Commutator Theory for Congruence Modular Varieties

Ralph Freese and Ralph McKenzie

Contents

Introduction

In the theory of groups, the important concepts of Abelian group, solvable group, nilpotent group, the center of a group and centralizers, are all defined from the binary operation $[x, y] = x^{-1}y^{-1}xy$. Each of these notions, except centralizers of elements, may also be defined in terms of the commutator of normal subgroups. The commutator $[\mathbf{M}, \mathbf{N}]$ (where $\mathbf{M}$ and $\mathbf{N}$ are normal subgroups of a group) is the (normal) subgroup generated by all the commutators $[x, y]$ with $x \in M$, $y \in N$. Thus we have a binary operation in the lattice of normal subgroups. This binary operation, in combination with the lattice operations, carries much of the information about how a group is put together. The operation is also interesting in its own right. It is a commutative, monotone operation, completely distributive with respect to joins in the lattice.

There is an operation naturally defined on the lattice of ideals of a ring, which has these properties. Namely, let $[\mathbf{J}, \mathbf{K}]$ be the ideal generated by all the products jk and kj, with $j \in J$ and $k \in K$. The congruity between these two contexts extends to the following facts: $[\mathbf{M}, \mathbf{M}]$ is the smallest normal subgroup $\mathbf{U}$ of $\mathbf{M}$ for which $\mathbf{M}/\mathbf{U}$ is a commutative group; $[\mathbf{J}, \mathbf{J}]$ is the smallest ideal $\mathbf{K}$ of $\mathbf{J}$ for which the ring $\mathbf{J}/\mathbf{K}$ is a commutative group; that is, a ring with trivial multiplication.

Now it develops, amazingly, that a commutator can be defined rather naturally in the congruence lattices of every congruence modular variety. This operation has the same useful properties that the commutator for groups (which is a special case of it) possesses. The resulting theory has many general applications and, we feel, it is quite beautiful.

In this book we present the basic theory of commutators in congruence modular varieties and some of its strongest applications. The book by H. P. Gumm [**41**] offers a quite different approach to the subject. Gumm developed a sustained analogy between commutator theory and affine geometry which allowed him to discover many of the basic facts about the commutator. We take a more algebraic approach, using some of the shortcuts that Taylor and others have discovered.

Historical remarks. The lattice of normal subgroups of a group, with the commutator operation, is a lattice ordered monoid. It is a residuated lattice (in G. Birkhoff's terminology) because $(a : b)$ (equal to the largest lattice element x such that $[b, x] \leq a$) always exists. The concept of a lattice ordered monoid, which arose naturally in ideal theory, has been studied by Krull, Birkhoff, Ward and Dilworth, and numerous others. (See Birkhoff's *Lattice Theory*, Ch. XIV, especially Section 8 on commutation lattices.)

The theory presented in this book does not lie in the tradition of these ongoing axiomatic studies, although it may throw some new light on the subject. The worth of our theory stems, rather, from its very broad applicability combined with depth. We shall be working within a broad class of algebras of diverse kinds, with a general definition of commutator which turns out to determine a unique operation over every algebra. The commutator proves to be an excellent tool for arriving at deep algebraic results in this very general setting. The first commutator theory approaching this level of generality was created by the English mathematician J. D. H. Smith, and presented in his 1976 book *Mal'cev Varieties*. Smith dealt with an important subclass of the congruence modular varieties, namely the varieties in whose algebras all congruences permute, which he called Mal'cev Varieties. His theory rapidly evolved into the theory we shall present. The work was done chiefly by the German mathematicians J. Hagemann and C. Herrmann, and presented in their papers Hagemann-Herrmann [**44**] and Herrmann [**45**]. Many important details and simplifications were worked out later by other people, notably by H. P. Gumm and W. Taylor.

General remarks. The operation we shall study is a binary operation defined for pairs of congruences $\langle \theta, \psi \rangle$ of an algebra and giving another congruence $[\theta, \psi]$. This operation can be easily defined for congruences of any algebra, but it seems to be especially well behaved only for algebras in congruence modular varieties. Two of its properties contribute most obviously to its strength in applications.

Let $\mathbf{A}$ be an algebra in a congruence modular variety, $\mathbf{L}$ be its lattice of congruences and θ and ψ be two members of L. If the commutator of θ and ψ is as large as the theory allows it to be – that is, if it is identical with the intersection of θ and ψ – then in the neighborhood of this pair of congruences $\mathbf{L}$ is very like a distributive lattice. Whenever $\psi \leq \psi_1 \vee \psi_2$, for example, then $\theta \wedge \psi \leq (\theta \wedge \psi_1) \vee (\theta \wedge \psi_2)$ (where $\vee$ and $\wedge$ denote join and meet in $\mathbf{L}$). There is a sophisticated way to state these facts. Consider this binary relation on $\mathbf{L}$: $\theta \sim \psi$ if and only if $\theta \vee \psi$ is solvable over $\theta \wedge \psi$. This is an equivalence relation and it respects commutators and lattice joins and meets. The quotient lattice

$\mathbf{L}/\sim$ is a distributive commutation lattice in which $[\alpha, \beta] = \alpha \wedge \beta$. We may remark that at one extreme end of the spectrum of congruence modular varieties, the congruence distributive varieties are precisely those in which the commutator is identical with the intersection in all congruence lattices.

The second important property concerns Abelian congruences. In a quotient algebra $\mathbf{B} = \mathbf{A}/[\theta, \psi]$, the congruence $\beta = \theta \wedge \psi/[\theta, \psi]$ is an Abelian congruence, that is $[\beta, \beta] = 0$. This implies that each equivalence class of β is an Abelian group and every operation of the algebra $\mathbf{B}$, with its variables restricted to range over fixed equivalence classes of β is a group homomorphism (plus a constant). In the extreme case, $\theta = \psi = 1_{\mathbf{A}}$ $(= \mathbf{A} \times \mathbf{A})$ and $[1_{\mathbf{A}}, 1_{\mathbf{A}}] = 0_{\mathbf{A}}$. The algebra $\mathbf{A}$ is then polynomially equivalent to a module over a ring.

Our presentation of commutator theory is essentially different from earlier published accounts. Hagemann and Herrmann defined the commutator of two congruences on an algebra $\mathbf{A}$, and derived its properties, by applying the modular law in a quite nontrivial fashion to congruences on subalgebras of $\mathbf{A}$, $\mathbf{A}^2$ and $\mathbf{A}^3$. A congruence of $\mathbf{A}$ is itself an algebra (a subalgebra of $\mathbf{A}^2$), and in fact they dealt mainly with congruences on congruences of $\mathbf{A}$. Gumm's approach to commutator theory (in [**38**], [**40**] and [**40**]) is heavily flavored with geometric analogies developed in his earlier papers [**36**] and [**39**], and is closer in spirit to what Smith did. Gumm made good use of A. Day's derived operations, whose existence for a variety is equivalent to congruence modularity. Our path to commutator theory is more direct than either of these. We define the commutator in any algebra by considering the set of all term operations of the algebra. Then assuming that algebra belongs to a congruence modular variety, we use Day's operations to present a set of generators for $[\theta, \psi]$. Following this result, the basic properties of commutators are easily derived.

This book is an expanded version of a manuscript entitled *The commutator, an overview* that we used as the text for a week long workshop on commutator theory held at the Puebla Conference on Universal Algebra and Lattice Theory in January 1982.

The first chapter of the present manuscript uses groups and rings to motivate the definition of the commutator. The second chapter gives a brief introduction to the results and definitions of universal algebra which will be required later. It also gives a proof of Day's characterization of varieties with modular congruence lattices. In the course of the proof we prove two useful lemmas. The third chapter gives several definitions of the commutator and proves some simple results which do not depend on congruence modularity. The fourth chapter

shows that all of these definitions of the commutator are equivalent in congruence modular varieties and proves some of the fundamental facts about the commutator.

The fifth chapter proves Herrmann's fundamental result on Abelian algebras and introduces Gumm's 3-ary term and his characterization of Abelian congruences. The sixth chapter proves various permutability theorems and gives Gumm's new Mal'cev condition for congruence modularity. The seventh chapter gives several results on nilpotent algebras, including a theorem describing the structure of such algebras. A result used in Burris-McKenzie [**8**], whose proof has not appeared in print before, is included. It is Proposition 7.8 (which was 8.7 in Burris-McKenzie).

Chapter 8 contains some results relating to congruence identities. These are identities in the join, meet and commutator operations satisfied by the congruence lattices. This subject is in its infancy and the results presented are far from representing a complete theory.

The blocks of an Abelian congruence of an algebra $\mathbf{A}$ in a (modular) variety $\mathcal{V}$ behave very much like modules over a ring built from the polynomials of $\mathbf{A}$. Chapter 9 defines rings naturally associated with $\mathcal{V}$. In our 1981 manuscript we only considered one ring for each $\mathcal{V}$, which we denoted $\mathbf{R}(\mathcal{V})$. In the present version we extend this concept in two ways. First we allow constants so that the ring is built from polynomials, not just terms. Secondly we form "matrix" rings. In this manner we are able to capture the polynomial action between different blocks of an Abelian congruence, not just the action within one block. Some strong structural connections between the module associated with an Abelian congruence and the algebra are proved. In the case that the variety consists solely of Abelian algebras the connection is especially strong. The last part of the chapter establishes the exact connection. In this case the algebra is polynomially equivalent to the module in a very specific way.

Chapter 10 uses the commutator theory to prove a variety of problems on structure and representation in modular varieties. The first section presents some generalizations of Jonsson's theorem to modular varieties. The second section proves various stronger results for finitely generated varieties. The third section uses some of the previous material and some results from Chapter 9 to prove the authors' characterization of finite algebras which generate a residually small variety. The fourth section defines the concept of chief factors and shows that if $\mathbf{A}$ is a finite algebra then the chief factors which occur in the variety generated by $\mathbf{A}$ have size bounded by $|A|$. As a corollary we

have that the simple algebras in the variety generated by $\mathbf{A}$ have size at most $|A|$.

Chapter 11 deals with joins and products of modular varieties. It is shown that for two such varieties, $\mathcal{V}_0$ and $\mathcal{V}_1$, if the subdirectly irreducible algebras in $\mathcal{V}_i$ have cardinality at most λ_i, $i = 0, 1$, then the subdirectly irreducible algebras in the join of those varieties have the cardinality at most $\lambda_0\lambda_1$. A generalization of a theorem of Herrmann on products of varieties is also given.

A finite simple algebra having no nontrivial subalgebras is called strictly simple. Chapter 12 deals with varieties generated by such algebras. We use the commutator theory to give relatively easy proofs of some of the results of D. Clark and P. Krauss. Chapter 13 studies Mal'cev conditions corresponding to the satisfaction by congruence lattices of certain lattice identities. Previously only the distributive law, the modular law, and the two trivial identities were known to have a Mal'cev condition. This chapter displays an infinite class of identities defined by Mal'cev conditions.

M. Vaughan-Lee has shown that a finite nilpotent algebra of prime power order having an equationally defined constant has a finite basis for its identities (assuming, of course that there are only finitely many basic operations). Chapter 14 proves this without the assumption that there is an equationally defined constant.

Exercises are given at the ends of most chapters. A great deal of important material is included in these exercises and the reader should at least glance at them. They include interesting examples and applications, as well as significant theorems. We have tried to avoid leaving routine calculations as exercises, and indeed some of the exercises require a substantial amount of ingenuity. But do not worry, you can always cheat: all of the solutions appear in the back. Because of this we have felt justified in using the results of the exercises.

The authors wish to thank C. Bergman, G. Birkhoff, A. Day, Heinz-Peter Gumm, W. Lampe and J. B. Nation for the interest and assistance they rendered us at several stages in the preparation of this manuscript.

CHAPTER 1

The Commutator in Groups and Rings

Let $\mathbf{G}$ be a group and let $\mathbf{L}(\mathbf{G})$ denote its lattice of normal subgroups. Suppose that $\mathbf{M}$, $\mathbf{N} \in \mathbf{L}(\mathbf{G})$. The group commutator (commutator of $\mathbf{M}$ and $\mathbf{N}$), written as $[\mathbf{M}, \mathbf{N}]$, is the subgroup of $\mathbf{G}$ generated by all elements $[m, n] = m^{-1}n^{-1}mn$, with $m \in \mathbf{M}$ and $n \in \mathbf{N}$. It is a normal subgroup of $\mathbf{G}$. We thus have a binary operation, called **commutator**, acting on normal subgroups. (The usual operations of a lattice are join and meet, here denoted by $\vee$ and $\wedge$.) If $\pi : \mathbf{G} \to \mathbf{G}'$ is an onto homomorphism, then $\mathbf{L}(\mathbf{G}')$ is naturally isomorphic to an interval in $\mathbf{L}(\mathbf{G})$ consisting of the members that lie above the kernel of π. We can easily determine commutators of normal subgroups in $\mathbf{G}'$ if we know the commutators of their inverse images in $\mathbf{G}$. (See (2) below.) Thus we are going to consider the commutator as an operation not just in one lattice $\mathbf{L}(\mathbf{G})$, but rather as a global operation, defined at once in all such lattices. The following properties are easily verified for $\mathbf{M}$, $\mathbf{N}$, $\mathbf{N}_i \in \mathbf{L}(\mathbf{G})$, $i \in I$, and $\pi : \mathbf{G} \twoheadrightarrow \mathbf{G}'$ a surjection.

(1) $$[\mathbf{M}, \mathbf{N}] \subseteq \mathbf{M} \cap \mathbf{N}$$

(2) $$[\pi(\mathbf{M}), \pi(\mathbf{N})] = \pi([\mathbf{M}, \mathbf{N}])$$

(3) $$[\mathbf{M}, \mathbf{N}] = [\mathbf{N}, \mathbf{M}]$$

(4) $$[\mathbf{M}, \bigvee_{i \in I} \mathbf{N}_i] = \bigvee_{i \in I} [\mathbf{M}, \mathbf{N}_i]$$

(5) $\mathbf{H} = [\mathbf{M}, \mathbf{N}]$ is the least normal subgroup of $\mathbf{G}$ such that in $\mathbf{G}/\mathbf{H}$ every element of $\mathbf{M}/\mathbf{H}$ commutes with every element of $\mathbf{N}/\mathbf{H}$.

The next property is not quite so obvious.

(6) The commutator is the greatest binary operation defined on $\mathbf{L}(\mathbf{G})$ for every group $\mathbf{G}$ and satisfying (1) and (2).

To prove this, we suppose that C is another binary operation defined in $\mathbf{L}(\mathbf{G})$ for every group $\mathbf{G}$ and that C satisfies (1) and (2). Let $\mathbf{M}$, $\mathbf{N} \in \mathbf{L}(\mathbf{G})$ for some group $\mathbf{G}$. We shall show that $C(\mathbf{M}, \mathbf{N}) \subseteq [\mathbf{M}, \mathbf{N}]$. To do this, we define four subgroups of $\mathbf{G} \times \mathbf{G}$:

$$\begin{aligned} \mathbf{G}(\mathbf{M}) &= \{\langle x, y\rangle : x \in G, x^{-1}y \in M\} \\ \Delta &= \{\langle x, y\rangle : x \in N, x^{-1}y \in [M, N]\} \\ \mathbf{B} &= \{\langle x, 1\rangle : x \in [M, N]\} \\ \mathbf{M}_1 &= \{\langle x, 1\rangle : x \in \mathbf{M}\}. \end{aligned}$$

Now one can verify that Δ, $\mathbf{B}$, $\mathbf{M}_1 \in \mathbf{L}(\mathbf{G}(\mathbf{M}))$. [This we leave to the reader. The fact that $\Delta \in \mathbf{L}(\mathbf{G}(\mathbf{M}))$ is what makes the proof work.] The projection homomorphism π of $\mathbf{G}(\mathbf{M})$ at the first coordinate maps $\mathbf{G}(\mathbf{M})$ homomorphically onto $\mathbf{G}$. Moreover, we obviously have that

$$\begin{aligned} \pi(\Delta) &= \mathbf{N} \\ \pi(\mathbf{B}) &= [\mathbf{M}, \mathbf{N}] \\ \pi(\mathbf{M}_1) &= \mathbf{M} \end{aligned}$$

From the fact that C satisfies (1) we get that

$$C(\mathbf{M}_1, \Delta) \subseteq \mathbf{M}_1 \wedge \Delta \subseteq \mathbf{B}.$$

To finish the argument we use (2):

$$C(\mathbf{M}, \mathbf{N}) = \pi(C(\mathbf{M}_1, \Delta)) \subseteq \pi(\mathbf{B}) = [\mathbf{M}, \mathbf{N}].$$

In the most general varieties of algebras, there is no such thing as a normal subgroup. The kernels of homomorphisms must be identified with congruences. For such a variety, we can replace normal subgroups by congruences in the formulation of (1) and (2), and consider binary congruence operations defined globally (in the congruence lattice of every algebra). It is quite easy to see that there must be a greatest such operation satisfying (1) and (2). We shall not be able to say very much in general about that operation. However, for congruence modular varieties we shall be able to say a great deal. But we need a better way to come to grips with the operation. Our approach in this book is to find a formulation of the property (5) which is capable of generalization to all algebras, and use that to build a more constructive

definition of a general commutator. Fortunately, this idea works out beautifully for congruence modular varieties. We get a commutator defined by an abstraction of (5), which satisfies (1) and (2), in fact is the greatest operation satisfying (1) and (2), and which also satisfies (3) and (4).

Our constructive definition of a commutator occurs in the third chapter. It is rather hard to see statement (5) behind that definition. The most we can do to motivate it is to work through the equivalence of the two for groups. That is what we shall now do.

Let $\mathbf{G}$ be a group and let $\mathbf{M}, \mathbf{N} \in \mathbf{L}(\mathbf{G})$ be such that $[\mathbf{M}, \mathbf{N}] = \{1\}$. This means of course that every member of $\mathbf{M}$ commutes with every member of $\mathbf{N}$. It implies that the term operations of the group, when applied to elements of $M \cup N$, take a simple form. Let $t(x_1, \ldots, x_p, y_1, \ldots, y_q)$ be any term operation of $p + q$ variables. It can be expressed in the form

$$t(x_1, \ldots, x_p, y_1, \ldots, y_q) = u_1 \ldots u_k$$

where each $u_i \in \{x_1, x_1^{-1}, \ldots, x_p, x_p^{-1}, y_1, y_1^{-1}, \ldots, y_q, y_q^{-1}\}$. Now if $\mathbf{m} = \langle m_1, \ldots, m_p \rangle \in \mathbf{M}^p$ and $\mathbf{n} = \langle n_1, \ldots, n_q \rangle \in \mathbf{N}^q$, then since m_i commutes with n_j, we have

$$t(\mathbf{m}, \mathbf{n}) = r(\mathbf{m}) \cdot s(\mathbf{n})$$

for a certain pair of term operations $r(\mathbf{x})$ and $s(\mathbf{y})$ which depend only on the term t (and not on any other parameters of the situation we are considering).

Now let $t(\mathbf{x}, \mathbf{y})$, $r(\mathbf{x})$ and $s(\mathbf{y})$ be terms related as above, and let $\mathbf{m}^1$, $\mathbf{m}^2 \in \mathbf{M}^p$ and $\mathbf{n}^1$, $\mathbf{n}^2 \in \mathbf{N}^q$. By substituting these elements for the variables in $t(\mathbf{x}, \mathbf{y})$, we obtain four elements of the group, and we arrange them in the form of a matrix

$$\begin{bmatrix} t(\mathbf{m}^1, \mathbf{n}^1) & t(\mathbf{m}^1, \mathbf{n}^2) \\ t(\mathbf{m}^2, \mathbf{n}^1) & t(\mathbf{m}^2, \mathbf{n}^2) \end{bmatrix} = \begin{bmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{bmatrix} \tag{5'}$$

Note that the elements in each column of this matrix belong to one coset of $\mathbf{M}$, and the elements in each row of this matrix belong to one coset of $\mathbf{N}$. Since

$$\begin{bmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{bmatrix} = \begin{bmatrix} r(\mathbf{m}^1) \cdot s(\mathbf{n}^1) & r(\mathbf{m}^1) \cdot s(\mathbf{n}^2) \\ r(\mathbf{m}^2) \cdot s(\mathbf{n}^1) & r(\mathbf{m}^2) \cdot s(\mathbf{n}^2) \end{bmatrix}$$

we have the following bi-implications:

$$\begin{aligned} t_{11} = t_{12} &\leftrightarrow t_{21} = t_{22} \\ t_{11} = t_{21} &\leftrightarrow t_{12} = t_{22} \end{aligned} \tag{5''}$$

It is this simple property that we shall exploit to make the general definition of the commutator. Our assumption that $[\mathbf{M}, \mathbf{N}] = \{1\}$

implies that $(5'')$ holds for every term operation $t(\mathbf{x}, \mathbf{y})$. Conversely, by choosing $t(x, y) = x^{-1}yx$, we get matrices of the form

$$\begin{bmatrix} t(m,n) & t(m,1) \\ t(1,n) & t(1,1) \end{bmatrix} = \begin{bmatrix} m^{-1}nm & 1 \\ n & 1 \end{bmatrix}$$

and so $(5'')$ for this term implies that $[\mathbf{M}, \mathbf{N}] = \{1\}$. The condition $(5'')$ has been called the **term condition**.

Now we turn to rings and consider what the commutator will turn out to be for congruences on rings. Let $\mathbf{J}$ and $\mathbf{K}$ be ideals of a ring $\mathbf{R}$. If the term condition is satisfied, then by considering matrices derived from the term operations $s(x, y) = x \cdot y$ and $t(x, y) = y \cdot x$, in fact the matrices

$$\begin{bmatrix} xy & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} xy & x0 \\ 0y & 00 \end{bmatrix}, \quad \begin{bmatrix} yx & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} yx & 0x \\ y0 & 00 \end{bmatrix} \qquad x \in J, y \in K.$$

we find that $\mathbf{J} \cdot \mathbf{K} = \mathbf{K} \cdot \mathbf{J} = \{0\}$. This suggests that we might define $[\mathbf{J}, \mathbf{K}]$, for any two ideals of a ring, as the ideal generated by $\mathbf{J} \cdot \mathbf{K} \cup \mathbf{K} \cdot \mathbf{J}$.

If we do make this definition, then it is easy to modify the argument we gave for groups, and prove that $[\mathbf{J}, \mathbf{K}]$ is the largest binary global operation on ideals in the variety of rings which satisfies (1) and (2). It is also easy to prove that $[\mathbf{J}, \mathbf{K}] = \{0\}$ if and only if the term condition is satisfied.

Exercise

1. Let $\mathcal{V}$ be the variety of modules over some ring. Identify congruences with submodules. Prove that the term condition holds for any two submodules of a module. Prove that $[\mathbf{M}, \mathbf{N}] = \{0\}$ is the only binary global operation on submodules in $\mathcal{V}$ which satisfies (1) and (2).

CHAPTER 2

Universal Algebra

We have to assume that our readers have had a basic introduction to universal algebra, and are familiar with the most elementary concepts of modern logic. Excellent references are the books of Birkhoff [**5**], Crawley and Dilworth [**15**], and Grätzer [**33**] and [**34**], (for everything pertaining to algebras and lattices) and the book of Burris and Sankappanavar [**10**] (for the logic and everything to do with varieties). With the aid of these references it is possible for a reader unfamiliar with universal algebra to read this book. Our purpose in this chapter is to establish our point of view, and the notation to be used.

The set $\{0, 1, 2, \dots\}$ of natural numbers is denoted by ω, and its members satisfy $n = \{0, 1, \dots, n-1\}$. We use A^n to denote the direct product of n copies of A.

By an **algebra** we mean any model for a first order language L whose nonlogical symbols are operation symbols F_i with arity $\rho(i)$, $i \in I$, where $\rho(i) \in \omega$. Thus an algebra consists of a nonvoid set A together with a collection $\{\bar{F}_i : i \in I\}$ of operations on A, i.e., maps $\bar{F}_i$ from $A^{\rho(i)}$ into A, one for each operation symbol in the language. We use boldfaced capital letters to denote algebras and the same plain capital letter for the corresponding underlying sets. The operation on the set A assigned to the operation F_i in an algebra $\mathbf{A}$ will be denoted $F_i^{\mathbf{A}}$; and thus an algebra $\mathbf{A}$ has the form $\langle A, F_i^{\mathbf{A}}(i \in I)\rangle$. Whenever we deal with a class of algebras, it will be assumed that all the algebras are models for one language, i.e., that they are of the same similarity type. Thus each class $\mathcal{K}$ of algebras is attached to a language $L(\mathcal{K}) = L$, and $\mathcal{K} \subseteq \mathrm{Mod}(L)$, where of course $\mathrm{Mod}(L)$ denotes the class of all models of L. When $\mathbf{A} \in \mathrm{Mod}(L)$ as above, then $F_i^{\mathbf{A}}$ is called the **interpretation** of F_i in $\mathbf{A}$, and is a $\rho(i)$-ary operation on the set A. The **type** of $\mathbf{A}$ is the function ρ and $\mathbf{A}$ has **finite type** if and only if the domain of ρ, that is I, is finite. Constants are the same as 0-ary operations. By the universe of an algebra $\mathbf{A}$ we mean the underlying set A of the algebra. The cardinality of A is denoted by $|A|$.

The set of **terms** in the variables v_i, $i \in \omega$, for a language L is the smallest set T containing the v_i and such that if $t_1, \dots, t_n \in T$ and

F_i is an operation symbol in L with $\rho(i) = n$, then $F_i(t_1, \ldots, t_n) \in T$. If $\mathbf{A} \in \mathrm{Mod}(L)$ is an algebra then to each term of L we can associate an operation on A in an obvious way. Thus if $t(v_0, \ldots, v_{n-1})$ is a term of L in which only the (distinct) variables $v_0, \ldots, v_{n-1}$ appear, then $t^{\mathbf{A}}$ denotes the corresponding n-ary operation on A. Such operations are called **term operations**, or in the older literature, **derived operations**. The set of term operations of $\mathbf{A}$ can also be defined as the smallest set of operations that is closed under composition and contains the basic operations $\{F_i^{\mathbf{A}} : i \in I\}$ and the trivial projection operations π_i^n (where $\pi_i^n(x_0, \ldots, x_{n-1}) = x_i$). The **polynomial operations** of $\mathbf{A}$ constitute the smallest set that is closed under composition and contains the basic operations of $\mathbf{A}$, the projection operations, and the constant 0-ary operations on A. For each polynomial operation $f(x_0, \ldots, x_{n-1})$ of $\mathbf{A}$, there exists a term operation $p(x_0, \ldots, x_{m-1})$ for some $m \geq n$ and elements $a_n, \ldots, a_{m-1}$ of A, such that $f(x_0, \ldots, x_{n-1}) = p(x_0, \ldots, x_{n-1}, a_n, \ldots, a_{m-1})$ holds identically. The expression *algebraic function* is often used in the literature to refer to what we call a polynomial operation.

Algebras $\mathbf{A}$ and $\mathbf{B}$ are called **equivalent** if and only if they have the same universe and exactly the same set of term operations. (Equivalent algebras need not be of the same type.) Algebras $\mathbf{A}$ and $\mathbf{B}$ are called **polynomially equivalent** if and only if they have the same universe and exactly the same polynomial operations.

Suppose that $\mathbf{A} \in \mathrm{Mod}(L)$ and that $s = s(v_0, \ldots, v_{n-1})$ and $t = t(v_0, \ldots, v_{n-1})$ are terms of L. The formula $s \approx t$ is called an **equation**. We write $\mathbf{A} \models s \approx t$ to denote that $s^{\mathbf{A}} = t^{\mathbf{A}}$, i.e., $s^{\mathbf{A}}(a_0, \ldots, a_{n-1}) = t^{\mathbf{A}}(a_0, \ldots, a_{n-1})$ for all $a_0, \ldots, a_{n-1} \in A$. When $\mathbf{A} \models s \approx t$ we say that $s \approx t$ is an **identity** of $\mathbf{A}$. We sometimes use the terminology *law* or *equation* to mean the same as identity. $\mathcal{K} \models s \approx t$ means that $\mathbf{A} \models s \approx t$ for all $\mathbf{A} \in \mathcal{K}$.

If Σ is a set of equations of L then

$$\mathrm{Mod}(\Sigma) = \{\mathbf{A} \in \mathrm{Mod}(L) : \mathbf{A} \models \varepsilon \text{ for all } \varepsilon \in \Sigma\}$$

Classes of the form $\mathrm{Mod}(\Sigma)$, Σ a set of equations of L are called **varieties** (or **equational classes**). By a theorem of G. Birkhoff [4], a class $\mathcal{V} \subseteq \mathrm{Mod}(L)$ is a variety if and only if $\mathcal{V}$ is closed under the formation of homomorphic images, subalgebras and products. The smallest variety containing a class $\mathcal{K} \subseteq \mathrm{Mod}(L)$ is identical with $\boldsymbol{HSP}(\mathcal{K})$, where $\boldsymbol{H}$, $\boldsymbol{S}$ and $\boldsymbol{P}$ are the operators which close classes under homomorphic images, subalgebras and direct products, respectively. We interpret these operators in such a way that the closure of $\mathcal{K}$ under any of them contains all isomorphic copies of its members. $\mathcal{V} \subseteq \mathrm{Mod}(L)$ is a variety

if and only if $\mathcal{V} = \boldsymbol{HSP}(\mathcal{V})$. We let $\boldsymbol{V}$ denote the operator $\boldsymbol{HSP}$, i.e., $\boldsymbol{V}(\mathcal{K}) = \boldsymbol{HSP}(\mathcal{K})$.

A **congruence** of an algebra $\mathbf{A}$ is an equivalence relation on the universe of $\mathbf{A}$ that is induced by some homomorphism with domain $\mathbf{A}$, i.e., two elements of A are related by the congruence if and only if they have the same image under the homomorphism. The congruences of an algebra $\mathbf{A}$ constitute a lattice (ordered by set inclusion) which we denote by **Con A**. The lattice operations of **Con A** will be denoted by $\vee$ for join, and $\wedge$ for meet, with $\bigvee$ and $\bigwedge$ for the infinitary versions. The least and greatest elements of the lattice will be denoted by 0 and 1 (or $0_{\mathbf{A}}$ and $1_{\mathbf{A}}$ for sake of clarity). If θ is in $\operatorname{Con}\mathbf{A}$, then the set of equivalence classes of θ can be made, in a natural way, into an algebra which we denote $\mathbf{A}/\theta$. For $x \in A$ we let x/θ denote the equivalence class containing x. The map $x \to x/\theta$ is a natural homomorphism from $\mathbf{A}$ onto $\mathbf{A}/\theta$. The notations $x \equiv y \pmod{\theta}$ and $x\ \theta\ y$ both signify that $\langle x, y\rangle \in \theta$. A similar notation with an entirely different meaning is $\alpha/\beta = \{\gamma \in \operatorname{Con}\mathbf{A} : \beta \leq \gamma \leq \alpha\}$. α/β is called a **quotient** or **interval** in the lattice **Con A**.

Congruences on $\mathbf{A}$ can alternatively be characterized as the equivalence relations R on A such that R is a subalgebra of $\mathbf{A} \times \mathbf{A}$. Congruences, in general, do not behave so well as they do in groups, rings and modules; for instance two congruences on $\mathbf{A}$ may share a block, $x/\alpha = x/\beta$, for some x, without being identical.

We call an algebra **simple** if it has exactly two congruences, and **subdirectly irreducible** if its congruence lattice has exactly one atom, called the **monolith** and usually denoted by μ, such that $\mu \leq \theta$ for every nonzero congruence θ. Another theorem of Birkhoff tells us that every algebra $\mathbf{A}$ is isomorphic to a subdirect product of subdirectly irreducible homomorphic images $\mathbf{A}_i$, $i \in I$. That is, $\mathbf{A}$ is isomorphic to an algebra $\mathbf{C} \leq \prod_{i\in I} \mathbf{A}_i$ such that $\mathbf{C}$ projects onto each factor $\mathbf{A}_i$.

An element c of a complete lattice is **compact** if $c \leq \bigvee X$ for some subset X of the lattice implies that $c \leq \bigvee F$ for some finite $F \subseteq X$. A complete lattice is **compactly generated** or **algebraic** if every element is the join of compact elements. Congruence lattices are always compactly generated. An element q of a lattice is **completely meet irreducible** if $q = \bigwedge Y$ implies $q \in Y$. An algebra $\mathbf{A}$ is subdirectly irreducible if and only if the least element of **Con A** is completely meet irreducible. Since if $\theta \in \operatorname{Con}\mathbf{A}$, $\mathbf{Con}(\mathbf{A}/\theta)$ is isomorphic to the interval $1/\theta$ in **Con A**, representations of $\mathbf{A}$ as a subdirect product of subdirectly irreducible algebras correspond to sets of completely meet

irreducible congruences of $\mathbf{A}$ which meet to 0. For compactly generated lattices, it is not hard to prove that every element is the meet of completely meet irreducible elements.

A lattice is **distributive** if it satisfies the distributive law, $x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z)$. It is **modular** if it satisfies the implication $x \geq y \to x \wedge (y \vee z) \approx y \vee (x \wedge z)$. In a modular lattice the notion of transposed quotients is very important. We say that α/β **transposes down onto** γ/δ (where $\alpha \geq \beta$ and $\gamma \geq \delta$, of course), and we write $\alpha/\beta \searrow \gamma/\delta$ if $\beta \wedge \gamma = \delta$ and $\beta \vee \gamma = \alpha$. We also write $\gamma/\delta \nearrow \alpha/\beta$ for this concept.

The congruence on $\mathbf{A}$ generated by X, a subset of $A \times A$, is denoted $\mathrm{Cg}_{\mathbf{A}}(X)$, or sometimes $\mathrm{Cg}(X)$, and we abbreviate $\mathrm{Cg}(\{\langle x, y\rangle\})$ as $\mathrm{Cg}(x, y)$. The subalgebra of $\mathbf{A}$ generated by Y is denoted $\mathrm{Sg}_{\mathbf{A}}(Y)$ or $\mathrm{Sg}(Y)$. Boldface symbols like $\mathbf{x}$ denote n-tuples of elements. $\mathrm{Hom}(\mathbf{A}, \mathbf{B})$ denotes the set of homomorphisms from $\mathbf{A}$ to $\mathbf{B}$; this can be the empty set. If $f \in \mathrm{Hom}(\mathbf{A}, \mathbf{B})$ then the **kernel** of f (i.e., the induced congruence on $\mathbf{A}$) is written $\ker f$. If $\mathbf{B}$ is a subalgebra of $\mathbf{A}$ and f is a map with domain A, $f|_{\mathbf{B}}$ denotes the restriction of f to $\mathbf{B}$. If $\theta \in \mathrm{Con}\,\mathbf{A}$, $\theta|_{\mathbf{B}}$ denotes the restriction of θ to $\mathbf{B}$, i.e., $\theta|_{\mathbf{B}} = \theta \cap (B \times B)$.

A variety $\mathcal{V}$ is called **distributive** if for all $\mathbf{A} \in \mathcal{V}$, **Con A** is distributive; **modular** if for all $\mathbf{A} \in \mathcal{V}$, **Con A** is modular; permutable if for all $\mathbf{A} \in \mathcal{V}$ and for all $\theta, \phi \in \mathrm{Con}\,\mathbf{A}$, $\theta \circ \phi = \phi \circ \theta$. (Here $\theta \circ \phi$ is the relational product: $\{\langle x, y\rangle : \exists z \in \mathbf{A}, x\ \theta\ z\ \phi\ y\}$. The equality implies $\theta \circ \phi = \theta \vee \phi$, and the condition implies that $\mathrm{Con}\,\mathbf{A}$ is modular.)

Let $\mathcal{V}$ be a variety which contains an algebra with at least two elements and X be a nonvoid set. There is an algebra $\mathbf{F} \in \mathcal{V}$ (unique up to isomorphism) having these properties:

(1) $\mathbf{F}$ contains X and is generated by X;

(2) whenever $\mathbf{A} \in \mathcal{V}$ and f maps X into A, then there exists a unique homomorphism $\hat{f} : \mathbf{F} \to \mathbf{A}$ such that $\hat{f} \supseteq f$ (i.e., $\hat{f}|_X = f$).

Such an algebra $\mathbf{F}$ is said to be a **free algebra** in $\mathcal{V}$, freely generated by X, and is denoted by $\mathbf{F}_{\mathcal{V}}(X)$. Some other notations may be used for denoting free algebras, such as $\mathbf{F}_{\mathcal{V}}(\lambda)$ (if $|X| = \lambda$), or $\mathbf{F}_{\mathcal{V}}(x, y, z)$ (if $X = \{x, y, z\}$). An important fact about free algebras is that for an algebra $\mathbf{A}$, $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(\lambda)$ is a subalgebra of $\mathbf{A}^{|A|^\lambda}$ (see Birkhoff [**5**]). Thus if $\mathbf{A}$ and λ are both finite, then so is $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(\lambda)$. Consequently, if $\mathbf{A}$ is a finite algebra then $\boldsymbol{V}(\mathbf{A})$ is **locally finite**, i.e., every finitely generated algebra in $\boldsymbol{V}(\mathbf{A})$ is finite.

The next theorems characterize permutability, distributivity, and modularity of the congruence lattices of the algebras in a variety by the existence of terms satisfying certain equations. Conditions of this form are known as *Mal'cev conditions*.

THEOREM 2.1. *For any variety we have:*

(1) (Mal'cev [**61**]) $\mathcal{V}$ *is permutable if and only if there is a term* $p(x, y, z)$ *in the language of* $\mathcal{V}$ *such that the following equations are valid in* $\mathcal{V}$.

$$p(x, x, y) \approx y \approx p(y, x, x)$$

(2) (Jónsson [**54**]) $\mathcal{V}$ *is distributive if and only if for some* n *there are terms* $d_0(x, y, z), \ldots, d_n(x, y, z)$ *such that* $\mathcal{V}$ *satisfies*

(i) $d_0(x, y, z) \approx x$, $d_n(x, y, z) \approx z$,

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

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

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

PROOF. The proof of (2) will be omitted since it is similar to the proof of Theorem 2.2 below and we will not use (2). To sketch (1) first suppose $\mathcal{V}$ has such a term p and that $x \; \theta \; y \; \psi \; z$, for some $\theta, \psi \in \operatorname{Con} \mathbf{A}$, where $\mathbf{A} \in \mathcal{V}$. Then $x = p(x, y, y) \; \psi \; p(x, y, z) \; \theta \; p(x, x, z) = z$, showing that θ and ψ permute. For the converse suppose that $\mathcal{V}$ is permutable and let $\mathbf{F}_{\mathcal{V}}(x, y, z)$ be the free $\mathcal{V}$–algebra generated by x, y and z. Let $\theta = \operatorname{Cg}(x, y)$ and $\psi = \operatorname{Cg}(y, z)$. Then $x \; \theta \; y \; \psi \; z$, so there is an element $\bar{p}$ in $\mathbf{F}_{\mathcal{V}}(x, y, z)$ with $x \; \psi \; \bar{p} \; \theta \; z$. Let $p(x, y, z)$ be a term which represents $\bar{p}$, that is, $p^{\mathbf{F}}(x, y, z) = \bar{p}$ in $\mathbf{F}_{\mathcal{V}}(x, y, z)$ where $p^{\mathbf{F}}(x, y, z)$ is the interpretation of p as a term operation of $\mathbf{F}_{\mathcal{V}}(x, y, z)$. Let σ be the endomorphism of $\mathbf{F}_{\mathcal{V}}(x, y, z)$ which maps x to x, y to y and z to y. One easily checks that ψ is the congruence associated with this endomorphism. Since σ is the identity map on the subalgebra generated by x and y, $x \; \psi \; p^{\mathbf{F}}(x, y, y)$ implies $x = p^{\mathbf{F}}(x, y, y)$. Similarly $z = p^{\mathbf{F}}(x, x, z)$. Of course these facts holding in the free algebra imply that the equations of (1) hold in $\mathcal{V}$. □

THEOREM 2.2. (Day [**19**]) *A variety $\mathcal{V}$ is modular if and only if for some n there are terms $m_0(x,y,z,u),\dots,m_n(x,y,z,u)$ such that $\mathcal{V}$ satisfies*

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

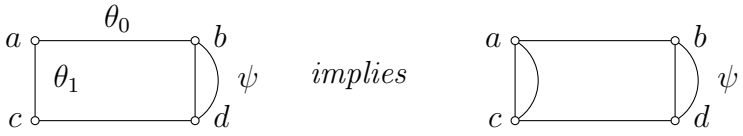
(ii) $m_i(x,y,y,x) \approx x$, $i \leq n$

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

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

LEMMA 2.3. *Let $\mathcal{V}$ be a variety having terms $m_i(x,y,z,u)$, $i = 0,\dots,n$, satisfying the conditions of Theorem 2.2, and let $\mathbf{A} \in \mathcal{V}$, $\gamma \in \operatorname{Con}\mathbf{A}$, a, b, c, $d \in \mathbf{A}$ with $\langle b,d\rangle \in \gamma$. Then $\langle a,c\rangle \in \gamma$ if and only if for all $i \leq n$, $m_i(a,a,c,c)\ \gamma\ m_i(a,b,d,c)$.*

LEMMA 2.4 (**The Shifting Lemma**). *Let $\mathcal{V}$ be a modular variety and let $\mathbf{A} \in \mathcal{V}$ and ψ, θ_0, $\theta_1 \in \operatorname{Con}\mathbf{A}$. Suppose that a, b, c, $d \in \mathbf{A}$, $\langle a,b\rangle$, $\langle c,d\rangle \in \theta_0$, $\langle a,c\rangle$, $\langle b,d\rangle \in \theta_1$, and $\psi \geq \theta_0 \wedge \theta_1$. Then $\langle b,d\rangle \in \psi$ implies $\langle a,c\rangle \in \psi$. Pictorially,*



NOTE. In diagrams like this, lines without labels are implicitly assumed to be labeled by (the endpoints are congruent modulo) any label appearing on a parallel line. Terms satisfying the requirements of Theorem 2.2 are called **Day terms**.

