a dual manner. □

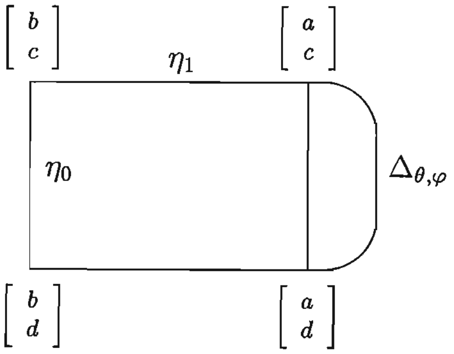
Lemma 2.23. [FM87, Exercise 4.4]

Let θ, φ be congruence relations on $\mathbf{A} \in V$, where V is a modular variety.
$$\textit{If } \begin{bmatrix} a & a \\ c & d \end{bmatrix} \in \Delta_{\theta,\varphi} \textit{ and } \begin{bmatrix} a \\ b \end{bmatrix} \in \theta, \textit{ then } \begin{bmatrix} b & b \\ c & d \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

Proof.

Let
$$\begin{bmatrix} a & a \\ c & d \end{bmatrix} \in \Delta_{\theta,\varphi} \text{ and } \begin{bmatrix} a \\ b \end{bmatrix} \in \theta.$$
We have $(a, c), (a, d), (a, b) \in \theta$ so, by symmetry of θ, $(b, a), (a, c) \in \theta$ and $(b, a), (a, d) \in \theta$ and so $(b, c), (b, d) \in \theta$ by transitivity.

Let $\eta_0, \eta_1 \in Con(\mathbf{A}(\theta))$ be the kernels of the first and second projections p_0, p_1 from $\mathbf{A}(\theta)$ onto $\mathbf{A}$. Then $\eta_0 \cap \eta_1 = id_{\mathbf{A}(\theta)} \subseteq \Delta_{\theta,\varphi}$ and we have the following diagram:


$\begin{bmatrix} b \\ c \end{bmatrix}$
η_1
$\begin{bmatrix} a \\ c \end{bmatrix}$
η_0
$\Delta_{\theta,\varphi}$
$\begin{bmatrix} b \\ d \end{bmatrix}$
$\begin{bmatrix} a \\ d \end{bmatrix}$

By the Shifting Lemma (Lemma 2.2),
$$\begin{bmatrix} b & b \\ c & d \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

□

Theorem 2.24. [FM87, Exercise 4.5]

Let $\theta, \varphi \in Con(\mathbf{A})$, $\mathbf{A} \in V$, where V is a modular variety. Then

(i) The relation

$$\eta = \{((x,y),(u,v)) : \begin{bmatrix} x & y \\ u & v \end{bmatrix} \in \Delta_{\theta,\varphi}\}$$

is transitive. We express this by saying that $\Delta_{\theta,\varphi}$ is a transitive relation on $\mathbf{A}(\varphi)$.

(ii) The relation η defined in (i) is equal to $\Delta^{\theta,\varphi}$. We express this as $\Delta_{\theta,\varphi} = \Delta^{\theta,\varphi}$.

Proof.

Let $((x,y),(u,v)),((u,v),(r,s)) \in \eta$, i.e.,

$$\begin{bmatrix} x & y \\ u & v \end{bmatrix}, \begin{bmatrix} u & v \\ r & s \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

Then $(x,u),(u,r) \in \theta$ so $(x,r) \in \theta$; $(y,v),(v,s) \in \theta$ so $(y,s) \in \theta$ and we can show $(x,y),(u,v),(r,s) \in \varphi$ (by Lemma 2.21 as in Proposition 2.22 (i)).

$$\text{Let } a = \begin{bmatrix} x \\ r \end{bmatrix}, b = \begin{bmatrix} x \\ u \end{bmatrix}, c = \begin{bmatrix} y \\ s \end{bmatrix}, d = \begin{bmatrix} y \\ v \end{bmatrix}, \text{let } \Delta = \Delta_{\theta,\varphi}.$$

Now

$$(b,d) = \begin{bmatrix} x & y \\ u & v \end{bmatrix} \in \Delta$$

by assumption and since

$$\begin{bmatrix} u \\ r \end{bmatrix} \Delta \begin{bmatrix} v \\ s \end{bmatrix}$$

and

$$\begin{bmatrix} u \\ u \end{bmatrix} \Delta \begin{bmatrix} v \\ v \end{bmatrix}$$

(by Definition 2.18). Let $m_1, \ldots, m_n$ be Day terms for V as described in Theorem 2.1. By compatibility,

$$m_i^{\mathbf{A}^2}\left(\begin{bmatrix} u \\ r \end{bmatrix}, \begin{bmatrix} u \\ u \end{bmatrix}, \begin{bmatrix} v \\ v \end{bmatrix}, \begin{bmatrix} v \\ s \end{bmatrix}\right) \Delta\, m_i^{\mathbf{A}^2}\left(\begin{bmatrix} u \\ r \end{bmatrix}, \begin{bmatrix} u \\ u \end{bmatrix}, \begin{bmatrix} u \\ u \end{bmatrix}, \begin{bmatrix} u \\ r \end{bmatrix}\right)$$

so

$$\begin{bmatrix} m_i^{\mathbf{A}}(u,u,v,v) \\ m_i^{\mathbf{A}}(r,u,v,s) \end{bmatrix} \Delta \begin{bmatrix} u \\ r \end{bmatrix}$$

by Theorem 2.1 (ii).

Since

$$\left(\begin{bmatrix} u \\ r \end{bmatrix}, \begin{bmatrix} u \\ r \end{bmatrix}\right), \left(\begin{bmatrix} u \\ r \end{bmatrix}, \begin{bmatrix} v \\ s \end{bmatrix}\right), \left(\begin{bmatrix} v \\ s \end{bmatrix}, \begin{bmatrix} v \\ s \end{bmatrix}\right), \left(\begin{bmatrix} v \\ s \end{bmatrix}, \begin{bmatrix} u \\ r \end{bmatrix}\right) \in \Delta,$$

we have

$$m_i^{\mathbf{A}^2}\left(\begin{bmatrix} u \\ r \end{bmatrix}, \begin{bmatrix} u \\ r \end{bmatrix}, \begin{bmatrix} v \\ s \end{bmatrix}, \begin{bmatrix} v \\ s \end{bmatrix}\right) \Delta\, m_i^{\mathbf{A}^2}\left(\begin{bmatrix} u \\ r \end{bmatrix}, \begin{bmatrix} v \\ s \end{bmatrix}, \begin{bmatrix} v \\ s \end{bmatrix}, \begin{bmatrix} u \\ r \end{bmatrix}\right).$$

Therefore

$$\begin{bmatrix} m_i^{\mathbf{A}}(u,u,v,v) \\ m_i^{\mathbf{A}}(r,r,s,s) \end{bmatrix} \Delta \begin{bmatrix} u \\ r \end{bmatrix}$$

(Theorem 2.1 (ii)) and so by transitivity

$$\begin{bmatrix} m_i^{\mathbf{A}}(u,u,v,v) \\ m_i^{\mathbf{A}}(r,u,v,s) \end{bmatrix} \Delta \begin{bmatrix} m_i^{\mathbf{A}}(u,u,v,v) \\ m_i^{\mathbf{A}}(r,r,s,s) \end{bmatrix}.$$

Now since $(u,x),(v,y) \in \theta$ we have $m_i^{\mathbf{A}}(u,u,v,v)\theta\, m_i^{\mathbf{A}}(x,x,y,y)$, therefore by Lemma 2.23,

$$\begin{bmatrix} m_i^{\mathbf{A}}(x,x,y,y) \\ m_i^{\mathbf{A}}(r,u,v,s) \end{bmatrix} \Delta \begin{bmatrix} m_i^{\mathbf{A}}(x,x,y,y) \\ m_i^{\mathbf{A}}(r,r,s,s) \end{bmatrix},$$

i.e.,

$$m_i^{\mathbf{A}^2}\left(\begin{bmatrix} x \\ r \end{bmatrix}, \begin{bmatrix} x \\ u \end{bmatrix}, \begin{bmatrix} y \\ v \end{bmatrix}, \begin{bmatrix} y \\ s \end{bmatrix}\right) \Delta\, m_i^{\mathbf{A}^2}\left(\begin{bmatrix} x \\ r \end{bmatrix}, \begin{bmatrix} x \\ r \end{bmatrix}, \begin{bmatrix} y \\ s \end{bmatrix}, \begin{bmatrix} y \\ s \end{bmatrix}\right),$$

i.e., $m_i^{\mathbf{A}}(a,b,d,c)\Delta m_i^{\mathbf{A}}(a,a,c,c)$. By Theorem 2.3 ((ii)$\Rightarrow$ (iii)), $a\Delta c$, i.e.,

$$\begin{bmatrix} x & y \\ r & s \end{bmatrix} \in \Delta,$$

i.e., $((x,y),(r,s)) \in \eta$.

Thus, we may regard $\Delta_{\theta,\varphi}$ as a transitive relation on $\mathbf{A}(\varphi)$ and as such, it contains $M(\theta,\varphi)$ (considered as a set of pairs of rows). Hence, by Lemma 2.20, $\Delta^{\theta,\varphi} \subseteq \Delta_{\theta,\varphi}$ (by which we really mean $\eta \subseteq \Delta_{\theta,\varphi}$).

In a similar sense, by symmetry, $\Delta^{\varphi,\theta} \subseteq \Delta_{\varphi,\theta}$. It follows directly from Definition 2.18 that $\Delta_{\theta,\varphi} = \Delta^{\varphi,\theta}$ and $\Delta_{\varphi,\theta} = \Delta^{\theta,\varphi}$. We have $\Delta_{\theta,\varphi} = \Delta^{\varphi,\theta} \subseteq \Delta_{\varphi,\theta} = \Delta^{\theta,\varphi}$ therefore, $\Delta_{\theta,\varphi} = \Delta^{\theta,\varphi}$.

□

The next theorem shows that the definitions of the commutator given originally by Hagemann and Herrmann [HH79] and subsequently by Gumm [Gum80a] and by Freese and McKenzie [FM87] are equivalent in any modular variety.

Theorem 2.25. [FM87, Theorem 4.9]

Let V be a modular variety. Let $\mathbf{A} \in V$ and $x, y \in A$. The following are equivalent:

(i)
$$(x, y) \in [\theta, \varphi],$$

(ii)
$$\begin{bmatrix} x & y \\ y & y \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

(iii)
$$\textit{For some } a, \begin{bmatrix} x & a \\ y & a \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

(iv)
$$\textit{For some } b, \begin{bmatrix} x & y \\ b & b \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

Proof.

(ii)⇒(iii): Let $a = y$ in (iii).

(iii)⇒(ii): By Lemma 2.21, since
$$\begin{bmatrix} x & a \\ y & a \end{bmatrix} \in \Delta_{\theta,\varphi},$$
there exist $(z_i, z_i') \in \theta, i = 0, 1, \ldots, n$ such that $(z_0, z_0') = (x, y), (z_n, z_n') = (a, a)$ and for $i \in \{1, \ldots, n\}$,
$$\begin{bmatrix} z_{i-1} & z_i \\ z_{i-1}' & z_i' \end{bmatrix} \in M(\theta, \varphi).$$
Now we have $(z_{i-1}', z_i') \in \varphi$ for $i \in \{1, \ldots, n\}$, so by transitivity $(z_0', z_n') \in \varphi$, i.e., $(y, a) \in \varphi$, so $(a, y) \in \varphi$, so
$$\begin{bmatrix} a & y \\ a & y \end{bmatrix} \in \Delta_{\theta,\varphi},$$
by Definition 2.18 (ii).

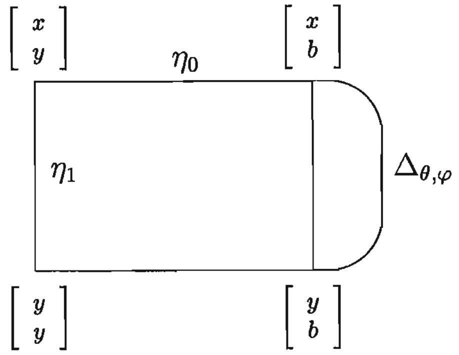
Now
$$\begin{bmatrix} x & a \\ y & a \end{bmatrix}, \begin{bmatrix} a & y \\ a & y \end{bmatrix} \in \Delta_{\theta,\varphi} \text{ so by transitivity, } \begin{bmatrix} x & y \\ y & y \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

(ii)⇒(iv): Let $b = y$ in (ii).

(iv)⇒(ii): Assume
$$\begin{bmatrix} x & y \\ b & b \end{bmatrix} \in \Delta_{\theta,\varphi}.$$
Then $(x,b),(y,b) \in \theta$, hence $(x,y) \in \theta$ by transitivity.

Let $p_0 : \mathbf{A}(\theta) \to \mathbf{A}$ and $p_1 : \mathbf{A}(\theta) \to \mathbf{A}$ be the first and second projection homomorphisms from $\mathbf{A}(\theta)$ onto $\mathbf{A}$. Let $\eta_0 = ker(p_0)$, so $((x,y),(x,b))$ and $((y,y),(y,b)) \in \eta_0$, and let $\eta_1 = ker(p_1)$, so $((x,y),(y,y))$ and $((x,b),(y,b)) \in \eta_1$.

We have the following diagram:


$\begin{bmatrix} x \\ y \end{bmatrix}$
η_0
$\begin{bmatrix} x \\ b \end{bmatrix}$
η_1
$\Delta_{\theta,\varphi}$
$\begin{bmatrix} y \\ y \end{bmatrix}$
$\begin{bmatrix} y \\ b \end{bmatrix}$

Now $\eta_0 \cap \eta_1 = id_{A(\theta)} \subseteq \Delta_{\theta,\varphi}$, so by the Shifting Lemma (Lemma 2.2), since V is modular,
$$\begin{bmatrix} x \\ b \end{bmatrix} \Delta_{\theta,\varphi} \begin{bmatrix} y \\ b \end{bmatrix} \text{implies} \begin{bmatrix} x \\ y \end{bmatrix} \Delta_{\theta,\varphi} \begin{bmatrix} y \\ y \end{bmatrix}, \text{ i.e., } \begin{bmatrix} x & y \\ y & y \end{bmatrix} \in \Delta_{\theta,\varphi}.$$
Thus, (ii), (iii) and (iv) are all equivalent.

(ii)⇒(i): We first show that $[\theta,\varphi]$ is the least congruence relation on $\mathbf{A}$ which is a union of $\Delta_{\theta,\varphi}$-classes. Suppose
$$\begin{bmatrix} a \\ b \end{bmatrix} \Delta_{\theta,\varphi} \begin{bmatrix} c \\ d \end{bmatrix}.$$
Since $\Delta_{\theta,\varphi}$ is the transitive closure of $M(\theta,\varphi)$ (by Lemma 2.21) there exist
$$\begin{bmatrix} x_0 \\ y_0 \end{bmatrix}, \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, \dots, \begin{bmatrix} x_n \\ y_n \end{bmatrix} \text{such that} \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} c \\ d \end{bmatrix}$$

and for $i \in \{1, \dots, n\}$,

$$\begin{bmatrix} x_{i-1} & x_i \\ y_{i-1} & y_i \end{bmatrix} \in M(\theta, \varphi) \text{ so } \begin{bmatrix} x_{i-1} & y_{i-1} \\ x_i & y_i \end{bmatrix} \in M(\varphi, \theta).$$

For any $i \in \{1, \dots, n\}$, if $(x_{i-1}, y_{i-1}) \in [\varphi, \theta] = [\theta, \varphi]$ (Proposition 2.9 (i)) then $(x_i, y_i) \in [\theta, \varphi]$ since $[\theta, \varphi]$ is the smallest congruence relation δ for which both $C(\theta, \varphi; \delta)$ and $C(\varphi, \theta; \delta)$ hold.
Thus, if in the first matrix

$$\begin{bmatrix} x_0 & y_0 \\ x_1 & y_1 \end{bmatrix}$$

we have $(x_0, y_0) = (a, b) \in [\theta, \varphi]$ then $(x_1, y_1) \in [\theta, \varphi]$, and so, repeating this argument, $(x_n, y_n) = (c, d) \in [\theta, \varphi]$. Therefore $(a, b)/\Delta_{\theta,\varphi} \subseteq [\theta, \varphi]$ whenever $(a, b) \in [\theta, \varphi]$. Thus, $[\theta, \varphi]$ contains the union of the $\Delta_{\theta,\varphi}$-classes of all its elements.

Conversely, if $(u, v) \in [\theta, \varphi] \subseteq \theta \cap \varphi$ then $(u, v) \in \theta$, so $(u, v) \in (u, v)/\Delta_{\theta,\varphi}$, so $[\theta, \varphi]$ is a union of $\Delta_{\theta,\varphi}-$classes. Now let δ be a congruence relation on $\mathbf{A}$ which is a union of some $\Delta_{\theta,\varphi}$-classes. Let

$$\begin{bmatrix} x & r \\ y & s \end{bmatrix} \in M(\varphi, \theta)$$

so $(x, y), (r, s) \in \varphi$ and $(x, r), (y, s) \in \theta$. Suppose $(x, r) \in \delta$. We show $(y, s) \in \delta$. We have

$$\begin{bmatrix} x & y \\ r & s \end{bmatrix} \in M(\theta, \varphi) \subseteq \Delta_{\theta,\varphi} \text{ so } \begin{bmatrix} y \\ s \end{bmatrix} \in \begin{bmatrix} x \\ r \end{bmatrix} /\Delta_{\theta,\varphi} \subseteq \delta$$

$$\text{(because } \begin{bmatrix} x \\ r \end{bmatrix} \in \delta \text{ and } \delta \text{ is a union of } \Delta_{\theta,\varphi}\text{-classes),}$$

so $(y, s) \in \delta$. Thus, $C(\varphi, \theta; \delta)$ holds.

By Proposition 2.11 (1), $[\theta, \varphi] \subseteq \delta$ (since V is modular). Therefore $[\theta, \varphi]$ is the least congruence relation on $\mathbf{A}$ that is a union of $\Delta_{\theta,\varphi}$-classes.

Now suppose

$$\begin{bmatrix} x & y \\ y & y \end{bmatrix} \in \Delta_{\theta,\varphi}, \text{ i.e., } \begin{bmatrix} x \\ y \end{bmatrix} \Delta_{\theta,\varphi} \begin{bmatrix} y \\ y \end{bmatrix}.$$

$$\text{Since} \begin{bmatrix} x \\ y \end{bmatrix} \in \begin{bmatrix} y \\ y \end{bmatrix} /\Delta_{\theta,\varphi} \text{ and } \begin{bmatrix} y \\ y \end{bmatrix} \in [\theta, \varphi], \text{ we have } \begin{bmatrix} x \\ y \end{bmatrix} \in [\theta, \varphi],$$

because $[\theta, \varphi]$ is the union of the $\Delta_{\theta,\varphi}$-classes of its elements.

(i)⇒(ii): Let

$$\alpha = \{\begin{bmatrix} x \\ y \end{bmatrix} \in A^2 : \begin{bmatrix} x & y \\ y & y \end{bmatrix} \in \Delta_{\theta,\varphi}\}.$$

We show α is a congruence relation on $\mathbf{A}$. Clearly, α is reflexive (by definition of $\Delta_{\theta,\varphi}$).

Symmetry:

$$\text{Let } \begin{bmatrix} x \\ y \end{bmatrix} \in \alpha. \text{ Then } \begin{bmatrix} x & y \\ y & y \end{bmatrix} \in \Delta_{\theta,\varphi} \text{ so } \begin{bmatrix} y & x \\ y & y \end{bmatrix} \in \Delta_{\theta,\varphi}$$

by symmetry of $\Delta_{\theta,\varphi}$. Therefore, since (iv) ⇒ (ii),

$$\begin{bmatrix} y & x \\ x & x \end{bmatrix} \in \Delta_{\theta,\varphi}, \text{ i.e., } \begin{bmatrix} y \\ x \end{bmatrix} \in \alpha.$$

Transitivity:

Let

$$\begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} y \\ z \end{bmatrix} \in \alpha. \text{ Then } \begin{bmatrix} z \\ y \end{bmatrix} \in \alpha$$

by symmetry of α, so

$$\begin{bmatrix} z & y \\ y & y \end{bmatrix} \in \Delta_{\theta,\varphi}. \text{ Therefore } \begin{bmatrix} x & y \\ y & y \end{bmatrix}, \begin{bmatrix} y & z \\ y & y \end{bmatrix} \in \Delta_{\theta,\varphi},$$

by symmetry of $\Delta_{\theta,\varphi}$. By transitivity of $\Delta_{\theta,\varphi}$,

$$\begin{bmatrix} x & z \\ y & y \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

Since (iv) ⇒ (ii),

$$\begin{bmatrix} x & z \\ z & z \end{bmatrix} \in \Delta_{\theta,\varphi}, \text{ i.e., } \begin{bmatrix} x \\ z \end{bmatrix} \in \alpha.$$

Compatibility:

Let f be an $n-$ary fundamental operation symbol of V. Suppose $(x_i, y_i) \in \alpha$ for $i \in \{1, 2, \ldots, n\}$.

Then

$$\begin{bmatrix} x_i & y_i \\ y_i & y_i \end{bmatrix} \in \Delta_{\theta,\varphi} \text{ for } i \in \{1, \ldots, n\}, \text{ i.e., } \begin{bmatrix} x_i \\ y_i \end{bmatrix} \Delta_{\theta,\varphi} \begin{bmatrix} y_i \\ y_i \end{bmatrix},$$

so by compatibility of $\Delta_{\theta,\varphi}$,

$$f^{\mathbf{A}^2}((x_1, y_1), \ldots, (x_n, y_n))(\Delta_{\theta,\varphi})f^{\mathbf{A}^2}((y_1, y_1), \ldots, (y_n, y_n)),$$

i.e., $(f^{\mathbf{A}}(x_1, \ldots, x_n), f^{\mathbf{A}}(y_1, \ldots, y_n))(\Delta_{\theta,\varphi})(f^{\mathbf{A}}(y_1, \ldots, y_n), f^{\mathbf{A}}(y_1, \ldots, y_n)),$

i.e.,

$$\begin{bmatrix} f^{\mathbf{A}}(x_1,\dots,x_n) & f^{\mathbf{A}}(y_1,\dots,y_n) \\ f^{\mathbf{A}}(y_1,\dots,y_n) & f^{\mathbf{A}}(y_1,\dots,y_n) \end{bmatrix} \in \Delta_{\theta,\varphi},$$

so $(f^{\mathbf{A}}(x_1,\dots,x_n), f^{\mathbf{A}}(y_1,\dots,y_n)) \in \alpha$.

We show α is the union of all $\Delta_{\theta,\varphi}$-classes of the form

$$\begin{bmatrix} p \\ q \end{bmatrix} / \Delta_{\theta,\varphi}$$

such that $(p,q) \in \alpha$. Let H be this union. Let $(x,y) \in \alpha$. Then

$$(x,y) \in \begin{bmatrix} x \\ y \end{bmatrix} / \Delta_{\theta,\varphi} \subseteq H.$$

Suppose $(x,y) \in \alpha$ and

$$\begin{bmatrix} x & r \\ y & s \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

Then (as in (iii) $\Rightarrow$ (ii), using Lemma 2.21) we can show $(y,s) \in \varphi$. Thus,

$$\begin{bmatrix} y & s \\ y & s \end{bmatrix} \in \Delta_{\theta,\varphi} \text{ and} \begin{bmatrix} x & y \\ y & y \end{bmatrix} \in \Delta_{\theta,\varphi}$$

(because $(x,y) \in \alpha$). By transitivity and symmetry of $\Delta_{\theta,\varphi}$,

$$\begin{bmatrix} x & s \\ y & s \end{bmatrix} \in \Delta_{\theta,\varphi}, \text{ i.e., } \begin{bmatrix} s & x \\ s & y \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

Now from

$$\begin{bmatrix} s & x \\ s & y \end{bmatrix}, \begin{bmatrix} x & r \\ y & s \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

we deduce

$$\begin{bmatrix} s & r \\ s & s \end{bmatrix} \in \Delta_{\theta,\varphi}, \text{ hence } \begin{bmatrix} r & s \\ s & s \end{bmatrix} \in \Delta_{\theta,\varphi}, \text{ and so } (r,s) \in \alpha.$$

Therefore

$$\begin{bmatrix} x \\ y \end{bmatrix} / \Delta_{\theta,\varphi} \subseteq \alpha, \text{ for all } \begin{bmatrix} x \\ y \end{bmatrix} \in \alpha,$$

i.e., $H \subseteq \alpha$ so $H = \alpha$.

It was shown in (ii) $\Rightarrow$ (i) that for any congruence δ on $\mathbf{A}$ that is a union of $\Delta_{\theta,\varphi}$-classes we have $[\theta,\varphi] \subseteq \delta$, so $[\theta,\varphi] \subseteq \alpha$. Therefore if $(x,y) \in [\theta,\varphi]$, then $(x,y) \in \alpha$, i.e.,

$$\begin{bmatrix} x & y \\ y & y \end{bmatrix} \in \Delta_{\theta,\varphi}.$$

Thus, (i) $\Rightarrow$ (ii).

□

2.5 The Commutator in Familiar Varieties.

2.5.1 Groups. Recall that the variety of groups is congruence modular (Example 2.4). Let $\mathbf{G} = \langle G; \cdot, ^{-1}, e\rangle$ be a group and let $\mathbf{Nor(G)}$ be its lattice of normal subgroups. Recall that the map $\mathbf{Con(G)} \to \mathbf{Nor(G)}$ defined by $\theta \mapsto e/\theta$ is a lattice isomorphism, with inverse isomorphism given by $N \mapsto \{(x,y) \in G^2 : xy^{-1} \in N\}$.

Recall that when $M, N \in Nor(\mathbf{G})$, the subgroup $[M,N]$ of $\mathbf{G}$ generated by $\{m^{-1}n^{-1}mn : m \in M \text{ and } n \in N\}$ is normal in $\mathbf{G}$ and is called the *commutator (subgroup) of M and N in* $\mathbf{G}$. We aim to show that if $\theta, \varphi \in Con(\mathbf{G})$ with $M = e/\theta$ and $N = e/\varphi$ then $[M,N] = e/[\theta,\varphi]$, i.e., for groups, the commutator defined earlier in this chapter coincides with the usual group-theoretic commutator (under the above lattice isomorphism).

Let $M, N \in Nor(\mathbf{G})$ and let $\rho : \mathbf{G} \to \mathbf{G}'$ be a surjective homomorphism. (Then $\mathbf{G}'$ is a group, since groups form a variety.) We shall need the following properties:

(1) $[M,N] \subseteq M \cap N$.

(2) $[\rho[M], \rho[N]] = \rho[[M,N]]$.

(3) The operation $[M,N]$ defined above is the largest binary operation defined on $\mathbf{Nor(G)}$ for every group $\mathbf{G}$ such that (1) and (2) are true.

We also have:

(4) $[M,N] = [N,M]$.

(5) $[M,N]$ is the least normal subgroup of $\mathbf{G}$ such that in $\mathbf{G}/[M,N]$, every element of $M/[M,N]$ commutes with every element of $N/[M,N]$ (hence $(\mathbf{M} \cap \mathbf{N})/[M,N]$ is an Abelian group).

Note that (1) follows from the normality of M and N in $\mathbf{G}$, and (4) from the fact that $[M,N]$ is closed under inverses. Also, (5) follows readily from the definitions and elementary group theory.

In (2), note that $\rho[M], \rho[N] \in Nor(\mathbf{G}')$ since, e.g., $\rho[M] = \rho[MK]$ (where $K = e/ker(\rho) = \rho[M \vee K]$), where $\vee$ denotes the join operation of $\mathbf{Nor(G)}$. From the definitions and the fact that ρ is a surjective homomorphism, we may verify (2) effortlessly.

We need to prove (3). Define

$$\begin{array}{rcl} G(M) & = & \{(x,y) \in G \times G : x^{-1}y \in M\}, \\ M_1 & = & \{(x,e) : x \in M\} = M \times \{e\}, \\ B & = & \{(x,e) : x \in [M,N]\} = [M,N] \times \{e\}, \\ \Delta & = & \{(x,y) \in N \times G : x^{-1}y \in [M,N]\}. \end{array}$$

Note that $G(M) = \theta$ (where $\theta \in Con(\mathbf{G})$ with $e/\theta = M$), so $G(M)$ is the universe of a subalgebra (i.e., subgroup) $\mathbf{G}(M)$ of $\mathbf{G} \times \mathbf{G}$. Also $M_1 \in Nor(\mathbf{G} \times \mathbf{G})$ because $M, \{e\} \in Nor(\mathbf{G} \times \mathbf{G})$; also $M_1 \subseteq G(M)$, so $M_1 \in Nor(\mathbf{G}(M))$. By the same argument, $B \in Nor(\mathbf{G} \times \mathbf{G})$ and $B \in Nor(\mathbf{G}(M))$ and $B \in Nor(\mathbf{M}_1)$, because $[M,N] \subseteq M$.

We show that $\Delta \in Nor(\mathbf{G}(M))$. Note that $(e,e) \in \Delta \subseteq G(M)$. Let $(x_1, y_1), (x_2, y_2) \in \Delta$. Then $x_1^{-1}y_1, x_2^{-1}y_2 \in [M,N]$. Consider $(x_1,y_1)(x_2,y_2)^{-1} = (x_1x_2^{-1}, y_1y_2^{-1})$. Now $x_1, x_2 \in N$ so $x_1x_2^{-1} \in N$.

We show $x_1x_2^{-1}(y_1y_2^{-1})^{-1} \in [M,N]$, i.e., that $x_1x_2^{-1}y_2y_1^{-1} \in [M,N]$. We have $x_1^{-1}y_1, x_2^{-1}y_2 \in [M,N]$. Let $x_1^{-1}y_1 = c_1$, $x_2^{-1}y_2 = c_2$, then $x_1^{-1} = c_1y_1^{-1}$ so $x_1 = y_1c_1^{-1}$. Then $x_1x_2^{-1}y_2y_1^{-1} = y_1c_1^{-1}c_2y_1^{-1} \in [M,N]$ since $c_1, c_2 \in [M,N]$, $y_1 \in G$ and $[M,N] \in Nor(\mathbf{G})$. Thus, Δ is a subgroup of $\mathbf{G}(M)$.

Let $(x_1, y_1) \in \Delta$ and $(x,y) \in G(M)$. Consider $(x,y)(x_1,y_1)(x,y)^{-1} = (xx_1x^{-1}, yy_1y^{-1})$. Now $xx_1x^{-1} \in N$, since $x \in G$ and $x_1 \in N \in Nor(\mathbf{G})$. We show $(xx_1x^{-1})^{-1}yy_1y^{-1} \in [M,N]$, i.e., that $xx_1^{-1}x^{-1}yy_1y^{-1} \in [M,N]$. Since $xy^{-1} = m$ for some $m \in M$, we have $y^{-1} = x^{-1}m$ and $y = m^{-1}x$. Also, $x_1^{-1}y_1 = c_1$ for some $c_1 \in [M,N]$ so $y_1 = x_1c_1$.

Now $xx_1^{-1}x^{-1}yy_1y^{-1} = xx_1^{-1}x^{-1}m^{-1}xx_1c_1x^{-1}m$
$= (m^{-1}xx^{-1}m)xx_1^{-1}x^{-1}m^{-1}xx_1c_1x^{-1}m$. We have $x^{-1}mx \in M$ and $x_1^{-1} \in N$ so if $c_2 = (x^{-1}mx)x_1^{-1}(x^{-1}m^{-1}x)x_1$ then $c_2 \in [M,N]$. Then $xx_1^{-1}x^{-1}yy_1y^{-1} = m^{-1}xc_2c_1x^{-1}m = m^{-1}xc_2c_1(m^{-1}x)^{-1} \in [M,N]$, since $m^{-1}x \in G$ and $c_2c_1 \in [M,N]$. Thus, $\Delta \in Nor(G(M))$.

Let π be the first projection homomorphism from $\mathbf{G} \times \mathbf{G}$ onto $\mathbf{G}$. Then $\pi[\Delta] = N$, $\pi[B] = [M,N]$ and $\pi[M_1] = M$. Let C be another binary operation on $\mathbf{Nor}(\mathbf{G})$ satisfying (1) and (2) above. By (1) $C(\mathbf{M}_1, \Delta) \subseteq \mathbf{M}_1 \cap \Delta \subseteq \mathbf{B}$. From (2) $C(M,N) = C(\pi[M_1], \pi[\Delta]) = \pi[C(M_1, \Delta)] \subseteq \pi[B]$. But $\pi[B] = [M,N]$, so $C(M,N) \subseteq [M,N]$. This proves (3).

Now the operation on $\mathbf{Nor}(\mathbf{G})$ defined by $C(e/\theta, e/\varphi) = e/[\theta,\varphi]$, $(\theta,\varphi) \in Con(\mathbf{G})$, satisfies (1), (2), so by (3), $e/[\theta,\varphi] \subseteq [M,N]$ whenever $e/\theta = M$ and $e/\varphi = N$.

