# Congruence modular varieties: commutator theory and its uses

Ralph McKenzie and John Snow

*Department of Mathematics*
*Vanderbilt University*
*Nashville, Tennessee 37240*

*Department of Mathematics*
*Concordia University*
*Seward, Nebraska 68434*

November, 2003

**Abstract**

We present the basic theory of commutators of congruences in congruence modular varieties (or equationally defined classes) of algebras. The theory we present was first introduced to the mathematical world in a 1976 monograph of J.D.H. Smith, devoted to varieties with permuting congruences. It was extended to congruence modular varieties in a 1979 paper by J. Hagemann and C. Herrmann, and has since been elaborated into an impressive machinery for attacking diverse problems in the domain of congruence modular varieties. Three notable applications of this commutator theory are presented in detail, and others are described.

**Contents:**

# 1 Introduction

The commutator in group theory is a natural operation defined on the lattice of normal subgroups of any group which plays a basic role in the definition and study of solvable and Abelian groups. This commutator has a companion operation in the theory of rings, defined on any lattice of ideals. These two operations share many common properties, including the ability to capture the notion of Abelian-ness.

In [43], J.D.H. Smith used category theory to extend structural properties of groups and rings to varieties with permuting congruences. In doing so, he laid the framework for generalizing the commutator from groups and rings to an operation on the congruence lattices of algebras in congruence permutable varieties.

J. Hagemann and C. Herrmann in [19] extended some of Smith's results to congruence modular varieties. Their techniques include subtle and difficult calculations in $\mathrm{Con}\,\mathbf{A}$, $\mathrm{Con}\,\mathbf{A}^2$, and $\mathrm{Con}\,\mathbf{A}^3$ using modular arithmetic. In their work, they mentioned the term condition which would later become the basis for what seems to be the most useful definition of the commutator in congruence modular varieties. H.-P. Gumm [17] further extended these structural results for congruence modular varieties by viewing the structure imposed on algebras by congruence relations geometrically. R. Freese and R. McKenzie [12] developed the commutator for congruence modular varieties based on the term condition mentioned by Hagemann and Herrmann.

In this manuscript, we give a gentle introduction to the commutator theory presented in [12]. We then present several applications of the commutator along with some open problems which may involve commutator theory. In Section 2 we review the classical commutator in groups and demonstrate how the term condition arises naturally in this environment. In Section 3 we lay out some basic notation which will be pervasive throughout the manuscript. In Section 4 we use the notion of centrality to define the commutator and prove a few properties of the commutator which hold in any environment. In Section 5 we give examples of the commutator in some familiar environments including rings, lattices, and modules. In Section 6 we give the classical Maltsev type characterizations of congruence permutability, distributivity, and modularity due to Maltsev, Jónsson, and Day. These characterizations are exploited heavily in the development of commutator theory for congruence modular varieties. In Section 7 we use Jónsson's characterization of congruence distributivity to prove that in a congruence distributive variety the commutator is nothing other than congruence intersection. In Section 8 we extend all of the properties of the group commutator mentioned in Section 2 to the commutator in congruence modular varieties. In Section 9 we prove the Fundamental Theorem of Abelian Algebras that every Abelian algebra (in a congruence modular variety) is affine (polynomially equivalent to a module). In Section 10 we extend the ideas of solvability and nilpotence using the commutator. We prove that every nilpotent or solvable algebra in a congruence modular variety has a Maltsev term and use this to give some structural results about nilpotent algebras. In Section 11 on applications, we briefly discuss seven outstanding instances of basic problems that have been solved, for modular varieties, with the aid of commutator theory. In the following sections, we present three of these applications in detail: In Section 12 we prove that every finitely generated, residually small, congruence modular variety has a finite residual bound, and that such varieties are characterized by a commutator equation. In Section 13 we characterize directly representable varieties—i.e., those finitely generated varieties that possess only a finite number of non-isomorphic finite,

directly indecomposable, algebras—and we characterize the larger family of finitely generated varieties whose spectrum is contained in a finitely generated monoid of positive integers. All of these varieties are shown to be congruence modular. In Section 14 we characterize the locally finite congruence modular varieties for which the function giving the number of non-isomorphic $n$-generated algebras is dominated by a polynomial in $n$. They are precisely the directly representable Abelian varieties. In Section 15 we survey some problems which either involve the commutator or for which there is evidence that the commutator might prove useful. We note that the results herein are not original. Excepting the results of Sections 13–14, almost all of them appear with proofs in [12].

## 2 The Commutator in Groups

In this section, we discuss the group commutator and some of its most basic properties, and we illustrate how the term condition arises naturally in this environment.

**Definition 2.1** *Suppose that* $\mathbf{G}$ *is a group and* $M$ *and* $N$ *are normal subgroups of* $\mathbf{G}$*. The group commutator of* $M$ *and* $N$ *is defined as*

$$[M, N] = \mathrm{Sg}_{\mathrm{G}}(\{m^{-1}n^{-1}mn : m \in M \text{ and } n \in N\}), \tag{2.1}$$

Suppose that $\mathbf{G}$ is a group, that $M$, $N$, and $\{N_i : i \in I\}$ are normal subgroups of $\mathbf{G}$, and that $f : \mathbf{G} \to \mathbf{H}$ is a surjective group homomorphism. Then the following properties of the group commutator are easy exercises in any first class on group theory.

(1) $[M, N] \subseteq M \cap N$.

(2) $f([M, N]) = [f(M), f(N)]$.

(3) $[M, N] = [N, M]$.

(4) $[M, \bigvee_{i\in I} N_i] = \bigvee_{i\in I}[M, N_i]$.

(5) For any normal subgroup $K$ of $\mathbf{G}$ included in $M \cap N$, the elements of $M/K$ commute with the elements of $N/K$ if and only if $K \supseteq [M, N]$.

(6) $\mathbf{G}$ is Abelian if and only if $[G, G] = \{1\}$ (where 1 is the identity element of $\mathbf{G}$).

When we generalize the commutator later to congruences in a congruence modular variety, we will want an operation which will share these properties. Our operation will be defined from a generalization of the condition (5). From this definition, we will get (1), (3), and (4) directly and a slight modification of (2). We will take (6) to be our definition of Abelian.

The group commutator has one more property which is less transparent but which will also carry over to the generalization (in fact, it also could be used to define the modular commutator). This is

(7) The commutator operation is the largest binary operation defined across all normal subgroup lattices of all groups which satisfies conditions (1) and (2).

Suppose that $C(x, y)$ is another binary operation defined on the normal subgroup lattice of every group which satisfies (1) and (2). Let $M$ and $N$ be normal subgroups of a group $\mathbf{G}$. We will prove that $C(M, N) \subseteq [M, N]$. To do so, we need to define four subgroups of $\mathbf{G} \times \mathbf{G}$.

$$\mathbf{G}(M) = \{\langle x, y\rangle : x, y \in \mathbf{G} \text{ and } x^{-1}y \in M\} \tag{2.2}$$

$$\Delta = \{\langle x, y\rangle : x \in N, y \in G, \text{ and } x^{-1}y \in [M, N]\} \tag{2.3}$$

$$B = \{\langle x, 1\rangle : x \in [M, N]\} \tag{2.4}$$

$$M_1 = \{\langle x, 1\rangle : x \in M\}. \tag{2.5}$$

The subgroups $\Delta$, $B$, and $M_1$ are normal subgroups of $\mathbf{G}(M)$. Let $\pi$ be the projection of $\mathbf{G}(M)$ to the first coordinate. Then the reader can check that

$$\pi(\mathbf{G}(M)) = \mathbf{G} \tag{2.6}$$

$$\pi(\Delta) = N \tag{2.7}$$

$$\pi(B) = [M, N] \tag{2.8}$$

$$\pi(M_1) = M. \tag{2.9}$$

From property (1) we see that $C(M_1, \Delta) \subseteq M_1 \cap \Delta \subseteq B$ and by (2)

$$C(M, N) = \pi(C(M_1, \Delta)) \subseteq \pi(B) = [M, N]. \tag{2.10}$$

We would now like to state a condition equivalent to (5) which will be the basis for our generalization of the commutator. Let $K = [M, N]$. Suppose that $t$ is an $(n + m)$-ary group term. We will address here how $t$ behaves in $\mathbf{G}/K$ when evaluated on elements of $M/K$ and $N/K$. For convenience in the following calculations, we will write $\bar{g}$ for elements $gK$ of $\mathbf{G}/K$. Suppose that $a_1, \ldots, a_n, b_1, \ldots, b_n \in M$ and $x_1, \ldots, x_m, y_1, \ldots, y_m \in N$ and that

$$t(\bar{a}_1, \ldots, \bar{a}_n, \bar{x}_1, \ldots, \bar{x}_m) = t(\bar{a}_1, \ldots, \bar{a}_n, \bar{y}_1, \ldots, \bar{y}_m). \tag{2.11}$$

Since $K = [M, N]$, we can permute some of the elements in this equation so that we have

$$t(\bar{a}_1, \ldots, \bar{a}_n, \bar{x}_1, \ldots, \bar{x}_m) = \bar{a}_{j_1}^{e_1}\bar{a}_{j_2}^{e_2} \cdots \bar{a}_{j_u}^{e_u}\bar{x}_{l_1}^{d_1}\bar{x}_{l_2}^{d_2} \cdots \bar{x}_{l_v}^{d_v} \tag{2.12}$$

where each $e_i$ and each $d_i$ is either 1 or $-1$. Similarly

$$t(\bar{a}_1, \ldots, \bar{a}_n, \bar{y}_1, \ldots, \bar{y}_m) = \bar{a}_{j_1}^{e_1}\bar{a}_{j_2}^{e_2} \cdots \bar{a}_{j_u}^{e_u}\bar{y}_{l_1}^{d_1}\bar{y}_{l_2}^{d_2} \cdots \bar{y}_{l_v}^{d_v}. \tag{2.13}$$

Combining these, we have

$$\bar{a}_{j_1}^{e_1}\bar{a}_{j_2}^{e_2} \cdots \bar{a}_{j_u}^{e_u}\bar{x}_{l_1}^{d_1}\bar{x}_{l_2}^{d_2} \cdots \bar{x}_{l_v}^{d_v} = \bar{a}_{j_1}^{e_1}\bar{a}_{j_2}^{e_2} \cdots \bar{a}_{j_u}^{e_u}\bar{y}_{l_1}^{d_1}\bar{y}_{l_2}^{d_2} \cdots \bar{y}_{l_v}^{d_v}. \tag{2.14}$$

Suitable cancellation and multiplication by $b$'s now gives

$$\bar{b}_{j_1}^{e_1}\bar{b}_{j_2}^{e_2} \cdots \bar{b}_{j_u}^{e_u}\bar{x}_{l_1}^{d_1}\bar{x}_{l_2}^{d_2} \cdots \bar{x}_{l_v}^{d_v} = \bar{b}_{j_1}^{e_1}\bar{b}_{j_2}^{e_2} \cdots \bar{b}_{j_u}^{e_u}\bar{y}_{l_1}^{d_1}\bar{y}_{l_2}^{d_2} \cdots \bar{y}_{l_v}^{d_v}. \tag{2.15}$$

After commuting as before, we end up with the equality

$$t(\bar{b}_1, \ldots, \bar{b}_n, \bar{x}_1, \ldots, \bar{x}_m) = t(\bar{b}_1, \ldots, \bar{b}_n, \bar{y}_1, \ldots, \bar{y}_m). \tag{2.16}$$

We have proven the following property which will replace property (5) above.

(5') Suppose that $t$ is an $(n+m)$-ary group term and that $a_1, \ldots, a_n, b_1, \ldots, b_n \in M$ and $x_1, \ldots, x_m, y_1, \ldots, y_m \in N$. Let $K = [M, N]$. If

$$t(a_1K, \ldots, a_nK, x_1K, \ldots, x_mK) = t(a_1K, \ldots, a_1K, y_1K, \ldots, y_mK) \tag{2.17}$$

then also

$$t(b_1K, \ldots, b_nK, x_1K, \ldots, x_mK) = t(b_1K, \ldots, b_1K, y_1K, \ldots, y_mK). \tag{2.18}$$

We will describe this situation by saying that $\mathbf{G}$ satisfies the $M, N$ term condition modulo $K$ or that $M$ centralizes $N$ modulo $K$. This term condition will be the basis of the modular commutator.

# 3 Notation

We assume that the reader is familiar with the basics of universal algebra, and we will usually use notation consistent with [37]. In this section, we emphasize a few key ideas and pieces of notation.

Generally, we will use plain text capital letters to refer to sets. We will use bold faced text to refer to algebras. Usually (but not always), the same letter will be used for the set and the algebra. For example, an algebra on a set $A$ will almost always be called $\mathbf{A}$. We use script letters (such as $\mathcal{V}$) to refer to varieties, classes of varieties, and classes of algebras. For any algebra $\mathbf{A}$ in a variety $\mathcal{V}$ and any term $t(x_0, \ldots, x_n)$ of $\mathcal{V}$, it is customary to use a superscript to denote the term operation of $\mathbf{A}$ induced by $t$ (that is, $t^{\mathbf{A}}(x_0, \ldots, x_n)$). In most of our proofs, the algebra will be understood, so we will often (usually) leave off the superscript to allow for cleaner notation. If $\mathbf{A}$ is an algebra, we will use bold faced lowercase letters to represent elements of direct powers of $\mathbf{A}$. For example, an element $\mathbf{a} \in A^n$ is a vector $\langle a_0, \ldots, a_{n-1} \rangle$. Notice that with this notation, we will always assume our subscripts begin at 0 and go to $n-1$. When applying an $(n+m)$-ary term $t$ to a vector $\langle x_0, \ldots, x_{n-1}, y_0, \ldots, y_{m-1} \rangle$, it is often more convenient (and notationally cleaner) to write $t(\mathbf{x}, \mathbf{y})$.

For the subalgebra of $\mathbf{A}$ generated by a subset $X \subseteq \mathbf{A}$, we will write $\mathrm{Sg}_{\mathbf{A}}(X)$. For the subalgebra generated by elements $a_1, \ldots, a_n$, we may abuse notation and write $\mathrm{Sg}_{\mathbf{A}}(a_1, \ldots, a_n)$. Similarly, we use $\mathrm{Cg}_{\mathbf{A}}(X)$ for the congruence on $\mathbf{A}$ generated by a subset $X \subseteq A^2$. For the principal congruence generated by identifying elements $a$ and $b$, we will write $\mathrm{Cg}_{\mathbf{A}}(a, b)$. In all cases, we may omit the subscripted $\mathbf{A}$ if the underlying algebra is understood. We will use $\mathrm{End}\ \mathbf{A}$ for the endomorphism monoid of $\mathbf{A}$.

Depending on context, there are three notations we may use to assert that two elements $x$ and $y$ are related by a binary relation $\alpha$. These are

$$x \alpha y$$

$$\langle x, y \rangle \in \alpha \text{ and}$$

$$x \equiv y \pmod{\alpha}.$$

By a tolerance on an algebra $\mathbf{A}$, we mean a subalgebra of $\mathbf{A}^2$ which is reflexive and symmetric (but not necessarily transitive). We will use $\mathrm{Con}\,\mathbf{A}$ to represent the congruence lattice of $\mathbf{A}$ and $\mathrm{Tol}\,\mathbf{A}$ to represent the tolerance lattice of $\mathbf{A}$. If $\alpha$ is any binary relation then $\mathrm{Tr}(\alpha)$ will

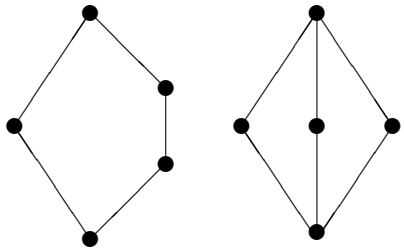

Figure 1: The lattices $\mathbf{N}_5$ (left) and $\mathbf{M}_3$ (right).

be the transitive closure of $\alpha$. The universal relation on a set $A$ will be denoted $1_A$, and the identity relation will be denoted by $0_A$.

If $\mathcal{V}$ is any variety, we will use the notation $\mathcal{V} \models_{\mathrm{Con}} \ldots$ to indicate that all congruences of all algebras in $\mathcal{V}$ satisfy the property $\ldots$. For example, $\mathcal{V} \models_{\mathrm{Con}} (\alpha \cap \beta \approx [\alpha, \beta])$ means that for every algebra $\mathbf{A} \in \mathcal{V}$ and for all $\alpha, \beta \in \operatorname{Con} \mathbf{A}$ the equality $\alpha \cap \beta = [\alpha, \beta]$ holds. Usually, $\approx$ will be used to represent the equality symbol of a first-order language, and $=$ will be used for a specific instance of equality.

Much of this manuscript will deal with congruence lattices which are modular or distributive. Therefore, we remind ourselves of the definitions of these properties and state some basic facts about them. The realization of the concept of a lattice as an independent algebraic object of interest and the formulation of the modular law dates back to Richard Dedekind [9].

**Definition 3.1** *Let $\mathbf{L} = \langle L, \wedge, \vee \rangle$ be a lattice. $\mathbf{L}$ is modular if for all elements $a, b, c \in \mathbf{L}$ with $c \leq a$ the equality $a \wedge (b \vee c) = (a \wedge b) \vee c$ holds. $\mathbf{L}$ is distributive if for all elements $a, b, c \in L$ the equality $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ holds.*

These characterizations of modularity and distributivity should be familiar.

**Theorem 3.2** *For any lattice $\mathbf{L}$, the following are equivalent.*

(1) *$\mathbf{L}$ is distributive.*

(2) *$a \wedge (b \vee c) \leq (a \wedge b) \vee (a \wedge c)$ for all $a, b, c \in \mathbf{L}$.*

(3) *$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ for all $a, b, c \in \mathbf{L}$.*

(4) *$\mathbf{L}$ has no sublattice isomorphic to either $\mathbf{N}_5$ or $\mathbf{M}_3$ (see Figure 1).*

**Theorem 3.3** *The following are equivalent for any lattice $\mathbf{L}$.*

(1) *$\mathbf{L}$ is modular.*

(2) *For any $a, b, c \in L$ if $c \leq a$ then $a \wedge (b \vee c) \leq (a \wedge b) \vee c$.*

(3) *$((a \wedge c) \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$ for all $a, b, c \in L$.*

(4) *$\mathbf{L}$ has no sublattice isomorphic to $\mathbf{N}_5$ (see Figure 1).*

## 4 Centrality and the Term Condition Commutator

**Definition 4.1** *Suppose that $\alpha$, $\beta$, and $\delta$ are congruences on an algebra $\mathbf{A}$. Then $\alpha$ centralizes $\beta$ modulo $\delta$ (in symbols $C(\alpha, \beta; \delta)$) if for any $(m+n)$-ary term operation $T$ of $\mathbf{A}$, for any $\mathbf{a}, \mathbf{b} \in A^m$ with $a_i \alpha b_i$ for all $i$, and for any $\mathbf{c}, \mathbf{d} \in A^n$ with $c_i \beta d_i$ for all $i$, the relation $T(\mathbf{a}, \mathbf{c}) \delta T(\mathbf{a}, \mathbf{d})$ holds if and only if $T(\mathbf{b}, \mathbf{c}) \delta T(\mathbf{b}, \mathbf{d})$. When $C(\alpha, \beta; \delta)$ holds, we will also say that $\mathbf{A}$ satisfies the $\alpha, \beta$ term condition modulo $\delta$.*

It will be convenient for us at times to view the elements of $\mathbf{A}^4$ as $2 \times 2$ matrices so that the 4-tuple $\langle x_0, x_1, x_2, x_3 \rangle$ corresponds to the matrix

$$\begin{pmatrix} x_0 & x_1 \\ x_2 & x_3 \end{pmatrix}.$$

**Definition 4.2** *Suppose that $\alpha$ and $\beta$ are congruences on an algebra $\mathbf{A}$. Define $M(\alpha, \beta)$ to be the subalgebra of $\mathbf{A}^4$ generated by all matrices either of the form*

$$\begin{pmatrix} a & a \\ b & b \end{pmatrix}$$

*where $a \alpha b$ or of the form*

$$\begin{pmatrix} c & d \\ c & d \end{pmatrix}$$

*where $c \beta d$.*

It follows immediately from the definitions that

**Lemma 4.3** *For any congruence $\alpha$, $\beta$, and $\delta$ on an algebra $\mathbf{A}$, $C(\alpha, \beta; \delta)$ holds if and only if for all $\begin{pmatrix} x & y \\ u & v \end{pmatrix} \in M(\alpha, \beta)$, $x \delta y \leftrightarrow u \delta v$.*

These basic properties of centrality hold without any additional assumptions about the underlying variety or algebra.

**Lemma 4.4** *Suppose that $\alpha$, $\beta$, $\delta$, $\{\alpha_i : i \in I\}$, and $\{\delta_j : j \in J\}$ are congruences on an algebra $\mathbf{A}$.*

(1) *If $C(\alpha_i, \beta; \delta)$ for all $i \in I$, then $C(\bigvee_{i \in I} \alpha_i, \beta; \delta)$.*

(2) *If $C(\alpha, \beta; \delta_j)$ for all $j \in J$, then $C(\alpha_j, \beta; \bigcap_{j \in J} \delta_j)$*

(3) *$C(\alpha, \beta; \alpha \cap \beta)$.*

**Proof** **(1)** Let $\gamma = \bigvee_{i \in I} \alpha_i$. Suppose that $T$ is an $(n+m)$-ary term of $\mathbf{A}$ and that $\mathbf{a}, \mathbf{b} \in A^n$ and $\mathbf{x}, \mathbf{y} \in A^m$. Assume also that $a_t \gamma b_t$ for all $t$ and $x_t \beta y_t$ for all $t$. There exist vectors $\mathbf{u}^1, \ldots, \mathbf{u}^l$ so that for each $t$

$$a_t = u_t^1 \alpha_{j_1} u_t^2 \alpha_{j_2} u_t^3 \ldots u_t^l = b_t$$

Suppose that $T(\mathbf{a}, \mathbf{x}) \delta T(\mathbf{a}, \mathbf{y})$. We can prove by induction that for each $i = 1, \ldots, l$ the relation $T(\mathbf{u}^i, \mathbf{x}) \delta T(\mathbf{u}^i, \mathbf{y})$ holds using $C(\alpha_{j_i}, \beta; \delta)$. It follows then that $T(\mathbf{b}, \mathbf{x}) \delta T(\mathbf{b}, \mathbf{y})$.

**(2)** Suppose that $C(\alpha, \beta; \delta_j)$ for all $j \in J$. If $\begin{pmatrix} x & y \\ u & v \end{pmatrix}$ is any matrix in $M(\alpha, \beta)$ so that $\langle x, y\rangle$ is in $\bigcap_{j\in J} \delta_j$, then $x\delta_j y$ for all $j$, so by centrality $u\delta_j v$ for all $j$. Hence $\langle u, v\rangle \in \bigcap_{j\in J} \delta_j$.

**(3)** Suppose that $\begin{pmatrix} x & y \\ u & v \end{pmatrix}$ is any matrix in $M(\alpha, \beta)$. If $x(\alpha \cap \beta)y$, then $u\alpha x(\alpha \cap \beta)y\alpha v$ so $u\alpha v$. Since $u\beta v$ by assumption, it follows that $u(\alpha \cap \beta)v$. □

This lemma makes possible the following definition

**Definition 4.5** *Suppose that* $\mathbf{A}$ *is any algebra and* $\alpha, \beta \in \operatorname{Con}\mathbf{A}$. *The commutator of* $\alpha$ *and* $\beta$ *is defined as* $[\alpha, \beta] = \bigcap\{\delta \in \operatorname{Con}\mathbf{A} : C(\alpha, \beta; \delta)\}$.

This lemma is an immediate consequence of the fact that if $\alpha' \subseteq \alpha$ and $\beta' \subseteq \beta$ then $M(\alpha', \beta) \subseteq M(\alpha, \beta)$ and $M(\alpha, \beta') \subseteq M(\alpha, \beta)$.

**Lemma 4.6** [ , ] *is monotone in both variables.*

This lemma follows immediately from (3) of Lemma 4.4.

**Lemma 4.7** *Suppose that* $\alpha$ *and* $\beta$ *are congruences on an algebra* $\mathbf{A}$. *Then* $[\alpha, \beta] \leq \alpha \cap \beta$.

We take the opportunity here to state our definition of what it means for an algebra, or a congruence, to be Abelian.

**Definition 4.8** *An algebra* $\mathbf{A}$ *is Abelian if* $\mathbf{A} \models [1_A, 1_A] = 0_A$. *A congruence* $\alpha$ *on* $\mathbf{A}$ *is Abelian if* $\mathbf{A} \models [\alpha, \alpha] = 0_A$.

By Lemma 4.4 (1), the following definition makes sense.

**Definition 4.9** *Suppose that* $\mathbf{A}$ *is any algebra. Define the center of* $\mathbf{A}$ *to be the largest congruence* $\zeta \in \operatorname{Con}\mathbf{A}$ *so that* $[\zeta, 1_A] = 0_A$. *Denote the center of* $\mathbf{A}$ *as* $\zeta_{\mathbf{A}}$.

From the definitions, it is clear that

**Lemma 4.10** *An algebra* $\mathbf{A}$ *is Abelian if and only if* $\zeta_{\mathbf{A}} = 1_A$.

We also have this useful universal substitution property of the center.

**Lemma 4.11** *Suppose* $\mathbf{A}$ *is any algebra. Then* $\zeta_{\mathbf{A}}$ *is the set of all* $\langle x, y\rangle$ *so that for all positive integers* $n$, *for all* $(n+1)$*-ary terms* $t$ *of* $\mathbf{A}$, *and for all* $\mathbf{a}, \mathbf{b} \in A^n$

$$t(x, \mathbf{a}) = t(x, \mathbf{b}) \leftrightarrow t(y, \mathbf{a}) = t(y, \mathbf{b}).$$

**Proof** Let $\theta$ be the set of all $\langle x, y\rangle$ satisfying the conditions of the lemma. We will prove that $\theta = \zeta_{\mathbf{A}}$. Since $[\zeta_{\mathbf{A}}, 1_A] = 0_A$, it should be clear that $\zeta_{\mathbf{A}} \subseteq \theta$. We need only establish the reverse inclusion. To do so, we need to know that $\theta$ is a congruence on $\mathbf{A}$ and that $[\theta, 1_A] = 0_A$. It is easy to see that $\theta$ is an equivalence relation. To prove that it is a congruence, we prove that $\theta$ is closed under all unary polynomials of $\mathbf{A}$. Let $p$ be any unary polynomial of $\mathbf{A}$. This means that for some $k$ there is an $(k+1)$-ary term $s$ of $\mathbf{A}$ and constants $\mathbf{c} \in \mathbf{A}^k$ so that $p(x) = s(x, \mathbf{c})$. Let $\langle x, y\rangle \in \theta$. We show that $\langle p(x), p(y)\rangle \in \theta$. Suppose that $t$ is an $(n+1)$-ary term of $\mathbf{A}$ and that $\mathbf{a}, \mathbf{b} \in \mathbf{A}^n$. Then $t(p(x), \mathbf{a}) = t(p(x), \mathbf{b})$ if and only if

$t(s(x,\mathbf{c}),\mathbf{a}) = t(s(x,\mathbf{c}),\mathbf{b})$. Since $x\theta y$, this happens if and only if $t(s(y,\mathbf{c}),\mathbf{a}) = t(s(y,\mathbf{c}),\mathbf{b})$, which happens if and only if $t(p(y),\mathbf{a}) = t(p(y),\mathbf{b})$. Thus $p(x)\theta p(y)$. The equivalence relation $\theta$ is closed under all unary polynomials of $\mathbf{A}$, so $\theta \in \operatorname{Con}\mathbf{A}$ as desired.

Now we only have left to prove that $[\theta, 1_A] = 0_A$. To do so, we show that $C(\theta, 1_A; 0_A)$. Suppose that $t$ is an $(n+m)$-ary term operation of $\mathbf{A}$, that $\mathbf{x},\mathbf{y} \in \mathbf{A}^m$, that $\mathbf{a},\mathbf{b} \in \mathbf{A}^n$ with $x_i\theta y_i$ for all $i$. Suppose that $t(\mathbf{x},\mathbf{a}) = t(\mathbf{x},\mathbf{b})$. We must establish that $t(\mathbf{y},\mathbf{a}) = t(\mathbf{y},\mathbf{b})$. We will prove by induction on $i = 0, 1, \ldots, (m-1)$ that

$$t(y_0,\ldots,y_i,x_{i+1},\ldots,x_{m-1},\mathbf{a}) = t(y_0,\ldots,y_i,x_{i+1},\ldots,x_{m-1},\mathbf{b}).$$

For $i = 0$, since $x_0\theta y_0$ and $t(\mathbf{x},\mathbf{a}) = t(\mathbf{x},\mathbf{b})$, it follows immediately that

$$t(y_0,x_1,\ldots,x_{m-1},\mathbf{a}) = t(y_0,x_1,\ldots,x_{m-1},\mathbf{b}).$$

Suppose then that $0 \leq i < m-1$ and that

$$t(y_0,\ldots,y_i,x_{i+1},\ldots,x_{m-1},\mathbf{a}) = t(y_0,\ldots,y_i,x_{i+1},\ldots,x_{m-1},\mathbf{b}).$$

That

$$t(y_0,\ldots,y_i,y_{i+1},x_{i+2},\ldots,x_{m-1},\mathbf{a}) = t(y_0,\ldots,y_i,y_{i+1},x_{i+2},\ldots,x_{m-1},\mathbf{b})$$

follows now from $x_{i+1}\theta y_{i+1}$. This completes the induction argument. Taking $i = m-1$ now yields $t(\mathbf{y},\mathbf{a}) = t(\mathbf{y},\mathbf{b})$ as desired. □

## 5 Examples

In this section we give a few examples of centrality and the commutator in some familiar varieties. Hopefully, these examples will motivate some of the results we will prove later and the techniques necessary to prove them. We first consider the commutator in rings.