PROOFS. Consider the following conditions for a variety $\mathcal{V}$.

(1) $\mathcal{V}$ is modular.

(2) $\mathcal{V}$ has Day terms.

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

(4) $\mathcal{V}$ satisfies the conclusion of the Shifting Lemma, i.e., if a, b, c, $d \in \mathbf{A} \in \mathcal{V}$ and ψ, θ_0, $\theta_1 \in \operatorname{Con}\mathbf{A}$ with $\psi \geq \theta_0 \wedge \theta_1$, then the implication of the figure holds.

We let (4′) be the condition identical to (4) except that we assume only that θ_0 is a reflexive, compatible relation (rather than θ_0 a congruence). Clearly (4′) → (4). To prove the theorem and the lemmas it suffices to show that (1) → (2) → (3) → (4′) → (1). This will also show that condition (3) is equivalent to modularity. After the proof we will outline a proof that (4) is also equivalent to modularity.

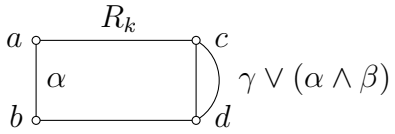
(1) → (2). Assume $\mathcal{V}$ is modular. Let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z, u)$ be the free $\mathcal{V}$–algebra on four generators, and let $\alpha = \operatorname{Cg}(x, u) \vee \operatorname{Cg}(y, z)$, $\beta = \operatorname{Cg}(x, y) \vee \operatorname{Cg}(z, u)$, and $\gamma = \operatorname{Cg}(y, z)$ be in $\mathbf{Con}\,\mathbf{F}$. Then $(x, u) \in \alpha \wedge (\beta \vee \gamma)$. Since $\mathcal{V}$ is modular, $\langle x, u\rangle \in \gamma \vee (\alpha \wedge \beta)$. This means that for some n there are elements $w_0 = x, w_1, \ldots, w_n = u$ of $\mathbf{F}_{\mathcal{V}}(x, y, z, u)$ such that $w_i \ \alpha \wedge \beta \ w_{i+1}$ if i is even, and $w_i \ \gamma \ w_{i+1}$ if i is odd. Let $x = m_0(x, y, z, u), m_1(x, y, z, u), \ldots, m_n(x, y, z, u) = u$ be the terms representing $w_0, w_1, \ldots, w_n$, i.e., $w_i = m_i^{\mathbf{F}}(x, y, z, u)$. Since $\gamma \leq \alpha$ all of the w_i's are in the same α class. Thus $x \ \alpha \ m_i^{\mathbf{F}}(x, y, z, u) \ \alpha \ m_i^{\mathbf{F}}(x, y, y, x)$. Since α restricted to the subalgebra generated by x and y is trivial, $x = m_i^{\mathbf{F}}(x, y, y, x)$. Hence $x \approx m_i(x, y, y, x)$ holds in $\mathcal{V}$. Similar arguments show that the other equations of Theorem 2.2 hold.

(2) → (3). Let $\mathcal{V}$ be a variety having Day terms and let $\mathbf{A} \in \mathcal{V}$, $\gamma \in \operatorname{Con}\mathbf{A}$, a, b, c, $d \in \mathbf{A}$, with $b \ \gamma \ d$. First assume $a \ \gamma \ c$. Then in $\mathbf{A}$ $m_i(a, a, c, c) \ \gamma \ m_i(a, a, a, a) = a$, and $m_i(a, b, d, c) \ \gamma \ m_i(a, b, b, a) = a$. For the converse, setting $u_i = m_i(a, a, c, c)$ and $v_i = m_i(a, b, d, c)$, and assuming $u_i \ \gamma \ v_i$ for all $i \leq n$, we can show $u_i \ \gamma \ u_{i+1}$ for all $i < n$; thus $a = u_0 \ \gamma \ u_n = c$. Namely, for even $i < n$, $u_i = u_{i+1}$; and for odd $i < n$, $u_i \ \gamma \ v_i \ \gamma \ m_i(a, b, b, c) = m_{i+1}(a, b, b, c) \ \gamma \ v_{i+1} \ \gamma \ u_{i+1}$.

(3) → (4′). Assume that $\mathcal{V}$ is a variety satisfying (3) and that the conditions implied by the left hand picture of Lemma 2.4 hold in algebra $\mathbf{A} \in \mathcal{V}$, where θ_1 and ψ are congruences on $\mathbf{A}$ and θ_0 is a reflexive, compatible relation. Then for any $i \leq n$, $m_i(a, a, c, c) \ \theta_0 \ m_i(a, b, d, c)$ and $m_i(a, a, c, c) \ \theta_1 \ m_i(a, a, a, a) = a = m_i(a, b, b, a) \ \theta_1 \ m_i(a, b, d, c)$. Hence, $m_i(a, a, c, c) \ \theta_0 \wedge \theta_1 \ m_i(a, b, d, c)$. Now the conclusion of Lemma 2.4 follows by applying (3) with $\gamma = \psi$, since $\psi \geq \theta_0 \wedge \theta_1$ and $(b, d) \in \psi$.

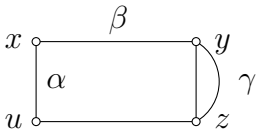
(4′) → (1). Suppose that $\mathcal{V}$ satisfies (4′) and that $\mathbf{A} \in \mathcal{V}$ and α, β, $\gamma \in \operatorname{Con}\mathbf{A}$ with $\alpha \geq \gamma$. We need to show that $\alpha \wedge (\beta \vee \gamma) = (\alpha \wedge \beta) \vee \gamma$. The left side may be written as $\bigcup_{n<\omega} (\alpha \cap R_n)$, where $R_0 = \beta$ and $R_{k+1} = R_k \circ \gamma \circ \beta$. Thus it suffices to show that $\alpha \cap R_n \subseteq (\alpha \wedge \beta) \vee \gamma$. This is clear for $n = 0$. Assume it is true for $n = k$. Let $\langle a, b\rangle \in \alpha \cap R_{k+1} =$

$\alpha \cap (R_k \circ \gamma \circ \beta)$. Then there are elements c and d in $\mathbf{A}$ with $a\ R_k\ c\ \gamma\ d\ \beta\ b$. Thus since $\beta \subseteq R_k$ we have



Now we conclude from (4′) that $\langle a, b\rangle \in \gamma \vee (\alpha \wedge \beta)$, as desired. □

Lemma 2.4 was discovered by H. P. Gumm, who also named it. It is quite important in the development of the theory of modular varieties and plays a central role in his geometric approach. *For a variety, the validity of the Shifting Lemma is equivalent to modularity*, as Gumm showed [**41**]. The above proof shows the Shifting Lemma holds in modular varieties. Or alternatively we can argue directly that if $\theta_0 \wedge \theta_1 \leq \psi$ and the conditions implied by the left hand figure of the Shifting Lemma hold then $(a, c) \in \theta_1 \wedge (\theta_0 \vee (\theta_1 \wedge \psi)) = (\theta_0 \wedge \theta_1) \vee (\theta_1 \wedge \psi) \leq \psi$. Conversely, if condition (4) holds in a variety $\mathcal{V}$, let $\mathbf{F}_{\mathcal{V}}(x, y, z, u)$ be the free $\mathcal{V}$–algebra and let $\alpha = \mathrm{Cg}(x, u) \vee \mathrm{Cg}(y, z)$, $\beta = \mathrm{Cg}(x, y) \vee \mathrm{Cg}(z, u)$, $\gamma = \mathrm{Cg}(y, z)$. Then

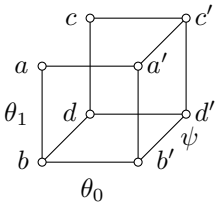


Thus $\langle x, u\rangle \in \gamma \vee (\alpha \wedge \beta)$. Just as in the proof that (1) → (2), this situation implies the existence of terms m_i which satisfy the equations in Theorem 2.2, which in turn imply modularity.

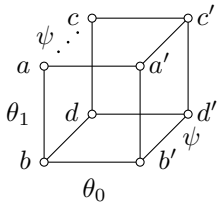
As we mentioned above, terms satisfying the equations of Theorem 2.2 will be called **Day terms**. A term satisfying the condition of Theorem 2.1(1) will be called a **Mal'cev term**, and of course terms satisfying Theorem 2.1(2) will be called **Jónsson terms**.

To underline the power of Lemma 2.3 we shall now derive one of Gumm's interesting geometrical results. Another one of his geometrical results is contained in the exercises. Neither of these results will be used in the sequel. We assume here that $\mathbf{A}$ is an algebra such that $\boldsymbol{V}(\mathbf{A})$ is modular.

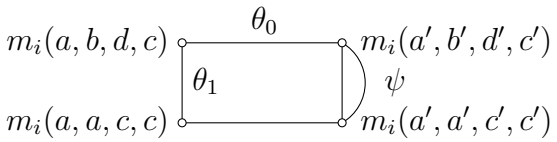
THEOREM 2.5. **(The Cube Lemma)** *Suppose that θ_0, θ_1, $\psi \in \mathrm{Con}\,\mathbf{A}$ and $\psi \geq \theta_0 \wedge \theta_1$. Let a, b, c, d, a', b', c', d' be elements of $\mathbf{A}$. Then*



implies



PROOF. One can readily verify the congruences of the following diagram, where $i \leq n$.



By the Shifting Lemma, $m_i(a,b,d,c)\ \psi\ m_i(a,a,c,c)$. Now the result follows from Lemma 2.3. □

Exercises

1. A *quasigroup* is an algebra $\langle A, \cdot, /, \backslash \rangle$ with three binary operations which satisfy the laws

$$x \cdot (x\backslash y) \approx y \qquad (x/y) \cdot y \approx x$$

$$x\backslash(x \cdot y) \approx y \qquad (x \cdot y)/y \approx x$$

A *loop* is a quasigroup with a constant 1 satisfying the law $1 \cdot x \approx x \cdot 1 \approx x$. Show that left multiplication by an element of a quasigroup $\mathbf{A}$ defines a bijection from A to A. Show that if $\mathbf{A}$ is a finite quasigroup, then there is a binary term $t(x,y)$ which uses only multiplication, such that $x/y = t(x,y)$.

2. Show that if $\langle A, \cdot, /, \backslash \rangle$ is a quasigroup then

$$p(x,y,z) = (x/(y\backslash y)) \cdot (y\backslash z)$$

and

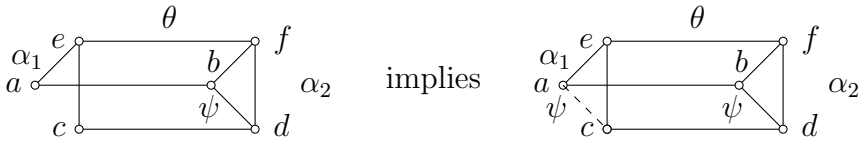
$$q(x,y,z) = ((x \cdot y)/x)\backslash(x \cdot z)$$

are both Mal'cev terms for $\mathbf{A}$. Hence the class of all quasigroups forms a permutable variety.

3. (A. Day) Let $\mathcal{V}$ be a permutable variety with Mal'cev term $p(x,y,z)$. Show that $\mathcal{V}$ is modular with Day terms $m_0(x,y,z,u) = x$, $m_1(x,y,z,u) = p(x,p(x,y,z),u)$, $m_2(x,y,z,u) = u$.

4. Prove that the following form of the Shifting Lemma, presented geometrically, is equivalent to that given in Lemma 2.4, where $\psi' = \psi \vee (\theta_0 \wedge \theta_1)$.

5. Use Lemma 2.3 and Lemma 2.4 to prove the following geometrical result of Gumm which is called the Little Desarguesian Theorem. Let θ, ψ, α_1, $\alpha_2 \in \operatorname{Con}\mathbf{A}$ with $\theta \wedge \alpha_i \leq \psi$, $i = 1, 2$, and let a, b, c, d, e, $f \in \mathbf{A}$. Then



CHAPTER 3

Several Commutators

In this chapter $\mathcal{V}$ denotes any variety, not assumed to be modular. The first "commutator" is defined with reference to $\mathcal{V}$, so its value may depend not only on the algebra $\mathbf{A}$ but also on the particular variety to which $\mathbf{A}$ belongs, under consideration. The next two "commutators" depend just on $\mathbf{A}$. (All three will turn out to be identical for modular varieties.)

DEFINITION 3.1. $C^{(\mathcal{V})}$ is the largest binary operation defined on $\mathbf{Con}\ \mathbf{A}$ for every $\mathbf{A} \in \mathcal{V}$ and satisfying (for any $\mathbf{A}, \mathbf{B} \in \mathcal{V}$, and $\theta, \psi \in \operatorname{Con} \mathbf{A}$, and $f \in \operatorname{Hom}(\mathbf{A}, \mathbf{B})$ a surjective homomorphism with kernel π)

$$
\begin{aligned}
&C^{(\mathcal{V})}(\theta, \psi) \leq \theta \wedge \psi \quad \text{and} \\
&C^{(\mathcal{V})}(\theta, \psi) \vee \pi = f^{-1} C^{(\mathcal{V})}(f(\theta \vee \pi), f(\psi \vee \pi)).
\end{aligned} \tag{1}
$$

A rigorous justification of this definition would involve us in considerations of axiomatic set theory rather far removed from the subject at hand. $C^{(\mathcal{V})}$ is the "pointwise join" of all binary congruence operations defined globally over $\mathcal{V}$ and satisfying the conditions. (Note that $C(\theta, \psi) = 0$ is such an operation, so there is at least one.) The other definitions of commutator are completely constructive.

The next definitions are motivated by fact $(5'')$ of Chapter 1 (a property of the commutator for groups).

DEFINITION 3.2. Let α, β, and δ be in $\operatorname{Con} \mathbf{A}$.

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

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

where $\mathbf{a}^i$, $i = 1, 2$ is a sequence of n elements of A, $\mathbf{b}^i$ is a sequence of m elements of A, $m, n \geq 0$, satisfying $\mathbf{a}^1_k\ \alpha\ \mathbf{a}^2_k$ and $\mathbf{b}^1_j\ \beta\ \mathbf{b}^2_j$ for $k < n$ and $j < m$, and t is a $n + m$ variable term operation on $\mathbf{A}$.

(2) We say α *centralizes* β modulo δ, and write $C(\alpha, \beta; \delta)$, provided that for every $\begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}$ in $M(\alpha, \beta)$, $u_{11}\ \delta\ u_{12}$ implies $u_{21}\ \delta\ u_{22}$.

(3) $[\alpha, \beta]$ is the smallest δ for wich $C(\alpha, \beta; \delta)$ holds.
(4) $[\alpha, \beta]_s$ is the smallest δ for which both $C(\alpha, \beta; \delta)$ and $C(\beta, \alpha; \delta)$ hold.[1]

Obviously $C(\alpha, \beta; \alpha \wedge \beta)$ holds and if $C(\alpha, \beta; \delta_i)$ holds for $i \in I$, then $C(\alpha, \beta; \bigwedge_{i \in I} \delta_i)$ holds. So the definitions make sense.

We will occasionally use the terminology δ satisfies the α, β–**term condition** when α centralizes β modulo δ. Another terminology for this situation is α **annihilates** β modulo δ. The origin of this terminology is ring theory: If $\mathbf{I}$ and $\mathbf{J}$ are ideals of a ring, $[\mathbf{I}, \mathbf{J}] = 0$ means $\mathbf{IJ} = \mathbf{JI} = 0$.

Each member of $M(\alpha, \beta)$ presents two demands, a row demand and a column demand. $[\alpha, \beta]$ is the least congruence satisfying all of the row demands, $[\beta, \alpha]$ is the least congruence satisfying all of the column demands, $[\alpha, \beta]_s$ is the least congruence satisfying all demands. The following facts are obvious.

PROPOSITION 3.3. *Let α, $\beta \in$ **Con A***

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

$$\begin{bmatrix} a & a \\ a' & a' \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} b & b' \\ b & b' \end{bmatrix}$$

where $\langle a, a' \rangle \in \alpha$ and $\langle b, b' \rangle \in \beta$.

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

In this completely general setting we can prove almost nothing about the three congruence operations just defined, except for the most obvious facts stated below. We expect that under rather weak conditions. $C^{(\gamma)}(\alpha, \beta) \leq [\alpha, \beta]$ must hold.

PROPOSITION 3.4. (1) *$C^{(\gamma)}$ is symmetric and satisfies 3.1(1).*
(2) $[\alpha, \beta] \leq [\alpha, \beta]_s = [\beta, \alpha]_s \leq \alpha \wedge \beta$.
(3) *$[\alpha, \beta]$ and $[\alpha, \beta]_s$ are monotone in both α and β.* □

Exercises

1. Show that if $\alpha \wedge \beta \leq \delta \leq \alpha$ or if $(\alpha \vee \delta) \wedge \beta \leq \delta$ then $C(\alpha, \beta; \delta)$ holds.

[1]This notation differs from the first edition where we used $C(\alpha, \beta)$ for what is here denoted $[\alpha, \beta]$ and $[\alpha, \beta]$ for what is here denoted $[\alpha, \beta]_s$. In a modular variety $[\alpha, \beta] = [\alpha, \beta]_s$.

2. If $C(\alpha_i, \beta; \delta)$ holds for all i, then $C(\bigvee \alpha_i, \beta; \delta)$ holds.

CHAPTER 4

One Commutator in Modular Varieties; Its Basic Properties

In this chapter $\mathcal{V}$ denotes a fixed modular variety with Day terms $m_0(x,y,z,u),\ldots,m_n(x,y,z,u)$ (see Theorem 2.2). We show that the commutators defined in Chapter 3 are identical for $\mathcal{V}$. The basic properties of the commutator are derived and its behavior with respect to homomorphisms, subalgebras, and direct products is described. Finally we introduce the Hagemann-Herrmann definition of the commutator and show it is equivalent to our definition. We also give the lattice theoretic characterization of the commutator due to these authors.

Recall the definitions of $M(\alpha,\beta)$, $[\alpha,\beta]$. and $[\alpha,\beta]_s$ from Chapter 3.

DEFINITION 4.1. For $\alpha,\beta \in \operatorname{Con}\mathbf{A}$, let $X(\alpha,\beta)$ be the set of ordered pairs $\langle m_i(a,b,d,c), m_i(a,a,c,c)\rangle$ where $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(\alpha,\beta)$ and $i \leq n$.

PROPOSITION 4.2. *Let $\alpha,\beta,\delta \in \operatorname{Con}\mathbf{A}$, $\mathbf{A} \in \mathcal{V}$, where $\mathcal{V}$ is modular.*

(1) *The following are equivalent*
  (i) $X(\alpha,\beta) \subseteq \delta$
  (ii) $X(\beta,\alpha) \subseteq \delta$
  (iii) $C(\alpha,\beta;\delta)$ *holds*
  (iv) $C(\beta,\alpha;\delta)$ *holds*
  (v) $[\alpha,\beta] \leq \delta$
(2) $[\alpha,\beta] = [\alpha,\beta]_s = \operatorname{Cg}(X(\alpha,\beta))$.

PROOF. To prove (1) we show first that (iii) $\Rightarrow$ (i) $\Rightarrow$ (iv). Then by exchanging α and β we have (iv) $\Rightarrow$ (ii) $\Rightarrow$ (iii), and it follows that all are equivalent. Assume first that $C(\alpha,\beta;\delta)$ holds. We have to show that for any term t, for any $\mathbf{a}^1 \equiv \mathbf{a}^2 \pmod{\alpha}$ and $\mathbf{b}^1 \equiv \mathbf{b}^2 \pmod{\beta}$, and for the resulting matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(\alpha,\beta)$, $u \equiv v \pmod{\delta}$ where $u = m_i(a,a,c,c)$ and $v = m_i(a,b,d,c)$. We will show that $\begin{bmatrix} u \\ v \end{bmatrix}$ is the

right hand column of a matrix $\begin{bmatrix} w & u \\ w & v \end{bmatrix} \in M(\beta, \alpha)$. (Hence $\langle u, v \rangle \in \delta$ as $\langle w, w \rangle \in \delta$ and $C(\alpha, \beta; \delta)$ holds.) In fact

$$u = m_i(t(\mathbf{a}^1, \mathbf{b}^1), t(\mathbf{a}^1, \mathbf{b}^1), t(\mathbf{a}^2, \mathbf{b}^1), t(\mathbf{a}^2, \mathbf{b}^1))$$
$$v = m_i(t(\mathbf{a}^1, \mathbf{b}^1), t(\mathbf{a}^1, \mathbf{b}^2), t(\mathbf{a}^2, \mathbf{b}^2), t(\mathbf{a}^2, \mathbf{b}^1))$$

and if we replace $\mathbf{a}^1$ by $\mathbf{a}^2$ at its second occurrence in each of these terms, and $\mathbf{a}^2$ by $\mathbf{a}^1$ at its second occurrence, then the results are equal ($= w = t(\mathbf{a}^1, \mathbf{b}^1)$ by Proposition 2.2(ii)). The term s that gives rise to $\begin{bmatrix} w & u \\ w & v \end{bmatrix}$ is

$$s(\mathbf{x}^1, \mathbf{x}^2, \mathbf{y}^1, \mathbf{y}^2, \mathbf{y}^3, \mathbf{y}^4, \mathbf{y}^5, \mathbf{y}^6) = m_i(t(\mathbf{y}^1, \mathbf{y}^2), t(\mathbf{x}^1, \mathbf{y}^3), t(\mathbf{y}^4, \mathbf{y}^5), t(\mathbf{x}^2, \mathbf{y}^6)).$$

To see (i) $\Rightarrow$ (iv), suppose $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(\alpha, \beta)$ and $\langle b, d \rangle \in \delta$. Lemma 2.3 implies $\langle a, c \rangle \in \delta$ showing $C(\beta, \alpha; \delta)$ holds. This concludes the proof of (1), (2) is immediate from (1). □

PROPOSITION 4.3. *For congruences θ, ψ, γ_i $(i \in I)$ on $\mathbf{A} \in \mathcal{V}$ we have*

$$[\theta, \psi] = [\psi, \theta] \leq \theta \wedge \psi$$

and

$$[\theta, \bigvee_{i \in I} \gamma_i] = \bigvee_{i \in I} [\theta, \gamma_i].$$

PROOF. The first statement is by Proposition 3.4(2). To prove the second equality, note first that the right side is contained in the left by monotonicity (i.e. by Proposition 3.4(3)). Denote the right side by α. By Proposition 4.2(1), to get equality we just have to show that γ centralizes θ modulo α, where $\gamma = \bigvee_{i \in I} \gamma_i$. By Proposition 4.2, γ_i centralizes θ modulo α for each $i \in I$.

So let $\begin{bmatrix} u & v \\ r & s \end{bmatrix}$ belong to $M(\theta, \gamma)$ and $\langle u, r \rangle \in \alpha$. It is clear that there exist finite sequences $x_0, \ldots, x_k$, $z_0, \ldots, z_k$ such that $\begin{bmatrix} x_j & x_{j+1} \\ z_j & z_{j+1} \end{bmatrix} \in M(\theta, \gamma_{i_j})$ for $j < k$ and $\begin{bmatrix} x_0 & x_k \\ z_0 & z_k \end{bmatrix} = \begin{bmatrix} u & v \\ r & s \end{bmatrix}$. The matrices are obtained from the same term operation that gives $\begin{bmatrix} u & v \\ r & s \end{bmatrix}$. Thus inductively $\langle x_{j+1}, z_{j+1} \rangle \in \alpha$ as γ_{i_j} centralizes θ modulo α, and finally $\langle v, s \rangle \in \alpha$. This concludes the proof. □

PROPOSITION 4.4.

(1) *If* $f \in Hom\ (\mathbf{A}, \mathbf{B})$ *is surjective, with kernel* π*, and* $\theta, \psi \in \operatorname{Con}\mathbf{A}$*, then*

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

.

(2) *If* $\mathbf{B}$ *is a subalgebra of* $\mathbf{A}$ *and* θ*,* $\psi \in \operatorname{Con}\mathbf{A}$*, then the restrictions to* $\mathbf{B}$ *satisfy*

$$[\theta|_{\mathbf{B}}, \psi|_{\mathbf{B}}] \leq [\theta, \psi]|_{\mathbf{B}}.$$

PROOF. For (1), by Proposition 4.3 $[\theta, \psi] \vee \pi = [\theta \vee \pi, \psi \vee \pi] \vee \pi$. Thus we may assume without loss of generality that $\theta, \psi \geq \pi$. Then f carries a set of generators of $[\theta, \psi] \vee \pi$ (namely $X(\theta, \psi) \cup \pi$) onto a set of generators for $[f(\theta), f(\psi)]$. Hence $f([\theta, \psi] \vee \pi) = [f(\theta), f(\psi)]$, which is equivalent to the desired conclusion.

For (2), $\theta|_{\mathbf{B}}$ centralizes $\psi|_{\mathbf{B}}$ modulo $[\theta, \psi]|_{\mathbf{B}}$, or argue by generators. □

PROPOSITION 4.5. *Let* $\mathbf{A} = \Pi_{i \in I}\mathbf{A}_i$ *and* $\theta_i \in \operatorname{Con}\mathbf{A}_i$*,* $i \in I$*. Then the map*

(3) $(\theta_i)_{i \in I} \to \{\langle \mathbf{a}, \mathbf{b} \rangle \in A^2; \langle a_i, b_i \rangle \in \theta_i$*, for all* $i \in I$*, and* $a_i = b_i$ *for all but finitely many* $i \in I\}$

is a lattice isomorphism from $\Pi_{i \in I}\mathbf{Con}\ \mathbf{A}_i$ *into* $\mathbf{Con}\ \mathbf{A}$*. Furthermore, this isomorphism preserves the commutator operation. In particular if* $\mathbf{A} = \mathbf{A}_0 \times \mathbf{A}_1$*, and* $\theta_i, \psi_i \in \operatorname{Con}\mathbf{A}_i$*,* $i = 0, 1$*, then*

$$[\theta_0 \times \theta_1, \psi_0 \times \psi_1] = [\theta_0, \psi_0] \times [\theta_1, \psi_1].$$

Moreover if $\Pi_{i \in I}\theta_i = \{\langle \mathbf{a}, \mathbf{b} \rangle \in A^2 : \langle a_i, b_i \rangle \in \theta_i, i \in I\}$*, then*

(4) $[\Pi_{i \in I}\theta_i, \Pi_{i \in I}\psi_i] \leq \Pi_{i \in I}[\theta_i, \psi_i]$.

PROOF. We give an argument avoiding the term condition, in order to show that conditions Definition 3.1(1) and additivity imply (3). Let $g : \Pi_I\,\mathbf{Con}\ \mathbf{A}_i \to \mathbf{Con}\ \mathbf{A}$ be the map defined in (3). We leave it to the reader to show that g defines a lattice isomorphism of $\Pi_I\,\mathbf{Con}\ \mathbf{A}_i$ into $\mathbf{Con}\ \mathbf{A}$. Let $\lambda = \{\langle \mathbf{a}, \mathbf{b} \rangle \in A^2 : a_i = b_i$ for all but finitely many $i \in I\}$. Let p_i be the projection homomorphism $\mathbf{A} \twoheadrightarrow \mathbf{A}_i$ and η_i its kernel. Let $\eta_i' = \bigwedge_{j \neq i} \eta_j$. For $\theta_i \in \operatorname{Con}\mathbf{A}_i$ let $\overline{\theta}_i = p_i^{-1}\theta_i \in \mathbf{Con}\ \mathbf{A}$. Note g sends $(\theta_i)_{i \in I}$ to $\lambda \wedge (\bigwedge_I \overline{\theta}_i)$. If $\theta_i, \psi_i \in \operatorname{Con}\mathbf{A}_i$, $i \in I$, we wish to show

$$[g((\theta_i)_{i \in I}), g((\psi_i)_{i \in I})] = g(([\theta_i, \psi_i])_{i \in I}).$$

Let α and β be the left and right sides of this equation. By Proposition 4.4(1) $\overline{[\theta_i, \psi_i]} = p_i^{-1}[\theta_i, \psi_i] = [\overline{\theta}_i, \overline{\psi}_i] \vee \eta_i$. Hence $\beta = \lambda \wedge$

$(\bigwedge_I([\overline{\theta}_i, \overline{\psi}_i] \vee \eta_i))$ and $\alpha = [\alpha \wedge (\bigwedge \overline{\theta}_i), \lambda \wedge (\bigwedge \overline{\psi}_i)]$. Now $\alpha \leq \beta$ follows from monotonicity.

To see the other inclusion first note that (by arguing with elements in the direct product) we have $\lambda \wedge (\bigwedge_I \overline{\theta}_i) = \bigvee_I \overline{\theta}_i \wedge \eta_i'$. Hence $\beta = \bigvee_I [(\overline{\theta}_i \wedge \overline{\psi}_i) \vee \eta_i] \wedge \eta_i'$. Now $\overline{\theta}_i = (\overline{\theta}_i \wedge \eta_i') \vee \eta_i$ by modularity. Hence $[\overline{\theta}_i, \overline{\psi}_i] \vee \eta_i = [(\overline{\theta}_i \wedge \eta_i') \vee \eta_i, \overline{\psi}_i \wedge \eta_i'] \vee \eta_i = [\overline{\theta}_i \wedge \eta_i', \overline{\psi}_i \wedge \eta_i'] \vee \eta_i$ by additivity. Now this and modularity (and $[\overline{\theta}_i \wedge \eta_i', \overline{\psi}_i \wedge \eta_i'] \leq \eta_i'$) yield $([\overline{\theta}_i, \overline{\psi}_i] \vee \eta_i) \wedge \eta_i' = [\overline{\theta}_i \wedge \eta_i', \overline{\psi}_i \wedge \eta_i']$. Now, since $\eta_i' \leq \lambda, \beta \leq \alpha$ by monotonicity.

The proof of (4) is similar to the proof of $\alpha \leq \beta$. □

REMARKS 4.6. The homomorphism property, Proposition 4.4(1) or Definition 3.1(1), is extremely useful in applications. **Con B** is naturally isomorphic with the interval $1/\pi$ of **Con A** under f. In the presence of additivity, Proposition 4.4(1) simply tells us that for $\theta, \psi \in 1/\pi$ we can compute the commutator of $f(\theta)$ and $f(\psi)$ already in **Con A**. It corresponds to the congruence $[\theta, \psi]_\pi = [\theta, \psi] \vee \pi$. We call the operation $[\theta, \psi]_\pi$ a relative commutator.

If $\alpha/\beta \nearrow \gamma/\delta$ in **Con A**, then the map $\theta \mapsto \theta \vee \delta$ for $\theta \in \alpha/\beta$ is a lattice isomorphism with inverse $\psi \mapsto \psi \wedge \alpha, \psi \in \gamma/\delta$. This is a classical result of modular lattice theory. The above isomorphism also respects the relative commutator. That is, if $\theta, \psi \in \alpha/\beta$ and $\theta', \psi' \in \gamma/\delta$, then

$$[\theta, \psi]_\beta \vee \delta = [\theta \vee \delta, \psi \vee \delta]_\delta$$

and

$$[\theta', \psi']_\delta \wedge \alpha = [\alpha \wedge \theta', \alpha \wedge \psi']_\beta.$$

The first equation is an easy consequence of additivity. To see the second, first note $\theta' = (\theta' \wedge \alpha) \vee \delta$. Hence

$$\begin{aligned}
[\theta', \psi']_\delta \wedge \alpha &= ([\theta', \psi'] \vee \delta) \wedge \alpha \\
&= ([(\theta' \wedge \alpha) \vee \delta, (\psi' \wedge \alpha) \vee \delta] \vee \delta) \wedge \alpha \\
&= ([\theta' \wedge \alpha, \psi' \wedge \alpha] \vee \delta) \wedge \alpha \\
&= [\theta' \wedge \alpha, \psi' \wedge \alpha] \vee (\delta \wedge \alpha) \\
&= [\theta' \wedge \alpha, \psi' \wedge \alpha]_\beta.
\end{aligned}$$

Our proof of (3) shows that g preserves any global congruence operation on $\mathcal{V}$ (which is modular) as long as it satisfies Definition 3.1(1) and is finitely additive.

We present now an example showing that the inequality in (4) may be strict. Let $\mathbf{A}_i$ be the ring of all polynomials over the rationals, with 0 constant term, in noncommuting indeterminates $x_1, ..., x_i$. Of course,

each congruence corresponds uniquely to a (two-sided) ideal and if I and J are ideals $[I, J] = IJ \vee JI$ where IJ is the ideal generated by $\{ab : a \in I, b \in J\}$. Clearly $x_1^2 \vee ... \vee x_i^2 \in [\mathbf{A}_i, \mathbf{A}_i]$. Thus, if a $\in \mathbf{A} = \Pi \mathbf{A}_i$ has i^{th} component $x_1^2 + \cdots + x_i^2$, then a $\in \Pi[\mathbf{A}_i, \mathbf{A}_i]$. However, a $\notin [\mathbf{A}, \mathbf{A}]$. If it were, then there would be elements $a_1, ..., a_k, b_1, ...b_k$ in A with $a = a_1b_1 + \cdots + a_kb_k$. Choose $n > k$ and let the n^{th} component of a_i and b_i be p_i and q_i respectively. Then

$$(*) \qquad x_1^2 + \cdots + x_n^2 = p_1q_1 + \cdots + p_kq_k.$$

Let $\overline{p}_i$ be the polynomial obtained from p_i by deleting all nonlinear terms and define $\overline{q}_i$ similarly. Since the constant terms of each of these polynomials are zero, the above equation is still valid if we replace p_i and q_i with $\overline{p}_i$ and $\overline{q}_i$. Thus we may assume p_i and q_i are linear: say, $p_i = \sum_{j=1}^n c_{ij}x_j$ and $q_i = \sum_{j=1}^n d_{ij}x_j, c_{ij}, d_{ij}$ rational. Then $(*)$ yields

$$\sum_{i=1}^{k} c_{is}d_{it} = \delta_{st} \qquad 1 \leq s, t \leq n$$

i.e.,

$$C^T D = I_n$$

where $C = (c_{ij}), D = (d_{ij})$ and C^T is the transpose of C. Since C is a k by n matrix over the rationals, with $k < n$, this is impossible.

We will now show that our commutator is identical with the one defined by Hagemann and Herrmann, and also with $C^{\mathcal{V}}$ defined in Definition 3.1. For the next few paragraphs θ and ψ will denote fixed congruences of an algebra $\mathbf{A}$. $\mathbf{A}(\theta)$ will denote θ viewed as a subalgebra of $\mathbf{A}^2$. Of course. $\mathbf{A}(\psi)$ is defined similarly. However, we shall write the elements of $\mathbf{A}(\theta)$ as $\begin{bmatrix} x \\ y \end{bmatrix}$ instead of $\langle x, y \rangle$. We shall write the elements of $\mathbf{A}(\psi)$ as $\begin{bmatrix} x & y \end{bmatrix}$ instead of $\langle x, y \rangle$. Thus we are thinking of the elements of $\mathbf{A}(\theta)$ as column vectors and those of $\mathbf{A}(\psi)$ as row vectors. Hence, in the following definition, an element $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ of $\mathbf{A}(\theta, \psi)$, can be thought of as a member of $\mathbf{A}(\theta) \times \mathbf{A}(\theta)$ and also of $\mathbf{A}(\psi) \times \mathbf{A}(\psi)$.

DEFINITION 4.7. (1) $\mathbf{A}(\theta, \psi) \subseteq \mathbf{A}^4$ is the subalgebra of all matrices whose columns belong to θ and rows belong to ψ.

(2) $\Delta_{\theta,\psi}$ is the congruence on $\mathbf{A}(\theta)$ generated by the set of all pairs of the form $\begin{bmatrix} u & v \\ u & v \end{bmatrix}$ in $\mathbf{A}(\theta, \psi)$.

(3) $\Delta^{\theta,\psi}$ is the congruence on $\mathbf{A}(\psi)$ generated by the set of all pairs of the form $\begin{bmatrix} x & x \\ y & y \end{bmatrix}$ in $\mathbf{A}(\theta, \psi)$.

In this notation, $\begin{bmatrix} x & r \\ y & s \end{bmatrix} \in \Delta_{\theta,\psi}$ is equivalent to $\begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} r \\ s \end{bmatrix} \pmod{\Delta_{\theta,\psi}}$. Another aspect of the symmetry of the commutator is that $\Delta_{\theta,\psi} = \Delta^{\theta,\psi}$. You will get a chance to prove this in the exercises.

LEMMA 4.8. *$\Delta_{\theta,\psi}$ is the least transitive relation on $\mathbf{A}(\theta)$ containing $M(\theta, \psi)$.*

PROOF. It is not hard to show that the transitive closure of $M(\theta, \psi)$, thought of as a relation on $\mathbf{A}(\theta)$, is a congruence Γ on $\mathbf{A}(\theta)$. Since the generators of $\Delta_{\theta,\psi}$ lie in $M(\theta, \psi)$, $\Delta_{\theta,\psi} \subseteq \Gamma$. But by Proposition 3.3(1) $M(\theta, \psi) \subseteq \Delta_{\theta,\psi}$. Hence. $\Gamma \subseteq \Delta_{\theta,\psi}$. □

THEOREM 4.9. *For $x, y \in \mathbf{A}$ the following are equivalent:*

(i) $\langle x, y \rangle \in [\theta, \psi]$,

(ii) $\begin{bmatrix} x & y \\ y & y \end{bmatrix} \in \Delta_{\theta,\psi}$,

(iii) *for some a,* $\begin{bmatrix} x & a \\ y & a \end{bmatrix} \in \Delta_{\theta,\psi}$,

(iv) *for some b,* $\begin{bmatrix} x & y \\ b & b \end{bmatrix} \in \Delta_{\theta,\psi}$.

PROOF. Clearly (ii) implies both (iii) and (iv). To see that (iii) implies (ii), suppose $\begin{bmatrix} x & a \\ y & a \end{bmatrix} \in \Delta_{\theta,\psi}$. It is easy to see that this implies that $y \ \psi \ a$. Therefore $\begin{bmatrix} a & y \\ a & y \end{bmatrix} \in \Delta_{\theta,\psi}$, and hence by transitivity, $\begin{bmatrix} x & y \\ y & y \end{bmatrix} \in \Delta_{\theta,\psi}$, proving (ii).

Now assume that $\begin{bmatrix} x & y \\ b & b \end{bmatrix} \in \Delta_{\theta,\psi}$. Since the columns are in $\mathbf{A}(\theta)$, x, y, and b are all in the same θ–class. Thus. if we let $\eta_0, \eta_1 \in \operatorname{Con} \mathbf{A}(\theta)$ be the congruences associated with the two projections, we have the situation diagrammed in Figure 1.

Hence, $\begin{bmatrix} x & y \\ y & y \end{bmatrix} \in \Delta_{\theta,\psi}$ by the Shifting Lemma. Thus (ii), (iii), and (iv) are all equivalent. We claim that $[\theta, \psi]$ is the least congruence

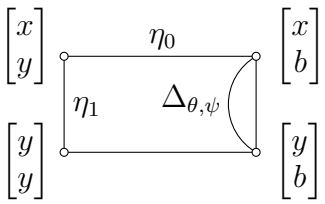


FIGURE 1.

on $\mathbf{A}$ which is a union of $\Delta_{\theta,\psi}$ classes. Indeed, by its definition (and Proposition 4.2), $[\theta, \psi]$ is the smallest congruence β such that if one column of a matrix in $M(\theta, \psi)$ is in β then the other is. Now if

$$\begin{bmatrix} a \\ b \end{bmatrix} \equiv \begin{bmatrix} c \\ d \end{bmatrix} \pmod{\Delta_{\theta,\psi}},$$

then, since $\Delta_{\theta,\psi}$ is the transitive closure of $M(\theta, \psi)$, there is a finite sequence of columns going from

$$\begin{bmatrix} a \\ b \end{bmatrix} \text{ to } \begin{bmatrix} c \\ d \end{bmatrix}$$

with each consecutive pair of columns forming a matrix in $M(\theta, \psi)$. It follows from the above, that if

$$\begin{bmatrix} a \\ b \end{bmatrix} \in [\theta, \psi], \text{ then } \begin{bmatrix} c \\ d \end{bmatrix} \in [\theta, \psi],$$

i.e. $[\theta, \psi]$ is a union of $\Delta_{\theta,\psi}$ classes. Of course, any congruence which is the union of $\Delta_{\theta,\psi}$ classes will satisfy the defining property of $[\theta, \psi]$. Thus the claim holds. From this, (ii) implies (i) follows immediately since certainly $\begin{bmatrix} y \\ y \end{bmatrix} \in [\theta, \psi]$.