Conversely, if $m \in M = e/\theta$ and $n \in N = e/\varphi$, let $t(x,y) = x^{-1}y^{-1}xy$. Then

$$\begin{bmatrix} e & e \\ m^{-1}n^{-1}mn & e \end{bmatrix} = \begin{bmatrix} t^{\mathbf{G}}(e,n) & t^{\mathbf{G}}(e,e) \\ t^{\mathbf{G}}(m,n) & t^{\mathbf{G}}(m,e) \end{bmatrix} \in M(\theta,\varphi)$$

and $C(\theta,\varphi;[\theta,\varphi])$ and $(e,e) \in [\theta,\varphi]$, so $(m^{-1}n^{-1}mn, e) \in [\theta,\varphi]$. Thus $\{m^{-1}n^{-1}mn : m \in M \text{ and } n \in N\} \subseteq e/[\theta,\varphi] \in Nor(\mathbf{G})$, so $[M,N] \subseteq e/[\theta,\varphi]$. Consequently, $[M,N] = e/[\theta,\varphi]$, as claimed.

Note that, by (5), the elements of M commute with those of N if and only if $[M,N] = \{e\}$ (if and only if $[\theta,\varphi] = id_G$). In particular, $[M/[M,N], N/[M,N]] = \{e/[M,N]\}$ in $\mathbf{G}/[M,N]$. Of course, $\mathbf{G}$ is an Abelian group if and only if $[G,G] = \{e\}$ (i.e., $[G^2,G^2] = id_G$).

2.5.2 Rings. Let $\mathbf{R} = \langle R; +, \cdot, -, 0\rangle$, be a ring (not assumed to have identity). Since $\mathbf{R} = \langle R; +, -, 0\rangle$ is a group, $\mathbf{R}$ is congruence modular, so the variety of all rings is congruence modular. Let $\mathbf{Id(R)}$ be the ideal lattice of $\mathbf{R}$. Recall that the map $\mathbf{Con(R)} \to \mathbf{Id(R)}$ defined by $\theta \mapsto 0/\theta$ is a lattice isomorphism, with inverse isomorphism given by $I \mapsto \{(x,y) \in R^2 : x - y \in I\}$. For $J, K \in Id(\mathbf{R})$, recall that $JK, J+K \in Id(\mathbf{R})$, where

$$\begin{aligned} JK &:= \{\sum_{i=0}^{n} a_i b_i : n \in \omega \text{ and } a_i \in J, \text{ and } b_i \in K \text{ for all } i \leq n\} \\ J+K &:= \{j+k : j \in J \text{ and } k \in K\}. \end{aligned}$$

Indeed, JK is the least ideal of $\mathbf{R}$ containing $\{jk : j \in J \text{ and } k \in K\}$ and $J+K$ is the least ideal of $\mathbf{R}$ containing $J \cup K$. Thus, if $F(J,K) := JK + KJ$ then
$F(J,K) = \{\sum_{i=0}^{n}(a_i b_i + b_i' a_i') : n \in \omega \text{ and } a_i, a_i' \in J, \text{ and } b_i, b_i' \in K \text{ for all } i < n\} = F(K,J)$

and $F(J,K)$ is the least ideal of $\mathbf{R}$ containing $\{jk : j \in J \text{ and } k \in K\} \cup \{kj : j \in J \text{ and } k \in K\}$.

Let $J, K \in Id(\mathbf{R})$ and let $\rho : \mathbf{R} \to \mathbf{R}'$ be a surjective homomorphism, where $\mathbf{R}'$ is a ring. Then $\rho[J], \rho[K] \in Id(\mathbf{R})$, and we have:

(1) $JK + KJ \subseteq J \cap K$.

(2) $\rho[J]\rho[K] + \rho[K]\rho[J] = \rho[JK + KJ]$.

(3) The operation $F(J,K) = JK + KJ$ is the largest binary operation defined on $Id(\mathbf{R})$ for every ring $\mathbf{R}$ such that (1) and (2) are true.

(1) is obvious and the proof of (2) is straightforward. The proof of (3) is a routine modification of the corresponding proof for normal subgroups of

groups. More precisely, if we define

$$\begin{aligned} R(J) &= \{(x,y) \in R \times R : x \in R, \text{ and } x - y \in J\}, \\ J_1 &= \{(x,0) : x \in J\}, \\ B &= \{(x,0) : x \in JK + KJ\}, \\ \Delta &= \{(x,y) \in K \times R : x - y \in JK + KJ\} \end{aligned}$$

then $R(J)$ is the universe of a subring $\mathbf{R}(J)$ of $\mathbf{R} \times \mathbf{R}$ and J_1, B, Δ are ideals (hence subuniverses) of $\mathbf{R}(J)$ and if π is the first projection homomorphism from $\mathbf{R} \times \mathbf{R}$ onto $\mathbf{R}$ then $\pi[B] = JK + KJ$, $\pi[J_1] = J$, $\pi[\Delta] = K$ and $J_1 \cap \Delta \subseteq B$.

Now if C is another binary operation on $Id(\mathbf{R})$ satisfying (1), (2) then, exactly as in the argument for groups, $C(J,K) \subseteq JK + KJ$.

Since the operation on $Id(\mathbf{R})$ defined by $C(0/\theta, 0/\varphi) = 0/[\theta,\varphi]$ $(\theta, \varphi \in Con(\mathbf{R}))$ satisfies (1), (2), we have $0/[\theta,\varphi] \subseteq JK + KJ$ whenever $J = 0/\theta$ and $K = 0/\varphi$, i.e., $[\theta,\varphi] = \{(x,y) \in R \times R : x - y \in JK + KJ\} \in \eta$, say.

Conversely, if $j \in J = 0/\theta$ and $k \in K = 0/\theta$ $(\theta, \varphi \in Con(\mathbf{R}))$, let $s(x,y) = xy$ and $t(x,y) = yx$. Then

$$\begin{bmatrix} 0 & 0 \\ jk & 0 \end{bmatrix} = \begin{bmatrix} s^{\mathbf{R}}(0,k) & s^{\mathbf{R}}(0,0) \\ s^{\mathbf{R}}(j,k) & s^{\mathbf{R}}(j,0) \end{bmatrix} \in M(\theta,\varphi)$$

and $(0,0) \in [\theta,\varphi]$, so $(jk, 0) \in [\theta,\varphi]$, i.e., $jk \in 0/[\theta,\varphi]$. Similarly, using t in place of s, we have $kj \in 0/[\theta,\varphi] \in Id(\mathbf{R})$, so $JK + KJ \subseteq 0/[\theta,\varphi]$. This shows that $JK + KJ = 0/[\theta,\varphi]$, i.e., that $[\theta,\varphi] = \eta$.

In particular $[\theta,\varphi] = id_R$ if and only if $IJ = JI = \{0\}$ (where $I = 0/\theta$ and $J = 0/\varphi$). Thus $[R^2, R^2] = id_R$ if and only if $\mathbf{R}$ has "zero multiplication", i.e., $ab = 0$ for all $a, b \in R$.

2.5.3 Modules. Let $\mathbf{R}$ be a ring, V the variety of all left $\mathbf{R}$–modules. Let $\mathbf{A} \in V$ and let $\langle A; +, -, 0\rangle$ be the Abelian group reduct of $\mathbf{A}$. Note that $\mathbf{A}$ is congruence modular (because $\langle A; +, -, 0\rangle$ is), so V is a congruence modular variety. Let $\mathbf{Sub(A)}$ denote the submodule (i.e., subalgebra) lattice of $\mathbf{A}$. Recall that the map $\mathbf{Con(A)} \to \mathbf{Sub(A)}$ defined by $\theta \mapsto 0/\theta$ is a lattice isomorphism, with inverse isomorphism given by $N \mapsto \{(x,y) \in A^2 : x - y \in N\}$.

We are going to show that $[\theta,\varphi] = id_A$ for all $\theta, \varphi \in Con(\mathbf{A})$.

Suppose D is a binary operation defined on $Sub(\mathbf{A})$ for all $\mathbf{A} \in V$ such that whenever $\rho : \mathbf{A} \to \mathbf{A}'$ is a surjective homomorphism in V and $M, N \in Sub(\mathbf{A})$, then

(1) $D(M,N) \subseteq M \cap N$ and

(2) $\rho[D(M,N)] = D(\rho[M], \rho[N])$.

We claim that $D(M,N) = \{0\}$ for all $M, N \in Sub(\mathbf{A})$ and all $\mathbf{A} \in V$.

To see this, let $\mathbf{A} \in V$ and let $\rho : \mathbf{A} \times \mathbf{A} \to \mathbf{A}$ be the surjective homomorphism defined by $\rho((a,b)) = a + b$ $(a, b \in A)$. Let $\theta, \varphi \in Con(\mathbf{A})$ with $M = 0/\theta$ and $N = 0/\varphi$. Define $\mathbf{N}_1 = \mathbf{N} \times \{0\}$ and $\mathbf{M}_1 = \{0\} \times \mathbf{M}$, so $N_1, M_1 \in Sub(\mathbf{A}\times\mathbf{A})$. Then $\rho[M_1] = M$ and $\rho[N_1] = N$ and $M_1 \cap N_1 = \{(0,0)\}$ so, by (1), $D(M_1, N_1) = \{(0,0)\}$.

By (2), $D(M,N) = D(\rho[M_1], \rho[N_1]) = \rho[D(M_1,N_1)] = \rho[\{(0,0)\}] = \{0\}$.

Now the operation $D(M,N) = 0/[\theta,\varphi]$ (where $M = 0/\theta$ and $N = 0/\varphi$) and $\theta, \varphi \in Con(\mathbf{A})$ $(\mathbf{A} \in V)$ satisfies (1), (2), so $0/[\theta,\varphi] = \{0\}$, i.e., $[\theta,\varphi] = id_A$ for all $\theta, \varphi \in Con(\mathbf{A})$ and all $\mathbf{A} \in V$.

2.5.4 Congruence distributive varieties.

Theorem 2.26. [HH79] [Gum83, Theorem 6.3]

Let V be a modular variety and $\mathbf{A} \in V$.

(i) If $\rho \cap \delta = [\rho, \delta]$ for all $\rho, \delta \in Con(\mathbf{A})$ then $\mathbf{A}$ is congruence distributive.

(ii) If every subalgebra of $\mathbf{A} \times \mathbf{A}$ is congruence distributive then $\alpha \cap \beta = [\alpha, \beta]$ for any $\alpha, \beta \in Con(\mathbf{A})$.

Proof.

(i) Let $[\rho, \delta] = \rho \cap \delta$ for all $\rho, \delta \in Con(\mathbf{A})$. Then for any $\alpha, \beta, \gamma \in Con(\mathbf{A})$, $\alpha \cap (\beta \vee \gamma) = [\alpha, \beta \vee \gamma] = [\alpha, \beta] \vee [\alpha, \gamma]$ (by additivity)
$= (\alpha \cap \beta) \vee (\alpha \cap \gamma)$. Thus $\mathbf{Con(A)}$ is a distributive lattice.

(ii) Let $\alpha, \beta \in Con(\mathbf{A})$. By Proposition 2.9 (i), $[\alpha, \beta] \subseteq \alpha \cap \beta$, so we need to show that $\alpha \cap \beta \subseteq [\alpha, \beta]$. Let $(x, y) \in \alpha \cap \beta$.
Since $(x, y) \in \beta$, we infer that $((x,x),(y,y)) \in \Delta_{\alpha,\beta}$. .... (1)

Let p_0 and p_1 be the first and second projection homomorphisms from $\mathbf{A}(\alpha)$ onto $\mathbf{A}$ (where $\mathbf{A}(\alpha)$ is α, considered as a subalgebra of $\mathbf{A} \times \mathbf{A}$), with kernels η_0 and η_1, respectively. Then $\eta_0, \eta_1 \in Con(\mathbf{A}(\alpha))$ and $\eta_0 \cap \eta_1 = id_{A(\alpha)}$.

Now $((x,y),(x,x)) \in \eta_0$. .... (2)

By (1) and (2), $((x,y),(y,y)) \in \Delta_{\alpha,\beta} \circ \eta_0 \subseteq \Delta_{\alpha,\beta} \vee \eta_0$. .... (3)

Also $((x,y),(y,y)) \in \eta_1$. .... (4)

By (3) and (4), $((x,y),(y,y)) \in (\Delta_{\alpha,\beta} \vee \eta_0) \cap \eta_1$
$= (\Delta_{\alpha,\beta} \cap \eta_1) \vee (\eta_0 \cap \eta_1)$ (because $\mathbf{A}(\alpha)$ is congruence distributive)
$= (\Delta_{\alpha,\beta} \cap \eta_1) \vee id_{A(\alpha)}$

$= \Delta_{\alpha,\beta} \cap \eta_1 \subseteq \Delta_{\alpha,\beta}$.

From $((x, y), (y, y)) \in \Delta_{\alpha,\beta}$ and by the equivalence of (i) and (ii) in Theorem 2.25, we infer that $(x, y) \in [\alpha, \beta]$, so $\alpha \cap \beta \subseteq [\alpha, \beta]$ and hence $\alpha \cap \beta = [\alpha, \beta]$.

□

Corollary 2.27. *A congruence modular variety V is congruence distributive if and only if for every $\mathbf{A} \in V$ and every $\alpha, \beta \in Con(\mathbf{A})$, $[\alpha, \beta] = \alpha \cap \beta$.*

Proof.

($\Leftarrow$) follows directly from (i) of the previous theorem.

($\Rightarrow$) Let $\mathbf{A} \in V$ where V is congruence distributive. Then $\mathbf{A} \times \mathbf{A}$ and all its subalgebras are in V and are therefore congruence distributive so the result follows from (ii) of the previous theorem.

□

In particular, if $\alpha, \beta \in Con(\mathbf{A})$, where $\mathbf{A}$ is a lattice or a Boolean algebra then $[\alpha, \beta] = \alpha \cap \beta$, since the varieties of lattices and of Boolean algebras are congruence distributive.

Chapter 3

Abelian Congruences and Abelian Algebras

In this chapter, we define and study *Abelian* algebras and *affine* algebras. An algebra $\mathbf{A}$ is Abelian if $[A^2, A^2] = id_A$. (Thus, a group is Abelian if and only if it is Abelian in the traditional sense. Also, all modules are Abelian algebras.) Affine algebras have a more complex definition but, roughly speaking (or, more precisely, "up to polynomial equivalence"), they are the same things as modules over rings. In particular, affine algebras are Abelian (and congruence modular, in fact permutable). The main theorem of the chapter, which is Herrmann's *Fundamental Theorem of Abelian Algebras* [Her79] establishes that, in a congruence modular variety V, the converse is also true: every Abelian algebra in V is affine. Since, for all $\mathbf{A} \in V$, the algebra $\mathbf{A}/[A^2, A^2]$ is Abelian (and in V), this result advances our understanding of modular varieties substantially.

A key tool in the proof is the existence, in any modular variety V, of a ternary "difference" term d, with certain useful properties (established in [Her79] and [Gum80a]). It is shown that for any $\mathbf{A} \in V$, and $\beta \in Con(\mathbf{A})$ with $[\beta, \beta] = id_A$, the congruence class u/β of any $u \in A$ is closed under $d^{\mathbf{A}}$. The algebra $\langle u/\beta; d^{\mathbf{A}} \rangle$ is called a "ternary group" because, using d, we may give u/β the structure of an Abelian group in a natural way. Moreover, locally, term functions of $\mathbf{A}$ may be regarded as group homomorphisms.

We begin by describing the *centre*, $\tau_{\mathbf{A}}$, of an algebra $\mathbf{A}$. (The definition generalizes that of the centre of a group.) In the first theorem, for modular varieties, a commutator-theoretic description of the centre is given, allowing us to deduce that, just as for groups, an algebra is Abelian if and only if its centre is as large as it can be.

3.1 Abelian and Affine Algebras. Recall that $\mathcal{T} = \langle \mathsf{F}, ar \rangle$ denotes a fixed but arbitrary type.

Definition 3.1. The *centre* of any $\mathcal{T}$-algebra $\mathbf{A}$ is the binary relation $\tau_{\mathbf{A}} \subseteq A^2$ defined by $(x, y) \in \tau_{\mathbf{A}}$ if and only if for any $n < \omega$, and any $(n+1)$-ary $\mathcal{T}$-term t, and any $\mathbf{u}, \mathbf{v} \in A^n$, the following is true:

$$t^{\mathbf{A}}(\mathbf{u}, x) = t^{\mathbf{A}}(\mathbf{v}, x) \text{ if and only if } t^{\mathbf{A}}(\mathbf{u}, y) = t^{\mathbf{A}}(\mathbf{v}, y).$$

Lemma 3.2. [FM87, Lemma 5.2]

The centre $\tau_{\mathbf{A}}$ of a $\mathcal{T}$-algebra $\mathbf{A}$ is a congruence relation on $\mathbf{A}$. If $\mathbf{A}$ belongs to a modular variety, then $\tau_{\mathbf{A}}$ is the largest congruence δ on $\mathbf{A}$ such that $[\delta, A^2] = id_A$.

Proof.

Let t be any $(n+1)$-ary $\mathcal{T}$-term and let $\mathbf{u}, \mathbf{v} \in A^n$. We first show $\tau_{\mathbf{A}}$ is a congruence relation on $\mathbf{A}$. Obviously, $\tau_{\mathbf{A}}$ is an equivalence relation.

Now let f be an n-ary fundamental operation symbol of $\mathcal{T}$ and for all $i \in \{1, \dots, n\}$, let $(x_i, y_i) \in \tau_{\mathbf{A}}$. .... (1)
Given an $(m+1)$-ary term $t = t(\mathbf{z}, w)$, define a new term $s = s_t$ by
$s(\mathbf{z}, x_1, \dots, x_n) = t(\mathbf{z}, f(x_1, \dots, x_n))$. Suppose for all $\mathbf{u}, \mathbf{v} \in A^m$,
$t^{\mathbf{A}}(\mathbf{u}, f^{\mathbf{A}}(x_1, \dots, x_n)) = t^{\mathbf{A}}(\mathbf{v}, f^{\mathbf{A}}(x_1, \dots, x_n))$, i.e., $s^{\mathbf{A}}(\mathbf{u}, x_1, \dots, x_n) =$
$s^{\mathbf{A}}(\mathbf{v}, x_1, \dots, x_n)$. Then $s^{\mathbf{A}}(\mathbf{u}, y_1, x_2, \dots, x_n) = s^{\mathbf{A}}(\mathbf{v}, y_1, x_2 \dots, x_n)$, by (1), and so $s^{\mathbf{A}}(\mathbf{u}, y_1, y_2, x_3, \dots, x_n) = s^{\mathbf{A}}(\mathbf{v}, y_1, y_2, x_3, \dots, x_n)$, by (1).

Continuing in this way, we get $s^{\mathbf{A}}(\mathbf{u}, y_1, \dots, y_n) = s^{\mathbf{A}}(\mathbf{v}, y_1, \dots, y_n)$, i.e., $t^{\mathbf{A}}(\mathbf{u}, f(y_1, \dots, y_n)) = t^{\mathbf{A}}(\mathbf{v}, f(y_1, \dots, y_n))$. The converse follows by symmetry, so $\tau_{\mathbf{A}} \in Con(\mathbf{A})$.

Now assume that V is a modular variety, with $\mathbf{A} \in V$. We show that $[\tau_{\mathbf{A}}, A^2] = id_A$. Let

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} = \begin{bmatrix} t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2) \\ t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1) & t^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2) \end{bmatrix} \in M(\tau_{\mathbf{A}}, A^2)$$

where $\mathbf{a}^i, i = 1, 2$, is a sequence of n elements of A, $\mathbf{b}^i, i = 1, 2$, is a sequence of m elements of A, $m, n \geq 0$, satisfying $a_k^1 \tau_{\mathbf{A}} a_k^2$ for $k < n$, and t is a $(n+m)$-ary $\mathcal{T}$-term.

Suppose $t^{\mathbf{A}}(a_1^1, \dots, a_n^1, \mathbf{b}^1) = t^{\mathbf{A}}(a_1^1, \dots, a_n^1, \mathbf{b}^2)$. Then by repeated use of the definition of $\tau_{\mathbf{A}}$, $t^{\mathbf{A}}(a_1^2, \dots, a_n^2, \mathbf{b}^1) = t^{\mathbf{A}}(a_1^2, \dots, a_n^2, \mathbf{b}^2)$ since $(a_k^1, a_k^2) \in \tau_{\mathbf{A}}$ for all $k \in \{1, \dots, n\}$, so $C(\tau_{\mathbf{A}}, A^2; id_A)$ holds. V is modular, so by Proposition 2.11, $[\tau_{\mathbf{A}}, A^2] \subseteq id_A$, so $[\tau_{\mathbf{A}}, A^2] = id_A$.

Let α be any congruence relation on $\mathbf{A}$ such that $[\alpha, A^2] = id_A$. Then both $C(\alpha, A^2; id_A)$ and $C(A^2, \alpha; id_A)$ hold. .... (2)

We show $\alpha \subseteq \tau_{\mathbf{A}}$. Let $(x,y) \in \alpha$. Then

$$\begin{bmatrix} t^{\mathbf{A}}(x,\mathbf{u}) & t^{\mathbf{A}}(x,\mathbf{v}) \\ t^{\mathbf{A}}(y,\mathbf{u}) & t^{\mathbf{A}}(y,\mathbf{v}) \end{bmatrix}$$

is an element of $M(\alpha, A^2)$ for any $\mathbf{u},\mathbf{v} \in A^n$ and any $(n+1)$-ary $\mathcal{T}$-term t. From (2), if $t^{\mathbf{A}}(x,\mathbf{u}) = t^{\mathbf{A}}(x,\mathbf{v})$, then $t^{\mathbf{A}}(y,\mathbf{u}) = t^{\mathbf{A}}(y,\mathbf{v})$. Since $(y,x) \in \alpha$, the converse follows by symmetry. Consequently, $\alpha \subseteq \tau_{\mathbf{A}}$.

Thus $\tau_{\mathbf{A}}$ is the largest congruence relation δ on $\mathbf{A}$ such that $[\delta, A^2] = id_A$.
□

Definition 3.3. For any algebra $\mathbf{A}$, a congruence $\theta \in Con(\mathbf{A})$ is called *Abelian* if $[\theta,\theta] = id_A$. $\mathbf{A}$ is *Abelian* if $[A^2, A^2] = id_A$ or, equivalently, $\tau_{\mathbf{A}} = A^2$.[16] A variety is *Abelian* if all its members are.

Proposition 3.4. *Let V be a modular variety and $\mathbf{A} \in V$ and $\theta \in Con(\mathbf{A})$. Then $\theta/[\theta,\theta]$ is an Abelian congruence of $\mathbf{A}/[\theta,\theta]$. In particular, $\mathbf{A}/[A^2, A^2]$ is an Abelian algebra.*

Proof.

Let $f : \mathbf{A} \to \mathbf{A}/[\theta,\theta] = \mathbf{B}$ be the natural epimorphism, so $ker(f) = [\theta,\theta] = \pi$, say. We must show that $[\theta/\pi, \theta/\pi] = id_B$. Since $\pi \subseteq \theta$,

$f^{-1}([\theta/\pi, \theta/\pi]) = f^{-1}([f(\theta \vee \pi), f(\theta \vee \pi)])$

$= [\theta,\theta] \vee \pi$ (by Proposition 2.14 (i))

$= \pi = f^{-1}(id_B)$.

Since, by the Correspondence Theorem, $\eta \mapsto f^{-1}(\eta)$ is a lattice isomorphism from $\mathbf{Con}(\mathbf{B})$ onto $\mathbf{int}(\pi, A^2)$, it follows that $[\theta/\pi, \theta/\pi] = id_B$. In particular $A^2/[A^2,A^2]$ is an Abelian congruence of $\mathbf{A}/[A^2,A^2]$. □

Using Propositions 2.14 and 2.17 it is easy to verify that the class V_{ab} of all Abelian algebras in a modular variety V is a subvariety of V, so every modular variety V has a largest Abelian subvariety V_{ab}. Of course if V is the variety of all groups then V_{ab} is the variety of Abelian groups.

Definition 3.5.

Consider a $\mathcal{T}$-algebra $\mathbf{A}$. If there is an Abelian group [17] $\langle A; +, - \rangle = \hat{\mathbf{A}}$ having the same universe as $\mathbf{A}$ and a ternary $\mathcal{T}$-term, $t(x,y,z)$ such that

(i) $t^{\mathbf{A}}(a,b,c) = a - b + c$ for all $a,b,c \in A$

[16] Note that these two definitions of an Abelian algebra $\mathbf{A}$ are equivalent even if $\mathbf{A}$ does not belong to any modular variety. Thus an Abelian variety is not assumed to be modular.

[17] For convenience here we treat groups as algebras of type $\langle 2,1 \rangle$ rather than $\langle 2,1,0 \rangle$.

then t is called a *difference operation* for $\mathbf{A}$, and the algebra $\langle A; t^{\mathbf{A}}\rangle$ is called a *ternary group*. If in addition,

(ii) $f^{\mathbf{A}}(\mathbf{a}-\mathbf{b}+\mathbf{c}) = f^{\mathbf{A}}(\mathbf{a}) - f^{\mathbf{A}}(\mathbf{b}) + f^{\mathbf{A}}(\mathbf{c})$ for any $n < \omega$ and any n-ary $\mathcal{T}$-term f and $\mathbf{a}, \mathbf{b}, \mathbf{c} \in A^n$,

we say that $\mathbf{A}$ is *t-affine*.

Proposition 3.6. *Any affine algebra is Abelian, and generates a congruence permutable (hence congruence modular) variety.*

Proof.

Let $\mathbf{A}$ be an affine $\mathcal{T}$-algebra and let t and $\hat{\mathbf{A}}$ be as in Definition 3.5. Let $n, m \in \omega$, let s be any $(n+m)$-ary $\mathcal{T}$-term, let $\mathbf{a}^i \in A^n$ and $\mathbf{b}^i \in A^m$ for $i = 1, 2$, and suppose $s^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1) = s^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2)$. Then

$s^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1) = s^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1) - s^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2) + s^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2)$ (since $\hat{\mathbf{A}}$ is a group)

$= s^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^1) - s^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^1) + s^{\mathbf{A}}(\mathbf{a}^1, \mathbf{b}^2)$ (by assumption)

$= s^{\mathbf{A}}(\mathbf{a}^2 - \mathbf{a}^1 + \mathbf{a}^1, \mathbf{b}^1 - \mathbf{b}^1 + \mathbf{b}^2)$ (by t-affinity)

$= s^{\mathbf{A}}(\mathbf{a}^2, \mathbf{b}^2)$.

This shows that if

$$\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \in M(A^2, A^2)$$

and $(u_{11}, u_{12}) \in id_A$ then $(u_{21}, u_{22}) \in id_A$, so $C(A^2, A^2; id_A)$, hence $[A^2, A^2] = id_A$.

Since t is a term of $V(\mathbf{A})$ and $\mathbf{A}$ (hence $V(\mathbf{A})$) satisfies $t(x, x, y) \approx y \approx t(y, x, x)$, it follows from Theorem 0.54 that $V(\mathbf{A})$ is congruence permutable. □

The next lemma is stated without proof in [FM87].

Lemma 3.7. *For a $\mathcal{T}$-algebra $\mathbf{A} = \langle A; \dots\rangle$ and an Abelian group $\hat{\mathbf{A}} = \langle A; +, -\rangle$ (with the same universe A), the following are equivalent:*

(i) *For any $n < \omega$ and any n-ary $\mathcal{T}$-term f and any $\mathbf{a}, \mathbf{b}, \mathbf{c} \in A^n$, $f^{\mathbf{A}}(\mathbf{a}-\mathbf{b}+\mathbf{c}) = f^{\mathbf{A}}(\mathbf{a}) - f^{\mathbf{A}}(\mathbf{b}) + f^{\mathbf{A}}(\mathbf{c})$.*

(ii) *For any $n < \omega$ and any fundamental n-ary operation symbol F of $\mathcal{T}$ there exist endomorphisms $\alpha_1, \dots, \alpha_n$ of $\hat{\mathbf{A}}$ and $a \in A$ such that, for any $\mathbf{a} = (a_1, \dots, a_n) \in A^n$, $F^{\mathbf{A}}(\mathbf{a}) = (\sum_{i=1}^{n} \alpha_i(a_i)) + a$.*

(iii) *$S := \{(a, b, c, d) \in A^4 : a + b = c + d\}$ is a subuniverse of $\mathbf{A}^4$.*

Therefore (ii) and (iii) hold whenever $\mathbf{A}$ is affine.

Proof.

Let $\mathbf{A} = \langle A; \dots \rangle$ be a $\mathcal{T}$-algebra and assume that for some binary operation $+$ and some unary operation $-$ on A, the algebra $\hat{\mathbf{A}} = \langle A; +, - \rangle$ is an Abelian group.

(i)$\Rightarrow$(ii): Assume (i). Let 0 be the identity element of $\hat{\mathbf{A}}$ and for $n < \omega$ let F be any fundamental n-ary operation symbol of $\mathcal{T}$. For $i = 1, \dots, n$ define $\alpha_i : A \to A$ by

$\alpha_i(a_i) = F^{\mathbf{A}}(0, \dots, 0, a_i, 0, \dots, 0) - F^{\mathbf{A}}(\mathbf{0})$, where $\mathbf{0} := (0, \dots, 0) \in A^n$ and $a_i \in A$ and in $(0, \dots, 0, a_i, 0, \dots, 0)$, a_i occurs in the i^{th} co-ordinate.

We show each α_i is an endomorphism of $\hat{\mathbf{A}}$, i.e., that $\alpha_i(a_i + b_i) = \alpha_i(a_i) + \alpha_i(b_i)$ for any $a_i, b_i \in A$.

$\alpha_i(a_i + b_i) = F^{\mathbf{A}}(0, \dots, 0, a_i + b_i, 0, \dots, 0) - F^{\mathbf{A}}(\mathbf{0})$

$= F^{\mathbf{A}}((0, \dots, 0, a_i, 0, \dots, 0) - (0, \dots, 0) + (0, \dots, 0, b_i, 0, \dots, 0)) - F^{\mathbf{A}}(\mathbf{0})$

$= F^{\mathbf{A}}(0, \dots, 0, a_i, 0, \dots, 0) - F^{\mathbf{A}}(\mathbf{0}) + F^{\mathbf{A}}(0, \dots, 0, b_i, 0, \dots, 0) - F^{\mathbf{A}}(\mathbf{0})$ (by (i))

$= \alpha_i(a_i) + \alpha_i(b_i)$.

It follows that for any $a_i \in A$, $\alpha_i(-a_i) = -\alpha_i(a_i)$ and $\alpha_i(0) = 0$, by a general property of group homomorphisms.

Let $c = -F^{\mathbf{A}}(\mathbf{0})$. For any $\mathbf{a}, \mathbf{b} \in A^n$,

$F^{\mathbf{A}}(\mathbf{a} + \mathbf{b}) = F^{\mathbf{A}}(\mathbf{a} - \mathbf{0} + \mathbf{b}) = F^{\mathbf{A}}(\mathbf{a}) - F^{\mathbf{A}}(\mathbf{0}) + F^{\mathbf{A}}(\mathbf{b})$ (by (i)),

$= F^{\mathbf{A}}(\mathbf{a}) + F^{\mathbf{A}}(\mathbf{b}) + (-F^{\mathbf{A}}(\mathbf{0}))$ (because $\hat{\mathbf{A}}$ is Abelian)

$= F^{\mathbf{A}}(\mathbf{a}) + F^{\mathbf{A}}(\mathbf{b}) + c$ .... (1)

Let $\mathbf{a} = (a_1, \dots, a_n) \in A^n$. Then

$F^{\mathbf{A}}(\mathbf{a}) = F^{\mathbf{A}}(a_1, \dots, a_n)$

$= F^{\mathbf{A}}([(a_1, 0, \dots, 0) + (0, a_2, 0, \dots, 0) + \dots + (0, \dots, 0, a_{n-1}, 0)] + (0, \dots, 0, a_n))$

$= F^{\mathbf{A}}((a_1, 0, \dots, 0) + \dots + (0, \dots, 0, a_{n-1}, 0)) + F^{\mathbf{A}}(0, \dots, 0, a_n) + c$ (by (1))

$= F^{\mathbf{A}}((a_1, 0, \dots, 0) + \dots + (0, \dots, a_{n-2}, 0, 0)) + F^{\mathbf{A}}(0, \dots, 0, a_{n-1}, 0) + c +$
$F^{\mathbf{A}}(0, \dots, 0, a_n) + c$ (by (1))

$= F^{\mathbf{A}}((a_1, 0, \dots, 0) + \dots + (0, \dots, a_{n-2}, 0, 0)) + F^{\mathbf{A}}(0, \dots, 0, a_{n-1}, 0) +$
$F^{\mathbf{A}}(0, \dots, 0, a_n) + 2c = \dots$

$= F^{\mathbf{A}}(a_1, 0, \dots, 0) + F^{\mathbf{A}}(0, a_2, \dots, 0) + \dots + F^{\mathbf{A}}(0, \dots, 0, a_{n-1}, 0) +$
$F^{\mathbf{A}}(0, \dots, 0, a_n) + nc$

$= \alpha_1(a_1) + \alpha_2(a_2) + \dots + \alpha_{n-1}(a_{n-1}) + \alpha_n(a_n)$

$= (\sum_{i=1}^{n} \alpha_i(a_i)) + 0$.