Suppose that $\mathbf{R}$ is a ring and let $I$, $J$, and $K$ be ideals of $\mathbf{R}$. Denote the congruence relations corresponding to $I$, $J$, and $K$ by $\alpha$, $\beta$, and $\delta$. Then, for example, $x\alpha y$ if and only if $x - y \in I$. Suppose further that $C(\alpha,\beta;\delta)$. Taking $x \in I$ and $y \in J$, we will use centrality to prove that $xy \in K$. We have the relations $x\alpha 0$ and $y\beta 0$, so the matrix

$$\begin{pmatrix} 0y & 00 \\ xy & x0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ xy & 0 \end{pmatrix}$$

is in $M(\alpha,\beta)$. Since obviously the top row of this matrix in in $\delta$, we have that $xy\delta 0$. This means that $xy = xy - 0 \in K$. A symmetric argument will show that $yx \in K$ also. This implies that $K$ must contain the ideal $IJ + JI$. Suppose on the other hand that $K$ is an ideal containing $IJ + JI$. We will use this assumption to prove that $C(\alpha,\beta;\delta)$. First of all, notice that in $\mathbf{R}/K$, the product of any element from $\mathbf{I}/K$ and an element from $J/K$ is 0. Suppose now that $t$ is an $(n+m)$-ary ring term, $\mathbf{a},\mathbf{b} \in R^n$ with $a_i\alpha b_i$ for all $i$, $\mathbf{x},\mathbf{y} \in R^m$ with $x_i\beta y_i$ for all $i$, and that $t(\mathbf{a},\mathbf{x})\delta t(\mathbf{a},\mathbf{y})$. We need to show that $t(\mathbf{b},\mathbf{x})\delta t(\mathbf{b},\mathbf{y})$. To simplify notation in the next calculations, we will write $\bar{r}$ for any coset $r + K$ in $\mathbf{R}/K$. Since $t(\mathbf{a},\mathbf{x})\delta t(\mathbf{a},\mathbf{y})$, in $\mathbf{R}/K$ we have $t(\bar{\mathbf{a}},\bar{\mathbf{x}}) = t(\bar{\mathbf{a}},\bar{\mathbf{y}})$. Through distribution we can find ring terms $q, r, s$ so that

$$t(\mathbf{u},\mathbf{v}) = q(\mathbf{u}) + r(\mathbf{v}) + s(\mathbf{u},\mathbf{v}) \tag{5.1}$$

where each of $q, r$, and $s$ is a sum of products of variables and negated variables and so that in each product of $s$ at least one $u_i$ and at least one $v_i$ occurs. Notice that by our assumptions

$$s(\bar{\mathbf{a}}, \bar{\mathbf{x}}) = s(\bar{\mathbf{a}}, \bar{\mathbf{y}}) = s(\bar{\mathbf{b}}, \bar{\mathbf{x}}) = s(\bar{\mathbf{b}}, \bar{\mathbf{y}}) = 0. \tag{5.2}$$

From $t(\bar{\mathbf{a}}, \bar{\mathbf{x}}) = t(\bar{\mathbf{a}}, \bar{\mathbf{y}})$ it follows that

$$q(\bar{\mathbf{a}}) + r(\bar{\mathbf{x}}) + s(\bar{\mathbf{a}}, \bar{\mathbf{x}}) = q(\bar{\mathbf{a}}) + r(\bar{\mathbf{y}}) + s(\bar{\mathbf{a}}, \bar{\mathbf{y}}) \tag{5.3}$$

and hence that

$$q(\bar{\mathbf{a}}) + r(\bar{\mathbf{x}}) + 0 = q(\bar{\mathbf{a}}) + r(\bar{\mathbf{y}}) + 0. \tag{5.4}$$

Appropriate cancellation and addition of $q(\bar{\mathbf{b}})$ now gives

$$q(\bar{\mathbf{b}}) + r(\bar{\mathbf{x}}) + 0 = q(\bar{\mathbf{b}}) + r(\bar{\mathbf{y}}) + 0 \tag{5.5}$$

and hence

$$q(\bar{\mathbf{b}}) + r(\bar{\mathbf{x}}) + s(\bar{\mathbf{b}}, \bar{\mathbf{x}}) = q(\bar{\mathbf{b}}) + r(\bar{\mathbf{y}}) + s(\bar{\mathbf{b}}, \bar{\mathbf{y}})\,. \tag{5.6}$$

This gives $t(\bar{\mathbf{b}}, \bar{\mathbf{x}}) = t(\bar{\mathbf{b}}, \bar{\mathbf{y}})$ or $t(\mathbf{b}, \mathbf{x}) \delta t(\mathbf{b}, \mathbf{y})$ as desired. We have proven that $C(\alpha, \beta; \delta)$ holds if and only if $K$ contains $IJ + JI$. This gives us

**Fact 5.1** *Let* $\mathbf{R}$ *be a ring and let* $I$ *and* $J$ *be ideals of* $\mathbf{R}$*. Suppose that* $\alpha$ *and* $\beta$ *are the congruences associated with* $I$ *and* $J$*. Then* $[\alpha, \beta]$ *is the congruence associated with the ideal* $IJ + JI$*.*

This fact tells us what Abelian rings look like. Suppose that $\mathbf{R}$ is an Abelian ring. This means that $[1_R, 1_R] = 0_R$, which by the last fact tells us that $R \cdot R + R \cdot R = \{0\}$. This happens exactly when multiplication in $\mathbf{R}$ is trivial in the sense that all products are 0. Hence

**Fact 5.2** *A ring* $\mathbf{R}$ *is Abelian if and only if all products in* $\mathbf{R}$ *are* 0*.*

Since we know what ring commutators look like, it is easy to see what the center of a ring is.

**Fact 5.3** *If* $\mathbf{R}$ *is any ring, then* $\zeta_{\mathbf{R}}$ *is the annihilator of* $\mathbf{R}$*—the set of all* $x \in R$ *so that* $xr = rx = 0$ *for all* $r \in R$*.*

We next turn our attention to the commutator in lattices. Suppose that $\mathbf{L}$ is a lattice and that $\alpha$ and $\beta$ are congruences on $\mathbf{L}$. We will prove that $[\alpha, \beta] = \alpha \cap \beta$. That $[\alpha, \beta] \subseteq \alpha \cap \beta$ is always true. We just need to prove the reverse inclusion. Suppose that $\langle a, b \rangle \in \alpha \cap \beta$. We will use the $\alpha, \beta$ term condition modulo $[\alpha, \beta]$ to show that $\langle a, b \rangle \in [\alpha, \beta]$. Consider the lattice term $t(x, y, z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$. This term satisfies

$$t(x, x, x) \approx t(x, x, y) \approx t(x, y, x) \approx t(y, x, x) \approx x. \tag{5.7}$$

Any ternary term which satisfies these equations is called a majority term. It is well known that any variety with a majority term is congruence distributive. The matrix

$$\begin{pmatrix} a & a \\ a & b \end{pmatrix} = \begin{pmatrix} t(a,a,a) & t(a,a,b) \\ t(a,b,a) & t(a,b,b) \end{pmatrix}$$

is in $M(\alpha, \beta)$. Since we have equality in the first row – and hence a relation via $[\alpha, \beta]$, the $\alpha, \beta$ term condition modulo $[\alpha, \beta]$ tells us the second row is in $[\alpha, \beta]$. We have proven

**Fact 5.4** *The commutator operation in the variety of lattices is congruence intersection.*

Actually, our argument proves

**Fact 5.5** *Suppose that $\mathcal{V}$ is any variety with a majority operation. Then the commutator operation in $\mathcal{V}$ is congruence intersection.*

We will extend this fact in Section 7 to all congruence distributive varieties. For now, we will use it to see what Abelian lattices look like. A lattice $\mathbf{L}$ is Abelian if and only if $0_L = [1_L, 1_L] = 1_L \cap 1_L = 1_L$. This happens if and only if $\mathbf{L}$ is a one element lattice. Thus

**Fact 5.6** *The only Abelian lattice is the one element lattice.*

This could also be proven quickly by considering the term $t(x, y, z) = x \wedge y \wedge z$ and the term condition. Since such an argument would only involve the one lattice operation, it would also establish the same result for semilattices. Also notice that since the commutator in lattices is intersection, the center of a lattice is trivial (the identity relation).

As a final example in this section, we will consider the commutator in modules. We will prove that the commutator in any module $\mathbf{M}$ over a ring $\mathbf{R}$ is constantly $0_M$. To do this, it suffices to show that $[1_M, 1_M] = 0_M$. In particular, we will see that every module is Abelian. Suppose that $t$ is any $(n+m)$-ary term of $\mathbf{M}$. We can assume that $\mathbf{R}$ has a unity. The term $t$ can be expressed as

$$t(\mathbf{u}, \mathbf{v}) = \sum_{i=1}^{l} r_i u_{j_i} + \sum_{i=1}^{l'} s_i v_{j_i} \tag{5.8}$$

where each $r_i$ and each $s_i$ is in $\mathbf{R}$. Let $\mathbf{a}, \mathbf{b} \in M^n$ and $\mathbf{x}, \mathbf{y} \in M^m$ and suppose that $t(\mathbf{a}, \mathbf{x}) = t(\mathbf{a}, \mathbf{y})$. This means that

$$\sum_{i=1}^{l} r_i a_{j_i} + \sum_{i=1}^{l'} s_i x_{j_i} = \sum_{i=1}^{l} r_i a_{j_i} + \sum_{i=1}^{l'} s_i y_{j_i}. \tag{5.9}$$

Appropriate cancellation and addition now gives

$$\sum_{i=1}^{l} r_i b_{j_i} + \sum_{i=1}^{l'} s_i x_{j_i} = \sum_{i=1}^{l} r_i b_{j_i} + \sum_{i=1}^{l'} s_i y_{j_i} \tag{5.10}$$

and hence that $t(\mathbf{b}, \mathbf{x}) = t(\mathbf{b}, \mathbf{y})$. Thus we have established that $C(1_M, 1_M; 0_M)$ so $[1_M, 1_M] = 0_M$. This means

**Fact 5.7** *Every module over a ring is Abelian.*

I follows, of course, that the center of any module is the universal relation. We will see in Section 9 that every Abelian algebra in a congruence modular variety is (polynomially equivalent to) a module over a ring.

# 6 Maltsev Conditions

A variety $\mathcal{W}$ is said to **interpret** a variety $\mathcal{V}$ if for every basic operation $t$ of $\mathcal{V}$ there is a $\mathcal{W}$-term $s_t$ so that for every algebra $\mathbf{A} \in \mathcal{W}$ the algebra $\langle A, \{s_t^{\mathbf{A}}\}\rangle$ is a member of $\mathcal{V}$. We denote this situation by $\mathcal{V} \leq \mathcal{W}$. We say that a class $\mathcal{K}$ of varieties is a **strong Maltsev class** (or that $\mathcal{K}$ is defined by a **strong Maltsev condition**) if and only if there is a finitely presented variety $\mathcal{V}$ so that $\mathcal{K}$ is precisely the class of all varieties $\mathcal{W}$ for which $\mathcal{V} \leq \mathcal{W}$. If there are finitely presented varieties $\ldots \leq \mathcal{V}_3 \leq \mathcal{V}_2 \leq \mathcal{V}_1$ so that $\mathcal{K}$ is the class of all varieties $\mathcal{W}$ so that $\mathcal{V}_i \leq \mathcal{W}$ for some $i$, then $\mathcal{K}$ is a **Maltsev class** (or is defined by a **Maltsev condition**). Finally, if $\mathcal{K}$ is the intersection of countably many Maltsev classes, then $\mathcal{K}$ is a **weak Maltsev class** (or is defined by a **weak Maltsev condition**).

Most Maltsev conditions in practice take the form of an assertion that a variety has a set of terms satisfying one of a sequence of sets of weaker and weaker equations. The first example of a strong Maltsev class was the class of all varieties with permuting congruences.

**Theorem 6.1** (A. I. Maltsev [31]) *A variety $\mathcal{V}$ has permuting congruences if and only if there is a term $p$ of the variety so that $\mathcal{V}$ models the equations:*

$$p(x,z,z) \approx x \text{ and } p(z,z,x) \approx x.$$

**Proof** Suppose that a variety $\mathcal{V}$ has such a term $p$. Let $\mathbf{A} \in \mathcal{V}$ and let $\theta$ and $\phi$ be congruences of $\mathbf{A}$. Suppose that $x, z \in A$ and $\langle x, z\rangle \in \theta \circ \phi$. Then there is a $y \in A$ so that $x\theta y$ and $y\phi z$, and we have

$$x = p^{\mathbf{A}}(x,z,z)\phi p^{\mathbf{A}}(x,y,z)\theta p^{\mathbf{A}}(x,x,z) = z.$$

Thus $\theta \circ \phi \subseteq \phi \circ \theta$. Also

$$\begin{aligned} \phi \circ \theta &= \phi^{\cup} \circ \theta^{\cup} \\ &= (\theta \circ \phi)^{\cup} \\ &\subseteq (\phi \circ \theta)^{\cup} \\ &= \theta^{\cup} \circ \phi^{\cup} \\ &= \theta \circ \phi\,. \end{aligned} \tag{6.1}$$

So $\theta \circ \phi = \phi \circ \theta$. It follows that $\mathcal{V}$ has permuting congruences.

Suppose now that $\mathcal{V}$ has permuting congruences. Let $\mathbf{F}$ be the algebra in $\mathcal{V}$ free on $\{x, y, z\}$. Let $f : \mathbf{F} \to \mathbf{F}$ be the homomorphism which maps $x$ and $y$ to $x$ and $z$ to $z$ and let $\theta = \ker f$. Let $g : \mathbf{F} \to \mathbf{F}$ be the homomorphism mapping $x$ to $x$ and $y$ and $z$ to $z$ and let $\phi = \ker g$. Clearly, we have $\langle x, z\rangle \in \theta \circ \phi$. Since we are assuming congruences permute, $\langle x, z\rangle \in \phi \circ \theta$, so there must be a $w \in F$ with $x\phi w\theta z$. Since $\mathbf{F}$ is generated by $\{x, y, z\}$, there is a term $p$ of $\mathcal{V}$ so that $p^{\mathbf{F}}(x, y, z) = w$. Observe:

$$x = g(x) = g(w) = g(p^{\mathbf{F}}(x,y,z)) = p^{\mathbf{F}}(g(x), g(y), g(z)) = p^{\mathbf{F}}(x,z,z).$$

Using $f$, we can similarly show that $p^{\mathbf{F}}(z,z,x) = x$. Since $\mathbf{F}$ is freely generated by $\{x, y, z\}$, it follows that these equalities hold throughout $\mathcal{V}$. □

The second example of a strong Maltsev class was found in 1963 by A. F. Pixley. It is the class of all varieties in which congruences permute and in which congruence lattices are distributive. Such varieties are called **arithmetical**. The fact that this is a Maltsev class is a consequence of the following theorem whose proof is similar to the proof of Maltsev's theorem:

**Theorem 6.2** (A.F. Pixley [38]) *A variety $\mathcal{V}$ is arithmetical if and only if it has a term $t$ so that $\mathcal{V}$ models*

$$t(x,y,y) \approx t(y,y,x) \approx t(x,y,x) \approx x.$$

The first class of varieties which was shown to be a Maltsev class but not a strong Maltsev class was the class of all varieties in which all congruence lattices are distributive. Such a variety is said to be congruence distributive.

**Theorem 6.3** (B. Jónsson [25]) *A variety $\mathcal{V}$ is congruence distributive if and only if for some positive integer $n$, $\mathcal{V}$ has ternary terms $d_0, \dots, d_n$ so that $\mathcal{V}$ models the following equations:*

$$\begin{array}{rcll} x & \approx & d_0(x,y,z) & \\ x & \approx & d_i(x,y,x) & \text{for } 0 \le i \le n \\ d_i(x,x,y) & \approx & d_{i+1}(x,x,y) & \text{for even } i < n \\ d_i(x,y,y) & \approx & d_{i+1}(x,y,y) & \text{for odd } i < n \\ d_n(x,y,z) & \approx & z. & \end{array}$$

**Proof** Suppose first that $\mathcal{V}$ has ternary terms as described. Let $\mathbf{A} \in \mathcal{V}$ and let $\theta, \phi$ and $\psi$ be congruences of $\mathbf{A}$. Suppose that $\langle a, c\rangle \in \theta \cap (\phi \vee \psi)$ and let $\alpha = (\theta \cap \phi) \vee (\theta \cap \psi)$. We show $\langle a, c\rangle \in \alpha$. There must be $a = x_0, x_1, \dots, x_k = c$ in $A$ with $\langle x_i, x_{i+1}\rangle \in \phi \cup \psi$ for $i < k$. For any $j \le n$ and for any $i < k$, we have that $\langle d_j^{\mathbf{A}}(a, x_i, c), d_j^{\mathbf{A}}(a, x_{i+1}, c)\rangle \in \phi \cup \psi$. Also, $d_j^{\mathbf{A}}(a, x_i, c)\theta d_j^{\mathbf{A}}(a, x_i, a) = a = d_j^{\mathbf{A}}(a, x_{i+1}, a)\theta d_j^{\mathbf{A}}(a, x_{i+1}, c)$. Hence, $\langle d_j^{\mathbf{A}}(a, x_i, c), d_j^{\mathbf{A}}(a, x_{i+1}, c)\rangle \in \alpha$. By transitivity, for all $0 \le j \le n$:

$$d_j^{\mathbf{A}}(a, a, c) = d_j^{\mathbf{A}}(a, x_0, c)\alpha d_j^{\mathbf{A}}(a, x_k, c) = d_j^{\mathbf{A}}(a, c, c).$$

By the third and fourth equations above, this yields $d_j^{\mathbf{A}}(a, c, c)\alpha d_{j+1}^{\mathbf{A}}(a, c, c)$ for all $j \le n$. Hence, $a = d_0^{\mathbf{A}}(a, c, c)\alpha d_n^{\mathbf{A}}(a, c, c) = c$. Thus, $\theta \cap (\phi \vee \psi) \subseteq (\theta \cap \phi) \vee (\theta \cap \psi)$. The reverse inclusion always holds, so we have established that $\operatorname{Con} \mathbf{A}$ is distributive.

Now assume that $\mathcal{V}$ is congruence distributive and let $\mathbf{F}$ be the free algebra in $\mathcal{V}$ generated by $\{x, y, z\}$. Let $f$, $g$, and $h$ be homomorphisms from $\mathbf{F}$ to $\mathbf{F}$ given by:

$$f(x) = f(y) = x,$$

$$f(z) = z,$$

$$g(x) = x,$$

$$g(y) = g(z) = y,$$

$$h(x) = h(z) = x, \text{ and}$$

$$h(y) = y.$$

Let $\phi = \ker f$, $\psi = \ker g$, and $\theta = \ker h$. Since $\langle x, z\rangle \in \theta \cap (\phi \vee \psi) \le (\theta \cap \phi) \vee (\theta \cap \psi)$, there must be elements $w_0 = x, x_1, \dots, w_n = z$ in $F$ so that

$$w_i \theta x \text{ for all } i \le n,$$

$$w_i \psi w_{i+1} \text{ for all even } i < n, \text{ and}$$

$$w_i \phi w_{i+1} \text{ for all odd } i < n.$$

Since $\mathbf{F}$ is generated by $\{x, y, z\}$, there must be ternary terms $d_0, \dots d_n$ so that $d_i^{\mathbf{F}}(x, y, z) = w_i$ for $i = 0, \dots, n$. That these terms satisfy the desired equations follows as in the proof of Maltsev's theorem above. □

The following Maltsev characterization of congruence modularity is critical for work with the modular commutator.

**Theorem 6.4** (A. Day [7]) *A variety $\mathcal{V}$ is congruence modular if and only if $\mathcal{V}$ has 4-ary terms $m_0, \dots, m_n$ for which $\mathcal{V}$ satisfies the equations*

$$\begin{array}{rcll} x & \approx & m_0(x, y, z, u) & \\ x & \approx & m_i(x, y, y, x) & \text{for all } i \\ m_i(x, x, z, z) & \approx & m_{i+1}(x, x, z, z) & \text{for } i \text{ even} \\ m_i(x, y, y, u) & \approx & m_{i+1}(x, y, y, u) & \text{for } i \text{ odd} \\ m_n(x, y, z, u) & \approx & u\,. & \end{array}$$

The terms in Theorem 6.4 are called Day terms. To prove Day's theorem, we need the following lemmas.

**Lemma 6.5** *Let $m_0, \dots, m_n$ be Day terms for a variety $\mathcal{V}$. Let $\mathbf{A} \in \mathcal{V}$ and $a, b, c, d \in A$. Let $\gamma \in \operatorname{Con}\mathbf{A}$ with $b\gamma d$. Then $a\gamma c$ if and only if $m_i(a, a, c, c)\gamma m_i(a, b, d, c)$ for each $i = 0, \dots, n$.*

**Proof** First suppose that $a\gamma c$. Then

$$m_i(a, a, c, c)\gamma m_i(a, a, a, a) = a = m_i(a, b, b, a)\gamma m_i(a, b, d, c). \tag{6.2}$$

Next, suppose that $m_i(a, a, c, c)\gamma m_i(a, b, d, c)$ for all $i$. We will prove by induction that $m_i(a, b, d, c)\gamma a$ for all $i$. This is trivial for $i = 0$ since $m_0(a, b, d, c) = a$. Assume that $0 \leq i < n$ and that $m_i(a, b, d, c)\gamma a$. If $i$ is odd, then

$$m_{i+1}(a, b, d, c)\gamma m_{i+1}(a, b, b, c) = m_i(a, b, b, c)\gamma m_i(a, b, d, c)\gamma a. \tag{6.3}$$

If $i$ is even, then

$$m_{i+1}(a, b, d, c)\gamma m_{i+1}(a, a, c, c) = m_i(a, a, c, c)\gamma m_i(a, b, d, c)\gamma a. \tag{6.4}$$

This finishes the proof that $m_i(a, b, d, c)\gamma a$ for all $i$. In particular, we now know that $a\gamma m_n(a, b, d, c) = c$. □

**Lemma 6.6** (Shifting Lemma – Gumm [17]) *Suppose that $\mathbf{A}$ is an algebra in a variety $\mathcal{V}$ with Day terms $m_0, \dots, m_n$. Let $\alpha, \gamma \in \operatorname{Con}\mathbf{A}$ and let $\beta$ be a compatible reflexive binary relation on $\mathbf{A}$. Suppose $\alpha \cap \beta \subseteq \gamma$. If $a\beta b$, $c\beta d$, $a\alpha c$, and $b(\alpha \cap \gamma)d$, then $a\gamma c$ (see figure 2).*

**Proof** We will employ Lemma 6.5, so we need $m_i(a, a, c, c)\gamma m_i(a, b, d, c)$ for all $i$. First note that for all $i$ our assumptions imply $m_i(a, a, c, c)\beta m_i(a, b, d, c)$. Next, note that for all $i$

$$m_i(a, a, c, c)\alpha m_i(a, a, a, a) = a = m_i(a, b, b, a)\alpha m_i(a, b, d, c)\,. \tag{6.5}$$

Thus, we have

$$\langle m_i(a, a, c, c, ), m_i(a, b, d, c)\rangle \in \alpha \cap \beta \subseteq \gamma. \tag{6.6}$$

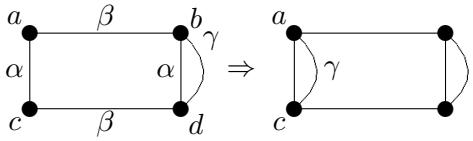


Figure 2: The Shifting Lemma.

By Lemma 6.5, $a\gamma c$. □

**Proof** (Theorem 6.4) Suppose first that $\mathcal{V}$ is a variety with terms $m_0, \ldots, m_n$ satisfying Day's equations. Let $\alpha$, $\beta$, and $\gamma$ be congruences on an algebra $\mathbf{A}$ in $\mathcal{V}$ with $\alpha \geq \gamma$. We must show that $\alpha \cap (\beta \vee \gamma) = (\alpha \cap \beta) \vee \gamma$. The inclusion $\supseteq$ is always true. We establish the forward inclusion. Define compatible reflexive binary relations $\Gamma_0, \Gamma_1, \ldots$ on $\mathbf{A}$ recursively by $\Gamma_0 = \beta$ and $\Gamma_{n+1} = \Gamma_n \circ \gamma \circ \Gamma_n$. Then $\beta \vee \gamma = \bigcup_{n=0}^{\infty} \Gamma_n$. We will prove by induction that $\alpha \cap \Gamma_n \subseteq (\alpha \cap \beta) \vee \gamma$ for all $n$. First, $\alpha \cap \Gamma_0 = \alpha \cap \beta$ which is clearly contained in $(\alpha \cap \beta) \vee \gamma$. Assume that $n \geq 0$ and $\alpha \cap \Gamma_n \subseteq (\alpha \cap \beta) \vee \gamma$. Let $\langle a, c \rangle \in \alpha \cap \Gamma_{n+1}$. Since $\gamma \leq \alpha$ and $\gamma \leq (\alpha \cap \beta) \vee \gamma$, we have the relations in Figure 3 for some $b$ and $d$. The Shifting

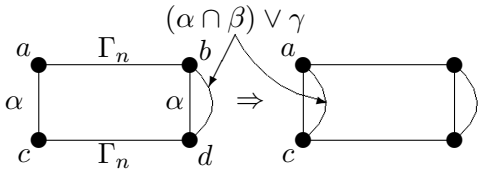


Figure 3: The inductive step for the first half of the proof of Theorem 6.4.

Lemma now gives that $\langle a, c \rangle \in (\alpha \cap \beta) \vee \gamma$. By induction, $\alpha \cap \Gamma_n \subseteq (\alpha \cap \beta) \vee \gamma$ for all $n$, so $\alpha \cap (\beta \vee \gamma) \subseteq (\alpha \cap \beta) \vee \gamma$. This inclusion gives equality and completes the proof that $\operatorname{Con} \mathbf{A}$ is modular.

Next, suppose that $\mathcal{V}$ is a congruence modular variety. Let $\mathbf{A}$ be the free algebra in $\mathcal{V}$ on the generators $\{x, y, z, u\}$. Let $\alpha = \operatorname{Cg}_{\mathbf{A}}(x, u) \vee \operatorname{Cg}_{\mathbf{A}}(y, z)$, $\beta = \operatorname{Cg}_{\mathbf{A}}(x, y) \vee \operatorname{Cg}_{\mathbf{A}}(u, z)$, and $\gamma = \operatorname{Cg}_{\mathbf{A}}(y, z)$. Then $\langle x, u \rangle$ is in $\alpha \cap (\beta \vee \gamma)$ which by modularity is equal to $(\alpha \cap \beta) \vee \gamma$. This means there are elements $u_0, \ldots, u_n \in A$ so that $x = u_0$, $u = u_n$, $u_i \alpha \cap \beta u_{i+1}$ for $i$ even, and $u_i \gamma u_{i+1}$ for $i$ odd. Let $m_0, \ldots, m_n$ be 4-ary terms so that $m_i(x, y, z, u) = u_i$. Immediately, then, we have $m_0(x, y, z, u) = x$ and $m_n(x, y, z, u) = u$. Since $\gamma \leq \alpha$, all of the $u_i$'s are $\alpha$ related. This means that $x \alpha m_i(x, y, z, u) \alpha m_i(x, y, y, x)$. However, by our definitions, $(x/\alpha) \cap \operatorname{Sg}_{\mathrm{A}}(x, y) = \{x\}$, so we have $m_i(x, y, y, x) = x$ for all $i$. Let $g : \mathbf{A} \to \mathbf{A}$ be the unique homomorphism defined by $g(x) = g(y) = x$ and $g(u) = g(z) = z$. Then $\ker g = \beta$. Suppose that $i$ is even. Since $m_i(x, y, z, u)(\alpha \cap \beta) m_{i+1}(x, y, z, u)$, we have

$$\begin{aligned} m_i(x, x, z, z) &= m_i(g(x), g(y), g(z), g(u)) \\ &= g(m_i(x, y, z, u)) \\ &= g(m_{i+1}(x, y, z, u)) \\ &= m_{i+1}(g(x), g(y), g(z), g(u)) \\ &= m_{i+1}(x, x, z, z). \end{aligned} \tag{6.7}$$

Let $f : \mathbf{A} \to \mathbf{A}$ be the unique homomorphism defined by $f(x) = x$, $f(y) = f(z) = y$, and

$f(u) = u$. Then $\ker f = \gamma$. Suppose that $i$ is odd. Since $m_i(x,y,z,u)\gamma m_{i+1}(x,y,z,u)$ we see

$$\begin{aligned} m_i(x,y,y,u) &= m_i(f(x),f(y),f(z),f(u)) \\ &= f(m_i(x,y,z,u)) \\ &= f(m_{i+1}(x,y,z,u)) \\ &= m_{i+1}(f(x),f(y),f(z),f(u)) \\ &= m_{i+1}(x,y,y,u). \end{aligned} \tag{6.8}$$

We have established these equalities in $\mathbf{A}$:

$$\begin{aligned} x &= m_0(x,y,z,u) \\ x &= m_i(x,y,y,x) \qquad \text{for all } i \\ m_i(x,x,z,z) &= m_{i+1}(x,x,z,z) \quad \text{for } i \text{ even} \\ m_i(x,y,y,u) &= m_{i+1}(x,y,y,u) \quad \text{for } i \text{ odd} \\ m_n(x,y,z,u) &= u. \end{aligned}$$

Since $\mathbf{A}$ is freely generated in $\mathcal{V}$ by $\{x,y,z,u\}$, it follows that these hold as equations in all of $\mathcal{V}$. □

The lemma usually referred to as the shifting lemma assumes the underlying variety is modular and that $\beta$ is a congruence. The version we have stated happens to be equivalent and is what we need to prove Day's theorem directly. We actually proved that the existence of Day terms implies the shifting lemma, that the shifting lemma implies congruence modularity, and that modularity implies the existence of Day terms. Thus, these three conditions are equivalent.

It has long been known that any lattice identity interpreted as a congruence equation is equivalent to a weak Maltsev condition [46, 39], but it is still an open problem as to which lattice equations are equivalent to Maltsev conditions. There are lattice equations which do not imply modularity among lattices but which, when satisfied by the congruence lattice of every algebra in a variety, do imply congruence modularity [8]. It was all but conjectured on page 155 of [12] that all of these equations are Maltsev conditions for congruences. This has recently been proven to be true.