Using that (ii) and (iv) are equivalent, it is not hard to show that the set of

$$\begin{bmatrix} x \\ y \end{bmatrix}$$

which satisfy (ii) is a congruence α. Now α is obviously the union of $\Delta_{\theta,\psi}$ classes, and hence $[\theta, \psi] \leq \alpha$, by the claim. Thus (i) implies (ii). □

The set of $\langle x, y \rangle$ which satisfy condition (iv) of the last theorem is the Hagemann-Herrmann commutator, and of course the theorem shows that it is the same as the one we have defined.

THEOREM 4.10. $C^{(\mathcal{V})}(\theta, \psi) = [\theta, \psi]$.

PROOF. By Proposition 4.4 $[\theta, \psi] \subseteq C^{(\mathcal{V})}(\theta, \psi)$. For the other inclusion we repeat the argument for groups given in Chapter 1. Consider the following congruences on $\mathbf{A}(\theta)$:

$$\Delta = \Delta_{\theta,\psi}$$
$$[\theta, \psi]_0 = \{\langle\langle x, u\rangle, \langle y, v\rangle\rangle \in \mathbf{A}(\theta)^2 : \langle x, y\rangle \in [\theta, \psi]\}$$
$$\eta_1 = \{\langle\langle x, u\rangle, \langle y, u\rangle\rangle \in \mathbf{A}(\theta)^2 : x\ \theta\ y\ \theta\ y\}$$

and let $P_0 : \mathbf{A}(\theta) \to \mathbf{A}$ be the first projection. In Con $\mathbf{A}(\theta)$ we have $C^{(\mathcal{V})}(\eta_1, \Delta) \leq \eta_1 \wedge \Delta \leq [\theta, \psi]_0$. The first inequality is part of the definition of $C^{(\mathcal{V})}$, and the second follows from the equivalence of (i) and (iv) in the last theorem. If for $\alpha \in \operatorname{Con}\mathbf{A}$ we put $\alpha_0 = p_0^{-1}(\alpha)$ and $\eta_0 = p_0^{-1}(0)$, then it is easy to see, by arguing on elements, that $\theta_0 = \eta_1 \vee \eta_0, \psi_0 = \Delta \vee \eta_0$. Hence, $\theta = p_0(\eta_1 \vee \eta_0)$ and $\psi = p_0(\Delta \vee \eta_0)$. Thus by the definition of $C^{(\mathcal{V})}$ we have

$$\begin{aligned} C^{(\mathcal{V})}(\theta, \psi) &= C^{(\mathcal{V})}(P_0(\eta_1 \vee \eta_0), P_0(\Delta \vee \eta_0)) \\ &= P_0(C^{(\mathcal{V})}(\eta_1, \Delta) \vee \eta_0) \\ &\leq [\theta, \psi]. \end{aligned}$$

completing the proof. □

The next theorem gives the Hagemann-Herrmann lattice theoretic characterization of the commutator. First we introduce some useful notation. For $\mathbf{B}$ a subalgebra of $\mathbf{A} \times \mathbf{A}$ and $\gamma \in \operatorname{Con}\mathbf{A}$, let $\gamma_i, i = 0, 1$, be the congruence on $\mathbf{B}$ defined by $\langle x_0, x_1\rangle\ \gamma_i\ \langle y_0, y_1\rangle$ if $x_i\ \gamma\ y_i$. We use η_1 to denote 0_i.

THEOREM 4.11. *Let $\mathbf{A}$ be an algebra in a modular variety $\mathcal{V}$ and let α, θ, $\psi \in \operatorname{Con}\mathbf{A}$. Then $a \geq [\theta, \psi]$ if and only if there is a $\mathbf{B} \in \mathcal{V}$ and a homomorphism $f : \mathbf{B} \twoheadrightarrow \mathbf{A}$ and σ, $\tau \in \operatorname{Con}\mathbf{B}$ with.*

$$\sigma \vee f^{-1}(\alpha) \geq f^{-1}(\psi)$$
$$\tau \vee f^{-1}(\alpha) \geq f^{-1}(\theta)$$
$$f^{-1}(\alpha) \geq \sigma \wedge \tau.$$

PROOF. First suppose that $\alpha \geq [\theta, \psi]$, and let $\beta = [\theta, \psi]$. Take $\mathbf{B} = \mathbf{A}(\theta), \sigma = \Delta_{\theta,\psi}, \tau = \eta_1 \in \operatorname{Con}\mathbf{B}$, and let f be the first projection. Then $\Delta_{\theta,\psi} \vee \beta_0 = \psi_0, \eta_1 \vee \beta_0 = \theta_0 = \theta_1$, and $\beta_0 \geq \Delta_{\theta,\psi} \wedge \eta_1$. As noted in the last theorem, the last inequality follows from Theorem 4.9, and the others follow from easy arguments on the elements. For example, if $\langle x, y\rangle\ \psi_0\ \langle u, v\rangle$, i.e., $x\ \pi\ u$ and $\langle x, y\rangle, \langle u, v\rangle \in \mathbf{A}(\theta)$, then $\langle x, y\rangle\ \beta_0\ \langle x, x\rangle\ \Delta\ \langle u, u\rangle\ \beta_0\ \langle u, v\rangle$. Since $\beta_0 = f^{-1}(\beta) \leq f^{-1}(\alpha)$, one direction of the theorem is proved.

For the other direction, suppose such a $\mathbf{B}, f, \sigma$ and τ exist. Then by additivity.

$$\begin{aligned}[f^{-1}(\theta), f^{-1}(\psi)] &\leq [\tau \vee f^{-1}(\alpha), \sigma \vee f^{-1}(\alpha)] \\ &\leq \sigma \wedge \tau \vee f^{-1}(\alpha) \\ &= f^{-1}(\alpha).\end{aligned}$$

Hence by Proposition 4.4, $[\theta, \psi] \leq \alpha$, □

The next definition defines the residuation operation which is important in multiplicative ideal theory. It also will play an important role here.

DEFINITION 4.12. For $\theta, \psi \in \operatorname{Con}\mathbf{A}$ we let $(\theta : \psi)$ denote the largest $\gamma \in \operatorname{Con}\mathbf{A}$ such that $[\psi, \gamma] \leq \theta$. This operation is known as **residuation**.

Exercises

1. Suppose that $\mathbf{A}$ lies in a permutable variety with Mal'cev term $p(x, y, x)$. Suppose $\theta, \psi \in \operatorname{Con}\mathbf{A}$ with $[\theta, \psi] = 0$ and let $b \in \mathbf{A}$ be fixed. Define $x + y = p(x, b, y)$. Show that if $x \; \theta \; b \; \psi \; y$ and z is arbitrary then $x + y = y + x$ and $x + (y + z) = (z + y) + z$.

2. Show that

$$\begin{bmatrix} x & y \\ u & v \end{bmatrix} \in \Delta^{\theta,\psi} \text{ if and only if } \begin{bmatrix} x & u \\ y & v \end{bmatrix} \in \Delta_{\psi,\theta}.$$

3. Show that if Δ is either $\Delta_{\theta,\psi}$ or $\Delta^{\theta,\psi}$ then

(i)

$$\begin{bmatrix} x & y \\ x & y \end{bmatrix} \in \Delta \text{ if and only if } \langle x, y \rangle \in \psi.$$

(ii)

$$\begin{bmatrix} x & x \\ u & u \end{bmatrix} \in \Delta \text{ if and only if } \langle x, u \rangle \in \theta.$$

(iii)

$$\begin{bmatrix} x & y \\ u & v \end{bmatrix} \in \Delta$$

implies

$$\begin{bmatrix} x & y \\ x & y \end{bmatrix}, \begin{bmatrix} x & x \\ u & u \end{bmatrix}, \begin{bmatrix} u & v \\ x & y \end{bmatrix}, \begin{bmatrix} y & x \\ v & u \end{bmatrix} \in \Delta.$$

4. Use the Shifting lemma to show that if

$$\begin{bmatrix} a & a \\ c & d \end{bmatrix} \in \Delta_{\theta,\psi}$$

and

$$\begin{bmatrix} a \\ b \end{bmatrix} \in \theta,$$

then

$$\begin{bmatrix} b & b \\ c & d \end{bmatrix} \in \Delta_{\theta,\psi}.$$

5. Prove $\Delta_{\theta,\psi} = \Delta^{\theta,\psi}$. (Hint: By Lemma 4.8 it suffices to show that if

$$\begin{bmatrix} x & y \\ u & v \end{bmatrix}, \begin{bmatrix} u & v \\ r & s \end{bmatrix} \in \Delta_{\theta,\psi}$$

then

$$\begin{bmatrix} x & y \\ r & s \end{bmatrix} \in \Delta_{\theta,\psi}.$$

Do this using Lemma 2.3 and the previous exercises.)

6. For $\alpha_i, \beta \in \operatorname{Con}\mathbf{A}$ show that the residuation defined in Definition 4.12 satisfies $(\bigwedge \alpha_i : \beta) = \bigwedge(\alpha_i : \beta)$.

CHAPTER 5

The Fundamental Theorem on Abelian Algebras

Initially we do not assume $\mathbf{A}$ lies in a modular variety.

DEFINITION 5.1. The center of any algebra $\mathbf{A}$ is the binary relation $\zeta_{\mathbf{A}} \subseteq \mathbf{A}^2$ defined by

$$\langle x, y\rangle \in \zeta_{\mathbf{A}} \Leftrightarrow (\forall t)(\forall u, v)\,(t(u, x) = t(v, x) \longleftrightarrow t(u, y) = t(v, y)).$$

(The first quantifier is over all term operations of $\mathbf{A}$, the second is over all n-tuples of $\mathbf{A}$, n depending on t.)

LEMMA 5.2. *$\zeta_{\mathbf{A}}$ is is the largest congruence α on $\mathbf{A}$ such that $[\alpha, 1_{\mathbf{A}}] = 0_{\mathbf{A}}$.* $\square$

This result follows easily from Definition 3.2. Henceforth, all varieties will be assumed to be modular and all algebras will be assumed to generate modular varieties.

DEFINITION 5.3. A congruence $\theta \in \operatorname{Con}\mathbf{A}$ is called **Abelian** if $[\theta, \theta] = 0$. An algebra $\mathbf{A}$ is Abelian if $[1_{\mathbf{A}}, 1_{\mathbf{A}}] = 0_{\mathbf{A}}$, or, what amounts to the same thing, $\zeta_{\mathbf{A}} = 1_{\mathbf{A}}$, variety is Abelian if all its members are.

DEFINITION 5.4. We call $\mathbf{A}$ **affine** if there is an Abelian group $\langle A, +, -\rangle = \hat{\mathbf{A}}$ having the same universe as $\mathbf{A}$, and a 3-ary term operation of $\mathbf{A}$, $t(x, y, z)$, such that:

(1) $t(x, y, z) = x - y + z$ for all $x, y, z \in A$
(2) $f(\mathbf{x} - \mathbf{y} + \mathbf{z}) = f(\mathbf{x}) - f(\mathbf{y}) + f(\mathbf{z})$ for each term operation f and $\mathbf{x}, \mathbf{y}, \mathbf{z} \in A^n$.

When these conditions hold, t is called a difference operation for $\mathbf{A}$, the algebra $\langle A, t\rangle$ is called a **ternary group**, and we say that $\mathbf{A}$ is **t-affine**.

Before proceeding further, we mention that Definition 5.4(2) has two equivalent forms, as the reader can verify. First, $\{\langle x, y, z, u\rangle : x + y = z + u\}$ is a subalgebra of $\mathbf{A}^4$. Second, each operation (and each term operation) of the algebra $\mathbf{A}$ is affine with respect to the group $\hat{\mathbf{A}}$, that is to say, for any given operation F (say F is n-ary) there are endomorphisms $\alpha_1, \ldots, \alpha_n$ of $\hat{\mathbf{A}}$ and an element $a \in \mathbf{A}$ such that F can

be expressed identically as

$$F(x_1, \dots, x_n) = \sum_{i=1}^{n} \alpha_i(x_i) + a.$$

In this chapter we shall prove Herrmann's result that in a modular variety every Abelian algebra is affine, and conversely. The proof we present is relatively short and direct. It also proves a generalization and establishes other facts we will use later. The proof combines ideas from several people. Credits will be given at the end of the chapter. We begin with some useful preliminary results.

THEOREM 5.5. *For each modular variety $\mathcal{V}$ there is a ternary term d, called a difference term, satisfying the following.*

(i) $d(x, x, y) \approx y$ *is an identity of* $\mathcal{V}$.

(ii) *If* $\langle x, y\rangle \in \theta \in \operatorname{Con}\mathbf{A}$, $\mathbf{A} \in \mathcal{V}$, *then* $d(x, y, y)\ [\theta, \theta]\ x$.

(iii) *If* $\alpha, \beta, \gamma \in \operatorname{Con}\mathbf{A}$, $\mathbf{A} \in \mathcal{V}$ *and* $\alpha \wedge \beta \leq \gamma$, *then the implication of* Figure 1 *holds.*

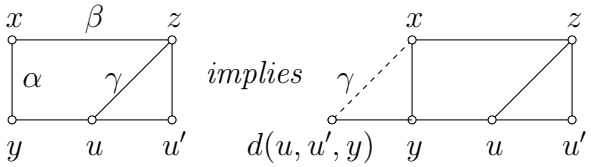


FIGURE 1.

PROOF. Since $\mathcal{V}$ is modular there are terms $m_0(x, y, z, u), \dots, m_n(x, y, z, u)$ which satisfy the identities of Theorem 2.2. Define $q_i(x, y, z)$, $i = 0, 1, \dots, n$ inductively by

$$q_0(x, y, z) = z$$

$$q_{i+1}(x, y, z) = \begin{cases} m_{i+1}(q_i(x, y, z), y, x, q_i(x, y, z)) & i \text{ odd} \\ m_{i+1}(q_i(x, yz), x, q_i(x, y, z)) & i \text{ even} \end{cases}$$

and set

$$d(x, y, z) = q_n(x, y, z).$$

It follows from Theorem 2.2(ii) that $q_i(x, x, y) \approx y$. Hence $d(x, x, y) \approx y$ holds in $\mathcal{V}$.

To show (ii) assume $\langle x, y\rangle \in \theta$. We prove inductively that

$$(1) \qquad \begin{aligned} &q_i(x,y,y)\ [\theta,\theta]\ m_i(y,y,y,x), && i \text{ odd} \\ &q_i(x,y,y)\ [\theta,\theta]\ m_i(y,y,x,x), && i \text{ even} \end{aligned}$$

Since $m_n(x, y, z, u) = u$, (ii) will then follow. The case $i = 0$ is immediate from Day's identities. Suppose i is odd and that (1) holds for i. Then

$$\begin{aligned} q_{i+1}(x,y,y) &= m_{i+1}(q_i(x,y,y), y, x, q_i(x,y,y)) \\ &\quad [\theta,\theta]\ m_{i+1}(m_i(y,y,y,x), y, x, m_i(y,y,y,x)). \end{aligned}$$

Now by Theorem 2.2

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

The term condition of Definition 3.2(2) says that if

$$t(x, x_1, \ldots, x_{n-1}) = t(x, y_1, \ldots, y_{n-1})$$

for certain elements of $\mathbf{A}$ with $x_i\ \theta\ y_i$, $i = 1, \ldots, n-1$, then $t(y, x_1, \ldots, x_{n-1})\ [\theta, \theta]$ $t(y, y_1, \ldots, y_{n-1})$ for any $y \in \mathbf{A}$ with $x\ \theta\ y$. Applying this to the sixth variable of the above equation, we get

$$\begin{aligned} &m_{i+1}(m_i(y,y,y,x), y, x, m_i(y,y,y,x)) \\ &\quad [\theta,\theta]\ m_{i+1}(m_i(y,y,y,y), y, x, m_i(x,x,x,x)) = m_{i+1}(y,y,x,x). \end{aligned}$$

Thus $q_{i+1}(x, y, y)\ [\theta, \theta]\ m_{i+1}(y, y, x, x)$.

Now suppose i is even and that (1) holds for i. Then

$$q_{i+1}(x,y,y)\ [\theta,\theta]\ m_{i+1}(m_i(y,y,x,x), x, y, m_i(y,y,x,x))$$

as before. Now

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

The term condition implies

$$\begin{aligned} m_{i+1}(m_i(y,y,x,x), &x, y, m_i(m_i(y,y,x,x)) \\ &\quad [\theta,\theta]\ m_{i+1}(m_i(y,y,y,y), y, y, m_i(x,x,x,x)) \\ &= m_{i+1}(y,y,y,x). \end{aligned}$$

Thus $q_{i+1}(x, y, y)\ [\theta, \theta]\ m_{i+1}(y, y, y, x)$.

To prove (iii) we shall show that any term $d(x, y, z)$ which satisfies (i) and (ii) satisfies (iii). Suppose $d(x, y, z)$ satisfies (i) and (ii), and that the relations of Figure 2 hold for congruences α, β, and γ where $\alpha \wedge \beta \leq \gamma$.

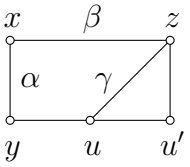


FIGURE 2.

Then $d(u, u', y)\ \beta\ d(y, y, y) = y$. Also

$$d(u, u', y)\ \gamma\ d(z, u', y) \tag{2}$$

$$d(z, u', y)\ \alpha\ d(z, z, x) = x \tag{3}$$

$$d(z, u', y)\ \beta\ d(x, y, y). \tag{4}$$

Since $\langle x, y\rangle \in \alpha \wedge (\beta \vee \gamma)$, (ii) yields $d(x, y, y)\ [\alpha \wedge (\beta \vee \gamma), \alpha \wedge (\beta \vee \gamma)]\ x$. But $[\alpha \wedge (\beta \vee \gamma), \alpha \wedge (\beta \vee \gamma)] \leq [\alpha, \beta \vee \gamma] = [\alpha, \beta] \vee [\alpha, \gamma] \leq (\alpha \wedge \beta) \vee (\alpha \wedge \gamma) = \alpha \wedge \gamma$. Thus by (4) $d(z, u', y)\ \beta \vee \alpha \wedge \gamma\ x$. Hence $d(z, u', y)\ \alpha \wedge (\beta \vee (\alpha \wedge \gamma))\ x$. But $\alpha \wedge (\beta \vee (\alpha \wedge \gamma)) = (\alpha \wedge \beta) \vee (\alpha \wedge \gamma) = \alpha \wedge \gamma$, that is, $d(z, u', y)\ \alpha \wedge \gamma\ x$. Hence by (2) $d(u, u', y)\ \gamma\ x$, proving (iii). □

We remark that a term which satisfies (iii) will satisfy (i) and (ii); see Exercise 6.

The term $d(x, y, z)$ constructed above plays an important role in our theory. We call a term which satisfies Theorem 5.5(i) and (ii) a **difference term** for $\mathcal{V}$, or a **Gumm difference term**. In what follows, d will always denote a difference term. Of course, in a permutable variety a Mal'cev term satisfies Theorem 5.5(i) and (ii) and thus is a difference term.

The next lemma proves Gumm's observation that a Mal'cev term (see Theorem 2.1(1)) which commutes with itself defines a ternary Abelian group.

LEMMA 5.6. *Let $t(x, y, z)$ be a 3-ary operation on a set S such that t commutes with itself and satisfies the Mal'cev equations $t(x, x, y) \approx y \approx t(y, x, x,)$. For any fixed $a \in S$ the operation $x + y = t(x, a, y)$ defines*

an Abelian group on S with a as null element and with $-x = t(a, x, a)$. Moreover, $t(x, y, z) = x - y + z$.

PROOF. That t commutes with itself means that for all $x_i, y_i, z_i \in S$

$$\begin{aligned} &t(t(x_1, y_1, z_1), t(x_2, y_2, z_2), t(x_3, y_3, z_3)) \\ &\qquad = t(t(x_1, x_2, x_3), t(y_1, y_2, y_3), t(z_1, z_2, z_3)). \end{aligned}$$

Clearly, $x + a = a + x = x$. For associativity

$$\begin{aligned} x + (y + z) &= t(x, a, t(y, a, z)) \\ &= t(t(x, a, a), t(a, a, a), t(y, a, z)) \\ &= t(t(x, a, y), t(a, a, a), t(a, a, z)) \\ &= t(t(x, a, y), a, z) \\ &= (x + y) + z. \end{aligned}$$

To see that $-x = t(a, x, a)$, we calculate

$$\begin{aligned} x + t(a, x, a) &= t(x, a, t(a, x, a)) \\ &= t(t(x, a, a), t(a, a, a), t(a, x, a)) \\ &= t(t(x, a, a), t(a, a, x), t(a, a, a)) \\ &= t(x, x, a) \\ &= a. \end{aligned}$$

Now

$$\begin{aligned} x + y &= t(x, a, y) \\ &= t(t(a, a, x), t(a, a, a), t(y, a, a)) \\ &= t(t(a, a, y), t(a, a, a), t(x, a, a)) \\ &= t(y, a, x) \\ &= y + x. \end{aligned}$$

To see that $x - y + z = t(x, y, z)$, we first show that $x - y = t(x, y, a)$:

$$\begin{aligned} x - y &= t(x, a, t(a, y, a)) \\ &= t(t(x, a, a), t(a, a, a), t(a, y, a)) \\ &= t(t(x, a, a), t(a, a, y), t(a, a, a)) \\ &= t(x, y, a). \end{aligned}$$

Finally

$$\begin{aligned} x - y + z &= t(t(x, y, a), a, z) \\ &= t(t(x, y, a), t(a, a, a), t(a, a, z)) \\ &= t(t(x, a, a), t(y, a, a), t(a, a, z))t(x, y, z). \end{aligned}$$

□

PROPOSITION 5.7. *Let $\alpha \geq \beta$ where $\alpha, \beta \in \operatorname{Con}\mathbf{A}$. The following are necessary and sufficient conditions in order that $[\alpha, \beta] = 0$. For any basic operation (and hence any term operation) $s(x_1, \ldots, x_n)$ and elements $x_i \ \beta \ y_i \ \alpha \ z_i$, $(i = 1, \ldots, n)$ we have*

$$d(s(\mathbf{x}), s(\mathbf{y}), s(\mathbf{z})) = s(d(x_1, y_1, z_1), \ldots, d(x_n, y_n, z_n))$$

and

$$\langle y, z\rangle \in \beta \quad \textit{implies} \quad d(y, z, z) = d(z, z, y) = y.$$

PROOF. Suppose first that $[\alpha, \beta] = 0$. By considering the congruences η_0, η_1 (first and second projections) and $\Delta = \Delta_{\alpha,\beta}$ on the algebra $\mathbf{A}(\alpha)$ (see Definition 4.7). When $x \ \beta \ y \ \alpha \ z$, we have the relations of Firure 3.

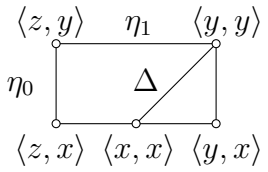


FIGURE 3.

Hence, by Theorem 5.5(iii)

$$\langle d(x, y, z), x\rangle \equiv \langle z, y\rangle \pmod{\Delta_{\alpha,\beta}}.$$

In particular

$$\langle d(s(\mathbf{x}), s(\mathbf{y}), s(\mathbf{z})), s(\mathbf{x})\rangle \equiv \langle s(\mathbf{z}), s(\mathbf{y})\rangle \pmod{\Delta_{\alpha,\beta}}.$$

But applying s to the n congruences $\langle d(x_i, y_i, z_i), x_i\rangle \equiv \langle z_i, y_i\rangle$ yields

$$\langle s(d(x_1, y_1, z_1), \ldots, d(x_n, y_n, z_n)), s(\mathbf{x})\rangle \ \Delta_{\alpha,\beta} \ \langle s(\mathbf{z}), s(\mathbf{y})\rangle.$$

Since $[\alpha, \beta] = 0$, and by the equivalence of (i) and (iv) in Theorem 4.9 the two displayed formulas above give the desired conclusion.

The last statement follows from Theorem 5.5.

Now suppose the conditions hold. Then the congruence $\Delta_{\beta,\alpha}$ on $\mathbf{A}(\beta)$ (see Definition 4.7) is characterized by

$$\langle x, y\rangle \ \Delta_{\beta,\alpha} \ \langle u, v\rangle \quad \text{iff} \quad x \ \beta \ y \ \alpha \ u \text{ and } v = d(y, x, u).$$

To see this let Δ' be the relation on $\mathbf{A}^2$ defined by the second part, that is, $\Delta' = \{\langle\langle x, y\rangle, \langle u, v\rangle\rangle : x \ \beta \ y \ \alpha \ u, v = d(y, x, u)\}$. That Δ' determines a congruence on $\mathbf{A}(\beta)$ follows from the properties of d and the conditions of Proposition 5.7. For example, to see that this relation

is symmetric suppose $x\ \beta\ y\ \alpha\ u$ and $v = d(y,x,u)$. Clearly $u\ \beta\ v\ \alpha\ x$ and since d commutes with itself.

$$\begin{aligned} d(v,u,x) &= d(d(y,x,u),d(x,x,u),d(x,x,x)) \\ &= d(d(y,x,x),d(x,x,x),d(u,u,x) \\ &= d(y,x,x) = y. \end{aligned}$$

which proves $\langle u,v\rangle\ \Delta'\ \langle x,y\rangle$, i.e., Δ' is symmetric.

Now $\Delta_{\beta,\alpha}$ is the congruence on $\mathbf{A}(\beta)$ generated by $\{\langle\langle x,x\rangle,\langle u,u\rangle\rangle : x\ \alpha\ u\}$. Clearly these generators are in Δ'. Hence $\Delta_{\beta,\alpha} \subseteq \Delta'$. Suppose $\langle x,y\rangle\ \Delta'\ \langle u,v\rangle$. Then $x\ \alpha\ u$ so that $\langle x,x\rangle\ \Delta_{\beta,\alpha}\ \langle u,u\rangle$. Now by calculations in $\mathbf{A}(\beta)$ we have

$$\langle x,y\rangle = \langle d(x,x,x),d(y,x,x)\rangle = d(\langle x,y\rangle,\langle x,x\rangle,\langle x,x\rangle)$$
$$\Delta_{\beta,\alpha}\ d(\langle x,y\rangle,\langle x,x\rangle,\langle u,u\rangle) = \langle d(x,x,u),d(y,x,u)\rangle = \langle u,v\rangle.$$

Hence $\Delta_{\beta,\alpha} = \Delta'$.

Now if $x\ [\alpha,\beta]\ y$ then $\langle x,x\rangle\ \Delta_{\beta,\alpha}\ \langle x,y\rangle$. Hence $y = d(x,x,x)$, i.e., $y = x$. □

The next corollary reformulates Proposition 5.7 for the case $\alpha = \beta$. For $u \in \mathbf{A}$ we let $\mathbf{M}(\beta,u) = \langle u/\beta, d\rangle$, the ternary group with universe the $\beta-$ block containing u. In Chapter 9 $\mathbf{M}(\beta,u)$ will be given a module structure.

COROLLARY 5.8. **A** *congruence* β *on* **A** *is Abelian if and only if each* $\mathbf{M}(\beta,u)$ *is a ternary group and whenever* $s(u_1,\ldots,u_n) = u$ *where* s *is an* n*–ary term operation then* $s : \mathbf{M}(\beta,u_1) \times \cdots \times \mathbf{M}(\beta,u_n) \to \mathbf{M}(\beta,u)$ *is a homomorphism, i.e.,* s *is affine between the* β*–blocks.*

PROOF. Since d is idempotent, the $\beta-$ block u/β is closed under d. If β is Abelian then, by Proposition 5.7, d commutes with itself on u/β and thus, by Lemma 5.6, $\mathbf{M}(\beta,u)$ is a ternary group. This corollary follows easily from Proposition 5.7. □

COROLLARY 5.9. *In a modular variety every Abelian algebra is affine, and conversely.* □

As the definition of affine and the remarks following it indicate, Abelian algebras are closely related to modules (in fact, each Abelian algebra is polynomially equivalent to a module). This connection is studied more thoroughly in Chapter 9.

The term $d(x,y,z)$ constructed in Theorem 5.5 was first constructed by Herrmann in [**45**]. The short proof that it satisfies (ii) is Taylor's. Gumm [**36**], [**38**], using his geometrical methods, constructed a term satisfying (iii) and showed (iii) implies (i) and (ii). Udi Hrushovskii

proved that (i) and (ii) imply (iii). Proposition 5.7 was proved by Gumm in [**38**]. Corollary 5.8 appeared in Herrmann [**45**]. Of course the fundamental theorem on Abelian algebras, Corollary 5.9, is Herrmann's [**45**]. It had been previously established for permutable varieties independently by Gumm and McKenzie.

Proposition 5.7 will play an important role in the rest of this book. Kiss [**56**] obtained a nice generalization of Theorem 5.5 and Proposition 5.7. He constructed a 4–ary term for each modular variety which he calls a 4–difference term. He then gave necessary and sufficient conditions for $[\alpha, \beta] = 0$ similar to those of Proposition 5.7. However his theorem does not require that $\alpha \geq \beta$. His results are described in more detail in the Related Literature chapter.

Exercises

All algebras are assumed to belong to a modular variety.

1. Show that if $\mathbf{M}_3$ (the five element modular, nondistributive lattice) is a 0, 1–sublattice of **Con** $\mathbf{A}$ then $\mathbf{A}$ is Abelian. (Assume $\boldsymbol{V}(\mathbf{A})$ is modular.)

2. Prove that for an algebra $\mathbf{A}$ in a modular variety the following are equivalent.

(i) $\mathbf{M}_3$ is a 0, 1–sublattice of $\mathbf{Con}(\mathbf{A} \times \mathbf{A})$,

(ii) the projection congruences of $\mathbf{A} \times \mathbf{A}$ have a common complement,

(iii) $\mathbf{M}_3$ is a 0, 1–sublattice of some subdirect product of two copies of $\mathbf{A}$.

(iv) $\mathbf{A}$ is Abelian.

3. Let $\mathbf{B}$ be a subdirect power of two copies of $\mathbf{A}$ such that the join of the kernels of the two projections is 1. Show that if $\mathbf{B}$ contains $\mathbf{M}_3$ as a 0, 1–sublattice then the subdirect product is direct.

4. Let α and β be the projection congruences of $\mathbf{A} \times \mathbf{B}$ and let $\gamma \in \mathbf{Con}(\mathbf{A} \times \mathbf{B})$ be arbitrary. Use Theorem Theorem 5.5(iii) to prove Gumm's result that every congruence permutes with the projection congruences of a direct product.

5. Suppose $\alpha \geq \beta$ and $[\alpha, \beta] = 0$. Then for $\langle u, v \rangle \in \alpha$ prove that the function $x \mapsto d(x, u, v)$ is an isomorphism from $\mathbf{M}(\beta, u)$ onto $\mathbf{M}(\beta, v)$.

6. Let $\mathcal{V}$ be a variety which has a term $d(x, y, z)$ satisfying Theorem 5.5(iii). Show that $\mathcal{V}$ is modular and Theorem 5.5(i) and (ii) hold for this d.

7. Show that if $\langle A, \cdot, /, \backslash, 1 \rangle$ is a loop which is Abelian then $x \cdot y$ is commutative and associative, i.e., $x \cdot y$ is an Abelian group operation.

8. Let $\mathbf{G}$ be the quasigroup with multiplication table

$\cdot$	0	1	2	3
0	3	2	0	1
1	2	3	1	0
2	1	0	2	3
3	0	1	3	2

Show $\mathbf{G}$ is Abelian (but $x \cdot y$ is neither commutative nor associative).

9. Let $\langle A, \cdot, /, \backslash \rangle$ be the quasigroup with multiplication

$\cdot$	0	1	2	3
0	0	1	2	3
1	2	3	0	1
2	1	2	3	0
3	3	0	1	2

For $c \in A$, define $x +_c y = p(x, c, y)$ where $p(x, y, z) = (x/(y \backslash y)) \cdot (y \backslash z)$. Show that for each c, $\langle A, +_c \rangle$ is an Abelian group but that $\langle A, \cdot, /, \backslash \rangle$ is not Abelian.

10. A subloop $\mathbf{H}$ of a loop $\mathbf{G}$ is called a **normal subloop** if there is some congruence on $\mathbf{G}$ whose class containing the identity element is $\mathbf{H}$. Exactly as for groups there is a one-to-one correspondence between normal subloops and congruences. Thus if $\mathbf{H}$ and $\mathbf{K}$ are normal subloops we can define $[\mathbf{H}, \mathbf{K}]$ to be the normal subloop corresponding to the commutator of the congruences associated with $\mathbf{H}$ and $\mathbf{K}$. This exercise will show that this correspondence is not as nice as one might hope. Namely if $\mathbf{G}$ is a group and $\mathbf{H}$ is a normal subgroup of $\mathbf{G}$ then $[\mathbf{H}, \mathbf{H}]$ is the derived subgroup of $\mathbf{H}$. In particular it depends only on $\mathbf{H}$ and not on $\mathbf{G}$. However for loops this is not the case; $[\mathbf{H}, \mathbf{H}]$ is not determined from just $\mathbf{H}$. One needs the whole congruence associated with $\mathbf{H}$ to determine $[\mathbf{H}, \mathbf{H}]$.

To see this let $\mathbf{Z}_4 = \{0, 1, 2, 3\}$ denote the group of integers under addition modulo 4. Let $G = Z_4 \times Z_4$ and define a binary operation on G by $\langle a, b \rangle \cdot \langle c, d \rangle = \langle a + c, b + d \rangle$ unless $b = d = 1$

in which case the operation is defined by the following table:

$\cdot$	01	11	21	31
01	12	02	22	32
11	02	22	32	12
21	22	32	12	02
31	32	12	02	22

Show that $\mathbf{G} = \langle G, \cdot \rangle$ is a loop with identity element $\langle 0, 0 \rangle$ and that the second projection is a homomorphism. Let θ be the congruence associated with this projection. Let $\mathbf{H} = \{\langle 0, 0 \rangle, \langle 1, 0 \rangle, \langle 2, 0 \rangle, \langle 3, 0 \rangle\}$ be the normal subloop associated with θ. Show that as a subloop of $\mathbf{G}$, $\mathbf{H}$ is isomorphic to the group $\mathbf{Z}_4$, and hence $\mathbf{H}$ is an Abelian loop. However, show that in $\mathbf{G}$, $[\theta, \theta] \neq 0$.

This fact may explain why the commutator was slow to be developed in the theory of loops.

11. Prove the following result of C. Herrmann [**46**]. Let $\mathcal{V}$ be a variety such that **Con A** is a complemented modular lattice for all $\mathbf{A} \in \mathcal{V}$. Prove that $\mathcal{V}$ is Abelian. The congruence λ defined in the proof of Proposition 4.5 may be useful.

CHAPTER 6

Permutability and a Characterization of Modular Varieties

One of the surprising consequences of commutator theory is that certain pairs of congruences are forced to permute. Most of the people who have worked with the commutator have proved results of this nature. For example, by Corollary 5.9 Abelian algebras have permutable congruences and the factor congruences of the direct product of two algebras permute with all congruences (see Exercise 5.4.). The best results on permutability have been obtained by H.-P. Gumm [**41**]. We present here a sample of these results, proving those parts we will use later and relegating the proofs of the remaining results to the exercises. We also give Gumm's characterization of modular varieties in terms of a Mal'cev condition which amalgamates Jónsson's condition for distributivity with Mal'cev's condition for permutability (see Theorem 2.1).

DEFINITION 6.1. Given $\alpha, \beta \in \mathbf{Con}\ \mathbf{A}$ we put $[\alpha]^0 = (\beta, \alpha]^0 = \alpha$, $[\alpha]^{n+1} = [[\alpha]^n, [\alpha^n]]$, $(\beta, \alpha]^{n+1} = [\beta, (\beta, \alpha]^n]$ for each $n < \omega$. Then

(1) α is **Abelian** if $[\alpha, \alpha] = 0$, **central** if $[1, \alpha] = 0$. k**-step solvable** if $[\alpha]^k = 0$. k**-step nilpotent** if $(\alpha, \alpha]^k = 0$
(2) $\mathbf{A}$ is k-step solvable if $1_{\mathbf{A}}$ is k-step solvable, k-step nilpotent or **nilpotent of class** k if $(1_{\mathbf{A}}, 1_{\mathbf{A}}]^k = 0$.
(3) α is co-solvable if $\mathbf{A}/\alpha$ is solvable (i.e., k-step solvable for some k).

In the following, $\alpha \circ \beta$ is the composition (or relation product) of α with β.

THEOREM 6.2. *For α, $\beta \in \mathbf{Con}\ \mathbf{A}$ we have for all $k < \omega$*

$$\alpha \circ \beta \subseteq [\alpha]^k \circ \beta \circ \alpha.$$

Every solvable and every co-solvable congruence permutes with all congruences, and every solvable algebra has permuting congruences.

PROOF. Induct on k. The result is trivial for $k = 0$. Suppose $x\ \alpha\ y\ \beta\ z$. Then by induction there are elements $u, v \in \mathbf{A}$ with $x\ [\alpha]^k\ u\ \beta\ v\ \alpha\ z$. Then, by Theorem 5.5, $x\ [\alpha]^{k+1}\ d(x, u, u)\ \beta$

$d(x,u,v)\ \alpha\ d(u,u,z) = z$, since $[\alpha]^k \leq \alpha$. The statement about solvable congruences follows immediately. If α is co-solvable then $[1]^k \leq \alpha$ for some, k. If $\beta \in \mathbf{Con\ A}$ is arbitrary, then $[\beta]^k \leq [1]^k \leq \alpha$. Hence $\beta \circ \alpha \subseteq [\beta]^k \circ \alpha \circ \beta = \alpha \circ \beta$. □

THEOREM 6.3. *The following conditions are equivalent where* $\alpha, \beta \in \mathbf{Con\ A}$.

(i) α *permutes with* β
(ii) $[\alpha]^m$ *permutes with* $[\beta]^n$ *for all* $m, n \in \omega$
(iii) $[\alpha]^m$ *permutes with* $[\beta]^n$ *for some* $m, n \in \omega$.

This theorem is due to Gumm. His proof is outlined in the exercises. He obtains various stronger results in [1983].

THEOREM 6.4. (Gumm [1981], Theorem 1.4) *Let* $\mathcal{V}$ *be a variety (or quasivariety). Then* $\mathcal{V}$ *is modular if and only if there exist terms* p *and* $q_0, \ldots, q_n$ *for some* n *such that the following are identities of* $\mathcal{V}$:

(1) $q_0(x,y,z) \approx x$,
(2) $q_i(x,y,x) \approx x$ i $\leq n$,
(3) $q_i(x,y,y) \approx q_{i+1}(x,y,y)$ for i even,
(4) $q_i(x,x,y) \approx q_{i+1}(x,x,y)$ for i odd,
(5) $q_n(x,y,y) \approx p(x,y,y)$,
(6) $p(x,x,y) \approx y$.