(ii)⇒(iii): Assume (ii). Let F be any fundamental n-ary operation symbol of $\mathcal{T}$ with $(a_i, b_i, c_i, d_i) \in S$ for $i \in \{1, \ldots, n\}$.
We show $F^{\mathbf{A}^4}((a_1, b_1, c_1, d_1), \ldots, (a_n, b_n, c_n, d_n)) \in S$.

$F^{\mathbf{A}^4}((a_1, b_1, c_1, d_1), \ldots, (a_n, b_n, c_n, d_n))$
$= (F^{\mathbf{A}}(a_1, \ldots, a_n), F^{\mathbf{A}}(b_1, \ldots, b_n), F^{\mathbf{A}}(c_1, \ldots, c_n), F^{\mathbf{A}}(d_1, \ldots, d_n))$
so we show
$F^{\mathbf{A}}(a_1, \ldots, a_n) + F^{\mathbf{A}}(b_1, \ldots, b_n) = F^{\mathbf{A}}(c_1, \ldots, c_n) + F^{\mathbf{A}}(d_1, \ldots, d_n)$.

For each $i \in \{1, \ldots, n\}$, we have $a_i + b_i = c_i + d_i$. .... (2)

Now $F^{\mathbf{A}}(a_1, \ldots, a_n) + F^{\mathbf{A}}(b_1, \ldots, b_n) = \sum_{i=1}^{n} \alpha_i(a_i) + a + \sum_{i=1}^{n} \alpha_i(b_i) + a$
$= \sum_{i=1}^{n} \alpha_i(a_i + b_i) + 2a$ (since $\hat{\mathbf{A}}$ is Abelian and each α_i is an endomorphism)
$= \sum_{i=1}^{n} \alpha_i(c_i + d_i) + 2a$ (by (2))
$= \sum_{i=1}^{n} \alpha_i(c_i) + a + \sum_{i=1}^{n} \alpha_i(d_i) + a$ (because $\hat{\mathbf{A}}$ is Abelian and each α_i is an endomorphism)
$= F^{\mathbf{A}}(c_1, \ldots, c_n) + F^{\mathbf{A}}(d_1, \ldots, d_n)$.

(iii)⇒(i): Assume (iii). Let f be any n-ary $\mathcal{T}$-term and let $\mathbf{a} = (a_1, \ldots, a_n)$, $\mathbf{b} = (b_1, \ldots, b_n)$, $\mathbf{c} = (c_1, \ldots, c_n) \in A^n$. For all $i \in \{1, \ldots, n\}$, $(a_i - b_i + c_i, b_i, a_i, c_i) \in S$, because $\hat{\mathbf{A}}$ is Abelian.

It is enough to show $(f^{\mathbf{A}}(\mathbf{a} - \mathbf{b} + \mathbf{c}), f^{\mathbf{A}}(\mathbf{b}), f^{\mathbf{A}}(\mathbf{a}), f^{\mathbf{A}}(\mathbf{c})) \in S$, since then $f^{\mathbf{A}}(\mathbf{a} - \mathbf{b} + \mathbf{c}) + f^{\mathbf{A}}(\mathbf{b}) = f^{\mathbf{A}}(\mathbf{a}) + f^{\mathbf{A}}(\mathbf{c})$, therefore $f^{\mathbf{A}}(\mathbf{a} - \mathbf{b} + \mathbf{c}) = f^{\mathbf{A}}(\mathbf{a}) - f^{\mathbf{A}}(\mathbf{b}) + f^{\mathbf{A}}(\mathbf{c})$, because $\hat{\mathbf{A}}$ is Abelian.

From (iii), $f^{\mathbf{A}^4}((a_1 - b_1 + c_1, b_1, a_1, c_1), \ldots, (a_n - b_n + c_n, b_n, a_n, c_n)) \in S$,
i.e., $(f^{\mathbf{A}}((a_1 - b_1 + c_1), \ldots, (a_n - b_n + c_n)), f^{\mathbf{A}}(\mathbf{b}), f^{\mathbf{A}}(\mathbf{a}), f^{\mathbf{A}}(\mathbf{c})) \in S$,
i.e., $(f^{\mathbf{A}}(\mathbf{a} - \mathbf{b} + \mathbf{c}), f^{\mathbf{A}}(\mathbf{b}), f^{\mathbf{A}}(\mathbf{a}), f^{\mathbf{A}}(\mathbf{c})) \in S$.

□

Affine algebras appear to have originated in [OS66]. Their significance lies in the fact that they are "almost" modules. We shall now make this statement more precise. For any algebra $\mathbf{A}$ and any $n \in \omega$, define

$Pol_n(\mathbf{A}) = \{f : f \text{ is an } n\text{-ary polynomial function of } \mathbf{A}\}$

and $Pol(\mathbf{A}) = \cup_{n \in \omega} Pol_n(\mathbf{A})$.

Definition 3.8. Two algebras $\mathbf{A}_1 = \langle A_1; F_1\rangle$ and $\mathbf{A}_2 = \langle A_2; F_2\rangle$ (of possibly different types) are said to be *polynomially equivalent* if $A_1 = A_2$ and $Pol(\mathbf{A}_1) = Pol(\mathbf{A}_2)$.

If $\mathbf{R} = \langle R; +, \cdot, -, 0^{\mathbf{R}}, 1\rangle$ is a ring with identity and $\mathbf{M} = \langle M; \{+, -, 0^{\mathbf{M}}\} \cup \{\tilde{r} : r \in R\}\rangle$ is a left unital module over $\mathbf{R}$ (where $\tilde{r}^{\mathbf{M}}(m) = rm$ for all $r \in R$ and $m \in M$), it is easy to see that $\mathbf{M}$ is an affine algebra. Conversely:

Theorem 3.9. [Gum79]

Let $\mathbf{A}$ *be an affine* $\mathcal{T}$*-algebra. Then there exists a ring with identity,* $\mathbf{R}$*, and a unital left* $\mathbf{R}$*-module* $\mathbf{M}$ *such that* $\mathbf{A}$ *and* $\mathbf{M}$ *are polynomially equivalent.*

Proof.

Let $\hat{\mathbf{A}} = \langle A; +, -\rangle$ and $\langle A; t^{\mathbf{A}}\rangle$ be an Abelian group and ternary group associated with $\mathbf{A}$, as in Definition 3.5, and let $0 \in A$ be the identity element of $\hat{\mathbf{A}}$.

The endomorphism ring $\mathbf{E} = \langle E; \oplus, \circ, -, \bar{0}, id_A\rangle$ of $\hat{\mathbf{A}}$ is the ring of all group homomorphisms from $\langle A; +, -, 0\rangle$ to itself, where, for $f, g \in E$ and $a \in A$,

$(f \oplus g)(a) = f(a) + g(a)$ and $(f \circ g)(a) = f(g(a))$ and $\bar{0}(a) = 0$.

Recall that $\langle A; \{+, -, 0\} \cup \{\tilde{e} : e \in E\}\rangle$ is a unital left $\mathbf{E}-$module, where $ea := e(a)$ for all $e \in E$ and $a \in A$.

Let $R = \{e \in Pol_1(\mathbf{A}) : e(0) = 0\}$. If $e \in R$ then there exist $k \in \omega$, a k-ary $\mathcal{T}$-term q and $\mathbf{u} = u_1, \dots, u_k \in A$ such that $e(a) = q^{\mathbf{A}}(a, \mathbf{u})$ for all $a \in A$. Then, for all $a, b, c \in A$,

$e(t^{\mathbf{A}}(a, b, c)) = q^{\mathbf{A}}(t^{\mathbf{A}}(a, b, c), \mathbf{u})$

$q^{\mathbf{A}}(t^{\mathbf{A}}(a, b, c), t^{\mathbf{A}}(u_1, u_1, u_1), \dots, t^{\mathbf{A}}(u_k, u_k, u_k))$ (by Definition 3.5(i))

$= t^{\mathbf{A}}(q^{\mathbf{A}}(a, \mathbf{u}), q^{\mathbf{A}}(b, \mathbf{u}), q^{\mathbf{A}}(c, \mathbf{u}))$ (by Definition 3.5(ii))

$= t^{\mathbf{A}}(e(a), e(b), e(c))$,

so e preserves $t^{\mathbf{A}}$ and 0, and therefore also + (since $a + b = t^{\mathbf{A}}(a, 0, b)$). Consequently, $e \in E$, so $R \subseteq E$. Also, $\bar{0}$, $id_A \in R$. Evidently, if $e, f \in R$ then, since $e(0) = 0 = f(0)$ and $f(a) + g(a) = t^{\mathbf{A}}(f(a), 0, g(a))$ and $-f = \bar{0} \oplus (-f)$, we have $e \oplus f, -f, e \circ f \in R$. This makes R the universe of a subring (with identity) $\mathbf{R}$ of $\mathbf{E}$, so $\mathbf{M} = \langle A; \{+, -, 0\} \cup \{\tilde{r} : r \in R\}\rangle$ is a unital left $\mathbf{R}$-module.

Since $+, -$ are definable in terms of $t^{\mathbf{A}}$ and 0 and since $R \subseteq Pol_1(\mathbf{A})$, we have $Pol(\mathbf{M}) \subseteq Pol(\mathbf{A})$. Conversely, if $n, m \in \omega$ and s is an $(n+m)$-ary $\mathcal{T}$-term and $\mathbf{b} = b_1, \dots, b_m \in A$, consider the n-ary polynomial f of $\mathbf{A}$ defined by

$$f(a) = s^{\mathbf{A}}(\mathbf{a}, \mathbf{b}) \quad (\mathbf{a} = a_1, \dots, a_n \in A).$$

By the proof of Lemma 3.7 ((i)⇒(ii)), there exist homomorphisms $\alpha_1, \ldots, \alpha_{n+m}$ of $\hat{\mathbf{A}}$ such that

$$f(\mathbf{a}) = s^{\mathbf{A}}(\mathbf{a}, \mathbf{b}) = \sum_{i=1}^{n} \alpha_i(a_i) + \sum_{j=1}^{m} \alpha_{n+j}(b_j) \quad (\mathbf{a} = a_1, \ldots, a_n \in A).$$

Moreover, for each $i \in \{1, \ldots, n+m\}$, we can choose α_i so that if $\mathbf{0} := (0, \ldots, 0) \in A^{n+m}$ then

$$\alpha_i(c) = s^{\mathbf{A}}(0, \ldots, 0, c, 0, \ldots, 0) - s^{\mathbf{A}}(\mathbf{0}) \text{ for all } c \in A$$

(the second occurrence of c above being in the i^{th} co-ordinate), whence $\alpha_i(0) = 0$, i.e., $\alpha_i \in R$. Thus, in the language of the module $\mathbf{M}$, setting $v = \sum_{j=1}^{m} \alpha_{n+j}(b_j)$ $\in A$), we have

$$f(\mathbf{a}) = \sum_{i=1}^{n} \alpha_i(a_i) + v \text{ for all } \mathbf{a} = a_1, \ldots, a_n \in A,$$

so $f \in Pol_n(\mathbf{A})$. Thus, $Pol(\mathbf{A}) = Pol(\mathbf{M})$. □

3.2 Abelian Algebras in Modular Varieties. A ternary term that satisfies (i) and (ii) of the following theorem is called a *difference term.* In the next two results, the existence of a difference term in any modular variety is established (a result due to Herrmann and Gumm), its properties are described and it is used to characterize modular varieties.

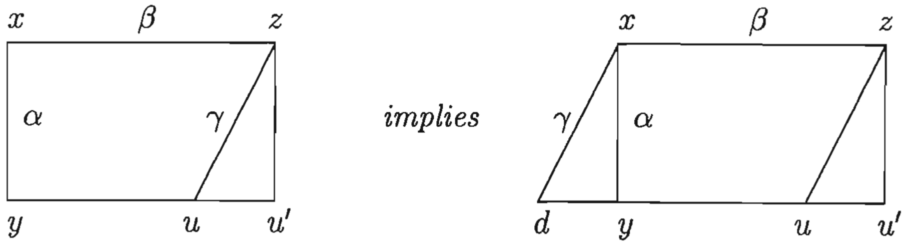
Theorem 3.10. [Her79] [Gum78] [Gum80a]

For each modular variety V of type $\mathcal{T}$ there is a ternary $\mathcal{T}$-term d, called a difference term, satisfying the following:

(i) $d(x, x, y) \approx y$ *is an identity of* V.

(ii) *If* $(a, b) \in \theta \in Con(\mathbf{A})$, *where* $\mathbf{A} \in V$, *then* $d^{\mathbf{A}}(a, b, b)[\theta, \theta]a$.

(iii) *If* $\alpha, \beta, \gamma \in Con(\mathbf{A})$, *where* $\mathbf{A} \in V$, *and* $x, y, z, u, u' \in A$ *and* $\alpha \cap \beta \subseteq \gamma$, *then*



with $d = d^{\mathbf{A}}(u, u', y)$.

Proof.

Let V be a modular $\mathcal{T}$-variety. Then there are $\mathcal{T}$-terms $m_0(x,y,z,u),\ldots,$ $m_n(x,y,z,u)$ such that V satisfies the identities of Theorem 2.1. Define $q_i(x,y,z), i=0,1,\ldots,n$, inductively by

$$\begin{aligned} q_0(x,y,z) &= z \\ q_{i+1}(x,y,z) &= \begin{cases} m_{i+1}(q_i(x,y,z),y,x,q_i(x,y,z)) & (i \text{ odd}) \\ m_{i+1}(q_i(x,y,z),x,y,q_i(x,y,z)) & (i \text{ even}) \end{cases} \end{aligned}$$

and set $d(x,y,z) = q_n(x,y,z)$.[18]

(i) We show by induction on i that $V \models q_i(x,x,y) \approx y$ for $i=1,\ldots,n$. This is clearly true for $i=0$. Suppose it is true for some $i \geq 0$. Then

$V \models q_{i+1}(x,x,y) \approx m_{i+1}(q_i(x,x,y),x,x,q_i(x,x,y))$

$\approx q_i(x,x,y)$ (by Theorem 2.1 (ii))

$\approx y$ (by the induction hypothesis),

as required. Now, setting $i=n$, we have $V \models d(x,x,y) \approx y$.

(ii) Let $\theta \in Con(\mathbf{A})$, where $\mathbf{A} \in V$. Let $(a,b) \in \theta$. We prove by induction on i that

$q_i^{\mathbf{A}}(a,b,b)[\theta,\theta]m_i^{\mathbf{A}}(b,b,b,a)$ for all odd $i \leq n$, and $q_i^{\mathbf{A}}(a,b,b)[\theta,\theta]m_i^{\mathbf{A}}(b,b,a,a)$ for all even $i \leq n$. .... (1)

Since, by Theorem 2.1 (i), $m_n(x,y,z,u) \approx u$, we shall then have $d^{\mathbf{A}}(a,b,b) = q_n^{\mathbf{A}}(a,b,b)[\theta,\theta]a$ (for n even or odd), as required.

By Theorem 2.1 (i) $(q_0^{\mathbf{A}}(a,b,b), m_0^{\mathbf{A}}(b,b,b,a)) = (b,b) \in id_A \subseteq [\theta,\theta]$.

Suppose i is odd and that (1) holds for i. Then $q_{i+1}^{\mathbf{A}}(a,b,b)$ $= m_{i+1}^{\mathbf{A}}(q_i^{\mathbf{A}}(a,b,b),b,a,q_i^{\mathbf{A}}(a,b,b))\,[\theta,\theta]\,m_{i+1}^{\mathbf{A}}(m_i^{\mathbf{A}}(b,b,b,a),b,a,m_i^{\mathbf{A}}(b,b,b,a))$.

Now by Theorem 2.1 (ii),

$m_{i+1}^{\mathbf{A}}(m_i^{\mathbf{A}}(b,b,b,a),b,b,m_i^{\mathbf{A}}(b,b,b,a)) = m_i^{\mathbf{A}}(b,b,b,a)$

$= m_{i+1}^{\mathbf{A}}(b,b,b,a)$ (by Theorem 2.1 (iv))

$= m_{i+1}^{\mathbf{A}}(m_i^{\mathbf{A}}(b,b,b,b),b,b,m_i^{\mathbf{A}}(a,a,a,a))$ (by Theorem 2.1 (ii)). .... (2)

Whenever $a_i\theta b_i, i=1,\ldots,n-1$, then for any n-ary term t,

$$\begin{bmatrix} t^{\mathbf{A}}(a,a_1,\ldots,a_{n-1}) & t^{\mathbf{A}}(a,b_1,\ldots,b_{n-1}) \\ t^{\mathbf{A}}(b,a_1,\ldots,a_{n-1}) & t^{\mathbf{A}}(b,b_1,\ldots,b_{n-1}) \end{bmatrix} \in M(\theta,\theta)$$

[18] This term was constructed by C. Herrmann [Her79]. The proof of this theorem given in [Gum80a] is different.

so if $t^{\mathbf{A}}(a, a_1, \ldots, a_{n-1}) = t^{\mathbf{A}}(a, b_1, \ldots, b_{n-1})$ then

$$(t^{\mathbf{A}}(b, a_1, \ldots, a_{n-1}), t^{\mathbf{A}}(b, b_1, \ldots, b_{n-1})) \in [\theta, \theta],$$

since $C(\theta, \theta; [\theta, \theta])$ holds. If we apply this term condition to the sixth argument of equation (2), we get

$$m^{\mathbf{A}}_{i+1}(m^{\mathbf{A}}_i(b,b,b,a), b, a, m^{\mathbf{A}}_i(b,b,b,a))[\theta,\theta]m^{\mathbf{A}}_{i+1}(m^{\mathbf{A}}_i(b,b,b,b), b, a, m^{\mathbf{A}}_i(a,a,a,a))$$

so $m^{\mathbf{A}}_{i+1}(m_i(b,b,b,a), b, a, m^{\mathbf{A}}_i(b,b,b,a))[\theta,\theta]m^{\mathbf{A}}_{i+1}(b,b,a,a)$, by Theorem 2.1 (ii), and by transitivity, $q^{\mathbf{A}}_{i+1}(a,b,b)[\theta,\theta]m^{\mathbf{A}}_{i+1}(b,b,a,a)$.

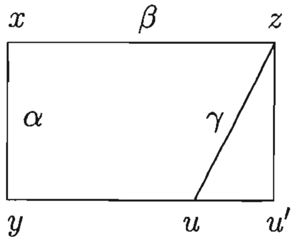
Now suppose i is even and that (1) holds for i. Then $q^{\mathbf{A}}_{i+1}(a,b,b)$
$= m^{\mathbf{A}}_{i+1}(q^{\mathbf{A}}_i(a,b,b), a, b, q^{\mathbf{A}}_i(a,b,b))[\theta,\theta]m^{\mathbf{A}}_{i+1}(m^{\mathbf{A}}_i(b,b,a,a), a, b, m^{\mathbf{A}}_i(b,b,a,a))$.
Now by Theorem 2.1 (ii),
$m_{i+1}(m^{\mathbf{A}}_i(b,b,a,a), a, a, m^{\mathbf{A}}_i(b,b,a,a)) = m^{\mathbf{A}}_i(b,b,a,a)$
$= m^{\mathbf{A}}_{i+1}(b,b,a,a)$ by Theorem 2.1 (iii)
$= m^{\mathbf{A}}_{i+1}(m^{\mathbf{A}}_i(b,b,b,b), b, a, m^{\mathbf{A}}_i(a,a,a,a))$ by Theorem 2.1 (ii). .... (3)

By an argument similar to the odd case, applied to the sixth argument of equation (3),

$$m^{\mathbf{A}}_{i+1}(m^{\mathbf{A}}_i(b,b,a,a), a, b, m^{\mathbf{A}}_i(b,b,a,a))[\theta,\theta]m^{\mathbf{A}}_{i+1}(m^{\mathbf{A}}_i(b,b,b,b), b, b, m^{\mathbf{A}}_i(a,a,a,a))$$

so $m^{\mathbf{A}}_{i+1}(m^{\mathbf{A}}_i(b,b,a,a), a, b, m^{\mathbf{A}}_i(b,b,a,a))[\theta,\theta]m^{\mathbf{A}}_{i+1}(b,b,b,a)$, by Theorem 2.1 (ii), and by transitivity, $q^{\mathbf{A}}_{i+1}(a,b,b)[\theta,\theta]m^{\mathbf{A}}_{i+1}(b,b,b,a)$ so the result follows[19].

(iii) Let $\alpha, \beta, \gamma \in Con(\mathbf{A})$, where $\mathbf{A} \in V$, and let $x, y, z, u, u' \in A$ and $\alpha \cap \beta \subseteq \gamma$. We show that any $\mathcal{T}$-term $d(x,y,z)$ which satisfies (i) and (ii) will satisfy (iii). Suppose $d(x,y,z)$ is a $\mathcal{T}$-term which which satisfies (i) and (ii) and that



where $\alpha \cap \beta \subseteq \gamma$.

We have $(u, y), (u', y) \in \beta$ so, by (i), $d^{\mathbf{A}}(u, u', y)\beta\, d^{\mathbf{A}}(y,y,y) = y$.

[19] According to [FM87], this proof of (ii) is due to W. Taylor [Tay82]. The proof of (iii) is really a proof that, for a ternary term d, (i) and (ii) imply (iii) and is due to Udi Hrushovskii (according to [FM87]).

Also $(u,z) \in \gamma$ so $d^{\mathbf{A}}(u,u',y)\gamma\, d^{\mathbf{A}}(z,u',y)$. .... (4)

Also $(u',z),(y,x) \in \alpha$ so, by (i), $d^{\mathbf{A}}(z,u',y)\alpha\, d^{\mathbf{A}}(z,z,x) = x$. .... (5)

Also $(z,x),(u',y) \in \beta$ so $d^{\mathbf{A}}(z,u',y)\beta\, d^{\mathbf{A}}(x,y,y)$. .... (6)

We have $(z,x) \in \beta$, and $(z,u) \in \gamma$ and $(u,y) \in \beta$ so $(x,y) \in \beta \circ \gamma \circ \beta \subseteq \beta \vee \gamma$, therefore $(x,y) \in \alpha \cap (\beta \vee \gamma)$.

By (ii), $d^{\mathbf{A}}(x,y,y)[\alpha \cap (\beta \vee \gamma), \alpha \cap (\beta \vee \gamma)]x$. .... (7)

By Propositions 2.9 and 2.12, $[\alpha \cap (\beta \vee \gamma), \alpha \cap (\beta \vee \gamma)] \subseteq [\alpha, \beta \vee \gamma] = [\alpha,\beta] \vee [\alpha,\gamma] \subseteq (\alpha \cap \beta) \vee (\alpha \cap \gamma) = \alpha \cap \gamma$, (since $\alpha \cap \beta \subseteq \gamma$).

By (7) therefore, $d^{\mathbf{A}}(x,y,y)(\alpha \cap \gamma)x$ and by (6), $d^{\mathbf{A}}(x,y,y)\beta\, d^{\mathbf{A}}(z,u',y)$ so $d^{\mathbf{A}}(z,u',y)(\beta \vee (\alpha \cap \gamma))x$. By (5), $d^{\mathbf{A}}(z,u',y)\alpha x$ so $d^{\mathbf{A}}(z,u',y)(\alpha \cap (\beta \vee (\alpha \cap \gamma)))x$. Now

$\alpha \cap (\beta \vee (\alpha \cap \gamma)) = (\alpha \cap \gamma) \vee (\alpha \cap \beta)$ (by modularity, since $\alpha \cap \gamma \subseteq \alpha$)

$= \alpha \cap \gamma$ so $d(z,u',y)(\alpha \cap \gamma)x$.

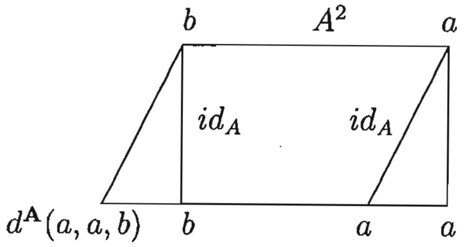
By (4) $d^{\mathbf{A}}(u,u',y)\gamma\, d^{\mathbf{A}}(z,u',y)$ so $d^{\mathbf{A}}(u,u',y)(\gamma \vee (\alpha \cap \gamma))x$, therefore $d^{\mathbf{A}}(u,u',y)\gamma x$. □

Corollary 3.11. [Gum80a]

Let V be a $\mathcal{T}$-variety and $d(x,y,z)$ a $\mathcal{T}$-term satisfying Theorem 3.10 (iii). Then V is modular and Theorem 3.10 (i) and (ii) hold for this d.

Proof.

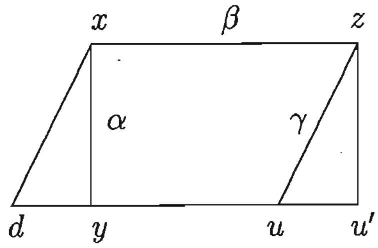
We first show Theorem 3.10 (i) holds for d. Let $a, b \in A$, where $\mathbf{A} \in V$. Consider the diagram:



Since $id_A, A^2 \in Con(\mathbf{A})$ and $id_A \cap A^2 \subseteq id_A$, Theorem 3.10 (iii) implies $(d^{\mathbf{A}}(a,a,b), b) \in id_A$. This holds for any $a, b \in A$, and for any $\mathbf{A} \in V$, therefore $d(x,x,y) \approx y$ is an identity of V.

We show V is modular. Let $\alpha, \beta, \gamma \in Con(\mathbf{A})$ with $\alpha \cap \beta \subseteq \gamma$. Suppose the situation depicted in the following diagram obtains.

By Theorem 3.10 (iii) we have $(x, d^{\mathbf{A}}(u,u',y)) \in \gamma$.



Taking $u = u^{'}$, we have $(z, u) \in \gamma$ and $d^{\mathbf{A}}(u, u^{'}, y) = d^{\mathbf{A}}(u, u, y) = y$ (by (i)). Thus, condition (iv) of Theorem 2.3 is satisfied. Therefore, by the equivalence of Theorem 2.3 (i) and (iv), V is modular.

We show Theorem 3.10 (ii) holds. Recall that $\mathbf{A}(\theta)$ denotes θ, considered as a subalgebra of $\mathbf{A}^2$. Let

$$\begin{bmatrix} a \\ b \end{bmatrix} \in \mathbf{A}(\theta).$$

Then $((b, b), (b, b)), ((a, b), (a, b)) \in \eta_0$ and $((b, b), (a, b)) \in \eta_1$ where η_0, η_1 are the kernels of the first and second projection homomorphisms p_0, p_1 (from $\mathbf{A}(\theta)$ onto $\mathbf{A}$) respectively.

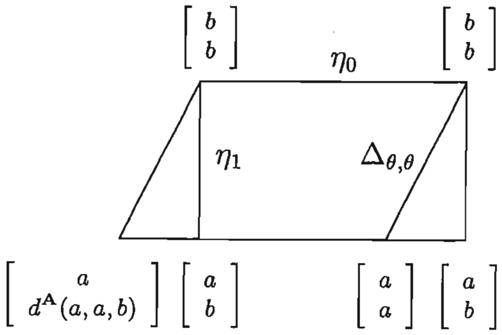
Let $\Delta_{\theta,\theta}$ and be as in Definition 2.18. Now

$$\begin{bmatrix} a & b \\ a & b \end{bmatrix} \in \Delta_{\theta,\theta}$$

since $(a, b) \in \theta$. By Theorem 3.10 (i), since $(a, b) \in \theta$, we have $(a, d^{\mathbf{A}}(a, b, b)) = (d^{\mathbf{A}}(a, a, a), d^{\mathbf{A}}(a, b, b)) \in \theta$ and

$$\begin{bmatrix} a \\ d^{\mathbf{A}}(a, b, b) \end{bmatrix}, \begin{bmatrix} a \\ b \end{bmatrix} \in \begin{bmatrix} a \\ a \end{bmatrix} / \eta_0.$$

We also have $\eta_0 \cap \eta_1 = id_A \subseteq \Delta_{\theta,\theta}$ so we have the following diagram:


$\begin{bmatrix} b \\ b \end{bmatrix}$
η_0
$\begin{bmatrix} b \\ b \end{bmatrix}$
η_1
$\Delta_{\theta,\theta}$
$\begin{bmatrix} a \\ d^{\mathbf{A}}(a, a, b) \end{bmatrix}$
$\begin{bmatrix} a \\ b \end{bmatrix}$
$\begin{bmatrix} a \\ a \end{bmatrix}$
$\begin{bmatrix} a \\ b \end{bmatrix}$

Thus by Theorem 3.10 (iii) we have

$$\begin{bmatrix} b \\ b \end{bmatrix} \Delta_{\theta,\theta}\, d^{\mathbf{A}}\left(\begin{bmatrix} a \\ a \end{bmatrix}, \begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} a \\ b \end{bmatrix}\right) = \begin{bmatrix} d^{\mathbf{A}}(a,a,a) \\ d^{\mathbf{A}}(a,b,b) \end{bmatrix} = \begin{bmatrix} a \\ d^{\mathbf{A}}(a,b,b) \end{bmatrix}$$

(by (i)) so

$$\begin{bmatrix} a & b \\ d^{\mathbf{A}}(a,b,b) & b \end{bmatrix} \in \Delta_{\theta,\theta}.$$

By Theorem 2.25 ((iii)⇒ (i)) we have $a[\theta,\theta]d^{\mathbf{A}}(a,b,b)$.

□

If S is a set then a ternary operation $f : S^3 \to S$ is said to *commute with itself* if, whenever $a_i, b_i, c_i \in S$ for all $i \in \{1,2,3\}$, then

$$t(t(a_1,b_1,c_1),t(a_2,b_2,c_2),t(a_3,b_3,c_3)) = t(t(a_1,a_2,a_3),t(b_1,b_2,b_3),t(c_1,c_2,c_3)).$$

Lemma 3.12. [FM87, Lemma 5.6]

Let $t(x,y,z)$ be a ternary operation on a set S such that t commutes with itself and S satisfies the Mal'cev equation $t(x,x,y) \approx y \approx t(y,x,x)$. For any fixed $a \in S$ the operation $x+y = t(x,a,y)$ defines an Abelian group on S with a as identity element and with $-x = t(a,x,a)$. Moreover, $t(x,y,z) = x-y+z$.

Proof.

We know that $\langle S;t\rangle$ satisfies $t(x,x,y) \approx y \approx t(y,x,x)$ .... (*)

Let $x,y,z \in S$.

(1) a is the identity element for the above operation $+$:

$x + a = t(x,a,a) = a = t(a,a,x) = a + x.$

(2) Associativity of $+$:

$x + (y+z) = t(x,a,t(y,a,z))$

$= t(t(x,a,a),t(a,a,a),t(y,a,z))$ (by (*))

$= t(t(x,a,y),t(a,a,a),t(a,a,z))$ (by commutativity of t with itself)

$= t(t(x,a,y),a,z)$ (by (*))

$= (x+y)+z.$

(3) Commutativity of $+$:

$x + y = t(x,a,y)$

$= t(t(a,a,x),t(a,a,a),t(y,a,a))$ (by (*))

$= t(t(a,a,y),t(a,a,a),t(x,a,a))$ (by commutativity of t with itself)

$= t(y,a,x)$ (by (*))

$= y + x$.

(4) Let $-x = t(a, x, a)$. Then

$x + (-x) = t(x, a, t(a, x, a))$

$= t(t(a, a, x), t(a, x, x), t(a, x, a))$ (by (*))

$= t(t(a, a, a), t(a, x, x), t(x, x, a))$ (by commutativity of t with itself)

$= t(a, a, a)$ (by (*))

$= a$. By (3), $(-x) + x = a$.

(5) We show $x - y + z = t(x, y, z)$. We first show $x - y = t(x, y, a)$:

$x - y = x + (-y) = t(x, a, t(a, y, a))$ (by (4))

$= t(t(x, a, a), t(a, a, a), t(a, y, a))$ (by (*))

$= t(t(x, a, a), t(a, a, y), t(a, a, a))$ (by commutativity of t with itself)

$= t(x, y, a)$ (by (*)).

Now $x - y + z = (x - y) + z = t(t(x, y, a), a, z)$

$= t(t(x, y, a), t(a, a, a), t(a, a, z))$ (by (*))

$= t(t(x, a, a), t(y, a, a), t(a, a, z))$ (by commutativity of t with itself)

$= t(x, y, z)$ (by (*)). □

It is easy to show that a difference operation t of a ternary group $\langle A; t\rangle$ commutes with itself (on A) (see Definition 3.5) . Recall that if V is a modular variety and d is a ternary term for which (i) and (ii) (and hence (iii)) of Theorem 3.10 are true then d is called a *difference term* for V.

Proposition 3.13. [Gum80a]

Let V be a modular variety and d any difference term for V. Let $\alpha, \beta \in Con(\mathbf{A})$, where $\mathbf{A} \in V$ and $\alpha \supseteq \beta$. Then $[\alpha, \beta] = id_A$ if and only if for any $n \in \omega$ and any n-ary fundamental operation (and hence any n-ary term operation) $s^{\mathbf{A}}$ and elements $\mathbf{a} = (a_1, \dots, a_n), \mathbf{b} = (b_1, \dots, b_n), \mathbf{c} = (c_1, \dots, c_n) \in A^n$ such that $a_i\beta b_i\alpha c_i$ $(i = 1, \dots, n)$, we have

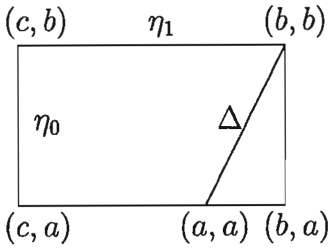
$$d^{\mathbf{A}}(s^{\mathbf{A}}(\mathbf{a}), s^{\mathbf{A}}(\mathbf{b}), s^{\mathbf{A}}(\mathbf{c})) = s^{\mathbf{A}}(d^{\mathbf{A}}(a_1, b_1, c_1), \dots, d^{\mathbf{A}}(a_n, b_n, c_n))$$

$$\text{and } (b, c) \in \beta \text{ implies } d^{\mathbf{A}}(b, c, c) = d^{\mathbf{A}}(c, c, b) = b.$$

Proof.