**Theorem 6.7** [6] *A variety $\mathcal{V}$ is congruence modular if and only if for all tolerances $\alpha$ and $\beta$ on any algebra in $\mathcal{V}$ it is the case that* $\mathrm{Tr}(\alpha) \cap \mathrm{Tr}(\beta) = \mathrm{Tr}(\alpha \cap \beta)$.

Using this theorem, it is easy to show that

**Theorem 6.8** [5] *Suppose that $\epsilon$ is a lattice equation so that for any variety $\mathcal{V}$ if $\mathcal{V} \models_{\mathrm{Con}} \epsilon$, then $\mathcal{V}$ is congruence modular. Then the class of all varieties $\mathcal{V}$ with $\mathcal{V} \models_{\mathrm{Con}} \epsilon$ is a Maltsev class.*

# 7 Congruence Distributive Varieties

The commutator in congruence distributive varieties reduces to congruence intersection. This can be proved later after we have derived some of the properties of the commutator in congruence modular varieties. However, we offer a proof here based on the Jónsson terms. This will illustrate in an isolated setting the intimate relationship between the commutator and equations for Maltsev conditions. The proof we are about to see should be reminiscent of Fact 5.5.

**Theorem 7.1** *A variety $\mathcal{V}$ is congruence distributive if and only*

$$\mathcal{V}\models_{\mathrm{Con}}[\alpha\vee\gamma,\beta]\approx[\alpha,\beta]\vee[\gamma,\beta] \text{ and } [\alpha,\beta]=\alpha\cap\beta. \tag{7.1}$$

**Proof** Half of this is almost obvious. Suppose that congruences in $\mathcal{V}$ satisfy the stated commutator equations. Let $\alpha,\beta,\gamma$ be congruences on an algebra $\mathbf{A}\in\mathcal{V}$. Then

$$\begin{aligned}(\alpha\cap\beta)\vee(\gamma\cap\beta) &= [\alpha,\beta]\vee[\gamma,\beta]\\ &= [\alpha\vee\gamma,\beta]\\ &= (\alpha\vee\gamma)\cap\beta.\end{aligned} \tag{7.2}$$

Thus $\operatorname{Con}\mathbf{A}$ is distributive.

For the reverse direction, we will need to use Jónsson's terms. Suppose that $\mathcal{V}$ is a congruence distributive variety and let $d_0,\dots,d_n$ be Jónsson terms for $\mathcal{V}$. Let $\mathbf{A}\in\mathcal{V}$ and $\alpha,\beta\in\operatorname{Con}\mathbf{A}$. We will prove that $[\alpha,\beta]=\alpha\cap\beta$. That $[\alpha,\beta]\subseteq\alpha\cap\beta$ is always true. We will prove the reverse inclusion. Let $\delta=[\alpha,\beta]$ and let $\langle x,y\rangle\in\alpha\cap\beta$. We will prove by induction that $d_i(x,y,x)\delta d_i(x,y,y)$ for all $i=0,\dots,n$. This is trivially true for $d_0$ since $x=d_0(x,y,x)=d_0(x,y,y)$. Suppose that $0\le i<n$ and $d_i(x,y,x)\delta d_i(x,y,y)$. There are two cases – either $i$ is even or it is odd. Supposing that $i$ is odd, then

$$d_{i+1}(x,y,x)=d_i(x,y,x)\delta d_i(x,y,y)=d_{i+1}(x,y,y). \tag{7.3}$$

Suppose next that $i$ is even. Since $\begin{pmatrix} d_i(x,y,x) & d_i(x,y,y)\\ d_i(x,x,x) & d_i(x,x,y)\end{pmatrix}\in M(\alpha,\beta)$, from $C(\alpha,\beta;\delta)$ we can conclude that $d_i(x,x,x)\delta d_i(x,x,y)$. It follows that

$$d_{i+1}(x,x,x)=d_i(x,x,x)\delta d_i(x,x,y)=d_{i+1}(x,x,y). \tag{7.4}$$

Now

$$\begin{pmatrix} d_{i+1}(x,x,x) & d_{i+1}(x,x,y)\\ d_{i+1}(x,y,x) & d_{i+1}(x,y,y)\end{pmatrix}\in M(\alpha,\beta),$$

so centrality now gives $d_{i+1}(x,y,x)\delta d_{i+1}(x,y,y)$. This completes the proof that for all $i\in\{0,\dots,n\}$, $d_i(x,y,x)\delta d_i(x,y,y)$. The particular case we care about is $i=n$, which gives

$$x=d_n(x,y,x)\delta d_n(x,y,y)=y. \tag{7.5}$$

Thus we have $\alpha\cap\beta\subseteq[\alpha,\beta]$, so these congruences are actually equal. We have that $\mathcal{V}\models_{\mathrm{Con}}[\alpha,\beta]=\alpha\cap\beta$. The other equation now follows immediately from distributivity. Suppose that $\alpha,\beta,\gamma$ are congruences on an algebra in $\mathcal{V}$. Then

$$\begin{aligned}[\alpha\vee\gamma,\beta] &= (\alpha\vee\gamma)\cap\beta\\ &= (\alpha\cap\beta)\vee(\gamma\cap\beta)\\ &= [\alpha,\beta]\vee[\gamma,\beta].\end{aligned} \tag{7.6}$$

□

Of course, this gives

**Corollary 7.2** *The only Abelian algebras in a congruence distributive variety are trivial.*

# 8 Congruence Modular Varieties

The commutator is particularly well behaved in congruence modular varieties. In fact, we can extend all of the properties listed for the group commutator in Section 2 to the commutator in congruence modular varieties. Our primary tool for doing so will be this next characterization of centrality in congruence modular varieties.

**Definition 8.1** *Suppose that $\alpha$ and $\beta$ are congruences on an algebra $\mathbf{A}$ in a variety with Day terms $m_0, \ldots, m_n$. Define $\chi(\alpha, \beta)$ to be the set of all pairs $\langle m_i(x,x,u,u), m_i(x,y,z,u)\rangle$ for which $\begin{pmatrix} x & y \\ u & z \end{pmatrix} \in M(\alpha, \beta)$ and $m_i$ is a Day term.*

**Theorem 8.2** (R. Freese, R. McKenzie [12]) *Suppose that $\alpha$, $\beta$, and $\gamma$ are congruences on an algebra $\mathbf{A}$ in a congruence modular variety. The following are equivalent.*

(1) $C(\alpha, \beta; \gamma)$.

(2) $\chi(\alpha, \beta) \subseteq \gamma$.

(3) $C(\beta, \alpha; \gamma)$.

(4) $\chi(\beta, \alpha) \subseteq \gamma$.

**Proof** We will prove that (1) $\rightarrow$ (2) $\rightarrow$ (3). Then exchanging $\alpha$ and $\beta$ in these implications will show that all four conditions are equivalent.

(1) $\rightarrow$ (2): Suppose that $C(\alpha, \beta; \gamma)$. Let $t$ be an $(n+m)$-ary term of $\mathbf{A}$. Let $\mathbf{a}, \mathbf{b} \in A^n$ and $\mathbf{x}, \mathbf{y} \in A^m$ with $a_i \alpha b_i$ for all $i$ and $x_i \beta y_i$ for all $i$. This makes $\begin{pmatrix} t(\mathbf{a},\mathbf{x}) & t(\mathbf{a},\mathbf{y}) \\ t(\mathbf{b},\mathbf{x}) & t(\mathbf{b},\mathbf{y}) \end{pmatrix}$ a generic element of $M(\alpha, \beta)$. To establish the implication, we need to prove that

$$m_i(t(\mathbf{a},\mathbf{x}), t(\mathbf{a},\mathbf{x}), t(\mathbf{b},\mathbf{x}), t(\mathbf{b},\mathbf{x})) \gamma m_i(t(\mathbf{a},\mathbf{x}), t(\mathbf{a},\mathbf{y}), t(\mathbf{b},\mathbf{y}), t(\mathbf{b},\mathbf{x}))\,. \tag{8.1}$$

The matrix

$$\begin{pmatrix} m_i(t(\mathbf{a},\mathbf{x}), t(\mathbf{b},\mathbf{x}), t(\mathbf{b},\mathbf{x}), t(\mathbf{a},\mathbf{x})) & m_i(t(\mathbf{a},\mathbf{x}), t(\mathbf{b},\mathbf{y}), t(\mathbf{b},\mathbf{y}), t(\mathbf{a},\mathbf{x})) \\ m_i(t(\mathbf{a},\mathbf{x}), t(\mathbf{a},\mathbf{x}), t(\mathbf{b},\mathbf{x}), t(\mathbf{b},\mathbf{x})) & m_i(t(\mathbf{a},\mathbf{x}), t(\mathbf{a},\mathbf{y}), t(\mathbf{b},\mathbf{y}), t(\mathbf{b},\mathbf{x})) \end{pmatrix} \tag{8.2}$$

is in $M(\alpha, \beta)$. Notice that by the Day equations both elements of the top row of this matrix equal $t(\mathbf{a}, \mathbf{x})$. In particular, the top elements are $\gamma$ related. It follows then that the bottom elements are also $\gamma$ related as desired.

(2) $\rightarrow$ (3): Suppose now that $\chi(\alpha, \beta) \subseteq \gamma$. Suppose that $\begin{pmatrix} b & d \\ a & c \end{pmatrix} \in M(\beta, \alpha)$ and that $b \gamma d$. It follows that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(\alpha, \beta)$ and hence that $\langle m_i(a,a,c,c), m_i(a,b,d,c)\rangle \in \gamma$ for all $i$. By Lemma 6.5 it follows that $a \gamma c$, so $C(\beta, \alpha; \gamma)$.

We now have (1) $\rightarrow$ (2) $\rightarrow$ (3). By trading $\alpha$ and $\beta$, we get (3) $\rightarrow$ (4) $\rightarrow$ (1), so the statements are equivalent. $\square$

We can now easily prove the following corollaries.

**Theorem 8.3** *Suppose that $\alpha$, $\beta$, and $\gamma$ are congruences on an algebra $\mathbf{A}$ in a congruence modular variety.*

(1) $C(\alpha, \beta; \gamma)$ *if and only if* $[\alpha, \beta] \leq \gamma$.

(2) $[\alpha, \beta] = \mathrm{Cg}_{\mathbf{A}}(\chi(\alpha, \beta)) = \mathrm{Cg}_{\mathbf{A}}(\chi(\beta, \alpha))$.

(3) $C(\alpha, \beta; \gamma)$ *if and only if* $C(\beta, \alpha; \gamma)$.

(4) $[\alpha, \beta] = [\beta, \alpha]$ .

(5) *If* $\{\alpha_t : t \in T\} \subseteq \mathrm{Con}\,\mathbf{A}$ *then* $[\bigvee_t \alpha_t, \beta] = \bigvee_t [\alpha_t, \beta]$.

(6) *For any surjective homomorphism* $f : \mathbf{A} \to \mathbf{B}$, *if* $\pi = \ker f$ *then*

$$[\alpha, \beta] \vee \pi = f^{-1}([f(\alpha \vee \pi), f(\beta \vee \pi)])$$

*and*

$$[f(\alpha \vee \pi), f(\beta \vee \pi)] = f([\alpha, \beta] \vee \pi).$$

*(See figure 4)*

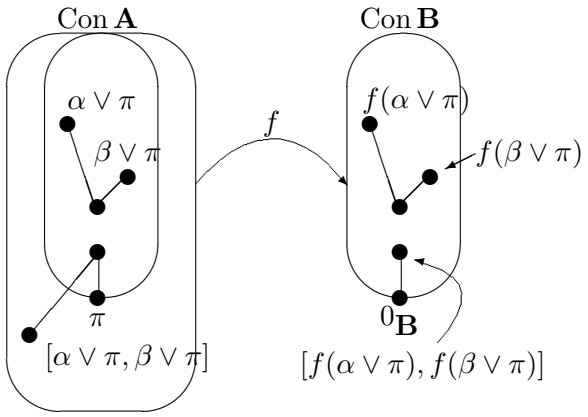


Figure 4: To calculate $[f(\alpha \vee \pi), f(\beta \vee \pi)]$, first pull back through $f$ to $\alpha \vee \pi$ and $\beta \vee \pi$. Their commutator $[\alpha, \beta]$ might not lie above $\pi$, so join with $\pi$. The image of this congruence under $f$ is $[f(\alpha \vee \pi), f(\beta \vee \pi)]$.

**Proof** (1)-(4) are immediate from the previous lemma and the definition of the commutator. We look first, then, at (5). That $\bigvee_t [\alpha_t, \beta] \subseteq [\bigvee_t \alpha_t, \beta]$ follows from monotonicity. To establish the reverse inclusion, it suffices to show that $C(\bigvee_t \alpha_t, \beta; \bigvee_t [\alpha_t, \beta])$. First, notice that by property (1), $C(\alpha_t, \beta; \bigvee_t [\alpha_t, \beta])$ holds for all $t$. Then Lemma 4.4(1) gives the desired result.

For part (6), note that by part (5) $[\alpha, \beta] \vee \pi = [\alpha \vee \pi, \beta \vee \pi] \vee \pi$; and from this the two statements can easily be seen to be equivalent. Part (6) now follows from the fact that the function induced by $f$ on $\mathbf{A}^4$ maps $M(\alpha \vee \pi, \beta \vee \pi)$ onto $M(f(\alpha \vee \pi), f(\beta \vee \pi))$ and maps $\chi(\alpha \vee \pi, \beta \vee \pi)$ onto $\chi(f(\alpha \vee \pi), f(\beta \vee \pi))$. □

The symmetry in the above theorem gives us this characterization of centrality in congruence modular varieties.

**Corollary 8.4** *Suppose that $\alpha$, $\beta$, and $\delta$ are congruences on an algebra in a congruence modular variety. Then $C(\alpha, \beta; \delta)$ if and only if for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(\alpha, \beta)$*

$$a \delta b \leftrightarrow c \delta d \text{ and } a \delta c \leftrightarrow b \delta d \,. \tag{8.3}$$

To make further arguments clearer, we will often write the elements of $\mathbf{A}^2$ as column vectors.

**Definition 8.5** *Suppose that $\mathbf{A}$ is an algebra in a congruence modular variety and $\alpha, \beta \in \operatorname{Con}\mathbf{A}$. Let $\mathbf{A}(\alpha)$ be the subalgebra of $\mathbf{A}^2$ whose universe is $\alpha$ and define these three congruences on $\mathbf{A}(\alpha)$*

$$[\alpha, \beta]_0 = \left\{ \left\langle \begin{pmatrix} x \\ u \end{pmatrix}, \begin{pmatrix} y \\ v \end{pmatrix} \right\rangle \in \mathbf{A}(\alpha)^2 : \langle x, y \rangle \in [\alpha, \beta] \right\} \tag{8.4}$$

$$[\alpha, \beta]_1 = \left\{ \left\langle \begin{pmatrix} u \\ x \end{pmatrix}, \begin{pmatrix} v \\ y \end{pmatrix} \right\rangle \in \mathbf{A}(\alpha)^2 : \langle x, y \rangle \in [\alpha, \beta] \right\} \tag{8.5}$$

$$\Delta_{\alpha,\beta} = \operatorname{Tr}\left( \left\{ \left\langle \begin{pmatrix} x \\ u \end{pmatrix}, \begin{pmatrix} y \\ z \end{pmatrix} \right\rangle : \begin{pmatrix} x & y \\ u & z \end{pmatrix} \in M(\alpha, \beta) \right\} \right) . \tag{8.6}$$

**Lemma 8.6** *Suppose that $\alpha$ and $\beta$ are congruences on an algebra $\mathbf{A}$ in a congruence modular variety. For $i \in \{0, 1\}$, let $\pi_i : \mathbf{A}^2 \to \mathbf{A}$ be the projection to the $i^{th}$ coordinate and let $\eta_i = \ker \pi_i|_{\mathbf{A}(\alpha)}$. Then*

(1) $\eta_1 \cap \Delta_{\alpha,\beta} \subseteq [\alpha, \beta]_0$.

(2) $\eta_0 \cap \Delta_{\alpha,\beta} \subseteq [\alpha, \beta]_1$.

(3) $\Delta_{\alpha,\beta} \vee \eta_0 = \pi_0^{-1}(\beta)$.

(4) $\Delta_{\alpha,\beta} \vee \eta_1 = \pi_1^{-1}(\beta)$

**Proof** For the proof, we will write $\Delta$ for $\Delta_{\alpha,\beta}$. Let $\left\langle \begin{pmatrix} x \\ u \end{pmatrix}, \begin{pmatrix} y \\ u \end{pmatrix} \right\rangle \in \eta_1 \cap \Delta$. Then we have the arrangement in Figure 5, so we can conclude that $\left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} y \\ y \end{pmatrix} \right\rangle \in \eta_1 \cap \Delta$. This means that there are $a_0, \ldots, a_n, b_0, \ldots, b_n \in A$ so that $a_0 = x$, $b_0 = a_n = b_n = y$

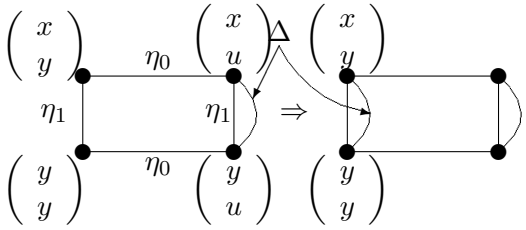


Figure 5: The shifting lemma for Lemma 8.6 (1).

and for each $i < n$ $\begin{pmatrix} a_i & a_{i+1} \\ b_i & b_{i+1} \end{pmatrix} \in M(\alpha, \beta)$. Since $\langle a_n, b_n \rangle = \langle y, y \rangle \in [\alpha, \beta]$, we can use

Corollary 8.4 to establish that $\langle a_i, b_i\rangle \in [\alpha,\beta]$ for all $i$. In particular, $\langle x, y\rangle \in [\alpha,\beta]$. This places $\left\langle \begin{pmatrix} x \\ u \end{pmatrix}, \begin{pmatrix} y \\ u \end{pmatrix} \right\rangle \in [\alpha,\beta]_0$ as desired. We have established that $\eta_1 \cap \Delta \subseteq [\alpha,\beta]_0$. This proves (1). (2) now follows because

$$\left\langle \begin{pmatrix} x \\ u \end{pmatrix}, \begin{pmatrix} y \\ v \end{pmatrix} \right\rangle \in [\alpha,\beta]_0 \Leftrightarrow \left\langle \begin{pmatrix} u \\ x \end{pmatrix}, \begin{pmatrix} v \\ y \end{pmatrix} \right\rangle \in [\alpha,\beta]_1 \tag{8.7}$$

and

$$\left\langle \begin{pmatrix} x \\ u \end{pmatrix}, \begin{pmatrix} y \\ v \end{pmatrix} \right\rangle \in \Delta \Leftrightarrow \left\langle \begin{pmatrix} u \\ x \end{pmatrix}, \begin{pmatrix} v \\ y \end{pmatrix} \right\rangle \in \Delta. \tag{8.8}$$

For (3), suppose that $x\beta y$, $x\alpha u$ and $y\alpha v$. Then

$$\begin{pmatrix} x \\ u \end{pmatrix} \eta_0 \begin{pmatrix} x \\ x \end{pmatrix} \Delta \begin{pmatrix} y \\ y \end{pmatrix} \eta_0 \begin{pmatrix} y \\ v \end{pmatrix}. \tag{8.9}$$

This shows $\pi_0^{-1}(\beta) \subseteq \eta_0 \vee \Delta$. The other inclusion is trivial. (4) is similar. □

**Theorem 8.7** *Suppose that $\mathcal{V}$ is a congruence modular variety. The commutator is the greatest binary operation defined on the congruence lattice of every algebra in $\mathcal{V}$ so that for any $\mathbf{A}, \mathbf{B} \in \mathcal{V}$, for any $\alpha, \beta \in \operatorname{Con}\mathbf{A}$, and for any surjective homomorphism $f : \mathbf{A} \to \mathbf{B}$*

$$[\alpha,\beta] \leq \alpha \cap \beta \text{ and} \tag{8.10}$$

$$[\alpha,\beta] \vee \pi = f^{-1}([f(\alpha \vee \pi), f(\beta \vee \pi)]). \tag{8.11}$$

**Proof** Let $C$ be any other binary operation on the congruence lattices of algebras in $\mathcal{V}$ satisfying the stated properties. We will prove that the commutator always dominates $C$. The proof is essentially the same as that of this property for groups presented in Section 2. Let $\alpha$ and $\beta$ be congruences on an algebra $\mathbf{A}$ in $\mathcal{V}$.

For $i \in \{0,1\}$, let $\pi_i : \mathbf{A}(\alpha) \to \mathbf{A}$ be the projection to the $i^{th}$ coordinate with $\eta_i = \ker \pi_i|_{\mathbf{A}(\alpha)}$. Let $\Delta = \Delta_{\alpha,\beta}$. In $\operatorname{Con}\mathbf{A}(\alpha)$ we have $C(\eta_1, \Delta) \subseteq \eta_1 \cap \Delta$ by our assumptions on $C$. Also, $\eta_1 \cap \Delta \subseteq [\alpha,\beta]_0$ by Lemma 8.6. Hence $C(\eta_1, \Delta) \subseteq [\alpha,\beta]_0$. Let $\alpha_0 = \pi_0^{-1}(\alpha)$ and $\beta_0 = \pi_0^{-1}(\beta)$. Then $\alpha_0 = \eta_0 \vee \eta_1$ and $\beta_0 = \eta_0 \vee \Delta$ so $\alpha = \pi_0(\eta_0 \vee \eta_1)$ and $\beta = \pi_0(\eta_0 \vee \Delta)$. It follows then by our assumptions on $C$ that

$$\begin{aligned} C(\alpha,\beta) &= C(\pi_0(\eta_0 \vee \eta_1), \pi_0(\eta_0 \vee \Delta)) \\ &= \pi_0(C(\eta_1, \Delta) \vee \eta_0) \\ &\subseteq \pi_0([\alpha,\beta]_0) \\ &= [\alpha,\beta]. \end{aligned} \tag{8.12}$$

This concludes the proof that $C$ is always dominated by the commutator. □

At this point in time, we have an extension of all seven of the properties of the group commutator listed in Section 2.

# 9 Abelian Algebras and Abelian Varieties

Recall that we defined an algebra $\mathbf{A}$ to be Abelian if $[1_A, 1_A] = 0_A$. In some respects, Abelian algebras and algebras generating congruence distributive varieties represent two extremes in congruence modular varieties. In Abelian algebras, the commutator is as small as possible. In algebras generating congruence distributive varieties, the commutator is as large as possible. This dichotomy is emphasized further in this theorem.

**Theorem 9.1** *Suppose that* $\mathbf{A}$ *is an algebra in a congruence modular variety. The following are equivalent.*

(1) *The projection congruences have a common complement in* $\operatorname{Con}\mathbf{A} \times \mathbf{A}$.

(2) $\mathbf{M}_3$ *is a* 0-1 *sublattice of* $\operatorname{Con}\mathbf{A}^2$.

(3) $\mathbf{M}_3$ *is a* 0-1 *sublattice of some subdirect product of two copies of* $\mathbf{A}$.

(4) $\mathbf{A}$ *is Abelian.*

**Proof** (1) $\to$ (2) and (2) $\to$ (3) are immediate. Suppose that $\mathbf{B}$ is a subalgebra of $\mathbf{A}^2$ which projects onto both coordinates and that $\mathbf{M}_3$ is a 0-1 sublattice of $\operatorname{Con}\mathbf{B}$. We claim that $\mathbf{B}$ is Abelian. Let $\alpha$, $\beta$, and $\gamma$ be the atoms of the copy of $\mathbf{M}_3$. Then

$$\begin{aligned} [1_B, 1_B] &= [\alpha \vee \beta, \alpha \vee \gamma] \\ &= [\alpha, \alpha] \vee [\alpha, \gamma] \vee [\beta, \alpha] \vee [\beta, \gamma] \\ &\subseteq \alpha \vee (\beta \cap \gamma) \\ &= \alpha \end{aligned} \tag{9.1}$$

so $[1_B, 1_B] \subseteq \alpha$. Similarly, $[1_B, 1_B]$ is below $\beta$ and $\gamma$. Thus, $[1_B, 1_B] = 0_B$ and $\mathbf{B}$ is Abelian. Let $\pi : \mathbf{B} \to \mathbf{A}$ be either projection and $\eta = \ker\pi$. Now by Theorem 8.3 (6) we have

$$\begin{aligned} [1_A, 1_A] &= [\pi(1_B), \pi(1_B)] \\ &= \pi([1_B, 1_B] \vee \eta) \\ &= \pi(\eta) \\ &= 0_A. \end{aligned} \tag{9.2}$$

Thus $\mathbf{A}$ is Abelian, so (3) $\to$ (4).

Now assume that $\mathbf{A}$ is Abelian. For $i = 0, 1$, let $\pi_i$ be the projection of $\mathbf{A}^2$ to the $i^{th}$ coordinate and let $\eta_i = \ker\pi_i$. Let $\Delta = \Delta_{1_A, 1_A}$. It follows from Lemma 8.6 that $\Delta \vee \eta_i = 1_A$ for $i = 0, 1$. Also, $\Delta \cap \eta_i \subseteq [1_A, 1_A]_{1-i} = \eta_{1-i}$ for $i = 0, 1$, so $\Delta \cap \eta_i = 0_{A^2}$. Thus, $\Delta$ is a complement of both projection kernels. □

**Definition 9.2** *Two algebras are polynomially equivalent if they have the same universe and the same polynomial operations. An algebra is affine if it is polynomially equivalent with a module over a ring.*

J.D.H. Smith and R. McKenzie independently proved that any Abelian algebra in a congruence permutable variety is affine. C. Herrmann [20] proved that any Abelian algebra in a congruence modular variety is affine using a complex directed union construction which

forced the existence of a Maltsev operation in the original algebra. This Maltsev operation is the key to the proof. H.-P. Gumm [13, 15] also constructed this term with his geometric arguments. Walter Taylor developed the following terms which we will be able to use to construct such a Maltsev term.

**Lemma 9.3** (W. Taylor [45]) *Suppose that $\mathcal{V}$ is a congruence modular variety and that $m_0, \dots m_n$ are Day terms for the variety. Define ternary terms $q_0, \dots, q_n$ recursively in the following manner*

$$\begin{array}{rcll} q_0(x,y,z) & = & z & \\ q_{i+1}(x,y,z) & = & m_{i+1}(q_i(x,y,z),x,y,q_i(x,y,z)) & \text{if } i \text{ is even} \\ q_{i+1}(x,y,z) & = & m_{i+1}(q_i(x,y,z),y,x,q_i(x,y,z)) & \text{if } i \text{ is odd}. \end{array}$$

*Then*

(1) $\mathcal{V} \models q_i(x,x,y) \approx y$ *for all* $i$.

(2) *For any congruence $\beta$ on an algebra $\mathbf{A} \in \mathcal{V}$ and any $\langle x,y\rangle \in \beta$, $\langle q_n(x,y,y),x\rangle \in [\beta,\beta]$.*

**Proof** Part (1) we prove by induction on $i = 0, 1, \dots, n$. It is trivial for $i = 0$. Suppose that $i \geq 0$ and $\mathcal{V} \models q_i(x,x,y) \approx y$. Then

$$\begin{array}{rcll} q_{i+1}(x,x,y) & \approx & m_{i+1}(q_i(x,x,y),x,x,q_i(x,x,y)) & i \text{ even or odd} \\ & \approx & m_{i+1}(y,x,x,y) & \\ & \approx & y. & \end{array} \tag{9.3}$$

Let $\beta$ be a congruence on an algebra $\mathbf{A}$ in $\mathcal{V}$ and let $x\beta y$. We will prove by induction that

$$q_i(x,y,y)[\beta,\beta]m_i(y,y,x,x) \quad \text{for even } i \text{ and} \tag{9.4}$$

$$q_i(x,y,y)[\beta,\beta]m_i(y,y,y,x) \quad \text{for odd } i. \tag{9.5}$$

This will be sufficient. The case of $i = 0$ is trivial. So suppose first that $i$ is even and $q_i(x,y,y)[\beta,\beta]m_i(y,y,x,x)$. It follows that

$$\begin{array}{rcl} q_{i+1}(x,y,y) & = & m_{i+1}(q_i(x,y,y),x,y,q_i(x,y,y)) \\ & [\beta,\beta] & m_{i+1}(m_i(y,y,x,x),x,y,m_i(y,y,x,x)). \end{array} \tag{9.6}$$

Also note that

$$\begin{array}{rcl} m_{i+1}(m_i(y,y,x,x),x,\underline{x},m_i(y,y,x,x)) & = & m_i(y,y,x,x) \\ & = & m_{i+1}(y,y,x,x) \\ & = & m_{i+1}(m_i(y,y,y,y),y,\underline{x},m_i(x,x,x,x)). \end{array} \tag{9.7}$$

By centrality, we can replace the underlined variable with the $\beta$-equivalent $y$ and maintain equivalence modulo $[\beta,\beta]$. Thus

$$m_{i+1}(m_i(y,y,x,x),x,\underline{y},m_i(y,y,x,x))[\beta,\beta]m_{i+1}(m_i(y,y,y,y),y,\underline{y},m_i(x,x,x,x)). \tag{9.8}$$

Combining this with 9.6 gives

$$q_{i+1}(x,y,y)[\beta,\beta]m_{i+1}(y,y,y,x). \tag{9.9}$$

The case when $i$ is odd is similar. □

Part (1) of the lemma tells us that $q_n$ obeys half of Maltsev's equations. In the case when $\mathbf{A}$ is Abelian, we can take $\beta$ in part (2) to be $1_A$ and get the other half of the equations. Once we have the Maltsev operation, we can prove that the Abelian algebra is affine. Any ternary term satisfying the two properties above for $q_n$ is called a Gumm difference term. The Gumm difference term is all we need to conclude that any Abelian algebra in a congruence modular variety is congruence permutable. A weak difference term for a variety $\mathcal{V}$ is a term $d$ so that whenever $\theta$ is a congruence on an algebra in $\mathcal{V}$ and $a\theta b$, then

$$d(b,b,a)[\theta,\theta]a[\theta,\theta]d(a,b,b).$$

The presence of just a weak difference term would be enough to conclude that all Abelian algebras are affine. In [28], K. Kearnes and A. Szendrei prove that having a weak difference term is equivalent to a Maltsev condition. In fact, any variety in which congruence lattices satisfy a nontrivial lattice equation has such a term.