PROOF. First suppose that $\mathcal{V}$ is modular and let $\mathbf{A} \in \mathcal{V}$, and let $\alpha,\ \beta,\ \gamma \in \mathbf{Con\ A}$ with $x\ \alpha\ y\ \beta\ z$ and $x\ \gamma\ z$. Let $\theta = \mathrm{Cg}(x,z)$ and note that $\theta \leq \gamma \wedge (\alpha \vee \beta)$. Hence $[\theta,\theta] \leq [\gamma, \alpha \vee \beta] = [\gamma,\alpha] \vee [\gamma,\beta] \leq (\gamma \wedge \alpha) \vee (\gamma \wedge \beta)$. Thus by Theorem 5.5 $x\ (\gamma \wedge \alpha) \vee (\gamma \wedge \beta)\ d(x,z,z)$. So

$$(7) \qquad x\ (\gamma \wedge \alpha) \vee (\gamma \wedge \beta)\ d(x,z,z)\ \beta\ d(x,y,z)\ \alpha\ d(x,x,z) = z.$$

Notice that this shows that every modular variety satisfies the congruence identity $(\alpha \circ \beta) \wedge \gamma \leq ((\gamma \wedge \alpha) \vee (\gamma \wedge \beta)) \circ \beta \circ \alpha$. Now we apply this to $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x,y,z)$ with $\alpha = \mathrm{Cg}(x,y), \beta = \mathrm{Cg}(y,z)$, and $\gamma = \mathrm{Cg}(x,z)$. By (7) there are terms $q_0(x,y,z) = x, q_1(x,y,z), \ldots, q_n(x,y,z) = d(x,z,z)$ such that, in $\mathbf{F}$, $q_i(x,y,z)\ \beta\ q_{i+1}(x,y,z)$ if i is even, $q_i(x,y,z)\ \alpha\ q_{i+1}(x,y,z)$ if i is odd, and $q_i(x,y,z)\ \gamma\ q_{i+1}(x,y,z)$ for $i = 0, \ldots, n$. As in the proof of Theorem 2.1, β restricted to the subalgebra generated by x and y is trivial, and thus for i even $q_i(x,y,y)\ \beta\ q_i(x,y,z)\ \beta\ q_{i+1}(x,y,z)\ \beta\ q_{i+1}(x,y,y)$ implies that, in $\mathbf{F}$, $q_i(x,y,y) = q_{i+1}(x,y,y)$ and hence (3) holds. Similarly (2)–(4) hold. Now if we let $p(x,y,z) = d(x,y,z)$ then (1), (5), and (6) hold as well.

Now suppose that $\mathcal{V}$ has terms satisfying the equations of the theorem. We may assume that n is even since if it is odd then equations (3) and (5) imply that $q_{n-1}(x,y,y) \approx p(x,y,y)$ and thus we could omit q_n. Define terms $m_0(x,y,z,u), \ldots, m_{2n+2}(x,y,z,u)$ as follows. Set $m_0(x,y,z,u) = x$. If i is even (and $1 \leq \mathrm{i} \leq n$), set

$$m_{2i-1}(x,y,z,u) = q_i(x,y,u)$$
$$m_{2i}(x,y,z,u) = q_i(x,z,u).$$

If i is odd set

$$m_{2i-1}(x,y,z,u) = q_i(x,z,u)$$
$$m_{2i}(x,y,z,u) = q_i(x,y,u).$$

Finally let $m_{2n+1}(x,y,z,u) = p(y,z,u)$ and let $m_{2n+2}(x,y,z,u) = u$. Then it is not difficult to show that these are Day terms for $\mathcal{V}$, i.e., they satisfy the equations of Theorem 2.2. □

The proof of the above theorem is based on Lakser, Taylor and Tschantz [**59**]. The congruence identity used in the proof is due to Steve Tschantz and is actually equivalent to modularity (see the next theorem). Gumm's original proof produced a similar congruence implication.

THEOREM 6.5. *A variety $\mathcal{V}$ is modular if and only if for all $\mathbf{A} \in \mathcal{V}$ and all α, β and $\gamma \in$ **Con** $\mathbf{A}$,*

$$(\alpha \circ \beta) \wedge \gamma \leq (\gamma \wedge \alpha + \gamma \wedge \beta) \circ \beta \circ \alpha \tag{8}$$

PROOF. The proof of Theorem 6.4 showed that (8) holds if $\mathcal{V}$ is modular. If (8) holds let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x,y,z)$, and let $\alpha = \mathrm{Cg}(x,y)$, $\beta = \mathrm{Cg}(y,z)$, and $\gamma = \mathrm{Cg}(x,z)$ in **Con** $\mathbf{F}$. Since $\langle x,z\rangle$ is in the left side of (8) it is in the right. Now an argument similar to the one in Theorem 6.4 yields terms $q_0, \ldots, q_n$, p which satisfy Theorem 6.4(1)–(6). Hence $\mathcal{V}$ is modular. □

Notice that our proof of Theorem 6.4 shows that any Gumm difference term can serve as the $p(x,y,z)$ of that theorem. One of the exercises proves the converse.

Exercises

1. Prove for $\alpha, \beta \in$ **Con** $\mathbf{A}$, $k < \omega$ that

$$\alpha \circ \beta \subseteq \beta \circ \alpha \circ [\beta]^k.$$

(this can be derived directly from the inclusion of Theorem 6.2. by reversing the roles of α and β.)

2. Use Theorem 6.2. to prove for all $m, m \in \omega$

$$\alpha \circ \beta \subseteq \beta \circ [\alpha]^m \circ [\beta]^n \circ \alpha.$$

Deduce (iii) $\to$ (i) in Theorem 6.3.

3. Prove (i) $\to$ (ii) in Theorem 6.3. First show that it suffices to prove that if $\alpha, \beta \in \mathbf{Con}\ \mathbf{A}$ and α permutes with β then $[\alpha, \alpha]$ permutes with β. Suppose $x\ [\alpha, \alpha]\ y\ \beta\ z$. Then there is a $u \in \mathbf{A}$ with $x\ \beta\ u\ \alpha\ z$. Use the Shifting Lemma to show $\langle u, z\rangle \in [\alpha, \alpha] \vee (\alpha \wedge \beta)$. Now use the previous exercise to show $[\alpha, \alpha]$ and $\alpha \wedge \beta$ permute.

4. Show that if α and β are nilpotent congruences, then $\alpha \vee \beta$ is nilpotent. Conclude that if $\mathbf{Con}\ \mathbf{A}$ satisfies the ascending chain condition then $\mathbf{A}$ has a unique largest nilpotent congruence.

5. Let $\mathcal{V}$ be a modular variety an let $q_0, \ldots, q_n, p$ be terms of $\mathcal{V}$ which satisfy Theorem 6.4(1)–(6). Show that p is a Gumm difference term for $\mathcal{V}$, i.e., show that for any x, $y \in \mathbf{A} \in \mathcal{V}$, $x\ [\theta, \theta]\ p(x, y, y)$ if $x\ \theta\ y$.

6. Let $\mathcal{V}$ be a modular variety with Gumm terms $q_0, \ldots, q_n$, p (see Theorem 6.4.). Suppose that $\mathbf{A} \in \mathcal{V}$ and that a, b, c, $d \in \mathbf{A}$. We write $C(a, b, c, d)$, and say that $\langle a, b\rangle$ **centralizes** $\langle c, d\rangle$, if and only if $[\mathrm{Cg}_{\mathbf{A}}(a, b), \mathrm{Cg}_{\mathbf{A}}(c, d)] = 0_{\mathbf{A}}$. This exercise involves finding an equational characterization of this 4–ary relation, equivalently, finding a uniformly describable set of generators for the congruence $[\mathrm{Cg}_{\mathbf{A}}(a, b), \mathrm{Cg}_{\mathbf{A}}(c, d)]$. We begin by defining two other 4–ary relations.

$$H(a, b, c, d) \iff$$
$$s(a, c, \mathbf{e}) = s(a, d, \mathbf{e}) \to s(b, c, \mathbf{e}) = s(b, d, \mathbf{e})$$

for every term operation $s(x, y, \mathbf{z})$ and for all $\mathbf{e}$.

$$K(a, b, c, d) \iff$$
$$q_i(s(a, \mathbf{e}), t(c, \mathbf{f}), s(b, \mathbf{e})) = q_i(s(a, \mathbf{e}), t(d, \mathbf{f}), s(b, \mathbf{e})) \quad \text{and}$$
$$p(r(a, c, \mathbf{e}), r(b, c, \mathbf{e}), r(b, d, \mathbf{e})) = p(r(a, d, \mathbf{e}), r(b, d, \mathbf{e}), r(b, d, \mathbf{e})).$$

for all term operations $s(x, \mathbf{y})$, $t(x, \mathbf{y})$, and $r(x, y, \mathbf{z})$, for every $\mathbf{e}$ and $\mathbf{f}$, and for every $i \leq n$. Using Gumm's equations, derive these facts:

(1) $C(a,b,c,d) \to H(a,b,c,d)$.

(2) $H(a,b,c,d) \to K(a,b,c,d)$.

(3) $K(a,b,c,d) \to H(c,d,a,b)$.

(4) $H(a,b,c,d) \longleftrightarrow K(a,b,c.d)$.

(5) $H(a,b,c,d) \longleftrightarrow H(a,b,d,c)$.

(6) $H(a,a,c,d)$.

(7) $H(a,b,c,d)$ and $H(b,e,c,d) \to H(a,e,c,d)$.

(8) If f is a basic n-ary operation of $\mathbf{A}$ and if $H(a_i,b_i,c,d)$ holds for each $i < n$, then $H(u,v,c,d)$ holds, where $u = f(\mathbf{a})$ and $v = f(\mathbf{b})$.

(9) For each $\langle a,b\rangle$ the set $K(a,b) = \{\langle c,d\rangle : K(a,b,c,d)\}$ is a congruence equal to $(0_{\mathbf{A}} : \mathrm{Cg}(a,b))$.

Conclude that $C(a,b,c,d) \longleftrightarrow K(a,b,c,d)$.

7. The starting assumptions are the same as in the previous exercise. Now suppose that α and β are congruences of $\mathbf{A}$ and that either α is Abelian, or that p satisfies the other Mal'cev equation $p(x,y,y) \approx x$. Prove that $[\alpha,\beta] = 0_{\mathbf{A}}$ if and only if $p : \mathbf{D} \to \mathbf{A}$ is a homomorphism, where $\mathbf{D}$ is the subalgebra of $\mathbf{A}^3$ consisting of the elements $\langle x,y,z\rangle$ with $x \;\alpha\; y \;\beta\; z$. See Gumm's characterization of Abelian congruences, Theorem 5.7.

8. Let $\mathbf{A}$ and $\mathbf{B}$ be algebras in a modular variety and suppose that the congruences of $\mathbf{A}$ permute, and the congruences of $\mathbf{B}$ permute. Prove that the congruences of $\mathbf{A} \times \mathbf{B}$ permute.

9. Let $d(x,y,z)$ be a Gumm difference term for a modular variety $\mathcal{V}$ and define $d_1(x,y,z) = d(x,y,z)$ and

$$d_{n+1}(x,y,z) = d_n(x, d_n(x,y,y), d_n(x,y,z))$$

Show that d_n is also a difference term. Moveover, if $\langle x,y\rangle \in \theta \in \mathrm{Con}\,\mathbf{A}$, $\mathbf{A} \in \mathcal{V}$, then $d_n(x,y,y)\;[\theta]^n\; x$.

CHAPTER 7

The Center and Nilpotent Algebras

In this chapter we show how an algebra $\mathbf{A}$ may be decomposed in terms of an Abelian algebra and $\mathbf{A}/\zeta$ where ζ is the center of $\mathbf{A}$. Some easy applications of this decomposition to nilpotent loops are given in the exercises. We also investigate nilpotent algebras, showing that they have uniform and regular congruences and that associated with each nilpotent algebra is a nilpotent loop. Finally we prove a proposition which played an important role in Burris-McKenzie [**8**].

Corollary 5.9 gave the structure of Abelian algebras. We shall now describe the structure of an algebra over its center. Suppose that $\mathbf{Q}$, $\mathbf{B} \in \mathcal{V}$, $\mathbf{Q}$ is Abelian with associated group $\hat{\mathbf{Q}} = \langle Q, +, - \rangle$ (so that $d(x, y, z) = x - y + z$ for x, y, $z \in Q$) and that we are given for each basic operation symbol F_i of $\mathcal{V}$ a map $T_i : \mathbf{B}^n :\to \mathbf{Q}$ where F_i is n–ary. Write $T = (T_i, i \in I)$ for the system of maps, and define an algebra $\mathbf{A} = \mathbf{Q} \otimes^T \mathbf{B}$ by taking $\mathbf{Q} \times \mathbf{B}$ for the universe of $\mathbf{A}$ and putting

$$F_i^{\mathbf{A}}(\langle q_1, b_1 \rangle, \ldots, \langle q_n, b_n \rangle) = \langle F_i^{\mathbf{Q}}(\mathbf{q}) + T_i(\mathbf{b}), F_i^{(B)}(\mathbf{b}) \rangle$$

for $i \in I$. Notice that since $\mathbf{Q}$ is Abelian and hence affine each term F for $\mathcal{V}$ has a corresponding transfer function T so that the above equation holds. This algebra $\mathbf{Q} \otimes^T \mathbf{B}$ need not belong to $\mathcal{V}$, of course, but we have the following.

PROPOSITION 7.1. *Given $\mathbf{A} \in \mathcal{V}$, let $\mathbf{B} = \mathbf{A}/\zeta_{\mathbf{A}}$. There is an Abelian algebra $\mathbf{Q} \in \mathcal{V}$ and α system T as above so that $\mathbf{A} \cong \mathbf{Q} \otimes^T \mathbf{B}$, and furthermore*

(1) *the center of $\mathbf{Q} \otimes^T \mathbf{B}$ is the kernel of the projection onto $\mathbf{B}$;*
(2) $\mathbf{Q} = \mathbf{A}(\zeta_{\mathbf{A}})/\Delta_{\zeta_{\mathbf{A}}, 1_{\mathbf{A}}}$.

PROOF. Recall from Chapter 4 and Definition 5.1 that $\mathbf{A}(\zeta_{\mathbf{A}})$ is the center of $\mathbf{A}$ (a congruence) regarded as an algebra, and that congruence $\Delta = \Delta_{\zeta_{\mathbf{A}}, 1_{\mathbf{A}}}$ on this algebra is generated by $\{\langle \langle x, x \rangle, \langle y, y \rangle \rangle : x, y \in \mathbf{A}\}$, As in the proof of Proposition 5.7 we have

$$(1) \quad \langle x, y \rangle \equiv \langle u, v \rangle \pmod{\Delta} \quad \Leftrightarrow \quad \langle x, y \rangle \in \zeta \text{ and } v = d(y, x, y).$$

That $\mathbf{Q}$ is Abelian is proved as follows. Where η_0, η_1 are the projection kernels on $A(\zeta)$, in $\mathbf{Con}\ \mathbf{A}(\zeta)$, we have $\eta_0 \vee \Delta = \eta_1 \vee \Delta = 1$

obviously. Thus $[1,1] \subseteq \Delta \vee (\eta_0 \wedge \eta_1) = \Delta$ by additivity. Then in **Con Q**, $[1,1] = 0$ by the homomorphism property of commutator (i.e. Proposition 4.4(1)).

Now let $r \in A^A$ be a choice function for the ζ–blocks, so that $r(x)\zeta x$ and $x\ \zeta\ y$ if and only if $f(x) = r(y)$. Then we get a one-one map of $\mathbf{A}$ onto $\mathbf{Q} \times \mathbf{B}$ by defining

$$\pi(x) = \langle \langle r(x), x \rangle / \Delta,\ x/\zeta \rangle.$$

(That π is bijective follows from (1) above and Theorem 5.5). For F_1 a basic operation of $\mathcal{V}$ and $u \in \mathbf{B}^n$, say $u_j = x_j/\zeta$, put

$$T_i(u_1, \ldots, u_n) = \langle r(F_i(\mathbf{x})), F_i(r(x_1), \ldots, r(x_n)) \rangle / \Delta.$$

We can choose $0 = \langle x, x \rangle / \Delta$ as the identity element of $\hat{\mathbf{Q}}$; then we have $a + b = d(a, 0, b)$ for $a,\ b \in \mathbf{Q}$.

What remains is to show that for F_i, $\mathbf{u}$, $\mathbf{x}$ as above with say $\pi(x_j) = \langle a_j, u_j \rangle$ for $1 \leq j \leq n$, that we have

$$\pi(F_i(\mathbf{x})) = \langle F_i(\mathbf{a}) + T_i(\mathbf{u}), F_i(\mathbf{u}) \rangle.$$

This is equivalent to showing

$$\langle r(F_i(\mathbf{x})), F_i(\mathbf{x}) \rangle / \Delta = \langle F_i(\mathbf{rx}), F_i(\mathbf{x}) \rangle / \Delta + \langle r(F_i(\mathbf{x})), F_i(\mathbf{rx}) \rangle / \Delta.$$

If we use that $0 = \langle F_i(\mathbf{rx}), F_i(\mathbf{rx}) \rangle / \Delta$ and $a + b = d(a, 0, b)$, and that $d(y, z, z) = y$ when $y\ \zeta\ z$, then the computation checks out. □

COROLLARY 7.2. *An algebra in a modular variety $\mathcal{V}$ is 2–step nilpotent if and only if it can be represented as $\mathbf{Q}_0 \otimes^T \mathbf{Q}_1$ where $\mathbf{Q}_0$ and $\mathbf{Q}_1$ are Abelian algebras in $\mathcal{V}$.*

PROOF. On one hand, if $\mathbf{A}$ in Proposition 7.1 is 2–step nilpotent, then $\mathbf{B}$ is Abelian. On the other hand, if $\mathbf{A} = \mathbf{Q}_0 \otimes^T \mathbf{Q}_1 \in \mathcal{V}$ and $\mathbf{Q}_0, \mathbf{Q}_1 \in \mathcal{V}$ are Abelian, then it is clear (from Def. 5.1.) that the projection congruence η of A onto $\mathbf{Q}_1$ satisfies $\eta \leq \zeta_{\mathbf{A}}$, and true also that $[1,1] \leq \eta$ since $\mathbf{Q}_1$ is Abelian. □

The next few results give additional information about nilpotent algebras. They show nilpotency has some rather strong consequences. Exercise 7, at the end of the chapter, shows that solvable algebras do not have these properties in general. By Proposition 4.4 and Proposition 4.5 the nilpotent algebras of class k in a modular variety from a subvariety. By Theorem 6.2, if $\mathbf{A}$ is nilpotent then $\boldsymbol{V}(\mathbf{A})$ is permutable. Thus for the next few results we assume our algebras lie in a permutable variety $\mathcal{U}$ with Mal'cev term $p(x, y, z)$. Define terms $f_n(y, b, c)$ inductively by $f_0(y, b, c) = y$ and

$$f_{n+1}(y, b, c) = p(b, p(b, y, p(f_n(y, b, c), b, c)), f_n(y, b, c)).$$

The congruence $(1,1]^k$ defined in Definition 6.1. will be denoted $(1]_k$. $\mathbf{A}$ is nilpotent if only if $(1]_k = 0$ for some k. The next lemma shows that the function $x \mapsto f_n(x,b,c)$ is the inverse to the function $x \mapsto p(x,b,c)$ if $\mathbf{A}$ is nilpotent of class n.

LEMMA 7.3. *If $\mathbf{A} \in \mathcal{U}$ and x, y, b, $c \in \mathbf{A}$ the for all n*

$$f_n(p(x,b,c),b,c)\ (1]_n\ x.$$

and

$$p(f_n(y,b,c),b,c)\ (1]_n\ y.$$

PROOF. We prove the second relation: the proof of the first is similar but easier. Induct on n. Since $(1]_0 = 1$ the result is trivial for $n = 0$. Let $y' = p(f_n(y,b,c),b,c)$. By induction $y'(1]_n y$. In the algebra $\mathbf{A}/(1]_{n+1}$, $(1]_n$ is contained in the center. Hence by Theorem 5.7 (since $b = p(b,y,y)\ (1]_n\ p(b,y,y')$)

$$\begin{aligned} p(f_{n+1}(y,b,c),b,c) &= p((p(b,p(b,y,y'),f_n(y,b,c)),b,c) \\ &= p(p(b,p(b,y,y'),f_n(y,b,c)),p(b,b,b),p(b,b,c)) \\ &\equiv p(p(b,b,b),p((p(b,y,y'),b,b),p(f_n(y,b,c),b,c)) \pmod{(1]_{n+1}} \\ &= p(b,p(b,y,y'),y'). \end{aligned}$$

Thus $p(f_{n+1}(y,b,c),b,c)\ (1]_{n+1}\ p((b,p(b,y,y'),y')$. The following matrix lies in $M((1]_n,1)$ (see Definition 3.2).

$$\begin{bmatrix} p(b,p(b,y,y'),y') & p(b,p(b,b,y'),y') \\ p(b,p(b,y,y),y) & p(b,p(b,b,y),y) \end{bmatrix} = \begin{bmatrix} p(b,p(b,y,y'),y') & b \\ y & b \end{bmatrix}$$

Hence

$$y\ (1]_{n+1}\ p(b,p(b,y,y'),y')\ (1]_{n+1}\ p(f_{n+1}(y,b,c),b,c).$$

□

COROLLARY 7.4. *If $\mathbf{A} \in \mathcal{U}$ is nilpotent and $b,c \in A$ then the function $x \mapsto p(x,b,c)$ is on-one and onto. Moreover if $\theta \in \mathbf{Con}\ \mathbf{A}$ then this function, restricted to b/θ, is a bijection from b/θ to c/θ.*

PROOF. The first statement is clear from Lemma 7.3. If f denotes the restricted function then f is clearly one-one and if $x \in b/\theta$ then $f(x) \in c/\theta$. Since $\mathbf{A}/\theta$ is also nilpotent the function, $x \mapsto p(x,b,c)$ induces a permutation of the θ–blocks. Hence the inverse images of every element of c/θ under this function lie in b/θ. Since $x \mapsto p(x,b,c)$ is onto it follows that f is also. □

COROLLARY 7.5. *If $\mathbf{A}$ is nilpotent then $\mathbf{A}$ has uniform congruences (i.e., all the blocks of any congruence θ have the same size).* □

LEMMA 7.6. *If* $\mathbf{A} \in \mathcal{U}$ *is nilpotent and* a, b, $c \in \mathbf{A}$ *then*

$$\mathrm{Cg}(a, b) = \mathrm{Cg}(p(a, b, c), c)$$

PROOF. Suppose $(1]_n = 0$ in $\mathbf{A}$. Then $p(f_n(c, b, c), b, c) = c = p(b, b, c)$. Hence $f_n(c, b, c) = b$. Now let $\psi = \mathrm{Cg}(p(a, b, c), c)$. Clearly $\psi \leq \mathrm{Cg}(a, b)$. But $p(a, b, c)\ \psi\ c$ implies $a = f_n(p(a, b, c), b, c)\ \psi\ f_n(c, b, c) = b$. □

COROLLARY 7.7. *If* $\mathbf{A}$ *is nilpotent then* $\mathbf{A}$ *has regular congruences, i.e., if two congruences have a block in common, they are equal.* □

In Chapter 5 we saw that Abelian algebras were closely connected with Abelian groups. Nilpotent algebras have a close connection with nilpotent loops. For suppose $\mathbf{A} \in \mathcal{U}$ is nilpotent. Let 0 be an arbitrary element of $\mathbf{A}$ and define $x + y = p(x, 0, y)$. Then by Corollary 7.4. this defines a loop with null element 0. Moreover by Lemma 7.3. the left and right division operations (perhaps we should call them subtraction operations) are also polynomials on $\mathbf{A}$. Also note that by Theorem 5.7 if $a\ \zeta\ 0$ and x, $y \in \mathbf{A}$ then $a + x = x + a$, $a + (x + y) = (a + x) + y$, and $(x + a) + y = x + (a + y)$.

In Exercise 7 we show how to construct solvable algebras in which the properties above fail.

PROPOSITION 7.8. *Let* $\mathbf{B}$ *be subdirectly irreducible with* $0_{\mathbf{B}} < \zeta_{\mathbf{B}}$, *and let* $\mathbf{B}' = \mathbf{B}^2/\Delta_{1,\zeta}$. *Then* $\mathbf{B}'$ *is subdirectly irreducible and*

$$\mathbf{B}'/\zeta_{B'}, \cong (B/\zeta_B)^2.$$

PROOF. We write Δ for $\Delta_{1,\zeta}$ and us the notation for congruences on $\mathbf{B}^2$ introduced before Theorem 4.11. Let β be the monolith of $\mathbf{B}$ (smallest nonzero congruence). So we have $\beta \leq \zeta$, and $\Delta + \eta_i = \zeta_i$, $\Delta \cdot \eta_i = 0$, $(i = 0, 1)$ by 4.11. We claim first that $(\beta_0 \wedge \beta_1) \vee \Delta$ *is the unique smallest congruence of* $\mathbf{B}^2$ *strictly above* Δ.

To see it, first $0 \neq \beta_0 \wedge \eta_1 \leq \beta_0 \wedge \beta_1$, $\Delta \wedge \eta_1 = 0$, so $\beta_0 \wedge \beta_1 \not\leq \Delta$. Suppose that $\lambda > \Delta$ in $\mathbf{Con}\ \mathbf{B}^2$. Notice that β_1 is the unique atom in $1/\eta_1 \cong \mathbf{Con}\ \mathbf{B}$, hence since $1/\eta_1$ transposes down onto $\eta_0/0$, $\eta_0 \wedge \beta_1$ is the unique atom below η_0. Likewise for $\beta_0 \wedge \eta_1$ below η_1. Now $\Delta \vee (\beta_0 \wedge \eta_1) \geq \eta_0 \wedge \beta_1$ because choosing $\langle x, y\rangle \in \beta - 0_{\mathbf{B}}$, we have $\langle x, x\rangle \Delta \langle y, y\rangle \beta_0 \wedge \eta_1 \langle x, y\rangle$, and hence $(\Delta \vee (\beta_0 \wedge \eta_1)) \wedge \eta_0 \neq 0$, so it contains $\eta_0 \wedge \beta_1$. Thus if $\lambda \wedge \eta_1 \neq 0$, then $\lambda \geq \beta_0 \wedge \eta_1$ and also $\lambda > \Delta$, so $\lambda \geq \beta_0 \cdot \beta_1$. Symmetrically, we are finished with the proof of the claim unless $\lambda \wedge \eta_0 = \lambda \wedge \eta_1 = 0$. This assumption leads to a contradiction: by modularity, $\lambda \vee \eta_0 = \chi_0$ for some $\chi > \zeta$ (else η_0 is a common complement of λ and Δ in $\zeta_0/0$). $[\chi_0, 1] = [\chi, 1]_0 \wedge [1, 1]_1$ by Proposition 4.5. Also $[\chi_0, 1] = [\lambda \vee \eta_0, \eta_1 \vee \eta_0] \leq \eta_0 \vee (\lambda \wedge \eta_1) = \eta_0$ by

additivity of commutator. The two equalities for $[\chi_0, 1]$ yield $[\chi, 1] = 0$, implying $\chi \leq \zeta$, a contradiction.

Next we claim that $\zeta_0 \wedge \zeta_1 = \zeta'$ *is the largest* $\gamma \in$ **Con** $\mathbf{B}^2$ *satisfying* $[\gamma, 1] \leq \Delta$.

First, $[\zeta', 1] = 0$ follows from Proposition 4.5 (in fact ζ' is the center of $\mathbf{B}^2$). Second, suppose that $\gamma \in$ **Con** $\mathbf{B}^2$, $[\gamma, 1] \leq \Delta$. Then $[\gamma, 1] = [\gamma, \eta_0 \vee \eta_1] \leq \eta_0 \vee [\gamma, \eta_1]$ and $[\gamma, \eta_1] \leq [\gamma, 1] \wedge \eta_1 \leq \Delta \wedge \eta_1 = 0$. Thus $[\gamma, 1] \leq \eta_0$. Similarly with subscripts interchanged, so $[\gamma, 1] = 0$. By (4.40 applied to the first projection homomorphism, $\gamma \leq \zeta_0$, similarly $\gamma \leq \zeta_1$. Thus the second claim is proved.

The first claim tells us that $\mathbf{B}'$ is subdirectly irreducible and the second tells us that $\zeta_0 \wedge \zeta_1 \geq \Delta$ projects onto the center of $\mathbf{B}'$. Thus $\mathbf{B}'/\zeta_{\mathbf{B}'} \cong \mathbf{B}^2/(\zeta_0 \wedge \zeta_1) \cong (\mathbf{B}/\zeta)^2$ obviously. □

This proposition was in the first draft manuscript of Freese-McKenzie[**29**], and later deleted. A much stronger result was proved by the same method. Let $\mathbf{B}$ be subdirectly irreducible with monolith β, and let $\gamma = (0 : \beta)$ be the centralizer of β, and let σ be the centralizer of γ. Suppose that $\beta \leq \sigma < \gamma$. Then the algebra $\mathbf{B}' = \mathbf{B}(\gamma)/\Delta_{\gamma,\sigma}$ can be proved to be subdirectly irreducible, and we have $\beta, \leq \sigma' < \gamma'$ where these congruences are defined for $\mathbf{B}'$ as for $\mathbf{B}$. From here, the unpublished argument showed that $\mathbf{B}''$ is isomorphic to a proper essential extension of $\mathbf{B}'$. This construction was iterated through the transfinite to build a tower $\mathbf{B}^{(\alpha)}$, α an ordinal, of subdirectly irreducible algebras. The argument was motivated by Herrmann's original proof of the fundamental theorem of Abelian algebras.

Corollaries 7.5 and 7.7 are due to C. Bergman. The fact that the inverse to the function $x \mapsto p(x, b, c)$ is a polynomial function in a nilpotent variety is new.

Exercises

1. It is well known that if $\mathbf{G}$ is a non-Abelian group then $\mathbf{G}/\mathbf{Z}$ is not cyclic. Use Proposition 7.2 to construct a nilpotent loop $\mathbf{L}$ of order 9 with $\mathbf{L}/\zeta \cong \mathbf{Z}/3$.

2. Show that a nilpotent (in fact any) loop with four elements is an Abelian group.

3. Show that if $\mathbf{A}$ is nilpotent and $\theta > 0$ in **Con** $\mathbf{A}$ then $\theta \wedge \zeta > 0$.

4. Show that if $\mathbf{A}$ is a finite nilpotent algebra and $\mathbf{B}$ is a subalgebra of $\mathbf{A}$, then $|B|$ divides $|A|$.

5. Let $\mathbf{A}$ be a nilpotent loop such that $|A| = p^2$, p a prime, and $|\mathbf{A}/\zeta| = p$. Show that $\mathbf{A}$ is one-generated (but it is not necessarily a cyclic group).

6. $\mathcal{U}$, p, f_n are defined before Lemma 7.3. Prove that $q(x, y, z) = f_n(x, z, y)$ is a Mal'cev term for any n–step nilpotent algebra in $\mathcal{U}$.

7. Let $\mathbf{G}$ and $\mathbf{H}$ be Abelian groups and let $\mathbf{A}$ be their disjoint union. Define a ternary operation $p(x, y, z)$ on $\mathbf{A}$ as follows. If x, y and z all lie in one of the groups, let $p(x, y, z) = x - y + z$. Otherwise two of x, y and z lie in one group and the other lies in the other group. In this case $p(x, y, z)$ is the one that is alone. Show $\boldsymbol{V}(\mathbf{A})$ is permutable and $\mathbf{A}$ is solvable. Use this to show the results Lemma 7.3–Corollary 7.7 cannot be extended to solvable algebras.

8. Prove the first relation in Lemma 7.3.

9. Show that if $\mathbf{A}$ and all its homomorphic images have uniform congruences then $\mathbf{A}$ has regular congruences (see Corollary 7.7).

CHAPTER 8

Congruence Identities

If an equation ε of the language of lattices holds in **Con A** for every $\mathbf{A} \in \mathcal{V}$ (where $\mathcal{V}$ is a variety) then we write $\mathcal{V} \models_{\text{con}} \varepsilon$, and say that ε is a **congruence identity** of $\mathcal{V}$. The most important congruence identities are the modular law and the distributive law (and of course this whole book is about the consequences of congruence modularity). In the early 1970's it was conjectured that possibly any nontrivial lattice law holding as a congruence identity of a variety must imply congruence modularity. The conjecture turned out to be false (Polin [**74**], see also Day-Freese [**23**]). In other words, there exist nonmodular varieties having nontrival congruence identities. As for the possible diversity of such identities, and their consequences for the structure of the algebras in a variety, our understanding is still very limited. There is an excellent survey article on this topic in the appendix to Grätzer [**34**], written by B. Jónsson. (On this topic, see also Example 11.2. and the entirety of Chapter 13.)

Recent studies of modular varieties have revealed that many popular properties of a variety are intimately connected with commutator identities for the congruences. For example, we shall see in Chapter 10, Section 3 that a residually small modular variety must satisfy $\alpha \wedge [\beta, \beta] = [\alpha \wedge \beta, \beta]$ (for congruences α and β in any algebra of the variety), and that this equation is also sufficient for residual smallness if the variety is generated by a finite algebra.

In this chapter we shall consider three special equations very much like the example above, as well as familiar equations like the nilpotency and solvability laws. These equations are not written in the pure language of lattices, but rather are equations in the language of algebras $\langle L, x \wedge y, x \vee y, [x, y], 0, 1\rangle$ which are lattices with 0 and 1 and an additional binary operation $[x, y]$. As usual, all varieties encountered are assumed to be modular and all algebras belong to modular varieties, so these equations can be evaluated in the congruence lattices. For an equation ε of this kind we shall write $\mathcal{V} \models_{\text{con}} \varepsilon$ with just the same

meaning as above, and we shall consider the equation as a possible congruence identity of a variety. Equations involving only lattice $\vee$ and $\wedge$, with no commutators, will be called pure lattice equations.

A systematic theory of congruence identities including the commutator does not exist at this time. Our aim here is to survey some of the interesting results that have been discovered, and stimulate the reader to think about the subject. All of the equations we shall discuss are listed below.

$$x \wedge [y, y] \approx [x \wedge y, y] \tag{C1}$$

$$[x, y] \approx x \wedge y \wedge [1, 1] \tag{C2}$$

$$[x, y] \approx x \wedge y \tag{C3}$$

$$[x, y] \approx 0 \tag{C4}$$

$$[1, 1] \approx 0 \tag{C5}$$

$$1, [1, 1]] \approx 0 \tag{C6}$$

$$[[1, 1], [1, 1]] \approx 0 \tag{C7}$$

$$[x, 1] \approx x \tag{C8}$$

For each of these equations, the property $\mathbf{Con}\ \mathbf{A} \models \varepsilon$ is preserved under the formation of quotient algebras and the formation of finite subdirect products. We shall prove this fact for (C1) (Theorem 8.1) and the reader can easily discover the proofs for the other equations. (C4) - (C7) are preserved under the formation of subalgebras and products of any length, while each of the other equations falls to possess either one of these preservation properties. Thus a variety generated by algebras whose congruence lattices satisfy (Ci), ($i \in \{4, 5, 6, 7\}$) obeys (Ci) as a congruence identity. It can be shown, for each of the equations (C1)–(C8), that a directed union of algebras whose congruences obey the equation must itself have this property.

Equations (C4) and (C5) are equivalent for any algebra, and define the class of Abelian algebras. A variety satisfying (C4) is called Abelian. (C6) defines the two step nilpotent algebras. (See Corollary 7.2 for the structure of these algebras.) An equally obvious equation defines the n step nilpotent algebras. For a given modular variety $\mathcal{V}$, there exists a set E_n of equations in the language of $\mathcal{V}$ such that an algebra $\mathbf{A}$ is n step nilpotent if and only if $\mathbf{A} \models E_n$. (This result

is due to Gumm; see Theorem 14.2.) (C7) defines the two step solvable algebras. The n step solvable algebras within a given variety also constitute a subvariety. We may remark that the (ordinary) equations defining this subvariety are much more difficult to construct than the equations for nilpotency.

Equation (C3) defines the class of congruence distributive varieties. The proof is easy (see Exercise 1). An algebra $\mathbf{A}$ such that $\mathbf{Con\ A} \models$ (C3) is called **neutral**. From the fact that finite subdirect products and quotients of neutral algebras are neutral, it follows easily that the join of two distributive subvarieties of a modular variety is distributive (a result of Hagemann and Herrmann, see Exercise 2). This in turn implies that a locally finite modular variety $\mathcal{V}$ has a largest distributive subvariety. To see this, let $\mathcal{W} = \bigvee_{i\in I} \mathcal{V}_i$ where $\mathcal{V}_i (i \in I)$ are the distributive subvarieties of $\mathcal{V}$. Then $\mathbf{F}_{\mathcal{W}}(3)$ is finite (a quotient of $\mathbf{F}_{\mathcal{V}}(3)$) and is a subdirect product of the $\mathbf{F}_{\mathcal{V}_i}(3)$. Hence it is a finite subdirect product of these algebras, and is neutral. This implies that $\mathbf{Con\ F}_{\mathcal{V}}(3)$ is distributive (see Exercise 1), and so $\mathcal{V}$ is distributive by Jónsonn's Theorem 2.1. An example showing that modularity is a necessary assumption for this result can be found in Chapter 11. The variety of rings is an example of a (nonlocally finite) modular variety having no largest distributive subvariety.

Equations (C1), (C2), and (C8) are rather different in their implications from the other equations. Let us consider first (C1). This equation implies the equation $[x,[x,x]] \approx [x,x]$. Therefore. in a variety with this congruence identity, every nilpotent algebra is Abelian, and every nilpotent congruence is Abelian. It is known that a locally finite variety of groups, or of rings, satisfies (C1) if and only if every nilpotent algebra in the variety is Abelian. An algebra whose congruences obey (C1) has a largest Abelian congruences. (See Exercise 5.)

Consider an algebra $\mathbf{A}$ such that $\mathbf{L} = \mathbf{Con\ A}$ satisfies (C1). For any $\beta \in \mathbf{L}$ define a mapping of $\mathbf{L}$ into $\mathbf{L}$ by taking $f_\beta(x) = [x,\beta]$. Then $f_\beta(\beta) = [\beta,\beta]$ is a fixed point for f_β as we observed above. In fact, (C1) implies that $f_\beta(x) = x$ for all $x \leq f_\beta(\beta)$. This property of the fixed points of f_β (holding for all β) is equivalent to (C1). Also each of the equations

$$[x,y] \approx (x \wedge [y,y]) \vee (y \wedge [x,x])$$

$$[x,y] \approx x \wedge y \wedge [x \vee y, x \vee y]$$

is equivalent to (C1). Thus if $\mathbf{L} = \mathbf{Con\ A}$ satisfies (C1) then the commutator in $\mathbf{L}$ is determined by the unary operation $f(x) = [x,x]$ and the lattice operations.

It is not hard to show that (C1) implies (for congruence lattices in a modular variety) the equation

$$([1,1] \wedge x) \vee ([1,1] \wedge y) \approx [1,1] \wedge (x \vee y).$$

which with the aid of the modular law implies

$$([1,1] \vee x) \wedge ([1,1] \vee y) \approx [1,1] \vee (x \wedge y).$$

The two displayed equations are actually equivalent in modular lattices; either of them signifies that [1,1] is a neutral element. In the same vein. If $\mathbf{L} = \mathbf{Con}\ \mathbf{A}$ satisfies (C1) and $\beta \in \mathbf{L}$ then $[\beta, \beta]$ is a neutral element in the interval lattice $\beta/0_{\mathbf{A}}$. Using these facts, A. Day and E. Kiss [**22**] prove that if a locally finite nondistributive variety $\mathcal{V}$ has (C1) as congruence identity, then the pure congruence identities (lattice equations) of $\mathcal{V}$ are the same as the pure congruence identities possessed by the variety of modules over the ring of the maximal Abelian subvariety of $\mathcal{V}$. (See Chapter 9 for the definition of this ring.)

We say that an algebra $\mathbf{A}$ satisfies a commutator equation hereditarily if the equation holds in the congruence lattice of every subalgebra of $\mathbf{A}$. The next result was proved in the paper of R. Freese and R. McKenzie [**29**].

THEOREM 8.1. *The equation* (C1) *is equivalent to the implication* $x \leq [y,y] \to x = [x,y]$. *Moreover, the class of algebras which satisfy* (C1) *hereditarily is closed under the formation of quotient algebras, subalgebras, and finite direct products.*

PROOF. First suppose that the implication holds. Clearly $x \wedge [y,y] \leq [y,y]$. Thus using the implication with x as $x \wedge [y,y]$ we obtain $x \wedge [y,y] = [x \wedge [y,y], y] \leq [x \wedge y, y] \leq x \wedge [y,y]$. Thus (C1) holds. Conversely if $x \leq [y,y]$, then (C1) gives $x = x \wedge [y,y] = [x \wedge y, y] = [x,y]$.

Now for the second statement. For subalgebras, the proof is trivial. For quotient algebras, let $\mathbf{A}$ satisfy (C1) hereditarily and $\mathbf{C} \leq \mathbf{A}/\theta$ for some $\theta \in \mathbf{Con}\ \mathbf{A}$. Then $\mathbf{C} = \mathbf{B}/\gamma$ where $\mathbf{B} \leq \mathbf{A}$. If (C1) fails for $\mathbf{C}$ then there are $\mu, \nu \in \mathbf{Con}\ \mathbf{B}$, $\mu, \nu \geq \gamma$, satisfying (by Remarks 4.6) $\nu \leq [\mu,\mu]_\gamma = [\mu,\mu] \vee \gamma$ while $[\nu,\mu]_\gamma = [\nu,\mu] \vee \gamma < \nu$. Then $\nu \leq \mu$ and $[\nu,\ \mu] \not\geq [\mu,\mu] \wedge \nu$, else $[\nu,\mu] \vee \gamma \geq ([\mu,\mu] \wedge \nu) \vee \gamma \geq \nu$ by modularity. Thus (C1) fails in $\mathbf{Con}\ \mathbf{B}$, a contradiction.