($\Rightarrow$) Suppose $[\alpha, \beta] = id_A$. Let $s^{\mathbf{A}}$ be an n-ary fundamental operation of $\mathbf{A}$ and let $\mathbf{a} = (a_1, \dots, a_n), \mathbf{b} = (b_1, \dots, b_n), \mathbf{c} = (c_1, \dots, c_n) \in A^n$ such that $a_i\beta b_i\alpha c_i$ for all $i \in \{1, \dots, n\}$. Then $s^{\mathbf{A}}(\mathbf{a})\beta s^{\mathbf{A}}(\mathbf{b})\alpha s^{\mathbf{A}}(\mathbf{c})$.

Let η_0, η_1 be the kernels of the first and second projection homomorphisms from the algebra $\mathbf{A}(\alpha)$ onto $\mathbf{A}$ and let $\Delta = \Delta_{\alpha,\beta}$ (as defined in Definition 2.18). Now $\eta_0 \cap \eta_1 = id_A \subseteq \Delta_{\alpha,\beta}$. Let $a, b, c \in A$ such that $a\beta b\alpha c$. Then we have the diagram:



By Theorem 3.10 (i),(iii),
$(d^{\mathbf{A}}(a,b,c),a) = (d^{\mathbf{A}}(a,b,c), d^{\mathbf{A}}(a,a,a)) = d^{\mathbf{A}^2}((a,a),(b,a),(c,a))\Delta(c,b)$.
In particular, $(d^{\mathbf{A}}(s^{\mathbf{A}}(\mathbf{a}), s^{\mathbf{A}}(\mathbf{b}), s^{\mathbf{A}}(\mathbf{c})), s^{\mathbf{A}}(\mathbf{a}))\Delta(s^{\mathbf{A}}(\mathbf{c}), s^{\mathbf{A}}(\mathbf{b}))$ ....(1)
and for $i \in \{1,\dots,n\}$, $(d^{\mathbf{A}}(a_i,b_i,c_i),a_i)\Delta(c_i,b_i)$, so by compatibility
$s^{\mathbf{A}^2}((d^{\mathbf{A}}(a_1,b_1,c_1),a_1),\dots,(d^{\mathbf{A}}(a_n,b_n,c_n),a_n))\Delta\, s^{\mathbf{A}^2}((c_1,b_1),\dots,(c_n,b_n))$,
i.e., $(s^{\mathbf{A}}(d^{\mathbf{A}}(a_1,b_1,c_1),\dots,d^{\mathbf{A}}(a_n,b_n,c_n)), s^{\mathbf{A}}(\mathbf{a}))\Delta\,(s^{\mathbf{A}}(\mathbf{c}), s^{\mathbf{A}}(\mathbf{b}))$. ....(2)

From (1) and (2) by transitivity we have
$(d^{\mathbf{A}}(s^{\mathbf{A}}(\mathbf{a}), s^{\mathbf{A}}(\mathbf{b}), s^{\mathbf{A}}(\mathbf{c})), s^{\mathbf{A}}(\mathbf{a}))\Delta\,(s^{\mathbf{A}}(d^{\mathbf{A}}(a_1,b_1,c_1),\dots,d^{\mathbf{A}}(a_n,b_n,c_n)), s^{\mathbf{A}}(\mathbf{a}))$,

i.e., $\begin{bmatrix} d^{\mathbf{A}}(s^{\mathbf{A}}(\mathbf{a}), s^{\mathbf{A}}(\mathbf{b}), s^{\mathbf{A}}(\mathbf{c})) & s^{\mathbf{A}}(d^{\mathbf{A}}(a_1,b_1,c_1),\dots,d^{\mathbf{A}}(a_n,b_n,c_n)) \\ s^{\mathbf{A}}(\mathbf{a}) & s^{\mathbf{A}}(\mathbf{a}) \end{bmatrix} \in \Delta.$

By the equivalence of (i) and (iv) in Theorem 2.25 (ii), we have
$(d^{\mathbf{A}}(s^{\mathbf{A}}(\mathbf{a}), s^{\mathbf{A}}(\mathbf{b}), s^{\mathbf{A}}(\mathbf{c})), s^{\mathbf{A}}(d^{\mathbf{A}}(a_1,b_1,c_1),\dots,d^{\mathbf{A}}(a_n,b_n,c_n))) \in [\alpha,\beta] = id_A$
so $d^{\mathbf{A}}(s^{\mathbf{A}}(\mathbf{a}), s^{\mathbf{A}}(\mathbf{b}), s^{\mathbf{A}}(\mathbf{c})) = s^{\mathbf{A}}(d^{\mathbf{A}}(a_1,b_1,c_1),\dots,d^{\mathbf{A}}(a_n,b_n,c_n))$.

Now suppose $(b,c) \in \beta$. By Theorem 3.10 (i), (ii), $d^{\mathbf{A}}(c,c,b) = b$ and $d^{\mathbf{A}}(b,c,c)[\beta,\beta]b$. But $\beta \subseteq \alpha$ and therefore $[\beta,\beta] \subseteq [\alpha,\beta] = id_A$ by order-preservation, so $d^{\mathbf{A}}(b,c,c) = b$.

($\Leftarrow$) Suppose the conditions on operations hold. We show $[\alpha,\beta] = id_A$.

We first show that the congruence relation $\Delta_{\beta,\alpha}$ on $\mathbf{A}(\beta)$ is characterized by $(a,b)\Delta_{\beta,\alpha}(c,v)$ if and only if $a\beta b\alpha c$ and $v = d^{\mathbf{A}}(b,a,c)$. Let Δ' be the relation on A^2 defined as follows:

$$\Delta' = \{((a,b),(c,v)) : a\beta b\alpha c \text{ and } v = d^{\mathbf{A}}(b,a,c)\}.$$

First note that $\Delta' \subseteq \beta \times \beta$ since if $((a,b),(c,v)) \in \Delta'$ then

$$c = d^{\mathbf{A}}(a,a,c)\beta d^{\mathbf{A}}(b,a,c) = v.$$

Reflexivity:

For $(a,b) \in \mathbf{A}(\beta)$, we have $a\beta b\beta a$ but $\beta \subseteq \alpha$ so $a\beta b\alpha a$. Also $d^{\mathbf{A}}(b,a,a) = b$, since $(b,a) \in \beta$, so $((a,b),(a,b)) \in \Delta'$.

Symmetry:

Let $((a,b),(c,v)) \in \Delta'$. Then $a\beta b\alpha c$ and $v = d^{\mathbf{A}}(b,a,c)$. .... (3)

We show $((c,v),(a,b)) \in \Delta'$, i.e., $c\beta v\alpha a$ and $b = d^{\mathbf{A}}(v,c,a)$.

Since $\Delta' \subseteq \beta \times \beta$, $(c,v),(a,b) \in \beta \subseteq \alpha$ and $(b,c) \in \alpha$ by (3). Therefore $(a,v) \in \alpha$ by transitivity of α, so $c\beta v\alpha a$. We also have

$d^{\mathbf{A}}(v,c,a) = d^{\mathbf{A}}(d^{\mathbf{A}}(b,a,c), d^{\mathbf{A}}(a,a,c), d^{\mathbf{A}}(a,a,a))$ (by (3) and Theorem 3.10 (i))

$= d^{\mathbf{A}}(d^{\mathbf{A}}(b,a,a), d^{\mathbf{A}}(a,a,a), d^{\mathbf{A}}(c,c,a))$ (by assumption since $b\beta a$ and $c\alpha a$)

$= d^{\mathbf{A}}(b,a,a) = b$ (by Theorem 3.10 (i) and since $(b,a) \in \beta$).

Transitivity:

Let $((a,b),(c,v)),((c,v),(r,s)) \in \Delta'$.

We show $((a,b),(r,s)) \in \Delta'$, i.e., $a\beta b\alpha r$ and $s = d^{\mathbf{A}}(b,a,r)$. We have $a\beta b\alpha c$, $c\beta v\alpha r$, $v = d^{\mathbf{A}}(b,a,c)$ and $s = d^{\mathbf{A}}(v,c,r)$ so $(b,c) \in \alpha$ and $(c,v) \in \beta \subseteq \alpha$ so $(b,c),(c,v),(v,r) \in \alpha$. Therefore $(b,r) \in \alpha$, by transitivity of α, so $a\beta b\alpha r$. By our assumptions and Theorem 3.10 (i) and since $(a,b) \in \beta$ and $(c,r) \in \alpha$,

$d^{\mathbf{A}}(b,a,r) = d^{\mathbf{A}}(d^{\mathbf{A}}(b,b,b), d^{\mathbf{A}}(a,b,b), d^{\mathbf{A}}(c,c,r))$

$= d^{\mathbf{A}}(d^{\mathbf{A}}(b,a,c), d^{\mathbf{A}}(b,b,c), d^{\mathbf{A}}(b,b,r))$

$= d^{\mathbf{A}}(v,c,r) = s.$

Compatibility:

Let f be an n-ary fundamental operation symbol of $\mathbf{A}$'s type. Suppose $((a_i,b_i),(c_i,v_i)) \in \Delta'$ for $i \in \{0,1,\dots,n\}$. Then for each i we have $a_i\beta b_i\alpha c_i$ and $v_i = d^{\mathbf{A}}(b_i,a_i,c_i)$.

We show $f^{\mathbf{A}(\beta)}((a_1,b_1),\dots,(a_n,b_n))\Delta' f^{\mathbf{A}(\beta)}((c_1,v_1),\dots,(c_n,v_n))$, i.e., we show

$f^{\mathbf{A}}(a_1,\dots,a_n)\beta f^{\mathbf{A}}(b_1,\dots,b_n)\alpha f^{\mathbf{A}}(c_1,\dots,c_n)$ and

$f^{\mathbf{A}}(v_1,\dots,v_n) = d^{\mathbf{A}}(f^{\mathbf{A}}(b_1,\dots,b_n), f^{\mathbf{A}}(a_1,\dots,a_n), f^{\mathbf{A}}(c_1,\dots,c_n))$.

For each $i \in \{1,\dots,n\}$ we have $f^{\mathbf{A}}(a_1,\dots,a_n)\beta f^{\mathbf{A}}(b_1,\dots,b_n)$ and $f^{\mathbf{A}}(b_1,\dots,b_n)\alpha f^{\mathbf{A}}(c_1,\dots,c_n)$ by compatibility of β, $\alpha \in Con(\mathbf{A})$.

Now $f^{\mathbf{A}}(v_1,\dots,v_n) = f^{\mathbf{A}}(d^{\mathbf{A}}(b_1,a_1,c_1),\dots,d^{\mathbf{A}}(b_n,a_n,c_n))$

$= d^{\mathbf{A}}(f^{\mathbf{A}}(b_1,\dots,b_n), f^{\mathbf{A}}(a_1,\dots,a_n), f^{\mathbf{A}}(c_1,\dots,c_n))$, by our assumptions.

Thus Δ' is a congruence relation on $\mathbf{A}(\beta)$.

$\Delta_{\beta,\alpha}$ is the congruence relation on $\mathbf{A}(\beta)$ generated by $\{((x,x),(u,u)) : x\alpha u\}$ by Definition 2.18. Now if $a, c \in A$ and $a\alpha c$ then $a\beta a\alpha c$ and $c = d^{\mathbf{A}}(a,a,c)$ by Theorem 3.10 (i), so $((a,a),(c,c)) \in \Delta'$. Thus, Δ' contains a set of generators of $\Delta_{\beta,\alpha}$, therefore $\Delta_{\beta,\alpha} \subseteq \Delta'$.

Suppose $(a,b)\Delta'(c,v)$. Then $a\beta b\alpha c$ so $(a,b) \in \alpha$ and $v = d^{\mathbf{A}}(b,a,c)$. By our assumptions and Theorem 3.10 (i)

$$\begin{bmatrix} a & c \\ b & v \end{bmatrix} = \begin{bmatrix} d^{\mathbf{A}}(a,b,b) & d^{\mathbf{A}}(b,b,c) \\ d^{\mathbf{A}}(a,a,b) & d^{\mathbf{A}}(b,a,c) \end{bmatrix} \in M(\beta,\alpha) \subseteq \Delta_{\beta,\alpha}$$

(using $t(x_1,y_1,y_2) := d(y_1,x_1,y_2)$ in the definition of $M(\beta,\alpha)$). Thus, $\Delta' \subseteq \Delta_{\beta,\alpha}$ so $\Delta' = \Delta_{\beta,\alpha}$. [20]

Finally, we show $[\alpha,\beta] = id_A$. Let $(a,b) \in [\alpha,\beta] = [\beta,\alpha]$. Then

$$\begin{bmatrix} a & b \\ b & b \end{bmatrix} \in \Delta_{\beta,\alpha}$$

by the equivalence of (i) and (ii) in Theorem 2.25. Now $(b,b)\Delta_{\beta,\alpha}(a,b)$ by symmetry, therefore $(b,b)\Delta'(a,b)$. Consequently, $d^{\mathbf{A}}(b,b,a) = b$ but $d^{\mathbf{A}}(b,b,a) = a$, by Theorem 3.10 (i). Therefore $b = a$, so $[\alpha,\beta] = id_A$. □

Suppose V is a modular variety with difference term d and $\mathbf{A} \in V$ and $u \in A$ and $\beta \in Con(\mathbf{A})$. Then the congruence class $u/\beta = \{a \in A : (a,u) \in \beta\}$ is closed under $d^{\mathbf{A}}$, because if $a,b,c \in u/\beta$ then $d^{\mathbf{A}}(a,b,c)\beta d^{\mathbf{A}}(u,u,u) = u$ (by Theorem 3.10 (i)). In this case, the algebra $\langle u/\beta; d^{\mathbf{A}}\rangle$ is denoted by $\mathbf{M}(\beta,u)$[21].

Setting $\alpha = \beta$ in the previous proposition, we get:

Corollary 3.14. [Her79]

Let V be a modular $\mathcal{T}$-variety with difference term d and let $\mathbf{A} \in V$. A congruence relation β on $\mathbf{A}$ is Abelian if and only if for each $u \in A$, $\mathbf{M}(\beta,u)$ is a ternary group and whenever $s^{\mathbf{A}}(u_1,\ldots,u_n) = u$ where s is an n-ary $\mathcal{T}$-term, then $s^{\mathbf{A}}$ restricts to a homomorphism $\mathbf{M}(\beta,u_1) \times \ldots \times \mathbf{M}(\beta,u_n) \to \mathbf{M}(\beta,u)$ (of ternary groups). We express this last property by saying that s is affine between the congruence classes of β. [22]

[20] In fact, our proof shows that $\Delta' = M(\beta,\alpha)$, so $M(\alpha,\beta) \in Con(\mathbf{A}(\beta))$ under the assumptions of this proposition.

[21] In Freese and McKenzie's notation $\mathbf{M}(\beta,u)$, the $\mathbf{M}$ is intended to suggest "module". The reader is entreated not to confuse $\mathbf{M}(\beta,u)$ with the $\mathbf{M}(\beta,\alpha)$ of Definition 2.6.

[22] In view of the proof and the previous proposition, this corollary clearly remains true if we replace "term" by "fundamental operation symbol".

Proof.

Let $\beta \in Con\mathbf{A}$.

($\Rightarrow$) Suppose $[\beta,\beta] = id_A$. Let $n \in \omega$ and $u, u_1, \ldots, u_n \in A$ and let s be an n-ary $\mathcal{T}$-term with $s^{\mathbf{A}}(u_1, \ldots, u_n) = u$. In what follows, $\mathbf{a} = (a_1, \ldots, a_n)$, $\mathbf{b} = (b_1, \ldots, b_n)$ and $\mathbf{c} = (c_1, \ldots, c_n)$ denote elements of A^n.

For $i = 1, \ldots, n$ if $a_i, b_i, c_i \in u_i/\beta$ then $a_i \beta b_i \beta c_i$. If this is true for all i then $s^{\mathbf{A}}(\mathbf{a}) \beta s^{\mathbf{A}}(\mathbf{b}) \beta s^{\mathbf{A}}(\mathbf{c}) \beta u$, so by Proposition 3.13,

$$s^{\mathbf{A}}(d^{\mathbf{A}^n}(\mathbf{a},\mathbf{b},\mathbf{c})) = s^{\mathbf{A}}(d^{\mathbf{A}}(a_1,b_1,c_1), \ldots, d^{\mathbf{A}}(a_n,b_n,c_n))$$
$$= d^{\mathbf{A}}(s^{\mathbf{A}}(\mathbf{a}), s^{\mathbf{A}}(\mathbf{b}), s^{\mathbf{A}}(\mathbf{c})), \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

whence $s^{\mathbf{A}}$ restricts a homomorphism from $\prod_{i=1}^n \mathbf{M}(\beta, u_i)$ into $\mathbf{M}(\beta, u)$. Also, for any $v, w \in u/\beta$, since $(v, w) \in \beta$, we have $d^{\mathbf{A}}(v, v, w) = w = d^{\mathbf{A}}(w, v, v)$. Moreover, setting $n = 3$ and $s = d$ and $u_1 = u_2 = u_3 = u$ in (1), we conclude that the restriction to u/β of $d^{\mathbf{A}}$ commutes with itself (on u/β). Thus, by Lemma 3.12, $\mathbf{M}(\beta, u)$ is a ternary group (and is d-affine).

($\Leftarrow$) Assume that the conditions of the corollary hold. If $(b, c) \in \beta$ then, since $\mathbf{M}(\beta, b) = \mathbf{M}(\beta, c)$ is a ternary group, $d^{\mathbf{A}}(b, c, c) = b = d^{\mathbf{A}}(c, c, b)$. Let $n, s, \mathbf{a}, \mathbf{b}, \mathbf{c}$ be as in Proposition 3.13, with $\alpha = \beta$. Then $\mathbf{M}(\beta, a_i) = \mathbf{M}(\beta, b_i) = \mathbf{M}(\beta, c_i)$ and $\mathbf{M}(\beta, s^{\mathbf{A}}(\mathbf{a})) = \mathbf{M}(\beta, s^{\mathbf{A}}(\mathbf{b})) = \mathbf{M}(\beta, s^{\mathbf{A}}(\mathbf{c}))$ are ternary groups for each $i \in \{1, \ldots, n\}$ and, by assumption, $s^{\mathbf{A}}$ restricts to a homomorphism from $\prod_{i=1}^n \mathbf{M}(\beta, a_i)$ into $\mathbf{M}(\beta, s^{\mathbf{A}}(a))$, which means just that (1) holds (with $u = s^{\mathbf{A}}(\mathbf{a})$). Thus, by Proposition 3.13, $[\beta, \beta] = id_A$.

□

We are now in a position to derive:

Corollary 3.15. (The Fundamental Theorem of Abelian Algebras) *(C. Herrmann* [Her79]*)*

In a modular variety every Abelian algebra is affine, and conversely.

Proof.

Let V be a modular variety. Let d be a difference term for V. Suppose $\mathbf{A} \in V$ is an Abelian algebra, i.e. A^2 is an Abelian congruence on $\mathbf{A}$. By Corollary 3.14, for any $u \in A$, $\mathbf{M}(A^2, u) = \langle u/A^2; d^{\mathbf{A}} \rangle = \langle A; d^{\mathbf{A}} \rangle$ is a ternary group and $\mathbf{A}$ is d-affine.

The converse follows from Proposition 3.6. □

3.3 More on Abelian Congruences. The remaining results of this chapter will be needed in Chapter 4. In particular, the following lemma is used in the proof of Theorem 4.11 where it replaces a complicated argument from [FM81].

Recall that if $\mathbf{A}$ is an algebra and $X \subseteq A^2$ then $\sigma^{\mathbf{A}}(X)$ is the least semicongruence (i.e. reflexive compatible relation) on $\mathbf{A}$ containing X.

Lemma 3.16. *Let V be a modular variety and let $\mathbf{A} \in V$ and let β be an Abelian congruence of $\mathbf{A}$. Let η be a semicongruence of $\mathbf{A}$ with $\eta \subseteq \beta$. Then $\eta \in Con(\mathbf{A})$. Thus, if $X \subseteq \beta$ then $\sigma^{\mathbf{A}}(X) = \Theta^{\mathbf{A}}(X)$.*

Proof.

Let d be a difference term for V. Thus $V \models d(x,x,y) \approx y$ and if $(u,v) \in \beta$ then $d^{\mathbf{A}}(u,v,v) = u$, by Proposition 3.13 (or Theorem 3.10, using $[\beta,\beta] = id_A$).

We need to show that η is symmetric and transitive. Let $a,b,c \in A$ with $(a,b),(b,c) \in \eta$. We need to show that $(b,a),(a,c) \in \eta$. Now

$b = d^{\mathbf{A}}(a,a,b)\eta\, d^{\mathbf{A}}(a,b,b) = a$ (because $(a,b) \in \eta \subseteq \beta$).

Also $b = d^{\mathbf{A}}(b,b,a)\eta\, d^{\mathbf{A}}(c,b,b) = c$ (because $(b,c) \in \eta \subseteq \beta$), as required. □

Definition 3.17.

Let $\mathbf{A} \in V$, where V is a modular $\mathcal{T}$-variety, let $z, z' \in A$ and let β be an Abelian congruence on $\mathbf{A}$. Let $Hom(\beta, z, z')$ denote the set of functions $g : \mathbf{M}(\beta, z) \to \mathbf{M}(\beta, z')$ of the form $g(x) = f^{\mathbf{A}}(x, z, z', c_0, \ldots, c_{k-1})$ .... (i)

where $k \in \omega$, $c_0, \ldots, c_{k-1} \in A$ and f is a $(k+3)$-ary $\mathcal{T}$-term, such that V satisfies $f(v, v, v', y_0, \ldots, y_{k-1}) \approx v'$. .... (ii)

Note that (i) and (ii) alone ensure that $g[M(\beta,\alpha)] \subseteq M(\beta, z')$. Also note that any $g \in Hom(\beta, z, z')$ is a homomorphism of ternary groups, by Corollary 3.14. Indeed, if $\mathbf{x} = (x_1, x_2, x_3) \in (z/\beta)^3$ and $\mathbf{w}$ abbreviates (w,w,w) whenever $w \in \{z, z', c_0, \ldots, c_{k-1}\}$ and $\mathbf{c} = (c_0, \ldots, c_{k-1})$ then

$g(d^{\mathbf{A}}(\mathbf{x})) = f^{\mathbf{A}}(d^{\mathbf{A}}(\mathbf{x}), d^{\mathbf{A}}(\mathbf{z}), d^{\mathbf{A}}(\mathbf{z}'), d^{\mathbf{A}}(\mathbf{c}_0), \ldots, d^{\mathbf{A}}(\mathbf{c}_{k-1}))$

$= d^{\mathbf{A}}(f^{\mathbf{A}}(x_1, z, z', \mathbf{c}), f^{\mathbf{A}}(x_2, z, z', \mathbf{c}), f^{\mathbf{A}}(x_3, z, z', \mathbf{c})) = d^{\mathbf{A}}(g(x_1), g(x_2), g(x_3))$.

Since $g(z) = z'$, it follows that g is also a homomorphism between the Abelian groups $\langle z/\beta; \oplus, -, z\rangle$ (where $x \oplus y = d^{\mathbf{A}}(x,z,y)$) and $\langle z'/\beta; \oplus, -, z'\rangle$ (where $x \oplus y = d^{\mathbf{A}}(x, z', y)$).

Lemma 3.18. [FM87, Lemma 9.1]

Let V be a modular $\mathcal{T}$-variety with difference term d. Let $\mathbf{A} \in V$ and $z, z' \in A$ and let β be an Abelian congruence of $\mathbf{A}$. Then $Hom(\beta, z, z')$ is the set of restrictions to z/β of unary polynomials on $\mathbf{A}$ which map z to z'.

Proof.

($\Rightarrow$) Let $g \in Hom(\beta, z, z')$, say $g(x) = f^{\mathbf{A}}(x, z, z', c_0, \ldots, c_{k-1})$ for all $x \in z/\beta$ where $k \in \omega$ and $c_0, \ldots, c_{k-1} \in A$ and f is a $(k+3)$-ary $\mathcal{T}$-term. Thus, g is the restriction to z/β of a unary polynomial $l : A \to A$

defined by $l(x) = f^{\mathbf{A}}(x, z, z', c_0, \dots, c_{k-1})$ for all $x \in A$. By (ii) above, $g(z) = f^{\mathbf{A}}(z, z, z', c_0, \dots, c_{k-1}) = z'$.

($\Leftarrow$) Let h be a $(k+1)$-ary $\mathcal{T}$-term, where $k \in \omega$, and let $c_0, \dots, c_{k-1} \in A$ such that $h^{\mathbf{A}}(z, c_0, \dots, c_{k-1}) = z'$. Let $g : A \to A$ be defined by $g(x) = h^{\mathbf{A}}(x, \mathbf{c})$, where $\mathbf{c} = c_0, \dots, c_{k-1}$, for all $x \in A$. Then g is a unary polynomial of $\mathbf{A}$ which maps z to z'. Define a $\mathcal{T}$-term f by:

$$f(u, v, v', \mathbf{y}) = d(h(u, \mathbf{y}), h(v, \mathbf{y}), v') \text{ where } \mathbf{y} = y_0, \dots, y_{k-1}.$$

f is a $(k+3)$-ary $\mathcal{T}$-term and $V \models f(v, v, v', \mathbf{y}) \approx d(h(v, \mathbf{y}), h(v, \mathbf{y}), v') \approx v'$ by Theorem 3.10 (i). Now for all $x \in M(\beta, z)$,

$f^{\mathbf{A}}(x, z, z', \mathbf{c}) = d^{\mathbf{A}}(h^{\mathbf{A}}(x, \mathbf{c}), h^{\mathbf{A}}(z, \mathbf{c}), z')$

$= d^{\mathbf{A}}(h^{\mathbf{A}}(x, \mathbf{c}), z', z')$ by definition of h. .... (1)

If $x \in z/\beta$, then $h^{\mathbf{A}}(x, \mathbf{c}) \beta h^{\mathbf{A}}(z, \mathbf{c}) = z'$, i.e., $h^{\mathbf{A}}(x, \mathbf{c}) \in z'/\beta$. By Theorem 3.10(ii), $d^{\mathbf{A}}(h^{\mathbf{A}}(x, \mathbf{c}), z', z')[\beta, \beta]h^{\mathbf{A}}(x, \mathbf{c})$, i.e., $d^{\mathbf{A}}(h^{\mathbf{A}}(x, \mathbf{c}), z', z') = h^{\mathbf{A}}(x, \mathbf{c})$ (since β is Abelian).

We therefore have $g|_{(z/\beta)}(x) = h^{\mathbf{A}}(x, \mathbf{c}) = f^{\mathbf{A}}(x, z, z', c_0, \dots, c_{k-1})$ (by (1)) for all $x \in M(\beta, z)$, so $g|_{(z/\beta)} \in Hom(\beta, z, z')$. □

Corollary 3.19. *Let V be a modular $\mathcal{T}$-variety with difference term d, let $\mathbf{A} \in V$ and let β be an Abelian congruence of $\mathbf{A}$ such that $\mathbf{A}/\beta$ is finite, say $A/\beta = \{z_1/\beta, \dots, z_n/\beta\}$ where $n = |A/\beta| \in \omega$. For each $i, j \in \{1, \dots, n\}$ and each $g \in Hom(\beta, z_i, z_j)$, there exists an $(n+1)$-ary $\mathcal{T}$-term $t_g = t_g(x_0, x_1, \dots, x_n)$ such that for all $x \in z_i/\beta$,*

$$g(x) = t_g^{\mathbf{A}}(x, z_1, \dots, z_n).$$

In particular, if $\mathbf{A}$ is finite, say $|A| = m \in \omega$, then

$$|Hom(\beta, z_i, z_j)| \leq m^{(m^{n+1})} \leq m^{(m^{m+1})}.$$

Proof.

Let $i, j \in \{1, \dots, n\}$ and $g \in Hom(\beta, z_i, z_j)$. By Lemma 3.18, there exist $k \in \omega$ and a $(k+3)$-ary $\mathcal{T}$-term f and $\mathbf{c} = c_0, \dots, c_{k-1} \in A$ such that for any $x \in z_i/\beta$,

$$g(x) = f^{\mathbf{A}}(x, z_i, z_j, \mathbf{c}) \text{ and } V \models f(v, v, v', \mathbf{y}) \approx v'.$$

For each $r \in \{0, \dots, k-1\}$, let $c_r \in z_{\sigma(r)}/\beta$ (so $\sigma(r) \in \{1, \dots, n\}$) and let $\mathbf{z}_\sigma = z_{\sigma(0)}, \dots, z_{\sigma(k-1)}$. Let $x \in z_i/\beta$. Then by Corollary 3.14 and Theorem 3.10,

$g(x) = f^{\mathbf{A}}(x, z_i, z_j, \mathbf{c})$

$$= f^{\mathbf{A}}(d^{\mathbf{A}}(x, z_i, z_i), d^{\mathbf{A}}(z_i, z_i, z_i), d^{\mathbf{A}}(z_j, z_j, z_j), d^{\mathbf{A}}(z_{\sigma(0)}, z_{\sigma(0)}, c_0),$$
$$\dots, d^{\mathbf{A}}(z_{\sigma(k-1)}, z_{\sigma(k-1)}, c_{k-1}))$$
$$= d^{\mathbf{A}}(f^{\mathbf{A}}(x, z_i, z_j, \mathbf{z}_\sigma), f^{\mathbf{A}}(z_i, z_i, z_j, \mathbf{z}_\sigma), f^{\mathbf{A}}(z_i, z_i, z_j, \mathbf{c}))$$
$$= d^{\mathbf{A}}(f^{\mathbf{A}}(x, z_i, z_j, \mathbf{z}_\sigma), z_j, z_j)$$
$$= f^{\mathbf{A}}(x, z_i, z_j, \mathbf{z}_\sigma) \quad \text{(because } f^{\mathbf{A}}(x, z_i, z_j, \mathbf{z}_\sigma)\beta f^{\mathbf{A}}(z_i, z_i, z_j, \mathbf{z}_\sigma) = z_j)$$
$$= t_g^{\mathbf{A}}(x, z_1, \dots, z_n)$$

if we define $t_g(x_0, x_1, \dots, x_n) = f(x_0, x_i, x_j, x_{\sigma(0)}, \dots, x_{\sigma(k-1)})$.

Now suppose $|A| = m \in \omega$ so $n \le m$. Define $\varphi : Hom(\beta, z_i, z_j) \to F = F_{V(\mathbf{A})}(\bar{x}_0, \dots, \bar{x}_n)$ by $g \mapsto t_g^{\mathbf{F}}$.

If $g, h \in Hom(\beta, z_i, z_j)$ and $t_g^{\mathbf{F}} = t_h^{\mathbf{F}}$ then, by Theorem 0.50, $V(\mathbf{A})$ (hence $\mathbf{A}$) satisfies
$t_g(x_0, x_1, \dots, x_n) \approx t_h(x_0, x_1, \dots, x_n)$, so $g(x') = h(x')$ for all $x' \in z_i/\beta$, whence $g = h$. Thus, φ is one-to-one and so

$$\begin{aligned} |Hom(\beta, z_i, z_j)| &\le |F_{V(\mathbf{A})}(\bar{x}_0, \dots, \bar{x}_n)| \\ &\le |A|^{(|A|^{n+1})} \text{ (by Lemma 0.51)} \\ &= m^{(m^{n+1})} \le m^{(m^{m+1})}. \end{aligned}$$

□

In this chapter we have presented those results about Abelian congruences in modular varieties that will be needed in Chapter 4, particularly for the main result, Theorem 4.11. The connection between modular varieties and the modules over rings goes much deeper, however. In particular, for every Abelian modular *variety* V there is a *single* ring $\mathbf{R}$ with identity such that V is equivalent, in a strong sense, to a variety of unital $\mathbf{R}$-modules. (This strengthens the Fundamental Theorem of Abelian Algebras.) The interested reader should consult Chapter 9 of [FM87], as well as [DK87].

Chapter 4

Residual Size in Modular Varieties

We have seen how the commutator in modular varieties plays a role in, amongst other things, the description of Abelian algebras and Abelian congruences. In this chapter we shall see that it can also be used to describe residually small modular varieties. We consider the commutator identity $x \wedge [y, y] \approx [x \wedge y, y]$ where (x, y) is a pair of variables ranging over the congruence relations of any algebra in a variety V. This identity is referred to as (C1). In Theorems 4.1 and 4.2 some of its properties are described. We also include a result that illustrates the link between (C1) and Abelian congruences.

There are a number of other commutator identities that distinguish significant classes of varieties (see [FM87, Chapter 8]). (C1) is singled out in this chapter because of its link with residually small varieties: we infer from Theorem 4.10 that a residually small variety must satisfy (C1). This result is due to Freese and McKenzie [FM81].