**Corollary 9.4** *(C. Herrmann [20]) If* $\mathbf{A}$ *is an Abelian algebra in a congruence modular variety, then any Gumm difference term of* $\mathbf{A}$ *is a Maltsev operation. In particular, every Abelian algebra in a congruence modular variety has permuting congruences.*

A little more generally:

**Corollary 9.5** *If* $\beta$ *is a congruence of an algebra* $\mathbf{A}$ *in a congruence modular variety and* $[\beta,\beta]=0_A$*, then every congruence of* $\mathbf{A}$ *permutes with* $\beta$*.*

**Proof** Suppose that $\beta$ is a congruence on $\mathbf{A}$ satisfying $[\beta,\beta]=0_A$ and $\alpha$ is any congruence on $\mathbf{A}$. We will prove that $\alpha\circ\beta=\beta\circ\alpha$. Suppose that $\langle x,z\rangle\in\beta\circ\alpha$. There is some $y\in\mathbf{A}$ with $x\beta y\alpha z$. Denote the Gumm difference term of $\mathbf{A}$ by $d$. Then $d(y,y,z)=z$ and since $[\beta,\beta]=0_A$, $d(x,y,y)=x$. Therefore,

$$x=d(x,y,y)\alpha d(x,y,z)\beta d(y,y,z)=z.$$

We have shown that $\beta\circ\alpha\subseteq\alpha\circ\beta$. It follows that $\alpha$ and $\beta$ commute as in the proof of Theorem 6.1. □

Before we prove that Abelian algebras in a congruence modular variety are affine, we need to know a few things about Abelian algebras with Maltsev terms.

**Definition 9.6** *Suppose that* $f(x_1,\dots,x_n)$ *and* $g(x_1,\dots,x_m)$ *are operations on a set* $A$*. Then* $f$ *and* $g$ *commute if they satisfy the equation*

$$\begin{aligned}&f(g(x_1^1,\dots,x_m^1),g(x_1^2,\dots,x_m^2),\dots,g(x_1^n,\dots,x_m^n))\\&=g(f(x_1^1,\dots,x_1^n),f(x_2^1,\dots,x_2^n),\dots,f(x_m^1,\dots,x_m^n)).\end{aligned}$$

Commutativity of operations can be viewed more easily using matrices. Consider an $m\times n$ matrix with entries from $A$:

$$\begin{pmatrix} x_1^1 & x_1^2 & \cdots & x_1^n \\ x_2^1 & x_2^2 & \cdots & x_2^n \\ & & \vdots & \\ x_m^1 & x_m^2 & \cdots & x_m^n \end{pmatrix}.$$

We could apply $g$ to each column of this matrix and then evaluate $f$ at the resulting vector, or we could evaluate $f$ along each row and apply $g$ to the result. If $f$ and $g$ commute, these will be the same.

**Definition 9.7** *A ternary Abelian group is an algebra with a single ternary basic operation which satisfies Maltsev's equations and commutes with itself.*

**Theorem 9.8** (H.-P. Gumm [13]) *Suppose that $\mathbf{A} = \langle A, d\rangle$ is an algebra with a single ternary basic operation. The following are equivalent.*

(1) $\mathbf{A}$ *is a ternary Abelian group.*

(2) *There is an Abelian group $\langle A, +, -, 0\rangle$ with universe $A$ so that $d(x, y, z) = x - y + z$.*

**Proof** If there is such a group, it is easy to check that $d(x, y, z) = x - y + z$ is a Maltsev operation which commutes with itself, so $\mathbf{A}$ is a ternary Abelian group. On the other hand, suppose that $\mathbf{A}$ is a ternary Abelian group. Let $0 \in A$ be arbitrary and define $x+y = d(x, 0, y)$ and $-x = d(0, x, 0)$. It is routine to check that these operations make $\langle A, +, -, 0\rangle$ an Abelian group and that $d(x, y, z) = x - y + z$. □

**Theorem 9.9** *The following are equivalent for any algebra $\mathbf{A}$.*

(1) $\mathbf{A}$ *is affine.*

(2) $\mathbf{A}$ *has a Maltsev polynomial and satisfies $C(1_A, 1_A; 0_A)$.*

(3) $\mathbf{A}$ *has a Maltsev polynomial which commutes with every polynomial operation of $\mathbf{A}$.*

(4) $\mathbf{A}$ *has a Maltsev term which commutes with every term operation of $\mathbf{A}$.*

(5) $\mathbf{A}$ *has a Maltsev term and is Abelian.*

**Proof** Suppose that $\mathbf{A}$ is affine. Then $\mathbf{A}$ is polynomially equivalent to a module. The proof that $C(1_A, 1_A; 0_A)$ can be gleaned from the discussion on modules in Section 5. Thus (1) → (2).

Suppose now that $\mathbf{A}$ has a Maltsev polynomial $m$ and that $C(1_A, 1_A; 0_A)$. We will prove that $m$ commutes with every polynomial operation of $\mathbf{A}$. Suppose that $t$ is an $(n + m)$-ary term of $\mathbf{A}$, $\mathbf{x}, \mathbf{y}, \mathbf{z} \in A^n$, and $\mathbf{c} \in A^m$. Then

$$m(t(\mathbf{y}, \mathbf{c}), t(\mathbf{y}, \mathbf{c}), t(\mathbf{z}, \mathbf{c})) = m(t(\mathbf{z}, \mathbf{c}), t(\mathbf{y}, \mathbf{c}), t(\mathbf{y}, \mathbf{c})).$$

Then

$$\begin{aligned} &m(t(m(\underline{y_0}, y_0, y_0), \ldots, m(\underline{y_{n-1}}, y_{n-1}, y_{n-1}), \mathbf{c}), t(\mathbf{y}, \mathbf{c}), t(\mathbf{z}, \mathbf{c})) \\ &= m(t(m(\underline{y_0}, y_0, z_0), \ldots, , m(\underline{y_{n-1}}, y_{n-1}, z_{n-1}), \mathbf{c}), t(\mathbf{y}, \mathbf{c}), t(\mathbf{y}, \mathbf{c})). \end{aligned}$$

Applying $C(1_A, 1_A; 0_A)$, we can replace the underlined variables with corresponding $x$'s to get

$$\begin{aligned} &m(t(m(\underline{x_0}, y_0, y_0), \ldots, m(\underline{x_{n-1}}, y_{n-1}, y_{n-1}), \mathbf{c}), t(\mathbf{y}, \mathbf{c}), t(\mathbf{z}, \mathbf{c})) \\ &= m(t(m(\underline{x_0}, y_0, z_0), \ldots, , m(\underline{x_{n-1}}, y_{n-1}, z_{n-1}), \mathbf{c}), t(\mathbf{y}, \mathbf{c}), t(\mathbf{y}, \mathbf{c})). \end{aligned}$$

Maltsev's equations now give

$$m(t(\mathbf{x},\mathbf{c}),t(\mathbf{y},\mathbf{c}),t(\mathbf{z},\mathbf{c})) = t(m(x_0,y_0,z_0),\ldots,,m(x_{n-1},y_{n-1},z_{n-1}),\mathbf{c}).$$

Thus $m$ commutes with any polynomial, so (2) $\to$ (3).

Now suppose that $\mathbf{A}$ has a Maltsev polynomial $m$ which commutes with every polynomial of $\mathbf{A}$. We know immediately that $m$ commutes with every term of $\mathbf{A}$ and with itself. We need only to prove that $m$ is a term operation of $\mathbf{A}$. Since $m$ is a polynomial of $\mathbf{A}$, there is a term operation $S$ of $\mathbf{A}$ and elements $a_1,\ldots,a_n \in A$ so that for any $x,y,z \in A$

$$m(x,y,z) = S(x,y,z,a_1,\ldots,a_n).$$

Let $x,y,z \in A$. We will express $m(x,y,z)$ as a term evaluated only at $x,y$, and $z$. Let $0 \in A$ be arbitrary and define $\alpha = S(0,0,0,y,\ldots,y)$. We have:

$$\begin{aligned}
m(x,y,z) &= m(m(x,y,z),m(0,0,0),m(\alpha,\alpha,0))\\
&= m(m(x,0,\alpha),m(y,0,\alpha),m(z,0,0))\\
&= m(m(x,0,\alpha),m(y,0,\alpha),z)\\
&= m(m(x,0,\alpha),m(m(y,0,\alpha),m(y,0,\alpha),m(y,0,\alpha)),\\
&\quad m(z,m(y,0,\alpha),m(y,0,\alpha)))\\
&= m(m(x,m(y,0,\alpha),z),m(0,m(y,0,\alpha),m(y,0,\alpha)),m(\alpha,\\
&\quad m(y,0,\alpha),m(y,0,\alpha)))\\
&= m(m(x,m(y,0,\alpha),z),0,\alpha)\\
&= m(m(x,m(m(y,y,y),m(0,0,0),\alpha),z),0,\alpha)\\
&= m(m(x,m(S(y,y,y,a_1,\ldots,a_n),S(0,0,0,a_1,\ldots,a_n),\\
&\quad S(0,0,0,y,\ldots,y)),z),0,\alpha)\\
&= m(m(x,S(m(y,0,0),m(y,0,0),m(y,0,0),m(a_1,a_1,y),\\
&\quad \ldots,m(a_n,a_n,y)),z),0,\alpha)\\
&= m(m(x,S(y,y,y,y,\ldots,y),z),0,\alpha)\\
&= m(S(x,S(y,y,y,y,\ldots,y),z,a_1,\ldots,a_n),S(0,0,0,a_1,\ldots,a_n),\\
&\quad S(0,0,0,y,\ldots,y)\\
&= S(m(x,0,0),m(S(y,y,y,y,\ldots,y),0,0),m(z,0,0),m(a_1,a_1,y),\\
&\quad \ldots,m(a_n,a_n,y))\\
&= S(x,S(y,y,y,y,\ldots,y),z,y,\ldots,y)\,.
\end{aligned} \tag{9.10}$$

Thus, $m$ is actually a term and we have established that (3) $\to$ (4).

Assume now that $\mathbf{A}$ has a Maltsev term $m$ which commutes with every term operation of $\mathbf{A}$. We will prove that $\mathbf{A}$ is affine. Let $0 \in A$ be arbitrary and define $x+y = m(x,0,x)$ and $-x = m(0,x,0)$. Then by Theorem 9.8, $\hat{\mathbf{A}} = \langle A,+,-,0\rangle$ is an Abelian group. We will define a ring $\mathbf{R}$ so that $\hat{\mathbf{A}}$ becomes an $\mathbf{R}$-module. Let $R$ be the set of all unary polynomials of $\mathbf{A}$ which fix the element 0. $R$ is nonempty since the unary projection operation and the constant 0 are both in $R$. Since $m$ commutes with the terms of $\mathbf{A}$ and is idempotent, $m$ also commutes with the polynomials of $\mathbf{A}$. Therefore, $m$ commutes with each $r \in R$. Since each $r \in R$ fixes 0, it follows that each $r$ is an endomorphism of $\hat{\mathbf{A}}$. Notice that $R$ is closed under the operations of the ring $\operatorname{End}\hat{\mathbf{A}}$. This is because $R$ contains the identity of $\operatorname{End}\hat{\mathbf{A}}$ (the unary projection) and the zero of $\operatorname{End}\hat{\mathbf{A}}$ (the constant 0), and because for each $r,s \in R$ the operations $r+s$, $-r$, and $rs = r\circ s$ are unary polynomials of $\mathbf{A}$ which fix 0. Thus $R$ is the universe of a subring $\mathbf{R}$ of $\operatorname{End}\hat{\mathbf{A}}$. Since $\mathbf{R} \subseteq \operatorname{End}\hat{\mathbf{A}}$, we have the natural structure of $\hat{\mathbf{A}}$ as an $\mathbf{R}$ module. We will

denote this module as ${}_{\mathbf{R}}\mathbf{A}$. We claim that $\mathbf{A}$ and ${}_{\mathbf{R}}\mathbf{A}$ are polynomially equivalent. We must show that $\operatorname{Pol}{}_{\mathbf{R}}\mathbf{A} = \operatorname{Pol}\mathbf{A}$. That $\operatorname{Pol}{}_{\mathbf{R}}\mathbf{A} \subseteq \operatorname{Pol}\mathbf{A}$ should be clear. We will prove inductively on rank that every polynomial $p(x_0, \dots, x_{n-1})$ of $\mathbf{A}$ is a polynomial of ${}_{\mathbf{R}}\mathbf{A}$. Suppose first that $p$ is a unary polynomial of $\mathbf{A}$. Let $r(x) = p(x) - p(0)$. Then $r$ is a unary polynomial of $\mathbf{A}$ which fixes 0 so $r \in \mathbf{R}$. Moreover, $p(x) = p(x) - p(0) + p(0) = r(x) + p(0)$. If $c = p(0)$, then $p(x) = rx + c$ is a polynomial of ${}_{\mathbf{R}}\mathbf{A}$ as desired. Next, assume that any $n$-ary polynomial of $\mathbf{A}$ is in $\operatorname{Pol}{}_{\mathbf{R}}\mathbf{A}$, and let $p$ be an $(n+1)$-ary polynomial of $\mathbf{A}$. Then

$$\begin{aligned} p(x_0, \dots, x_n) &= p(m(x_0, 0, 0), \dots, m(x_{n-1}, 0, 0), m(0, 0, x_n)) \\ &= m(p(x_0, \dots, x_{n-1}, 0), p(0, \dots, 0), p(0, \dots, 0, x_n)) \\ &= p(x_0, \dots, x_{n-1}, 0) - p(0, \dots, 0) + p(0, \dots, 0, x_n). \end{aligned} \tag{9.11}$$

Now, $p(x_0, \dots, x_{n-1}, 0)$ is an $n$-ary polynomial of $\mathbf{A}$, and $p(0, \dots, 0, x_n)$ is a unary polynomial of $\mathbf{A}$. As such, each of these is a polynomial of ${}_{\mathbf{R}}\mathbf{A}$. Since $p(0, \dots, 0)$ is a constant, this makes $p$ a polynomial of ${}_{\mathbf{R}}\mathbf{A}$. This proves that $\operatorname{Pol}{}_{\mathbf{R}}\mathbf{A} = \operatorname{Pol}\mathbf{A}$ and completes the proof that (4) $\to$ (1).

We have proven that (1) $-$ (4) are equivalent. It is easy to see that these combined are equivalent to (5). □

Suppose that $\mathbf{A}$ is an Abelian algebra in a congruence modular variety. Then $\mathbf{A}$ has a Maltsev term by Corollary 9.4. By the previous theorem, $\mathbf{A}$ is affine. On the other hand, any affine algebra is Abelian; so we have the *Fundamental Theorem of Abelian Algebras*:

**Theorem 9.10** (C. Herrmann [20]) *An algebra in a congruence modular variety is Abelian if and only if it is affine.*

This theorem has been extended by K. Kearnes and A. Szendrei [28] to the following.

**Theorem 9.11** *If a variety $\mathcal{V}$ satisfies a nontrivial lattice equation as a congruence equation, then the Abelian algebras in $\mathcal{V}$ are affine.*

A congruence modular variety in which every algebra is Abelian is termed an *Abelian variety* or an *affine variety*. In Sections 13 and 14, we will need some information about these varieties. We develop that information now without giving proofs (which in every case are easy and routine). For more detail on this topic, see R. Freese, R. McKenzie [12], Chapter IX.

**Definition 9.12** *Two varieties $\mathcal{V}$ and $\mathcal{W}$ are said to be polynomially equivalent if every algebra in each of the varieties is polynomially equivalent with an algebra in the other.*

Suppose that $\mathcal{A}$ is a congruence modular, Abelian variety. Let $d(x, y, z)$ be a Gumm term for $\mathcal{A}$ and let $\mathbf{F}$ be the free algebra on $\mathcal{A}$ freely generated by $\{x, y\}$. Let $R$ be the set of all $t(x, y) \in F$ such that $\mathbf{A} \models t(x, x) \approx x$. For $r = r(x, y)$ and $s = s(x, y)$ in $R$, put $r \circ s = r(s(x, y), y)$, $r + s = d(r(x, y), y, s(x, y))$, $-r = d(y, r(x, y), y)$, $0 = y$, $1 = x$. Then $\mathbf{R} = \langle R, +, \circ, 0, 1\rangle$ is a ring with unit and we have the *Fundamental Theorem of Affine Varieties*:

**Theorem 9.13** *If a variety $\mathcal{A}$ is congruence modular and Abelian, then $\mathcal{A}$ is polynomially equivalent with the variety ${}_{\mathbf{R}}\mathcal{M}$ of unitary left $\mathbf{R}$-modules where $\mathbf{R}$ is the ring of idempotent binary terms of $\mathbf{A}$ defined above.*

In fact, if $\mathbf{A} \in \mathcal{A}$, then the universe of $\mathbf{A}$ becomes an $\mathbf{R}$-module, denoted ${}_{\mathbf{R}}\mathbf{A}$, by choosing some element $a \in A$ and putting $0 = a$, $rb = r^{\mathbf{A}}(b, 0)$, $b + c = d^{\mathbf{A}}(b, 0, c)$, and $-b = d^{\mathbf{A}}(0, b, 0)$ for $\{b, c\} \subseteq A$ and $r \in R$. This module is, up to isomorphism, independent of the choice of 0 in $A$. The two algebras $\mathbf{A}$ and ${}_{\mathbf{R}}\mathbf{A}$ are polynomially equivalent. The Gumm term comes out to be $d^{\mathbf{A}}(x, y, z) = x - y + z$ (evaluated in the module). The passage from $\mathbf{A}$ to ${}_{\mathbf{R}}\mathbf{A}$ is generally many-to-one—i.e., ${}_{\mathbf{R}}\mathbf{A}_0 \cong {}_{\mathbf{R}}\mathbf{A}_1$ does not imply $\mathbf{A}_0 \cong \mathbf{A}_1$. But every $\mathbf{R}$-module occurs as ${}_{\mathbf{R}}\mathbf{A}$ for some $\mathbf{A} \in \mathcal{A}$.

Every algebra $\mathbf{A} \in \mathcal{A}$ is closely associated with an algebra $\mathbf{A}_\nabla$ with a one-element subalgebra (although $\mathbf{A}$ need not have any one-element subalgebra). Namely, $\mathbf{A}_\nabla = (\mathbf{A} \times \mathbf{A})/\Delta_{1,1}$ with $\Delta_{1,1}$ the congruence on $\mathbf{A} \times \mathbf{A}$ generated by $\{\langle\langle x, x\rangle, \langle y, y\rangle\rangle : \{x, y\} \subseteq A\}$. One verifies that if we choose $0 = a$ in ${}_{\mathbf{R}}\mathbf{A}$ and $0 = \langle a, a\rangle$ in ${}_{\mathbf{R}}(\mathbf{A} \times \mathbf{A})$, then ${}_{\mathbf{R}}(\mathbf{A} \times \mathbf{A}) = {}_{\mathbf{R}}\mathbf{A} \times {}_{\mathbf{R}}\mathbf{A}$. Since $\mathbf{A} \times \mathbf{A}$ and ${}_{\mathbf{R}}(\mathbf{A} \times \mathbf{A})$ have the same congruences (being polynomially equivalent), it is easily seen that $\Delta_{1,1} = \{\langle\langle x, y\rangle, \langle u, v\rangle\rangle \in A^2 \times A^2 : x - y = u - v\}$. Then ${}_{\mathbf{R}}\mathbf{A}_\nabla \cong {}_{\mathbf{R}}\mathbf{A}$ while $\mathbf{A}_\nabla$ has the one-element subalgebra $\nabla = \{\langle x, x\rangle : x \in A\}$.

## 10 Solvability and Nilpotence

We can use the commutator to extend the ideas of solvability and nilpotence to congruence modular varieties. Before we tackle this topic, we will derive H.-P. Gumm's Maltsev characterization of congruence modularity—which is (relatively) easy to do thanks to the Gumm difference term supplied by W. Taylor's equations.

**Theorem 10.1** (H.-P. Gumm [16]) *A variety $\mathcal{V}$ is congruence modular if and only if $\mathcal{V}$ has ternary terms $d_0, \ldots, d_n$ and $q$ satisfying*

$$\begin{array}{rcll} x & \approx & d_0(x, y, z) & \\ x & \approx & d_i(x, y, x) & \text{for all } i \\ d_i(x, x, z) & \approx & d_{i+1}(x, x, z) & \text{for even } i \\ d_i(x, z, z) & \approx & d_{i+1}(x, z, z) & \text{for odd } i \\ d_n(x, z, z) & \approx & q(x, z, z) & \\ q(x, x, z) & \approx & z\,. & \end{array}$$

**Proof** Suppose that $\mathcal{V}$ is a congruence modular variety, and let $q$ be a Gumm difference term for $\mathcal{V}$. Let $\mathbf{F}$ be the free algebra in $\mathcal{V}$ on the generators $\{x, y, z\}$. Let $\alpha = \mathrm{Cg}_{\mathbf{F}}(x, y)$, $\beta = \mathrm{Cg}_{\mathbf{F}}(y, z)$, and $\gamma = \mathrm{Cg}_{\mathbf{F}}(x, z)$. Then $\langle x, z\rangle \in \gamma \cap (\alpha \vee \beta)$. Now by the property of the difference term, $\langle x, q(x, z, z)\rangle \in [\gamma \cap (\alpha \vee \beta), \gamma \cap (\alpha \vee \beta)]$. However

$$\begin{array}{rcll} [\gamma \cap (\alpha \vee \beta), \gamma \cap (\alpha \vee \beta)] & \leq & [\gamma, \alpha \vee \beta] & \\ & = & [\gamma, \alpha] \vee [\gamma, \beta] & (10.1) \\ & \leq & (\gamma \cap \alpha) \vee (\gamma \cap \beta). & \end{array}$$

Thus $\langle x, d(x, z, z)\rangle \in (\gamma \cap \alpha) \vee (\gamma \cap \beta)$. This means there are $u_0, \ldots, u_n \in A$ with $u_0 = x$, $u_n = q(x, z, z)$, $u_i \alpha u_{i+1}$ if $i$ is even, $u_i \beta u_{i+1}$ if $i$ is odd, and $u_i \gamma u_{i+1}$ for all $i$. There are ternary terms $d_0, \ldots, d_n$ so that $u_i = d_i(x, y, z)$ for each $i$. Now, $x = d_0(x, y, z)$ holds by design. Define $f, g, h : \mathbf{F} \to \mathbf{F}$ to be the unique homomorphisms defined by

$$f(x) = f(y) = x, f(z) = z \tag{10.2}$$

$$g(x) = x, g(y) = g(z) = z \tag{10.3}$$

$$h(x) = h(z) = x, h(y) = y\,. \tag{10.4}$$

Then $\ker f = \alpha$, $\ker g = \beta$, and $\ker h = \gamma$. For any $i$, notice that

$$\begin{aligned} x &= d_0(x,y,x) \\ &= d_0(h(x),h(y),h(z)) \\ &= h(d_0(x,y,z)) \\ &= h(d_i(x,y,z)) \\ &= d_i(h(x),h(y),h(z)) \\ &= d_i(x,y,x). \end{aligned} \tag{10.5}$$

Suppose now that $i < n$ is even. Then

$$\begin{aligned} d_i(x,x,z) &= d_i(f(x),f(y),f(z)) \\ &= f(d_i(x,y,z)) \\ &= f(d_{i+1}(x,y,z)) \\ &= d_{i+1}(f(x),f(y),f(z)) \\ &= d_{i+1}(x,x,z). \end{aligned} \tag{10.6}$$

If $i < n$ is odd then

$$\begin{aligned} d_i(x,z,z) &= d_i(g(x),g(y),g(z)) \\ &= g(d_i(x,y,z)) \\ &= g(d_{i+1}(x,y,z)) \\ &= d_{i+1}(g(x),g(y),g(z)) \\ &= d_{i+1}(x,z,z). \end{aligned} \tag{10.7}$$

Finally, $d_n(x,z,z) = q(x,z,z)$ by design, and $q(x,x,z) = z$ since $q$ is a Gumm difference term. Since these terms satisfy these equations in $\mathbf{F}$, they satisfy the equations throughout $\mathcal{V}$.

Finally, assume that $\mathcal{V}$ has terms $d_0, \ldots, d_n, q$ satisfying the equations in (3). If $n$ were even, then the equations would imply that $d_{n-1}(x,z,z) \approx q(x,z,z)$ also, so we can assume that $n$ is odd. Define 4-ary terms $m_0, \ldots, m_{2n+2}$ in the following manner. $m_0(x,y,z,u) = x$ and

$$m_{2i-1}(x,y,z,u) = d_i(x,y,u) \text{ for } i \text{ odd} \tag{10.8}$$

$$m_{2i-1}(x,y,z,u) = d_i(x,z,u) \text{ for } i \text{ even} \tag{10.9}$$

$$m_{2i}(x,y,z,u) = d_i(x,z,u) \text{ for } i \text{ odd} \tag{10.10}$$

$$m_{2i}(x,y,z,u) = d_i(x,y,u) \text{ for } i \text{ even.} \tag{10.11}$$

Also, let $m_{2n+1} = q(y,z,u)$ and $m_{2n+2}(x,y,z,u) = u$. It is routine now to check that these are Day terms for $\mathcal{V}$. Hence $\mathcal{V}$ is congruence modular. □

H.-P. Gumm's Maltsev condition for congruence modularity may be viewed as a composition of B. Jónsson's condition for congruence distributivity and A.I. Maltsev's condition for congruence permutability. Notice that in the proof of Gumm's theorem, the term $q$ was chosen to be the difference term of $\mathcal{V}$. Thus every difference term has Gumm terms associated with it. On the other had, every $q$ arising from the Gumm terms is a difference term. Hence

**Theorem 10.2** *The following are equivalent for any ternary term $q$ in a variety $\mathcal{V}$.*

(1) *$\mathcal{V}$ is congruence modular; $\mathcal{V} \models q(x,x,y) \approx y$; and for all $\mathbf{A} \in \mathcal{V}$, for all $\beta \in \operatorname{Con}\mathbf{A}$, for all $\langle a,b\rangle \in \beta$, $\langle a, q(a,b,b)\rangle$ is in $[\beta,\beta]$.*

(2) *For this particular $q$, there exist ternary terms $d_0, \ldots, d_n$ satisfying Gumm's equations for congruence modularity.*

**Proof** All we need to prove is that if $d_0, \ldots, d_n, q$ are Gumm terms for a variety $\mathcal{V}$, then $q$ is a difference term. Suppose that $\beta$ is a congruence on an algebra $\mathbf{A}$ in $\mathcal{V}$ and that $a\beta b$ in $\mathbf{A}$. We only need to establish that $\langle a, q(a,b,b)\rangle \in [\beta,\beta]$ since the other equation is part of Gumm's equations. We will first establish $\langle d_i(a,b,b), d_i(a,a,b)\rangle \in [\beta,\beta]$ for all $i$. This is true by centrality since

$$\begin{pmatrix} d_i(a,b,a) & d_i(a,a,a) \\ d_i(a,b,b) & d_i(a,a,b) \end{pmatrix} = \begin{pmatrix} a & a \\ d_i(a,b,b) & d_i(a,a,b) \end{pmatrix} \tag{10.12}$$

is in $M(\beta,\beta)$. Next, we establish $\langle d_i(a,b,b), d_{i+1}(a,b,b)\rangle \in [\beta,\beta]$ for all $i$. If $i$ is odd, this is actually an equality, so there is nothing to show. If $i$ is even then

$$d_i(a,b,b)[\beta,\beta]d_i(a,a,b) = d_{i+1}(a,a,b)[\beta,\beta]d_{i+1}(a,b,b). \tag{10.13}$$

Now it follows that

$$a = d_0(a,b,b)[\beta,\beta]d_n(a,b,b) = q(a,b,b). \tag{10.14}$$

□

**Definition 10.3** *Suppose that $\beta$ is a congruence on an algebra $\mathbf{A}$ in a congruence modular variety. Define $(\beta]^0, (\beta]^1, (\beta]^2, \ldots$ recursively as follows. First, $(\beta]^0 = \beta$. Next, if $(\beta]^n$ is defined, then $(\beta]^{n+1} = [\beta, (\beta]^n]$. If $(\beta]^n = 0$ for some $n$, then $\beta$ is $n$-step nilpotent. If $1_A$ is $n$-step nilpotent, then $\mathbf{A}$ is also called $n$-step nilpotent. Also define the sequence $[\beta]^0$, $[\beta]^1$, $[\beta]^2, \ldots$ recursively by $[\beta]^0 = \beta$ and $[\beta]^{n+1} = [[\beta]^n, [\beta]^n]$. If $[\beta]^n = 0_A$ for some $n$, then $\beta$ is $n$-step solvable. If $1_A$ is $n$-step solvable, then $\mathbf{A}$ is also called $n$-step solvable.*

**Definition 10.4** *Suppose that $q$ is a Gumm difference term for a congruence modular variety $\mathcal{V}$. Define a sequence of ternary terms $q_0, q_1, q_2, \ldots$ recursively by $q_0 = q$ and $q_{n+1}(x,y,z) = q_0(x, q_n(x,y,y), q_n(x,y,z))$. We will call these terms generalized Gumm terms.*

**Theorem 10.5** (H.-P. Gumm [17]) *Suppose that $\alpha$ and $\beta$ are congruences on an algebra $\mathbf{A}$ in a congruence modular variety. Then $\alpha \circ \beta \subseteq [\alpha]^n \circ \beta \circ \alpha$ and $\alpha \circ \beta \subseteq (\alpha]^n \circ \beta \circ \alpha$ for all $n$.*

**Proof** We prove this by induction on $n$. For $n = 0$, $[\alpha]^n = \alpha$, so the inclusion is trivial. Suppose that the inclusion holds for $n \geq 0$ and suppose that $a\alpha b\beta c$. By our induction hypothesis, there are $x$ and $y$ so that $a[\alpha]^n x\beta y\alpha c$. Let $q$ be the Gumm difference term of $\mathbf{A}$. Then

$$\langle a, q(a,x,x)\rangle \in [[\alpha]^n, [\alpha]^n] \subseteq [\alpha]^{n+1}. \tag{10.15}$$

Therefore

$$a[\alpha]^{n+1} q(a,x,x)\beta q(a,x,y)\alpha q(x,x,c) = c \tag{10.16}$$

so $\langle a, c\rangle \in [\alpha]^{n+1} \circ \beta \circ \alpha$. The other claim in the theorem is proved similarly. □

If $\alpha$ is $n$-step solvable, then $[\alpha]^n = 0$, so this theorem gives $\alpha \circ \beta \subseteq \beta \circ \alpha$. It follows that $\alpha$ and $\beta$ permute (as in the proof of Theorem 6.1). Hence

**Corollary 10.6** *Suppose that $\alpha$ is an $n$-step solvable (or nilpotent) congruence of an algebra $\mathbf{A}$ in a congruence modular variety. Then $\alpha$ permutes with every congruence of $\mathbf{A}$.*

If $\mathbf{A}$ is $n$-step solvable, then every congruence on $\mathbf{A}$ is $n$-step solvable, so $\mathbf{A}$ has permuting congruences. Moreover, we can adapt the above proof using the generalized Gumm terms to manufacture a Maltsev term for $\mathbf{A}$ so that the entire variety generated by $\mathbf{A}$ has permuting congruences.