For products, suppose that $\mathbf{C} = \mathbf{A} \times \mathbf{B}$ where $\mathbf{A}$, $\mathbf{B}$ satisfy (C1) hereditarily, and $\mathbf{D} \leq \mathbf{C}$. We can clearly assume that the projections map $\mathbf{D}$ onto $\mathbf{A}$ and $\mathbf{B}$, i.e. $p_0(\mathbf{D}) = \mathbf{A}, p_1(\mathbf{D}) = \mathbf{B}$. Let $\eta_1 = kerp_i (i = 0, 1)$. Now suppose that $\sigma, \mu \in \mathbf{Con}\ \mathbf{D}$ and $\nu = \sigma \wedge [\mu,\mu]$. We shall show that $\nu \leq [\nu,\mu]$ (which implies $\sigma \wedge [\mu,\mu] = [\sigma \wedge \mu, \mu]$) . Since $\nu \leq [\mu,\mu]$ we have $\nu \vee \eta_0 \leq [\mu \vee \eta_0, \mu \vee \eta_0]_{\eta_0}$. Since $\mathbf{A}$ satisfies (C1),

then

$$\nu \vee \eta_0 = [\nu \vee \eta_0, \mu \vee \eta_0]\eta_0 = [\nu, \mu] \vee \eta_0.$$

Thus $\nu = \nu \wedge ([\nu, \mu] \vee \eta_0) = [\nu, \mu] \vee (\eta_0 \wedge \nu)$. Likewise $\nu = [\nu, \mu] \vee (\eta_1 \wedge \nu)$.

In just the same way we can show that

$$(\eta_1 \wedge \nu) \vee \eta_0 = [(\eta_1 \wedge \nu) \vee \eta_0, \mu \vee \eta_0]_{\eta_0}$$

and

$$\eta_1 \wedge \nu \leq [\eta_1 \wedge \nu, \mu] \vee \eta_0.$$

Thus $\eta_1 \wedge \nu = [\eta_1 \wedge \nu, \mu] \vee (\eta_0 \wedge \eta_1 \wedge \nu) = [\eta_1 \wedge \nu, \mu]$. Therefore

$$\nu = [\nu, \mu] \vee (\eta_1 \wedge \nu) = [\nu, \mu] \vee [\eta_1 \wedge \nu, \mu] = [\nu, \mu].$$

□

The second statement in Theorem 8.1 holds for each of the equations (C1) - (C8). The proofs are quite similar to the one above.

We turn now to consider (C2). This equation clearly implies (C1): moreover it is rather directly implied by each of the equations (C3) and (C4). The next theorem will yield the conclusion (which is Exercise 6) that any congruence equation implied both by (C3) and (C4) is implied also by (C2).

THEOREM 8.2. *The congruence lattice of an algebra satisfies one of the following if and only if it satisfies all.*

$$[x, y] \approx x \wedge y \wedge [1, 1] \tag{1}$$

$$[x, x] \approx x \wedge [1, 1] \tag{2}$$

$$[x, y] \approx [x, 1] \wedge y \tag{3}$$

$$[x \wedge y, z] \approx x \wedge [y, z] \tag{4}$$

$$x \leq [1, 1] \to [x, x] = x \tag{5}$$

PROOF. Using the commutative law of the commutator and other basic properties of commutators, one easily shows that (1) implies each of (2), (3), (4) and that each of these equations implies (5). We shall now prove that (5) implies (1). Suppose that (5) holds in **Con A** and let congruences α and β be given. That $[\alpha, \beta] \leq \alpha \wedge \beta \wedge [1, 1]$ is clear. Let $\sigma = \alpha \wedge \beta \wedge [1, 1]$. Thus $\sigma = [\sigma, \sigma]$ by (5), and it's clear that $[\sigma, \sigma] \leq [\alpha, \beta]$. Thus we conclude that (1) holds. □

THEOREM 8.3. *A variety $\mathcal{V}$ has* (C2) *as congruence identity if and only if every non-Abelian subdirectly irreducible algebra in $\mathcal{V}$ has a non-Abelian monolith.*

PROOF. In one direction (necessity of the condition) this is immediate from the last theorem (the equivalence of (1) and (5)). For the converse (sufficiency of the condition), assume that $\mathcal{V}$ does not satisfy (C2). Then we can choose $\mathbf{A} \in \mathcal{V}$ and a congruence λ of $\mathbf{A}$ such that $[\lambda, \lambda] < \lambda \leq [1, 1]$ (by the previous theorem). There exists a congruence σ such that $[\lambda, \lambda] \leq \sigma, \lambda \not\leq \sigma$, and $\mathbf{A}/\sigma$ is subdirectly irreducible. Let $\hat{\sigma} > \sigma$ be the congruence corresponding to the monolith of $\mathbf{A}/\sigma$. Then $\lambda \vee \sigma \geq \hat{\sigma}$, so that

$$[\hat{\sigma}, \hat{\sigma}] \leq [\lambda, \lambda] \vee \sigma \leq \sigma,$$

implying that the monolith of $\mathbf{A}/\sigma$ is Abelian. (See Proposition 4.4.) Since $[1, 1] \not\leq \sigma$, we also have that $\mathbf{A}/\sigma$ is non-Abelian. □

A congruence β of an algebra is called prime if and only if $\beta \geq [\sigma, \gamma]$ always implies $\beta \geq \sigma$ or $\beta \geq \gamma$. An algebra is called prime if and only if the commutator of any two of its non-zero congruences is non-zero. Theorem 8.3 says that a variety satisfies (C2) if and only if its subdirectly irreducible algebras are Abelian or prime. It is known that a locally finite variety of groups having this property must be Abelian. However, quite a few well studied properties of varieties are known to imply (C2). The equation arose first in the investigation of locally finite varieties with decidable first order theory (in Burris-McKenzie [**8**]). All such decidable varieties satisfy (C2). Semi-simple varieties (in which the subdirectly irreducible algebras are simple) obviously satisfy (C2). (It follows from Theorem 8.3).

An algebra $\mathbf{A}$ is said to have the congruence extension property if and only if for every subalgebra $\mathbf{B} \leq \mathbf{A}$ and congruence β on $\mathbf{B}$, there is a congruence α on $\mathbf{A}$ for which $\alpha|_B = \beta$. A variety has the congruence extension property if all of its algebras have the property. E.Kiss [**55**] has proved that every modular variety with the congruence extension property satisfies (C2). Our next theorem (and Theorem 8.2) are due to him.

THEOREM 8.4. *Suppose that* $\mathbf{A} \times \mathbf{A}$ *has the congruence extension property. Then* $\mathbf{Con}\ \mathbf{A} \models$ (C2). *Moreover, if* $\alpha, \beta \in \mathbf{Con}\ \mathbf{A}$ *and* $\mathbf{B} \leq \mathbf{A}$ *the* $[\alpha|_{\mathbf{B}}, \beta|_B] = [\alpha, \beta]|_{\mathbf{B}}$.

PROOF. We assume throughout the argument that $\mathbf{A}^2$ has the congruence extension property. To prove that (C2) holds, we use the equivalent from (3) from Theorem 8.2. Let $\alpha, \beta \in \mathbf{Con}\ \mathbf{A}$. We are to show that $[\alpha, \beta] \supseteq [\alpha, 1] \wedge \beta$. Let $\Delta_{\beta,\alpha}$ be the congruence on $\mathbf{A}(\beta)$, and $\Delta_{1,\alpha}$ be the congruence on $\mathbf{A}^2$, defined in Definition 4.7. These congruences are generated in the respective algebras by the same set. Thus since $\mathbf{A}^2$ has the congruence extension property, it follows that $\Delta_{1,\alpha}|_{\mathbf{A}(\beta)} = \Delta_{\beta,\alpha}$.

Now suppose that $\langle x, y\rangle \in [\alpha, 1] \wedge \beta$. We can employ Theorem 4.9. We have that $\langle x, y\rangle, \langle x, x\rangle \in \mathbf{A}(\beta)$ and $\langle x, y\rangle \equiv \langle x, x\rangle \pmod{\Delta_{1,\alpha}}$. Therefore $\langle x, y\rangle \equiv \langle x, x\rangle \pmod{\Delta_{\beta,\alpha}}$, implying that $\langle x, y\rangle \in [\alpha, \beta]$ as desired.

To prove the other commutator property (restriction of commutators), let α and β be as before, and let $\mathbf{B} \leq \mathbf{A}$. We first observe that our hypothesis implies that $\mathbf{B}^2$ has the congruence extension property, and thus by what was proved, the congruences in $\mathbf{B}$ satisfy (C2). Using (C2) in both algebras, we see that it will suffice to prove the restriction property in the case $\alpha = 1_{\mathbf{A}} = \beta$: i.e. to prove that $[1_{\mathbf{A}}, 1_{\mathbf{A}}]|_{\mathbf{B}} = [1_{\mathbf{B}}, 1_{\mathbf{B}}]$. Let λ be the congruence on $\mathbf{A}$ generated by the set $1_{\mathbf{B}}$. Clearly

$$\Delta_{1_{\mathbf{A}},\lambda} = \mathrm{Cg}_{\mathbf{A}^2}(\Delta_{1_{\mathbf{B}},1_{\mathbf{B}}}).$$

Thus

$$\Delta_{1_{\mathbf{B}},1_{\mathbf{B}}} = \Delta_{1_{\mathbf{A}},\lambda}|_{\mathbf{B}^2}$$

implying that

$$[1_{\mathbf{A}}, \lambda]|_{\mathbf{B}} = [1_{\mathbf{B}}, 1_{\mathbf{B}}].$$

Now using (C2) for $\mathbf{A}$ and the fact that $\lambda \geq 1_{\mathbf{B}}$ we get the desired equation $[1_{\mathbf{A}}, 1_{\mathbf{A}}]|_{\mathbf{B}} = [1_{\mathbf{B}}, 1_{\mathbf{B}}]$. □

Several of the useful properties possessed by the commutator in every modular variety can be written as congruence identities, namely

$$[x, y] \approx [y, x] \approx x \wedge y \wedge [x, y].$$

and

$$[x, y \vee z] \approx [x, y] \vee [x, z].$$

Although (C3) is a congruence identity of every distributive variety, it is easy to show that it cannot be derived from the basic equations above and the equations defining distributive lattices in the same way we proved Theorem 8.2 (using only the machinery of equational logic). Likewise, (C8) is equivalent for varieties to the equation $[1, 1] \approx 1$; and this equivalence is a theorem not of equational logic, but of commutator theory.

THEOREM 8.5. *The following are equivalent for a variety* $\mathcal{V}$.

1. $\mathcal{V} \models_{\mathrm{con}} [x, 1] \approx x$.
2. $\mathcal{V} \models_{\mathrm{con}} [1, 1] \approx 1$.
3. $\mathcal{V}$ *does not possess nontrivial Abelian algebras.*
4. *Every algebra* $\mathbf{A} \in \mathcal{V}$ *is centerless, i.e.,* $\zeta_{\mathbf{A}} = 0_{\mathbf{A}}$.
5. *If* $\mathbf{A}, \mathbf{B} \in \mathcal{V}$, *then* $\mathbf{Con}(\mathbf{A} \times \mathbf{B}) \cong \mathbf{Con}\ \mathbf{A} \times \mathbf{Con}\ \mathbf{B}$ *naturally.*

PROOF. The equivalences (1) $\iff$ (4) and (2) $\iff$ (3) are immediate. Moreover (4) $\Rightarrow$ (3) is trivial. The (surprising) implication (3)

$\Rightarrow$ (4) is by Proposition 7.1. Thus (1)–(4) are seen to be mutually equivalent.

Next we show that (5) $\Rightarrow$ (1). Suppose that we have $\mathbf{A} \in \mathcal{V}$ and $\beta \in \mathbf{Con}\ \mathbf{A}$ and (5) holds. The meaning of (5) is that every congruence of $\mathbf{A}^2$ should be of the form $\gamma_0 \wedge \delta_1$, where γ and δ are congruences of $\mathbf{A}$ and $\langle x, y\rangle \equiv \langle u, v\rangle \pmod{\gamma_0}$ if and only if $\langle x, u\rangle \in \gamma$, and $\langle x, y\rangle \equiv \langle u, v\rangle \pmod{\delta_1}$ if and only if $\langle y, v\rangle \in \delta$. Now suppose that $\Delta_{1_\mathbf{A},\beta} = \gamma_0 \wedge \delta_1$. Since $\langle x, x\rangle\ \Delta_{1_\mathbf{A},\beta}\ \langle y, y\rangle$ whenever $\langle x, y\rangle \in \beta$ it follows that $\beta \leq \gamma \wedge \delta$. But now $\beta_0 \wedge \beta_1 \leq \gamma_0 \wedge \delta_1 = \delta_{1_\mathbf{A},\beta}$. This certainly implies that $[\beta, 1_\mathbf{A}] = [1_\mathbf{A}, \beta] = \beta$ by Theorem 4.9.

We conclude the proof by showing that (1) $\Rightarrow$ (5). Suppose that (1) holds and that $\theta \in \mathbf{Con}(\mathbf{A} \times \mathbf{B})$ with $\mathbf{A}, \mathbf{B} \in \mathcal{V}$. We write η_0, η_1 for the kernels of the projection homomorphisms. It will suffice to show that $\theta = \bar{\theta}$ where $\bar{\theta} = (\eta_0 \vee \theta) \wedge (\eta_1 \vee \theta)$. Now

$$[1, \bar{\theta}] \leq [\eta_0 \vee \eta_1, \eta_0 \vee \theta] \leq \eta_0 \vee (\eta_1 \wedge \theta).$$

and similarly $[1, \bar{\theta}] \leq \eta_1 \vee (\eta_0 \wedge \theta)$. Thus

$$\bar{\theta} = [1, \bar{\theta}] \leq (\eta_0 \vee (\eta_1 \wedge \theta)) \wedge (\eta_1 \vee (\eta_0 \wedge \theta)) \leq \theta$$

by two applications of the modular law and the fact that $\eta_0 \wedge \eta_1 \leq \theta$. $\square$

REMARK 8.6. It is an immediate consequence of the theorem that a modular variety obeys (C8) if and only if the finite products of its algebras possess no skew (see Exercise 3) congruences. Compare this with the fact that a modular variety obeys (C3) (is distributive) if and only if the finite subdirect products of its algebras possess no skew congruences. The variety of rings with unit obeys (C8). See Exercise 8 for an interesting application of (C8): An algebra whose congruences obey (C8) has the refinement property (Chang-Jónsson-Tarski [**11**]) for direct decompositions, and so can be represented in at most one way as a direct product of directly indecomposable algebras.

REMARK 8.7. A variety is distributive if and only if all of its algebras generated by three elements have distributive congruence lattices. A variety is modular if and only if all of its algebras generated by four elements have modular congruence lattices. These facts are immediate consequences of Theorems 2.1 and 2.2. Much more generally, it can be proved that every congruence equation expressed in the operations $x \vee y, x \wedge y, [x, y]$ and 0 and 1 is local - holds in a modular variety $\mathcal{V}$ if and only if it holds in every finitely generated algebra in $\mathcal{V}$.

REMARK 8.8. We remarked that each of the equations (C1)–(C8) is preserved under the formation of quotient algebras. This is not true of

every congruence equation, as may be seen by considering this equation which is weaker than (C1):

$$[x, x] \wedge [y, y] \leq [x, y].$$

Let $\mathbf{G}$ be a group with $|\mathbf{Z}(\mathbf{G})| = 2$, $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ non-Abelian, and $\mathbf{Z}(\mathbf{G})$ the only nontrival normal subgroup of $\mathbf{G}$, for example $\mathbf{G} = \mathbf{SL}$*Proposition* 4.3. This information determines the commutator operation on $\mathbf{Con}\ \mathbf{G}$. Now $\mathbf{Con}(\mathbf{G} \times \mathbf{G})$ is the lattice of Figure 1.

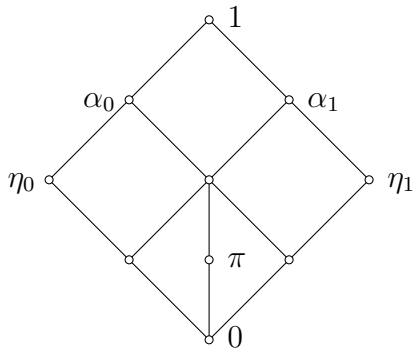


FIGURE 1.

Every congruence of $\mathbf{G} \times \mathbf{G}$ is a direct product congruence except π. Thus the commutator on $\mathbf{Con}(\mathbf{G} \times \mathbf{G})$ is determined by Proposition 4.5(3), and by the fact the π is in the center. For example, $[\alpha_0, \alpha_0] = \eta_0$. Using these facts, the reader can show that the equation above holds in $\mathbf{Con}(\mathbf{G} \times \mathbf{G})$. However, it fails in $(\mathbf{G} \times \mathbf{G})/\pi$ (take $x = \alpha_0/\pi$ and $y = \alpha_1/\pi$).

REMARK 8.9. Each of the equations (C1)–(C8) is preserved under finite subdirect products, and also had the property that it holds as a congruence identity of a variety $\mathcal{V}$ if and only if it holds in the congruence lattice of each subdirectly irreducible algebra in $\mathcal{V}$. Now if ε is a congruence equation that is preserved by taking quotient algebras and finite subdirect products then, since the validity of ε is in addition a local property, we can conclude that for any finite algebra $\mathbf{F}$, $\boldsymbol{V}(\mathbf{F}) \models_{\text{con}} \varepsilon$ if and only if $\mathbf{F}$ satisfies ε hereditarily. In particular, it follows that a finite algebra $\mathbf{F}$ generates a distributive variety if and only if $\mathbf{F}$ is hereditarily neutral (satisfies (C3) hereditarily). This is a result of Hagemann-Hermann [**44**].

PROBLEM 8.10. *Find some simple commutator equations that hold in every modular variety, but do not follow in equational logic from the*

equations defining modular lattices and the equations expressing commutativity and additivity of the commutator, and the equation $[x, y] \leq x \wedge y$. *(The Arguesian equation of B. Jónsson is one example, but it is a pure equation, without commutator, and is rather complex.)*

PROBLEM 8.11. *Is it true that for every modular and nondistributive variety* $\mathcal{V}$*, the pure congruence identities are the same as the pure congruence identities possessed by the variety of modules over the ring of the maximal Abelian subvariety of* $\mathcal{V}$*?*

This problem was refuted by P. P. Pálfy and C. Szabó in [**69**] and [**68**]; see Chapter 15 where some positive results along these lines are also presented.

Exercises

1. Show that if $\mathbf{Con}\ \mathbf{A} \models [x, y] \approx x \wedge y$ then $\mathbf{Con}\ \mathbf{A}$ is a distributive lattice.

2. An algebra whose congruence lattice obeys (C3) is said to be **neutral**. Prove that a subdirect product of finitely many neutral algebras is neutral. Consequently, the join of two distributive subvarieties of a modular variety is distributive.

3. If $\mathbf{A} \subseteq \mathbf{A}_0 \times \mathbf{A}_1$ is a subdirect product, a congruence α of $\mathbf{A}$ is said to be **skew** if and only if α is not of the form $\gamma_0 \wedge \Delta_1$ (with $\gamma \in \mathbf{Con}\ \mathbf{A}_0$ and $\Delta \in \mathbf{Con}\ \mathbf{A}_1$). Prove the equivalence of the following statements for any modular variety. (See the proof of Theorem 8.5.)

(i) $\mathcal{V}$ is distributive,
(ii) $\mathcal{V} \models_{\text{con}}$ (C3) ,
(iii) Subdirect products of two (or of n) algebras in $\mathcal{V}$ have no skew congruences.

4. Prove that in any modular lattice $\mathbf{L}$ with 0 and 1, an element a satisfies $a \wedge (x \vee y) = (a \wedge x) \vee (a \wedge y)$ for all elements x and y if and only if a satisfies $(a \vee x) \wedge (a \vee y) = a \vee (x \wedge y)$ for all elements x and y if and only if the mapping $x \to \langle a \vee x, a \wedge x \rangle$ is a subdirect embedding of $\mathbf{L}$ into the product of its interval sublattices $1/a$ and $a/0$. (Such an element a is called neutral.) Conclude that if $\mathbf{Con}\ \mathbf{A} \models$ (C1) then $\mathbf{Con}\ \mathbf{A}$ is subdirectly embeddable into $(1_{\mathbf{A}}/[1_{\mathbf{A}}, 1_{\mathbf{A}}]) \times ([1_{\mathbf{A}}, 1_{\mathbf{A}}]/0_{\mathbf{A}})$.

5. Show that if $\mathbf{Con}\ \mathbf{A} \models$ (C1) the the join of two Abelian congruences of $\mathbf{A}$ is Abelian. Then conclude that $\mathbf{A}$ has a largest Abelian congruence.

6. Show that a congruence equation is implied by (C2) if and only if it is implied by each of (C3) and (C4). [There is a way to use the result of Exercise 4. This exercise is true whether "imply" is construed in the sense of equational logic (the basic commutator equations and the modular law being implicatly assumed) or in the sense that every variety obeying the one as a congruence equation obeys also the other.]

7. Show that rings with unit obey (C8).

8. Suppose that $\mathbf{Con}\ \mathbf{A} \models$ (C8). Let α and β be complements in $\mathbf{Con}\ \mathbf{A}$ such that $\alpha \circ \beta = \beta \circ \alpha$. Show that the mapping $\lambda \to \beta \vee \lambda$ is an endomorphism of $\mathbf{Con}\ \mathbf{A}$ that commutes with the complete lattice operations. (This is essentially the **strict refinement property** of Chang-Jónsson-Tarski.)

9. Let k be a positive integer not less than 3. Let $\langle V, +, -, 0\rangle$ be a group of cardinality 2^k satisfying $x + x = 0$ (i.e. a vector space of dimension k over the 2 element field). Let $\cdot$ and $\oplus$ be any operations such that $\langle V, \cdot, \oplus\rangle$ is a lattice. Let $\mathbf{A}$ be the algebra whose universe is V and basic operations are $+, -, f$ defined by

$$f(x_0, \ldots, x_{k+1}) = \begin{cases} x_k \cdot x_{k+1} & \text{if } x_0, \ldots, x_{k-1} \text{ are} \\ & \qquad \text{linearly independent} \\ 0 & \text{otherwise} \end{cases}$$

and a $k+2$-ary operation g defined the same way from $\oplus$. Prove that $\mathbf{A}$ is neutral, but that every algebra generated by $k-1$ or fewer elements in $\boldsymbol{V}(\mathbf{A})$ is Abelian.

10. Prove that a variety of groups has the congruence extension property if and only if the variety consists of Abelian groups.

CHAPTER 9

Rings Associated With Modular Varieties: Abelian Varieties

Let $\mathcal{V}$ be a modular variety and let $\mathcal{A}$ be all Abelian algebras in $\mathcal{V}$. By Proposition 4.4 and Proposition 4.5, $\mathcal{A}$ is a subvariety of $\mathcal{V}$. Let $\mathbf{A} \in \mathcal{V}$, and let $\beta \in \mathbf{Con}\ \mathbf{A}$ be an Abelian congruence. Recall that, by Corollary 5.8, each block of β is an Abelian group with addition $x + y = d(x, z, y)$, where z is any fixed element of the block and of course d is a Gumm difference term. Moreover the unary polynomials of $\mathbf{A}$ induce affine maps (i.e., maps which preserve $d(x, y, z)$) between the β blocks. In this chapter we will construct matrix rings for $\mathcal{V}$, acting on the direct sum of the blocks, which capture these affine actions. In this way the direct sum of the blocks becomes a module over one of our rings. There is a strong connection between the structure of this module and the structure of $\mathbf{A}$ (see, for example, Theorem 9.9). Several of the results of this chapter will be applied in the subsequent chapters.

In the case $\mathcal{V}$ is Abelian, i.e. $\mathcal{V} = \mathcal{A}$, only one of these rings is needed and the variety $\mathcal{V}$ is closely related (in fact polynomially equivalent) to the variety of modules over this ring. The connection, which is actually stronger than this, is established at the end of the chapter.

Before commencing with the constructions and proofs, let us remark that affine algebras and varieties composed of then have been studied, for different reasons, by a number of authors since Osterman and Schmidt first (it seems) gave them serious consideration in [**67**]. The papers of Bela Csakany, [**16**] and [**17**], and Gumm's [**37**], have between them a good set of references to this literature. Chapters 4 and 5 of Smith's book [**79**] should also be consulted. In our opinion the treatment presented here is essentially novel, and more satisfactory in several respects than the previous treatments. (Our readers, of course, will have their own opinions.) Nevertheless, the subject is not as easy as it first looks and work remains to be done. As stated above the results of this chapter will be useful in some of the applications presented in the later chapters. The detailed description of Abelian varieties given at the end of the chapter has been applied in Baldwin-McKenzie [**1**], Burris-McKenzie [**8**], and McKenzie [**63**].

Let $\mathbf{A} \in \mathcal{V}$, z, $z' \in \mathbf{A}$ and let β be an Abelian congruence on $\mathbf{A}$. Recall that $\mathbf{M}(\beta, z)$ is the β block, z/β, of A containing z and that it is an Abelian group under $x+y = d(x, z, y)$ with z as the zero element. Let $\mathrm{Hom}(\beta, z, z')$ denote the set of functions $g : \mathbf{M}(\beta, z) \to \mathbf{M}(\beta, z')$ of the form

$$g(x) = f(x, z, z', c_0, \ldots, c_{k-1}) \tag{1}$$

where $c_0, \ldots, c_{k-1} \in \mathbf{A}$ and f is a $k+3$-ary term, $k < \omega$, such that $\mathcal{V}$ satisfies

$$f(v, v, v', y_0, \ldots, y_{k-1}) \approx v'. \tag{2}$$

The next lemma gives a much simpler description of $\mathrm{Hom}(\beta, z, z')$ and shows that it does not depend on $\mathcal{V}$.

LEMMA 9.1. $\mathrm{Hom}(\beta, z, z')$ *is the set of restrictions to* z/β *of unary polynomials on* $\mathbf{A}$ *which map* z *to* z'.

PROOF. Let h be a $(k+1)$-ary term such that

$$h(z, c_0, \ldots, c_{k-1}) = z'.$$

Define a term f by

$$f(u, v, v', \mathbf{y}) = d(h(u, \mathbf{y}), h(v, \mathbf{y}), v')$$

where $\mathbf{y} = (y_0, \ldots, y_{k-1})$. Clearly $\mathcal{V}$ satisfies (2) and, since β is Abelian.

$$f(x, z, z', c_0, \ldots, c_{k-1}) = h(x, c_0, \ldots, c_{k-1})$$

for all $x \in \mathbf{M}(\beta, z)$ by Theorem 5.5(ii) □

By Corollary 5.8 each $g \in \mathrm{Hom}(\beta, z, z')$ is a group homomorphism from $\mathbf{M}(\beta, z)$ into $\mathbf{M}(\beta, z')$. $\mathrm{Hom}(\beta, z, z')$ is an Abelian group under the operation $(g+h)(x) = d(g(x), z', h(x))$, for $g, h \in \mathrm{Hom}(\beta, z, z')$. If z'' is another element of $\mathbf{A}$ and if $g \in \mathrm{Hom}(\beta, z, z')$ and $h \in \mathrm{Hom}(\beta, z', z'')$ then we define hg by $hg(x) = h(g(x))$, of course. As an exercise the reader can show that the distributive laws hold. In particular, $\mathrm{Hom}(\beta, z, z)$ is a ring with 1. Also note that if $f(x_1, \ldots, x_n)$ is a polynomial on $\mathbf{A}$ and $f(z_1, \ldots, z_n) = z$ then f defines a group homomorphism of $\mathbf{M}(\beta, z_1) \times \cdots \times \mathbf{M}(\beta, z_n)$ into $\mathbf{M}(\beta, z)$, by Corollary 5.8. Moreover, if we let $g_i(x_i) = f(z_1, \ldots, z_{i-1}, x_i, z_{i+1}, \ldots, z_n)$ then $g_i \in \mathrm{Hom}(\beta, z_i, z)$ and

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} g_i(x_i). \tag{3}$$

If $\mathbf{R}$ is the ring of n by n matrices whose $(i, j)^{\text{th}}$ elements lie in $\mathrm{Hom}(\beta, z_j, z_i)$, then this ring acts naturally on $\mathbf{M}(\beta, z_1) \times \cdots \times \mathbf{M}(\beta, z_n)$

and by the equation displayed above a great deal of information about the algebraic structure of $\mathbf{A}$ is contained in this action.

In this chapter we construct a class of matrix rings for $\mathcal{V}$ which will act on the direct sum of some of the blocks of an Abelian congruence. The class will have two parameters: λ, the size of the matrices, and κ, the number of constants. Thus let $X = \{u\} \cup \{v_i : i < \lambda\} \cup \{y_i : i < \kappa\}$, where $\lambda \geq 1$ and $\kappa \geq 0$ are cardinals and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(X)$. Let e_i denote the endomorphism of $\mathbf{F}$ which sends u to v_i and fixes all other generators. Let $\theta_i = \mathrm{Cg}(u, v_i)$.

Definition 9.2. Let $H_{ij} = \{r \in \mathbf{F} : e_i r = v_j\}$ and let $\bar{H}_{ij} = \{r/[\theta_i, \theta_i] : r \in H_{ij}\}$.

If $r = r(u, \mathbf{v}, \mathbf{y})$ and $s = s(u, \mathbf{v}, \mathbf{y})$ are in H_{ij} and $t = t(u, \mathbf{v}, \mathbf{y})$ is in H_{jk} then we define

$$\begin{aligned} r + s &= d(r, v_j, s) \\ -r &= d(v_j, r, v_j) \\ t \circ r &= t(r, \mathbf{v}, \mathbf{y}) \end{aligned} \tag{4}$$

Let π_r denote the canonical projection of $\mathbf{F}$ onto $\mathbf{F}/[\theta_i, \theta_i]$. Operations on the $\bar{H}_{ij}$'s are defined by

$$\begin{aligned} \pi_i(r) + \pi_i(s) &= \pi_i(r + s) \\ -\pi_i(r) &= \pi_i(-r) \\ \pi_j(t) \circ \pi_i(r) &= \pi_i(t \circ r) \end{aligned} \tag{5}$$

Notice that H_{ij} is simply the set of those elements of $\mathbf{F}$ which can be represented by a term $r(u, v, y)$ such that $r(v_i, v, y) \approx v_j$ holds in $\mathcal{V}$. It is easy to see that the above operations on the $\bar{H}'_{ij}s$ are well defined except possibly for composition where the problem is to show that if $t \ [\theta_j, \theta_j] \ t'$, for some $t, t' \in H_{jk}$, and $r \in H_{ij}$ then $t \circ r \ [\theta_i, \theta_i] \ t' \circ r$. Let ℓ be the endomorphism of $\mathbf{F}$ which sends u to r and fixes all other generators. Note that $e_i \ell = e_j$ (since $r \in H_{ij}$) and that $\ker e_k = \theta_k$. Thus $\ell^{-1}(\theta_i) = \theta_j$. Indeed, $(a, b) \in \ker e_j$ if and only if $e_j a = e_j b$ if and only if $e_i \ell a = e_i \ell b$ if only if $(\ell a, \ell b) \in \ker e_i$ if and only if $(a, b) \in \ell^{-1}(\ker e_i)$. Now using Proposition 4.4(2) and then Proposition 4.4(1) we have

$$\begin{aligned} \ell^{-1}[\theta_i, \theta_i] &\geq \ell^{-1}[\theta_i|_{\mathrm{rng}\,\ell}, \theta_i|_{\mathrm{rng}\,\ell}] \\ &= \ell^{-1}[\ell\ell^{-1}(\theta_i), \ell\ell^{-1}(\theta_i)] \\ &= [\ell^{-1}(\theta_i), \ell^{-1}(\theta_i)] \vee \ker \ell \\ &\geq [\theta_j, \theta_j] \end{aligned}$$

Hence $\ell[\theta_j, \theta_j] \subseteq [\theta_i, \theta_i]$. Now $t \circ r = \ell(t)$ and $t' \circ r = \ell(t')$. Thus $t \circ r \; [\theta_i, \theta_i] \; t' \circ r$, as desired.

It follows easily from Proposition 5.7 that $\bar{H}_{ij}$ is an Abelian group with $\pi_i(v_j)$ as null element. The composition satisfies the associative and distributive laws. For example, if $r, s \in H_{ij}$ and $t \in H_{jk}$ then since $r \; \theta_i \; v_j \; \theta_i \; s$, we have by Proposition 5.7

$$\begin{aligned} t \circ (r + s) &= t(r + s, \mathbf{v}, \mathbf{y}) \\ &= t(d(r, v_j, s), \mathbf{v}, \mathbf{y}) \\ &\equiv d(t(r, \mathbf{v}, \mathbf{y}), t(v_j, \mathbf{v}, \mathbf{y}), t(s, \mathbf{v}, \mathbf{y})) \pmod{[\theta_i, \theta_i]} \\ &= d(t \circ r, v_k, t \circ s) \\ &= t \circ r + t \circ s, \end{aligned}$$

proving the left distributive law.

In particular $\bar{H}_{ii}$ is a ring with $0 = \pi_i(v_i)$ and $1 = \pi_i(u)$. Also, by Proposition 5.7, one can show that the group $\bar{H}_{ij}$ does not depend on the choice of $d(x, y, z)$, so long as it satisfies Theorem 5.5(i,ii).

DEFINITION 9.3. Let $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$ be the ring of all λ by λ matrices (m_{ij}) with $m_{ij} \in \bar{H}_{ji}$ such that each column contains only finitely many nonzero entries. Addition and multiplication are the ordinary matrix operations. The zero of this ring is the matrix whose $(i, j)^{\text{th}}$ element is $\pi_j v_i$. The unit element of this ring has $(i, j)^{\text{th}}$ element $\pi_j v_i$, for $i \neq j$, and $\pi_i u$ for $i = j$. We let $\mathbf{R}(\mathcal{V}, \lambda) = \mathbf{R}(\mathcal{V}, \lambda, 0)$ and $\mathbf{R}(\mathcal{V}) = \mathbf{R}(\mathcal{V}, 1)$.

Now let $\mathbf{A} \in \mathcal{V}$, β an Abelian congruence on $\mathbf{A}$ and $z_i \in \mathbf{A}$, $i < \lambda$. Let $\mathbf{M} = \sum_{i<\lambda} \mathbf{M}(\beta, z_i)$ denote the direct sum of the Abelian groups $\mathbf{M}(\beta, z_i)$, i.e., $\mathbf{M} = \{(a_i)_{i<\lambda} : a_i = z_i$ for all but finitely many i's$\}$. For each choice of constants $c_k \in \mathbf{A}$, $k < \kappa$, we make $\mathbf{M}$ into an $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$–module. Let $(m_{ij}) \in \mathbf{R}(\mathcal{V}, \lambda, \kappa)$ and let $m_{ij} = \pi_j r_{ij} \in \bar{H}_{ji}$, with $r_{ij} = r(u, \mathbf{v}, \mathbf{y}) \in H_{ji}$. If $a_j \in z_j/\beta$ then we define

$$m_{ij} \cdot a_j = (\pi_j r_{ij}) \cdot a_j = r(a_j, \mathbf{z}, \mathbf{c}). \tag{6}$$

More formally, this means $(\pi_j r_{ij}) \cdot a_j$ is the image of r_{ij} under the homomorphism $\sigma : F \to A$ sending u to a_j, v_k to z_k, and y_k to c_k. Since $r_{ij} \in H_{ji}$, $r(v_j, \mathbf{v}, \mathbf{v}) \approx v_i$ holds in $\mathcal{V}$, and hence the map $a_j \to (\pi_j r_{ij}) \cdot a_j$, defined above, is an element of $\text{Hom}(\beta, z_j z_i)$ by Lemma 9.1. Moreover, looking at the proof of Lemma 9.1, we see that every element of $\text{Hom}(\beta, z_j, z_i)$ can be represented in this way (provided κ is sufficiently large).

In order to show that the multiplication given by (6) is well defined, we need to check that the map given above is well defined. That is, we need to show that it is independent of the choice of r_{ij}. To do this

we must show that if r, $r' \in H_{ij}$ and $r(u, \mathbf{v}, \mathbf{y})\ [\theta_j, \theta_j]\ r'(u, \mathbf{v}, \mathbf{y})$ then $r(a_j, \mathbf{z}, \mathbf{c}) = r'(a_j, \mathbf{z}, \mathbf{c})$ for $a_j \in z_j/\beta$. To see this let $\sigma : \mathbf{F} \to \mathbf{A}$ be the homomorphism defined above and let π be the kernel of σ. Now $\sigma(\theta_j + \pi) = \sigma(\mathrm{Cg}(u, v_j) + \pi) = \mathrm{Cg}(\sigma(u), \sigma(v_j)) = \mathrm{Cg}(a_j, z_j) \leq \beta$. By Proposition 4.4(1)

$$\begin{aligned}\sigma([\theta_j, \theta_j] + \pi) &= [\sigma(\theta_j + \pi), \sigma(\theta_j + \pi)] \\ &\leq [\beta, \beta] \\ &= 0\end{aligned}$$

Thus, since $r(a_j, \mathbf{z}, \mathbf{c})$ and $r'(a_j, \mathbf{z}, \mathbf{c})$ are related by the congruence on the left, they are equal.

Now if $\mathbf{m} = (m_{ij})$ is a matrix in $\mathbf{R} = \mathbf{R}(\mathcal{V}, \lambda, \kappa)$ and $\mathbf{a} = (a_i) \in \sum \mathbf{M}(\beta, z_i)$ we define $\mathbf{m} \cdot \mathbf{a} = \mathbf{b}$, where $b = (b_i)$ with $b_i = \sum_{j<\lambda} m_{ij} \cdot a_j$, that is, m acts by ordinary matrix multiplication, where we view $\mathbf{a}$ and $\mathbf{b}$ as column vectors. Since $m_{ij} \cdot a_j \in \mathbf{M}(\beta, z_i)$ and, for all but finitely many j, $a_j = z_j$, the sum defining b_i makes sense. Moreover, since $\mathbf{m}$ is column finite, $b_i = z_i$ for all but finitely many i, so that $b \in \sum \mathbf{M}(\beta, z_i)$. To see that $\mathbf{M}$ is a module under this action we need to check four things. First it is easy to see that if $\mathbf{1}$ is the identity of $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$ then $\mathbf{1} \cdot \mathbf{a} = \mathbf{a}$. If $\mathbf{n} = (n_{ij})$ is also in $\mathbf{R}$, we need to show that $(\mathbf{m} \cdot \mathbf{n}) \cdot \mathbf{a} = \mathbf{m} \cdot (\mathbf{n} \cdot \mathbf{a})$. This follows from the fact that $(m_{ik} \cdot n_{kj}) \cdot a_j = m_{ik} \cdot (n_{kj} \cdot a_j)$, which in turn follows easily from the definitions. (Essentially this is just the fact that function composition is associative.) We also need to show that both distributive laws hold. The law $(\mathbf{m} + \mathbf{n}) \cdot \mathbf{a} = \mathbf{m} \cdot \mathbf{a} + \mathbf{n} \cdot \mathbf{a}$ follows directly from the definition and the argument for the other distributive law is similar to the proof of the distributive law given above. The details are left to the reader.

Notice that, in particular, $\mathbf{M}(\beta, z)$ is an $\mathbf{R}(\mathcal{V}, 1, \kappa)$–module for each choice of constants $c_k \in \mathbf{A}$, $k < \kappa$.

Arbitrary polynomials as well as unary polynomials are closely related to the sets $\mathrm{Hom}(\beta, z_i, z_j)$. Indeed, if $f(x_1, \ldots, x_{n-1})$ is a polynomial on $\mathbf{A}$ with $f(z_1, \ldots, z_{n-1}) = z_0$ then

$$g_i(x) = f(z_1, \ldots, z_{i-1}, z, z_{i+1}, \ldots, z_{n-1}) \in \mathrm{Hom}(\beta, z_i, z_0).$$

Hence there is an $m_i \in \bar{H}_{i0}$ with $g_i(x) = m_i \cdot x$. Thus we have the representation

$$f(a_1, \ldots, a_{n-1}) = \sum_{i=1}^{n-1} m_i \cdot a_i, \quad a_i \in z_i/\beta. \tag{7}$$

As an example, let $\lambda = 1$ and let $\mathcal{V}$ be the variety of groups. An Abelian congruence of $\mathbf{G} \in \mathcal{V}$ corresponds to an Abelian normal subgroup $\mathbf{H}$. We will use v in place of v_0 since there is only one v. For $k < \kappa$, let $r_k(u, v, \mathbf{y}) = y_k u v^{-1} y_k^{-1} v$. Since $r_k(v, v, \mathbf{y}) \approx v$, $r_k(u, v, \mathbf{y}) \in H_{00}$. If $g_k \in G$ are fixed and we choose the correspondence $y_k \to g_k$ and let z (the image of v in $\mathbf{G}$) be the identity of $\mathbf{G}$, and if $x \in \mathbf{H}$, then $(\pi_0 r_k) \cdot x = g_k^{-1} x g_k$. Thus the action on $\mathbf{H}$ of conjugation by a set of elements of $\mathbf{G}$ is included in the $\mathbf{R}(\mathcal{V}, 1, \kappa)$ action on $\mathbf{H}$. This action is extremely important in group theory. The ring $\mathbf{R}(\mathcal{V}, 1, 0)$ does not contain this action on $\mathbf{H}$.