The main result of this chapter (and this thesis) is found in Theorem 4.11 and is also due to Freese and McKenzie [FM81]. It provides a partial positive answer to the RS Conjecture which asks: if a finite algebra generates a residually small variety, must that variety have a finite residual bound? Theorem 4.11 proves that the conjecture is true for the case of finite algebras in a *modular* variety. McKenzie in [McK96a] has shown the RS Conjecture to be false in general, however.

4.1 A Congruence Identity. Consider the "congruence identity"[23]

(C1) $\quad x \wedge [y, y] \approx [x \wedge y, y]$

in the language of lattices augmented by the binary operation symbol $[,]$. We say that an algebra $\mathbf{A}$ *satisfies* (C1) if $\langle Con(\mathbf{A}); \cap, \vee, [,] \rangle \models (C1)$. We say $\mathbf{A}$ *satisfies* (C1) *hereditarily* if $\langle Con(\mathbf{B}); \cap, \vee, [,] \rangle \models (C1)$ for all subalgebras

[23] We follow the literature in calling (C1) an "identity"; strictly speaking it is an equation.

B of **A**. For the sake of notational brevity we denote $\langle Con(\mathbf{A}); \cap, \vee, [,]\rangle$ by **Con**(**A**).

Theorem 4.1. [FM81]

Let V be a variety and $\mathbf{A} \in V$. *In* **Con**(**A**), *the identity (C1) is equivalent to the quasi-identity* $x \leq [y,y] \rightarrow x \approx [x,y]$.

Proof.

Suppose $\mathbf{Con}(\mathbf{A}) \models x \leq [y,y] \rightarrow x \approx [x,y]$ (where $\subseteq$ interprets $\leq$). Clearly $\mathbf{Con}(\mathbf{A}) \models x \wedge [y,y] \leq [y,y]$, so by the quasi-identity,

$\mathbf{Con}(\mathbf{A}) \models x \wedge [y,y] \approx [x \wedge [y,y], y]$

$\leq [x \wedge y, y]$ (by order-preservation since $\mathbf{Con}(\mathbf{A}) \models [y,y] \leq y \wedge y \approx y$)

$\leq x \wedge [y,y]$ (since $\mathbf{Con}(\mathbf{A}) \models [x \wedge y, y] \leq x \wedge y \leq x$ and $[x \wedge y, y] \leq [y,y]$).

Thus, $\mathbf{Con}(\mathbf{A}) \models x \wedge [y,y] \approx [x \wedge y, y]$, i.e., **A** satisfies (C1).

Conversely, suppose **A** satisfies (C1). Then, over **Con**(**A**),

$x \leq [y,y] \rightarrow x \approx x \wedge [y,y] \approx [x \wedge y, y]$ (by (C1))

$\leq [x,y]$.

Also $\mathbf{Con}(\mathbf{A}) \models [x,y] \leq x$ (by Proposition 2.9 (i)). Thus, $\mathbf{Con}(\mathbf{A}) \models$ $x \leq [y,y] \rightarrow x \approx [x,y]$. □

Theorem 4.2. [FM81]

Let V be a modular variety of type $\mathcal{T} = \langle \mathsf{F}, ar\rangle$. Then the class of algebras in V which satisfy (C1) hereditarily is closed under the formation of quotient algebras, subalgebras and finite direct products.

Proof.

Let $\mathbf{A} \in V$ and suppose that **A** satisfies (C1) hereditarily.

If **B** is any subalgebra of **A** and **C** any subalgebra of **B** then since **C** is a subalgebra of **A**, (C1) will be satisfied by **Con**(**C**). Thus, **B** satisfies (C1) hereditarily.

Let $\mathbf{C} \leq \mathbf{A}/\theta$ for some $\theta \in Con(\mathbf{A})$. Then $C = B/\gamma$ where $B = \{x \in A : x/\theta \in C\}$ and $\gamma = \theta \cap (B \times B)$. Let $x_1, \ldots, x_n \in B$. Then $x_1/\theta, \ldots, x_n/\theta \in C$, so $f^{\mathbf{C}}(x_1/\theta, \ldots, x_n/\theta) \in C$, whenever $f \in \mathsf{F}$ with $ar(f) = n$, that is $f^{\mathbf{A}}(x_1, \ldots, x_n)/\theta \in C$, so $f^{\mathbf{A}}(x_1, \ldots, x_n) \in B$, so B is a subuniverse of **A** and the algebra **B** satisfies (C1).

Suppose (C1) fails for $\mathbf{C} = \mathbf{B}/\gamma$. Let f be the isomorphism from $\mathbf{int}(\gamma, B^2)$ to $\mathbf{Con}(\mathbf{B}/\gamma)$ defined by $f(\theta) = \theta/\gamma$. There exist $\mu, \nu \in int(\gamma, B^2)$ such that

$f(\nu) \subseteq [f(\mu), f(\mu)]$ (in $\mathbf{Con(B/\gamma)}$) and $f(\nu) \neq [f(\nu), f(\mu)]$ by the previous theorem, and the Correspondence Theorem.

Now $\nu \subseteq f^{-1}([f(\mu), f(\mu)])$ and $\nu \neq f^{-1}([f(\nu), f(\mu)])$ so by Remark 2.15,
$\nu \subseteq [\mu, \mu] \vee \gamma = [\mu, \mu]_\gamma$ in $\mathbf{Con(B)}$ and $\nu \neq [\nu, \mu]_\gamma$. .... (1)

Now $\nu \subseteq [\mu, \mu]_\gamma \subseteq (\mu \cap \mu) \vee \gamma = \mu \vee \gamma = \mu$. Also $[\nu, \mu]_\gamma \subseteq (\nu \cap \mu) \vee \gamma = \nu \cap \mu = \nu$ (since $\gamma \subseteq \mu \cap \nu$ and $\nu \subseteq \mu$). But by (1) we must have
$[\nu, \mu]_\gamma \subset \nu$. .... (2)

Suppose $[\nu, \mu] \supseteq [\mu, \mu] \cap \nu$. Then we would have $[\nu, \mu] \vee \gamma \supseteq ([\mu, \mu] \cap \nu) \vee \gamma = (\gamma \vee [\mu, \mu]) \cap \nu$ (by modularity, since $\gamma \subseteq \nu$)
$= [\mu, \mu]_\gamma \cap \nu = \nu$ since $\nu \subseteq [\mu, \mu]_\gamma$. However, $[\nu, \mu]_\gamma \supseteq \nu$ contradicts (2), so we must have $[\nu, \mu] \not\supseteq [\mu, \mu] \cap \nu$.

Since $\nu \subseteq \mu$, $[\mu \cap \nu, \mu] = [\nu, \mu] \not\supseteq [\mu, \mu] \cap \nu$, i.e., (C1) fails in $\mathbf{Con(B)}$, a contradiction. Thus, $\mathbf{C}$ satisfies (C1).

Finally, consider an algebra $\mathbf{C} = \mathbf{A} \times \mathbf{B}$ where $\mathbf{A}$ and $\mathbf{B}$ satisfy (C1) hereditarily and suppose $\mathbf{D}$ is a subalgebra of $\mathbf{C}$. Let p_0 and p_1 be the projection homomorphisms from $\mathbf{D}$ to $\mathbf{A}$ and $\mathbf{B}$ respectively, and let η_0 and η_1 be their respective kernels. Now $p_0[\mathbf{D}] \leq \mathbf{A}$ and $p_1[\mathbf{D}] \leq \mathbf{B}$ so $p_0[\mathbf{D}]$ and $p_1[\mathbf{D}]$ satisfy (C1) hereditarily, because $\mathbf{A}$ and $\mathbf{B}$ do, so the roles of $\mathbf{A}$ and $\mathbf{B}$ in the proof can be taken by $p_0[\mathbf{D}]$ and $p_1[\mathbf{D}]$ respectively, i.e., we may assume without loss of generality that p_0 and p_1 are onto.

Suppose $\delta, \mu \in Con(\mathbf{D})$. Let $\nu = \delta \cap [\mu, \mu]$. Since $\nu \subseteq [\mu, \mu]$, we have $\nu \vee \eta_0 \subseteq [\mu \vee \eta_0, \mu \vee \eta_0] \vee \eta_0$ (in $\mathbf{Con(D)}$). Recall that $p_0(\nu \vee \eta_0) \in Con(\mathbf{A})$ because $\nu \vee \eta_0 \supseteq \eta_0 = ker(p_0)$, so in $\mathbf{Con(A)}$,

$p_0(\nu \vee \eta_0) \subseteq p_0([\mu \vee \eta_0, \mu \vee \eta_0] \vee \eta_0)$
$= p_0(p_0^{-1}[p_0(\mu \vee \eta_0), p_0(\mu \vee \eta_0)])$ (by Proposition 2.14 (i))
$\subseteq [p_0(\mu \vee \eta_0), p_0(\mu \vee \eta_0)]$ (in $\mathbf{Con(A)}$).

$\mathbf{A}$ satisfies (C1) hereditarily so by the equivalent quasi-identity, $p_0(\nu \vee \eta_0) = [p_0(\nu \vee \eta_0), p_0(\mu \vee \eta_0)]$. Now $\nu \vee \eta_0 \subseteq p_0^{-1}[p_0(\nu \vee \eta_0), p_0(\mu \vee \eta_0)] = [\nu \vee \eta_0, \mu \vee \eta_0] \vee \eta_0$ by Proposition 2.14 (i).

Conversely, $[\nu \vee \eta_0, \mu \vee \eta_0] \vee \eta_0 \subseteq \nu \vee \eta_0 \vee \eta_0 = \nu \vee \eta_0$ so
$\nu \vee \eta_0 = [\nu \vee \eta_0, \mu \vee \eta_0] \vee \eta_0$ .... (3)
$= [\nu, \mu] \vee [\eta_0, \mu] \vee [\nu, \eta_0] \vee [\eta_0, \eta_0] \vee \eta_0$ (by Proposition 2.9 (i))
$= [\nu, \mu] \vee \eta_0$.
We therefore have $\nu \vee \eta_0 = [\nu, \mu] \vee \eta_0$. .... (4)

Thus $\nu = \nu \cap (\nu \vee \eta_0) = \nu \cap ([\nu, \mu] \vee \eta_0)$ (by (4)) and $[\nu, \mu] \subseteq \nu$ so by the Modular Law, $\nu = [\nu, \mu] \vee (\nu \cap \eta_0)$. Similarly, $\nu = [\nu, \mu] \vee (\nu \cap \eta_1)$. ....(5)

Now the only special property of ν that was used above is $\nu \subseteq [\mu, \mu]$. Since $\eta_1 \cap \nu \subseteq [\mu, \mu]$, exactly the same argument will work if we replace ν throughout by $\eta_1 \cap \nu$. We then get in place of (3) above,

$$(\eta_1 \cap \nu) \vee \eta_0 = [(\eta_1 \cap \nu) \vee \eta_0, \mu \vee \eta_0] \vee \eta_0$$

and in place of (4) above we get

$$(\eta_1 \cap \nu) \vee \eta_0 = [\eta_1 \cap \nu, \mu] \vee \eta_0,$$

the left hand side of which contains $\eta_1 \cap \nu$, so $\eta_1 \cap \nu \subseteq [\eta_1 \cap \nu, \mu] \vee \eta_0$.

We therefore have $\eta_1 \cap \nu = \eta_1 \cap \nu \cap ([\eta_1 \cap \nu, \mu] \vee \eta_0)$
$= [\eta_1 \cap \nu, \mu] \vee (\eta_1 \cap \nu \cap \eta_0)$ (by the Modular Law because $\eta_1 \cap \nu \supseteq [\eta_1 \cap \nu, \mu]$)
$= [\eta_1 \cap \nu, \mu] \vee id_D = [\eta_1 \cap \nu, \mu]$, so we have $\eta_1 \cap \nu = [\eta_1 \cap \nu, \mu]$. .... (6)
Now $\nu = [\nu, \mu] \vee (\nu \cap \eta_1)$ (by (5))
$= [\nu, \mu] \vee [\nu \cap \eta_1, \mu]$ (by (6))
$= [\nu, \mu]$ because $\nu \cap \eta_1 \subseteq \nu$. Therefore $\nu = [\nu, \mu]$. □

Corollary 4.3. [FM87, Exercise 8.5]

Let V be a modular variety and $\mathbf{A} \in V$, let α, β be Abelian congruences of $\mathbf{A}$ and suppose $\mathbf{A}$ satisfies (C1). Then $\alpha \vee \beta$ is Abelian. Moreover, $\mathbf{A}$ has a largest Abelian congruence.

Proof.

We need to show $[\alpha \vee \beta, \alpha \vee \beta] = id_A$, i.e. (by Proposition 2.12) we must show $[\alpha, \alpha] \vee [\alpha, \beta] \vee [\beta, \beta] \vee [\beta, \alpha] = id_A$.

Now $[\alpha, \beta] = [\beta, \alpha]$ and, since α and β are Abelian, $[\alpha, \alpha] = [\beta, \beta] = id_A$. Hence we need only show $[\alpha, \beta] = id_A$. Now $[\alpha, \beta] \subseteq [\alpha \vee \beta, \alpha \vee \beta]$ by order-preservation.

Since $\mathbf{Con(A)} \models (C1)$, by Theorem 4.1, we have $[\alpha, \beta] = [[\alpha, \beta], \alpha \vee \beta] = [[\alpha, \beta], \alpha] \vee [[\alpha, \beta], \beta] \subseteq [\alpha, \alpha] \vee [\beta, \beta] = id_A$, so $\alpha \vee \beta$ is Abelian.

Now let $X = \{\rho \in Con(\mathbf{A}) : \rho \text{ is an Abelian congruence}\} = \{\rho_i : i \in I\}$, say. By the above argument, $[\rho_i, \rho_j] = id_A$ for all $i, j \in I$. Let $\gamma = \bigvee_{i \in I} \rho_i$. We show $\bigvee_{i \in I} \rho_i$ is Abelian, i.e., that $[\gamma, \gamma] = id_A$. Now by Proposition 2.12, $[\gamma, \gamma] = [\bigvee_{i \in I} \rho_i, \bigvee_{j \in I} \rho_j] = \bigvee_{i \in I} \bigvee_{j \in I} [\rho_i, \rho_j] = id_A$, so γ is the largest Abelian congruence of $\mathbf{A}$. □

4.2 Subdirectly Irreducible Algebras in Modular Varieties. Let K be a class of algebras of the same type. Recall that K_{SI} denotes the class of all subdirectly irreducible algebras in K and that I, H, S, P, P_S, P_U denote closures under isomorphic and homomorphic images, subalgebras, direct and subdirect products, and ultraproducts, respectively. By theorems of Birkhoff and Tarski (Theorems 0.23, 0.25, 0.26 and 0.40),

$$V(K) = HSP(K) = IP_S(V(K)_{SI})$$

(where as usual, $V(K)$ is the smallest variety containing K).

Recall that when $V(K)$ is congruence distributive, Jónsson's Theorem (Theorem 0.34) improves the above description of $V(K)$: it says that $V(K)_{SI} \subseteq HSP_U(K)$,[24] whence

$$V(K) = IP_SHSP_U(K).$$

Since every congruence distributive variety is congruence modular, one might ask whether Jónsson's Theorem remains true under the weaker assumption that $V(K)$ is modular. Example 4.12 shows that this is not the case. Nevertheless, Theorem 4.6 below will provide a description of $V(K)_{SI}$ (hence of $V(K)$) when $V(K)$ is modular and the specialization of this result to distributive varieties $V(K)$ turns out to be just Jónsson's Theorem. Theorem 4.6 is jointly due to Hagemann, Herrmann, Freese, McKenzie and U. Hrushovskii ([HH79], [Her79], [FM81], [FM87]). Our approach largely follows [FM87], which attributes the next lemma to J.B. Nation. (No assumption about modularity is made in this lemma.)

Lemma 4.4. *Let* $\mathbf{B}$ *be a subdirectly irreducible* $\mathcal{T}$*-algebra. Then* $\mathbf{B}$ *is isomorphic to a subalgebra of an ultraproduct of a family* $\mathbf{B}_i, i \in I$, *of finitely generated, subdirectly irreducible algebras from* $HS(\mathbf{B})$.

Moreover, if μ_i *is the monolith of each* $\mathbf{B}_i$ *then there is an ultrafilter* $\mathcal{U}$ *over* I *and an embedding* $h : \mathbf{B} \to \mathbf{B}' = \prod_{i \in I} \mathbf{B}_i/\theta_{\mathcal{U}}$ *such that* $\mu|_{h[\mathbf{B}]} \neq id_{h[B]}$, *where* $\mu := (\theta_{\mathcal{U}} \vee \prod_{i \in I} \mu_i)/\theta_{\mathcal{U}} \in Con(\mathbf{B}')$.

Proof.

We can assume $\mathbf{B}$ is infinite, otherwise, setting each $\mathbf{B}_i = \mathbf{B}$, the result is trivial (see Lemma 0.33). Let $\Theta^{\mathbf{B}}(a, b)$ be the monolith of $\mathbf{B}$ where $a, b \in B$ and $a \neq b$.

Let φ be the set of all finite subsets of B which contain a and b. For each $S \in \varphi$, let $\psi_S \in Con(\mathbf{Sg}^{\mathbf{B}}(S))$ be maximal among congruences of $\mathbf{Sg}^{\mathbf{B}}(S)$ that do not contain (a, b).

[24] At first glance, ultraproducts appear to complicate the description but, by Loś' Theorem, they are "nicer" than they look. Recall also that when K is a finite set of finite algebras then $P_U(K) \subseteq I(K)$ (Lemma 0.33).

We show that if $S \in \varphi$ then such a ψ_S exists. Let $A = \{\gamma \in Con(\mathbf{Sg}^{\mathbf{B}}(S)) : (a,b) \notin \gamma\}$. A is not empty (since $id_{Sg^{\mathbf{B}}(S)} \in A$) and A is partially ordered by $\subseteq$.

Let $\langle C; \subseteq \rangle$ be a chain in A. We show that C has a $\subseteq$-upper bound in A. We can assume C is nonempty otherwise any element of A is an upper bound of $\emptyset$ in A. $\cup C \in Con(\mathbf{Sg}^{\mathbf{B}}(S))$ because $\mathbf{Con}(\mathbf{Sg}^{\mathbf{B}}(S))$ is an algebraic lattice. Suppose $(a,b) \in \cup C$. Then there exists some $\gamma \in C$ such that $(a,b) \in \gamma$, a contradiction. Thus $(a,b) \notin \cup C$, therefore $\cup C \in A$ and $\cup C$ is an upper bound in A for C.

By Zorn's Lemma, A has a maximal element ψ_S, i.e., ψ_S is maximal among congruences η of $Sg^{\mathbf{B}}(S)$ such that $(a,b) \notin \eta$.

For each $S \in \varphi$, $\mathbf{G} := \mathbf{Sg}^{\mathbf{B}}(S)/\psi_S$ is subdirectly irreducible, since $\Theta^{\mathbf{G}}(a/\psi_S, b/\psi_S)$ is clearly its monolith. Let $\mathcal{F}$ be the set of all subsets T of φ such that there is an $S_0 \in \varphi$ with $\{S \in \varphi : S \supseteq S_0\} \subseteq T$. We show that $\mathcal{F}$ is a filter over φ, i.e., a filter of the Boolean algebra whose universe is $\mathcal{P}(\varphi)$ (the set of all subsets of φ).

Now $\varphi \in \mathcal{F}$, because $\varphi \supseteq \{S \in \varphi : \{a,b\} \subseteq S\}$.

Let $T_1, T_2 \in \mathcal{F}$. Then there exist $S_1, S_2 \in \varphi$ such that $\{S \in \varphi : S \supseteq S_1\} \subseteq T_1$ and $\{S \in \varphi : S \supseteq S_2\} \subseteq T_2$ so $\{S \in \varphi : S \supseteq S_1 \cup S_2\} \subseteq T_1 \cap T_2$ and $S_1 \cup S_2 \in \varphi$ because $(a,b) \in S_1 \cup S_2$ and $S_1 \cup S_2$ is finite. Therefore $T_1 \cap T_2 \in \mathcal{F}$.

Let $T_1 \subseteq T' \subseteq \varphi$. Then $\{S \in \varphi : S \supseteq S_1\} \subseteq T_1 \subseteq T'$ so $T' \in \mathcal{F}$. Thus, $\mathcal{F}$ is a filter over φ.

For all $S_0 \in \varphi, \{S \in \varphi : S \supseteq S_0\} \nsubseteq \emptyset$ so $\emptyset \notin \mathcal{F}$, therefore $\mathcal{F}$ is a proper filter. There exists an ultrafilter $\mathcal{U}$ over φ with $\mathcal{F} \subseteq \mathcal{U}$ (by Theorem 0.31). Let $\varphi = \{S_i : i \in I\}$. For each i, let $\mathbf{B}_i = \mathbf{Sg}^{\mathbf{B}}(S_i)/\psi_{S_i}$, and let u_i be an arbitrary element of S_i.

Let $g' : \mathbf{B} \to \prod_{i \in I} \mathbf{Sg}^{\mathbf{B}}(S_i)$ be defined by :

$$(g'(x))(i) = x \text{ if } x \in Sg^{\mathbf{B}}(S_i);\ (g'(x))(i) = u_i \text{ otherwise.}$$

Let $\mathbf{D}$ be $\prod_{i \in I} \mathbf{B}_i = \prod_{i \in I}(\mathbf{Sg}^{\mathbf{B}}(S_i)/\psi_{S_i})$. Let $g : \mathbf{B} \to \mathbf{D}$ be given by $(g(x))(i) = (g'(x))(i)/\psi_{S_i}$. Let $\mathbf{D}/\theta_{\mathcal{U}}$ (denoted $\mathbf{D}/\mathcal{U}$) be the ultraproduct of the $\mathbf{Sg}^{\mathbf{B}}(S_i)/\psi_{S_i}$ corresponding to $\mathcal{U}$ so $\theta_{\mathcal{U}}$ is defined as follows:
For any $x, y \in \prod_{i \in I}(Sg^{\mathbf{B}}(S_i)/\psi_{S_i})$, $(x,y) \in \theta_{\mathcal{U}}$ if and only if $[[x = y]] := \{S_i : i \in I \text{ and } x(i) = y(i)\} \in \mathcal{U}$. (Note that $\theta_{\mathcal{U}} \in Con(\prod_{i \in I}(\mathbf{Sg}^{\mathbf{B}}(S_i)/\psi_{S_i}))$.)

Consider the natural homomorphism $\lambda : \mathbf{D} \to \mathbf{D}/\mathcal{U}$. Let $\hat{g} = \lambda \circ g$. Then $\hat{g} : \mathbf{B} \to \mathbf{D}/\mathcal{U}$ is defined by $\hat{g}(x) = g(x)/\mathcal{U}$ for all $x \in B$.

We show $\hat{g}$ is a homomorphism, i.e., for any n-ary operation symbol f of $\mathcal{T}$ and any $x_1, \dots, x_n \in B$, we show $\hat{g}(f^{\mathbf{B}}(x_1, \dots, x_n)) = f^{\mathbf{D}/\mathcal{U}}(\hat{g}(x_1), \dots, \hat{g}(x_n))$.

$f^{\mathbf{D}/\mathcal{U}}(\hat{g}(x_1),\ldots,\hat{g}(x_n)) = f^{\mathbf{D}/\mathcal{U}}(g(x_1)/\mathcal{U},\ldots,g(x_n)/\mathcal{U})$
$= (f^{\mathbf{D}}(g(x_1),\ldots,g(x_n)))/\theta_{\mathcal{U}}$ and $\hat{g}(f^{\mathbf{B}}(x_1,\ldots,x_n)) = (g(f^{\mathbf{B}}(x_1,\ldots,x_n)))/\theta_{\mathcal{U}}$.

Now $(f^{\mathbf{D}}(g(x_1),\ldots,g(x_n)))/\theta_{\mathcal{U}} = (g(f^{\mathbf{B}}(x_1,\ldots,x_n)))/\theta_{\mathcal{U}}$
if and only if $(f^{\mathbf{D}}(g(x_1),\ldots,g(x_n)), g(f^{\mathbf{B}}(x_1,\ldots,x_n))) \in \theta_{\mathcal{U}}$
if and only if $Y := [[f^{\mathbf{D}}(g(x_1),\ldots,g(x_n)) = g(f^{\mathbf{B}}(x_1,\ldots,x_n))]] \in \mathcal{U}$. Note that $Y = \{S_i : i \in I$ and $(f^{\mathbf{D}}(g(x_1),\ldots,g(x_n)))(i) = (g(f^{\mathbf{B}}(x_1,\ldots,x_n)))(i)\}$.

Let $T = \{S \in \varphi : S \supseteq \{x_1,\ldots,x_n\}\}$. Then $T \in \mathcal{F}$, so $T \in \mathcal{U}$. Let $T = \{S_j : j \in J\}$, where $J \subseteq I$. Then for all $j \in J$,
$(f^{\mathbf{D}}(g(x_1),\ldots,g(x_n)))(j) = f^{\mathbf{B}_j}(x_1/\psi_{S_j},\ldots,x_n/\psi_{S_j})$
$= f^{\mathbf{B}}(x_1,\ldots,x_n)/\psi_{S_j} = (g(f^{\mathbf{B}}(x_1,\ldots,x_n)))(j)$, since for each $j \in J, \{x_1,\ldots,x_n\} \in S_j$, hence $f^{\mathbf{B}}(x_1,\ldots,x_n) \in Sg^{\mathbf{B}}(S_j)$. Thus, $Y \supseteq T \in \mathcal{U}$ and so $Y \in \mathcal{U}$ because $\mathcal{U}$ is closed under supersets.

We show $\hat{g}$ is one-to-one. Let $c, d \in B$ with $c \neq d$. We must show that $\hat{g}(c) \neq \hat{g}(d)$, i.e., that $g(c)/\mathcal{U} \neq g(d)/\mathcal{U}$, i.e., that $Z := \{S_i : i \in I$ and $(g(c))(i)/\psi_{S_i} = (g(d))(i)/\psi_{S_i}\} \notin \mathcal{U}$. ....(1)
Note that $Z = \{S_i : i \in I$ and $((g(c))(i), (g(d))(i)) \in \psi_{S_i}\}$.

Now as $c \neq d$, $\Theta^{\mathbf{B}}(c,d) \neq id_B$ so $\Theta^{\mathbf{B}}(a,b) \subseteq \Theta^{\mathbf{B}}(c,d)$ because $\Theta^{\mathbf{B}}(a,b)$ is the monolith of $\mathbf{B}$. Therefore $(a,b) \in \Theta^{\mathbf{B}}(c,d)$. By Mal'cev's Lemma (Theorem 0.37), there are terms $p_i(x_0,x_1,y_1,\ldots,y_k)$ $(1 \leq i \leq m \in \omega)$ and elements $e_1,\ldots,e_k \in B$ such that

$$\begin{aligned} a &= p_1^{\mathbf{B}}(c,d,\mathbf{e}) \text{ (where } \mathbf{e} = e_1,\ldots,e_k) \\ p_1^{\mathbf{B}}(d,c,\mathbf{e}) &= p_2^{\mathbf{B}}(c,d,\mathbf{e}) \\ &\vdots \\ p_m^{\mathbf{B}}(d,c,\mathbf{e}) &= b. \end{aligned}$$

Let $S_0 = \{a,b,c,d,\mathbf{e}\}$, so $S_0 \in \varphi$. Let $U = \{S \in \varphi : S \supseteq S_0\} = \{S \in \varphi : a,b,c,d,\mathbf{e} \in S\}$. Then $U \in \mathcal{F} \subseteq \mathcal{U}$ so $U \in \mathcal{U}$.

Let $\mathbf{E} = \mathbf{Sg}^{\mathbf{B}}(S)$. Let $S \in U$. Since $c,d,\mathbf{e} \in S$, for $1 \leq i \leq m$, $p_i^{\mathbf{B}}(d,c,\mathbf{e}), p_i^{\mathbf{B}}(c,d,\mathbf{e}) \in Sg^{\mathbf{B}}(S) = E$. Thus we have $a,b,c,d,e_1,\ldots,e_k \in S$ and

$$\begin{aligned} a &= p_1^{\mathbf{E}}(c,d,\mathbf{e}) \\ p_1^{\mathbf{E}}(d,c,\mathbf{e}) &= p_2^{\mathbf{E}}(c,d,\mathbf{e}) \\ &\vdots \\ p_m^{\mathbf{E}}(d,c,\mathbf{e}) &= b. \end{aligned}$$

By Mal'cev's Lemma, $(a,b) \in \Theta^{\mathbf{E}}(c,d)$.

Now suppose $(c,d) \in \psi_S$. Then $\Theta^{\mathbf{E}}(c,d) \subseteq \psi_S$, so $(a,b) \in \psi_S$, but this contradicts the definition of ψ_S. Thus, for any $S \in U, (c,d) \notin \psi_S$.

Let $S = S_i \in U$, where $i \in I$. Then $c, d \in S$, so by definition of g, $(g(c))(i)/\psi_S = c/\psi_S \neq d/\psi_S = (g(d))(i)/\psi_S$. Let $W = \{S_i : i \in I$ and $((g(c))(i),(g(d))(i)) \notin \psi_{S_i}\}$. Then $W \supseteq U$ so $W \in \mathcal{U}$. Consider $W^c = \{S \in \varphi : S \notin W\}$. $W^c \notin \mathcal{U}$, otherwise $\emptyset = W \cap W^c \in \mathcal{U}$, contradicting the propriety of $\mathcal{U}$. But $W^c = Z$ so (1) is proved.

Therefore $\hat{g}$ is an embedding and so $\mathbf{B}$ is isomorphic to a subalgebra of $(\prod_{i\in I} \mathbf{B}_i)/\mathcal{U}$, so $\mathbf{B} \in ISP_U(K)$ where $K = \{\mathbf{B}_i : i \in I\}$ and each $\mathbf{B}_i = \mathbf{Sg}^{\mathbf{B}}(S_i)/\psi_{S_i} \in HS(\mathbf{B})$.

For each i, let μ_i be the monolith of $\mathbf{B}_i$, i.e., of $\mathbf{Sg}^{\mathbf{B}}(S_i)/\psi_{S_i}$. Then $\mu_i = \Theta_i^{\mathbf{B}}(a/\psi_{S_i}, b/\psi_{S_i})$, by maximality of ψ_{S_i}. Let μ be the ultraproduct congruence determined by the μ_i, i.e., $\mu = (\theta_{\mathcal{U}} \vee \prod_{i\in I}\mu_i)/\theta_{\mathcal{U}} \in Con(\prod_{i\in I}\mathbf{B}_i/\mathcal{U})$. Now $((a/\psi_{S_i})_{i\in I}, (b/\psi_{S_i})_{i\in I}) \in \prod_{i\in I}\mu_i$.

For U as above, $[[g(a) = (a/\psi_{S_i})_{i\in I}]], [[g(b) = (b/\psi_{S_i})_{i\in I}]] \supseteq U \in \mathcal{U}$, so $(\hat{g}(a), \hat{g}(b)) = ((a/\psi_{S_i})_{i\in I}/\mathcal{U}, (b/\psi_{S_i})_{i\in I}/\mathcal{U}) \in \mu$ and $\hat{g}(a) \neq \hat{g}(b)$ (since $\hat{g}$ is an embedding and $a \neq b$), so $\mu|_{\hat{g}[\mathbf{B}]} \neq id_{\hat{g}[B]}$. □

Let V be a modular variety and $\mathbf{A} \in V$ and $\beta, \delta \in Con(\mathbf{A})$. Let $S = \{\gamma \in Con(\mathbf{A}) : [\gamma,\beta] \subseteq \delta\}$. Then $S \neq \emptyset$; indeed $int(id_A, \delta) \subseteq S$. Let $\alpha = \bigvee S$. By Proposition 2.12, $[\alpha,\beta] = \bigvee_{\gamma\in S}[\gamma,\beta] \subseteq \delta$, so $\alpha \in S$. Thus, α is the largest element of S. This justifies the following definition.

Definition 4.5. Let V be a modular variety and $\mathbf{A} \in V$ and $\beta, \delta \in Con(\mathbf{A})$. Then $(\delta : \beta)$ shall denote the largest $\alpha \in Con(\mathbf{A})$ such that $[\alpha,\beta] \subseteq \delta$. We call $(id_A : \beta)$ the *centralizer of* β. Thus $(id_A : \beta)$ is the largest $\alpha \in Con(\mathbf{A})$ such that $[\alpha,\beta] = id_A$.

For example, if V is modular and $\mathbf{A} \in V$ then the *centre* $\tau_{\mathbf{A}}$ of $\mathbf{A}$ is the centralizer $(id_A : A^2)$ of A^2 in $\mathbf{A}$, by Lemma 3.2, and a congruence β of $\mathbf{A}$ is Abelian if and only if $\beta \subseteq (id_B : \beta)$.

Theorem 4.6. [FM87, Theorem 10.1]

Suppose K is a class of algebras of the same type such that $V(K)$ is modular. Let $\mathbf{B} \in V(K)$ be subdirectly irreducible and let α be the centralizer of the monolith μ of $\mathbf{B}$. Then $\mathbf{B}/\alpha \in HSP_U(K)$. Moreover, if $V(K)$ is locally finite, then $\mathbf{B}/\gamma \in ISP_UHS(K)$ for some $\gamma \subseteq \alpha$.