**Theorem 10.7** *Suppose that $\mathbf{A}$ is an algebra in a congruence modular variety with generalized Gumm terms $q_0, q_1, q_2, \ldots$. If $\mathbf{A}$ is $(n+1)$-step solvable (or nilpotent) for some $n$, then $\mathbf{A}$ has permuting congruences, and the term $q_n$ is a Maltsev term for $\mathbf{A}$.*

**Proof** Let $a, b \in \mathbf{A}$. We will first prove that $\langle a, q_k(a,b,b)\rangle \in [1_A]^{k+1}$ for all $k$. We proceed by induction on $k$. Since $q_0$ is a difference term and $\langle a, b\rangle \in 1_A$, we clearly have $\langle a, q_0(a,b,b)\rangle \in [1_A, 1_A] = [1_A]^1$. Now assume that $k \geq 0$ and that $\langle a, q_k(a,b,b)\rangle \in [1_A]^{k+1}$. Since $q_0$ is a difference term, $\langle a, q_0(a, q_k(a,b,b), q_k(a,b,b))\rangle \in [[1_A]^{k+1}, [1_A]^{k+1}] = [1_A]^{k+2}$, as desired. We have proved that $\langle a, q_k(a,b,b)\rangle \in [1_A]^{k+1}$ for all $k$. Since $[1_A]^{n+1} = 0_A$, this means that $a = q_n(a,b,b)$.

Next, we will prove by induction that $q_k(a,a,b) = b$ for all $k$. This is true for $k = 0$ since $q_0$ is a difference term. Assume that $k \geq 0$ and that $q_k(a,a,b) = b$. Then $q_{k+1}(a,a,b) = q_0(a, q_k(a,a,a), q_k(a,a,b)) = q_0(a,a,b) = b$. We have shown that $q_k(a,a,b) = b$ for all $k$. In particular $q_n(a,a,b) = b$.

We have proven that for arbitrary $a, b \in A$, $q_n(a,b,b) = a$ and $q_n(a,a,b) = b$. Therefore, $q_n$ is a Maltsev term for $\mathbf{A}$ and the result follows. The claim for nilpotence is proven in a similar manner. □

**Theorem 10.8** *The class of $n$-step solvable (nilpotent) algebras in a congruence modular variety $\mathcal{V}$ is a variety.*

**Proof** We prove the theorem for the case of nilpotence. Let $\mathcal{K}$ be the class of $n$-step nilpotent algebras in $\mathcal{V}$. We will prove that $\mathcal{K}$ is closed under homomorphic images, subalgebras, and products.

Suppose that $\mathbf{A} \in \mathcal{K}$ and that $f : \mathbf{A} \to \mathbf{B}$ is a surjective homomorphism with $\ker f = \pi$. We will prove by induction on $k$ that $(1_B]^k = f((1_A]^k \vee \pi)$ for all $k$. This is trivial for $k = 0$, so assume that $k \geq 0$ and that $(1_B]^k = f((1_A]^k \vee \pi)$. Then

$$\begin{aligned} (1_B]^{k+1} &= [1_B, (1_B]^k] \\ &= [f(1_A \vee \pi), f((1_A]^k \vee \pi)] \\ &= f([1_A, (1_A]^k] \vee \pi) \\ &= f((1_A]^{k+1} \vee \pi). \end{aligned} \tag{10.17}$$

It now follows that $(1_B]^n = f((1_A]^n \vee \pi) = f(\pi) = 0_B$ so $\mathbf{B}$ is $n$-step nilpotent and is in $\mathcal{K}$.

Next, suppose that $\mathbf{A} \in \mathcal{K}$ and that $\mathbf{B}$ is a subalgebra of $\mathbf{K}$. For any congruences $\alpha, \beta, \delta \in \operatorname{Con}\mathbf{A}$, it should be clear that $C(\alpha, \beta; \delta)$ (in $\mathbf{A}$) implies that $C(\alpha \cap B^2, \beta \cap B^2; \delta \cap B^2)$ (in $\mathbf{B}$). Therefore $[\alpha \cap B^2, \beta \cap B^2] \subseteq [\alpha, \beta] \cap B^2$. It follows that $(1_B]^n \subseteq (1_A]^n \cap B^2 = 0_B$, so $\mathbf{B}$ is $n$-step nilpotent and $\mathbf{B} \in \mathcal{K}$.

Finally, suppose that $\{\mathbf{A}_i : i \in I\} \subseteq \mathcal{K}$. Let $\mathbf{B} = \prod_{i \in I} \mathbf{A}_i$. Let $\pi_i : \mathbf{B} \to \mathbf{A}_i$ be the canonical projection and let $\eta_i = \ker \pi_i$. As we showed above, $\pi_i((1_B]^n \vee \eta_i) = (1_A]^n = 0_A$.

Thus, $(1_B]^n \subseteq \eta_i$ for all $i$. Therefore, $(1_B]^n = 0_B$. Thus $\mathbf{B}$ is $n$-step nilpotent and is in $\mathcal{K}$. This finishes the proof that $\mathcal{K}$ is a variety. The proof of the theorem for solvable algebras is similar. □

To prove the next lemma, we need the following commutativity result.

**Lemma 10.9** *Suppose that $\alpha$ and $\delta$ are congruence on an algebra $\mathbf{A}$ with a Maltsev term $m$ and that $C(\alpha, 1_A; \delta)$. If $\mathbf{a}, \mathbf{b}, \mathbf{c} \in A^3$ with $a_i \alpha b_i$ for all $i$ then*

$$m(m(a_0, b_0, c_0), m(a_1, b_1, c_1), m(a_2, b_2, c_2))\delta m(m(a_0, a_1, a_2), m(b_0, b_1, b_2), m(c_0, c_1, c_2)) . \tag{10.18}$$

**Proof** Maltsev's equations give us

$$m(m(b_0, b_1, b_2), m(b_0, b_1, b_2), m(c_0, c_1, c_2)) = m(m(c_0, c_1, c_2), m(b_0, b_1, b_2), m(b_0, b_1, b_2)) .$$

We expand the first subterm of each side of this equality to get

$$m(m(m(\underline{b_0}, b_0, b_0), m(\underline{b_1}, b_1, b_1), m(\underline{b_2}, b_2, b_2)), m(b_0, b_1, b_2), m(c_0, c_1, c_2))$$

$$= m(m(m(\underline{b_0}, b_0, c_0), m(\underline{b_1}, b_1, c_1), m(\underline{b_2}, b_2, c_2)), m(b_0, b_1, b_2), m(b_0, b_1, b_2)) .$$

By centrality, we can replace the underlined $b_i$'s with corresponding $a_i$'s and maintain equivalence modulo $\delta$ so that

$$m(m(m(\underline{a_0}, b_0, b_0), m(\underline{a_1}, b_1, b_1), m(\underline{a_2}, b_2, b_2)), m(b_0, b_1, b_2), m(c_0, c_1, c_2))$$

$$\delta m(m(m(\underline{a_0}, b_0, c_0), m(\underline{a_1}, b_1, c_1), m(\underline{a_2}, b_2, c_2)), m(b_0, b_1, b_2), m(b_0, b_1, b_2)) .$$

Maltsev's equations now give

$$m(m(a_0, a_1, a_2), m(b_0, b_1, b_2), m(c_0, c_1, c_2)) \ \delta \ m(m(a_0, b_0, c_0), m(a_1, b_1, c_1), m(a_2, b_2, c_2)) .$$

□

**Lemma 10.10** *Suppose that $\mathbf{A}$ is an $n$-step nilpotent algebra with a Maltsev term $m$. There are ternary terms $l$ and $r$ so that for all $b, c \in A$ the function $l(-, b, c)$ is the inverse of $m(-, b, c)$ and the function $r(-, b, c)$ is the inverse of $m(c, b, -)$.*

**Proof** We will prove the existence of $l$. The existence of $r$ is similar. We will prove this by induction on $n$. If $n = 0$, then $\mathbf{A}$ is trivial. If $n = 1$, then $\mathbf{A}$ is Abelian. For any $x \in \mathbf{A}$, Define $u +_x v = m(u, x, v)$ and $-_x u = m(x, u, x)$ for all $u, v \in \mathbf{A}$. Then by Theorem 9.8 these operations define an Abelian group on $A$ with identity $x$ so that $m(u, v, w) = u -_x v +_x w$. For any $b, c \in A$, the inverse of $m(x, b, c) = x -_x b +_x c$ is clearly $l(x, b, c) = x -_x c +_x b = m(x, c, b)$.

Next suppose that $n \geq 1$ and that the lemma holds for $n$-step nilpotent algebras. Suppose that $\mathbf{A}$ is $(n + 1)$-step nilpotent. Let $\theta = (1_A]^n$. Then $C(1_A, \theta; 0)$, and $A/\theta$ is $n$-step nilpotent. By our induction hypothesis, there is a term $l'$ so that $l'(-, b/\theta, c/\theta)$ is the inverse of $m(-, b/\theta, c/\theta)$ for all $b, c, \in A$. Let $l(y, b, c) = m(m(y, m(l'(y, b, c), b, c), y), y, l'(y, b, c))$. We

will show that $l$ is the desired term. Let $y, b, c \in A$. Let $z = l'(y, b, c)$. By our choice of $l'$, we know at least that $m(z, b, c)\theta y$. Then

$$\begin{aligned} m(l(y,b,c),b,c) &= m(m(m(y,m(z,b,c),y),y,z),m(y,y,b),m(y,y,c)) \\ &= m(m(m(y,m(z,b,c),y),y,y),m(y,y,y),m(z,b,c)) \\ &= m(m(y,m(z,b,c),y),y,m(z,b,c)) \end{aligned} \tag{10.19}$$

where the second equality follows from Lemma 10.9 since $m(z, b, c)\theta y$ and since $C(\theta, 1_A; 0)$. The set $y/\theta$ is closed under $m$ since $m$ is idempotent, and by Lemma 10.9 $m$ commutes with itself on this $\theta$ block. Define $u +_y v = m(u, y, v)$ and $-_y u = m(y, u, y)$ on $y/\theta$. By Theorem 9.8, these are Abelian group operations on $y/\theta$ with $y$ as an identity. Then we can continue our calculations to see

$$\begin{aligned} m(l(y,b,c),b,c) &= m(m(y,m(z,b,c),y),y,m(z,b,c)) \\ &= -_y m(z,b,c) +_y m(z,b,c) \\ &= y\,. \end{aligned} \tag{10.20}$$

Now we look at the composition in the reverse order. Let $z = l'(m(y, b, c), b, c)$. Then $z\theta y$ and

$$\begin{aligned} l(m(y,b,c),b,c) &= m(m(m(y,b,c),m(z,b,c),m(y,b,c)),m(y,b,c),z) \\ &= m(m(m(y,z,y),m(b,b,b),m(c,c,c)),m(y,b,c),z) \\ &= m(m(m(y,z,y),b,c),m(y,b,c),z) \\ &= m(m(m(y,z,y),b,c),m(y,b,c),m(y,y,z)) \\ &= m(m(m(y,z,y),y,y),m(b,b,y),m(c,c,z)) \\ &= m(m(y,z,y),y,z) \\ &= -_y z +_y z \\ &= y. \end{aligned} \tag{10.21}$$

Note that the second and fifth equalities follow from Lemma 10.9 since $z\theta y$. □

The real mechanics of this proof are hidden from sight, but there is an elegant structure to these algebras. The Maltsev term $m$ gives each block of $\theta$ the structure of a ternary Abelian group. For any $b, c \in A$, the functions $m(-, b, c) : b/\theta \to c/\theta$ and $m(-, c, b) : c/\theta \to b/\theta$ are inverse isomorphisms of these group structures which exchange $b$ and $c$, so all of the blocks are isomorphic to a ternary Abelian group $\mathbf{G}$. The algebra $\hat{\mathbf{A}} = \langle A, m\rangle$ is a sort of semi-direct product of $\hat{\mathbf{A}}/\theta$ and $\mathbf{G}$. To find the term $l$, we try to solve the equation $m(x, b, c) = y$ for $x$, assuming that there is a solution $z$ modulo $\theta$. To solve this equation, we use the isomorphisms $m(-, b, y)$, $m(-, c, y)$, and $m(-, z, y)$ to map everything into $y/\theta$. Then we can treat $y/\theta$ as an Abelian group with identity $y$ to solve the new equation. The nature of the semi-direct product is such that when we pull this solution back to $z/\theta$ using $m(-, y, z)$ we have a solution to the original equation.

More generally, if $\alpha$ is any congruence on $\mathbf{A}$ and $b, c \in A$ then the maps $m(-, b, c) : b/\alpha \to c/\alpha$ and $m(-, c, b) : c/\alpha \to b/\alpha$ may not be inverses, but they are both injective. Hence the congruence classes are the same size. Thus

**Corollary 10.11** *Any $n$-step nilpotent algebra in a congruence modular variety has uniform congruences.*

Suppose that $a, b$ and $c$ are elements of an $n$-step nilpotent algebra $\mathbf{A}$ in a congruence modular variety with Maltsev term $m$ and that $\theta \in \operatorname{Con}\mathbf{A}$. If $a\theta b$, then $m(a,b,c)\theta m(b,b,c) = c$ so $m(a,b,c)\theta c$. On the other hand, if $m(a,b,c)\theta c$, then $a = l(m(a,b,c),b,c)\theta l(c,b,c)$. However, $m(l(c,b,c),b,c) = c = m(b,b,c)$, so by Lemma 10.10 $l(c,b,c) = b$. This means that $a\theta b$. We have that $a\theta b$ if and only if $m(a,b,c)\theta c$. This means that $\theta$ consists precisely of those pairs $\langle a,b\rangle$ for which $m(a,b,c) \in c/\theta$. Hence, $\theta$ is uniquely determined by any equivalence class $c/\theta$. Thus

**Corollary 10.12** *Any $n$-step nilpotent algebra in a congruence modular variety has regular congruences.*

Suppose now that $\mathbf{A}$ is an $n$-step nilpotent algebra in a congruence modular variety. Let $l$ and $r$ be the terms guaranteed by the previous lemma and let $0 \in A$ be arbitrary. Now define these operations on $A$

$$\begin{aligned} u \cdot v &= m(u,0,v) \\ u/v &= l(u,0,v) \\ u\backslash v &= r(u,0,v). \end{aligned} \tag{10.22}$$

Then these are the multiplication and division operations of a loop on $A$. Hence

**Theorem 10.13** *Suppose that $\mathbf{A}$ is an $n$-step nilpotent algebra in the congruence modular variety $\mathcal{V}$. There is a loop operation in* $\operatorname{Pol}\mathbf{A}$ *whose left and right division operations are also in* $\operatorname{Pol}\mathbf{A}$.

# 11 Applications

We briefly describe here some of the important results that have been achieved through the application of commutator theory in the study of basic questions about varieties. We make no attempt at completeness.

In 1979 there appeared the paper J. Hagemann, C. Herrmann [19], which provided the first proofs of much of the basic commutator theory we have developed in the preceeding sections, and the same year appeared H.-P. Gumm, C. Herrmann [18] in which the new theory was applied to obtain new cancellation, refinement and uniqueness results for direct products of algebras in congruence modular varieties. H.-P Gumm and C. Herrmann proved, among other results, that if $\mathbf{A} \times \mathbf{B} \cong \mathbf{A} \times \mathbf{C}$ and if $\mathbf{A} \times \mathbf{B}$ belongs to a congruence modular variety, and if the congruence lattice of $\mathbf{A}$ has the ascending chain condition and the center of $\mathbf{A}$ is a congruence of "finite rank", then $\mathbf{B}$ is "affine-isotopic" to $\mathbf{C}$.

In 1981 appeared R. Freese, R. McKenzie [11] in which commutator theory was used to show that every residually small congruence modular variety $\mathcal{V}$ obeys a certain commutator law (C1), which must hold in the congruence lattice of every algebra of $\mathcal{V}$ augmented by the commutator operation. Conversely, if $\mathcal{V}$ is congruence modular and generated by a finite algebra $\mathbf{A}$ and if $\mathbf{A}$, along with all of its subalgebras, obeys (C1) then $\mathcal{V}$ is residually small, in fact has a finite residual bound.

Also in 1981 appeared a monograph by S. Burris and R. McKenzie [4], containing a proof that every locally finite congruence modular variety with decidable first-order theory must decompose as the varietal product of two subvarieties, a decidable affine variety and a decidable discriminator variety. Commutator theory was the essential tool for this work.

The authors also provided an algorithm which can be used to reduce the question whether HSP($\mathbf{A}$) has decidable theory, where $\mathbf{A}$ is a given finite algebra, (the decidability problem) to the question whether the variety of $\mathbf{R}$-modules has decidable theory, where $\mathbf{R}$ is a certain finite ring correlated with $\mathbf{A}$, produced by the algorithm. The problem to characterize in some fashion those finite $\mathbf{A}$ for which the class of finite members of HSP($\mathbf{A}$) has decidable theory (the finite decidability problem) seems to be much more difficult than the decidability problem. In 1997, P. M. Idziak [22] provided a solution to the finite decidability problem for finite algebras in congruence modular varieties. His result is equally as satisfactory as the result of S. Burris and R. McKenzie, but is rather more difficult to state.

In 1982 appeared R. McKenzie [32] which used commutator theory to characterize the locally finite varieties having a finite bound on the cardinalities of their finite directly indecomposable members (the "directly representable" varieties). A breakthrough result achieved in the paper was the fact that every directly representable variety has permuting congruences.

The 1987 monograph R. Freese, R. McKenzie [12], which has been the principal source for the first ten sections of this text, contains the result (Chapter XIV) that any finite nilpotent algebra of finite type (i.e., which possesses only finitely many basic operations) which lies in a congruence modular variety and decomposes as the direct product of algebras of prime-power orders, has a finitely axiomatizable equational theory. R. McKenzie [33] proves that any finite algebra $\mathbf{F}$ belonging to a residually small congruence modular variety of finite type has a finitely axiomatizable equational theory. A main ingredient in this proof is the demonstration that $\mathbf{F}$ obeys finitely many equations which collectively imply that an algebra (which satisfies them) satisfies the commutator equation (C1) discovered by R. Freese and R. McKenzie.

In 1989 appeared K. A. Kearnes [26] which used commutator theory to prove that every residually small, congruence modular variety with the amalgamation property possesses the congruence extension property. Whether the words "congruence modular" can be removed from this result is unknown.

In 1996, P. M. Idziak and J. Berman began a study of the "generative complexity" of locally finite varieties. They define the generative complexity, or G-function, of a variety $\mathcal{V}$ to be the function $\mathrm{G}_{\mathcal{V}}$ defined for all positive integers $n$ so that $\mathrm{G}_{\mathcal{V}}(n)$ is the number of non-isomorphic $n$-generated algebras in $\mathcal{V}$. Perhaps their deepest result is a characterization of finitely generated congruence modular varieties $\mathcal{V}$ for which $\mathrm{G}_{\mathcal{V}}(n) \leq 2^{cn}$ (for all $n \geq 1$) for some constant $c$. The characterization is of the same order as P. M. Idziak's characterization of finite decidability for HSP($\mathbf{A}$) but even more complicated. A much easier result of P. M. Idziak and R. McKenzie [23] will be proved in Section 14 below; namely, a locally finite congruence modular variety $\mathcal{V}$ satisfies $\mathrm{G}_{\mathcal{V}}(n) \leq n^c$ (for all $n \geq 1$), for a constant $c$, iff $\mathcal{V}$ is Abelian and directly representable.

Perhaps this is the appropriate place to mention the tame congruence theory of D. Hobby, R. McKenzie [21]. With this theory, it became possible to extend most of the above-mentioned results that deal with finite algebras or locally finite varieties, either to all finite algebras and all locally finite varieties, or to a domain much broader than congruence modular varieties. Sometimes, tame congruence theory simply produces the result that every locally finite variety possessing a certain property must be congruence modular. For instance, it is proved in [21], Chapter 10 that every residually small locally finite variety that satisfies any non-trivial congruence equation must be congruence modular (i.e., must satisfy the modular law as a congruence equation).

In the book R. McKenzie, M. Valeriote [34] it is proved that every locally finite variety with decidable first-order theory decomposes as the varietal product of three decidable subvarieties: an affine variety, a discriminator variety and a combinatorial variety. This result contains the result proved five years earlier by S. Burris and R. McKenzie for congruence modular varieties. In the modular case, the combinatorial variety must consist just of one-element algebras.

P. M. Idziak, R. McKenzie and M. Valeriote [24] (unpublished) have extended the above-mentioned result of P. M. Idziak and R. McKenzie into a characterization of all locally finite varieties $\mathcal{V}$ with the property that $\mathrm{G}_{\mathcal{V}}(n) \leq n^c$ for all $n \geq 1$, for some constant $c$. Such a variety is a varietal product of an affine, directly representable, subvariety and a very special kind of combinatorial subvariety.

Successful applications of tame congruence theory, like those mentioned in the two previous paragraphs, have frequently begun with the idea to attempt an extension of results proved earlier for locally finite congruence modular varieties with the help of commutator theory. Tame congruence theory is a powerful tool for such efforts but, unlike modular commutator theory, its application appears to be essentially restricted to the realm of locally finite varieties.

## 12 Residual Smallness

An algebra $\mathbf{A}$ is called subdirectly irreducible if it has a smallest non-zero congruence, (called the monolith of $\mathbf{A}$). According to a theorem of G. Birkhoff, every algebra can be embedded into a product, $\prod_{t\in T} \mathbf{S}_t$, of subdirectly irreducible algebras $\mathbf{S}_t$ in such a way that it projects onto each factor $\mathbf{S}_t$ (subdirect embedding).

**Definition 12.1** *A variety $\mathcal{V}$ is residually small if there is a cardinal bound on the size of subdirectly irreducible algebras in $\mathcal{V}$. If $\mathcal{V}$ is residually small, then we will write* $\mathrm{resb}(\mathcal{V})$ *for the least cardinal $\kappa$ such that every subdirectly irreducible algebra in $\mathcal{V}$ has cardinality less than $\kappa$. If the cardinalities of subdirectly irreducible algebras in $\mathcal{V}$ have no cardinal upper bound, then we write* $\mathrm{resb}(\mathcal{V}) = \infty$*, and say that $\mathcal{V}$ is residually large. For an algebra $\mathbf{A}$, we put* $\mathrm{resb}(\mathbf{A}) = \mathrm{resb}(\mathrm{HSP}(\mathbf{A}))$*. A variety $\mathcal{V}$ will be called residually finite if* $\mathrm{resb}(\mathcal{V}) \leq \aleph_0$*. A residual bound for $\mathcal{V}$ is any cardinal $\kappa \geq \mathrm{resb}(\mathcal{V})$.*

R. W. Quackenbush [42] proved that if a locally finite variety has an infinite subdirectly irreducible algebra, then it has unboundedly large finite subdirectly irreducible algebras. He posed the question, "Does every finitely generated residually finite variety have a finite residual bound?" While in general the answer to this question is no (R. McKenzie [35]), the answer is affirmative for finite algebras in congruence modular varieties (R. Freese and R. McKenzie [11]). Moreover, the class of finite algebras $\mathbf{A}$ in congruence modular varieties for which $\mathrm{HSP}(\mathbf{A})$ is residually finite is defined by a commutator equation. This equation, which takes the form $x \wedge [y, y] \leq [x, y]$, is called (C1). Notice that (C1) is equivalent to $x \wedge [y, y] = [x \wedge y, y]$, as can be proved by substituting $x \wedge y$ for $x$.

**Theorem 12.2** *Suppose that $\mathbf{A}$ is a finite algebra and that* $\mathrm{HSP}(\mathbf{A})$ *is congruence modular. The following are equivalent.*

(1) $\mathrm{resb}(\mathbf{A}) < \infty$.

(2) $\mathrm{resb}(\mathbf{A})$ *is a positive integer.*

(3) $\mathrm{HSP}(\mathbf{A}) \models_{\mathrm{Con}} (\alpha \wedge [\beta,\beta] \leq [\alpha,\beta])$.

(4) $\mathrm{S}(\mathbf{A}) \models_{\mathrm{Con}} (\alpha \wedge [\beta,\beta] \leq [\alpha,\beta])$.

**Proof** The implications (3) $\to$ (4) and (2) $\Rightarrow$ (1) are trivial. We will prove that (4) implies the validity of (C1) in finite algebras of $\mathrm{HSP}(\mathbf{A})$, and that this in turn implies (2). Finally, we shall prove that (1) $\Rightarrow$ (3).

To begin, suppose that $\mathrm{S}(\mathbf{A}) \models$ (C1). Let $\mathbf{B}$ be any finite algebra in $\mathrm{HSP}(\mathbf{A})$. There is a positive integer $n$, a subalgebra $\mathbf{D}$ of $\mathbf{A}^n$, and a congruence $\theta$ on $\mathbf{D}$ such that $\mathbf{B}$ is isomorphic to $\mathbf{D}/\theta$. First, we show that $\mathbf{D} \models$ (C1); then using that, we show that $\mathbf{B} \models$ (C1). So let $\{\alpha,\beta\} \subseteq \mathrm{Con}\,\mathbf{D}$. We write $\eta_i$ for the kernel of the $i$th projection homomorphism of $\mathbf{D}$ into $\mathbf{A}$, so that $\mathbf{D}/\eta_i \in \mathrm{S}(\mathbf{A})$.

To get a contradiction, we assume that $\alpha \wedge [\beta,\beta] \neq [\alpha \wedge \beta, \beta]$. This means that $\alpha \wedge [\beta,\beta] > [\alpha \wedge \beta, \beta]$. Since $\mathbf{D}/\eta_0 \models$ (C1), using statement (6) of Theorem 8.3, we have that

$$[\alpha \wedge \beta, \beta] \vee \eta_0 = [(\alpha \wedge \beta) \vee \eta_0, \beta \vee \eta_0] \vee \eta_0 = ((\alpha \wedge \beta) \vee \eta_0) \wedge ([\beta \vee \eta_0, \beta \vee \eta_0] \vee \eta_0)\,;$$

which gives that

$$[\alpha \wedge \beta, \beta] \vee \eta_0 \geq \alpha \wedge \beta \wedge [\beta,\beta] = \alpha \wedge [\beta,\beta]\,. \tag{12.1}$$

Modularity of $\mathrm{Con}\,\mathbf{D}$ thus implies that

$$\eta_0 \wedge \alpha \wedge [\beta,\beta] > \eta_0 \wedge [\alpha \wedge \beta, \beta] \geq [\eta_0 \wedge \alpha \wedge \beta, \beta]\,.$$

Replacing $i = 0$ by $i = 1$ and $\alpha$ by $\eta_0 \wedge \alpha$ in this argument, leads to

$$\eta_1 \wedge \eta_0 \wedge \alpha \wedge [\beta,\beta] > [\eta_1 \wedge \eta_0 \wedge \alpha \wedge \beta, \beta]\,. \tag{12.2}$$

Continuing in this fashion, we eventually reach the conclusion that

$$\bigwedge_{i<n} \eta_i \wedge \alpha \wedge [\beta,\beta] > [\bigwedge_{i<n} \eta_i \wedge \alpha \wedge \beta, \beta]\,,$$

which is absurd since $\bigwedge_{i<n} \eta_i = 0_D$. This contradiction establishes that $\alpha \wedge [\beta,\beta] = [\alpha \wedge \beta, \beta]$. Thus $\mathbf{D} \models$ (C1).

Now to see that $\mathbf{B} \cong \mathbf{D}/\theta$ satisfies (C1), let $\{\alpha,\beta\} \subseteq \mathrm{Con}\,\mathbf{D}$ with $\alpha \wedge \beta \geq \theta$. By Theorem 8.3, statement (6), what we need to show is that $\alpha \wedge ([\beta,\beta] \vee \theta) = [\alpha \wedge \beta, \beta] \vee \theta$. Since $\mathbf{D} \models$ (C1), and $\alpha \geq \theta$, we have that

$$\alpha \wedge ([\beta,\beta] \vee \theta) = (\alpha \wedge [\beta,\beta]) \vee \theta = [\alpha \wedge \beta, \beta] \vee \theta\,,$$

as required.

Next, suppose that all the finite algebras in $\mathrm{HSP}(\mathbf{A})$ satisfy (C1). If $\mathrm{HSP}(\mathbf{A})$ had an infinite subdirectly irreducible algebra, then the variety would contain arbitrarily large finite subdirectly irreducible algebras by [42]. Therefore, we need only find a finite bound on the size of the finite subdirectly irreducible algebras in the variety generated by $\mathbf{A}$. Let $\mathbf{B}$ be a finite subdirectly irreducible algebra in the variety generated by $\mathbf{A}$. Choose a positive integer $n$, a subalgebra $\mathbf{D}$ of $\mathbf{A}^n$, and a congruence $\theta$ on $\mathbf{D}$ with $\mathbf{B}$ isomorphic to $\mathbf{D}/\theta$. Let $\beta$ be the monolith of $\mathbf{B}$.