Before we begin our study of Abelian congruences, we prove there easy results about $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$.

PROPOSITION 9.4. *If $\kappa \leq \kappa'$ then $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$ is both a subring and a homomorphic image of $\mathbf{R}(\mathcal{V}, \lambda, \kappa')$.*

PROOF. Let X be as before and let $X' = \{u\} \cup \{v_i : i < \lambda\} \cup \{y_k : k < \kappa'\}$, and let $\mathbf{F}' = \mathbf{F}_{\mathcal{V}}(X')$ and view $\mathbf{F} \subseteq \mathbf{F}'$. Let $\varphi : \mathbf{F}' \to \mathbf{F}$ map y_k to v_0 for $\kappa \leq k < \kappa'$ and fix all other generators. Clearly $H_{ij} \subseteq H'_{ij}$ and $\varphi(H'_{ij}) = H_{ij}$. Now let $\theta'_i = \mathrm{Cg}_{\mathbf{F}'}(u, v_i)$ and note $\theta_i = \theta'_i \cap \mathbf{F}^2$ and $\varphi(\theta'_i \vee \ker \varphi) = \theta_i$. By Proposition 4.4(1) $\varphi([\theta'_i, \theta'_i] \vee \ker \varphi) = [\theta_i, \theta_i]$ and from this and Proposition 4.4(2) we obtain $[\theta_i, \theta_i] = [\theta'_i, \theta'_i] \cap \mathbf{F}^2$. From this it follows that for r, $s \in \mathbf{F}$, $r\ [\theta_i, \theta_i]\ s$ if and only if $r\ [\theta'_i, \theta'_i]\ s$ and hence the natural map from $\bar{H}_i$ into $\bar{H}_{ij}$ is well defined and injective. Since $\varphi(\theta'_i) = \theta_i$, $\varphi([\theta'_i, \theta'_i]) \subseteq [\theta_i, \theta_i]$. From this it follows that there is a natural map $\bar{\varphi}$ from $\bar{H}_{ij}$ onto $\bar{H}_{ij}$. These injections can be combined into an injection of $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$ into $\mathbf{R}(\mathcal{V}, \lambda, \kappa')$ which is a ring homomorphism. Similarly the natural surjections can be combined into a ring surjection of $\mathbf{R}(\mathcal{V}, \lambda, \kappa')$ onto $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$. The details are left to the reader. □

THEOREM 9.5. *Let $\mathcal{V}$ be a modular variety and $\mathcal{A}$ its maximal Abelian subvariety. Then the following are equivalent*

(i) *$\mathcal{V}$ is distributive,*
(ii) *$|\mathbf{R}(\mathcal{V}, \lambda, \kappa)| = 1$ for all $\lambda \geq 1$ and $\kappa \geq 0$,*
(iii) *$|\mathbf{R}(\mathcal{V}, 1, 0)| = 1$,*
(iv) *$|\mathbf{R}(\mathcal{V}, \lambda, \kappa)| = 1$ for some $\lambda \geq 1$ and $\kappa \geq 0$.*

Moreover, $\mathcal{V}$ satisfies (C8) (of Chapter 8) if and only if $|\mathbf{R}(\mathcal{A}, 1, 0)| = 1$.

PROOF. If $\mathcal{V}$ is distributive then $[\theta_i, \theta_i] = \theta_i$. Hence $\bar{H}_{ij} = \{\pi_i(v_j)\}$ and so $|\mathbf{R}(\mathcal{V}, \lambda, \kappa)| = 1$. If (iv) holds and β is an Abelian congruence on $\mathbf{A} \in \mathcal{V}$, then $\sum_{i<\lambda} \mathbf{M}(\beta, z_i)$ is an $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$–module. This forces $\mathbf{M}(\beta, z)$ to be trivial for $z \in \mathbf{A}$. Hence $\beta = 0$. This easily implies that $\mathcal{V}$ is distributive.

Clearly (ii) implies (iii) implies (iv). The last statement follows from the fact that $\mathcal{V}$ satisfies (C8) if and only if $\mathcal{A}$ is trivial. But an Abelian variety is trivial if and only if it is distributive. □

PROPOSITION 9.6. *If $\mathcal{U}$ is a subvariety of $\mathcal{V}$ then $\mathbf{R}(\mathcal{U}, \lambda, \kappa)$ is a homomorphic image of $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$.*

PROOF. If $\mathcal{U}$ is the trivial variety that result is clear. So assume that $\mathcal{U}$ is nontrivial and let f be the homomorphism of $\mathbf{F}_{\mathcal{V}}(X)$ onto $\mathbf{F}_{\mathcal{V}}(X)$ which is the identity on X. This clearly induces a map from $H_{ij}(\mathcal{V})$ to $H_{ij}(\mathcal{U})$. The proof of Lemma 9.1 shows this map is onto. By Proposition 4.4(1) this induces a map of $\bar{H}_{ij}(\mathcal{V})$ onto $\bar{H}_{ij}(\mathcal{U})$. It is easy to see that this map respects addition and composition from which it follows that $\mathbf{R}(\mathcal{U}, \lambda, \kappa)$ is a homomorphic image of $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$. □

We now look more closely at the ring action on an Abelian congruence β of an algebra $\mathbf{A}$. Let z_i, $i < \lambda$, and c_k, $k < \kappa$, be elements of $\mathbf{A}$. Recall that if $r(u, \mathbf{v}, \mathbf{y}) \in H_{ij}$ Then the restriction of $g(x) = r(x, \mathbf{z}, \mathbf{c})$ to z_i/β is in $\mathrm{Hom}(\beta, z_i, z_j)$. When can every element of $\mathrm{Hom}(\beta, z_i z_j)$ be represented in this way? It follows from Lemma 9.1 that his will be the case if there are enough constants. One way to ensure this is to choose a constant for each element of $\mathbf{A}$ (so that $\kappa = |\mathbf{A}|$). Although the example of the Abelian normal subgroup before Pproposition 9.4 shows that we do need the constants for our ring, we will see that in many important cases we can get by without them. We will see below in Theorem 9.12 that they are not necessary at all for Abelian varieties.

Let β an Abelian congruence on $\mathbf{A}$ and let $z_i \in \mathbf{A}$, $i < \lambda$. Choose constants c_k, $k < \kappa$, and another set of constants c'_k, $k < \kappa$. These sets of constants determine two ring actions on $\sum \mathbf{M}(\beta, z_i)$. The next result relates these actions.

THEOREM 9.7. *Let β, z_i, $i < \lambda$, c_k, c'_k, $k < \kappa$, be as described above. Let $\gamma = (0 : \beta)$ be the centralizer of β. If $c_k \ \gamma \ c'_k$, for $k < \kappa$, then the two ring actions of $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$ on $\sum \mathbf{M}(\beta, z_i)$ determined by the two sets of constants are the same.*

PROOF. Let $r(u, \mathbf{v}, \mathbf{y})$ be a term representing an element of H_{ij}, so that $r(v_i, \mathbf{v}, \mathbf{y}) \approx v_j$ is an identity of $\mathcal{V}$. Then in $\mathbf{A}$ $r(z_i, \mathbf{z}, \mathbf{c}) = z_j = r(z_i, \mathbf{z}, \mathbf{c}')$. Since $\mathbf{c} \ \gamma \ \mathbf{c}'$ and $[\beta, \gamma] = 0$, the term condition implies that $r(a_i, \mathbf{z}, \mathbf{c}) = r(a_i, \mathbf{z}, \mathbf{c}')$ for $a_i \in z_i/\beta$. From this it follows easily that the two ring actions are the same. □

Again suppose β is an Abelian congruence on $\mathbf{A}$ and let $\gamma = (0 : \beta)$ be its centralizer. Let $z_i \in \mathbf{A}$, $i < \lambda$ and suppose that each γ–class is represented by some z_i. (Notice that this is weaker than the assumption

that each β–class is represented.) In this case we will not need any c_k's; the z_i's will serve as constants. To see this suppose that c_k, $k < \kappa$, are elements of $\mathbf{A}$. Let $x = \{u\} \cup \{v_i : i < \lambda\} \cup \{y_k : k < \kappa\}$ and $X_0 = \{u\} \cup \{v_i : i < \lambda\}$. Then $\mathbf{M} = \sum \mathbf{M}(\beta, z_i)$ is both an $\mathbf{R} = \mathbf{R}(\mathcal{V}, \lambda, \kappa)$ and an $\mathbf{R}_0 = \mathbf{R}(\mathcal{V}, \lambda) = \mathbf{R}(\mathcal{V}, \lambda, 0)$ module. By the definition of a module this means that there are ring homomorphisms from both $\mathbf{R}$ and $\mathbf{R}_0$ into the ring of endomorphisms of $\mathbf{M}$ as an Abelian group. Using the last theorem we can see that the images of these two homomorphisms are the same and thus the two modules ${}_{\mathbf{R}}\mathbf{M}$ and ${}_{\mathbf{R}_0}\mathbf{M}$ are the same. The idea is this. If $r(u, \mathbf{v}, \mathbf{y})$ is a term representing and element in H_{ij} then let $s(u, \mathbf{v})$ be the term obtained from r by replacing each y_k with v_m, where m is the (first say) index such that $c_k \ \gamma \ z_m$. As in the last theorem it is easy to see that $s(u, \mathbf{v}) \in \mathrm{H}^0_{ij}$ (the H_{ij} associated with X_0) and that the elements of $\mathrm{Hom}(\beta, z_i, z_j)$ determined by r and s are the same, i.e., $(\pi_i r)\cdot x = (\pi_i s)\cdot x$ for $x \in z_i/\beta$. Thus in summary, if β is an Abelian congruence on $\mathbf{A}$ with centralizer $r = (0 : \beta)$ and $z_i \in \mathbf{A}$, i $< \lambda$, represents all the γ–classes, then the actions of $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$ and of $\mathbf{R}(\mathcal{V}, \lambda)$ on $\sum \mathbf{M}(\beta, z_i)$ are the same. Thus in studying $\sum \mathbf{M}(\beta, z_i)$ we take $\mathbf{R}(\mathcal{V}, \lambda, 0)$ as our ring. For future reference we record the fact that each element of $\mathrm{Hom}(\beta, z_i, z_j)$ can be represented by an element of H^0_{ij}.

LEMMA 9.8. *With A, β, γ, z_i, $i < \lambda$ and H^0_{ij} as above, let $h \in \mathrm{Hom}(\beta, z_i, z_j)$. Then there is an element $r \in \mathrm{H}^0_{ij}$ (and so representable by a term $r(u, v)$, with $r(v_i, v) \approx v_j$ in $\mathcal{V}$) such that $h(x) = (\pi_i r) \cdot x = r(x, z)$ for all $x \in z_i/\beta$.* □

The map described above, which sends the y_k to v_i where i is the first index such that $c_k \ \gamma \ z_i$, induces a ring homomorphism of $\mathbf{R}$ onto $\mathbf{R}_0$. In Exercise 6 you are asked to show that the kernel of this ring homomorphism is contained in the kernel of the action of $\mathbf{R}$ on $\mathbf{M}$.

The next theorem shows that there is a strong connection between $\mathbf{A}$ and the module $\sum \mathbf{M}(\beta, z_i)$.

THEOREM 9.9. *Let $\mathbf{A} \in \mathcal{V}$ and let $\beta \in \mathbf{Con\ A}$ be an Abelian congruence. Let $\gamma \in \mathbf{Con\ A}$ satisfy $\gamma \geq \beta$ and $[\beta, \gamma] = 0$, i.e., $\beta \leq \gamma \leq (0 : \beta)$. Let z_i, $i < \lambda$, be elements of $\mathbf{A}$ such that each γ–class contains at least one z_i. Then the lattice of submodules of the module $\sum \mathbf{M}(\beta, z_i)$ over $\mathbf{R}(\mathcal{V}, \lambda)$ is isomorphic to the interval $\beta/0$ in $\mathbf{Con\ A}$.*

PROOF. We now let $\mathbf{R} = \mathbf{R}(\mathcal{V}, \lambda)$ $(= \mathbf{R}(\mathcal{V}, \lambda, 0))$ and take H^0_{ij} to be as in the previous lemma. If $\delta \leq \beta$ let $\mathbf{M}(\delta) = \sum_{i<\lambda} \mathbf{M}(\delta, z_i)$. It is easy to see that $\mathbf{M}(\delta)$ is a submodule of $\mathbf{M} = \mathbf{M}(\beta)$, and the map $\delta \mapsto \mathbf{M}(\delta)$ is order-preserving.

For the inverse map suppose that $\mathbf{N}$ is a submodule of $\mathbf{M}$. Define a relation $\alpha_{\mathbf{N}}$ on $\mathbf{A}$ by $x\ \alpha_{\mathbf{N}}\ y$ if and only if two conditions hold. First $x\beta y$. Since $\beta \leq \gamma$ this implies that $x\gamma y$ and thus there is an i such that $x, y, \in z_i/\gamma$. For $j < \lambda$, let $\iota_j : \mathbf{M}(\beta, z_j) \to \mathbf{M}$ be the map which sends $a_j \in \mathbf{M}(\beta, z_j)$ to the vector whose j^{th} coordinate is a_j and whose other coordinates are 0 (i.e., whose k^{th} coordinate is z_k, for $k \neq j$). The second condition is that $\iota_i d(x, y, z_i)$ is in $\mathbf{N}$. This last condition is equivalent to saying that there is some element of $\mathbf{N}$ whose i^{th} entry is $d(x, y, z_i)$. Moreover, there could be more than one i with $x,\ y \in z_i/\gamma$, but the definition is independent of which i is used. To see the former statement let $a \in N$ have i^{th} entry $d(x, y, z_i)$. Let $\mathbf{m}$ be the matrix in $\mathbf{R}$ whose $(i, i)^{\text{th}}$ entry is $1 (= \pi_i(u))$ and whose other entries are 0. Then $\iota_i d(x, y, z_i) = \mathbf{m} \cdot \mathbf{a} \in \mathbf{N}$, proving the first claim. To see the second statement suppose that $x,\ y \in z_i/\gamma$ and $x,\ y \in z_j/\gamma$. Let $r = d(u, v_i, v_j) \in H_{ij}$. It follows easily form Proposition 5.7 that $(\pi_i r) \cdot d(x, y, z_i) = r(d(x, y, z_i), z_i, z_j) = d(x, y, z_j)$. Let $\mathbf{m}$ be the matrix in $\mathbf{R}$ whose $(j, i)^{\text{th}}$ entry is $\pi_i(r)$ and whose other entries are 0. If $\mathbf{a} = \iota_i d(x, y, z_i)$ and $\mathbf{b} = \iota_j d(x, y, z_j)$ then $\mathbf{m} \cdot \mathbf{a} = \mathbf{b}$, which proves the second claim.

Using Proposition 5.7 and the Abelian group operations on $\mathbf{N}$, one can show that $\alpha_{\mathbf{N}}$ is an equivalence relation on $\mathbf{A}$. To see that it is a congruence let g be a unary polynomial on $\mathbf{A}$. Assume that $x\ \alpha_{\mathbf{N}}\ y$ and that $x,\ y \in z_i/\gamma$. We need to show that $g(x)\ \alpha_{\mathbf{N}}\ g(y)$. Choose j so that $g(z_i) \in z_j/\gamma$. Let $h(w) = d(g(w), g(z_i), z_j)$. Then $h(z_i) = z_j$, so $h \in \text{Hom}(\beta, z_i, z_j)$ by Lemma 9.1. By the previous lemma, there is an element $r \in \text{H}^0_{ij}$ such that $(\pi_i r) \cdot c = h(c)$ for all $c \in z_i/\beta$. Let $x\ \alpha_N\ y$ and let $\mathbf{a} = \iota_i d(x, y, z_i)$. Then $\mathbf{a} \in \mathbf{N}$ by the definition of $\alpha_{\mathbf{N}}$. Let $\mathbf{m} \in \mathbf{R}$ be the matrix whose $(j, i)^{\text{th}}$ entry is $\pi_i r$ and whose other entries are all 0. Since $\mathbf{N}$ is a submodule, $\mathbf{m} \cdot \mathbf{a} \in \mathbf{N}$. All components of $\mathbf{m} \cdot \mathbf{a}$ are 0 except the j^{th} which is $h(d(x, y, z_i))$. Now since $x\ \beta\ y\ \gamma\ z_i$, Proposition 5.7 yields $h(d(x, y, z_i)) = d(h(x), h(y), z_j)$. Thus $\iota_j d(h(x), h(y), z_j) \in \mathbf{N}$. This shows that $h(x)\ \alpha_{\mathbf{N}}\ h(y)$. Now we calculate

$$\begin{aligned} d(h(x), h(y), z_j) &= d(d(g(x), g(z_i), z_j), d(g(y), g(z_i), z_j), d(z_j, z_j, z_j)) \\ &= d(d(g(x), g(y), z_j), d(g(z_i), g(z_i), z_j), d(z_j, z_j, z_j)) \\ &= d(d(g(x), g(y), z_j), z_j, z_j) \\ &= d(g(x), g(y), z_j) \end{aligned}$$

The second equality follows from Proposition 5.7 "backwards" since $g(x)\ \beta\ g(y)\ \gamma\ z_j$ and $g(z_i)\ \gamma\ z_j$. The last equality is valid since

$$d(g(x), g(y), z_j)\ \beta\ d(g(x), g(x), z_j) = z_j.$$

Thus $g(x)\ \alpha_{\mathbf{N}}\ g(y)$. Hence $\alpha_{\mathbf{N}}$ is a congruence. Clearly, $\alpha_{\mathbf{N}} \leq \beta$ and the map $\mathbf{N} \to \alpha_{\mathbf{N}}$ preserves order.

We now have two order-preserving maps between the lattices. We need to show that they are mutually inverse, i.e., we need to show that for $\delta \leq \beta$, $\delta = \alpha_{\mathbf{M}(\delta)}$, and for $\mathbf{N}$ a submodule of $\mathbf{M}$, $\mathbf{N} = \mathbf{M}(\alpha_{\mathbf{N}})$. To see the first, let $x\beta y$ and $x,\ y \in z_i/\gamma$. Then since $x\beta y$,

$$\begin{aligned} x\ \alpha_{\mathbf{M}(\delta)}\ y &\Leftrightarrow \iota_i d(x, y, z_i) \in \mathbf{M}(\delta) \\ &\Leftrightarrow d(x, y, z_i)\ \delta\ z_i \\ &\Leftrightarrow x\delta y. \end{aligned}$$

That $d(x, y, z_i)\ \delta\ z_i$ implies $x\ \delta\ y$ follows from the fact that $x = d(d(x, y, z_i), z_i, y)$ which follows Proposition 5.7 since

$$\begin{aligned} d(d(x, y, z_i), z_i, y) &= d(d(x, y, z_i), d(y, y, z_i), d(y, y, y)) \\ &= d(d(x, y, y), d(y, y, y), d(z_i, z_i, y)) \\ &= d(x, y, y) = x. \end{aligned}$$

Now if $\mathbf{a} \in \mathbf{M}$ and $\mathbf{N}$ is a submodule, then $\mathbf{a} \in \mathbf{N}$ if and only if $\iota_i a_i \in \mathbf{N}$ for each i. That $\mathbf{a} \in \mathbf{N}$ implies $\iota_i a_i \in \mathbf{N}$ was shown earlier in the proof. Since $\mathbf{a} \in \mathbf{N}$ implies that all but finitely many coordinates are 0, $\mathbf{a}$ is the sum of finitely many of the $\iota_i a_i$, proving the other direction. Hence

$$\begin{aligned} \mathbf{a} \in \mathbf{M}(\alpha_{\mathbf{N}}) &\Leftrightarrow a_i \alpha_{\mathbf{N}} z_i \text{ for all } i \\ &\Leftrightarrow \iota_i d(a_i, z_i, z_i), \in N \text{ for all } i \\ &\Leftrightarrow \iota_i a_i \in \mathbf{N} \text{ for all } i \\ &\Leftrightarrow \mathbf{a} \in \mathbf{N}. \end{aligned}$$

This completes the proof. □

The behavior of the above isomorphism on finitely generated congruences and finitely generated submodules is developed in the exercises.

COROLLARY 9.10. *Let $\beta > 0$ be an Abelian congruence on $\mathbf{A}$ and let $\gamma \in \mathbf{Con}\ \mathbf{A}$ satisfy $\beta \leq \gamma \leq (0 : \beta)$. Let z_i, $i < \lambda$, be elements of $\mathbf{A}$ such that each γ–class contains at least one z_i.*

(i) *If β is a minimal congruence, then $\sum \mathbf{M}(\beta, z_i)$ is simple as an $\mathbf{R}(\mathcal{V}, \lambda)$–module.*

(ii) *If* $\mathbf{A}$ *is subdirectly irreducible, then* $\sum \mathbf{M}(\beta, z_i)$ *is subdirectly irreducible as an* $\mathbf{R}(\mathcal{V}, \lambda)$*–module.*

PROPOSITION 9.11. *Suppose that* $[\alpha, \beta] = 0$ *in* $\mathbf{Con}\ \mathbf{A}$ *where* $\alpha \geq \beta$*, and* $z\ \alpha\ z'$*. Then the map* $x \mapsto d(x, z, y')$ *is an* $\mathbf{R}(\mathcal{V}, 1, \kappa)$*–module isomorphism of* $\mathbf{M}(\beta, z)$ *onto* $\mathbf{M}(\beta, z')$ *with inverse* $y \mapsto d(y, z', z)$*.*

PROOF. This follows from straightforward calculations using Proposition 5.7 Let ψ be the map given in the proposition. To see that ψ respects the ring multiplication, let $r(u, v, \mathbf{y}) \in \mathbf{R}(\mathcal{V}, 1, \kappa)$ we use v in place of v_0) and $x \in \mathbf{M}(\beta, z)$ and $c_k \in \mathbf{A}$, $k < \kappa$. Then

$$\begin{aligned} r \cdot \psi(x) &= r(d(x, z, z'), z', \dots, c_k, \dots) \\ &= r(d(x, z, z'), d(z, z, z'), \dots, d(c_k, c_k, c_k), \dots) \\ &= d(r(x, z, \mathbf{c}), r(z, z, \mathbf{c}), r(z', z', \mathbf{c})) \\ &= d(r(x, z, \mathbf{c}), z, z') \\ &= \psi(r \cdot x) \end{aligned}$$

We leave the rest of the proof to the reader. □

Now we begin our study of Abelian varieties. The next result shows that the situation for Abelian varieties is much simpler than the general case. If $\mathbf{R}$ is a ring we let $\mathbf{M}_\lambda(\mathbf{R})$ denote the ring of all λ by λ matrices over $\mathbf{R}$ such that all but finitely many entries of each column are 0.

THEOREM 9.12. *Suppose that* $\mathcal{V} = \mathcal{A}$ *is an Abelian variety. Then*

$$\mathbf{R}(\mathcal{A}, \lambda, \kappa) \cong \mathbf{R}(\mathcal{A}, \lambda, 0) \tag{1}$$

$$\mathbf{R}(\mathcal{A}, \lambda, \kappa) \cong \mathbf{M}_\lambda(\mathbf{R}(\mathcal{A}, 1, \kappa + \lambda - 1)) \tag{2}$$

Consequently, $\mathbf{R}(\mathcal{V}, \lambda, \kappa) \cong \mathbf{M}_\lambda \mathbf{R}(\mathcal{A}, 1, 0)$.

PROOF. Since $\mathcal{A}$ is Abelian, $[\theta_i, \theta_i] = 0$, and so $\bar{H}_{ij} = H_{ij}$. As usual let $X = \{u\} \cup \{v_i : i < \lambda\} \cup \{y_k : k < \kappa\}$ and let $X_0 = \{u\} \cup \{v_i : i < \lambda\}$. Recall that H^0_{ij}, which we defined before Lemma 9.8, is defined just as H_{ij} except that we use $\mathbf{F}_\mathcal{A}(X_0)$ instead of $\mathbf{F}_\mathcal{A}(X)$. There is an obvious embedding of H^0_{ij} into H_{ij}. To see that this embedding is onto let $r(u, \mathbf{v}, \mathbf{y}) \in H_{ij}$ and let $s(u, \mathbf{v}) = r(u, \mathbf{v}, \mathbf{v}_0)$ where $\mathbf{v}_0$ is the vector of all v_0's. (More formally s is the image of r under the endomorphism sending each y_k to v_0). Note $s(u, \mathbf{v}) \in H^0_{ij}$, since $r(v_i, \mathbf{v}, \mathbf{y}) = v_j = s(v_i, \mathbf{v}) = r(v_i, \mathbf{v}, \mathbf{v}_0)$. Since the term condition holds universally in $\mathcal{A}$, this last equation implies $r(u, \mathbf{v}, \mathbf{y}) = r(u, \mathbf{v}, \mathbf{v}_0) = s(u, \mathbf{v})$, showing $H^0_{ij} = H_{ij}$. It is easy to see that these embeddings may be combined to give a ring isomorphism which proves (1).

To see (2), fix i and consider the map $\psi_{kj} : \mathbf{M}(\theta_i, v_k) \to \mathbf{M}(\theta_i, v_j)$ given by $\psi_{kj}(x) = d(x, v_k, v_j)$. Since $[\theta_i, 1] = 0$, Proposition 9.11 implies that ψ_{kj} is a isomorphism with inverse ψ_{jk}. Now if $r(u, \mathbf{v}, \mathbf{y}) \in H_{ij}$, then $r^*(u, \mathbf{v}, \mathbf{y}) = \psi_{j0}(r(\psi_{0i}), \mathbf{v}, \mathbf{y}))$ is in H_{00} since $r^*(v_0, \mathbf{v}, \mathbf{y}) = v_0$. Note that we have the isomorphism $H_{00} \cong \mathbf{R}(\mathcal{A}, 1, \kappa + \lambda - 1)$ by treating v_i, $1 \leq i < \lambda$, as "y variables". Now if $(r_{ij}) \in \mathbf{R}(\mathcal{A}, \lambda, \kappa)$, map (r_{ij}) to $(r^*_{ij}) \in \mathbf{M}_\lambda(\mathbf{R}(\mathcal{A}, 1, \kappa + \lambda - 1))$. Using Proposition 9.11, one can easily verify that this map is one-to-one and onto. To see that it is a homomorphism one needs to show that if r, $t \in H_{ij}$, and $s \in H_{jk}$, then $(r + t)^* = r^* + t^*$, and $(s \cdot r)^* = s^* \cdot r^*$. Then, using Proposition 9.11, and suppressing all but the first variable we have

$$\begin{aligned}(r + t)^* &= (d(r(u), v_j, t(u))^* \\ &= \psi_{j0} d(r(\psi_{0i} u), v_j, t(\psi_{0i} u)) \\ &= d(\psi_{j0} r(\psi_{0i} u), \psi_{j0} v_j, t(\psi_{0i} u)) \\ &= d(\psi_{j0} r(\psi_{0i} u), v_0, \psi_{i0} t(\psi_{0i} u)) \\ &= r^* + t^*\end{aligned}$$

and

$$\begin{aligned}(s \cdot r)^* &= \psi_{k0} s(r(\psi_{0i} u)) \\ &= \psi_{k0} s(\psi_{0j} \psi_{j0} r(\psi_{0i} u)) \\ &= s^* \cdot r^*\end{aligned}$$

This completes the proof. □

Theorem 9.12 shows that for an Abelian variety $\mathcal{A}$ only the ring $\mathbf{R}(\mathcal{A}, 1, 0)$ is needed. We denote this ring $\mathbf{R}(\mathcal{A})$ and call it the ring of $\mathcal{A}$. The ideas developed above can be carried much further for Abelian varieties, and we shall now discuss the Abelian case in detail. For the rest of the chapter we will be working with a fixed Abelian variety $\mathcal{A}$ and its ring $\mathbf{R} = \mathbf{R}(\mathcal{A})$. Thus $\mathbf{R} = \{r \in \mathbf{F}_{\mathcal{A}}(u, v) : r(v, v) = v\}$ with operations

$$\begin{aligned}r + s &= d(r, v, s) \\ -r &= d(v, r, v) \\ r \cdot s &= r(s(u, v), v).\end{aligned}$$

The variety of left $\mathbf{R}$–modules is denoted $\mathcal{M}(\mathbf{R})$. If $z \in \mathbf{A} \in \mathcal{A}$ and $\beta = 1_{\mathbf{A}}$ then we let $\mathbf{M}(\mathbf{A}, z)$ denote $\mathbf{M}(1_{\mathbf{A}}, z)$. The action of $\mathbf{R}$ on $\mathbf{A}$, given by (6), has the simple form

$$r \cdot a = r(a, z) \tag{8}$$

By the last proposition, the isomorphism type of this module is independent of z. When the concrete representation of this module is immaterial, we shall simply write it as $\mathbf{M}(\mathbf{A})$.

The correspondence between pairs $(\mathbf{A}, z)$ where $z \in \mathbf{A} \in \mathcal{A}$ and modules $\mathbf{M} \in \mathcal{M}(\mathbf{R})$ where $\mathbf{M} = \mathbf{M}(\mathbf{A}, z)$, is actually onto $\mathcal{M}(R)$, as we shall see. To completely specify the pair $(\mathbf{A}, z)$ we need, in general, not just the module $\mathbf{M} = \mathbf{M}(\mathbf{A}, z)$ but also a certain homomorphism of modules, $\varphi : \mathbf{J} \to \mathbf{M}$ where $\mathbf{J}$ is a module now to be defined. In fact we put $\mathbf{J} = \mathbf{M}(\mathbf{F}_{\mathcal{A}}(v), v)$, a module derived from the $\mathcal{A}$–free algebra on one generator. For $z \in \mathbf{A} \in \mathcal{A}$, we write $\varphi^{(z)}$ for the $\mathcal{A}$–homomorphism of $\mathbf{F}_{\mathcal{A}}(v)$ into $\mathbf{A}$ which carries v to z, ($\varphi^{(z)}$ is also a homomorphism of modules by formula (8).)

Here is how we can construct $\mathbf{A}$, given $\mathbf{M} = \mathbf{M}(\mathbf{A}, z)$ and $\varphi = \varphi^{(z)}$. For an arbitrary n-ary term $f(x_1, \ldots, x_n)$ for $\mathcal{A}$ we define n elements of $\mathbf{R}$:

$$t^{(j)}(u, v) = d(t(v, \ldots, v, \overset{j}{u}, v, \ldots, v), t(v, \ldots, v), v) \tag{9}$$

where $1 \leq j \leq n$. One can easily check the following, using the fact that every algebra in $\mathcal{A}$ is d-affine. For t an n-ary term operation, $\mathbf{A} \in \mathcal{A}$, and $y_1, \ldots, y_n, z \in \mathbf{A}$ we have

$$t(y_1, \ldots, y_n) = \sum_1^n t^{(j)} \cdot y_j + t(z, \ldots, z) \tag{10}$$

(expressed with operations of $\mathbf{M}(\mathbf{A}, z)$).

We can now construct an algebra $\mathbf{A}(\mathbf{M}, \varphi)$ corresponding to any $\mathbf{M} \in \mathcal{M}(\mathbf{R})$ and $\varphi \in \mathrm{Hom}(\mathbf{J}, \mathbf{M})$. We suppose that algebras in $\mathcal{A}$ are in the form $a = \langle \mathbf{A}, F_i^{\mathbf{A}}(i \in I) \rangle$ with F_i n_i-ary. Define $b_i \in \mathbf{J}$ by

$$b_i = F_i(v, \ldots, v). \tag{11}$$

For the universe of $\mathbf{A}(\mathbf{M}, \varphi)$ we take the universe of $\mathbf{M}$; and for $i \in I$, $y_1, \ldots, y_{n_i} \in \mathbf{M}$ we define

$$F_i(y_1, \ldots, y_{n_i}) = \sum_1^{n_i} F_i^{(j)} \cdot y_j + \varphi(b_i). \tag{12}$$

Then it is clear from (10), (11), (12) that, for $z \in \mathbf{A} \in \mathcal{A}$, we have $\mathbf{A} = \mathbf{A}(\mathbf{M}(\mathbf{A}, z), \varphi^{(z)})$. It is more difficult to verify that $\mathbf{A}(\mathbf{M}, \varphi) \in \mathcal{A}$ for an arbitrary pair $(\mathbf{M}, \varphi)$. The proof begins with a lemma.

LEMMA 9.13. (1) *Let* $\mathbf{A}$, $\mathbf{B} \in \mathcal{A}$, $\psi \in \mathrm{Hom}(\mathbf{A}, \mathbf{B})$ *and* $\psi(z) = z'$. *Then* $\psi \in \mathrm{Hom}(\mathbf{M}(\mathbf{A}, z), \mathbf{M}(\mathbf{B}, z'))$.

(2) *Let* $n \geq 1$ *and* $\mathbf{F}_{\mathcal{A}}(n+1) = \mathbf{F}_{\mathcal{A}}(x_1, \ldots, x_n, v)$. *Then* $\mathbf{M}(\mathbf{F}_{\mathcal{A}}(n+1), v) = \mathbf{R} \cdot x_1 \oplus \cdots \oplus \mathbf{R} \cdot x_n \oplus \mathbf{J}$ *and* $\mathbf{R} \cdot x_i$ *is the free cyclic* $\mathbf{R}$*–module.*

PROOF. The first part follows immediately from formula (8) which defines the operations on the modules derived from $\mathbf{A}$ and $\mathbf{B}$.

For the second part, we first note that any element of $\mathbf{M} = \mathbf{M}(\mathbf{F}_{\mathcal{A}}(n+1), v)$ can be written as an $\mathcal{A}$–term in $x_1, \ldots, x_n v$, and by (10)

$$\begin{aligned} t(x_1, \ldots, x_n, v) &= \sum_1^n t^{(j)} \cdot x_j + t^{(n+1)} \cdot v + t(v, \ldots, v) \\ &\in \mathbf{R} \cdot x_1 + \cdots + \mathbf{R} \cdot x_n + \mathbf{J} \end{aligned}$$

since $v = 0$ in the module $\mathbf{M}$ (i.e., since $t^{(n+1)} \cdot v = v$). To see that the sum is direct and $\mathbf{R} \cdot x_i$ is free, suppose that

$$(*) \qquad \sum_1^n r_j \cdot x_j + s(v) = v$$

in $\mathbf{M}$, with $r_j \in \mathbf{R}$, and $s(v) \in \mathbf{J}$. Let e and ℓ be the endomorphisms of $F_{\mathcal{A}}(n+1)$ satisfying $e(x_1) = x_1$, $e(x_2) = \ldots e(x_n) = e(v) = v$, $\ell(x_1) = \ell(v) = v$. By (9,13)(1) e and ℓ are endomorphisms of $\mathbf{M}$. Applying ℓ to $(*)$ we see that $s(v) = v$ and applying e to $(*)$ gives $r_1 \cdot x_1 = v$. This second relation says that $\mathcal{A}$ satisfies $r_1(x_1, v) \approx v$, i.e., $r_1 = 0$ in $\mathbf{R}$. Similarly, $r_i = 0$, $i = 2, \ldots, n$. □

LEMMA 9.14. *Let* $\mathbf{M} \in \mathcal{M}(\mathbf{R})$ *and* $\varphi \in \mathrm{Hom}(\mathbf{J}, \mathbf{M})$. *Then* $\mathbf{A}(\mathbf{M}, \varphi) \in \mathcal{A}$.

PROOF. We show that for any finite set $\{y_1, \ldots, y_m\} \subseteq \mathbf{A} = \mathbf{A}(\mathbf{M}, \varphi)$, the subalgebra $\mathbf{Sg}_{\mathbf{A}}(\{y_1, \ldots, y_m\} \cup \varphi(\mathbf{J}))$ is a homomorphic image of $\mathbf{F}_{\mathcal{A}}(m+1) = \mathbf{F}_{\mathcal{A}}(x_1, \ldots, x_m, v)$. By Lemma 9.13 there is a homomorphism of modules $\psi : \mathbf{M}(\mathbf{F}_{\mathcal{A}}(m+1), v) \to \mathbf{M}$ with $\psi(x_i) = y_i$, $1 \leq i \leq m$, and $\psi|_{\mathbf{J}} = \varphi$. We just have to check that ψ is also a homomorphism of $\mathbf{F}_{\mathcal{A}}(m+1)$ into $\mathbf{A}$. Let $i \in I$ and $u_1, \ldots, u_{n_i} \in \mathbf{F}_{\mathcal{A}}(m+1)$. Then using (10), (11), and then (12) we have

$$\begin{aligned} \psi(F_i(u_1, \ldots, u_{n_i})) &= \psi(\sum_1^{n_i} F_i^{(j)} \cdot u_j + F_i(v, \ldots, v)) \\ &= \sum_i^{n_i} F_i^{(j)} \cdot \psi(U_j) + \psi(b_i) \\ &= F_i^{(\mathbf{A})}(\psi(u_1), \ldots, \psi(u_{n_i})) \end{aligned}$$

since $\psi(b_i) = \varphi(b_i)$. □

LEMMA 9.15. *Let* $\mathbf{M} \in \mathcal{M}(R), \varphi \in \mathrm{Hom}(\mathbf{J}, \mathbf{M})$, *and* $\mathbf{A} = \mathbf{A}(\mathbf{M}, \varphi)$. *Then* $\mathbf{M} = \mathbf{M}(\mathbf{A}, 0)$ *and* $\varphi = \varphi^{(0)} : \mathbf{F}_{\mathcal{A}}(v) \to \mathbf{A}$ *where* 0 *is the zero element of* $\mathbf{M}$.

PROOF. That $\mathbf{M}$ and $\mathbf{M}(\mathbf{A}, 0)$ have the same operations as $\mathbf{R}$-modules follows from (8), and from the fact that for any a, b, $c \in \mathbf{A}$, the homomorphism $\psi : \mathbf{F}_{\mathcal{A}}(x_1, x_2, x_3, v) \to \mathbf{A}$ mapping x_1, x_2, x_3 onto a, b, c and v onto 0 is a homomorphism of $\mathbf{M}(\mathbf{F}_{\mathcal{A}}(4), v)$ into $\mathbf{M}$, as shown in the proof of Lemma 9.14. Since $\psi|_{\mathbf{F}_{\mathcal{A}}(v)} = \varphi$, it follows $\varphi = \varphi^{(0)}$. □

Our proofs of the foregoing lemmas obscure the difficult point, which was to show that in $\mathbf{A} = \mathbf{A}(\mathbf{M}, \varphi)$, $d^{(\mathbf{A})}(a, b, c) = a - b + c$ evaluated in $\mathbf{M}$. This is certainly not obvious, since d may be a complicated composition of the basic operations of $\mathcal{A}$, but it is true by Lemmas 9.14 and 9.15.

Let us now define $\mathcal{M}(\mathbf{R}, \mathbf{J})$ to be the variety whose members are all the algebras $\mathbf{B} = (\mathbf{M}, d_j)_{j \in \mathbf{J}}$ in which $\mathbf{M} \in \mathcal{M}(\mathbf{R})$ and $\varphi(j) = d_j$ defines a homomorphism of $\mathbf{J}$ into $\mathbf{M}$. It is convenient to identify each such algebra $\mathbf{B}$ with the corresponding ordered pair $(\mathbf{M}, \varphi)$. Recall the definition of the ring elements $F_i^{(j)}$ (for $i \in I$, $1 \leq j \leq n_i$). The following theorem summarizes the facts proved above, and a little more.