Proof.

Since $V(K) = HSP(K)$ (Theorem0.25), $\mathbf{B}$ is a homomorphic image of a subalgebra of a direct product of elements of K, so by the Homomorphism

Theorem, we can assume $\mathbf{B} = \mathbf{C}/\theta$ for some $\mathbf{C} \leq \prod_{i\in I} \mathbf{A}_i$, where $\mathbf{A}_i \in K$ for all $i \in I$, and some $\theta \in Con(\mathbf{C})$.

For any $J \subseteq I$, let $\lambda_J : \mathbf{C} \to \prod_{i\in J} \mathbf{A}_i$ be the homomorphism defined by $(\lambda_J(a))(j) = a(j)$ for all $a \in C$ and $j \in J$. Let $\eta_J = ker(\lambda_J)$. Then for any $J, E \subseteq I$, $\eta_J \cap \eta_E = \eta_{J\cup E}$. Thus, if $J \subseteq E \subseteq I$ then $\eta_J \supseteq \eta_E$.

Let f be the natural homomorphism from $\mathbf{C}$ onto $\mathbf{C}/\theta = \mathbf{B}$, so $ker(f) = \theta$. By the Correspondence Theorem there is a lattice isomorphism $g : \mathbf{Con(B)} \to \mathbf{int}(\theta, C^2) := \{\eta : \theta \subseteq \eta \in Con(\mathbf{C})\}$ defined by $\gamma \mapsto f^{-1}(\gamma) := \{(c_1, c_2) \in C^2 : (f(c_1), f(c_2)) \in \gamma\}$. Since $\mathbf{B}$ is subdirectly irreducible, θ in $\mathbf{Con(C)}$ (which corresponds to id_B in $\mathbf{Con(B)}$), is uniquely covered in $\mathbf{Con(C)}$ by a congruence ψ (which corresponds to the monolith μ of $\mathbf{B}$), so $g(\mu) = \psi$, i.e., $\mu = \psi/\theta$.

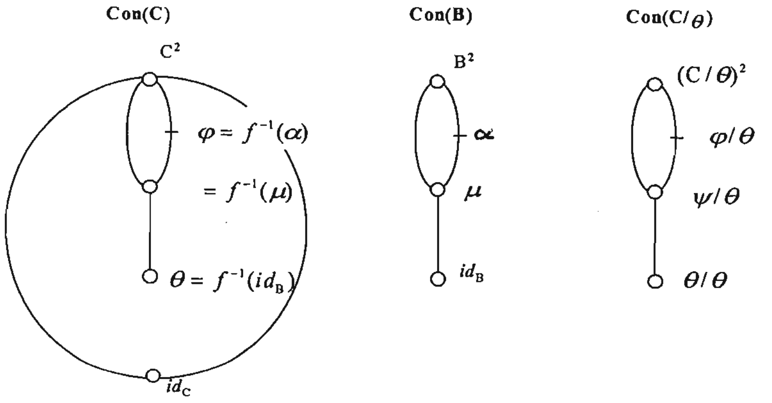
Let $\varphi = (\theta : \psi)$ and let $\alpha = (id_B : \mu)$.

Note that for all $\rho \in Con(\mathbf{B})$, $[\mu, \rho] \subseteq id_B$ if and only if $\rho \subseteq \alpha$. .... (1)

Note too that for all $\gamma \in int(\theta, C^2)$, $[\gamma, \psi] \subseteq \theta$ if and only if $\gamma \subseteq \varphi$. ...... (2)

We claim $g(\alpha) = \varphi$.

For any $\gamma \in int(\theta, C^2)$, we have $\gamma/\theta \in Con(\mathbf{B})$ and $[\gamma, \psi] = f^{-1}([\gamma/\theta, \mu])$, by Proposition 2.14 (i), so $[\gamma, \psi] \subseteq \theta$ if and only if $[\gamma/\theta, \mu] \subseteq f(\theta) = id_B$; if and only if $\gamma/\theta \subseteq \alpha$ (by (1)); if and only if $\gamma \subseteq f^{-1}(\alpha) = g(\alpha)$. By (2), therefore, $g(\alpha) = \varphi$, as claimed. It follows that $\theta \subseteq \varphi$ and $\alpha = \varphi/\theta$.



By the Second Isomorphism theorem, $\mathbf{B}/\alpha = (\mathbf{C}/\theta)/(\varphi/\theta) \cong \mathbf{C}/\varphi$. Let $\beta, \gamma \in Con(\mathbf{C})$. We show that if $\beta \cap \gamma \subseteq \theta$ then either $\beta \subseteq \theta$ or $\gamma \subseteq \theta$ or both $\beta \subseteq \varphi$ and $\gamma \subseteq \varphi$. .... (3)

Suppose $\beta \cap \gamma \subseteq \theta$ and $\beta \not\subseteq \theta$ and $\gamma \not\subseteq \theta$. Now $\theta \subseteq \beta \vee \theta$ but ψ is the unique cover of θ so $\beta \vee \theta \supseteq \psi$ and so $[\gamma, \psi] \subseteq [\gamma, \beta \vee \theta]$ by order-preservation. Now

$[\gamma, \beta \vee \theta] = [\gamma, \beta] \vee [\gamma, \theta]$ (by Proposition 2.12 (additivity))

$\subseteq (\gamma \cap \beta) \vee \theta$ (by Proposition 2.9 (i))

$= \theta$ (since $\gamma \cap \beta \subseteq \theta$).

Thus $[\gamma, \psi] \subseteq \theta$, therefore $\gamma \subseteq \varphi$ (by definition of φ). Similarly, $\beta \subseteq \varphi$.

Let $S = \{\mathcal{F} \subseteq \mathcal{P}(I) : \mathcal{F}$ is a filter over I and for all J, if $J \in \mathcal{F}$ then $\eta_J \subseteq \theta\}$.

Choose $\mathcal{F} = \{I\}$. Then $\mathcal{F}$ is a filter over I. Since $\lambda_I : \mathbf{C} \to \prod_{i \in I} \mathbf{A}_i$ is the inclusion map, $\eta_I = id_C \subseteq \theta$ so $\mathcal{F} \in S$, so $S \neq \emptyset$. S is partially ordered by $\subseteq$. Let $\langle C; \subseteq \rangle$ be a chain in S. We claim that C has an upper bound in S. Assume C is nonempty otherwise any element of S is an upper bound of $\emptyset$ in S.

Clearly, $\cup C$ is a filter over I. If $J \in \cup C$ then $J \in \mathcal{F}$ for some $\mathcal{F} \in C$ so $\eta_J \subseteq \theta$. From the above, $\cup C \in S$, and $\cup C$ is an upper bound for C in S. By Zorn's Lemma, S has a maximal element $\mathcal{F}_m$, i.e., $\mathcal{F}_m$ is maximal among filters $\mathcal{F}$ over I such that $J \in \mathcal{F}$ implies $\eta_J \subseteq \theta$.

Now $\lambda_\emptyset(c) = \emptyset$ for all $c \in C$ so $\eta_\emptyset = C^2 \not\subseteq \theta$ (since $\mathbf{B}$, being subdirectly irreducible, is nontrivial), so $\emptyset \notin \mathcal{F}_m$, i.e., $\mathcal{F}_m$ is a proper filter. Consequently, there is an ultrafilter $\mathcal{U}$ over I extending $\mathcal{F}_m$ (by Theorem 0.31).

We claim that $J \in \mathcal{U}$ implies $\eta_J \subseteq \varphi$.

(i) If $J \in \mathcal{F}_m$, clearly $\eta_J \subseteq \theta \subseteq \varphi$ by definition of $\mathcal{F}_m$.

(ii) Assume $J \in \mathcal{U} \setminus \mathcal{F}_m$. We show $\eta_J \subseteq \varphi$.

Consider $\mathcal{F}_1 = \langle \mathcal{F}_m \cup \{J\} \rangle$ (i.e. the intersection of all filters over I containing $\mathcal{F}_m \cup \{J\}$) and $\mathcal{F}_2 = \langle \mathcal{F}_m \cup \{J'\} \rangle$ where $J' := I \setminus J = \{i \in I : i \notin J\}$. Clearly, $\mathcal{F}_1 = \{E \in \mathcal{P}(I) : E \supseteq K \cap J$ for some $K \in \mathcal{F}_m\}$.

By maximality of $\mathcal{F}_m$, there exists $E \in \mathcal{F}_1$ such that $\eta_E \not\subseteq \theta$. Now $E \supseteq K_1 \cap J$ for some $K_1 \in \mathcal{F}_m$ and $\eta_E \subseteq \eta_{K_1 \cap J}$, so $\eta_{K_1 \cap J} \not\subseteq \theta$. Similarly, there exists $K_2 \in \mathcal{F}_m$, such that $\eta_{K_2 \cap J'} \not\subseteq \theta$. Now $M := K_1 \cap K_2 \in \mathcal{F}_m$ and $\eta_{M \cap J} \supseteq \eta_{K_1 \cap J}$, therefore $\eta_{M \cap J} \not\subseteq \theta$; similarly, $\eta_{J' \cap M} \not\subseteq \theta$. Now

$\eta_{J \cap M} \cap \eta_{J' \cap M} = \eta_{(J \cap M) \cup (J' \cap M)}$

$= \eta_{M \cap (J \cup J')}$

$= \eta_{M \cap I} = \eta_M \subseteq \theta$ (by definition of $\mathcal{F}_m$).

Hence by (3), $\eta_{J \cap M} \subseteq \varphi$. But since $J \cap M \subseteq J$, we have $\eta_J \subseteq \eta_{J \cap M} \subseteq \varphi$, which proves the claim.

Let $\theta_\mathcal{U}$ be the congruence on $\prod_{i \in I} \mathbf{A}_i$ defined by $(a, b) \in \theta_\mathcal{U}$ if and only if $[[a = b]] \in \mathcal{U}$. Let $\zeta = \theta_\mathcal{U}|_\mathbf{C} \in Con(\mathbf{C})$. Then $\mathbf{C}/\zeta$ is a subalgebra of $\prod_{i \in I} \mathbf{A}_i/\theta_\mathcal{U}$. Let $(c, d) \in \zeta$. Then $c, d \in C$ and there exists $J \in \mathcal{U}$ such that $J \subseteq \{i \in I : c(i) = d(i)\}$, therefore $\eta_J \subseteq \varphi$, by the previous claim, and $(c, d) \in \eta_J$. Thus, $\zeta \subseteq \eta_J$ so $\zeta \subseteq \varphi$.

We have shown $\mathbf{B}/\alpha \cong \mathbf{C}/\varphi$. We show $\mathbf{C}/\varphi \in HSP_U(K)$.

$\mathbf{C}/\zeta$ is a subalgebra of $\prod_{i\in I} \mathbf{A}_i/\theta_{\mathcal{U}}$, so $\mathbf{C}/\zeta \in SP_U(K)$. Now $\zeta, \varphi \in Con(\mathbf{C})$ and $\zeta \subseteq \varphi$ so $\varphi/\zeta \in Con(\mathbf{C}/\zeta)$ and by the Second Isomorphism Theorem, $(\mathbf{C}/\zeta)/(\varphi/\zeta) \cong \mathbf{C}/\varphi$, so $\mathbf{C}/\varphi$ is a homomorphic image of $\mathbf{C}/\zeta$. Now $\mathbf{C}/\varphi \in HSP_U(K)$ and so $\mathbf{B}/\alpha \in HSP_U(K)$.

Suppose $V(K)$ is locally finite. We show $\mathbf{B}/\gamma \in SP_UHS(K)$ for some $\gamma \subseteq \alpha$.

By Lemma 4.4, there is a family $\{\mathbf{B}_i : i \in I\}$ of finitely generated subdirectly irreducible algebras such that $\mathbf{B} \in ISP_U(\{\mathbf{B}_i : i \in I\})$ and for all $i \in I, \mathbf{B}_i \in HS(\mathbf{B}) \subseteq V(K)$. Since each $\mathbf{B}_i$ is finitely generated and in $V(K)$, each $\mathbf{B}_i$ is finite. Fix $i \in I$. Now $\mathbf{B}_i$ is a homomorphic image of a finitely generated $V(K)-$free algebra $\mathbf{F}$ (Corollary 0.48). Since $\mathbf{F} \in V(K)$, $\mathbf{F}$ is finite. It follows that, up to isomorphism, $\mathbf{F}$ has only finitely many homomorphic images, each of which is finite.

By Theorem 0.49, $\mathbf{F} \in ISP(K)$, so there is a family $\{E_j : j \in J\}$ (with $\mathbf{E}_j \in K$ for all $j \in J$) and an embedding $h : \mathbf{F} \to \prod_{j\in J} \mathbf{E}_j$. Let $\pi_k : \prod_{j\in J} \mathbf{E}_j \to \mathbf{E}_k$ be the k^{th} projection homomorphism, for each $k \in J$. Then $\mathbf{A}_j := (\pi_j \circ h)[\mathbf{F}]$ is a subalgebra of $\mathbf{E}_j$ for each $j \in J$ (because $\pi \circ h$ is a homomorphism). Thus $\mathbf{A}_j \in S(K)$ for each $j \in J$.

We now have that $h : \mathbf{F} \to \prod_{j\in J} \mathbf{A}_j$ is a subdirect embedding (by definition of $\mathbf{A}_j$). Thus $\mathbf{F} \in IP_S(\{\mathbf{A}_j : j \in J\})$. Now for each $j \in J$, $\mathbf{A}_j$ is a homomorphic image of $\mathbf{F}$, so $\mathbf{A}_j$ is finite and $\{\mathbf{A}_j : j \in J\}$ partitions into a finite number of isomorphic classes, say $\{\mathbf{A}_j : j \in J_1\}, \dots, \{\mathbf{A}_j : j \in J_r\}$.

For each $s \in \{1, \dots, r\}$, choose one representative, say $\mathbf{G}_s \in \{\mathbf{A}_j : j \in J_s\}$. Then define $K_1 = \{\mathbf{G}_1, \dots, \mathbf{G}_r\}$, so K_1 is a finite subset of $S(K)$, and all elements of K_1 are finite algebras.

We can construct a subdirect embedding $h' : \mathbf{F} \to \prod_{j\in J} \mathbf{L}_j$ where for each $j \in J$, $\mathbf{L}_j = \mathbf{G}_s$ for the unique $s \in \{1, \dots, r\}$ such that $j \in J_s$. (If $h_{js} : \mathbf{A}_j \cong \mathbf{G}_s$, define, for all $\bar{f} \in F, (h'(\bar{f}))(j) = h_{js}((h(\bar{f}))(j))$, $j \in J$.) It follows that $\mathbf{F} \in IP_S(\{\mathbf{G}_1, \dots, \mathbf{G}_r\}) = IP_S(K_1)$.

Now $\mathbf{B}_i \in H(\mathbf{F})$, so $\mathbf{B}_i \in HIP_S(K_1) = HP_S(K_1) \subseteq V(K_1)$. Note that $V(K_1) \subseteq V(S(K)) \subseteq V(K)$, so $V(K_1)$ is modular and locally finite. Since $\mathbf{B}_i$ is subdirectly irreducible and in $V(K_1)$, the first part of this theorem shows that $\mathbf{B}_i/\alpha_i \in HSP_U(K_1)$, where $\alpha_i = (id_{B_i} : \mu_i)$ is the centralizer of μ_i, the monolith of $\mathbf{B}_i$. But K_1 is a finite set of finite algebras, so $P_U(K_1) \subseteq I(K_1)$ (by Lemma 0.33). Thus, $\mathbf{B}_i/\alpha_i \in HSI(K_1) = HS(K_1) \subseteq HS(S(K))$, so $\mathbf{B}_i/\alpha_i \in HS(K)$.

Recall that $\mathbf{B}$ is a subalgebra of an ultraproduct $(\prod_{i\in I}\mathbf{B}_i)/\theta_{\mathcal{U}}$ of $\{\mathbf{B}_i : i \in I\}$, where $\mathcal{U}$ is an ultrafilter over I. Let $\bar{\alpha} = ((\prod_{i\in I}\alpha_i) \vee \theta_{\mathcal{U}})/\theta_{\mathcal{U}}$ and $\bar{\mu} = ((\prod_{i\in I}\mu_i) \vee \theta_{\mathcal{U}})/\theta_{\mathcal{U}}$, so $\bar{\alpha}, \bar{\mu} \in Con((\prod_{i\in I}\mathbf{B}_i)/\mathcal{U})$.

By Proposition 2.17 (ii), in $\prod_{i\in I}\mathbf{B}_i$, $[\prod_{i\in I}\alpha_i, \prod_{i\in I}\mu_i] \subseteq \prod_{\imath\in I}[\alpha_i, \mu_i] = \prod_{i\in I} id_{B_i} = id_{(\prod_{i\in I} B_i)}$.

Let h_1 be the natural homomorphism from $\prod_{i\in I}\mathbf{B}_i$ onto $(\prod_{i\in I}\mathbf{B}_i)/\theta_{\mathcal{U}}$ (so $\theta_{\mathcal{U}} = ker(h_1)$). By Proposition 2.14 (i) and the above,

$[\bar{\alpha}, \bar{\mu}] = (h_1^{-1}[\bar{\alpha}, \bar{\mu}])/\theta_{\mathcal{U}}$

$= ([\prod_{i\in I}\alpha_i, \prod_{i\in I}\mu_i] \vee \theta_{\mathcal{U}})/\theta_{\mathcal{U}}$

$= \theta_{\mathcal{U}}/\theta_{\mathcal{U}} = id_{(\prod_{i\in I} B_i)/\theta_{\mathcal{U}}}$.

Recall that μ is the monolith of $\mathbf{B}$ and that $\alpha = (id_B : \mu)$. Let $\gamma = \bar{\alpha}|_{\mathbf{B}}$ and $\beta = \bar{\mu}|_{\mathbf{B}}$ in $Con(\mathbf{B})$. By Lemma 4.4 $\beta \neq id_B$, so $\mu \subseteq \beta$. By Proposition 2.14 (ii), $[\gamma, \mu] \subseteq [\gamma, \beta] \subseteq [\bar{\alpha}, \bar{\mu}]|_{\mathbf{B}} = id_B$ so $\gamma \subseteq \alpha$.

We have $\gamma = \bar{\alpha}|_{\mathbf{B}}$ and $\mathbf{B} \leq \prod_{i\in I}\mathbf{B}_i/\theta_{\mathcal{U}}$ so $\mathbf{B}/\gamma$ can be embedded in $((\prod_{i\in I}\mathbf{B}_i)/\theta_{\mathcal{U}})/\bar{\alpha}$. We claim $((\prod_{i\in I}\mathbf{B}_i)/\theta_{\mathcal{U}})/\bar{\alpha} \cong (\prod_{i\in I}(\mathbf{B}_i/\alpha_i))/\phi_{\mathcal{U}}$ where $\phi_{\mathcal{U}} = \{(b^1, b^2) \in (\prod_{i\in I}(\mathbf{B}_i/\alpha_i))^2 : \{i \in I : b^1(i) = b^2(i)\} \in \mathcal{U}\}$. Then $\mathbf{B}/\gamma \in ISP_U(HS(K))$ since we have proved $\mathbf{B}_i/\alpha_i \in HS(K)$ for all $i \in I$.

By Lemma 0.32, $\theta_{\mathcal{U}} \vee (\prod_{i\in I}\alpha_i) = \{(b^1, b^2) \in (\prod_{i\in I}\mathbf{B}_i)^2 : \{i \in I : (b^1(i), b^2(i)) \in \alpha_i\} \in \mathcal{U}\}$. Therefore the map $\psi : \prod_{i\in I}(\mathbf{B}_i/\alpha_i) \to ((\prod_{i\in I}\mathbf{B}_i)/\theta_{\mathcal{U}})/\bar{\alpha}$ given by

$$\psi((b_i/\alpha_i)_{i\in I}) = (((b_i)_{i\in I})/\theta_{\mathcal{U}})/\bar{\alpha} \;\; (= (b/\theta_{\mathcal{U}})/\bar{\alpha} \text{ where } b = (b_i)_{i\in I})$$

is well-defined and it is straightforward to verify that ψ is a surjective homomorphism with $ker(\psi) = \phi_{\mathcal{U}}$. Then $((\prod_{i\in I}\mathbf{B}_i)/\theta_{\mathcal{U}})/\bar{\alpha} \cong (\prod_{i\in I}(\mathbf{B}_i/\alpha_i))/\phi_{\mathcal{U}}$ by the Homomorphism Theorem.

□

Corollary 4.7. *Let K be a class of algebras of the same type such that $V(K)$ is congruence modular, and let $\mathbf{B} \in V(K)$ be subdirectly irreducible with monolith μ. Let α be the centralizer of μ.*

(i) *μ is an Abelian congruence if and only if $\alpha \neq id_B$.*

(ii) *μ is an Abelian congruence or $\mathbf{B} \in HSP_U(K)$.*

Proof.

(i) If μ is Abelian, i.e., $[\mu, \mu] = id_B$, then $\alpha \supseteq \mu$, so $\alpha \neq id_B$. Conversely, if $\alpha \neq id_B$ then $\mu \subseteq \alpha$, whence $[\mu, \mu] \subseteq [\mu, \alpha] = id_B$, so μ is Abelian.

(ii) If μ is not Abelian, $\alpha = id_B$ (by (i)). Then by Theorem 4.6, $\mathbf{B} = \mathbf{B}/\alpha \in HSP_U(K)$. □

Remark 4.8.

Suppose $V(K)$ is a congruence distributive variety, and $\mathbf{B} \in V(K)$ is subdirectly irreducible with monolith μ. Let α be the centralizer of μ. If $\alpha \supseteq \mu$ then, by Corollary 2.27, $[\mu, \alpha] \supseteq [\mu, \mu] = \mu \cap \mu = \mu \supset id_B = [\alpha, \mu]$, a contradiction, so $\alpha \not\supseteq \mu$, hence $\alpha = id_B$. By the previous corollary, α is non-Abelian and so $\mathbf{B} \in HSP_U(K)$. Thus, Jónsson's Theorem is a special case of Theorem 4.6. Moreover, when $V(K)$ is also locally finite, we get a stronger form of Jónsson's Theorem, viz. $\mathbf{B} \in ISP_U HS(K)$.

4.3 Residually Small Modular Varieties. From Proposition 2.9 (i), for an algebra $\mathbf{A}$ and $\beta, \gamma \in Con(\mathbf{A})$, $[\beta, \gamma] \subseteq \beta \cap \gamma \subseteq \beta$. If $\mathbf{A}$ is a member of a modular variety V and if $\beta \subseteq [\gamma, \gamma]$ and $[\beta, \gamma] \subset \beta$, Theorem 4.10 (below) states that V will not be residually small. Hence a modular variety V is residually small only if $\mathbf{Con(A)} \models (C1)$ for all $\mathbf{A} \in V$, since the congruence quasi-identity $x \leq [y, y] \rightarrow [x, y] \approx x$ is equivalent to (C1) by Theorem 4.1.

As stated previously, Theorem 4.11 (below) contains a crucial result on the size of subdirectly irreducible algebras in residually small modular varieties. In addition, this theorem states that if an algebra $\mathbf{A}$ is finite and $V(\mathbf{A})$ is modular, then $V(\mathbf{A})$ has a finite residual bound if and only if the subalgebras of $\mathbf{A}$ satisfy (C1).

Lemma 4.9. [FM87, Theorem 10.14]

Let V be a modular variety containing an algebra $\mathbf{A}$ with congruences β and γ satisfying $\beta \subseteq [\gamma, \gamma]$ and $[\beta, \gamma] \subset \beta$. Then there exist a subdirectly irreducible algebra $\mathbf{A}' \in V$ and congruences $\beta', \gamma' \in Con(\mathbf{A})$ such that β' is the monolith of $\mathbf{A}'$ and $\beta' \subseteq [\gamma', \gamma']$ and $[\beta', \gamma'] = id_{A'}$.

Proof.

We claim that there is a $\theta \in Con(\mathbf{A})$ such that θ is completely meet irreducible, $[\beta, \gamma] \subseteq \theta$ and $\beta \not\subseteq \theta$.

By Birkhoff's Subdirect Decomposition Theorem, $\mathbf{A}/[\beta, \gamma]$ is a subdirect product of subdirectly irreducible homomorphic images of itself. These may be assumed to be of the form $(\mathbf{A}/[\beta, \gamma])/(\theta_i/[\beta, \gamma]), i \in I$, where $[\beta, \gamma] \subseteq \theta_i \in Con(\mathbf{A})$ for each $i \in I$, by the Homomorphism Theorem and the Correspondence Theorem. It follows that $(\cap_{i \in I} \theta_i)/[\beta, \gamma] = id_{A/[\beta, \gamma]}$, i.e., that $\cap_{i \in I} \theta_i = [\beta, \gamma]$. Since $\mathbf{A}/\theta_i \cong (\mathbf{A}/[\beta, \gamma])/(\theta_i/[\beta, \gamma])$ is subdirectly irreducible, each θ_i is completely meet irreducible in $\mathbf{Con(A)}$ by Theorem 0.21.

There exists $i \in I$ such that $\beta \not\subseteq \theta_i$. For, otherwise $\beta \subseteq \cap_{i \in I} \theta_i = [\beta, \gamma]$, a contradiction. Choose $i \in I$ such that $\beta \not\subseteq \theta_i$. We have $[\beta, \gamma] \subseteq \theta_i$, so we may take $\theta = \theta_i$ in the above claim. Since $\mathbf{A}/\theta$ is subdirectly irreducible, θ must have a unique cover in **Con**(**A**). Let θ^* be this unique cover of θ (so θ^*/θ is the monolith of $\mathbf{A}/\theta$).

We show $\theta^* \subseteq [\theta \vee \gamma, \theta \vee \gamma] \vee \theta$. ....(1)

Certainly, $\theta \subseteq [\theta \vee \gamma, \theta \vee \gamma] \vee \theta$. Suppose $\theta = [\theta \vee \gamma, \theta \vee \gamma] \vee \theta$. Then $\theta \supseteq [\theta \vee \gamma, \theta \vee \gamma] \supseteq [\gamma, \gamma]$ by order-preservation, but $\beta \subseteq [\gamma, \gamma]$ so $\theta \supseteq \beta$, a contradiction. We therefore have $\theta \subset [\theta \vee \gamma, \theta \vee \gamma] \vee \theta$, but θ^* is the unique cover for θ, so $[\theta \vee \gamma, \theta \vee \gamma] \vee \theta \supseteq \theta^*$.

We show $[\theta^*, \theta \vee \gamma] \subseteq \theta$. ....(2)

Now $\theta \subseteq \theta \vee \beta$, but $\beta \not\subseteq \theta$ so $\theta \subset \theta \vee \beta$. Since θ^* is the unique cover for θ, $\theta^* \subseteq \theta \vee \beta$. Therefore

$[\theta^*, \theta \vee \gamma] \subseteq [\theta \vee \beta, \theta \vee \gamma]$ (by order-preservation)

$= [\theta, \theta] \vee [\theta, \beta] \vee [\theta, \gamma] \vee [\beta, \gamma]$ (by additivity)

$\subseteq \theta$ (by Proposition 2.9 and since $[\beta, \gamma] \subseteq \theta$).

Thus, $[\theta^*, \theta \vee \gamma] \subset \theta^*$.

Define $\mathbf{A}' := \mathbf{A}/\theta$, and $\gamma' := (\theta \vee \gamma)/\theta \in Con(\mathbf{A}')$. Then $\mathbf{A}' \in V_{SI}$ (since V is closed under H). Let β' be the monolith θ^*/θ of $\mathbf{A}'$. Then

$[\beta', \gamma'] = [\theta^*/\theta, (\theta \vee \gamma)/\theta]$

$= ([\theta^*, \theta \vee \gamma] \vee \theta)/\theta$ (by Proposition 2.14 (i))

$= id_{A'}$ (by (2)).

Also $\beta' = \theta^*/\theta \subseteq ([\theta \vee \gamma, \theta \vee \gamma] \vee \theta)/\theta$ (by (1))

$= [(\theta \vee \gamma)/\theta, (\theta \vee \gamma)/\theta]$ (by Proposition 2.14 (i))

$= [\gamma', \gamma']$ as required. □

Theorem 4.10. [FM87, Theorem 10.14]

Let V be a modular variety containing an algebra $\mathbf{A}$ with congruences β and γ satisfying $\beta \subseteq [\gamma, \gamma]$ and $[\beta, \gamma] \subset \beta$. Then V is not residually small.

Proof.

By the previous lemma we may assume without loss of generality that $\mathbf{A}$ is subdirectly irreducible with monolith β and that $[\gamma, \beta] = id_A$. Recall that $\mathbf{A}(\gamma)$ is γ regarded as a subalgebra of $\mathbf{A} \times \mathbf{A}$. Let $\kappa = \Delta_{\gamma,\beta}$, i.e., κ is the congruence on $\mathbf{A}(\gamma)$ generated by the set of all pairs of the form

$$((u,u),(v,v)) = \begin{bmatrix} u & v \\ u & v \end{bmatrix} \in M(\gamma, \beta).$$

(See Definition 2.18.)

Let $\eta_0, \eta_1 \in Con(\mathbf{A}(\gamma))$ be the respective kernels of the first and second projection homomorphisms p_0, p_1 from $\mathbf{A} \times \mathbf{A}$ onto $\mathbf{A}$. We show $\kappa \cap \eta_0 = \kappa \cap \eta_1 = id_{A(\gamma)}$.

If $a \in \kappa \cap \eta_0$, then a has the form $((u,x),(u,y))$ where $u\gamma x$ and $u\gamma y$, and

$$a = \begin{bmatrix} u & u \\ x & y \end{bmatrix} \in \Delta(\gamma,\beta), \text{ therefore} \begin{bmatrix} x & y \\ u & u \end{bmatrix} \in \Delta(\gamma,\beta)$$

(by Proposition 2.22). By Theorem 2.25, we have $(x,y) \in [\gamma,\beta]$, i.e., $x = y$. Therefore $\kappa \cap \eta_0 = id_{A(\gamma)}$.

Similarly, Theorem 2.25 (alone) yields $\kappa \cap \eta_1 = id_{A(\gamma)}$.

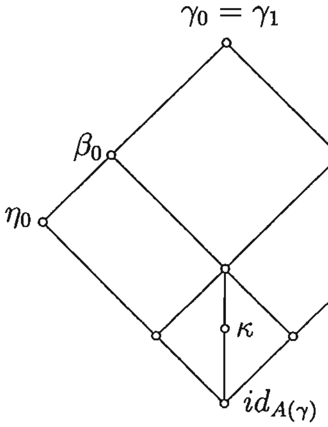
We show $\kappa \vee \eta_0 = \beta_0$ and $\kappa \vee \eta_1 = \beta_1$ where β_0 denotes $p_0^{-1}(\beta)$ and β_1 denotes $p_1^{-1}(\beta)$. Clearly, $\kappa \vee \eta_i \subseteq \beta_i$ for $i = 1, 2$.

Let $((x_1,y_1),(x_2,y_2)) \in \beta_0$. Then $(x_1,y_1),(x_2,y_2) \in \gamma$ and $(x_1,x_2) \in \beta$. Also $((x_1,y_1),(x_1,x_1)) \in \eta_0$, $((x_2,x_2),(x_2,y_2)) \in \eta_0$ and

$$((x_1,x_1),(x_2,x_2)) = \begin{bmatrix} x_1 & x_2 \\ x_1 & x_2 \end{bmatrix} \in \kappa$$

(since $(x_1,x_2) \in \beta$) so there exist $c_1, c_2, c_3, c_4 \in A(\gamma)$, namely $c_1 = (x_1,y_1), c_4 = (x_2,y_2), c_2 = (x_1,x_1), c_3 = (x_2,x_2)$ such that $(c_1,c_2) \in \eta_0$, $(c_2,c_3) \in \kappa$, $(c_3,c_4) \in \eta_0$ so $((x_1,y_1),(x_2,y_2)) = (c_1,c_4) \in \kappa \vee \eta_0$ (Theorem 0.8). Thus $\beta_0 \subseteq \kappa \vee \eta_0$.

Similarly, $\eta_1 \vee \kappa = \beta_1$.



Let $\aleph$ be an arbitrary cardinal and let

$$B = \{(a_\delta)_{\delta<\aleph} \in A^\aleph : a_\delta \gamma a_\epsilon \text{ for all ordinals } \delta, \epsilon < \aleph\}.$$

By the compatibility of γ, B is the universe of a subalgebra $\mathbf{B}$ of $\mathbf{A}^\aleph$ and so $\mathbf{B} \in V$. For any $\psi \in Con(\mathbf{A})$ and any $\epsilon < \aleph$, define $\psi_\epsilon \in Con(\mathbf{B})$ by

$(a_\delta)_{\delta<\aleph}\psi_\epsilon(b_\delta)_{\delta<\aleph}$ if and only if $a_\epsilon\psi b_\epsilon$. .... (1)
By transitivity of γ, $\gamma_\delta = \gamma_\epsilon$ for any $\delta, \epsilon < \aleph$. We write $\hat{\gamma} = \gamma_\delta$ (for any $\delta < \aleph$). For convenience, we write (a_ρ) for $(a_\rho)_{\rho<\aleph}$.