By additivity of the commutator, $\mathbf{B}$ has a largest congruence $\zeta$ such that $[\zeta, \beta] = 0_B$. We will prove that $\mathbf{B}/\zeta \in \mathrm{HS}(\mathbf{A})$. Let $\alpha \in \mathrm{Con}\,\mathbf{D}$ be the congruence of $\mathbf{D}$ corresponding to $\zeta$ via the isomorphism of $\mathbf{B}$ with $\mathbf{D}/\theta$, and $\theta'$ be the congruence of $\mathbf{D}$ corresponding to $\beta$. (So that $\theta'$ is the unique cover of $\theta$.) By our choice of $\zeta$, $\alpha$ is the largest congruence in $\mathrm{Con}\,\mathbf{D}$ with $[\alpha, \theta'] \leq \theta$. For each $i = 0, \ldots, n-1$, let $\eta_i$ be the kernel of the projection of $\mathbf{D}$ to the $i^{th}$ coordinate. We will prove that there is some $i$ so that $\eta_i \leq \alpha$. This will show that $\mathbf{B}/\zeta \cong \mathbf{D}/\alpha \in \mathrm{HS}(\mathbf{A})$. We do so by contradiction. Suppose that $\eta_i \not\leq \alpha$ for all $i$. By our choice of $\alpha$, this means that $[\theta', \eta_i] \not\leq \theta$ for all $i$. It follows that for all $i$, $[\theta', \eta_i] \vee \theta$ is strictly larger than $\theta$ but contained in $\theta'$. Hence, $[\theta', \eta_i] \vee \theta = \theta'$. If we substitute $[\theta', \eta_0] \vee \theta$ for $\theta'$ in $\theta' = [\theta', \eta_1] \vee \theta$, we get

$$\begin{array}{rcl} \theta' & = & [([\theta', \eta_0] \vee \theta), \eta_1] \vee \theta \\ & \leq & [(\theta' \cap \eta_0) \vee \theta, \eta_1] \vee \theta \\ & = & [(\theta' \cap \eta_0), \eta_1] \vee [\theta, \eta_1] \vee \theta \\ & \leq & (\theta' \cap \eta_0 \cap \eta_1) \vee \theta. \end{array} \tag{12.3}$$

Since the reverse inclusion is also true, we actually have $\theta' = (\theta' \cap \eta_0 \cap \eta_1) \vee \theta$. By substituting this result into the equation $\theta' = [\theta', \eta_2] \vee \theta$, we similarly find that $\theta' = (\theta' \cap \eta_0 \cap \eta_1 \cap \eta_2) \vee \theta$. Proceeding inductively, repeatedly applying this argument, we eventually obtain that $\theta' = (\theta' \wedge \bigwedge_{0 \leq i < n} \eta_i) \vee \theta$. This means that $\theta' = \theta$, which is the desired contradiction. The assumption that $\eta_i \not\leq \alpha$ for all $i$ must be false, as we claimed.

Now $\mathbf{B}/\zeta \in \mathrm{HS}(\mathbf{A})$ implies $|\mathbf{B}/\zeta| \leq |\mathbf{A}|$. We shall conclude this proof that (4) $\rightarrow$ (2) by demonstrating that each $\zeta$-class is no larger than $2^M$ where $M$ is the cardinality of the free algebra in $\mathrm{HSP}(\mathbf{A})$ on $|A| + 2$ generators. This will prove that $|\mathbf{B}| \leq |\mathbf{A}| \cdot 2^M$.

Next, we observe that $[\zeta, \zeta] = 0_B$, equivalently, $[\alpha, \alpha] \leq \theta$. This is true because $\mathbf{D} \models$ (C1), so that $\theta' \wedge [\alpha, \alpha] \leq [\theta', \alpha] \leq \theta$. But if $[\alpha, \alpha] \not\leq \theta$, then $\theta' \leq [\alpha, \alpha] \vee \theta$, giving that $\theta' = (\theta' \wedge [\alpha, \alpha]) \vee \theta = \theta$ by modularity, a contradiction. Thus $[\zeta, \zeta] = 0_B$.

Denote the Gumm difference term of $\mathrm{HSP}(\mathbf{A})$ by $q$. Since $[\zeta, \zeta] = 0$, we know that the restriction of $q$ to any $\zeta$-class is a Maltsev operation, and gives that set the structure of a ternary Abelian group. Select $\langle 0, b \rangle \in \beta - 0_B$, and let $+$ and $-$ denote the Abelian group operations on $0/\zeta$ with neutral element 0 induced by $q$. Letting $u$ be any element of $\mathbf{B}$, we now proceed to prove that $|u/\zeta| \leq 2^M$. Suppose that $x, y \in u/\zeta$ and $x \neq y$. Since $\beta$ is the monolith of $\mathbf{B}$, $\langle 0, b \rangle \in \mathrm{Cg}_{\mathbf{B}}(x, y)$. This means that there are elements $v_0 = 0, v_2, \ldots, v_k = b$ and unary polynomials $p_0, \ldots, p_{k-1}$ so that $\{p_i(x), p_i(y)\} = \{v_i, v_{i+1}\}$ for all $i$. We can apply the difference term $q$ and manipulate its local Maltsev characteristics to shorten the chain of $v_i$'s until $k = 2$. This means that there is a unary polynomial $f$ so that $\{f(x), f(y)\} = \{0, b\}$. Moreover, if $f(x) = b$ and $f(y) = 0$, then we can replace $f$ by the polynomial $b - f(z)$ so that we can assume $f(x) = 0$ and $f(y) = b$. We will bound the number of constants necessary to construct $f$. Let $c_0, \ldots, c_{l-1}$ be representatives of the $\zeta$-classes with $c_0 = 0$. Note that $l \leq |\mathbf{A}|$. There are constants $r_0, \ldots, r_{m-1}$ and an $(m+1)$-ary term $t$ so that $f(z) = t(z, \mathbf{r})$ for all $z \in \mathbf{B}$. For each $j = 1, \ldots, m-1$, select $i_j$ so that $c_{i_j} \zeta r_j$. For notational convenience, let $s_j = c_{i_j}$. If $z \in x/\zeta$, then the matrix

$$\begin{pmatrix} t(x, \mathbf{r}) - t(x, \mathbf{r}) + 0 & t(x, \mathbf{s}) - t(x, \mathbf{s}) + 0 \\ t(z, \mathbf{r}) - t(x, \mathbf{r}) + 0 & t(z, \mathbf{s}) - t(x, \mathbf{s}) + 0 \end{pmatrix}$$

is in $M(\zeta, \zeta)$. Since the top row of the matrix is an equality, so is the bottom since $[\zeta, \zeta] = 0_B$. It follows then that $f(z) = t(z, \mathbf{r}) = t(z, \mathbf{s}) - t(x, \mathbf{s}) + 0$. Let $c_l = t(x, \mathbf{s})$. Then for all $z \in x/\zeta$

we have $f(z) = q(t(z, \mathbf{s}), c_l, c_0)$ (recall that $0 = c_0$). Since each $s_j = c_{i_j}$, we have an $(l+2)$-ary term $t'$ so that $f(z) = t'(z, c_0, \ldots, c_l)$ for all $z \in u/\zeta$. We have proven that for all $x \neq y \in u/\zeta$ there exists an $(l+2)$-ary term $t'$ so that $t'(x, c_0, \ldots, c_l) = 0$ iff $t'(y, c_0, \ldots, c_l) \neq 0$. Define $\Sigma$ to be the set of all functions $t(-, c_0, \ldots, c_l)$ with $t$ an $(l+2)$-ary term of $\mathbf{B}$. Notice that $|\Sigma| \leq |\mathbf{F}_{\mathrm{HSP}(\mathbf{A})}(l+2)| = M$ where $\mathbf{F}_{\mathrm{HSP}(\mathbf{A})}(l+2)$ is the free algebra in $\mathrm{HSP}(\mathbf{A})$ on $l+2$ generators. Define an equivalence relation $\sim$ on $u/\zeta$ by $x \sim y$ if for all $f \in \Sigma$, $f(x) = 0$ if and only if $f(y) = 0$. Then $|(u/\zeta)/\sim| \leq 2^{|\Sigma|} \leq 2^M$. However, since we can separate points of $u/\zeta$ with functions in $\Sigma$, it follows that $\sim$ is the identity relation on $u/\zeta$, so we have that $|u/\zeta| \leq 2^M$ as desired. As stated above, it follows that

$$|B| \leq |A| \cdot 2^M \leq |A| \cdot 2^{|A|^{|A|^{|A|+2}}},$$

and this gives a finite upper bound to $\mathrm{resb}(\mathbf{A})$. We have proven that (4) $\to$ (2).

To complete the proof of this theorem, it only remains to establish that (1) $\to$ (3). Assume that (3) does not hold. We will prove that $\mathrm{HSP}(\mathbf{A})$ has arbitrarily large subdirectly irreducibles. There is an algebra $\mathbf{E}$ in $\mathrm{HSP}(\mathbf{A})$ with congruences $\beta'$ and $\gamma$ so that $\beta' \cap [\gamma, \gamma] \not\leq [\beta', \gamma]$. Let $\beta = \beta' \cap [\gamma, \gamma]$. Then $\beta \leq [\gamma, \gamma]$ and $[\beta, \gamma] < \beta$ (because otherwise, $\beta' \cap [\gamma, \gamma] = \beta = [\beta, \gamma] \leq [\beta', \gamma]$). Choose a strictly meet irreducible congruence $\theta$ which exceeds $[\beta, \gamma]$ but not $\beta$. Let $\theta'$ be the unique cover of $\theta$. It follows that $\theta' \leq [\gamma \vee \theta, \gamma \vee \theta] \vee \theta$ and

$$[\theta', \gamma \vee \theta] \leq [\beta \vee \theta, \gamma \vee \theta] \leq [\beta, \gamma] \vee \theta = \theta,$$

because $\theta' \leq \beta \vee \theta \leq [\gamma, \gamma] \vee \theta$. Therefore, we can change notation (replacing $\mathbf{E}$ by $\mathbf{E}/\theta$) and assume that $\mathbf{E}$ is subdirectly irreducible with monolith $\beta$. We have that $\beta \leq [\gamma, \gamma]$ and $[\beta, \gamma] = 0_E$.

Let $\Delta = \Delta_{\gamma,\beta}$ be the congruence on $\mathbf{E}(\gamma)$ as in Lemma 8.6. Let $\pi_i : \mathbf{E}(\gamma) \to \mathbf{E}$ for $i = 0, 1$ be the canonical projections with $\eta_i = \ker \pi_i$. For $i = 0, 1$, let $\beta_i = \pi^{-1}(\beta)$. From Lemma 8.6 we have that $\Delta \cap \eta_i = 0_{\mathbf{E}(\gamma)}$ and $\Delta \vee \eta_i = \beta_i$.

Let $\aleph$ be an arbitrary cardinal. We will follow the tradition that $\aleph = \{\sigma : \sigma < \aleph\}$ and extend the notation for elements of $\mathbf{E}^\aleph$ which we have been using for finite direct powers up to now. That is, we will represent elements of $\mathbf{E}^\aleph$ as bold faced vectors $\mathbf{a}$, and for $\delta \in \aleph$, we will denote the $\delta$ coordinate of $\mathbf{a}$ as $a_\delta$. Let $\mathbf{B} = \{\mathbf{a} \in \mathbf{E}^\aleph : a_\delta \gamma a_\epsilon \text{ for all } \delta, \epsilon \in \aleph\}$. For any $\epsilon \in \aleph$, let $\gamma_\epsilon \in \mathrm{Con}\,\mathbf{B}$ be defined by $\mathbf{a} \gamma_\epsilon \mathbf{b}$ iff $a_\epsilon \gamma b_\epsilon$, and define $\beta_\epsilon$ analogously. From our definition of $\mathbf{B}$, it follows that $\gamma_\delta = \gamma_\epsilon$ for all $\epsilon, \delta \in \aleph$. We will denote this congruence as $\gamma$. For each $\epsilon \in \aleph$, let $\eta_\epsilon$ be the kernel of the projection of $\mathbf{B}$ to the $\epsilon$ coordinate and let $\eta'_\epsilon = \bigcap_{\delta \neq \epsilon} \eta_\delta$. Then $\eta_\epsilon \vee \eta_\delta = \gamma$ for all $\{\delta, \epsilon\} \subseteq \aleph$, $\delta \neq \epsilon$. For each $\sigma \in \aleph$, let $\theta_\sigma$ be defined as

$$\theta_\sigma = \{\langle \mathbf{a}, \mathbf{b} \rangle : a_\sigma \beta b_\sigma \text{ and for all } \epsilon \neq \sigma,\ a_\epsilon = b_\epsilon\}.$$

For each $\sigma \in \aleph \setminus \{0\}$, let $\Delta_\sigma$ be defined as

$$\Delta_\sigma = \{\langle \mathbf{a}, \mathbf{b} \rangle : \langle a_0, a_\sigma \rangle \Delta \langle b_0, b_\sigma \rangle \text{ and for all } \epsilon \notin \{0, \sigma\},\ a_\epsilon = b_\epsilon\}.$$

Finally, let $\theta = \bigvee_\sigma \theta_\sigma$ and $\kappa = \bigvee_{\sigma > 0} \Delta_\sigma$.

We claim that $\theta_0 \leq \theta_\delta \vee \Delta_\delta$ and that $\theta_\delta \leq \theta_0 \vee \Delta_\delta$ for $\delta \neq 0$. Suppose that $\mathbf{a}\theta_0\mathbf{b}$. This means that $a_0 \beta b_0$ and otherwise $\mathbf{a}$ and $\mathbf{b}$ are equal. Now, since $\langle a_0, a_0\rangle \Delta \langle b_0, b_0\rangle$ we have

$$\begin{array}{rcl} \mathbf{a} & = & \langle a_0, \ldots, a_\delta, \ldots\rangle \\ & \eta'_\delta & \langle a_0, \ldots, a_0, \ldots\rangle \\ & \Delta_\delta & \langle b_0, \ldots, b_0, \ldots\rangle \\ & \eta'_\delta & \langle b_0, \ldots, b_\delta, \ldots\rangle \\ & = & \mathbf{b} \end{array} \tag{12.4}$$

so $\theta_0 \leq \eta'_\delta \vee \Delta_\delta$. If we meet with $\theta_0 \vee \theta_\delta$, then using modularity several times, observing that $\Delta_\delta \leq \theta_0 \vee \theta_\delta$ and $\eta'_\delta \wedge (\theta_0 \vee \theta_\delta) = (\eta'_\delta \wedge \theta_0) \vee \theta_\delta = \theta_\delta$ (since $\eta'_\delta \geq \theta_\delta$), we obtain that

$$\theta_0 \leq (\theta_0 \vee \theta_\delta) \wedge (\eta'_\delta \vee \Delta_\delta) = \{(\theta_0 \vee \theta_\delta) \wedge \eta'_\delta\} \vee \Delta_\delta = \theta_\delta \vee \Delta_\delta \,.$$

That $\theta_\delta \leq \theta_0 \vee \Delta_\delta$ can be proven similarly.

For any $\delta \neq 0 \neq \epsilon$ this gives

$$\begin{array}{rcl} \kappa \vee \theta_\delta & = & \kappa \vee \Delta_\delta \vee \Delta_\epsilon \vee \theta_\delta \\ & = & \kappa \vee \Delta_\epsilon \vee \theta_0 \vee \theta_\delta \\ & = & \kappa \vee \theta_\epsilon \vee \theta_0 \vee \theta_\delta \\ & \geq & \theta_\epsilon \vee \theta_0. \end{array} \tag{12.5}$$

It follows from our definitions that $\kappa \vee \theta_\delta = \theta$ for all $\delta$ including $\delta = 0$.

We also claim that $\theta_\delta \not\leq \kappa$. We first show that $\theta_0 \not\leq \kappa$. The case for $\delta \neq 0$ then follows since $\kappa \vee \theta_0 = \kappa \vee \theta_\delta$. Since $0_E \prec \beta$ in $\operatorname{Con}\mathbf{E}$, we know that $0_B \prec \theta_\delta$ in $\operatorname{Con}\mathbf{B}$. Hence, $\theta_\delta$ is compact. If $\theta_0 \leq \kappa$, then by compactness, $\theta_0$ would be exceeded by a join of finitely many of the $\Delta_\epsilon$. We will prove by induction on $n \geq 1$ that $\theta_0$ is not exceeded by a join of $n$ of the $\Delta_\epsilon$. It must be that $\theta_0 \cap \Delta_\epsilon = 0_B$ for all $\epsilon$. To see this, suppose that $\langle \mathbf{a}, \mathbf{b}\rangle \in \theta_0 \cap \Delta_\epsilon$. This means that $a_\delta = b_\delta$ for all $\delta \neq 0$ and that $\langle a_0, a_\epsilon\rangle \Delta \langle b_0, b_\epsilon\rangle = \langle b_0, a_\epsilon\rangle$. By Lemma 8.6 this means that $\langle a_0, b_0\rangle \in [\gamma, \beta] = 0_E$. Hence, we also have that $a_0 = b_0$ so $\mathbf{a} = \mathbf{b}$. Since $\theta_0 \cap \Delta_\epsilon = 0_B$ for all $\epsilon$, it cannot be that $\theta_0 \leq \Delta_\epsilon$ for any $\epsilon$. Now suppose that $n > 1$ and that $\theta_0$ is not exceeded by any join of fewer than $n$ of the $\Delta_\epsilon$. Suppose that $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$ are $n$ distinct members of $\aleph$. Then we know that $\Delta_{\epsilon_1} \leq \theta_0 \vee \theta_{\epsilon_1}$, that $\bigvee_{i\geq 2} \Delta_{\epsilon_i} \leq \theta_0 \vee (\bigvee_{i\geq 2} \theta_{\epsilon_i})$, and that $\theta_0 \cap (\bigvee_{i\geq 2} \Delta_{\epsilon_i}) = 0_B$ (since $0_B \prec \theta_0$). Also, it is not difficult to prove that the $\theta_\delta$'s are independent. Putting all of this together gives

$$\begin{array}{rcl} \theta_0 \cap \left(\bigvee_{1\leq i\leq n} \Delta_{\epsilon_i}\right) & = & \theta_0 \cap (\theta_0 \vee \theta_{\epsilon_1}) \cap \left(\bigvee_{1\leq i\leq n} \Delta_{\epsilon_i}\right) \\ & = & \theta_0 \cap \left(\Delta_{\epsilon_1} \vee \left[(\theta_0 \vee \theta_{\epsilon_1}) \cap \left(\theta_0 \vee \left(\bigvee_{i\geq 2} \theta_{\epsilon_i}\right)\right) \cap \left(\bigvee_{i\geq 2} \Delta_{\epsilon_i}\right)\right]\right) \\ & = & \theta_0 \cap \left(\Delta_{\epsilon_1} \vee \left[\theta_0 \cap \left(\bigvee_{i\geq 2} \Delta_{\epsilon_2}\right)\right]\right) \\ & = & \theta_0 \cap \Delta_{\epsilon_1} \\ & = & 0_B. \end{array} \tag{12.6}$$

This means, of course, that $\theta_0 \not\leq \bigvee_{1\leq i\leq n} \Delta_{\epsilon_i}$. By induction, it cannot be that $\theta_0$ is less than any finite join of $\Delta_\epsilon$'s. It follows then that $\theta_0 \not\leq \kappa$ and that $\theta_\delta \not\leq \kappa$ for any $\delta$.

Since $\kappa \vee \theta_\delta = \theta$ but $\theta_\delta \not\leq \kappa$ for all $\delta$, it follows that $\kappa < \theta$. Therefore, there is a completely meet irreducible $\lambda \in \operatorname{Con}\mathbf{B}$ which contains $\kappa$ and not $\theta$. In $\operatorname{Con}\mathbf{B}$, $\eta_\delta \cap \eta'_\delta = 0_B$ and $\eta_\delta \vee \eta'_\delta = \gamma$. So the interval from $\eta_\delta$ to $\gamma$ is isomorphic to the interval from 0 to $\eta'_\delta$. Since

**E** is subdirectly irreducible, the interval from $\eta_\delta$ to $\gamma$ has a unique atom. Hence, the interval from 0 to $\eta'_\delta$ has a unique atom—which is $\theta_\delta$ in our notation. This implies that $\lambda \cap \eta'_\delta = 0_B$. If this were not the case, then $\lambda \geq \theta_\delta$ and so $\lambda \geq \theta_\delta \vee \kappa = \theta$ which is a contradiction. We have then that $\eta_\delta \vee \eta'_\delta = \gamma$ and that $\lambda \cap \eta'_\delta = 0_B$. We claim that for all $\delta$, $\lambda \vee \eta_\delta \not\geq \gamma$. To see this, suppose that $\lambda \vee \eta_\delta \geq \gamma$. Then $[\gamma, \gamma] \leq [\eta_\delta \vee \eta'_\delta, \eta_\delta \vee \lambda] \leq \eta_\delta \vee (\lambda \cap \eta'_\delta) = \eta_\delta$. Since $\mathbf{E} \cong \mathbf{B}/\eta_\delta$, this would imply that in $\operatorname{Con}\mathbf{E}$, $[\gamma, \gamma] = 0_E$—which is not true. Now, since $\eta_\delta \vee \eta_\epsilon = \gamma$ for all $\delta \neq \epsilon \in \aleph$, the congruences $\lambda \vee \eta_\delta$, $\delta \in \aleph$, are pairwise distinct. Therefore $\mathbf{B}/\lambda$—which is subdirectly irreducible—has at least $\aleph$ congruences. Since $\aleph$ is an arbitrary infinite cardinal, it follows that $\mathrm{HSP}(\mathbf{A})$ has no residual bound. We have proven the contrapositive of (1) $\rightarrow$ (3).

□

## 13 Directly Representable Varieties

**Definition 13.1** *A variety $\mathcal{V}$ is directly representable iff there is a finite set $\mathcal{D}$ of finite algebras such that $\mathcal{V} = \mathrm{HSP}(\mathcal{D})$ and every finite algebra in $\mathcal{V}$ belongs to $\mathrm{IP}(\mathcal{D})$, equivalently, $\mathcal{V}$ is locally finite and has, up to isomorphism, only a finite set of finite directly indecomposable algebras. The finite spectrum of a class $\mathcal{K}$ of algebras is the set of positive integers $n$ such that $\mathcal{K}$ has an $n$-element algebra. A class $\mathcal{K}$ of algebras is said to be narrow iff there is a finite set $\{p_0, \ldots, p_{k-1}\}$ of prime integers such that every member of the finite spectrum of $\mathcal{K}$ takes the form $\prod_{i<k} p_i^{a_i}$ for some integers $a_i$.*

In this section, we prove that every narrow locally finite variety has permuting congruences, characterize finite algebras that generate narrow varieties, and using the commutator, characterize finite algebras that generate directly representable varieties. The results proved here are drawn from R. McKenzie [32].

**Theorem 13.2** *Let $\mathcal{V}$ be any locally finite variety and consider these possible properties of $\mathcal{V}$.*

(1) *$\mathcal{V}$ is directly representable.*

(2) *$\mathcal{V}$ is narrow.*

(3) *All congruences on finite algebras in $\mathcal{V}$ are uniform.*

(4) *$\mathcal{V}$ has permuting congruences.*

*We have (1) $\rightarrow$ (2) $\rightarrow$ (3) $\rightarrow$ (4).*

**Proof** Clearly (1) implies (2).

To prove that (2) implies (3), suppose that $\mathcal{V}$ is a narrow variety, that $\mathbf{A}$ is a finite algebra in $\mathcal{V}$, and that $\theta \in \operatorname{Con}\mathbf{A}$. For $n$ a positive integer, define $\mathbf{A}_n(\theta)$ to be the algebra (subalgebra of $\mathbf{A}^n$) consisting of all sequences $\mathbf{u} \in A^n$ such that $u_i \theta u_j$ for all $\{i, j\} \subseteq \{0, \ldots, n-1\}$. We assume that $|\mathbf{A}/\theta| = k$ and that the $k$ distinct $\theta$-equivalence classes have cardinalities $a_0, \ldots, a_{k-1}$. We are going to show that $a_0 = a_1 = \cdots = a_{k-1}$. Observe that

$$|\mathbf{A}_n(\theta)| = a_0^n + \cdots + a_{k-1}^n = s_n(\mathbf{a}) \tag{13.1}$$

where $\mathbf{a} = \langle a_0, \ldots, a_{k-1}\rangle$. Let $\{p_0, \ldots, p_{\ell-1}\}$ be a finite set of prime integers that include all the prime divisors of the members of the finite spectrum of $\mathcal{V}$, and hence all the prime divisors of the integers $s_n(\mathbf{a})$, $n \geq 1$. Let $d = \gcd\{a_i : i < k\}$ and let $\mathbf{b} = \langle b_0, \ldots, b_{k-1}\rangle$ where $db_i = a_i$. Choose $M$ to be any positive integer such that $2^M \geq k$. For $j < \ell$, put $q_j = (p_j - 1)p_j^M$. An easy calculation, based on the Euler-Fermat theorem, shows that

$$b_i^{q_j} \equiv 0, 1 \pmod{p_j^{M+1}} \text{ for } i < k,\ j < \ell\,. \tag{13.2}$$

Thus for any positive integer $N$, $b_i^{q_j N} \equiv 0, 1 \pmod{p_j^{M+1}}$, and we have

$$s_{q_j N}(\mathbf{b}) \equiv u_j \pmod{p_j^{M+1}} \tag{13.3}$$

where $u_j$ is the number of $i < k$ such that $b_i$ is prime to $p_j$. Note that $1 \leq u_j \leq k$, since the $b_i$ have no positive common divisors other than 1, and $p_j^{M+1} > k$. Thus $p_j^{M+1}$ cannot divide $s_{q_j N}(\mathbf{b})$.

Now taking $q = \prod_{j<\ell} q_j$ and $N$ any positive integer, it follows from the above analysis that $s_{qN}(\mathbf{b})$ is not divisible by $p_j^{M+1}$ for any $j < \ell$. Since $s_{qN}(\mathbf{b})$ is a product of powers of the $p_j$, it follows that

$$s_{qN}(\mathbf{b}) \leq P = \prod_{j<\ell} p_j^M\,. \tag{13.4}$$

If we had $b_i > 1$ for some $i$, then the sequence $\langle s_{qN}(\mathbf{b}) : N \geq 1\rangle$ would be a strictly increasing sequence of integers. Because the sequence is bounded, we must have $b_0 = b_1 = \cdots = b_{k-1} = 1$. Thus we conclude our proof that $\mathbf{a}$ is a constant sequence, or in other words, $\theta$ is a uniform congruence.

To prove that (3) implies (4), suppose that $\mathcal{V}$ is locally finite and its finite algebras have uniform congruences. We first observe that as an easy corollary of the proof of Theorem 6.1, a variety has permuting congruences iff its free algebra on three generators has permuting congruences. Since $\mathcal{V}$ is locally finite, it therefore suffices to show that the finite algebras in $\mathcal{V}$ have permuting congruences. Thus suppose that $\mathbf{A} \in \mathcal{V}$ is finite and $\{\alpha, \beta\} \subseteq \operatorname{Con}\mathbf{A}$. Let $\mathbf{B}$ be the algebra $\mathbf{A}_2(\alpha) \leq \mathbf{A} \times \mathbf{A}$ consisting of all pairs $\langle x, y\rangle$ with $x\alpha y$. Let $\theta$ (on $\mathbf{B}$) be the congruence $\beta \times \beta|_B$, so that $\langle x, y\rangle\theta\langle u, v\rangle$ iff $x\beta u$ and $y\beta v$. By assumption, the congruences $\beta, \alpha \cap \beta, \theta$ are uniform. Let $b, c, e$ be the respective block-sizes for these congruences. Choose any $a \in A$. Then $\langle a, a\rangle/\theta$ consists of all $\langle x, y\rangle \in A \times A$ such that $x \in a/\beta$ and $y \in x/(\alpha \cap \beta)$; thus $e = bc$.

Now, to conclude this proof, we assume that there are elements $u, v, w$ in $A$ with $u\alpha v\beta w$ and $\langle u, w\rangle \notin \beta \circ \alpha$, and we derive a contradiction. This assumption implies that there is no $x \in A$ with $\langle x, w\rangle \in \langle u, v\rangle/\theta$. Note that for any $z \in A$, if $\langle x, z\rangle \in \langle u, v\rangle/\theta$ for some $x = x_0$ then $\langle x, z\rangle \in \langle u, v\rangle/\theta$ precisely for the elements $x \in x_0/(\alpha \cap \beta)$. Thus $|\langle u, v\rangle/\theta| = b'c$ where $b'$ is the number of $z \in v/\beta$ such that such $\langle u, z\rangle \in \beta \circ \alpha$. We have that $b' < b$ since $w \in v/\beta$ and $\langle u, w\rangle \notin \beta \circ \alpha$. Thus $|\langle u, v\rangle/\theta| = b'c < bc = |\langle u, v\rangle/\theta|$, which is the promised contradiction. □

**Lemma 13.3** *In a directly representable variety, every finite subdirectly irreducible algebra is Abelian or simple.*

**Proof** Assume that $\mathcal{V}$ is a directly representable variety. By Theorem 13.2, $\mathcal{V}$ is congruence-modular; in fact, it is a Maltsev variety. Since subdirectly irreducible algebras are directly

indecomposable, $\mathcal{V}$ has a finite bound on the size of its finite subdirectly irreducible algebras. As we noted in our proof of Theorem 12.2, this implies that the locally finite variety $\mathcal{V}$ has $\mathrm{resb}(\mathcal{V}) < \omega$, and $\mathcal{V} \models$ (C1). Now let $\mathbf{A}$ be a finite subdirectly irreducible algebra in $\mathcal{V}$. To get a contradiction, we suppose that $\mathbf{A}$ is neither Abelian nor simple. Where $\beta$ is the monolith of $\mathbf{A}$, this supposition means that $0_A \prec \beta < 1_A$ and $\beta \leq [1_A, 1_A]$. Applying (C1), we find that $\beta = [\beta, 1_A]$.