THEOREM 9.16. *For an Abelian variety* $\mathcal{A}$, $\mathbf{R} = \mathbf{R}(\mathcal{A})$, *and* $\mathbf{J}$ *as defined we have:*

(1) $\mathcal{A} = \{\mathbf{A}(\mathbf{M}, \varphi) : (\mathbf{M}, \varphi) \in \mathcal{M}(\mathbf{R}, \mathbf{J})\}$,
(2) $\mathbf{R}$ *is generated as a ring with identity by its elements* $\{F_i^{(j)}\}$, *and* $\mathbf{J}$ *is generated as an* $\mathbf{R}$*–module by its element* $\{b_i\}$.
(3) *For* $z \in \mathbf{A} \in \mathcal{A}$, *we have that* $(\mathbf{M}, \varphi) = (\mathbf{M}(\mathbf{A}, z), \varphi^{(z)})$ *belongs to* $\mathcal{M}(\mathbf{R}, \mathbf{J})$ *and* $\mathbf{A}(\mathbf{M}, \varphi) = \mathbf{A}$.
(4) *For* $(\mathbf{M}, \varphi) \in \mathcal{M}(\mathbf{R}, \mathbf{J})$ *we have that* $\mathbf{A} = \mathbf{A}(\mathbf{M}, \varphi)$ *belongs to* $\mathcal{A}$, *and* $\mathbf{M} = \mathbf{M}(\mathbf{A}, 0)$, *and* $\varphi = \varphi^{(0)}$.
(5) *For* $\mathbf{A} = \mathbf{A}(\mathbf{M}, \varphi)$, $\mathbf{A}' = \mathbf{A}(\mathbf{M}', \varphi')$ *and any mapping* $\psi : A \to A'$ *of sets,* ψ *is an* $\mathcal{M}(\mathbf{R}, \mathbf{J}) - -$*homomorphism if and only if* ψ *is an* $\mathcal{A}$*–homomorphism and* $\psi(0) = 0'$.
(6) $\mathbf{F}_{\mathcal{A}}(k+1) \cong \mathbf{A}(\mathbf{R}^{(k)} \oplus \mathbf{J}, \iota)$ *with* ι *the inclusion map, for any cardinal* $k \geq 0$.
(7) $\mathcal{A} = \mathcal{V}(\mathbf{F}_{\mathcal{A}}(2))$.

PROOF. All parts except (2) and (7) are obvious from Lemma 9.13, Lemma 9.14, and Lemma 9.15 and their proofs. We leave (2) and (7) to the reader. Note that in (7), what is to be proved is that any identity $s(x_1, \ldots, x_n) \approx t(x_1, \ldots, x_n)$ which fails to hold in $\mathcal{A}$ is refuted in some algebra of $\mathcal{A}$ generated by two elements. The proof uses the affine representations of s and t given by (10). □

REMARK 9.17. The theorem can be viewed as stating the definitional equivalence of the variety $\mathcal{M}(\mathbf{R}, \mathbf{J})$ with the variety $\mathcal{A}_{(1)}$ of pointed $\mathcal{A}$-algebras, i.e., algebras $(\mathbf{A}, z)$ where $\mathbf{A} \in \mathcal{A}$ and z is an arbitrary element of $\mathbf{A}$. The operations of the corresponding algebras under this definitional equivalence, $(\mathbf{M}, \varphi)$ and $(\mathbf{A}(\mathbf{M}, \varphi), 0)$, are uniformly interdefinable by terms, those of the one algebra from those of the other. We note that $\mathcal{M}(\mathbf{R})$ is essentially the class $\{(\mathbf{M}, \varphi) : \varphi \equiv 0\}$ and thus is contained in $\mathcal{A}$, in a sense (see the comments below). $\mathcal{A}$ is definitionally equivalent with $\mathcal{M}(\mathbf{R})$ if and only if $\mathcal{A}$ has a constant term $t(x)$, i.e., $t(x) \approx t(y)$ holds in $\mathcal{A}$, whose value is an idempotent element in every algebra of $\mathcal{A}$.

We have seen that any Abelian variety $\mathcal{A}$ determines a system $\sigma(\mathcal{A}) = (\mathbf{R}, \mathbf{J}, F_i^{(j)}, b_j)_{i \in I, j \leq n_i}$ where $\{F_i^{(j)}\}$ generates $\mathbf{R}$ as a ring and $\{b_i\}$ generates $\mathbf{J}$ as an $\mathbf{R}$-module. Conversely, $\mathcal{A}$ is completely determined by $\sigma(\mathcal{A}) = \sigma$, i.e., $\mathcal{A} = \mathcal{A}(\sigma)$. It would probably be worthwhile to study the conditions under which an arbitrary system $(\mathbf{R}, \mathbf{J}, \mathbf{F}, \mathbf{b}) = \sigma$ will determine a modular Abelian variety $\mathcal{A}(\sigma)$ via the definitions (12). [Note that $\mathcal{A}(\sigma) = \{\mathbf{A}(\mathbf{M}, \varphi) : (\mathbf{M}, \varphi) \in \mathcal{M}(\mathbf{R}, \mathbf{J})\}$, defined by (12), will not always be a variety.] We have not studied this question, although it is the natural first step in generating and classifying all possible Abelian varieties.

We close this section with some observations that have been useful in applications. Let $\mathcal{A}$, $\mathbf{R}$, and $\mathbf{J}$ be as in theorem 9.16. The zero map $\varphi(j) \equiv 0$ of J into any module will be denoted by 0. Call an algebra $\mathbf{A} \in \mathcal{A}$ *linear* if $\mathbf{A} = \mathbf{A}(\mathbf{M}, 0)$ for some $\mathbf{M}$. This condition is obviously equivalent to: $\mathbf{A}$ has a one element subalgebra $\{e\}$, i.e., an idempotent element e (for then we can take $\mathbf{M} = \mathbf{M}(\mathbf{A}, e)$ and we have $\varphi^{(e)} = 0$). The class of linear algebras in $\mathcal{A}$ need not be a variety. (For an interesting case in which it is, see Theorem 12.4.)

There are two ways to construct a linear algebra from a given $\mathbf{A} \in \mathcal{A}$, and they give the same result, up to isomorphism. Recall the definition of $\Delta_{1,1}$ given in Chapter 4. We define the linearization of $\mathbf{A}$ to be $\mathbf{A}_\nabla = \mathbf{A}^2/\Delta_{1,1}$.

PROPOSITION 9.18. *Let $\mathbf{A} \in \mathcal{A}$ where $\mathcal{A}$ is an Abelian variety. Then*

(i) *For any $z \in \mathbf{A}$, $\mathbf{A}_\nabla \cong \mathbf{A}(\mathbf{M}(\mathbf{A}, z), 0)$, thus it is linear.*
(ii) $\mathbf{A} \times \mathbf{A}_\nabla \cong \mathbf{A} \times \mathbf{A}$.

PROOF. From the proof of Proposition 5.7 we have $\langle x, y \rangle \; \Delta_{1,1} \; \langle u, v \rangle$ if and only if $v = d(y, x, u)$ if and only if $v - u = y - x$ in one (equivalently all) of the modules $\mathbf{M}(\mathbf{A}, z)$. Now the map which sends $\langle x, \langle y, z \rangle \rangle$

to $\langle x, d(x,y,z)\rangle$ is a homomorphism of $\mathbf{A}\times\mathbf{A}^2$ onto $\mathbf{A}^2$ and its kernel is precisely $0_{\mathbf{A}}\times\Delta_{1,1}$, hence we have (ii).

For (i) we have $\mathbf{A}=\mathbf{A}(\mathbf{M}(\mathbf{A},z),\varphi^{(z)})$ and so the map $\langle x,y\rangle\mapsto d(y,x,z)$ is easily seen to be a homomorphism of $\mathbf{A}^2$ onto $\mathbf{A}(\mathbf{M}(\mathbf{A},z),0)$. The kernel of this homomorphism is $\Delta_{1,1}$. □

PROPOSITION 9.19. *Let $z\in\mathbf{A}\in\mathcal{A}$ where $\mathcal{A}$ is an Abelian variety.*

(i) $\mathbf{Con}\ \mathbf{A}=\mathbf{Con}(\mathbf{M}(\mathbf{A},z))$,

(ii) *If $\mathbf{A}$ is simple, then it has no proper subalgebras except one element subalgebras.*

PROOF. $\mathbf{A}$ and $\mathbf{M}(\mathbf{A},z)$ have the same polynomial operations, hence the same congruences. If $\mathbf{S}$ is any subalgebra of $\mathbf{A}$ and $s_0\in\mathbf{S}$, then $\{\langle x,y\rangle : d(x,y,z_0)\in\mathbf{S}\}=\theta$ is a congruence of $\mathbf{A}$ and $s_0/\theta=\mathbf{S}$. □

Exercises

1. Let $(A,\cdot,/,\backslash)$ be a quasigroup. Show that $\mathbf{A}$ satisfies the identity $(x\cdot y)\cdot(u\cdot v)=(z\cdot u)\cdot(y\cdot v)$ if and only if $\mathbf{A}$ is Abelian and $\mathbf{R}(\mathcal{V}(\mathbf{A}))$ is commutative. For an arbitrary algebra $\mathbf{A}$ in a modular variety show that $\mathbf{A}$ is Abelian and $\mathbf{R}(\mathcal{V}(\mathbf{A}))$ is commutative if and only if $\mathcal{V}(\mathbf{A})$ is permutable and every basic operation of $\mathbf{A}$ commutes with every idempotent term operation of $\mathbf{A}$.

2. Show that if $\mathcal{V}$ is the variety of quasigroups then $\mathbf{R}(\mathcal{V})$ is not commutative.

3. Let $\beta>0$ in $\mathbf{Con}\ \mathbf{A}$, $\mathbf{A}\in\mathcal{A}$, and suppose that β is an Abelian congruence. Let z_i, $\mathrm{i}<\lambda$, be a system of representatives for the β-classes and let $\mathbf{R}=\mathbf{R}(\mathcal{V},\lambda)$. By Corollary 9.10 $\mathbf{M}(\beta)$ is a simple $\mathbf{R}$–module. Let $\mathbf{D}$ be the endomorphism ring of $\mathbf{M}(\beta)$ as an $\mathbf{R}$–module. Then show that $\mathbf{D}$ is a division ring and each $\mathbf{M}(\beta,z_i)$ is a $\mathbf{D}$-subspace of $\mathbf{M}(\beta)$. Moreover, show that if $a_1,\dots,a_n$ is a finite set of $\mathbf{D}$-linearly independent elements of $\mathbf{M}(\beta,z_i)$ and $b_1,\dots,b_n\in\mathbf{M}(\beta,z_j)$ then there is a $g\in\mathrm{Hom}(\beta,z_i,z_j)$ with $g(a_k)=b_k$, $k=1,\dots,n$. If $\mathbf{A}$ is finite show there is a fixed prime p such that each β-block has order p^i for some i with i but not p depending on the block.

4. Suppose that α/β and γ/δ are projective quotients in $\mathbf{Con}\ \mathbf{A}$. Then the centralizer of α over β equals the centralizer of γ over δ, i.e.,

$$(\beta:\alpha)=(\delta:\gamma).$$

Suppose in addition that $[\alpha, \alpha] \leq \beta$ and $[\gamma, \gamma] \leq \delta$ and let $\varphi = (\beta : \alpha) = (\delta : \gamma)$. Let z_i, $i < \lambda$, be a system of representatives of the φ classes of A. Let $\mathbf{M}(\alpha/\beta, z_i)$ denote $\mathbf{M}_{\mathbf{A}/\beta}(\alpha/\beta, z_i/\beta)$. Prove that $\sum_i \mathbf{M}(\alpha/\beta, z_i) \cong \sum_i \mathbf{M}(\gamma/\delta, z_i)$ as $\mathbf{R}(\mathcal{V}, \lambda)$–modules. This can be viewed as a version of the second isomorphism theorem.

5. Consider the situation of Theorem 9.9. Show that, under the lattice isomorphism of $\beta/0$ onto the submodule lattice of $\sum \mathbf{M}(\beta, z_i)$ given in the proof of that theorem, principal congruences contained in β map to cyclic submodules. Hence n-generated congruences are mapped to n-generated modules.

6. Let β be an Abelian congruence on $\mathbf{A}$, $\gamma = (0 : \beta)$, and let $z_i \in \mathbf{A}$, $i < \lambda$ represent all the classes of γ. Let $c_k \in \mathbf{A}$, $k < \kappa$. Let $X_0 = \{u\} \cup \{v_i : i < \lambda\}$, and $X = X_0 \cup \{y_k : k < \kappa\}$. Show that the map $\sigma : X \to X_0$ which fixes the elements of X_0 and maps $y_k \mapsto v_i$, where i is the first index with $c_k \; \gamma \; z_i$, induces a ring homomorphism of $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$ onto $\mathbf{R}(\mathcal{V}, \lambda)$ $(= \mathbf{R}(\mathcal{V}, \lambda, 0))$. Show that the kernel of this homomorphism is contained in the kernel of the action of $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$ on $\sum \mathbf{M}(\beta, z_i)$.

7. Let β be an Abelian congruence on $\mathbf{A} \in \mathcal{V}$ and let $\gamma = (0 : \beta)$. Suppose z_i, z'_i, $i \in I$, are elements of $\mathbf{A}$ such that $z_i \; \gamma \; z'_i$. Show that $\sum \mathbf{M}(\beta, z_i)$ and $\sum \mathbf{M}(\beta, z'_i)$ are isomorphic as $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$–modules, for any choice of constants $c_k \in \mathbf{A}$, $k < \kappa$.

CHAPTER 10

Structure and Representation in Modular Varieties

We begin with some generalizations to modular varieties of Jónsson's theorem for distributive varieties.

1. Birkhoff-Jónsson Type Theorems For Modular Varieties

Recall that the operators $\boldsymbol{H}$, $\boldsymbol{S}$, $\boldsymbol{P}$, $\boldsymbol{P}_s$, and $\boldsymbol{P}_u$ are the closures under homomorphic images, subalgebras, direct products, subdirect products, and ultraproducts, respectively. We understand these in the inclusive sense so that $\boldsymbol{S}(\mathcal{K})$, for instance, includes all isomorphic copies of its members. Garrett Birkhoff's theorem that $\boldsymbol{HSP}(\mathcal{K})$ is identical with the variety generated by $\mathcal{K}$ (when $\mathcal{K}$ is a class of similar algebras) was strengthened by Bjarni Jónsson [**54**] for the case that $\boldsymbol{V}(\mathcal{K})$ is distributive, to read $\boldsymbol{V}(\mathcal{K}) = \boldsymbol{P}_s\boldsymbol{HSP}_u(\mathcal{K})$, i.e., every subdirectly irreducible algebra in $\boldsymbol{V}(\mathcal{K})$ is a homomorphic image of a subalgebra of an ultraproduct of algebra in $\mathcal{K}$. This theorem has had a profound influence in shaping the themes and emphasis of subsequent research on varieties.

Under the weaker assumption of modularity. Jónsson's theorem is not true. The following theorem, however, does generalize Jónsson's theorem to modular varieties. It represents the combined work of Hagemann, Herrmann, Freese, McKenzie, and Hrushovskii. Recall that the monolith of a subdirectly irreducible algebra is its least nontrivial congruence μ and that the centralizer (or annihilator) of μ is the largest congruence α with $[\mu, \alpha] = 0$, i.e., $\alpha = (0 : \mu)$. In particular if μ is non-Abelian then $\alpha = 0$.

THEOREM 10.1. *Suppose that $\boldsymbol{V}(\mathcal{K})$ is modular. If $\mathbf{B} \in \boldsymbol{V}(\mathcal{K})$ is subdirectly irreducible and α is the centralizer of the monolith of $\mathbf{B}$, then $\mathbf{B}/\alpha \in \boldsymbol{HSP}_u(\mathcal{K})$. Moreover, if $\boldsymbol{V}(\mathcal{K})$ is locally finite, then $\mathbf{B}/\gamma \in \boldsymbol{SP}_u\boldsymbol{HS}(\mathcal{K})$ for some $\gamma \leq \alpha$.*

Note that if $\boldsymbol{V}(\mathcal{K})$ is distributive then $\alpha = 0$ and we obtain Jónsson's Theorem. Also note that the theorem implies that either $\mathbf{B}$ has an Abelian monolith or $\mathbf{B} \in \boldsymbol{HSP}_u(\mathcal{K})$.

PROOF. By Birkhoff's theorem that $\boldsymbol{V}(\mathcal{K}) = \boldsymbol{HSP}(\mathcal{K})$, we may assume that $\mathbf{B} = \mathbf{C}/\theta$ where $\mathbf{C} \subseteq \prod_{i\in I} \mathbf{A}_i$, $\mathbf{A}_i \in \mathcal{K}$. For $J \subseteq I$, let η_J be the kernel of the natural map from $\mathbf{C}$ to $\prod_{i\in J} \mathbf{A}_i$. Note that $\eta_J \wedge \eta_K = \eta_{J\cup K}$ and that $J \subseteq K$ implies $\eta_J \geq \eta_K$. Since $\mathbf{B}$ is subdirectly irreducible, θ is uniquely covered by a congruence ψ. If we let $\varphi = (\theta : \psi)$, then $\mathbf{B}/\alpha \cong \mathbf{C}/\varphi$ by Proposition 4.4 and Remark 4.6.

If $\beta, \gamma \in \mathbf{Con}\ \mathbf{C}$, then

$$\beta \wedge \gamma \leq \theta \qquad \text{implies either}$$
$$\beta \leq \theta \text{ or } \gamma \leq \theta \quad \text{or both} \quad \beta \leq \varphi \text{ and } \gamma \leq \varphi.$$

For suppose $\beta \wedge \gamma \leq \theta$, $\beta \not\leq \theta$, and $\gamma \not\leq \theta$. Then $\beta \vee \theta \geq \psi$ and hence $[\gamma, \psi] \leq [\gamma, \beta \vee \theta] = [\gamma, \beta] \vee [\gamma, \theta] \leq (\gamma \wedge \beta) \vee \theta = \theta$. Hence $\gamma \leq \varphi$. Similarly $\beta \leq \varphi$.

Let $\mathcal{F}$ be a filter on I maximal with respect to the property $J \in \mathcal{F}$ implies $\eta_J \leq \theta$. Let $\mathcal{U}$ be an ultrafilter extending $\mathcal{F}$. We claim that $J \in \mathcal{U}$ implies $\eta_J \leq \varphi$. This is clear if $J \in \mathcal{F}$, so assume $J \in \mathcal{U} - \mathcal{F}$. By the maximality of $\mathcal{F}$ neither J nor its complement J' can be adjoined to $\mathcal{F}$. This implies that there is a $K \in \mathcal{F}$ such that $\eta_{J\cap K} \not\leq \theta$ and $\eta_{J'\cap K} \not\leq \theta$. Now $\eta_{J\cap K} \wedge \eta_{J'\cap K} = \eta_K \leq \theta$. Hence by what we have shown above, $\eta_{J\cap K} \leq \varphi$. But $\eta_J \leq \eta_{J\cap K}$, so the claim is proved.

Let $\eta_{\mathcal{U}} \in \mathbf{Con}\ \mathbf{C}$ be the restriction of the ultraproduct congruence on $\prod_I \mathbf{A}_i$ to $\mathbf{C}$. Then $\mathbf{C}/\eta_{\mathcal{U}}$ is a subalgebra of the ultraproduct of $\prod_I \mathbf{A}_i$ by $\mathcal{U}$. It follows from the claim that $\eta_{\mathcal{U}} \leq \varphi$ so that $\mathbf{B}/\alpha \cong \mathbf{C}/\varphi \in \boldsymbol{HSP}_u(\mathcal{K})$.

In order to prove the last statement of the theorem we need a lemma shown to us by J. B. Nation.

LEMMA 10.2. *If $\mathbf{B}$ is a subdirectly irreducible algebra, then $\mathbf{B}$ is a subalgebra of an ultraproduct of a family $\mathbf{B}_i$, $i \in I$, of finitely generated, subdirectly irreducible algebras from $\boldsymbol{HS}(\mathbf{B})$. Moreover, if μ_i is the monolith of $\mathbf{B}_i$ and μ is the ultraproduct congruence determined by the μ_i, then μ restricted to $\mathbf{B}$ is nonzero.*

PROOF. Let $\mathrm{Cg}(a, b)$ be the monolith of $\mathbf{B}$. Let $\mathcal{S}$ be the collection of all finite subsets of B which contain a and b. For $S \in \mathcal{S}$ let $\psi_S \in \mathbf{Con}\ \mathbf{Sg}(S)$ be a maximal congruence not containing $\langle a, b\rangle$. Let $\mathcal{F}$ be the filter on $\mathcal{S}$ consisting of all $\mathcal{T} \subseteq \mathcal{S}$ such that there is an $S_0 \in \mathcal{S}$ with $\{S : S \supseteq S_0\} \subseteq \mathcal{T}$. Let $\mathcal{U}$ be an ultrafilter extending $\mathcal{F}$. Let $\mathbf{D} = \prod_{\mathcal{S}} \mathbf{Sg}(S)/\psi_S$. Let $\varphi : \mathbf{B} \to \mathbf{D}$ be given by $\varphi(x)_S = x/\psi_S$ if $x \in S$ and an arbitrary element of $\mathrm{Sg}(S)/\psi_S$ otherwise. Let $\mathbf{D}/\mathcal{U}$ be the ultraproduct of the $\mathbf{Sg}(S)/\psi_S$ corresponding to $\mathcal{U}$. We leave it to the reader to check that the composite map $\bar{\varphi} : \mathbf{B} \to \mathbf{D}/\mathcal{U}$ is a homomorphism. It is an embedding because $\bar{\varphi}(a) \neq \bar{\varphi}(b)$. The last

part of the lemma follows from the fact that $\langle \bar{\varphi}(a), \bar{\varphi}(b) \rangle$ is in the ultraproduct congruence determined by the monoliths of the factors. □

Returning to the proof of the theorem, suppose that $\boldsymbol{V}(\mathcal{K})$ is locally finite and $\mathbf{B} \in \boldsymbol{V}(\mathcal{K})$ is subdirectly irreducible. By the lemma, $\mathbf{B}$ is a subalgebra of an ultraproduct $(\prod \mathbf{B}_i)/\mathcal{U}$ of finite subdirectly irreducible algebras $\mathbf{B}_i$ in $\boldsymbol{V}(\mathcal{K})$. Let α_i be the centralizer of the monolith μ_i of $\mathbf{B}_i$. By the first part of the theorem, $\mathbf{B}_i/\alpha_i \in \boldsymbol{HSP}_u(\mathcal{K})$. Since $\mathbf{B}_i$ is finite and $\boldsymbol{V}(\mathcal{K})$ is locally finite, this implies $\mathbf{B}_i/\alpha_i \in \boldsymbol{HS}(\mathcal{K})$, because $\mathbf{B}_i$ is a homomorphic image of a finite free algebra in $\boldsymbol{V}(\mathcal{K})$ and thus there is a finite subset $\mathcal{K}_1 \subseteq \boldsymbol{S}(\mathcal{K})$ of finite algebras with $\mathbf{B}_1 \in \boldsymbol{V}(\mathcal{K}_1)$.

Let $\bar{\alpha} = (\Pi\alpha_i)/\mathcal{U}$ and $\bar{\mu} = (\Pi\mu_i)/\mathcal{U} \in \mathbf{Con}(\Pi\mathbf{B}_i/\mathcal{U})$ be the corresponding ultraproduct congruences. Using our syntactic definition Definition 3.2 of the commutator, it is easy to see that $[\bar{\alpha}, \bar{\mu}] = 0$ in $\mathbf{Con}(\Pi\mathbf{B}_i/\mathcal{U})$. Let γ be the restriction of $\bar{\alpha}$ and β be the restriction of $\bar{\mu}$ to B. By the lemma $\beta > 0$ and so $\beta \geq \mu$. By Proposition 4.4(2), $[\beta, \gamma] = 0$ in $\mathbf{Con}\ \mathbf{B}$. Thus $\gamma \leq \alpha$. Moreover, $\mathbf{B}/\gamma \in \boldsymbol{SP}_u\, \boldsymbol{HS}(\mathcal{K})$. □

For distributive, locally finite varieties Theorem 10.1 gives a strengthening of Jónsson's theorem. Explicitly we have:

COROLLARY 10.3. *Let $\boldsymbol{V}(\mathcal{K})$ be distributive and locally finite. If $\mathbf{A} \in \boldsymbol{V}(\mathcal{K})$ is subdirectly irreducible, then $\mathbf{A} \in \boldsymbol{SP}_u\, \boldsymbol{HS}(\mathcal{K})$.*

REMARK 10.4.

(1) Let $\mathbf{A}$ be finite and let $\mathbf{B} \in V(\mathbf{A})$ be subdirectly irreducible with monolith μ and $\alpha = (0 : \mu)$ its centralizer. Theorem 10.1 gives the following. If $|B| > |A|$, then $\alpha \geq \mu$ and by Proposition 9.11, there are at most $|A|$ isomorphism types of modules among the $M(\mu, x), x \in B$. Also, each of these modules has size at most $|A|$ by Theorem 10.16 to follow. This situation will be investigated more thoroughly in the next section.

(2) The following example shows that $\mathbf{B}/\gamma \in SP_u\, \boldsymbol{HS}(\mathcal{K})$ requires local finiteness (or some similar assumption), in both Theorem 10.1 and Corollary 10.3. Take $\mathcal{K}$ to be all finite semidistributive lattices. These include all splitting lattices and so by a result of A. Day [**21**], $\boldsymbol{V}(\mathcal{K})$ is the variety of all lattices. Hence by Jónsson's Lemma $\boldsymbol{HSP}_u(\mathcal{K})$ contains all subdirectly irreducible lattices. Clearly $\boldsymbol{S}(\mathcal{K}) = \mathcal{K}$ and since the members of $\mathcal{K}$ are finite, $\boldsymbol{H}(\mathcal{K}) = \mathcal{K}$ also. Thus $\boldsymbol{SP}_u\, \boldsymbol{HS}(\mathcal{K}) = \boldsymbol{SP}_u(\mathcal{K})$. The latter class is clearly contained in the class of semidistributive lattices. But obviously there are subdirectly lattices

which are not semidistributive. Hence $\boldsymbol{SP}_u\boldsymbol{HS}(\mathcal{K})$ is properly contained in $\boldsymbol{HSP}_u(\mathcal{K})$.

The next theorem is a nice application of Theorem 10.1.

THEOREM 10.5. *Suppose that* $\mathbf{B} \in \boldsymbol{V}(\mathcal{K})$, *where* $\boldsymbol{V}(\mathcal{K})$ *is modular. If* $\mathbf{Con}\ \mathbf{B}$ *has finite length (in particular if* $\mathbf{B}$ *is finite) then* $\mathbf{B}$ *has a nilpotent congruence* θ *such that* $\mathbf{B}/\theta$ *is a subdirect product of algebras in* $\boldsymbol{HSP}_u(\mathcal{K})$.

PROOF. Let $\varphi = \bigwedge_{\beta<\alpha}(\beta : \alpha)$ be the intersection of all the centralizers of the prime quotients of $\mathbf{Con}\ \mathbf{B}$. If $0 \neq \gamma \in \mathbf{Con}\ \mathbf{B}$ is arbitrary then since $\mathbf{Con}\ \mathbf{B}$ has finite length, there is a $\delta < \gamma$. By definition $[\varphi, \gamma] \leq \delta$. Hence for any $\gamma \neq 0, [\varphi, \gamma] < \gamma$. It follows immediately from this and the finite length of $\mathbf{Con}\ \mathbf{B}$ that φ is nilpotent. (In fact it is easy to see that φ is the largest nilpotent congruence, *cf.* Exercise 6.4.) Now let $\beta < \alpha$ and let δ be a completely meet irreducible congruence with $\delta \geq \beta$ but $\delta \not\geq \alpha$. Let $\gamma = \alpha \vee \delta$. Then $\alpha/\beta \nearrow \gamma/\delta$. By Exercise 9.4 $(\beta : \alpha) = (\delta : \gamma)$ and by Theorem 10.1 $\mathbf{B}/(\delta : \gamma) \in \boldsymbol{HSP}_u(\mathcal{K})$. Since φ is the intersection of such congruences, the theorem follows. □

As we mentioned above, φ is the largest nilpotent congruence. It is called the **Fitting congruence** in analogy to group theory. Notice that even without the assumption that $\mathbf{Con}\ \mathbf{B}$ has finite length we obtain a congruence φ with $\mathbf{B}/\varphi$ a subdirect product of algebras in $\boldsymbol{HSP}_u(\mathcal{K})$ and $[\varphi, \gamma] \leq \delta$ whenever $\gamma > \delta$. You are asked to prove a slightly stronger result in Exercise 1.

2. Subdirectly Irreducible Algebras in Finitely Generated Varieties

In this section we strengthen the results of the last section in the case $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$, $\mathbf{A}$ finite. We begin with the concept of similarity.

Let θ be an Abelian congruence on an algebra $\mathbf{A} \in \mathcal{V}$ and let α be its centralizer, i.e., $\alpha = (0 : \theta)$. Let z_1, $i < \lambda$, be a set of distinct representatives of the α–classes. Recall the definition of the matrix ring $\mathbf{R}(\mathcal{V}, \lambda) = \mathbf{R}(\mathcal{V}, \lambda, 0)$ (Definition 9.3) and of the modules $\mathbf{M}(\theta, z_i)$. As pointed out in Chapter 9, $\sum_{i<\lambda} \mathbf{M}(\theta, z_i)$ is an $\mathbf{R}(\mathcal{V}, \lambda)$–module.

DEFINITION 10.6. Let $\theta \in \mathbf{Con}\ \mathbf{A}$ and $\psi \in \mathbf{Con}\ \mathbf{B}$ be Abelian congruences with centralizers α and β, respectively. We say that θ **in** $\mathbf{A}$ **is similar to** ψ **in** $\mathbf{B}$ if the following two conditions hold. First the is an isomorphism $\sigma : \mathbf{A}/\alpha \to \mathbf{B}/\beta$. Let z_i, and w_i, $i < \lambda$, be a systems of distinct representatives of the α–classes of $\mathbf{A}$ and the β–classes of $\mathbf{B}$, respectively, indexed so that $\sigma(z_i/\alpha) = w_i/\beta$. The second

condition is that $\sum_{i<\lambda} \mathbf{M}(\theta, z_i)$ and $\sum_{i<\lambda} \mathbf{M}(\psi, w_i)$ are isomorphic as $\mathbf{R}(\mathcal{V}, \lambda)$–modules.

DEFINITION 10.7. Subdirectly irreducible algebras $\mathbf{A}$ and $\mathbf{B}$ and said to be **similar** if they are isomorphic or both have Abelian monoliths and $\mu_{\mathbf{A}}$ in $\mathbf{A}$ is similar to $\mu_{\mathbf{B}}$ in $\mathbf{B}$. We denote this by $\mathbf{A} \sim \mathbf{B}$.

Notice that if $\mathbf{A}$ and $\mathbf{B}$ are similar with Abelian monoliths, then the Abelian groups determined by the blocks of the respective monoliths are isomorphic if these blocks lie in corresponding blocks of the centralizers. This follows easily from the fact that $\sum \mathbf{M}(\theta, z_i)$ is isomorphic to $\sum \mathbf{M}(\psi, w_i)$. The main result of this section shows that if $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$ is subdirectly irreducible and $\mathbf{A}$ is finite, then $\mathbf{B}$ is similar to an algebra in $\boldsymbol{HS}(\mathbf{A})$. Notice that this is considerably stronger than Theorem 10.1.

The next theorem gives a useful lattice-theoretic characterization of similarity.

THEOREM 10.8. *Let $\mathbf{A}$ and $\mathbf{B}$ be subdirectly irreducible algebras in a modular variety $\mathcal{V}$. Then $\mathbf{A} \sim \mathbf{B}$ if and only if there is an algebra $\mathbf{C} \in \mathcal{V}$ and γ, δ, η, $\epsilon \in \mathbf{Con}\ \mathbf{C}$, η and ϵ completely meet irreducible (with upper covers η^* and ϵ^*, such that $\mathbf{A} \cong \mathbf{C}/\eta$, $\mathbf{B} \cong \mathbf{C}/\epsilon$, and*

$$\eta^*/\eta \searrow \gamma/\delta \nearrow \epsilon^*/\epsilon.$$

Moreover, if $\mathbf{A} \sim \mathbf{B}$ then such a $\mathbf{C}$ can be taken to be a subdirect product of $\mathbf{A}$ and $\mathbf{B}$ with η and ϵ as the projection kernels.

PROOF. Let $\mathbf{A}$ and $\mathbf{B}$ have monoliths μ and ν with centralizers α and β, respectively. Suppose $\mathbf{C}$ and γ, δ, η, and ϵ are as described in the theorem. That $\mathbf{A}$ is similar to $\mathbf{B}$ is precisely the content of Exercise 4.

Now assume $\mathbf{A} \sim \mathbf{B}$. The case $\mathbf{A} \cong \mathbf{B}$ is easy so we assume μ and ν are Abelian and thus $\alpha \geq \mu$ and $\beta \geq \nu$. Let z_i, w_i, $i < \lambda$, be as in the definition of similarity. Let τ be a $\mathbf{R}(\mathcal{V}, \lambda)$ isomorphism of $\sum_{i<\lambda} \mathbf{M}(\mu, z_i)$ onto $\sum_{i<\lambda} \mathbf{M}(\nu, w_i)$ and let τ_i be its restriction to $\mathbf{M}(\mu, z_i)$. Since τ is a $\mathbf{R}(\mathcal{V}, \lambda)$ isomorphism, τ_i is an $\mathbf{R}(\mathcal{V}, 1)$ isomorphism of $\mathbf{M}(\mu, z_i)$ onto $\mathbf{M}(\nu, w_i)$.

Let $\mathbf{D} = \mathbf{A}/\lambda$ and let h be the natural map of $\mathbf{A}$ onto $\mathbf{D}$ and let $k : \mathbf{B} \to \mathbf{D}$ with $\ker k = \beta$. We may assume that $h(z_i) = k(w_i)$. Let $\mathbf{C}$ be the subalgebra of $\mathbf{A} \times \mathbf{B}$ with universe $C = \{(x, y) \in A \times B : h(x) = k(y)\}$.

Define $\gamma \in \operatorname{Con} \mathbf{C}$ by $(a, b)\ \gamma\ (a', b')$ if $a\ \mu\ a'$, $b\ \nu\ b'$, and $\tau_i(d(a', a, z_i)) = d(b', b, w_i)$ where i is the index with $a\ \lambda\ z_i$. (Note that $b\ \beta\ w_i$ since $k(b) = h(a)$ by the definition of $\mathbf{C}$, $h(a) = h(z_i)$ as $a\ \alpha\ z_i$ and α is the

kernel of h, and $h(z_i) = k(w_i)$ by our assumption. Thus $k(b) = k(w_i)$ and, since β is the kernel of k, $b\ \beta\ w_i$.) We view $d(a', a, z_i)$ as the element of $\sum \mathbf{M}(\mu, z_i)$ whose i^{th} coordinate is $d(a', a, z_i)$ and whose other coordinates are 0. To see that γ is a congruence is just a matter of checking a few details. To see symmetry, for example, note that since τ is a module homomorphism $\tau(-x) = -\tau(x)$, i.e., $\tau(d(z_i, x, z_i)) = d(w_i, \tau(x), w_i)$, for $x \in \mathbf{M}(\mu, z_i)$. Now suppose $(a, b)\ \gamma\ (a', b')$ so that $\tau(d(a', a, z_i)) = d(b', b, w_i)$. By Proposition 5.7

$$\begin{aligned} d(z_i, d(a', a, z_i), z_i) &= d(d(a, a, z_i), d(a', a, z_i), d(a', a', z_i)) \\ &= d(d(a, a', a'), d(a, a, a'), d(z_i, z_i, z_i)) \\ &= d(a, a', z_i). \end{aligned}$$

Hence $\tau(d(a, a', z_i)) = d(b, b', w_i)$.

Let $\eta, \varepsilon \in \operatorname{Con}\mathbf{C}$ be the kernels of the projections and let η^* and ε^* be their unique upper covers. We will show that $\eta \wedge \gamma = \varepsilon \wedge \gamma = 0$. Indeed, if $(a, b)\ \eta \wedge \gamma\ (a', b')$, then $a = a'$ since η is the kernel of the first projection, and so by the definition of γ, $w_i = \tau_i = \tau_i(z_i) = \tau_i(d(a, a, z_i)) = d(b', b, w_i)$. Hence $d(b, b, w_i) = w_i = d(b, b, w_i)$. From this it follows that $b = b'$ (which follows from the term condition and the fact that $b'\ \nu\ b\ \beta\ w_i)$). Thus $\eta \wedge \gamma = 0$. Clearly $\gamma \leq \eta^* \succ \eta$ as $\langle a, b\rangle\ \gamma\ \langle a', b'\rangle$ implies $a\ \mu\ a'$ by definition. Now $\gamma \neq 0$. In fact if a, $a' \in \mathbf{M}(\mu, z_i)$ and $b \in \mathbf{M}(\nu, w_i)$ then there is a b' with $\langle a, b\rangle\ \gamma\ \langle a', b'\rangle$. Indeed, since τ is a $\mathbf{R}(\mathcal{V}, \lambda)$ isomorphism, τ restricted to $\mathbf{M}(\mu, z_i)$ maps $\mathbf{M}(\mu, z_i)$ onto $\mathbf{M}(\nu, w_i)$. Now the claim follows from Proposition 9.11 (or directly from Proposition 5.7). It follows that $\eta \vee \gamma = \eta^*$, and hence $\eta^*/\eta \searrow \gamma/0 \nearrow \eta^*/\varepsilon$. □

Definition 10.9. Let $\mathbf{A}$ be subdirectly irreducible with monolith μ and centralizer $\alpha = (0 : \mu)$. If μ is non-Abelian let $\mathrm{D}(\mathbf{A}) = \mathbf{A}$. Otherwise let $\mathrm{D}(\mathbf{A}) = \mathbf{A}(\mu)/\Delta_{\mu,\alpha'}$. (Recall that $\mathbf{A}(\mu) = \{\langle x, y\rangle \in A \times A : x\ \mu\ y\}$ and that $\Delta_{\mu,\alpha}$ is the congruence on $\mathbf{A}(\mu)$ generated by $\{\langle\langle x, x\rangle, \langle y, y\rangle\rangle : x\ \alpha\ y\}$).

Part of **Con** $\mathbf{A}(\mu)$ is shown in Figure 1.

In the case μ_A is Abelian, $\mathrm{D}(\mathbf{A})$ has two nice properties. First, the next theorem will show that in $\mathrm{D}(\mathbf{A})$, $\mu = \alpha$. Secondly, $\mathrm{D}(\mathbf{A})$ has a subalgebra which is a transversal for its monolith. Namely, $\{\langle x, x\rangle/\Delta_{\mu,\alpha} : x \in A\}$ is such a subalgebra.

Theorem 10.10. *Suppose that* $\mathbf{A}$ *is subdirectly irreducible. Then* $\mathrm{D}(\mathbf{A})$ *is subdirectly irreducible and* $\mathbf{A} \sim \mathrm{D}(\mathbf{A})$. *Moreover if the monolith of* $\mathbf{A}$ *is Abelian then the monolith of* $\mathrm{D}(\mathbf{A})$ *is its own centralizer and*

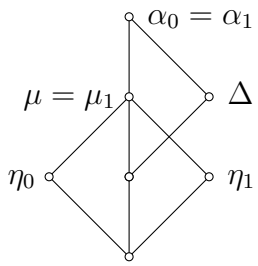


FIGURE 1.

$\{\langle x, x\rangle/\Delta_{\mu,\alpha} : x \in A\}$ *is a subalgebra of* $\mathrm{D}(\mathbf{A})$ *which is a transversal for the monolith of* $\mathrm{D}(\mathbf{A})$.

PROOF. Recall that if $\theta \in \mathbf{Con}\ \mathbf{A}$ then $\theta_i \in \mathbf{Con}\ \mathbf{A}(\mu), i = 0, 1$, is defined by $\langle a_0, a_1\rangle\ \theta_i\ \langle b_0, b_1\rangle$ if $a_i\ \theta\ b_i$. Let η_i, $i = 0, 1$, be the projection kernel of the projection map, i.e., $\eta_i = 0_i$. Since the theorem is obvious if μ is non-Abelian, we assume μ is Abelian and let $\alpha = (0 : \mu)$. Write Δ for $\Delta_{\mu,\alpha}$. We will show that the following transposition holds in $\mathbf{Con}\ \mathbf{A}(\mu)$ (see Figure 1).

$$(*) \qquad \alpha_0/\Delta \searrow \eta_1/0 \nearrow \mu_0/\eta_0$$

First it is not hard to see that $\mu_0 = \mu_1$, $\alpha_0 = \alpha_1$, and $\eta_0 \vee \eta_1 = \mu_0 = \mu_1$. Indeed, if $\langle a_0, a_1\rangle\ \alpha_0\ \langle b_0, b_1\rangle$ in $\mathbf{A}(\mu)$ then, by the definition of $\mathbf{A}(\mu)$ and of α_0, $a_1\ \mu\ a_0\ \alpha\ b_0\ \mu\ b_1$. Since $\mu \leq \alpha$, $\langle a_0, a_1\rangle\ \alpha_1\ \langle b_0, b_1\rangle$. The proof of the first equality is the same. To see the third equality suppose that $\langle a_0, a_1\rangle\ \mu_0\ \langle b_0, b_1\rangle$. Then all four elements are in the same μ–class and so $\langle a_0, a_1\rangle\ \eta_0\ \langle a_0, b_1\rangle\ \eta_1\ \langle b_0, b_1\rangle$. Since the other inclusion is trivial, this proves the third equality. Now if $\langle a_0, a_1\rangle\ \alpha_0\ \langle b_0, b_1\rangle$ then $a_0\ \alpha\ b_0$ and so $\langle a_0, a_1\rangle\ \eta_0\ \langle a_0, a_0\rangle\ \Delta\ \langle b_0, b_0\rangle\ \eta_0\ \langle b_0, b_1\rangle$. Hence $\alpha_0 = \alpha_1 = \Delta \vee \eta_0$, and similarly $\alpha_0 = \alpha_1 = \Delta \vee \eta_1$. If $\langle a_0, a_1\rangle\ \Delta \wedge \eta_1\ \langle b_0, b_1\rangle$ then $a_1 = b_1$. Now by Theorem 4.9(iv), $a_0\ [\alpha, \nu]\ b_0$, i.e., $a_0 = b_0$ and so $\Delta \wedge \eta_1 = 0$. Thus $(*)$ holds. By Theorem 10.8 this will show that $\mathbf{A} \sim \mathrm{D}(\mathbf{A})$ once we have shown that $\mathrm{D}(\mathbf{A})$ is subdirectly irreducible. To do this we will show that Δ is uniquely covered by $\alpha_0 = \alpha_1$.