For all $\epsilon < \aleph$, define $\eta_\epsilon = ker(p_\epsilon)$ where $p_\epsilon : \mathbf{B} \to \mathbf{A}$ is the projection homomorphism given by $p_\epsilon((a_\rho)) = a_\epsilon$, so $\eta_\epsilon \in Con(\mathbf{B})$. Now $\eta_\epsilon = (id_B)_\epsilon$ as defined in (1).

Also, define $\eta'_\delta = \cap_{\delta\neq\epsilon<\aleph}\eta_\epsilon \in Con(\mathbf{B})$ $(\delta < \aleph)$. Let $\delta < \aleph$. We show $\eta'_\delta \vee \eta_\delta = \hat{\gamma}$. Clearly, $\eta'_\delta \vee \eta_\delta \subseteq \hat{\gamma}$.

Let $((a_\rho), (b_\rho)) \in \hat{\gamma}$. Then since $\gamma_\delta = \hat{\gamma}$, $a_\delta\gamma b_\delta$ and since $(a_\rho), (b_\rho) \in B$, for all $\rho, \sigma < \aleph$, we have $a_\rho\gamma a_\sigma$, and $b_\rho\gamma b_\sigma$. Let $c_1 = (a_\rho), c_3 = (b_\rho)$ and let c_2 be defined by

$$c_2(\rho) = \begin{cases} a_\rho, & \rho \neq \delta \\ b_\rho, & \rho = \delta, \end{cases}$$

i.e., $c_1 = (a_0, \dots, a_\epsilon, \dots, a_\delta, \dots)$
$c_2 = (a_0, \dots, a_\epsilon, \dots, b_\delta, \dots)$
$c_3 = (b_0, \dots, b_\epsilon, \dots, b_\delta, \dots)$.

We have shown that for all $\rho < \aleph$, $a_\rho\gamma a_\delta$ so for all $\rho < \aleph$, $a_\rho\gamma b_\delta$. Hence $c_2(\lambda)\gamma c_2(\rho)$ for all $\rho, \lambda < \aleph$, by transitivity, therefore $c_2 \in B$. Now $(c_1, c_2) \in \eta'_\delta$, and $(c_2, c_3) \in \eta_\delta$ so $((a_\rho), (b_\rho)) = (c_1, c_3) \in \eta'_\delta \vee \eta_\delta$. Thus, $\hat{\gamma} \subseteq \eta'_\delta \vee \eta_\delta$, hence $\hat{\gamma} = \eta'_\delta \vee \eta_\delta$. It follows that $\hat{\gamma} = \eta_\delta \vee \eta_\epsilon$ whenever $\delta \neq \epsilon < \aleph$.

For all $\delta < \aleph$ we define

$$\kappa_\delta := \{((a_\rho), (b_\rho)) \in B^2 : (a_0, a_\delta)\Delta_{\gamma,\beta}(b_0, b_\delta) \text{ and } a_\epsilon = b_\epsilon \text{ for all } \epsilon \in \aleph \setminus \{0, \delta\}\}$$

$$(= \{((a_\rho), (b_\rho)) \in B^2 : \begin{bmatrix} a_0 & b_0 \\ a_\delta & b_\delta \end{bmatrix} \in \Delta_{\gamma,\beta} \text{ and } a_\epsilon = b_\epsilon, \text{ for all } \epsilon \in \aleph \setminus \{0, \delta\}\}.)$$

Since $\Delta_{\gamma,\beta} \in Con(\mathbf{A}(\gamma))$, it is straightforward to verify that $\kappa_\delta \in Con(\mathbf{B})$.

For all $\delta < \aleph$, we define

$$\theta_\delta := \{((a_\epsilon), (b_\epsilon)) \in B^2 : a_\delta\beta b_\delta \text{ and } a_\epsilon = b_\epsilon, \text{ for all } \epsilon \in \aleph \setminus \{\delta\}\} \in Con(\mathbf{B}).$$

Suppose $0 < \delta < \aleph$. We show $\theta_0 \subseteq \eta'_\delta \vee \kappa_\delta$.

Let $((a_\epsilon), (b_\epsilon)) \in \theta_0$ where $(a_\epsilon), (b_\epsilon) \in B$. Then $(a_0, b_0) \in \beta$ and $a_\epsilon = b_\epsilon$, whenever $\epsilon \neq 0$. .... (2)

Let $(a_\epsilon) = (a_0, \dots, a_\delta, a_{\delta+1}, \dots) = c_1$ and let $c_2 = (a_0, \dots, a_0, a_{\delta+1}, \dots)$, i.e.,

$$c_2(\epsilon) = \begin{cases} a_\epsilon & \text{for } \epsilon \neq \delta \\ a_0 & \text{for } \epsilon = \delta. \end{cases}$$

Whenever $\delta \neq \epsilon < \aleph$, then $c_1(\epsilon) = c_2(\epsilon)$ so $(c_1, c_2) \in \eta_\epsilon$, therefore $(c_1, c_2) \in \bigcap_{\delta \neq \epsilon < \aleph} \eta_\epsilon = \eta'_\delta$.

Let $c_3 = (b_0, \dots, b_0, b_{\delta+1}, \dots)$, i.e.,

$$c_3(\epsilon) = \begin{cases} b_\epsilon & \text{for } \epsilon \neq \delta \\ b_0 & \text{for } \epsilon = \delta. \end{cases} \qquad \text{Then } \begin{bmatrix} a_0 & b_0 \\ a_0 & b_0 \end{bmatrix} \in \Delta_{\gamma,\beta}.$$

By (2), $(c_2(0), c_2(\delta))\Delta_{\gamma,\beta}(c_3(0), c_3(\delta))$ and $c_2(\epsilon) = c_3(\epsilon)$, for $\epsilon \notin \{0, \delta\}$ so $(c_2, c_3) \in \kappa_\delta$. Also $c_2, c_3 \in B$, since $(a_\epsilon), (b_\epsilon) \in B$.

Let $c_4 = (b_\epsilon) = (b_0, \dots, b_\delta, \dots)$. Then $(c_3, c_4) \in \eta'_\delta$. Therefore $((a_\epsilon), (b_\epsilon)) \in \eta'_\delta \circ \kappa_\delta \circ \eta'_\delta \subseteq \eta'_\delta \vee \kappa_\delta$, so $\theta_0 \subseteq \eta'_\delta \vee \kappa_\delta$.

We claim that $\theta_0 \subseteq \kappa_\delta \vee \theta_\delta$.

By Lemma 2.21, $\kappa_\delta \subseteq \beta_\delta$ and clearly $\theta_0 \subseteq \beta_\delta$. Also, by the definitions, $\eta'_\delta \cap \beta_\delta = \theta_\delta$. By modularity, since $\kappa_\delta \subseteq \beta_\delta$, we have $\theta_0 = \theta_0 \cap \beta_\delta \subseteq \beta_\delta \cap (\eta'_\delta \vee \kappa_\delta) = \kappa_\delta \vee (\eta'_\delta \cap \beta_\delta) = \kappa_\delta \vee \theta_\delta$, as claimed. By a similar argument, $\theta_\delta \subseteq \theta_0 \vee \kappa_\delta$.

Let $\theta := \bigvee_{\delta < \aleph} \theta_\delta \in Con(\mathbf{B})$ and let $\kappa := \bigvee_{0 < \delta < \aleph} \kappa_\delta \in Con(\mathbf{B})$. For $0 < \delta, \epsilon < \aleph$, we have $\theta_0 \subseteq \kappa_\delta \vee \theta_\delta$ and $\theta_\delta \subseteq \kappa_\delta \vee \theta_0$ so

$\kappa \vee \theta_\delta = \kappa \vee \kappa_\delta \vee \kappa_\epsilon \vee \theta_\delta$ (because $\kappa_\delta \vee \kappa_\epsilon \subseteq \kappa$)

$= \kappa \vee [(\kappa_\delta \vee \theta_\delta) \vee \theta_0] \vee \kappa_\epsilon$ (because $\kappa_\delta \vee \theta_\delta \supseteq \theta_0$)

$= \kappa \vee \theta_\delta \vee \theta_0 \vee \kappa_\epsilon$ (because $\kappa_\delta \subseteq \kappa$)

$= \kappa \vee \theta_\delta \vee [(\theta_0 \vee \kappa_\epsilon) \vee \theta_\epsilon]$ (because $\kappa_\epsilon \vee \theta_0 \supseteq \theta_\epsilon$)

$= \kappa \vee \theta_\delta \vee \theta_0 \vee \theta_\epsilon$ (because $\kappa_\epsilon \subseteq \kappa$).

Therefore $\kappa \vee \theta_\delta \supseteq \theta_\epsilon \vee \theta_0$. Thus, $\kappa \vee \theta_\delta \supseteq (\bigvee_{\epsilon \neq 0,\delta} \theta_\epsilon) \vee \theta_0$, therefore $\kappa \vee \theta_\delta \supseteq (\bigvee_{\epsilon \neq 0,\delta} \theta_\epsilon) \vee \theta_0 \vee \theta_\delta = \theta$.

Also, for $0 < \delta < \aleph$, $\kappa \vee \theta_0 \supseteq \theta_\delta \vee \theta_0$, so $\kappa \vee \theta_0 \supseteq \theta$. Thus, for all $\delta \in \aleph$, $\kappa \vee \theta_\delta \supseteq \theta$. We shall show that equality holds.

For $0 < \delta < \aleph$, we claim that $\kappa_\delta \subseteq \theta$.

Let $((a_\epsilon), (b_\epsilon)) \in \kappa_\delta$. Then $(a_0, a_\delta)\Delta_{\gamma,\beta}(b_0, b_\delta)$ and $a_\epsilon = b_\epsilon$ for $\epsilon \in \aleph \setminus \{0, \delta\}$. We write (b_ϵ) as $(b_0, a_1, a_2, \dots, b_\delta, a_{\delta+1}, \dots)$. By Lemma 2.21, $(a_0, b_0) \in \beta$ and $(a_\delta, b_\delta) \in \beta$.

Let $d_0 = (a_\epsilon), d_2 = (b_\epsilon)$ and define $d_1 \in A^{\aleph}$ by

$$d_1(\epsilon) := \begin{cases} b_0 & \text{for } \epsilon = 0 \\ a_\epsilon & \text{for } \epsilon \neq 0. \end{cases}$$

i.e., $d_0 = (a_0, a_1, \ldots, a_\delta, a_{\delta+1}, \ldots)$

$d_1 = (b_0, a_1, \ldots, a_\delta, a_{\delta+1}, \ldots)$

$d_2 = (b_0, a_1, \ldots, b_\delta, a_{\delta+1}, \ldots)$.

Clearly, $d_1 \in B$.

Now $(d_0, d_1) \in \theta_0$ and $(d_1, d_2) \in \theta_\delta$ so $((a_\epsilon), (b_\epsilon)) = (d_0, d_2) \in \theta_0 \vee \theta_\delta \subseteq \theta$. Therefore $\kappa_\delta \subseteq \theta$, as claimed, and so $\kappa \subseteq \theta$.

Obviously, $\theta_\delta \subseteq \theta$, so we infer that $\theta_\delta \vee \kappa \subseteq \theta$, hence

$\theta_\delta \vee \kappa = \theta$ for all $\delta < \aleph$. ....(3)

By similar arguments, $\kappa_\epsilon \subseteq \theta_0 \vee \theta_\epsilon$ for any $\epsilon < \aleph$. Therefore

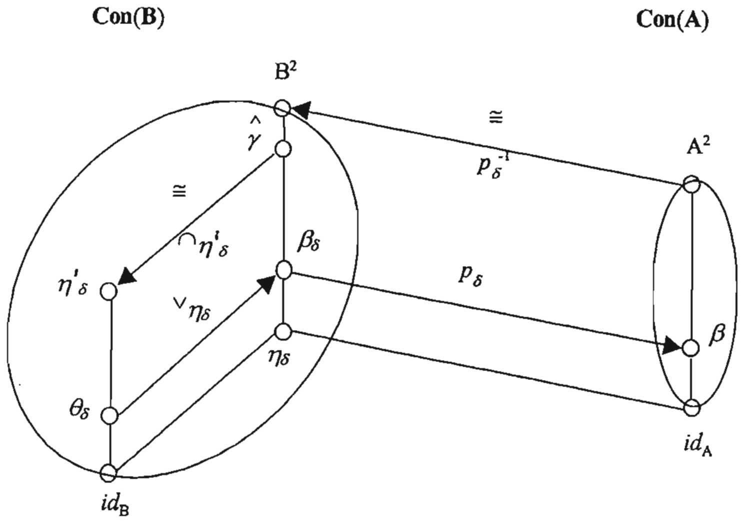
$\kappa_{\epsilon_1} \vee \ldots \vee \kappa_{\epsilon_r} \subseteq \theta_0 \vee \theta_{\epsilon_1} \vee \ldots \vee \theta_{\epsilon_r}$ for all $\epsilon_1, \ldots, \epsilon_r < \aleph$. ....(4)

Let $\delta < \aleph$. We show that $\theta_\delta \succ id_B$ in **Con(B)**.

By the Correspondence Theorem, since the δ^{th} projection homomorphism $p_\delta : \mathbf{B} \to \mathbf{A}$ is surjective and $ker(p_\delta) = \eta_\delta$, the map $\xi \mapsto p_\delta^{-1}(\xi)$ is a lattice isomorphism from **Con(A)** onto $\mathbf{int}(\eta_\delta, B^2)$, so in **Con(B)**, $\eta_\delta \prec p_\delta^{-1}(\beta) = \beta_\delta$ (because in **Con(A)**, $id_A \prec \beta$). Since $\beta \subseteq \gamma$, we have $\beta_\delta \subseteq \hat{\gamma}$. Recall that $\eta_\delta \vee \eta_\delta^{'} = \hat{\gamma}$ and clearly, $\eta_\delta \cap \eta_\delta^{'} = id_B$. Thus, **Con(B)** is a modular lattice in which

$$int(\eta_\delta, \hat{\gamma}) \searrow int(id_B, \eta_\delta^{'}),$$

so the map $\alpha \mapsto \alpha \cap \eta_\delta^{'}$ is a lattice isomorphism from $\mathbf{int}(\eta_\delta, \hat{\gamma})$ onto $\mathbf{int}(id_B, \eta_\delta^{'})$ (by Theorem 0.3). Consequently, in **Con(B)**, $id_B \prec \beta_\delta \cap \eta_\delta^{'} = \theta_\delta$.



Choosing any $((a_\epsilon),(b_\epsilon)) \in \theta_\delta \setminus id_B$, we have $id_B \neq \Theta^{\mathbf{B}}((a_\epsilon),(b_\epsilon)) \subseteq \theta_\delta$ but since $\theta_\delta \succ id_B$, $\Theta^{\mathbf{B}}((a_\epsilon),(b_\epsilon)) = \theta_\delta$. Thus θ_δ is a principal (hence compact) congruence (see Theorem 0.10). Since θ_δ is compact, if $\theta_\delta \subseteq \kappa$, then $\theta_\delta \subseteq \kappa_{\epsilon_1} \vee \ldots \vee \kappa_{\epsilon_n}$ for some $\epsilon_1, \ldots, \epsilon_n$.

We show that if J is a finite subset of $\aleph$ then $\bigvee_{\delta \in J} \theta_\delta = \{((a_\delta),(b_\delta)) \in B^2 : a_\delta \beta b_\delta$ for all $\delta \in J$ and $a_\delta = b_\delta$ for all $\delta \in \aleph \setminus J\}$. . . . . (5)

If $\rho = \{((a_\delta),(b_\delta)) \in B^2 : a_\delta \beta b_\delta$ for all $\delta \in J$ and $a_\delta = b_\delta$ for all $\delta \in \aleph \setminus J\}$ then clearly $\theta_\delta \subseteq \rho \in Con(\mathbf{B})$ for all $\delta \in J$, so $\bigvee_{\delta \in J} \theta_\delta \subseteq \rho$.

Conversely, if $((a_\epsilon),(b_\epsilon)) \in \rho$, and $J = \{\delta_1, \ldots, \delta_m\}$, say, then we can construct $(c^1_\epsilon), (c^2_\epsilon), \ldots, (c^{m+1}_\epsilon)$ as follows: let each (c^i_ϵ) differ from (c^{i+1}_ϵ) only in the co-ordinate δ_i, where $c^i_{\delta_i} = a_{\delta_i}$ and $c^{i+1}_{\delta_i} = b_{\delta_i}$. Then $(a_\epsilon) = (c^1_\epsilon)$, $(b_\epsilon) = (c^{m+1}_\epsilon)$ and $(c^i_\epsilon)\theta_{\delta_i}(c^{i+1}_\epsilon)$ for $i = 1, \ldots, m$ so $(a_\epsilon, b_\epsilon) \in \theta_{\delta_1} \circ \theta_{\delta_2} \circ \ldots \circ \theta_{\delta_m} \subseteq \bigvee_{\delta \in J} \theta_\delta$, as required.

It follows from (5) that if I and J are finite subsets of $\aleph$ with $I \cap J = \emptyset$ then $(\bigvee_{\delta \in I} \theta_\delta) \cap (\bigvee_{\delta \in J} \theta_\delta) = id_B$. . . . . (6)

We claim that for any positive integer m, if I is an m-element subset of $\aleph$, then $\theta_0 \not\subseteq \bigvee_{\epsilon \in I} \kappa_\epsilon$. The claim is proved by induction on m.

Suppose $m = 1$:

We first show that for any nonzero $\epsilon < \aleph$, $\theta_0 \cap \kappa_\epsilon = id_B$. Let $((a_\delta),(b_\delta)) \in \theta_0 \cap \kappa_\epsilon$. Then $a_0 \beta b_0$ and $a_\delta = b_\delta$, for all $\delta \neq 0$ and $(a_0, a_\epsilon)\Delta_{\gamma,\beta}(b_0, b_\epsilon)$. Now

$$((a_0, a_\epsilon),(b_0, b_\epsilon)) = \begin{bmatrix} a_0 & b_0 \\ a_\epsilon & b_\epsilon \end{bmatrix} = \begin{bmatrix} a_0 & b_0 \\ a_\epsilon & a_\epsilon \end{bmatrix} \text{ (since } \epsilon \neq 0)$$

so by Theorem 2.25, $(a_0, b_0) \in [\gamma, \beta] = id_B$. This means $a_0 = b_0$, therefore $(a_\delta) = (b_\delta)$ and so $\theta_0 \cap \kappa_\epsilon = id_B$, whence $\theta_0 \not\subseteq \kappa_\epsilon$, as required.

Now assume that $1 < m < \omega$ and that whenever $1 \leq l < m$ and I is an l-element subset of $\aleph$, then $\theta_0 \not\subseteq \bigvee_{\epsilon \in I} \kappa_\epsilon$.

Let $I = \{\epsilon_1, \ldots, \epsilon_m\}$ be an m-element subset of $\aleph$ (so $\epsilon_i \neq \epsilon_j$ for $i \neq j$). Suppose that $\theta_0 \subseteq \bigvee_{\epsilon \in I} \kappa_\epsilon$.

Then $\theta_0 = \theta_0 \cap (\bigvee_{\epsilon \in I} \kappa_\epsilon)$

$= \theta_0 \cap (\theta_0 \vee \theta_{\epsilon_1}) \cap (\kappa_{\epsilon_1} \vee (\bigvee_{i=2}^m \kappa_{\epsilon_i}))$ (because $\theta_0 \subseteq \theta_0 \vee \theta_{\epsilon_1}$)

$= \theta_0 \cap [\kappa_{\epsilon_1} \vee ((\theta_0 \vee \theta_{\epsilon_1}) \cap (\bigvee_{i=2}^m \kappa_{\epsilon_i}))]$ (by modularity as $\kappa_{\epsilon_1} \subseteq \theta_0 \vee \theta_{\epsilon_1}$, by (4))

$= \theta_0 \cap [\kappa_{\epsilon_1} \vee ((\theta_0 \vee \theta_{\epsilon_1}) \cap (\theta_0 \vee (\bigvee_{i=2}^m \theta_{\epsilon_i})) \cap (\bigvee_{i=2}^m \kappa_{\epsilon_i}))]$ (by (4))

We assume, without loss of generality, that $0 \notin \{\epsilon_2, \ldots, \epsilon_m\}$, so

$(\theta_0 \vee \theta_{\epsilon_1}) \cap (\theta_0 \vee (\bigvee_{i=2}^m \theta_{\epsilon_i}))$

$= \theta_0 \vee [(\theta_0 \vee \theta_{\epsilon_1}) \cap (\bigvee_{i=2}^m \theta_{\epsilon_i})]$ (by modularity because $\theta_0 \subseteq \theta_0 \vee \theta_{\epsilon_1}$)

$= \theta_0 \vee id_B$ (by (6), since $0 \notin \{\epsilon_2, \ldots , \epsilon_m\}$)

$= \theta_0$.

Thus $\theta_0 = \theta_0 \cap [\kappa_{\epsilon_1} \vee (\theta_0 \cap (\bigvee_{i=2}^{m} \kappa_{\epsilon_i}))]$. .... (7)

By the induction hypothesis, $\theta_0 \not\subseteq \bigvee_{i=2}^{m} \kappa_{\epsilon_i}$ so $id_B \subseteq \theta_0 \cap (\bigvee_{i=2}^{m} \kappa_{\epsilon_i}) \subset \theta_0$, but $\theta_0 \succ id_B$ so $\theta_0 \cap (\bigvee_{i=2}^{m} \kappa_{\epsilon_i}) = id_B$. Now (7) reads $\theta_0 = \theta_0 \cap \kappa_{\epsilon_1} = id_B$ (see the case $m = 1$), a contradiction. Thus $\theta_0 \not\subseteq \bigvee_{\epsilon \in I} \kappa_\epsilon$. By induction, if I is a finite subset of $\aleph$ then $\theta_0 \not\subseteq \bigvee_{\epsilon \in I} \kappa_\epsilon$. .... (8)

We claim $\theta_0 \not\subseteq \kappa$. If $\theta_0 \subseteq \kappa = \bigvee_{\delta < \aleph} \kappa_\delta$ then, since θ_0 is compact in **Con(B)** there exists a finite subset $I = \{\epsilon_1, \ldots , \epsilon_n\}$ of $\aleph$ such that $\theta_0 \subseteq \bigvee_{\epsilon \in I} \kappa_\epsilon$. This contradicts (8), so the claim is true.

We claim that for all $\delta \in \aleph$, $\theta_\delta \not\subseteq \kappa$. We consider $\delta \neq 0$ and show that $\kappa \vee \theta_\delta = \kappa \vee \theta_0$. Indeed, $\kappa \vee \theta_0 = \kappa \vee \kappa_\delta \vee \theta_0 \supseteq \kappa \vee \theta_\delta$ (since $\kappa \vee \theta_0 \supseteq \theta_\delta$), and $\kappa \vee \theta_\delta = \kappa \vee \kappa_\delta \vee \theta_\delta \supseteq \kappa \vee \theta_0$ (since $\kappa \vee \theta_\delta \supseteq \theta_0$).

Now $\kappa \vee \theta_\delta = \kappa \vee \theta_0 = \theta$ (by (3)) for all $\delta < \aleph$. If $\delta < \aleph$ then $\theta_\delta \not\subseteq \kappa$ because $\theta_0 \not\subseteq \kappa$. We have $\kappa \subseteq \kappa \vee \theta_\delta = \theta$ for all $\delta < \aleph$. By the last claim, $\theta \not\subseteq \kappa$ (otherwise we would have $\theta_\delta \subseteq \kappa$, a contradiction). Thus $\kappa \subset \theta$.

Exactly as at the start of the proof of Lemma 4.9, there is a completely meet irreducible $\lambda \in Con(\mathbf{B})$ such that $\theta \not\subseteq \lambda$ and $\kappa \subseteq \lambda$. Thus, $\mathbf{B}/\lambda$ is subdirectly irreducible and in V.

For each $\delta < \aleph$, we must have $\lambda \cap \eta_\delta' = id_B$. For otherwise, $\lambda \cap \eta_\delta' \supseteq \theta_\delta$ since θ_δ is the unique atom of $\mathbf{int}(id_B, \eta_\delta')$; but then $\lambda \supseteq \theta_\delta \vee \kappa = \theta$, a contradiction.

If for some $\delta < \aleph$, $\lambda \vee \eta_\delta \supseteq \hat{\gamma}$, then

$[\hat{\gamma}, \hat{\gamma}] = [\eta_\delta \vee \eta_\delta', \hat{\gamma}] \subseteq [\eta_\delta \vee \eta_\delta', \eta_\delta \vee \lambda]$

$= [\eta_\delta, \eta_\delta] \vee [\eta_\delta, \eta_\delta'] \vee [\eta_\delta, \lambda] \vee [\eta_\delta', \lambda]$ (by additivity)

$\subseteq \eta_\delta \vee (\eta_\delta \cap \eta_\delta') \vee (\eta_\delta \cap \lambda) \vee (\eta_\delta' \cap \lambda)$ (by Proposition 2.9 (i))

$= \eta_\delta$ (since $\eta_\delta' \cap \lambda = id_B = \eta_\delta \cap \eta_\delta'$).

Thus, by Proposition 2.14 (i), $[\gamma, \gamma] = [p_\delta(\hat{\gamma}), p_\delta(\hat{\gamma})] = [p_\delta(\hat{\gamma} \vee \eta_\delta), p_\delta(\hat{\gamma} \vee \eta_\delta)] = p_\delta([\hat{\gamma}, \hat{\gamma}] \vee \eta_\delta) = p_\delta(\eta_\delta) = id_A$, contradicting $\beta \subseteq [\gamma, \gamma]$. Thus for each $\delta < \aleph$, $\lambda \vee \eta_\delta \not\supseteq \hat{\gamma}$.

By the Correspondence Theorem, $\mathbf{int}(\lambda, B^2) \cong \mathbf{Con}(\mathbf{B}/\lambda)$. For each $\delta < \aleph$, we have $\lambda \vee \eta_\delta \in int(\lambda, B^2)$. We show that the $\lambda \vee \eta_\delta$ are pairwise distinct. Suppose $\delta, \epsilon < \aleph$ and $\delta \neq \epsilon$ and $\lambda \vee \eta_\delta = \lambda \vee \eta_\epsilon$. Then $\lambda \vee \hat{\gamma} = \lambda \vee \eta_\delta \vee \eta_\epsilon = \lambda \vee \eta_\epsilon$. Now $\hat{\gamma} \subseteq \lambda \vee \hat{\gamma} = \lambda \vee \eta_\epsilon$, a contradiction. Thus, the $\lambda \vee \eta_\delta$ are pairwise distinct.

Let $C = \{\lambda \vee \eta_\delta : \delta < \aleph\}$. Then $|C| = \aleph$ (because the $\lambda \vee \eta_\delta$ are pairwise distinct). It follows that $|int(\lambda, B^2)| \geq \aleph$, so $|Con(\mathbf{B}/\lambda)| \geq \aleph$.

If V were residually small there would exist a cardinal, say m, such that for any subdirectly irreducible algebra $\mathbf{A}$ in V, $|A| < \mathsf{m}$. Since $Con(\mathbf{A}) \subseteq \mathcal{P}(A \times A)$, this would imply $|Con(\mathbf{A})| \leq 2^{|A \times A|} = 2^{(|A|^2)} \leq 2^{(\mathsf{m}^2)}$, so the sizes of the congruence lattices of all the subdirectly irreducible algebras of V would be bounded by $2^{(\mathsf{m}^2)}$.

We have shown, however, that for an arbitrary cardinal $\aleph$, there is a subdirectly irreducible algebra (viz. $\mathbf{B}/\lambda$ above) in V whose congruence lattice has cardinality at least $\aleph$. This is a contradiction, since we can choose $\aleph > 2^{(\mathsf{m}^2)}$. Thus, V is not residually small. □

We are finally in a position to derive a major result of Freese and McKenzie, which shows that a finitely generated congruence modular residually small variety has a finite residual bound.

Theorem 4.11. [FM81]

Let $\mathbf{A}$ be an algebra in a modular variety and let $|A| = m \in \omega$. Then the following conditions are equivalent:

(i) $V(\mathbf{A})$ *is residually small.*

(ii) $V(\mathbf{A})$ *is residually* $< 1 + ((l+1)!m)$ *where* $l = m^{(m^{m+1})}$.

(iii) For any $\mu, \nu \in Con(\mathbf{C})$ *where* $\mathbf{C} \leq \mathbf{A}$, $\nu \subseteq [\mu, \mu]$ *implies* $\nu = [\nu, \mu]$.

Proof.

(ii)⇒(i) is clear.

(i)⇒(iii): If $\mathbf{C}$ is a subalgebra of $\mathbf{A}$ then $\mathbf{C} \in V(\mathbf{A})$. Now the result follows directly from Theorem 4.10.

(iii)⇒(ii): Assume (iii). Note that $V(\mathbf{A})$ is locally finite by Theorem 0.52, since it is finitely generated. Suppose $V(\mathbf{A})$ contains an infinite subdirectly irreducible algebra $\mathbf{B}$. Then by Quackenbush's Theorem (Theorem 1.26), $V(\mathbf{A})$ contains arbitrarily large finite subdirectly irreducible algebras, i.e., for each $k \in \omega$ there exists $\mathbf{C} \in V(\mathbf{A})_{SI}$ and such that $k < |C| < \aleph_0$.

We therefore need only show that every *finite* subdirectly irreducible algebra in $V(\mathbf{A})$ has cardinality bounded as in (ii), since then $V(\mathbf{A})$ will not have arbitrarily large subdirectly irreducible algebras and so $V(\mathbf{A})$ will not contain an infinite subdirectly irreducible algebra (completing the proof of (ii)).

We first show that every finite algebra in $V(\mathbf{A})$ satisfies (C1) of Theorem 4.1.

Let $\mathbf{D} \in V(\mathbf{A})$ with $|D| = q \in \omega$. Then $\mathbf{D} \in H(\mathbf{F})$ where $\mathbf{F} = \mathbf{F}_{V(\mathbf{A})}(\bar{x}_1, \ldots, \bar{x}_q)$ (Corollary 0.48). In addition, by Theorem 0.49, $\mathbf{F} \in$

$V(\mathbf{A})$ and $\mathbf{F}$ is finitely generated, therefore $\mathbf{F}$ is finite (since $V(\mathbf{A})$ is locally finite). Let $|F| = u \in \omega$.

Now there exists $g \in Hom(\mathbf{F}, \prod_{j\in J}\mathbf{A})$ (J possibly infinite) such that g is one-to-one (because $\mathbf{F} \in ISP(\mathbf{A})$). For each $j \in J$, let π_j be the j^{th} projection homomorphism from $\prod_{i\in J}\mathbf{A}$ onto $\mathbf{A}$. Then $\pi_j \circ g : \mathbf{F} \to \mathbf{A}$. Since $\mathbf{F}$ and $\mathbf{A}$ are both finite, there are only finitely many functions from F to A (at most $m^u = |A|^{|F|}$) so $\{\pi_j \circ g : j \in J\}$ is a finite set and there exist $p \in \omega$, with $p \leq m^u$ and $j_1, \dots, j_p \in J$ such that $\{\pi_j \circ g : j \in J\} = \{\pi_{j_1} \circ g, \dots, \pi_{j_p} \circ g\}$.

Define $g' : \mathbf{F} \to \prod_{i=1}^p \mathbf{A}$ by $g^{'}(\bar{t}) = ((\pi_{j_1} \circ g)(\bar{t}), \dots, (\pi_{j_p} \circ g)(\bar{t}))$ where $\bar{t} \in F$. Then, $g^{'}$ is a subdirect embedding, so we have $\mathbf{F} \in IS(\prod_{i=1}^p \mathbf{A})$.

By (iii), and Theorem 4.1 $\mathbf{A}$ satisfies (C1) hereditarily. By Theorem 4.2, since p is finite, $\prod_{i=1}^p \mathbf{A}$ and $\mathbf{F}$ and therefore $\mathbf{D} \in H(\mathbf{F})$ all satisfy (C1) hereditarily. Thus, every finite algebra in $V(\mathbf{A})$ satisfies (C1) hereditarily.

Now let $\mathbf{B} \in V(\mathbf{A})$ be a finite subdirectly irreducible algebra with monolith β. If β is not Abelian, then by Corollary 4.7, $\mathbf{B} \in HSP_U(\mathbf{A})$. Since $\mathbf{A}$ is finite, $P_U(\mathbf{A}) \subseteq I(\mathbf{A})$ by Lemma 0.33 so $\mathbf{B} \in HS(\mathbf{A})$, hence $|B| \leq |A| = m \leq (l+1)!m$, so $\mathbf{B}$ is bounded as in (ii). We may therefore assume that β is Abelian. Let $\gamma = (id_B : \beta)$, the centralizer of β. By Theorem 4.6, $\mathbf{B}/\gamma \in HSP_U(\mathbf{A})$ so $\mathbf{B}/\gamma \in HS(\mathbf{A})$ (as above).

By Corollary 4.7, $\gamma \neq id_B$. In $\mathbf{Con}(\mathbf{B})$ if $[\gamma, \gamma] \neq id_B$, then $[\gamma, \gamma] \supseteq \beta$, the monolith of $\mathbf{B}$. Since γ is the centralizer of β, $[\beta, \gamma] = id_B \neq \beta$.