Choose any positive integer $n$. Once again, we consider the algebra $\mathbf{A}_n(\beta)$ of $\beta$-constant $n$-tuples. Our goal this time is to prove that $\mathbf{A}_n(\beta)$ is directly indecomposable. Since $|\mathbf{A}_n(\beta)| > 2^n$, this will contradict the ground assumption that $\mathcal{V}$ is directly representable. {This is the fourth time that we have used this fruitful construction after Section 11.}

Suppose, for sake of contradiction, that $\mathbf{A}_n(\beta)$ is not directly indecomposable. Then it possesses a pair of congruences $\langle \delta_0, \delta_1 \rangle$ such that $0 < \delta_\varepsilon < 1$, $\delta_0 \vee \delta_1 = 1$, $\delta_0 \wedge \delta_1 = 0$. We write $\eta_i$ for the kernel of the projection homomorphism of $\mathbf{A}_n(\beta)$ to $\mathbf{A}$ at the $i$ coordinate (as usual) and put $\eta_i' = \bigwedge_{j \neq i} \eta_j$. We write $\beta_i$ for the kernel of the homomorphism of $\mathbf{A}_n(\beta)$ to $\mathbf{A}/\beta$ through the $i$ coordinate, so that $\beta_i = \beta_j$ for alll $\{i, j\} \subseteq \{0, \ldots, n-1\}$, and we write simply $\beta$ for this congruence. The fact that $\mathbf{A} \models \beta = [\beta, 1]$ gives $\mathbf{A}_n(\beta) \models \beta = \eta_i \vee [\beta, 1]$ for each $i < n$. (Here we have used Theorem 8.3, statement (6), again.) For $i < n$ we have $\eta_i \prec \beta$, $\beta = \eta_i \vee \eta_i'$, and $\eta_i \wedge \eta_i' = 0$. Then by modularity, $0 \prec \eta_i'$.

We can now show that for each $i < n$ and $\varepsilon \in \{0, 1\}$, if $\delta_\varepsilon \not\leq \eta_i$ then $\eta_i' \leq \delta_\varepsilon$. Indeed, if $\delta_\varepsilon \not\leq \eta_i$, then $\beta \leq \eta_i \vee \delta_\varepsilon$, giving $\beta = \eta_i \vee (\beta \wedge \delta_\varepsilon)$. Then

$$[\eta_i', \delta_{1-\varepsilon}] \leq [\beta, \delta_{1-\varepsilon}] = [\eta_i \vee (\beta \wedge \delta_\varepsilon), \delta_{1-\varepsilon}] \leq \eta_i \vee [\delta_\varepsilon, \delta_{1-\varepsilon}] = \eta_i \,. \tag{13.5}$$

Thus $[\eta_i', \delta_{1-\varepsilon}] \leq \eta_i' \wedge \eta_i = 0$. Then since $[\beta, 1] = [\eta_i \vee \eta_i', 1] \not\leq \eta_i$ we have

$$0 \neq [\eta_i', 1] = [\eta_i', \delta_0 \vee \delta_1] = [\eta_i', \delta_0] \vee [\eta_i', \delta_1] = [\eta_i', \delta_\varepsilon] \,. \tag{13.6}$$

Since $\eta_i'$ is an atom, then

$$\eta_i' = [\eta_i', \delta_\varepsilon] \leq \delta_\varepsilon \,. \tag{13.7}$$

So indeed, $\delta_\varepsilon \not\leq \eta_i$ implies $\eta_i' \leq \delta_\varepsilon$.

Since $\bigvee_i \eta_i = \beta < 1 = \delta_0 \vee \delta_1$, then there is $\varepsilon \in \{0, 1\}$ such that $\delta_\varepsilon \leq \eta_i$ holds for no $i$. Then $\delta_\varepsilon \geq \bigvee_i \eta_i' = \beta$. This implies that $\delta_{1-\varepsilon} \geq \eta_i'$ holds for no $i$ since $\delta_0 \wedge \delta_1 = 0$; consequently, $\delta_{1-\varepsilon} \leq \eta_i$ for all $i < n$. But that forces $\delta_{1-\varepsilon} = 0$. This contradiction proves the lemma. □

For the final theorem of this section, we will need this lemma.

**Lemma 13.4** (I. Fleischer [10]) *Let $\mathbf{A} \leq \mathbf{A}_0 \times \mathbf{A}_1$ be a subdirect product, where $\mathbf{A}$ has permuting congruences. Then $\mathbf{A}$ is the equalizer of a pair of surjective homomorphisms $\pi_i : \mathbf{A}_i \to \mathbf{K}$ for some algebra $\mathbf{K}$. Consequently, if $\mathbf{A}$ has permuting congruences and $\mathbf{A}$ is a subdirect product of a finite system of simple algebras, $\mathbf{A} \leq \prod_{t \in T} \mathbf{S}_t$, then for some $W \subseteq T$, the projection of $\mathbf{A}$ into $\prod_{t \in W} \mathbf{S}_t$ is an isomorphism $\pi_W : \mathbf{A} \cong \prod_{t \in W} \mathbf{S}_t$.*

**Proof** This is left as an exercise for the reader. □

**Theorem 13.5** (1) *In a directly representable variety, every finite algebra is isomorphic, for some $m \geq 0$, with a direct product $\mathbf{B}_0 \times \mathbf{B}_1 \times \cdots \times \mathbf{B}_m$ where $\mathbf{B}_0$ is Abelian and $\mathbf{B}_i$ is a simple non-Abelian algebra for $i \geq 1$.*

(2) *Let* $\mathbf{A}$ *be a finite algebra.* $\mathrm{HSP}(\mathbf{A})$ *is directly representable iff* $\mathbf{A}$ *has a Maltsev term, every subalgebra of* $\mathbf{A}$ *is isomorphic with a direct product of an Abelian algebra and a product of simple non-Abelian algebras, and the variety* $\mathcal{A}$ *generated by the collection of all Abelian direct factors of subalgebras of* $\mathbf{A}$ *is directly representable.*

(3) *Let* $\mathbf{A}$ *be a finite algebra.* $\mathrm{HSP}(\mathbf{A})$ *is narrow iff* $\mathbf{A}$ *has a Maltsev term and every subalgebra of* $\mathbf{A}$ *has uniform congruences.*

**Proof** To prove (1), suppose that $\mathcal{V}$ is directly representable and $\mathbf{A}$ is a finite algebra in $\mathcal{V}$.

By Lemma 13.3, and G. Birkhoff's subdirect representation theorem, $\mathbf{A}$ is isomorphic, for some integer $m \geq 0$, to an algebra $\mathbf{A}' \leq \prod_{i \leq m} \mathbf{B}_i$ where $\mathbf{B}_0$ is Abelian and $\mathbf{B}_i$ $(i \geq 1)$ is non-Abelian and simple. (Here we have used that any subdirect product of Abelian algebras is Abelian.) We assume that $m$ is as small as it can be.

Let $\eta_i$ denote the kernel of the $i$ coordinate projection of $\mathbf{A}'$ onto $\mathbf{B}_i$. Put $\delta_0 = \eta_0$ and $\delta_1 = \bigwedge_{1 \leq i \leq m} \eta_i$. Since $\mathcal{V}$ has permuting congruences, the minimality of $m$ and Lemma 13.4 tells us that the projection of $\mathbf{A}'$ into $\mathbf{B}_1 \times \cdots \times \mathbf{B}_m$ (an algebra isomorphic to $\mathbf{A}'/\delta_1$) is the full direct product of $\mathbf{B}_1, \ldots, \mathbf{B}_m$.

Next we claim that $\mathbf{A}'/\delta_1 \models [1,1] = 1$. This actually follows from the fact that in a modular variety, the class of algebras satisfying $[x,y] = x \wedge y$ for congruences—called "neutral algebras"—is closed under binary subdirect products. (Simple, non-Abelian algebras are neutral.) To see this, suppose that $\mathbf{E} \leq \mathbf{E}_0 \times \mathbf{E}_1$ is a subdirect product and $\mathbf{E}_i \models_{\mathrm{CON}} [x,y] = x \wedge y$. Let $\rho_0, \rho_1$ denote the two projection congruences on $\mathbf{E}$, and let $\{\alpha, \beta\} \subseteq \mathrm{Con}\,\mathbf{E}$. Then $\mathbf{E}/\rho_0$ neutral implies that

$$\alpha \wedge \beta \leq (\alpha \vee \rho_0) \wedge (\beta \vee \rho_0) = [\alpha, \beta] \vee \rho_0\,. \tag{13.8}$$

Since $[\alpha,\beta] \leq \alpha \wedge \beta$, by modularity it follows that if $[\alpha,\beta] < \alpha \wedge \beta$ then $[\alpha,\beta] \wedge \rho_0 < \alpha \wedge \beta \wedge \rho_0$. Suppose that this strict inclusion holds. Now $(\alpha \wedge \beta \wedge \rho_0) \wedge \rho_1 = 0$, hence by modularity we must have $([\alpha,\beta] \wedge \rho_0) \vee \rho_1 < (\alpha \wedge \beta \wedge \rho_0) \vee \rho_1$. But since $\mathbf{E}/\rho_1$ is neutral, we can calculate that

$$\begin{aligned} ([\alpha,\beta] \wedge \rho_0) \vee \rho_1 &\geq [[\alpha,\beta], \rho_0] \vee \rho_1 \\ &= [[\alpha \vee \rho_1, \beta \vee \rho_1], \rho_0 \vee \rho_1] \vee \rho_1 \\ &= (\alpha \vee \rho_1) \wedge (\beta \vee \rho_1) \wedge (\rho_0 \vee \rho_1) \\ &\geq (\alpha \wedge \beta \wedge \rho_0) \vee \rho_1\,. \end{aligned} \tag{13.9}$$

This final contradiction shows that $[\alpha,\beta] = \alpha \wedge \beta$, as claimed.

Thus we have proved that $\mathbf{A}'/\delta_1 \models [1,1] = 1$. This means that $\mathbf{A}' \models 1 = \delta_1 \vee [1,1]$. Since $\mathbf{B}_0$ is Abelian, then $[1,1] \leq \delta_0$. Thus $\delta_1 \vee \delta_0 = 1$. Since $\delta_0 \wedge \delta_1 = 0$ by definition, and since $\delta_0$ and $\delta_1$ must commute, then it follows that $\mathbf{A}'$ is the direct product of $\mathbf{B}_0$ and the projection of $\mathbf{A}'$ into $\prod_{i \geq 1} \mathbf{B}_i$—i.e., $\mathbf{A}' = \prod_{i \leq m} \mathbf{B}_i$.

Now let $\mathbf{A}$ be any finite algebra. To prove (2), observe that we have already proved that $\mathrm{HSP}(\mathbf{A})$ directly representable implies the truth of the other three conditions. Conversely, suppose that these conditions are valid. Let $\mathcal{A}$ be the variety generated by the Abelian direct factors of subalgebras of $\mathbf{A}$. Every finite algebra $\mathbf{B}$ in $\mathrm{SP}(\mathbf{A})$ is isomorphic to a subdirect product of subalgebras of $\mathbf{A}$, and thus is isomorphic to a subdirect product $\mathbf{B}' \leq \prod_{i \leq m} \mathbf{B}_i$ with $\mathbf{B}_0 \in \mathcal{A}$ and $\mathbf{B}_i$ simple and non-Abelian for $1 \leq i \leq m$. Choosing $m$ minimal for $\mathbf{B}$, the above argument yields that $\mathbf{B}' = \prod_{i \leq m} \mathbf{B}_i$. Now let $\theta$ be any congruence of $\mathbf{B}'$. Write, as before, $\delta_0$ and $\delta_1$ for the kernels of the projections of $\mathbf{B}'$ onto $\mathbf{B}_0$ and $\mathbf{B}_1 \times \cdots \times \mathbf{B}_m$,

respectively. The neutrality of $\mathbf{B}'/\delta_1$ yields $\theta \vee \delta_1 = [\theta, 1] \vee \delta_1 = [\theta, \delta_0] \vee \delta_1$ (by replacing 1 by $\delta_0 \vee \delta_1$). Modularity gives $\theta = [\theta, \delta_0] \vee (\theta \wedge \delta_1)$ and $\theta \vee \delta_0 = \delta_0 \vee (\theta \wedge \delta_1)$. Then

$$\begin{aligned} (\delta_0 \vee \theta) \wedge (\delta_1 \vee \theta) &= (\delta_0 \vee (\theta \wedge \delta_1)) \wedge (\delta_1 \vee [\theta, \delta_0]) \\ &= (\delta_0 \vee (\theta \wedge \delta_1)) \wedge \delta_1) \vee [\theta, \delta_0]) \\ &= (\delta_0 \wedge \delta_1) \vee (\theta \wedge \delta_1) \vee [\theta, \delta_0]) \\ &\leq \theta\,. \end{aligned} \tag{13.10}$$

Thus

$$(\delta_0 \vee \theta) \wedge (\delta_1 \vee \theta) = \theta\,. \tag{13.11}$$

Since also,

$$(\delta_0 \vee \theta) \vee (\delta_1 \vee \theta) = 1\,, \tag{13.12}$$

it follows that $\mathbf{B}'/\theta \cong (\mathbf{B}'/(\delta_0 \vee \theta)) \times (\mathbf{B}'/(\delta_1 \vee \theta))$, the product of an algebra in $\mathcal{A}$ and a quotient of $\mathbf{B}'/\delta_1$. Since $\mathbf{B}'/\delta_1$ is neutral, it has distributive congruence lattice, and every quotient of this algebra is isomorphic to a direct product of a subsystem of the simple algebras $\mathbf{B}_i$, $1 \leq i \leq m$.

We have now shown that every finite algebra in $\mathrm{HSP}(\mathbf{A})$ is isomorphic to a product of an algebra in $\mathcal{A}$ and a product of a system of simple non-Abelian direct factors of subalgebras of $\mathbf{A}$. Since $\mathcal{A}$ is directly representable, then $\mathcal{V}$ has, within isomorphism, only a finitely number of directly indecomposable finite algebras.

To prove (3), suppose that the finite algebra $\mathbf{A}$ has a Maltsev term and all subalgebras of $\mathbf{A}$ have uniform congruences. We first show that $\mathrm{SP}(\mathbf{A})$ is narrow, in fact, that every prime divisor of the finite spectrum of $\mathrm{SP}(\mathbf{A})$ divides the cardinality of some subalgebra of $\mathbf{A}$. To do this, we use Lemma 13.4. If $\mathbf{B} \leq \mathbf{B}_0 \times \mathbf{B}_1$ is a subdirect product in a Maltsev variety, then $\mathbf{B}$ is the equalizer of surjective homomorphisms $\pi_i : \mathbf{B}_i \to \mathbf{K}$. If the kernel of $\pi_1$ is a uniform congruence on $\mathbf{B}_1$ with congruence classes of size $c$, then it is trivial to see that $|\mathbf{B}| = |\mathbf{B}_1|c$. Now suppose that that $\mathbf{F} \leq \mathbf{F}_1 \times \cdots \times \mathbf{F}_n$ is a subdirect product where $\mathbf{F}_i$ are subalgebras of $\mathbf{A}$. By induction on $n$, using the preceeding observation and the fact that all congruences on every $\mathbf{F}_i$ are uniform, we find that $|\mathbf{F}|$ is the product of $|\mathbf{F}_1|$ and a sequence of integers $c_2, \ldots, c_n$ where $c_i$ is the block size of a uniform congruence on $\mathbf{F}_i$. Thus $|\mathbf{F}| = c_1 c_2 \cdots c_n$ with $c_i$ a divisor of $|\mathbf{F}_i|$.

Now since $\mathrm{SP}(\mathbf{A})$ is narrow, our proof of Theorem 13.2, (2) $\to$ (3), shows that the finite algebras in $\mathrm{SP}(\mathbf{A})$ have uniform congruences. If an algebra $\mathbf{B}$ has uniform congruences, then $|\mathbf{B}/\theta|$ divides $|\mathbf{B}|$ for every congruence $\theta$. Thus $\mathrm{HSP}(\mathbf{A})$ is narrow, as claimed. □

In [44] it is proven that on any finite set $A$ there altogether only finitely many clones $F$ so that the algebra $\langle A, F\rangle$ satisfies the conditions of (2) in Theorem 13.5. Each of these clones is generated by its operations of $|A| + 2$ variables. To finish our presentation of this topic, we characterize, in a fashion, the directly representable affine varieties.

**Theorem 13.6** *For an Abelian, congruence modular variety $\mathcal{A}$, the following are equivalent:*

(1) *$\mathcal{A}$ is directly representable.*

(2) *$\mathcal{A}$ is locally finite and the polynomially equivalent variety ${}_{\mathbf{R}}\mathcal{M}$ of modules is directly representable.*

(3) *$\mathcal{A}$ is locally finite and the ring of $\mathcal{A}$, $\mathbf{R}$, is a finite ring of finite representation type.*

**Proof** If $\mathbf{A} \in \mathcal{A}$ and $\mathbf{M} \in {}_{\mathbf{R}}\mathcal{M}$ and $\mathcal{A}$ and $\mathbf{M}$ are polynomially equivalent, then these algebras have the same universe and the same congruence lattice $\mathbf{L}$. Hence $\mathbf{A}$ is directly indecomposable iff $\mathbf{M}$ is directly indecomposable, since direct decompositions in algebras with permuting congruences correspond to complement pairs of congruences—$(\theta, \psi)$ with $\theta \cap \psi = 0$, $\theta \vee \psi = 1$. If $\mathcal{A}$ is locally finite, then $\mathbf{R}$ is finite, and each of these varieties has, for each integer $n$, only finitely many non-isomorphic $n$-element algebras. (They are all homomorphic images of the free algebra on $n$ generators in the variety.) Then $\mathcal{A}$ is directly representable iff ${}_{\mathbf{R}}\mathcal{M}$ is directly representable iff there is a finite bound to the size of finite directly indecomposable algebras in $\mathcal{A}$. A ring $\mathbf{R}$ with the property that up to isomorphism there are only finitely many finitely generated, directly indecomposable, $\mathbf{R}$-modules is said to be of finite representation type. The equivalence of (1), (2) and (3) should now be clear. □

## 14 Varieties with Very Few Models

**Definition 14.1** *For a class $\mathcal{C}$ of algebras and a cardinal $k$, let $G_{\mathcal{C}}(k)$ denote the number of pairwise non-isomorphic members of $\mathcal{C}$ that are generated by at most $k$ elements. We call this function, restricted to positive integral $k$, the G-spectrum (or generative complexity) of $\mathcal{C}$. We say that $\mathcal{C}$ has very few models iff there is a positive integer $N$ such that for all positive integral $k > 1$, $G_{\mathcal{C}}(k) \leq k^N$.*

Below is the chief result of P. M. Idziak, R. McKenzie [23], which will be proved in this section.

**Theorem 14.2** *A locally finite, congruence modular, variety has very few models iff it is Abelian and polynomially equivalent to the variety of unitary modules over some finite ring of finite representation type.*

In the next two lemmas, $\mathcal{V}$ denotes a fixed, locally finite, congruence modular variety with very few models. We first show that all finite algebras in $\mathcal{V}$ are nilpotent. Then by Corollary 10.6, the finite algebras in $\mathcal{V}$ have permuting congruences. Since the free algebra on three generators in $\mathcal{V}$ is finite, it follows that $\mathcal{V}$ has a Maltsev term. Then to prove that $\mathcal{V}$ is Abelian, it suffices to show that all finite algebras in $\mathcal{V}$ are Abelian. Assuming that this fails, we show by direct construction that $\mathrm{G}_{\mathcal{V}}(k)$ is not bounded by any polynomial function of $k$, thus getting a contradiction. Our proofs will be modifications of those appearing in P. M. Idziak, R. McKenzie [23]. As we mentioned in Section 11, all locally finite varieties with very few models have recently been completely characterized in P. M. Idziak, R. McKenzie, M. Valeriote [24]. Each such variety consists entirely of Abelian algebras.

Notation: The following notation will be used in the next two lemmas. For any sets $B \subseteq X$, and elements $a, b$ in an algebra $\mathbf{A}$, we define a member of $\mathbf{A}^X$: $[a, b]_B$ denotes the function $f \in A^X$ such that $f(x) = b$ for $x \in B$ and $f(x) = a$ for $x \in X \setminus B$. Then for $x \in X$, we use $[a, b]_x$ to denote $[a, b]_B$ with $B = \{x\}$.

**Lemma 14.3** *Every finite algebra in $\mathcal{V}$ is nilpotent.*

**Proof** Assume that this fails. By taking a quotient of a finite non-nilpotent algebra, we can find a finite algebra $\mathbf{A} \in \mathcal{V}$ with a minimal congruence $\mu$ such that $[1, \mu] = \mu$. For $n > 0$, let $X$ be a set of cardinality $2^n$ and let $\{X_{i,j} : 0 \leq i < n, 0 \leq j < 2\}$ be a system of $2n$ subsets of $X$ so that for all $x \in X$ there is a function $p : \{0, 1, \ldots, n-1\} \to \{0, 1\}$ such that

$$\{x\} = \bigcap_{i<n} X_{i,p(i)}\,.$$

For example, we can take $X_{i,0}$ and $X_{i,1}$ to be $B_i$ and its complement, where $B_0, \ldots, B_{n-1}$ is a set of generators of the Boolean algebra of all subsets of $X$.

Let $\mathbf{K}_n$ be the subalgebra of $\mathbf{A}^X$ generated by the set of all functions $[a, b]_{X_{i,0}}$ where $a$ and $b$ are any two elements of $A$ and $0 \leq i \leq n-1$. (See the note on notation above.) Thus $\mathbf{K}_n$ is generated by a set of $a(a-1)n+a$ elements, where $a = |\mathbf{A}|$. We shall show that $\mathbf{K}_n$ has a set of $2^n + 1$ pairwise non-isomorphic homomorphic images. Since these are all generated by at most $a(a-1)n + a$ elements, then we can conclude that $\mathrm{G}_{\mathcal{V}}(a(a-1)n+1) \geq 2^n$. But this conclusion is obviously incompatible with the assumption that $\mathcal{V}$ has very few models.

Suppose that $X = \{x_0, \ldots, x_{2^n-1}\}$. For $0 \leq i \leq 2^n$ let $\theta_i$ be the congruence of $\mathbf{K}_n$ consisting of all pairs $\langle f, g\rangle \in \mathbf{K}_n^2$ such that $f(x_j) = g(x_j)$ for all $0 \leq j < i$. Then for $i < j$ we have $\theta_j \leq \theta_i$. We shall show that $\theta_j < \theta_i$. This will imply that $|\mathbf{K}_n/\theta_i| < |\mathbf{K}_n/\theta_j|$ so that the two quotient algebras are non-isomorphic, as desired.

Actually, given $x \in X$, we shall show that $\mathbf{K}_n$ contains two distinct functions $f, g$ such that $f(y) = g(y)$ for all $y \in X \setminus \{x\}$. Taking $x = x_i$, this certainly implies that $\theta_i > \theta_j$ whenever $i < j \leq 2^n$.

So let $x \in X$ and write

$$\{x\} = \bigcap_{i<n} X_{i,p(i)}\,,$$

where $p$ is a certain function mapping $\{0, 1, \ldots, n-1\} \to \{0, 1\}$. We shall now produce, by induction on $i$, pairs of functions $\langle f_i, g_i\rangle \in K_n^2$ for $0 \leq i \leq n-1$, so that where $[\![f_i \neq g_i]\!]$ is the set of all $z \in X$ with $f_i(z) \neq g_i(z)$, we have

$$[\![f_i \neq g_i]\!] = \bigcap_{0\leq j\leq i} X_{i,p(i)}\,.$$

Then $f_{n-1}, g_{n-1}$ will be the desired pair of functions $f, g$ with $[\![f \neq g]\!] = \{x\}$. The inductive construction requires that $f_i(z)\,\mu\,g_i(z)$ for all $z \in X$—i.e., $\langle f_i, g_i\rangle \in \mu_X$—and that each of $f_i, g_i$ is constant on the set $[\![f_i \neq g_i]\!]$.

Choosing $\langle a, b\rangle \in \mu$, $a \neq b$, we put $f_0 = [a, a]_{X_{0,p(0)}}$, $g_0 = [a, b]_{X_{0,p(0)}}$ so that $\{f_0, g_0\} \subseteq K_n$, $\langle f_0, g_0\rangle \in \mu_X$, $[\![f_0 \neq g_0]\!] = X_{0,p(0)}$ and each of $f_0, g_0$ is constant on $X_{0,p(0)}$. Now suppose that $i < n-1$ and we have succeeded in constructing $f_i, g_i$ with the required properties. Let $a_i, b_i$ be the constant value of $f_i$, respectively $g_i$, on the set $[\![f_i \neq g_i]\!]$. Since $0 \prec \mu = [1, \mu]$, then $\langle a_i, b_i\rangle$ does not belong to the center of $\mathbf{A}$. Hence there must exist a term $t(u, \bar{w})$ and tuples of elements $\bar{c}, \bar{d}$ in $\mathbf{A}$ so that

$$t(a_i, \bar{c}) = t(a_i, \bar{d}) \leftrightarrow t(b_i, \bar{c}) \neq t(b_i, \bar{d})\,.$$

Without losing generality, assume that $t(b_i, \bar{c}) = t(b_i, \bar{d})$ and $t(a_i, \bar{c}) \neq t(a_i, \bar{d})$. Taking $\gamma$ in the Shifting Lemma (Lemma 6.6) to be the equality relation, we find that there is a Day term $m(x, y, z, u)$ such that

$$m(t(a_i, \bar{c}), t(a_i, \bar{c}), t(a_i, \bar{d}), t(a_i, \bar{d})) \neq m(t(a_i, \bar{c}), t(b_i, \bar{c}), t(b_i, \bar{d}), t(a_i, \bar{d}))\,.$$

Let $a_{i+1}$ be the left hand side of this inequality and $b_{i+1}$ be the right. We can choose tuples of (two-valued) functions $\bar{h}, \bar{k}$ in $K_n$ so that for all $z \in X_{i+1,p(i+1)}$, $\bar{h}(z) = \bar{c}$ and $\bar{k}(z) = \bar{d}$ while for all $z \in X_{i+1,1-p(i+1)}$, $\bar{h}(z) = \bar{k}(z)$. Then consider the functions

$$\begin{aligned} f_{i+1} &= m(t(f_i, \bar{h}), t(f_i, \bar{h}), t(f_i, \bar{k}), t(f_i, \bar{k})) \\ g_{i+1} &= m(t(f_i, \bar{h}), t(g_i, \bar{h}), t(g_i, \bar{k}), t(f_i, \bar{k}))\,. \end{aligned}$$

Since $\mathcal{V} \models m(u, v, v, u) \approx u$, then $f_{i+1}(z) = g_{i+1}(z)$ for all $z \in X$ for which either $f_i(z) = g_i(z)$ or $\bar{h}(z) = \bar{k}(z)$. In particular, $f_{i+1}(z) = g_{i+1}(z)$ when $z \notin \bigcap_{j \leq i+1} X_{j,p(j)}$. On the other hand, if $z \in \bigcap_{j \leq i+1} X_{j,p(j)}$ then

$$f_{i+1}(z) = a_{i+1} \neq b_{i+1} = g_{i+1}(z)\,.$$

The two functions $f_{i+1}, g_{i+1}$ obviously satisfy all our requirements. This concludes our proof of the lemma. □

**Lemma 14.4** *Every algebra in $\mathcal{V}$ is Abelian.*

**Proof** We assume that the lemma is false, in order to get a contradiction. let $\mathbf{A}$ be a non-Abelian algebra in $\mathcal{V}$ of least cardinality. Then it follows that $\mathbf{A}$ is finite, is subdirectly irreducible, and where $\mu$ is the monolith of $\mathbf{A}$, we have that $\mathbf{A}/\mu$ is Abelian. By Lemma 14.3, we have $[1_A, \mu] = 0_A$, and our assumption of least cardinality implies that $\mu = [1_A, 1_A]$.

Our proof will consist in constructing, for every structure $(X, E)$ consisting of an equivalence relation $E$ over a finite set $X$, an algebra $\mathbf{R}(X, E) = \mathbf{A}^X/\Theta_E$ (for a certain congruence $\Theta_E$ on $\mathbf{A}^X$), and proving that $\mathbf{R}(X, E_1) \cong \mathbf{R}(X, E_2)$ iff $(X, E_1) \cong (X, E_2)$. If $|X| = k$ then the number of non-isomorphic equivalence-relation structures $(X, E)$ is $\pi(k)$, the number of partitions of the integer $k$. Thus $\mathbf{A}^k$ has at least $\pi(k)$ non-isomorphic quotient algebras.

We shall show that $\mathbf{A}^k$ is generated by a set of at most $|A|k$ many elements. Thus it will follow that $\mathrm{G}_{\mathcal{V}}(|A|^2 k) \geq \pi(k)$. But $\pi(k)$ is known to be asymptotic to

$$\frac{1}{4k\sqrt{3}} e^{\left(\pi\sqrt{\frac{2k}{3}}\right)}$$

(confer G. E. Andrews [1], p. 70). Thus we have a clear contradiction to our assumption that $\mathcal{V}$ has very few models. The contradiction will establish that all algebras in $\mathcal{V}$ are Abelian.

Let $d(x, y, z)$ be a Maltsev term for $\mathcal{V}$. Suppose that $X = \{1, \ldots, k\}$. Choose $a_0 \in A$. We show that $\mathbf{A}^X$ is generated by the set

$$G = \{[a_0, b]_x : b \in A \text{ and } x \in X\}\,,$$

thus establishing that $\mathbf{A}^X$ is $|A|k$-generated. Indeed, if $(a_1, a_2, \ldots, a_k) \in A^X$, then each of the functions $f_i = [a_0, a_i]_i$ $(0 \leq i \leq k)$ belongs to $G$, and therefore

$$(a_1, \ldots, a_k) = d(d(\ldots(d(d(f_1, f_0, f_2), f_0, f_3)\ldots, f_0, f_{k-1}), f_0, f_k)$$

belongs to the subalgebra generated by $G$.

Now let $(X, E)$ be a finite equivalence-relation structure. Before defining $\Theta_E$, we choose and fix a non-trivial $\mu$-equivalence class $N$, and an element of $N$ which we will denote by 0. Let $\mathbf{A}|_N$ denote the set $N$ supplied with all the functions $f : N^m \to N$ (for any positive integral $m$) such that $f = g|_N$ for some polynomial operation $g$ of the algebra $\mathbf{A}$. Since $\mu$ is an Abelian congruence, and $d|_N$ is a Maltsev operation on $N$, then $\mathbf{A}|_N$ is an Abelian algebra in a certain congruence modular variety. By Theorem 9.10, $\mathbf{A}_N$ is polynomially equivalent to a module $\mathbf{M}$ over a ring $\mathbf{R}$ with unit. Without any loss of generality, we can assume that 0 is the zero-element of this module.