Now $\mathbf{B}$ is a finite algebra in $V(\mathbf{A})$ that fails to satisfy (C1), a contradiction. Thus in $\mathbf{Con}(\mathbf{B}), [\gamma, \gamma] = id_B$ so γ is an Abelian congruence with, say, q congruence classes, where $1 \leq q \leq m$. Now $(id_B : \gamma)$ is the largest congruence α in $\mathbf{Con}(\mathbf{B})$ such that $[\gamma, \alpha] \subseteq id_B$. Now $[\gamma, \gamma] = id_B$ so $\gamma \subseteq \alpha = (id_B : \gamma)$.

We have $q = |B/\gamma|$ and since $\mathbf{B}/\gamma \in HS(\mathbf{A})$, $|B/\gamma| \leq |A|$, i.e., $q \leq m$. Let $B/\gamma = \{z_1/\gamma, \dots, z_q/\gamma\}$. Let d be a difference term for $V(\mathbf{A})$.

For any $(b, e) \in \beta/id_B$, we have $id_B \neq \Theta^{\mathbf{B}}(b, e) \subseteq \beta$, so $\beta = \Theta^{\mathbf{B}}(b, e)$. Since $\beta \subseteq \gamma$, b and e belong to the same congruence class of γ, say $b, e \in z_j/\gamma$, where $j \in \{1, \dots, q\}$. Let $a = d^{\mathbf{B}}(b, e, z_j)$. Then $a \in z_j/\gamma$ also.

By Corollary 3.14, since γ is Abelian, $\langle z_j/\gamma; d\rangle = \mathbf{M}(\gamma, z_j)$ is a ternary group. Let $\mathbf{G}_j = \langle z_j/\gamma; +, -, z_j\rangle$ be its associated Abelian group with z_j as its identity element, so $d^{\mathbf{B}}(u, v, w) = u - v + w$ for all $u, v, w \in z_j/\gamma$.

Since $b \neq e$, we have $z_j \neq b - e = b - e + z_j = d^{\mathbf{B}}(b, e, z_j) = a$, but since $(b, e) \in \beta$, we also have $a\beta d^{\mathbf{B}}(e, e, z_j) = z_j$, so $id_B \neq \Theta^{\mathbf{B}}(z_j, a) \subseteq \beta$, whence $\beta = \Theta^{\mathbf{B}}(z_j, a)$.

We are going to show that $|z_i/\gamma| \leq (l+1)!$ for $i = 1, \ldots, q$. It will then follow that $|B| \leq (l+1)!q \leq (l+1)!m$, as required.

To this end, let $z_i \neq c \in z_i/\gamma$ where $i \in \{1, \ldots, q\}$. Since $V(\mathbf{A})$ is modular and γ is Abelian and $\{(z_i, c)\} \subseteq \gamma$, it follows from Lemma 3.16 that $\Theta^{\mathbf{B}}(z_i, a) = \sigma^{\mathbf{B}}(z_i, c)$ (the semicongruence of $\mathbf{B}$ generated by $\{(z_i, c)\}$).

Now $\beta \subseteq \Theta^{\mathbf{B}}(z_i, c)$ (since $z_i \neq c$), i.e., $(z_j, a) \in \sigma^{\mathbf{B}}(z_i, c)$. By Lemma 0.38, there is a unary polynomial g of $\mathbf{B}$ such that $g(z_i) = z_j$ and $g(c) = a$. Thus, $h := g|_{z_i/\gamma} \in Hom(\gamma, z_i, z_j)$, by Lemma 3.18. Then by the remarks preceding Lemma 3.18, h is a homomorphism between the Abelian groups $\mathbf{G}_i$ and $\mathbf{G}_j$, and $h(c) = a$. Let $k = |Hom(\gamma, z_i, z_j)|$. Then $k \leq m^{(m^{m+1})} = l$, by Corollary 0.51.

To summarize: $\mathbf{G}_i = \langle z_i/\gamma; +, -, z_i\rangle$ and $\mathbf{G}_j = \langle z_j/\gamma; +, -, z_j\rangle$ are finite Abelian groups and $z_j \neq a \in G_j$ and there is a set S of homomorpisms from $\mathbf{G}_i$ to $\mathbf{G}_j$ with $0 < |S| = k \leq l$ such that whenever $z_i \neq c \in G_i$, there exists $h \in S$ with $h(c) = a$. It remains only to show that $|G_i| \leq (l+1)!$. This will be true if $|G_i| \leq (k+1)!$. It therefore suffices to prove the following group theoretic result:

Claim: Let $0 < k \in \omega$. If $\mathbf{K}$ and $\mathbf{L}$ are finite Abelian groups and $0 \neq a \in L$ and there are k homomorphisms $r_1, \ldots, r_k \in Hom(\mathbf{K}, \mathbf{L})$ such that for each nonzero $c \in K$ there exists $i \in \{1, \ldots, k\}$ with $r_i(c) = a$, then $|K| \leq (k+1)!$.

We prove the claim by induction on k.

Let $k = 1$ and assume the hypotheses of the claim. Then there is one homomorphism, $r_1 \in Hom(\mathbf{K}, \mathbf{L})$, such that for each nonzero $c \in K$, $r_1(c) = a$. Suppose $|K| > 2$. Then K contains at least 2 nonzero elements. Let $c_1, c_2 \in K$ such that $c_1, c_2 \neq 0$, and $c_1 \neq c_2$. Then $r_1(c_1) = a = r_1(c_2)$.

Now $c_1 - c_2 \neq 0$ so $r_1(c_1 - c_2) = a$, i.e., $r_1(c_1) - r_1(c_2) = a$ (because r_1 is a homomorphism) but $r_1(c_1) - r_1(c_2) = 0$, implying $a = 0$, a contradiction. Thus $|K| \leq 2 = 2!$ and the claim is true for $k = 1$.

Assume that the claim is true for $k - 1$ (where $k \geq 2$). We show it is true for k. Again, assume the hypotheses of the claim. For each $i \in \{1, \ldots, k\}$, let $X_i = \{c \in K : c \neq 0 \text{ and } r_i(c) = a\}$. By assumption, $K \setminus \{0\} = \cup_{i=1}^{k} X_i$. Let $t = max\{|X_i| : i \in \{1, \ldots, k\}\}$ and choose $i \in \{1, \ldots, k\}$ such that $|X_i| = t$, say $X_i = \{c_1, \ldots, c_t\}$. Then $|X_j| \leq t$ for $i \neq j \in \{1, \ldots, k\}$ so $|K \setminus \{0\}| \leq k.t$, therefore $|K| \leq 1 + k.t$. .... (1)

Let $K_1 = 0/ker(r_1) = \{d \in K : r_1(d) = 0\}$. For $j \in \{1, \ldots, t\}$, we have $r_1(c_1) = a = r_1(c_j)$, so $r_1(c_1 - c_j) = 0$, therefore $c_1 - c_j \in K_1$. Therefore $|K_1| \geq t$ and so (1) gives $|K| \leq 1 + k.|K_1|$.

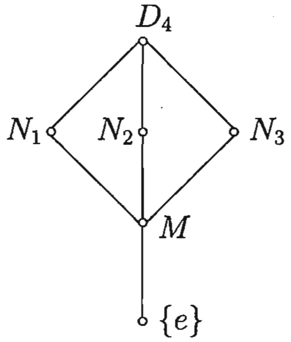
Now r_1 maps the elements of K_1 to $0 \neq a$ so for each nonzero c in K_1 there is an $i \in \{2, \dots, k\}$ such that $r_i(c) = a$.

Now K_1 is the universe of a subgroup $\mathbf{K}_1$ of $\mathbf{K}$. By the induction hypothesis, applied to $\mathbf{K}_1, \mathbf{L}, a$ and $r_2, \dots, r_k$, we deduce that $|K_1| \leq k!$. Thus $|K| \leq 1 + k.k! \leq k! + k.k! = (k+1).k! = (k+1)!$, as required. □

Example 4.12.

Theorem 4.11 (or Theorem 4.10) can be used to explain why the variety $V(\mathbf{D}_4)$ generated by the dihedral group $\mathbf{D}_4$ is not residually small.

Recall that $\mathbf{D}_4 = \langle D_4; \cdot, ^{-1}, e\rangle$ is the 8-element 2-generated (non-Abelian) group with $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\} = Sg^{\mathbf{D}_4}(\{a, b\})$, $a^4 = b^2 = e$ and $ba = a^{-1}b (= a^3b)$. By Example 2.4, $V(\mathbf{D}_4)$ is modular. The centre $e/\tau_{\mathbf{D}_4}$ of $\mathbf{D}_4$ is $M = \{e, a^2\}$. The normal subgroup lattice of $\mathbf{D}_4$ is



where

$$\begin{aligned} N_1 &= Sg^{\mathbf{D}_4}(\{a\}) = \{e, a, a^2, a^3\} \\ N_2 &= Sg^{\mathbf{D}_4}(\{a^2, b\}) = \{e, a^2, b, a^2b\} \\ N_3 &= Sg^{\mathbf{D}_4}(\{a^2, ab\}) = \{e, a^2, ab, a^3b\}. \end{aligned}$$

Recall (Lemma 3.2) that $[\tau_{\mathbf{D}_4}, D_4^2] = id_{D_4}$, i.e., $[M, D_4] = \{e\}$. Recall also (see 2.5.1 (5)) that $[D_4, D_4]$ is the smallest normal subgroup N of $\mathbf{D}_4$ such that $\mathbf{D}_4/N$ is Abelian. Since $|D_4/M| = 4$, $\mathbf{D}_4/M$ is an Abelian group (in fact $\mathbf{D}_4/M \cong \mathbb{Z}_2 \times \mathbb{Z}_2$), while $\mathbf{D}_4/\{e\} \cong \mathbf{D}_4$ is not Abelian (e.g., $ba = a^3b \neq ab$). Thus, $[D_4, D_4] = M$. Now we have

$$M \subseteq [D_4, D_4] \text{ but } M \supset [M, D_4]$$

so $\mathbf{Con}(\mathbf{D}_4) \not\models (C1)$. Since $\mathbf{D}_4$ is finite, it follows from Theorem 4.11 ((i)$\Rightarrow$(iii)) (or from Theorem 4.10) that $V(\mathbf{D}_4)$ is not residually small.

This shows that Jónsson's Theorem can fail for modular varieties: by the above, $V(\mathbf{D}_4)_{SI}$ has infinite members, but by Lemma 0.33, $HSP_U(\mathbf{D}_4) = HS(\mathbf{D}_4)$ contains only finite groups, so $V(\mathbf{D}_4)_{SI} \not\subseteq HSP_U(\mathbf{D}_4)$.

Theorem 4.11 shows that in *modular* varieties, the RS Conjecture is true. Subsequent progress on the RS Conjecture (for nonmodular varieties) is discussed in the conclusion.

For a finite algebra $\mathbf{A}$ of finite type such that $V(\mathbf{A})$ is modular, it is obviously possible to check mechanically, in finite time, whether condition (iii) of Theorem 4.11 is true of $\mathbf{A}$. Thus, there is an *algorithm* to decide, given such an $\mathbf{A}$, whether $V(\mathbf{A})$ is residually small. (See the conclusion for the nonmodular case.)

For $2 \leq m \in \omega$, let $f(m)$ be the least $n \in \omega$ such that for any algebra $\mathbf{A}$ with $2 \leq |A| \leq m$, if $V(\mathbf{A})$ is modular and residually small then $V(\mathbf{A})$ is residually $< n$. Theorem 4.11 shows that $f(m) \leq 1 + ((m^{(m^{m+1})} + 1)!m)$. No "best possible" upper bound for $f(m)$ is known but, according to [Kis97], it is known that such a bound must be an at-least-exponential function of m.

Conclusion

Let $\mathbf{A}$ be a finite algebra of type $\mathcal{T} = \langle \mathsf{F}, ar \rangle$ such that $V(\mathbf{A})$ is residually small. The *residual spectrum* $RSp(\mathbf{A})$ of $\mathbf{A}$ is the set $\{|B| : \mathbf{B} \in V(\mathbf{A})_{SI}\}$; recall that the *residual bound* $\kappa(\mathbf{A})$ of $\mathbf{A}$ (or of $V(\mathbf{A})$) is the smallest cardinal strictly greater than all elements of $RSp(\mathbf{A})$.

By Theorem 1.22 (v), $\kappa(\mathbf{A}) \leq (2^{\mathsf{n}})^+$ where $\mathsf{n} = \aleph_0 + |\mathsf{F}|$. Since $|A|$ is finite, however, it can have only countably many truly different operations so we may assume here that $|\mathsf{F}| \leq \aleph_0$, hence $\kappa(\mathbf{A}) \leq (2^{\aleph_0})^+$. Since trivial algebras are subdirectly reducible, $\kappa(\mathbf{A}) \geq 3$. More strongly, it has been known for a long time that

$$\kappa(\mathbf{A}) \in \{3, 4, \ldots, \aleph_0, \aleph_1, (2^{\aleph_0})^+\}$$

(see [MS74]). R. Quackenbush's Theorem (Proposition 1.26) implies that $\kappa(\mathbf{A}) < \aleph_0$ whenever the *finite* cardinals in $RSp(\mathbf{A})$ have a *finite* upper bound. Quackenbush's Conjecture [Qua71] is the claim that $\kappa(\mathbf{A}) \neq \aleph_0$ (i.e. if $V(\mathbf{A})_{SI}$ includes arbitrarily large finite algebras then it includes an infinite algebra). In its original form this conjecture assumed not only that $|A|$ is finite but that it also has finite type, i.e. that $|\mathsf{F}| < \aleph_0$. In this form, the problem remains open. The RS Conjecture is the stronger claim that $\kappa(\mathbf{A}) < \aleph_0$ (assuming still that $|A|$ is finite and $V(\mathbf{A})$ is residually small but not that $\mathbf{A}$ has finite type).

The final theorem presented in this thesis (Theorem 4.11) shows that the RS Conjecture is true whenever $V(\mathbf{A})$ is congruence modular. Most naturally occurring varieties are modular, so this result of R. Freese and R. McKenzie [FM81] is widely applicable. The conjecture is also true if $\mathbf{A}$ is a semigroup (in which case $V(\mathbf{A})$ need not be modular) [McK81] [GS82]. D. Hobby and McKenzie invented "tame congruence theory" (see [HM88]) largely with a view to resolving the RS Conjecture in general and proved the conjecture in the case where the members of $V(\mathbf{A})$ "omit types **1** and **5**". We shall not define this condition here, but the result implies that the conjecture is true whenever there is a nontrivial lattice identity $s \approx t$ (i.e. an identity $s \approx t$ in the language $\{\wedge, \vee\}$ that fails in at least one lattice) such that the congruence lattices of all algebras in $V(\mathbf{A})$ satisfy $s \approx t$. However, the proof strategy consists of showing that every locally finite residually small variety with this property is congruence modular, and then invoking Theorem 4.11. Rather than eclipsing Theorem 4.11, therefore, this result demonstrates the breadth of its application. A summary of further positive results that use this strategy appears in [Wil97, 1.4]. Going strictly beyond the modular case, the RS Conjecture has recently been proved in the case where all algebras in $V(\mathbf{A})$ are Abelian [KKV99].

By the early 1990's this body of positive results had led to a belief among researchers that the RS Conjecture, in its most general form, should be true. In [McK], McKenzie wrote that "a counterexample, if it exists, must be a ridiculously unorthodox algebra". By the mid-1990s, however, he had constructed just such an algebra [McK96a] and had, in the process, developed new techniques that enabled him to resolve two further longstanding problems [McK96b], [McK96c]. These three papers constitute a major advance for the general theory of algebras. The featured joint review of them by J. Berman [Ber97] is a helpful guide to the material.

In [McK96a], McKenzie showed that for each cardinal $\mathsf{m} \in \{3, 4, \ldots, \aleph_0, \aleph_1, (2^{\aleph_0})^+\}$ there is a 4-element algebra $\mathbf{A}_\mathsf{m}$ with $\kappa(\mathbf{A}_\mathsf{m}) = \mathsf{m}$. For the finite cardinals m, $\mathbf{A}_\mathsf{m}$ has finite type, but this is not true for the last three (infinite) values of m. This already (and unexpectedly) refuted the RS Conjecture. In the same paper, McKenzie also showed that there is an 8-element algebra $\mathbf{A}$ of *finite type* such that $\kappa(\mathbf{A}) = \aleph_1$. According to [McK96a], C. Latting (unpublished) showed that $(2^{\aleph_0})^+$ is also the residual bound of a finite algebra of finite type. It remains an open question, however, whether $\aleph_0$ is the residual bound of a finite algebra of finite type: this was the original Quackenbush problem. McKenzie also proved that there is no algorithm which decides, given a finite algebra $\mathbf{A}$ of finite type, whether $V(\mathbf{A})$ has a finite residual bound, and that the same is true if we replace "has a finite residual bound" by "is residually finite" [McK96b]. He subsequently proved the same result for the property "residually small"; in the meantime, Latting had dealt likewise with "residually countable" i.e. with "$\kappa(\mathbf{A}) \leq \aleph_1$". (Here we are quoting from [Ber97] and [McK96b]).)

The RS Conjecture aside, in the last two decades a number of other important results concerning residually small varieties have been proved for which space has not been found in the body of the thesis.

McKenzie [McK82] showed that a variety V of rings (or of linear associative algebras over a commutative ring) is residually small exactly when the congruence lattices of its algebras satisfy (C1); the assumption that V be finitely generated is not required in this case.

It is known that injections are transferable in a variety V if and only if V has the congruence extension property (CEP) and the "amalgamation property" (AP): see [Bac72], [Tay72]. We proved part of this in Proposition 1.41 but did not discuss the AP. A variety has the AP if and only if for any embeddings $\mathbf{A} \xrightarrow{f} \mathbf{B} \in V$ and $\mathbf{A} \xrightarrow{g} \mathbf{C} \in V$ there exist $\mathbf{D} \in V$ and embeddings $\mathbf{B} \xrightarrow{h} \mathbf{D}$ and $\mathbf{C} \xrightarrow{k} \mathbf{D}$ such that $h \circ f = k \circ g$. Using commutator theory and extending earlier results of E. Kiss [Kis85] and of C. Bergman and McKenzie [BM88],

K. Kearnes [Kea89] proved that any residually small modular variety with the AP also has the CEP; it therefore has enough injectives (by Theorem 1.44).

S. Burris and McKenzie [BM81a], [BM81b] used the commutator theory to obtain structural characterizations of locally finite modular varieties with a decidable first order theory. Using tame congruence theory, McKenzie and M. Valeriote [MV89] extended this work to the nonmodular case.

McKenzie proved [McK87] that every finitely generated residually small modular variety V is finitely axiomatized by identities. One cannot drop from this result the assumption that V be residually small, in view of an example of S. Polin [Pol76] (in which V consists of nonassociative rings). Recall that finitely generated congruence distributive varieties always have finite residual bounds, by Jónsson's Theorem. The fact that these varieties are finitely axiomatized was discovered (before 1970) by K. Baker [Bak77]. In contrast, [McK96c] shows that there is no algorithm to decide, given an arbitrary finite algebra $\mathbf{A}$ of finite type, whether $V(\mathbf{A})$ is finitely axiomatized.

Kearnes and McKenzie [KM92] extended commutator theory from varieties to the class of "relatively modular" quasivarieties. The *varieties* in this class are modular and the definitions specialize in them to the ones discussed in this thesis. Certain varietal results (e.g. C. Herrmann's Fundamental Theorem of Abelian Algebras) fail to generalize to this framework, however, and others are open problems. The building blocks (in terms of subdirect decomposition) of a quasivariety K are its "relatively subdirectly irreducible" algebras; if K is finitely generated, i.e., if $K = ISP(\mathbf{A})$ for some finite algebra $\mathbf{A}$, then the sizes of these building blocks are always bounded above by $|A|$. Thus the analogue of the RS Conjecture does not arise for quasivarieties. It is an open problem, however, whether a finitely generated relatively modular quasivariety is necessarily finitely axiomatized by quasi-identities. (This becomes true if we strengthen "relatively modular" to "relatively distributive" [Pi88].) For some quasivarieties, this question is connected, in a currently mysterious way, to the theory of residually small *varieties*: for a finite group or (associative) ring $\mathbf{A}$, the quasivariety $ISP(\mathbf{A})$ generated by $\mathbf{A}$ is finitely axiomatized if and only if the variety $V(\mathbf{A})$ is residually small (see [Ol's74] for groups and [Bel78] for rings). In this case $V(\mathbf{A})$, being modular, has a finite residual bound, by Theorem 4.11. For a finite group $\mathbf{A}$, $V(\mathbf{A})$ is residually small if and only if all Sylow subgroups of $\mathbf{A}$ are Abelian [Ol's69] (also see [FM81]). At a universal algebraic level, no general argument exists at present that would explain these phenomena.

Bibliography

[Bac72] P.D. Bacsich, *Injectivity in model theory*, Colloq. Math. **25** (1972), 165-176.

[Bak77] K. Baker, *Finite equational bases for finite algebras in congruence distributive equational classes*, Advances in Mathematics **24** (1977), 207-243.

[BB75] J.T. Baldwin, J. Berman, *The number of subdirectly irreducible algebras in a variety*, Algebra Universalis **5** (1975), 379-389.

[Ban70] B. Banaschewski, *Injectivity and essential extensions in equational classes of algebras*, Proceedings of the Conference on Universal Algebra, Oct. 1969, Queen's University, Kingston, 1970, pp131-147.

[BN72] B. Banaschewski, E. Nelson, *Equational compactness in equational classes of algebras*, Algebra Universalis **2** (1972), 152-165.

[Bel78] V. P. Belkin, *Quasi-identities of finite rings and lattices*, Algebra i Logika **17** (1978), 247-259.

[BM88] C. Bergman, R. McKenzie, *On the relationship of AP, RS and CEP in congruence modular varieties, II*, Proc. Amer. Math. Soc. **103** (2) (1988), 335-342.

[Ber97] J. Berman (reviewer), Mathematical Reviews **97e** : 08002a,b,c.

[Bir44] G. Birkhoff, *Subdirect unions in universal algebra*, Bull. Amer. Math. Soc. **50** (1944), 764-768 .

[BM81a] S. Burris, R. McKenzie, *Decidable varieties with modular congruence lattices*, Bull. Amer. Math. Soc. **4** (1981), 350-352.

[BM81b] S. Burris, R. McKenzie, *Decidability and Boolean representations*, Mem. Amer. Math. Soc. **246** (1981).

[BS81] S. Burris, H.P. Sankappanavar, "A Course in Universal Algebra", Graduate Texts in Mathematics, Springer-Verlag, New York, 1981.

[Day69] A. Day, *A characterization of modularity for congruence lattices of algebras*, Canad. Math. Bull. **12** (1969), 167-173.

[Day71] A. Day, *A note on the congruence extension property*, Algebra Universalis **1** (1971), 234-235.

[DK87] A. Day, E. Kiss, *Frames and rings in congruence congruence modular varieties*, J. Algebra **109** (1987), 475-507.

[Dud83a] J Duda, *Mal'cev conditions for regular and weakly regular subalgebras of the square*, Acta. Sci. Math. (Szeged) **51** (1983), 33-35.

[Dud83b] J Duda, *On two schemes applied to Mal'cev type theorems*, Annales Universitatis Scientarium Budapestiesis. Sectio Mathematica **26** (1983), 39-45.

[ER56] P. Erdös, R. Rado, *A partition calculus in set theory*, Bull. Amer. Math. Soc. **62** (1956), 427-489.

[FM81] R. Freese, R. McKenzie, *Residually small varieties with modular congruence lattices*, Trans. Amer. Math. Soc. **264** (1981), 419-430.

[FM87] R. Freese, R. McKenzie, "Commutator Theory for Congruence Modular Varieties", London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge, 1987.

[FN42] N. Funayama, T. Nakayama, *On the distributivity of a lattice of lattice congruences*, Proc. Imp. Acad. Tokyo **18** (1942), 553-554.

[GS82] A.E. Golubov, M.V. Sapir, *Varieties of finitely approximable semigroups*, Izv. Vysš. Učebn. Zaved Matematika **11** (1982), 21-29; see also Soviet Math. Dokl. **20** (4) (1979), 828-832.

[Grä79] G. Grätzer, "Universal Algebra", 2nd ed., Springer-Verlag, New York, 1979.

[GL71] G. Grätzer, H. Lakser, *The structure of pseudocomplemented distributive lattices, II. Congruence extension and amalgamation*, Trans. Amer. Math. Soc. **156** (1971), 353-356.

[Gum78] H.-P. Gumm, *Über die Losungermenge von Gleichungsystemen über allgemeinen Algebren*, Math. Z. **162** (1978), 51-62.

[Gum79] H.-P. Gumm, *Algebras in permutable varieties: geometric properties of affine algebras*, Algebra Universalis **9** (1979), 8-34.

[Gum80a] H.-P. Gumm, *An easy way to the commutator in modular varieties*, Arch. Math. **34** (1980), 220-228.

[Gum80b] H.-P. Gumm, *The little Desarguesian theorem for algebras in modular varieties*, Proc. Amer. Math. Soc. **80** (1980), 393-397.

[Gum83] H.-P. Gumm, *Geometric methods in congruence modular varieties*, Mem. Amer. Math. Soc. **45** (1983), No. 286.

[HH79] J. Hagemann, C. Herrmann, *A concrete ideal multiplication for algebraic systems and its relation to congruence-distributivity*, Arch. Math. **32** (1979), 234-245.

[Her79] C. Herrmann, *Affine algebras in congruence modular varieties*, Acta. Sci. Math. (Szeged) **41** (1979), 119-125.

[Hig71] D. Higgs, *Remarks on residually small varieties*, Algebra Universalis **1** (1971/72), 383-385.

[HM88] D. Hobby, R. McKenzie, "The structure of finite algebras", Contemporary Mathematics 76, American Mathematical Society, Providence, 1988.

[Hod97] W. Hodges, "A Shorter Model Theory", Cambridge University Press, Cambridge, 1997.

[Jón67] B. Jónsson, *Algebras whose congruence lattices are distributive*, Math. Scandinavica **21** (1967), 110–121.

[Kea89] K. Kearnes, *The relationship between AP, RS and CEP*, Proc. Amer. Math. Soc. **105** (1989), 827-839.

[KKV99] K. Kearnes, E.W. Kiss, M. Valeriote, *A geometric consequence of residual smallness*, Annals of Pure and Applied Logic **99** (1999), 137-169.

[KM92] K. Kearnes, R. McKenzie, *Commutator theory for relatively modular quasivarieties*, Trans. Amer. Math. Soc. **331** (1992), 465-502.

[Kis85] E.W. Kiss, *Injectivity and related concepts in modular varieties, I. Two commutator properties, II. The congruence extension property*, Bull. Australian Math. Soc. **32** (1985), 33-44 and 44-55.

[Kis97] E.W. Kiss, *An introduction to tame congruence theory*, in "Algebraic Model Theory", B.T. Hart et al. (eds.), Kluwer Academic Publishers, 1997, pp119-143.

[KMPT83] E. W. Kiss, L. Màrki, P. Pröhle, W. Tholen, *Categorical algebraic properties. A compendium on amalgamation, congruence extension, epimorphisms, residual smallness and injectivity*, Studia Scientiarium Mathematicarum Hungarica **18** (1983), 79-141.

[Lam66] J. Lambek, "Lectures on Rings and Modules", Blaisdell Publishing Co., Waltham, Mass., 1966.

[Mal54] A.I. Mal'cev, *On the general theory of algebraic systems (Russian)*, Mat. Sb. **77** (**35**) (1954), 3-20.

[McK81] R. McKenzie, *Residually small varieties of semigroups*, Algebra Universalis **13** (1981), 171-201.

[McK82] R. McKenzie, *Residually small varieties of K-rings*, Algebra Universalis **14** (1982), 181-196.

[McK87] R. McKenzie, *Finite equational bases for congruence modular varieties*, Algebra Universalis **24** (1) (1987), 224-250.

[McK] R. McKenzie, *Some interactions between group theory and the general theory of algebras*, Manuscript, c. 1991.

[McK96a] R. McKenzie, *The residual bounds of finite algebras*, Internat. J. Algebra Comput. **6** (1) (1996), 1-28.

[McK96b] R. McKenzie, *The residual bound of a finite algebra is not computable*, Internat. J. Algebra Comput. **6** (1) (1996), 29-48.

[McK96c] R. McKenzie, *Tarski's finite basis problem is undecidable*, Internat. J. Algebra Comput. **6** (1) (1996), 49-104.

[MS74] R. McKenzie, S. Shelah, *The cardinals of simple models for universal theories*, Proceedings of the Tarski Symposium, Volume 25 of Symposia in Pure Mathematics, Amererican Mathematical Society, Providence, 1974, pp53-74.

[MV89] R. McKenzie, M. Valeriote, "The structure of decidable locally finite varieties", Progress in Math. 79, Birkhauser, Boston, 1989.

[Men87] E. Mendelson, "Introduction to Mathematical Logic", third edition, Wadsworth and Brooks/Cole, Monterey, California, 1987.

[Ol's69] A.Yu. Ol'shanskii, *Varieties of finitely approximable groups*, Izv. Akad. Nauk SSSR Ser. Mat. **33** (4) (1969), 915-927.

[Ol's74] A.Yu. Ol'shanskii, *Conditional identities in finite groups*, Siber. Math. **15** (1974), 1000-1003.

[OS66] F. Ostermann, J. Schmidt, *Der baryzentrische Kalkül als axiomatische Grundlage der affinen Geometrie*, J. Reine Math. **224** (1966), 44-57.

[Pi88] D. Pigozzi, *Finite basis theorems for relatively congruence distributive quasivarieties*, Trans. Amer. Math. Soc. **310** (1988), 499–533.

[Pol76] S. V. Polin, *The identities of finite algebras*, Siberian Math. J. **17** (1976), 1356-1366.

[Qua71] R. Quackenbush, *Equational classes generated by finite algebras*, Algebra Universalis, **1** (1971), 265-266.

[Smi76] J.D.H. Smith, "Mal'cev Varieties", Lecture Notes in Math., 554, Springer-Verlag, Berlin, 1976.

[Tay72] W. Taylor, *Residually small varieties*, Algebra Universalis **2**, (1972), 33-53.

[Tay82] W. Taylor, *Some applications of the term conditions*, Algebra Universalis **14**, (1982), 11-24.

[Wil97] R. Willard, *Three lectures on the RS problem*, in "Algebraic Model Theory", B.T. Hart et al. (eds.), Kluwer Academic Publishers, 1997, pp231-254.

Index

List of Symbols

$\mathcal{P}(A)$	3
$\lvert A\rvert$	3
$A \setminus B$	3
B^A	3
$f[A], f^{-1}[A]$	3
ω	3
$\aleph_0$	3
m, m^+	4
$\sim$	4
$\overset{\sim}{\equiv}$, $\sim\rvert_B$, $\sim_B$	4
$\langle P; \leq \rangle$	4
$\bigvee_\mathbf{P}$, $\bigwedge_\mathbf{P}$	4
$a \vee b$, $a \wedge b$	4
$a < b$, $a \prec b$	4
$\cong$	5
$int(x, y)$	5
$\searrow$, $\nearrow$	5
$\theta \circ \varphi$	7
$Eq(A)$	7
id_A	8
ar	8
$\mathcal{T}$	8
F	8
$\langle \mathsf{F}, ar \rangle$	8
$\mathbf{A}$, $\langle A; F \rangle$	8
$f^\mathbf{A}$	8
$Sg^\mathbf{A}(X)$	9
$Sub(A)$	9
a/θ, $\mathbf{A}/\theta$	10
$Con(\mathbf{A})$	10
$\Theta^\mathbf{A}(X)$, $\Theta^\mathbf{A}(a, b)$	10
$\theta\rvert_\mathbf{B}$	11
$Hom(\mathbf{A}, \mathbf{B})$	11
$ker(h)$	12
φ/θ	12
$\prod_{i \in I} \mathbf{A}_i$	13
I, H, S, P, P_S	15
$V(K)$	15
$\mathcal{F}$	17
$[[a = b]]$	17
P_U	18
$\mathsf{F}[\mathbf{A}], \mathcal{T}[\mathbf{A}]$	19
$T(X)$	19
$t(x_1, \ldots, x_n)$	19
$Sc(\mathbf{A})$, $\sigma^\mathbf{A}(X)$	21
$\Phi(x_1, \ldots, x_n)$, $\Phi[t_1, \ldots, t_n]$	22
$\models$, $\vdash$	22
$D(\mathbf{A})$	22
$\bar{\Phi}$	22
$\Sigma \vdash_{Th(\mathcal{T})}$	22
$\bar{x}$, $\bar{X}$	26
$\mathbf{F}_K(\bar{X})$	26
$\aleph_1$	43
$M(\alpha, \beta)$	73
$C(\alpha, \beta; \delta)$, $C(\alpha, \beta)$	73
$[\alpha, \beta]$	73
$[\theta, \varphi]_\pi$	84
$\mathbf{A}(\theta)$	88
$\Delta_{\theta,\varphi}$, $\Delta^{\theta,\varphi}$	89
$\tau_\mathbf{A}$	108
$Pol_n(\mathbf{A})$, $Pol(\mathbf{A})$	112
$M(\beta, u)$	122
$Hom(\beta, z, z')$	125
(C1)	128
$(\delta : \beta)$, $(id_A : \beta)$	135