Where $\bar{0}$ denotes the constant function in $N^X$ with value 0, we define $\Theta_E$ to be the congruence relation of $\mathbf{A}^X$ generated by the set

$$G_E = \left\{ (f, \bar{0}) : f \in N^X \text{ and } \sum_{x \in Z} f(x) = 0 \text{ for all } Z \in X/E \right\}.$$

The sums in this definition are finite sums in the module.

Since all generating pairs of $\Theta_E$ are $\bar{\mu}$-related, we get

$$\Theta_E \subseteq \bar{\mu}\,, \tag{14.1}$$

where $\bar{\mu}$ is the kernel of the homomorphism of $\mathbf{A}^X$ onto $(\mathbf{A}/\mu)^X$. Moreover,

$$\begin{aligned} &\text{if } f^0, f^1 \in N^X \text{ then } \langle f^0, f^1 \rangle \in \Theta_E \text{ iff } \textstyle\sum_{x \in Z} f^0(x) = \sum_{x \in Z} f^1(x) \\ &\text{for all } Z \in X/E\,. \end{aligned} \tag{14.2}$$

To prove the "if" in (14.2), note that the assumption that $\sum_{x \in Z} f^0(x) = \sum_{x \in Z} f^1(x)$ for all $Z \in X/E$ gives $f^0 - f^1 \equiv \bar{0} \pmod{\Theta_E}$ and therefore $\langle f^0, f^1 \rangle \in \Theta_E$.

Conversely, assume that $f^0, f^1 \in N^X$ and $\langle f^0, f^1 \rangle \in \Theta_E$. Then the congruence permutability of the variety generated by $\mathbf{A}$ implies that there is a polynomial, say $n$-ary, $H(x_1, \ldots, x_n)$ of $\mathbf{A}^X$ and $f_1, \ldots, f_n \in N^X$ such that $\sum_{x \in Z} f_i(x) = 0$ for all $Z \in X/E$ and

$$f^0 = H(f_1, \ldots, f_n),\ f^1 = H(\bar{0}, \ldots, \bar{0})\,.$$

This means that there is an $n+m$-ary polynomial $h(x_1, \ldots, x_n, y_1, \ldots, y_m)$ of $\mathbf{A}$ and $g_1, \ldots, g_m \in A^X$ with

$$f^0 = h(f_1, \ldots, f_n, g_1, \ldots, g_m),\ f^1 = h(\bar{0}, \ldots, \bar{0}, g_1, \ldots, g_m)\,.$$

It follows that $h(a_1, \ldots, a_n, g_1(x), \ldots, g_m(x)) \in N$ whenever $\{a_1, \ldots, a_n\} \subseteq N$ and $x \in X$ (since $N$ is an equivalence class of the congruence $\mu$).

Choose $x_0 \in X$ and put $Z = x_0/E$. We apply the fact that $[\mu, 1_A] = 0_A$ to the equation

$$h(\underline{0}, \ldots, \underline{0}, \bar{g}(x)) - h(0, \ldots, 0, \bar{g}(x)) = h(\underline{0}, \ldots, \underline{0}, \bar{g}(x_0)) - h(0, \ldots, 0, \bar{g}(x_0))$$

replacing the underlined elements to obtain

$$h(u_1, \ldots, u_n, \bar{g}(x)) - h(0, \ldots, 0, \bar{g}(x)) = h(u_1, \ldots, u_n, \bar{g}(x_0)) - h(0, \ldots, 0, \bar{g}(x_0))$$

for all $x \in Z$ and $u_1, \ldots, u_n \in N$. Thus

$$h(u_1, \ldots, u_n, \bar{g}(x)) = h(u_1, \ldots, u_n, \bar{g}(x_0)) - h(0, \ldots, 0, \bar{g}(x_0)) + h(0, \ldots, 0, \bar{g}(x))\,.$$

The map $(u_1, \dots, u_n) \mapsto h(u_1, \dots, u_n, \bar{g}(x_0)) - h(0, \dots, 0, \bar{g}(x_0))$ is a polynomial of the module $\mathbf{M}$ that maps $(0, \dots, 0)$ to 0; thus it must be of the form $(u_1, \dots, u_n) \mapsto \sum_{1 \le i \le n} \lambda_i u_i$ for some $\lambda_i \in R$. Thus

$$h(u_1, \dots, u_n, \bar{g}(x)) = \sum_{i=1}^{i=n} \lambda_i u_i + h(0, \dots, 0, \bar{g}(x))$$

for all $x \in Z$ and $u_1, \dots, u_n \in N$. This implies that

$$f^0(x) = h(f_1(x), \dots, f_n(x), \bar{g}(x)) = \sum_{i=1}^{i=n} \lambda_i f_i(x) + h(0, \dots, 0, \bar{g(x)})$$

$$= \sum_{i=1}^{i=n} \lambda_i f_i(x) + f^1(x)\,.$$

Together with $\sum_{x \in Z} f_i(x) = 0$, this gives

$$\sum_{x \in Z} f^0(x) = \sum_{x \in Z} f^1(x)$$

as required in (14.2).

Now, for a subset $B \subseteq X$ we define the following congruences of $\mathbf{A}^X$:

$$\eta_B = \left\{ \langle f, g \rangle \in A^X \times A^X : f_t = g_t \ \text{ for all } t \in B \right\},\ \eta'_B = \eta_{X \setminus B}\,.$$

For a congruence $\phi$ of $\mathbf{A}$ we put

$$\phi_B = \left\{ \langle f, g \rangle \in A^X \times A^X : \langle f_t, g_t \rangle \in \phi \ \text{ for all } t \in B \right\},\ \phi'_B = \phi_B \cap \eta'_B\,.$$

Also, we write $\eta_t, \eta'_t, \phi_t, \phi'_t$ instead of $\eta_{\{t\}}, \eta'_{\{t\}}, \phi_{\{t\}}, \phi'_{\{t\}}$, respectively. For any congruence $\gamma$ of $\mathbf{A}^X$, the congruence $(\gamma \vee \Theta_E)/\Theta_E$ of $\mathbf{A}^X/\Theta_E$ will be denoted by $\tilde{\gamma}$.

Next, we observe that

$$\mu'_t \ \text{ is the unique atom of } \mathbf{Con}(\mathbf{A}^X) \text{ that is below } \eta'_t\,. \tag{14.3}$$

To see this, note that $\eta_t \vee \eta'_t = 1$ and $\eta_t \wedge \eta'_t = 0$, hence by modularity in the congruence lattice, the intervals $I[0, \eta'_t]$ and $I[\eta_t, 1]$ are transposes, and hence isomorphic. Thus the interval $I[0, \eta'_t]$, isomorphic to $\mathbf{Con}\,\mathbf{A}$, has the unique atom $\mu_t \wedge \eta'_t = \mu'_t$.

Choose and fix any $a \in N \setminus \{0\}$, and for $x \in X$ put $a^x = [0, a]_x$. Note that we have $\mu'_x = \mathrm{Cg}(\bar{0}, a^x)$ (the congruence generated by the pair $\langle \bar{0}, a^x \rangle$) since $\mu'_x$ is an atom. Then since $\langle \bar{0}, a^x \rangle \notin \Theta_E$ (by (14.2)), the covering pair $0 \prec \mu'_x$ projects up to $\Theta_E \prec \Theta_E \vee \mu'_x$ and therefore

$$\tilde{\mu}'_x \ \text{ is an atom in } \mathbf{Con}(\mathbf{A}^X/\Theta_E)\,. \tag{14.4}$$

Moreover,

$$\tilde{\mu}'_t = \tilde{\mu}'_s \ \text{ iff } \ \langle t, s \rangle \in E\,. \tag{14.5}$$

In fact, if $\langle t, s \rangle \in E$ then (14.2) gives $\langle a^t, a^s \rangle \in \Theta_E$, which easily yields the "if" direction in (14.5).

Conversely, suppose that $\langle t, s\rangle \notin E$. If $\tilde{\mu}'_t = \tilde{\mu}'_s$, then $\langle a^t, \bar{0}\rangle \in \Theta_E \vee \mu'_s$. Then by congruence permutability, we have an element $f \in A^X$ with

$$a^t \,\Theta_E\, f \,\mu'_s\, \bar{0}\,.$$

Since $\langle a^t, f\rangle \in \bar{\mu}$ then $f \in N^X$. Then applying (14.2) to $a^t\,\Theta_E\, f$ and $Z = s/E$ we get that $\sum_{z\in Z} f(z) = 0$. On the other hand, from $f\,\mu'_s\,\bar{0}$ we have that $f(z) = 0$ for all $z \in X \setminus \{s\}$. Consequently, $f = \bar{0}$, i.e., $\langle a^t, \bar{0}\rangle \in \Theta_E$, which contradicts (14.2).

Next we show:

$$\text{For } \gamma \in \mathrm{Con}(\mathbf{A}^X) \text{ and } t \in X \text{ either } [\gamma, 1] \subseteq \eta_t \text{ or } \mu'_t \subseteq [\gamma, 1]\,. \tag{14.6}$$

Indeed, suppose that $[\gamma, 1] \not\subseteq \eta_t$. Then there is a term $\tau(x, \bar{y})$, a pair $\langle f, g\rangle \in \gamma$ and tuples $\bar{c}, \bar{d}$ in $\mathbf{A}^X$ such that $\langle \tau(f, \bar{c}), \tau(f, \bar{d})\rangle \in \eta_t$ and $\langle \tau(g, \bar{c}), \tau(g, \bar{d})\rangle \notin \eta_t$. Let $\bar{d}' = [\bar{c}, \bar{d}]_t$. Then $\tau(f, \bar{c}) = \tau(f, \bar{d}')$, $\tau(g, \bar{c}) \neq \tau(g, \bar{d}')$, so that $0 \neq [\gamma, \eta'_t] \leq \eta'_t$. Then (14.3) gives $\mu'_t \subseteq [\gamma, 1]$, as required.

Let us call a congruence of $\mathbf{A}^X/\Theta_E$ *regular* if it is the only atom below a congruence of the form $[\gamma, 1]$. We prove:

$$\begin{aligned}&\text{A congruence of } \mathbf{A}^X/\Theta_E \text{ is regular iff it is of the form } \tilde{\mu}'_t \text{ for some}\\ &t \in X\,.\end{aligned} \tag{14.7}$$

First, suppose that $\alpha, \gamma \geq \Theta_E$ are such that $\tilde{\alpha}$ is the unique atom below $[\gamma/\Theta_E, 1/\Theta_E]$. Then $[\gamma, 1] \neq 0$ and we can choose $t$ such that $[\gamma, 1] \not\leq \eta_t$. By (14.6), we have $\mu'_t \leq [\gamma, 1]$. Thus $\tilde{\mu}'_t \leq [\gamma/\Theta_E, 1/\Theta_E]$. By uniqueness of $\tilde{\alpha}$, we have that $\tilde{\alpha} = \tilde{\mu}'_t$ as required.

To prove that $\tilde{\mu}'_t$ is regular, it suffices to show that $\mu'_t \vee \Theta_E$ is the only congruence $\alpha$ with $\Theta_E \prec \alpha \subseteq [\eta'_t, 1] \vee \Theta_E$. Obviously, $[\eta'_t, 1] \subseteq [1, 1] \subseteq \bar{\mu}$ and so $[\eta'_t, 1] \subseteq \eta'_t \cap \bar{\mu} = \mu'_t$. Since $\eta'_t \vee \eta_t = 1$ and $\mathbf{A} \models [1, 1] \neq 0$, then $[\eta'_t, 1] \neq 0$. We now have that $[\eta'_t, 1] = \mu'_t$ since $\mu'_t$ is an atom. We know that $\Theta_E \prec \mu'_t \vee \Theta_E$ by (14.3). Thus it follows that $\tilde{\mu}'_t$ is regular.

From (14.5) and (14.7) we have that the number of $E$-classes in $X$ can be recovered from $\mathbf{A}^X/\Theta_E$—it is the number of regular atoms in the congruence lattice of this algebra.

We will prove that non-isomorphic structures $(X, E)$, $(X, E')$ give rise to non-isomorphic algebras $\mathbf{A}^X/\Theta_E$, $\mathbf{A}^X/\Theta_{E'}$ by showing that the sizes of the equivalence classes of $E$ are also recoverable from $\mathbf{A}^X/\Theta_E$.

Note that for the center $\zeta$ of $\mathbf{A}$ we have $\mu \leq \zeta < 1$. Obviously,

$$\mathbf{A}^X/\zeta_B \text{ is isomorphic to } (\mathbf{A}/\zeta)^B, \text{ for any } B \subseteq X\,. \tag{14.8}$$

We have $\Theta_E \subseteq \bar{\mu} \subseteq \zeta_X \subseteq \zeta_B$ for $B \subseteq X$, whence $(\mathbf{A}^X/\Theta_E)/(\zeta_B/\Theta_E) \cong (\mathbf{A}/\zeta)^B$ and $|B|$ is the logarithm of the cardinality of this algebra to the base $|\mathbf{A}/\zeta|$. Thus, we can finish the proof of this lemma by showing that the set of congruences of the form $\zeta_{X\setminus Z}/\Theta_E$ with $Z$ ranging over $X/E$ is definable in $\mathbf{A}^X/\Theta_E$.

Let us call a congruence $\delta$ of $\mathbf{A}^X/\Theta_E$ *co-regular* if $\delta$ is a maximal congruence with the property that the commutator $[\delta, 1]$ contains exactly one atom. We conclude our proof by showing:

$$\text{A congruence } \delta \text{ is co-regular iff } \delta = \zeta_{X\setminus Z}/\Theta_E \text{ for some } Z \in X/E. \tag{14.9}$$

To begin, let $t \in Z \in X/E$. Now $\zeta_{X\setminus Z} \vee \eta_t = 1$, so $[\zeta_{X\setminus Z}, 1] \vee \eta_t = [1,1] \vee \eta_t = \mu_t$, implying $[\zeta_{X\setminus Z}, 1] \not\leq \eta_t$. Then by (14.6), $[\zeta_{X\setminus Z}, 1] \geq \mu'_t$. On the other hand, clearly we have

$$[\zeta_{X\setminus Z}, 1] \leq \mu'_Z = \bigvee_{s\in Z} \mu'_s$$

and this combined with the above conclusion yields

$$[\zeta_{X\setminus Z}, 1] = \mu'_Z = \bigvee_{s\in Z} \mu'_s \,.$$

Then

$$[\zeta_{X\setminus Z}/\Theta_E, 1/\Theta_E] = [\zeta_{X\setminus Z}, 1] \vee \Theta_E = \bigvee_{s\in Z} \tilde{\mu}'_s = \tilde{\mu}'_t \,.$$

Next, suppose that $\Theta_E \leq \gamma$ and $\gamma/\Theta_E$ is co-regular. Then $[\gamma/\Theta_E, 1/\Theta_E]$ contains exactly one atom, and by (14.7), this atom must be of the form $\tilde{\mu}'_t$. Say $\tilde{\mu}'_t \leq [\gamma/\Theta_E, 1/\Theta_E]$ and $t/E = Z$. Then for $s \in X \setminus Z$, $[\gamma, 1]$ cannot contain $\mu'_s$ and so by (14.6), $[\gamma, 1] \leq \eta_s$. Since this holds for all $s \in X \setminus Z$, we have $[\gamma, 1] \leq \eta'_Z$. This is easily seen to imply that $\gamma \leq \zeta_{X\setminus Z}$. We have seen in the last paragraph that $[\zeta_{X\setminus Z}/\Theta_E, 1/\Theta_E] = \tilde{\mu}'_t$. The maximality of $\gamma$ now gives that $\gamma = \zeta_{X\setminus Z}$. The results of this paragraph and the last one, combined, yield (14.9). □

The next lemma completes our proof of Theorem 14.2.

**Lemma 14.5** *A locally finite affine variety has very few models iff it is directly representable.*

**Proof** Assume that $\mathcal{A}$ is a locally finite, congruence modular, Abelian variety, and let $\mathbf{R}$ denote the finite ring such that $\mathcal{A}$ is polynomially equivalent with ${}_{\mathbf{R}}\mathcal{M}$.

For a positive integer $n$, let $\mathbf{F} = \mathbf{F}_{\mathcal{A}}(n)$ be the free algebra in $\mathcal{A}$ freely generated by $x_1, \ldots, x_n$. Let $\mathbf{M}$ be the $\mathbf{R}$-module polynomially equivalent to $\mathbf{F}$, with $x_n$ chosen as the zero element. Every element $w \in F$ can be written as $t^{\mathbf{F}}(x_1, \ldots, x_n)$ for a term $t$, and the operation $t^{\mathbf{F}}$ in $F$ can be expressed as

$$t^{\mathbf{F}}(b_1, \ldots, b_n) = \sum_{1\leq i\leq n} r_i b_i + c$$

for some $r_i \in R$ and $c \in F$. Thus $w = \sum_{1\leq i\leq n-1} r_i x_i + c$ is determined by the sequence $\langle r_i : 1 \leq i \leq n-1\rangle$ and the element $t^{\mathbf{F}}(x_n, \ldots, x_n) = c$. This means that $f_n = |\mathbf{F}_{\mathcal{A}}(n)| \leq r^{n-1} f_1$ where $r = |R|$ and $f_1 = |\mathbf{F}_{\mathcal{A}}(1)|$.

Now suppose that $\mathcal{A}$ is directly representable. Let $\mathbf{D}_0, \ldots, \mathbf{D}_{k-1}$ be a list of all the directly indecomposable finite algebras in $\mathcal{A}$, up to isomorphism. If $\mathbf{B}$ is an $n$-generated member of $\mathcal{A}$, then $|B| \leq f_n \leq r^{n-1} f_1$. We can write

$$\mathbf{B} \cong \mathbf{D}_0^{\ell_0} \times \cdots \times \mathbf{D}_{k-1}^{\ell_{k-1}}$$

for some non-negative integers $\ell_i$, and here

$$\sum_i \ell_i \leq \log_2(f_n) \leq M(n-1)$$

for some positive integer $M$, independently of $n$. The number of solutions $(m_i)$ of the inequality $\sum_i m_i \leq M(n-1)$ is

$$\left( \begin{array}{c} M(n-1)+k \\ k \end{array} \right) \leq (M(n-1)+k)^k .$$

Thus $\mathrm{G}_{\mathcal{A}}(n) \leq (M(n-1)+k)^k$ which estabishes that $\mathcal{A}$ has very few models.

Conversely, suppose that $\mathcal{A}$ is not directly representable. Let $\mathcal{A}_p$ denote the class of all algebras in $\mathcal{A}$ that have a one-element subalgebra. Since $\mathcal{A}$ has at most $2^{f_n^2}$ non-isomorphic $n$-element members, then there is no finite bound on the size of the finite directly indecomposable members of $\mathcal{A}$. For $\mathbf{A} \in \mathcal{A}$, the algebra $\mathbf{A}_\nabla \in \mathcal{A}_p$ has the same corresponding module, up to isomorphism, and is directly indecomposable iff $\mathbf{A}$ is. (Confer the discussion at the end of Section 9.) Where $d(k)$ denotes the number of non-isomorphic, directly indecomposable, $k$-generated algebras in $\mathcal{A}_p$, we thus have that $d(k)$ is unbounded.

For a fixed $k$, let $\mathbf{D}_0, \ldots, \mathbf{D}_{d-1}$ be pairwise non-isomorphic, directly indecomposable, $k$-generated members of $\mathcal{A}_p$, where $d(k) = d$. By a theorem of G. Birkhoff (see, for example, R. McKenzie, G. McNulty, W. Taylor [37], Theorem 5.3), finite algebras with permuting congruences and a one-element subalgebra have the unique factorization property. This means that if $\langle m_i \rangle_{i<d}$, $\langle m'_i \rangle_{i<d}$ are sequences of non-negative integers and $\prod_{i<d} \mathbf{D}_i^{m_i} \cong \prod_{i<d} \mathbf{D}_i^{m'_i}$ then $m_i = m'_i$ for all $i < d$. Now if $\sum_{i<d} m_i \leq n$ then $\prod_{i<d} \mathbf{D}_i^{m_i}$ is $nk$ generated. (This follows by the same argument used in the proof of Lemma 14.4 to show that $\mathbf{A}^k$ is $|A|k$-generated.) Thus $\mathrm{G}_{\mathcal{A}_p}(nk)$ is at least as great as the number of systems $\langle m_i \rangle_{i<d}$ of non-negative integers satisfying $\sum_{i<d} m_i \leq n$. I.e., we have

$$\mathrm{G}_{\mathcal{A}_p}(nk) \geq \left( \begin{array}{c} n+d(k) \\ n \end{array} \right) .$$

In particular, $\mathrm{G}_{\mathcal{A}}(k^2) \geq \left( \begin{array}{c} k+d(k) \\ k \end{array} \right)$. For any fixed positive integer $M$, we have $d(k) \geq M$ for large $k$, and for such $k$, it follows that $\mathrm{G}_{\mathcal{A}}(k^2) \geq \left( \begin{array}{c} k+M \\ k \end{array} \right)$. Since this is a polynomial of degree $M$ in $k$, then $\mathrm{G}_{\mathcal{A}}(k)$ cannot be bounded for all $k$ by a polynomial of degree $< M/2$. This ends our proof that if $\mathcal{A}$ is not directly representable then $\mathrm{G}_{\mathcal{A}}$ is not bounded by any polynomial function. □

## 15 Problems

**Problem 15.1** Is there an algorithm to determine, given a finite ring $\mathbf{R}$ with unit, whether the variety $\mathbf{R}\mathcal{M}$ of left unitary $\mathbf{R}$-modules is decidable? F. Point, M. Prest [40] and M. Prest [41] provide a starting point for the exploration of what is known about this problem.

**Problem 15.2** Is there an algorithm to determine, given a finite algebra $\mathbf{F}$ of finite type such that $\mathrm{HSP}(\mathbf{F})$ has modular congruence lattices, whether $\mathrm{HSP}(\mathbf{F})$ (or $\mathrm{SP}(\mathbf{F})$) is finitely axiomatizable? By a famous theorem of K. Baker [2], every finitely generated congruence distributive variety of finite type is finitely axiomatizable. R. McKenzie [36] proved that there is no algorithm to determine if $\mathrm{HSP}(\mathbf{F})$ is finitely axiomatizable where $\mathbf{F}$ ranges over all finite algebras with one binary operation.

**Problem 15.3** Prove or disprove that for every finite set $A$ and every operation $m = m(x, y, z)$ over $A$ that satisfies Maltsev's equations $m(x, x, y) \approx y \approx m(y, x, x)$, there are only countably many clones of operations on $A$ containing $m$. A. A. Bulatov, P. M. Idziak [3] has results on this problem.

**Problem 15.4** Is it true that every congruence modular variety of finite type that is residually finite has a finite residual bound? K. Kearnes, R. Willard [29] proved that this implication holds for congruence distributive varieties of finite type, and more generally for congruence meet semi-distributive varieties of finite type.

**Problem 15.5** Characterize the locally finite congruence modular varieties $\mathcal{V}$ that possess first-order definable principal congruences—i.e., there is a first-order formula $\theta(x, y, u, v)$ so that for all $\mathbf{A} \in \mathcal{V}$ and $\{a, b, c, d\} \subseteq A$, $\mathbf{A} \models \theta(a, b, c, d)$ iff $\langle a, b\rangle$ lies in the congruence of $\mathbf{A}$ generated by $\langle c, d\rangle$.

## References

[1] G. E. Andrews, *The Theory of Partitions,* Encyclopedia Math. Appl. 2, Addison-Wesley, Reading, MA, 1976.

[2] Finite equational bases for finite algebras in congruence-distributive equational class, *Advances in Math.* **24** (1977), 207–243.

[3] A. A. Bulatov and P. M. Idziak, Counting Maltsev clones on small sets, *Discrete Math.* **268** (2003), no. 1–3, 59–80.

[4] S. Burris and R. McKenzie, *Decidability and Boolean Representations*, AMS Memoirs **32**, no. 246, 1981.

[5] G. Czédli and E. Horváth, All congruence identities implying modularity have Maltsev conditions (preprint).

[6] G. Czédli and E. Horváth and P. Lipparini, Optimal Maltsev conditions for congruence modular varieties (preprint).

[7] A. Day, A characterization of modularity for congruence lattices of algebras, *Canadian Math. Bull.* **12** (1969), 167–173.

[8] A. Day and R. Freese, A Characterization of Identities Implying Congruence Modularity, *Can. J. Math.* **32** (1980), 1140–1167.

[9] R. Dedekind, Uber die von drei modulun erzeugte dualgruppe, *Math. Ann.* **53** (1900), 371–403.

[10] I. Fleischer, A note on subdirect products, *Acta Math. Acad. Sci. Hungar.* **6** (1955), 463–465.

[11] R. Freese and R. McKenzie, Residually small varieties with modular congruence lattices, *Transactions Amer. Math. Soc.* **264** (1981), 419–430.

[12] R. Freese and R. McKenzie, *Commutator theory for congruence modular varieties*, London Mathematical Society Lecture Note Series, no. 125, Cambridge University Press, 1987.

[13] H.-P. Gumm, Uber die losungermenge von gleichungssystemen uber allgemeinen algebren, *Math Z.* **162** (1978), 51–62.

[14] H.-P. Gumm, Algebras in permutable varieties: geometrical properties of affine algebras, *Algebra Universalis* **9** no. 1, (1979), 8–34.

[15] H.-P. Gumm, An easy way to the commutator in modular varieties, *Proc. Amer. Math. Soc.* **80** (1980), 393–397.

[16] H.-P. Gumm, Congruence modularity is permutability composed with distributivity, *Archiv der Math. (Basel)* **36** (1981), 569–576.

[17] H.-P. Gumm, *Geometrical methods in congruence modular varieties*, AMS Memoir **36**, no. 286, 1983.

[18] H.-P. Gumm and C. Herrmann, Algebras in modular varieties: Baer refinements, cancellation and isotopy, *Houston J. Math.* **5** (1979), 503–523.

[19] J. Hagemann and C. Herrmann, A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity, *Arch. Math.* Basel **32** (1979), 234–245.

[20] C. Herrmann, Affine algebras in congruence modular varieties, *Acta Sci. Math. (Szeged)* **41** (1979), 119–125.

[21] D. Hobby and R. McKenzie, *The Structure of Finite Algebras,* American Mathematical Society Contemporary Mathematics Series, no. 76, 1988 [revised edition 1996].

[22] P. M. Idziak, A characterization of finitely decidable congruence modular varieties, *Transactions Amer. Math. Soc.* **349** (1997), 903–934.

[23] P. M. Idziak and R. McKenzie, Varieties with polynomially many models, *Fundamenta Mathematicae* **170** (2001), 53–68.

[24] P. M. Idziak and R. McKenzie and M. Valeriote, The structure of locally finite varieties with polynomially many models, preprint

[25] B. Jónsson, Algebras whose congruence lattices are distributive, *Math. Scand.* **21** (1967), 110–121.

[26] K. A. Kearnes, On the relationship between AP, RS and CEP, *Proc. American Math. Soc.* **105** (1989), no. 4, 827–839.

[27] K. A. Kearnes and R. McKenzie, Commutator theory for relatively modular quasivarieties, *Transactions Amer. Math. Soc.* **331** (1992), 465–502.

[28] K. A. Kearnes and A. Szendrei, The relationship between two commutators, *Inter. J. Algebra. Comput.* **8** (1998), 497–531.

[29] K. A. Kearnes and R. Willard, Residually finite, congruence meet semi-distributive varieties of finite type have a finite residual bound, *Proc. Amer. Math. Soc.* **127** (1999), no. 10, 2841–2850.

[30] H. Lakser and W. Taylor and S. T. Tschantz, A new proof of Gumm's theorem, *Algebra Universalis* **20** (1985), 115–122.

[31] A. I. Maltsev, On the general theory of algebraic systems, *Mat. Sbornik* **77** (1954), 3–20.

[32] R. McKenzie, Narrowness implies uniformity, *Algebra Universalis* **15** (1982), 67–85.

[33] R. McKenzie, Finite equational bases for congruence modular varieties, *Algebra Universalis* **24** (1987), 224–250.

[34] R. McKenzie and M. Valeriote, *The Structure of Decidable Locally Finite Varieties*, Birkhauser, Progress in Mathematics, vol. 79, 1989.

[35] R. McKenzie, The residual bounds of finite algebras, *Inter. J. Algebra. Comput.* **6** (1996), 1–28.

[36] R. McKenzie, Tarski's finite basis problem is undecidable, *Inter. J. Algebra. Comput.* **6** (1996), 49–104.

[37] R. McKenzie and G. McNulty and W. Taylor, *Algebras, Lattices, Varieties,* Volume I, Wadsworth and Brooks/Cole, Monterey, California, 1987.

[38] A. F. Pixley, Distributivity and permutability of congruence relations in equational classes of algebras, *Proc. Amer. Math. Soc.* **14** (1963), 105–109.

[39] A. F. Pixley, Local Malcev conditions, *Canad. Math. Bull.* **15** (1972), 559–568.

[40] F. Point and M. Prest, Decidabity for theories of modules, *J. London Math. Soc. (2)* **38** (1988), no. 2, 193–206.

[41] M. Prest, *Model Theory and Modules*, London Mathematical Society Lecture Note Series, 130, Cambridge University Press, Cambridge, 1988.

[42] R. W. Quackenbush, Equational classes generated by finite algebras, *Algebra Universalis* **1** (1971), 265–266.

[43] J. D. H. Smith, *Mal'cev Varieties*, Springer-Verlag, Lecture Notes in Mathematics, vol. 554, New York, 1976.

[44] J.W. Snow, Generating primitive positive clones, *Algebra Universalis* **44** (2000), 169–185.

[45] W. Taylor, Some applications of the term condition, *Algebra Universalis* **14** (1982), 11–24.

[46] R. Wille, *Kongruenzklassengeometrien*, Springer-Verlag, Lecture Notes in Mathematics, vol. 113, New York, 1970.

## Index of Terms and Notation