Suppose $\varphi > \Delta$ in $\mathbf{Con}\ \mathbf{A}(\mu)$. If $\varphi \geq \eta_1$ then $\varphi \geq \eta_1 \vee \Delta = \alpha_0$. If $\varphi \not\geq \eta_1$ then $\varphi \wedge \eta_1 = 0$ as $\eta_1 \succ 0$ (which follows from the the fact that $\eta_1/0 \nearrow \mu_0/\eta_0$ and $\eta_0 \prec \mu_0$). Now $[\varphi \vee \eta_0, \mu_0] = [\varphi \vee \eta_0, \eta_0 \vee \eta_1] \leq \eta_0 \vee (\varphi \wedge \eta_1) = \eta_0$. It now follows from the definition of α that $\varphi \leq \varphi \vee \eta_0 \leq \alpha_0$. Since $\alpha_0 > \Delta$ by $(*)$, we must have $\varphi = \alpha_0$, contrary to $\varphi \not\geq \eta_1$. Thus Δ is completely meet irreducible and $\mathrm{D}(\mathbf{A})$ is therefore subdirectly irreducible.

To show that the monolith of $\mathrm{D}(\mathbf{A}) = \mathbf{A}(\mu)/\Delta$ it its own centralizer we need to show that $(\Delta : \alpha_0) = \alpha_0$ in $\mathbf{Con}\ \mathbf{A}(\mu)$. Clearly (by $(*)$

for example) $\alpha_0 \leq (\Delta : \alpha_0)$. To see the other inclusion, suppose that $\varphi \in \mathbf{Con}\ \mathbf{A}(\mu)$ satisfies $[\varphi, \alpha_0] \leq \Delta$. Then $[\varphi, \eta_0] \leq [\varphi, \alpha_0] \leq \Delta$. So $[\varphi, \eta_0] \leq \Delta \wedge \eta_0 = 0$. Similarly $[\varphi, \eta_1] = 0$ and thus $[\varphi, \mu_0] = [\varphi \wedge \eta_0 \vee \eta_1] = 0$. Since $\alpha_0 = (\eta_0 : \mu_0)$, $\varphi \leq \alpha_0$, as desired.

For the last statement of the theorem let $S = \{\langle x, x\rangle/\Delta_{\mu,\alpha} : x \in A\}$. Clearly S is a subalgebra of $\mathrm{D}(\mathbf{A}) = \mathbf{A}(\mu)/\Delta$. To see that it is a transversal of the monolith of $\mathrm{D}(\mathbf{A})$ it suffices to show that if $\langle x, x\rangle\ \alpha_0\ \langle y, y\rangle$ then $\langle x, x\rangle\ \Delta\ \langle y, y\rangle$ and if $\langle x, y\rangle \in \mathbf{A}(\mu)$ then $\langle x, y\rangle\ \alpha_0\ \langle y, y\rangle$. By its definition $\Delta = \Delta_{\mu,\alpha}$ is the congruence of $\mathbf{A}(\mu)$ generated by the pairs $\langle\langle x, x\rangle, \langle y, y\rangle\rangle$ such that $x\ \alpha\ y$ and hence the first implication above holds. Since $\mu \leq \alpha$, the second implication is trivial. □

THEOREM 10.11. *Suppose that* $\mathbf{A}$ *and* $\mathbf{B}$ *are subdirectly irreducible. Then* $\mathbf{A} \sim \mathbf{B}$ *if and only if* $\mathrm{D}(\mathbf{A}) \cong \mathrm{D}(\mathbf{B})$.

PROOF. If $\mathrm{D}(\mathbf{A}) \cong \mathrm{D}(\mathbf{B})$ then by the previous theorem $\mathbf{A} \sim \mathrm{D}(\mathbf{A}) \sim \mathrm{D}(\mathbf{B}) \sim \mathbf{B}$. For the other direction, assume $\mathbf{A} \sim \mathbf{B}$. If they have non-Abelian monoliths then $\mathrm{D}(\mathbf{A}) \cong \mathrm{D}(\mathbf{B})$, trivially. So we assume the monoliths are Abelian. Now $\mathrm{D}(\mathbf{A}) \sim \mathbf{A} \sim \mathbf{B} \sim \mathrm{D}(\mathbf{B})$; so it suffices to show that if $\mathbf{A}$ and $\mathbf{B}$ are similar algebras, each with its centralizer equal to its monolith and each having a subalgebra which is a transversal for its monolith, then $\mathbf{A} \cong \mathbf{B}$.

Since $\mathbf{A} \sim \mathbf{B}$ we have an isomorphism τ of $\sum_{i<\lambda} \mathbf{M}(\mu, z_i)$ onto $\sum_{i<\lambda} \mathbf{M}(\nu, w_i)$ where of course μ is the monolith of $\mathbf{A}$, ν is the monolith of B, z_i, $i < \lambda$, is a transversal for $\alpha = (0 : \mu)$, and w_i, $i < \lambda$, are a transversal for ν. As pointed out earlier, τ maps $\mathbf{M}(\mu, z_i)$ isomorphically onto $\mathbf{M}(\nu, w_i)$. Since $\mu = (0 : \mu)$, $\mathbf{A}$ is the disjoint union of the $\mathbf{M}(\mu, z_i)$'s and similarly $\mathbf{B}$ is the union of the $\mathbf{M}(\beta, w_i)$'s. Thus τ defines a bijection from $\mathbf{A}$ to $\mathbf{B}$. We shall show that τ is a homomorphism. By Exercise 7 the isomorphism type of $\sum_{i<\lambda} \mathbf{M}(\mu, z_i)$ does not change if we replace z_i with an element which is in the same μ–class. Now $\mathbf{A}$ has a subalgebra which is a transversal for μ which, by these remarks, we may assume is $\{z_i : i < \lambda\}$ and similarly, we may assume that $\{w_i : i < \lambda\}$ is a subalgebra of $\mathbf{B}$. Let f be a term and $x_1, \ldots, x_m \in A$. Let $x_0 = f(x_1, \ldots, x_n)$ and suppose $x_t \in z_t/\mu$, $t = 0, 1, \ldots, n$. Since $f(z_1, \ldots, z_n)\ \mu\ f(x_1, \ldots, x_n) = x_0\ \mu\ z_0$, and the z_i's form a subalgebra, $f(z_1, \ldots, z_n) = z_0$. Now an easy application of Proposition 5.7 shows

$$f(x_1, \ldots, x_n) = f(x_1, z_2, \ldots, z_n) + \ldots + f(z_1, \ldots, z_{m-1}, x_n).$$

The addition hare is in $\mathbf{M}(\mu, z_0)$ where z_0 is the zero element. Since τ preserves addition, it suffices to show that

$$\tau f(x_1, z_2, \ldots, z_n) = f(\tau x_1, w_2, \ldots, w_n).$$

This follows easily from the fact that τ is a $\mathbf{R}(\mathcal{V}, \lambda)$–homomorphism (see the comment after Definition 9.3. □

THEOREM 10.12. *If* $\mathbf{B}$ *is a subdirectly irreducible algebra in* $\boldsymbol{V}(\mathbf{A})$*, where* $\mathbf{A}$ *is finite, then* $\mathbf{B}$ *is similar to a subdirectly irreducible algebra in* $\boldsymbol{HS}(\mathbf{A})$*.*

PROOF. By the last theorem it suffices to prove this for $\mathrm{D}(\mathbf{A})$. So we may assume that $B = \mathrm{D}(\mathbf{A})$. Let μ be the monolith of $\mathbf{B}$. If $(0 : \mu) = 0$, then $\mathbf{B} \in \boldsymbol{HS}(\mathbf{A})$ by Theorem 10.1. So we may assume that $(0 : \mu) = \mu$. By Theorem 10.1, $\mathbf{B}/\mu \in HS(\mathbf{A})$. Theorem 10.16 below shows that each block of μ has size at most $|A|$. Hence $|B| \leq |A|^2$. In particular, $\mathbf{B}$ is finite. If follows that $\mathbf{B} = \mathbf{C}/\theta$ for some $\theta \in \mathbf{Con}\ \mathbf{C}$, where $\mathbf{C}$ is a subdirect product of subdirectly irreducible algebras $\mathbf{A}_0, \ldots, \mathbf{A}_{k-1} \in \boldsymbol{HS}(\mathbf{A})$. Let $\eta_0, \ldots, \eta_{k-1} \in \mathbf{Con}\ \mathbf{C}$ be the projection kernels. For subsets $\{a_i\}$ and $\{b_j\}$ of a lattice let $\{a_i\} \gg \{b_j\}$ mean that for each i there is a j with $a_i \geq b_j$. Since C is finite, we may choose $\theta_0, \ldots, \theta_{m-1} \in \mathbf{Con}\ \mathbf{C}$ maximal in the ordering $\gg$ such that $\bigwedge \theta_i \leq \theta$ and $\{\theta_i\} \gg \{\eta_j\}$. By relabeling these θ_i's as η_i's (this amounts to a new choice of the A_i's, but by the second condition above they are still in $\boldsymbol{HS}(\mathbf{A})$ and of course subdirectly irreducible) we may assume that if $\varphi_0, \ldots, \varphi_{m-1} \in \mathbf{Con}\ \mathbf{C}$ satisfy (1) $\bigwedge \varphi_i \leq \theta$, and (2) for each $i < m$ there is a j with $\varphi_i \geq \eta_j$, then $\{\eta_0, \ldots, \eta_{m-1}\} \subseteq \{\varphi_0, \ldots, \varphi_{m-1}\}$. If $\theta \wedge \eta_i' > 0$ we could replace η_i with $\eta_i \vee (\theta \wedge \eta_i')$ and violate the above conditions. So $\theta \wedge \eta_i' = 0$. $\theta \geq \eta_i'$ would also violate the above conditions. Thus $\theta \vee \eta_i' \geq \theta^*$, where θ^* is the unique congruence covering θ. It follows that $\theta^* \vee \eta_i' = \theta \vee \eta_i'$. Modularity now yields that $\theta^* \wedge \eta_i' > 0$. Hence $\theta^*/\theta \searrow \theta^* \wedge \eta_i'/0$. Since $\eta_i \wedge \eta_i' = 0$ and $\theta^* \wedge \eta_i' > 0$, $\eta_i \vee (\theta^* \wedge \eta_i') = \eta_i^*$. Thus

$$\theta^*/\theta \searrow \theta^* \wedge \eta_i'/0 \nearrow \eta_i^*/\eta_i.$$

Hence by Theorem 10.8 $\mathbf{B} \sim \mathbf{A}_i$, $i = 0, \ldots, k-1$. □

We record the fact the similarity types cannot mix in the next corollary.

COROLLARY 10.13. *If* $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$ *is subdirectly irreducible,* $\mathbf{A}$ *and* $\mathbf{B}$ *are finite, then for some* n*,* $\mathbf{B} \in \boldsymbol{V}(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ *with* $\mathbf{A}_i \in \boldsymbol{HS}(\mathbf{A})$ *and* $\mathbf{B} \sim \mathbf{A}_i$*,* $i = 1, \ldots, n$*.* □

3. Residually Small Varieties

In this section we continue our study of subdirectly irreducible algebras in a finitely generated variety. A variety is residually small if it has only a set of isomorphism types of subdirectly irreducible algebras.

Equivalently, there is a cardinal κ bounding the cardinality of all the subdirectly irreducible algebras in the variety. Quackenbush's problem asks the following question. If a finitely generated variety contains no infinite subdirectly irreducible algebras is there an integer n bounding the size of all subdirectly irreducible algebras in the variety? In this section we show that this is true for modular varieties. In fact we will show more. Namely we will show that any finitely generated, residually small, modular variety has a finite bound n for its subdirectly irreducible algebras. We will also show that a finitely generated variety is residually small if and only if it satisfies the congruence identity (C1) of Chapter 8. In fact any residually small modular variety satisfies (C1). The next theorem pertains to any modular variety, not just finitely generated varieties.

THEOREM 10.14. *Let $\mathcal{V}$ we a modular variety containing an algebra $\mathbf{A}$ with congruences β and γ satisfying*

$$\beta \leq [\gamma, \gamma] \quad \textit{and} \quad [\beta, \gamma] < \beta.$$

Then $\mathcal{V}$ is not residually small.

PROOF. We will actually prove more. We will show that if λ is any cardinal the is a subdirectly irreducible algebra in $\mathcal{V}$ whose congruence lattice has cardinality at least λ. Let $\mathbf{A} \in \mathcal{V}$ satisfy the hypotheses of the theorem. Choose θ a completely meet irreducible congruence such that $\theta \geq [\beta, \gamma]$ and $\theta \not\geq \beta$. Let θ^* be the unique cover of θ. Then it is easy to see that $\theta^* \leq [\theta \vee \gamma, \theta \vee \gamma] \vee \theta$ and $[\theta^*, \theta \vee \gamma] \leq \theta$, since $\theta^* \leq \theta \vee \beta$. Hence, by changing notation, we may assume that $\mathbf{A}$ is subdirectly irreducible and that β is its monolith. Recall that $algA(\gamma)$ is γ thought of as a subalgebra of $algA \times algA$. Let $\kappa = \Delta_{\gamma,\beta}$, where $\Delta_{\gamma,\beta}$ is the congruence on $A(\gamma)$ defined in Definition 4.7. Let $\eta_0, \eta_1 \in \mathbf{Con}\ \mathbf{A}(\gamma)$ be the kernels of the two projections onto A. From the definition of $\Delta_{\gamma,\beta}$ we easily see that $\kappa \wedge \eta_0 = \kappa \wedge \eta_1 = 0$ and that $\kappa \vee \eta_i = \beta_i$, $i = 0, 1$. See Figure 2.

Let $\aleph$ be an arbitrary cardinal and let $\mathbf{B} = \{(a_\delta) \in \mathbf{A}^\aleph : a_\delta\ \gamma\ a_\epsilon \text{ for all } \delta, \epsilon < \aleph\}$. Recall that if $\psi \in \mathbf{Con}\ \mathbf{A}$ then $\psi_\epsilon \in \mathbf{Con}\ \mathbf{B}$ is defined by $(a_\delta)\ \psi_\epsilon\ (b_\delta)$ if and only if $a_\epsilon\ \psi\ b_\epsilon$. Note that $\gamma_\delta = \gamma_\epsilon$ for all $\epsilon, \delta < \aleph$. We again denote this congruence by γ. Easy calculations on the elements show that $\eta_\epsilon \vee \eta_\delta = \gamma$ for $\epsilon \neq \delta$. Let $\kappa_\delta \in \mathbf{Con}\ \mathbf{B}$ be

$$\{\langle (a_\epsilon), (b_\epsilon)\rangle : \langle a_0, a_\delta\rangle\ \Delta_{\gamma,\beta}\ \langle b_0, b_\delta\rangle \text{ and } a_\epsilon = b_\epsilon,\ \epsilon \neq 0,\ \delta\}.$$

i.e., all pairs of elements of $\mathbf{B}$ equal in all coordinates except 0 and δ and such that the image of the projection onto $\mathbf{A} \times \mathbf{A}$ determined by

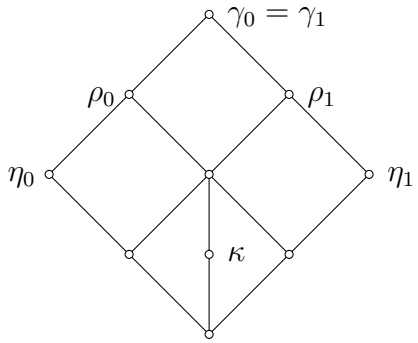


FIGURE 2.

the 0^{th} and δ coordinate is in $\Delta_{\gamma,\beta}$. Define

$$\theta_\delta = \{\langle (a_\epsilon), (b_\epsilon)\rangle : a_\delta \ \beta \ b_\delta \text{ and } a_\epsilon = b_\epsilon, \ \epsilon \neq \delta\}.$$

Let $\eta'_\delta = \bigwedge_{\epsilon\neq\delta} \eta_\epsilon$. Finally set $\theta = \bigvee_\delta \theta_\delta$ and $\kappa = \bigvee_{\delta>0} \kappa_\delta$. Note $\theta_0 \leq \theta_\delta \vee \kappa_\delta$ for $\delta \neq 0$. To see this let $(a_\epsilon)\ \theta_0\ (b_\epsilon)$ so that $a_0\ \beta\ b_0$ and all other coordinates are equal. Now by making changes only in the 0 and δ coordinates, and using the fact that $\langle a_0, a_0\rangle\ \Delta_{\gamma,\beta}\ \langle b_0, b_0\rangle$ by its definition, we have

$$\begin{aligned}(a_0, \ldots, a_\delta, \ldots)\ &\eta'_\delta\ (a_0, \ldots, a_0, \ldots)\\ &\kappa_\delta\ (b_0, \ldots, b_0, \ldots)\\ &\eta'_\delta\ (b_0, \ldots, b_\delta, \ldots)\end{aligned}$$

Thus $\theta_0 \leq \eta'_\delta \vee \kappa_\delta$ and meeting with β_δ gives $\theta_0 \leq \theta_\delta \vee \kappa_\delta$ by modularity. A similar argument shows that $\theta_\delta \leq \theta_0 \vee \kappa_\delta$.

Hence for $\delta \neq 0 \neq \epsilon$ we have

$$\begin{aligned}\kappa \vee \theta_\delta &= \kappa \vee \kappa_\delta \vee \kappa_\epsilon \vee \theta_\delta\\ &= \kappa \vee \kappa_\epsilon \vee \theta_0 \vee \theta_\delta\\ &= \kappa \vee \theta_\epsilon \vee \theta_0 \vee \theta_\delta\\ &\geq \theta_\epsilon \vee \theta_0\end{aligned}$$

It follows that $\kappa \vee \theta_\delta = \theta$ for all δ and this holds for $\delta = 0$ as well.

We also claim that $\theta_\delta \not\geq \kappa$. To see this first note that since $\beta > 0$ in **Con A**, $\theta_\delta > 0$ in **Con B**, and is thus compact. Hence if $\theta_\delta \leq \kappa$, then $\theta_\delta \leq \kappa_{\epsilon_1} \vee \cdots \vee \kappa_{\epsilon_n}$, for some $\epsilon_1, \ldots, \epsilon_n$. First consider the case $\delta = 0$ and induct on n. Observe that $\theta_0 \wedge \kappa_\epsilon = 0$ since if $\langle (a_\delta), (b_\delta)\rangle$ is in this intersection then $a_\delta = b_\delta$ for all $\delta \neq 0$, and $\langle a_0, a_\epsilon\rangle\ \Delta_{\gamma,\beta}\ \langle b_0, b_\epsilon\rangle = \langle b_0, a_\epsilon\rangle$. By Theorem 4.9 this implies that $\langle a_0, b_0\rangle \in [\gamma, \beta] = 0$. This proves that $n > 1$. Arguing on elements it is easy to see that the θ_δ's

are independent. Using this, and the fact that $\kappa_{\epsilon_1} \leq \theta_0 \vee \theta_{\epsilon_1}$, and that $\kappa_{\epsilon_2} \vee \cdots \vee \kappa_{\epsilon_n} \leq \theta_0 \vee \theta_{\epsilon_2} \vee \cdots \vee \theta_{\epsilon_n}$, and the induction hypothesis we have

$$\begin{aligned}
\theta_0 &= \theta_0 \wedge (\kappa_{\epsilon_1} \vee \cdots \vee \kappa_{\epsilon_n}) \\
&= \theta_0 \wedge (\theta_0 \vee \theta_{\epsilon_1}) \wedge (\kappa_{\epsilon_1} \vee \cdots \vee \kappa_{\epsilon_n}) \\
&= \theta_0 \wedge (\kappa_{\epsilon_1} \vee [(\theta_0 \vee \theta_{\epsilon_1}) \wedge (\theta_0 \vee \cdots \vee \theta_{\epsilon_n}) \wedge (\kappa_{\epsilon_2} \vee \cdots \vee \kappa_{\epsilon_n})]) \\
&= \theta_0 \wedge (\kappa_{\epsilon_1} \vee (\theta_0 \wedge (\kappa_{\epsilon_2} \vee \ldots \vee \kappa_{\epsilon_n}))) \\
&= \theta_0 \wedge \kappa_{\epsilon_1} = 0
\end{aligned}$$

This contradiction shows $\theta_0 \not\geq \kappa$. The case $\delta \neq 0$ follows from the fact that $\kappa \vee \theta_\delta = \kappa \vee \theta_0$.

If follows that $\kappa < \theta$. Let $\lambda \in \mathbf{Con}\ \mathbf{B}$ be a maximal congruence which contains κ but not θ. Then λ is completely meet irreducible, i.e., $\mathbf{B}/\lambda$ is subdirectly irreducible. Now in $\mathbf{Con}\ \mathbf{B}$, $\gamma/\eta_\delta \searrow \eta'_\delta/0$. Since $\mathbf{A}$ is subdirectly irreducible with monolith β, the interval γ/η_δ has a unique atom β_δ and the interval $\eta'_\delta/0$ has a unique atom θ_δ. Hence $\lambda \wedge \eta'_\delta = 0$, for otherwise $\lambda \geq \theta_\delta$, which implies $\lambda \geq \theta_\delta \vee \kappa = \theta$, a contradiction. Thus $\eta_\delta \vee \eta'_\delta = \gamma$ and $\lambda \wedge \eta'_\delta = 0$. If for some δ, $\lambda \vee \eta_\delta \geq \gamma$, then $[\gamma, \gamma] \leq [\eta_\delta \vee \eta'_\delta, \eta_\delta \vee \lambda] \leq \eta_\delta \vee (\lambda \wedge \eta'_\delta) = \eta_\delta$. By Proposition 4.4 this would imply that in $\mathbf{Con}\ \mathbf{A}$, $[\gamma, \gamma] = 0$, contrary to hypothesis. Thus for each δ, $\lambda \vee \eta_\delta \not\geq \gamma$. Since $\eta_\delta \vee \eta_\epsilon = \gamma$ for $\delta \neq \epsilon$, the $\lambda \vee \eta_\delta$, $\delta < \aleph$, must be pairwise distinct. Hence $|\mathbf{Con}\ \mathbf{B}/\lambda| \geq \aleph$, proving the theorem. □

THEOREM 10.15. *Let* $\mathbf{A}$ *be an algebra in a modular variety and let* $|A| = m < \omega$. *Then the following are equivalent.*

(1) $\boldsymbol{V}(\mathbf{A})$ *is residually small.*
(2) $\boldsymbol{V}(\mathbf{A})$ *is residually* $\leq m + \ell\,!$ *where* $\ell = m^{m^{m+3}}$.
(3) *For any* μ, $\nu \in \mathbf{Con}\ \mathbf{C}$, *where* $\mathbf{C} \subseteq \mathbf{A}$, $\nu \leq [\mu, \mu]$ *implies* $\nu = [\mu, \nu]$.

PROOF. Trivially (2) implies (1) and Theorem 10.14 shows that (1) implies (3). So assume that (3) holds. It follows directly from Lemma 10.2 that if $\boldsymbol{V}(\mathbf{A})$ contained an infinite subdirectly irreducible algebra, it would have arbitrarily large finite subdirectly irreducible algebras (cf. Quackenbush [**75**]). Thus we only need to show that every finite subdirectly irreducible algebra in $\boldsymbol{V}(\mathbf{A})$ has cardinality bounded as stated in (2). By Theorem 8.1, the condition of (3) holds in every finite algebra in $\boldsymbol{V}(\mathbf{A})$.

Let $B \in \boldsymbol{V}(\mathbf{A})$ be a finite subdirectly irreducible algebra with monolith β. If β is not Abelian then $\mathbf{B} \in \boldsymbol{HS}(\mathbf{A})$ by Theorem 10.1 and $\mathbf{B}$ is bounded as in (2). Thus we assume that β is Abelian and let

$\gamma = (0 : \beta)$ be the centralizer of β. By Theorem 10.1 $\mathbf{B}/\gamma \in \boldsymbol{HS}(\mathbf{A})$. If $[\gamma, \gamma] \neq 0$, then $[\gamma, \gamma] \geq \beta$, and since γ is the centralizer of β, $[\beta, \gamma] = 0$. This however violates (3) so we conclude that $[\gamma, \gamma] = 0$. Thus γ is an Abelian congruence with, say, k blocks where $k \leq m = |A|$. Let $z_1, \ldots, z_k$ be a system of distinct representatives for these blocks. Then by Corollary 9.10, $\mathbf{M}(\gamma) = \sum_{i=1}^{k} \mathbf{M}(\gamma, z_i)$ is a subdirectly irreducible $\mathbf{R}(\boldsymbol{V}(\mathbf{A}), k) = \mathbf{R}(\boldsymbol{V}(\mathbf{A}), k, 0)$–module.

Now

$$|\mathbf{R}(\boldsymbol{V}(\mathbf{A}), k, 0)| \leq \left[m^{m^{k+1}}\right]^{k^2} \leq m^{m^{k+3}} \leq m^{m^{m+3}}.$$

These bounds follow from the fact that $\mathbf{R}(\boldsymbol{V}(\mathbf{A}), k)$ consists of k by k matrices whose $(i, j)^{\text{th}}$ elements lie in $\overline{\mathbf{H}}_{ij}$ which has cardinality at most $|\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(k + 1)|$. Thus $\mathbf{M}(\gamma)$ is a subdirectly irreducible module over a ring with cardinality bounded in terms of $m = |A|$ as above. Thus we have reduced our problem to the special classical case of bounding the size of subdirectly irreducible modules over a finite ring in terms of the size of the ring. (The variety of left (unitary) $\mathbf{R}$–modules is generated by $\mathbf{R}$ as a left $\mathbf{R}$–module and thus is finitely generated when $\mathbf{R}$ is finite. A bound on $\mathbf{M}(\gamma)$ easily gives a bound on $\mathbf{B}$, see below.) At this point we could use the classical results of Rosenberg and Zelinsky [**78**] to obtain a bound for $\mathbf{M}(\gamma)$. Instead we will give a direct argument.

Thus suppose that $\mathbf{M}$ is a subdirectly irreducible module over a finite ring $\mathbf{R}$. Let $\mathbf{N}$ be the unique minimal submodule of $\mathbf{M}$, and let $a \in \mathbf{N}$, $a \neq 0$. Then, if $c \neq 0$ is in $\mathbf{M}$, $\mathbf{N} \subseteq \mathbf{R}c$. Hence for each $c \neq 0$ in $\mathbf{M}$ we can assign an $r \in \mathbf{R}$ such that $rc = a$. This implies that $|M| \leq |R|!$. We can prove this by induction as follows. We prove that if we have Abelian groups $\mathbf{K}$ and $\mathbf{L}$ and an element $a \neq 0$ in $\mathbf{L}$ and k homomorphisms $r_1, \ldots, r_k \in \mathrm{Hom}(\mathbf{K}, \mathbf{L})$ such that for each $c \neq 0$ in $\mathbf{K}$ there is an r_i with $r_i c = a$, then $|K| \leq (k + 1)!$. We induct on k; the initial case is left to the reader. Now each nonzero element of $\mathbf{K}$ is assigned to some r_i. Suppose that r_1 has the most elements assigned to it, say $c_1, \ldots, c_t$. Then $|K| \leq 1 + kt$. Now let $\mathbf{K}_1$ be the kernel of r_1. Since $c_1 - c_i$, $i = 1, \ldots, t$, is in $\mathbf{K}_1$, $|K_1| \geq t$. Thus $|K| \leq 1 + k|K_1|$. Now $\mathbf{K}_1$ satisfies the same hypothesis as $\mathbf{K}$ using $r_2, \ldots, r_k$. Thus by induction $|K_1| \leq k!$, and $|K| \leq 1 + k \cdot k! \leq (k + 1)!$, proving the claim.

Hence we conclude that $|M(\gamma)| \leq \ell\,!$, where $\ell = m^{m^{+3}}$. Now $\mathbf{M}(\gamma)$ is the direct product of the γ–blocks of $\mathbf{B}$, so $|M(\gamma)| = \prod_{i=1}^{k} |M(\gamma, z_i)|$. Clearly $|B| = \sum_{i=1}^{k} |M(\gamma, z_i)|$. From this it follows that $|B| \leq m + |M(\gamma)| \leq m + \ell\,!$, as desired. □

4. Chief Factors and Simple Algebras

Every compactly generated (i.e., algebraic) lattice is weakly atomic; that is, if $\theta < \psi$ in **Con A** the there are α, $\beta \in$ **Con A** with $\theta \leq \beta \prec \alpha \leq \psi$ (α covers β). In our paper [**29**] we defined $\sharp\alpha/\beta$ to be the supremum of the cardinalities of the sets $\{y/\beta : y \in x/\alpha\}$ for $x \in A$, i.e., $\sharp\alpha/\beta$ is the supremum of the number of β–blocks lying in a single α–block. These prime intervals α/β and their associated numbers $\sharp\alpha/\beta$ were loosely construed as a general analogue of what, in group theory, are called the chief factors of a group. [There are some open problems here, It would be nice to have some canonical algebra associated with α, β with properties similar to chief factors in groups. A candidate for such an algebra in the case α/β is Abelian is $\mathbf{M} = \sum \mathbf{M}(\alpha/\beta, z_i)$, where the z_i, s represent the classes of the congruence $(\beta : \alpha)$, ($\mathbf{M}(\alpha/\beta, z_i)$ is defined in Exercise 4). By Definition 9.3, $\mathbf{M}$ is a simple module. See Exercise 3 for additional properties of $\mathbf{M}$.]

We proved some theorems in [**29**] about these "chief factors" of finite algebras in a modular variety generated by finite algebra. These results extended similar results proved by J. B. Nation and Walter Taylor for permutable varieties. Here we improve these results.

THEOREM 10.16. *Let* $\mathbf{A}$ *be a finite algebra in a modular variety and let* $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$.

(1) *If* $\alpha \succ \beta$ *in* **Con B**, *then* $\sharp\alpha/\beta \leq |A|$.
(2) *If the length of* **Con B** *is* n, *then* $|B| \leq |A|^n$.
(3) *If* $\mathbf{B}$ *is simple, then* $|B| \leq |A|$.

PROOF. The following facts are elementary and are left as exercises to the reader (or see Freese-McKenzie [**29**]): (i) If $\gamma \leq \beta \prec \alpha$ then $\sharp\alpha/\beta$ is the same in $\mathbf{A}$ as in $\mathbf{A}/\gamma$. (ii) If $\alpha/\beta \searrow \gamma/\delta$ then $\sharp\alpha/\beta \geq \sharp\gamma/\delta$ and equality obtains if β and γ permute.

To prove 1. we first observe that we may assume that $\mathbf{B}$ is subdirectly irreducible, $\beta = 0$, and α is the monolith. Indeed let λ be a completely meet irreducible congruence with $\lambda \geq \beta$ and $\lambda \not\geq \alpha$. Then $\lambda \vee \alpha/\lambda \searrow \alpha/\beta$ and so by (i) and (ii) it suffices to show that the monolith of $\mathbf{B}/\lambda$ satisfies 1.

Assuming first that $\mathbf{B}$ is finite, let $\mathbf{B} = \mathbf{C}/\theta$, where $\mathbf{C} \subseteq \mathbf{A}^m$ with m minimal. Let ψ be the unique cover of θ. By (i) it suffices to show that $\sharp\psi/\theta \leq |A|$. Let $\eta \in \operatorname{Con}\mathbf{C}$ be the kernel of the projection to the first coordinate, and η' the kernel of the projection to the other coordinates. Since $\eta' \not\geq \theta$ by the minimality of m,

$$\psi/\theta \searrow \psi \wedge \eta'/\theta \wedge \eta' \nearrow \eta \vee (\psi \wedge \eta')/\eta \vee (\theta \wedge \eta') \subseteq 1/\eta.$$

If α is non-Abelian then by Theorem 10.1 $\mathbf{B} \in \boldsymbol{HS}(\mathbf{A})$ and 1. clearly holds. Hence we assume that $[\psi, \psi] \leq \theta$ and thus by the results of Chapter 6, θ and $\psi \wedge \eta'$ permute and the result follows from (ii).

Now assume that $\mathbf{B}$ is infinite. As above we may assume $\mathbf{B}$ is subdirectly irreducible with monolith α. Since $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$, which is locally finite, Lemma 10.2 implies that $\mathbf{B}$ is a subalgebra of an ultraproduct of finite algebras $\mathbf{B}_i \in \boldsymbol{HS}(\mathbf{B})$. Lemma 10.2 also tells us that if μ_i is the monolith of $\mathbf{B}_i$, then α is contained in the ultraproduct of the μ_i's restricted to $\mathbf{B}$. Since $\sharp \mu_i/0 \leq |A|$ for each i by the finite case. $\sharp \mu/0 \leq |A|$, from which 1. follows. The other parts of the theorem follow easily. □

Exercises

1. Let $\mathbf{C} \subseteq \prod_{i=1}^{n} \mathbf{A}_i$ be a subdirect representation of $\mathbf{C}$. Let $\alpha \succ \beta$ in $\mathbf{Con}\ \mathbf{C}$ and let η_i be the projection congruences. Prove that there is an i such that $\eta_i \leq (\beta : \alpha)$. Thus, in the situation of Theorem 10.5, if $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$ is subdirectly irreducible, and $\mathbf{A}$ and $\mathbf{B}$ are finite, then there exists a nilpotent congruence $\theta \in \mathbf{Con}\ \mathbf{B}$ such that $\theta = \bigwedge_{i=1}^{n} (\theta \vee \eta_i)$.

CHAPTER 11

Joins and Products of Modular Varieties

The two main results of this chapter are easy but not obvious. The first bounds the size of the subdirectly irreducible algebras in the join of two modular varieties. It was noticed in the case of finitely generated varieties in Freese-McKenzie [**29**], then it turned out to be true for rings (McKenzie [**64**]) so it gradually became obvious. An example is given showing that result is false without the modularity assumption. The second result shows that if two varieties intersect trivially and one is solvable then they are independent. A theorem of C. Herrmann is derived as a corollary.

THEOREM 11.1. *Let $\mathcal{V} = \mathcal{V}_0 \vee \mathcal{V}_1$ be a modular variety. If $\mathcal{V}_i$ is residually $\leq \lambda_i$, $i = 0, 1$, then $\mathcal{V}$ is residually $\leq \lambda_0\lambda_1$.*

PROOF. This theorem is an immediate consequence of the following lemma: if $\mathcal{V} = \mathcal{V}_0 \vee \mathcal{V}_1$ is modular and $\mathbf{B} \in \mathcal{V}$ is subdirectly irreducible, then $\mathbf{B} = \mathbf{C}/\theta$ where $\mathbf{C}$ is a subdirect product of subdirectly irreducible algebras $\mathbf{A}_0$ and $\mathbf{A}_1$, $\mathbf{A}_i \in \mathcal{V}_i$.

To see the lemma let $\mathbf{B} \in \mathcal{V}$ be subdirectly irreducible and assume $\mathbf{B} \notin \mathcal{V}_0 \cup \mathcal{V}_1$. Then $\mathbf{B} = \mathbf{C}/\theta$ where $\mathbf{C} \subseteq \mathbf{A}_0 \times \mathbf{A}_1$, $\mathbf{A}_i \in \mathcal{V}_i$. Let $\eta_i \in \mathbf{Con}(\mathbf{C})$ be the projection kernels. Using the upper continuity of $\mathbf{Con}(\mathbf{C})$, choose θ_0 and $\theta_1 \in \mathbf{Con}(\mathbf{C})$ maximal such that $\theta_i \geq \eta_i$ and $\theta_0 \wedge \theta_1 \leq \theta$. The proof of the lemma will be done when we show θ_0 and θ_1 are completely meet irreducible.

First note that $(\theta \vee \theta_0) \wedge (\theta \vee \theta_1) > \theta$. For otherwise $\mathbf{B} \in \mathcal{V}_0$ or $\mathcal{V}_1$. Moreover, $(\theta \vee \theta_0) \wedge (\theta \vee \theta_1)/\theta \searrow \theta_1 \wedge (\theta \vee \theta_0)/\theta \wedge \theta_1$. Now $\theta \wedge \theta_1 = \theta_0 \wedge \theta_1$ since otherwise we could replace θ_0 with $\theta_0 \vee (\theta \wedge \theta_1)$ and violate the maximality of θ_0. Hence $\theta_1 \wedge (\theta \vee \theta_0)/\theta_0 \wedge \theta_1$ is isomorphic to $(\theta \vee \theta_0) \wedge (\theta \vee \theta_1)/\theta$. Since θ is completely meet irreducible, there is a $\varphi \succ \theta_0 \wedge \theta_1$ such that $\theta_0 \wedge \theta_1 < \alpha \leq \theta_1 \wedge (\theta \vee \theta_0)$ implies $\varphi \leq \alpha$. Since $\theta_1 \wedge (\theta \vee \theta_0)/\theta_0 \wedge \theta_1 \nearrow (\theta_0 \vee \theta_1) \wedge (\theta_0 \vee \theta)/\theta_0$, $\theta_0 \prec \theta_0 \vee \varphi$. Suppose $\psi \in \mathbf{Con}(\mathbf{C})$ satisfies $\psi \wedge (\theta_0 \vee \varphi) = \theta_0$. Then $\psi \not\geq \varphi$, which implies $\psi \wedge \theta_1 \wedge (\theta \vee \theta_0) = \theta_0 \wedge \theta_1$. Now

$$(\theta \vee \theta_0) \wedge ((\psi \wedge \theta_1) \vee \theta) = \theta \vee (\psi \wedge \theta_1 \wedge (\theta \vee \theta_0)) = \theta.$$

Since θ is meet irreducible, either $\theta \geq \theta_0 \geq \eta_0$, a contradiction, or $\psi \wedge \theta_1 \leq \theta$. But then $\psi = \theta_0$ by the maximality of θ_0. This proves θ_0 is completely meet irreducible. □

EXAMPLE 11.2. Polin constructed a nonmodular variety $\mathcal{V}$, whose congruence lattices nevertheless did satisfy nontrivial lattice identities, solving an old problem. His variety is generated by a four element algebra $\mathbf{A}$ with a binary, two unary, and a nullary operation (see Polin [**74**], Day-Freese [**23**]). Now $\mathbf{A} = \mathbf{A}_0 \times \mathbf{A}_1$ with each $\mathbf{A}_i$ equivalent to the two element Boolean algebra. Hence $\mathcal{V} = \mathcal{V}_0 \vee \mathcal{V}_1$ with $\mathcal{V} = V(A_i)$ and $\mathcal{V}_i$ is distributive, permutable, and residually ≤ 2. Nevertheless $\mathcal{V}$ is nonmodular and residually large. Thus modularity is necessary in Theorem 11.1. This example also shows that modularity is necessary in the result of Hagemann and Herrmann (see Exercise 8.2), that the join of two distributive varieties in a modular variety is distributive.

Two varieties $\mathcal{V}_0$ and $\mathcal{V}_1$ of the same type are *independent* if there is a term $t(x_0, x_1)$ such that $\mathcal{V}_i$ satisfies $t(x_0, x_1) = x_i$, $i = 0, 1$. If $\mathcal{V}_0, \mathcal{V}_1 \subseteq \mathcal{V}$, we write $\mathcal{V} = \mathcal{V}_0 \otimes \mathcal{V}_1$ provided that $\mathcal{V}_0$ and $\mathcal{V}_1$ are independent and $\mathcal{V} = \mathcal{V}_0 \vee \mathcal{V}_1$ (i.e. the variety generated by $\mathcal{V}_0 \cup \mathcal{V}_1$ is $\mathcal{V}$). Note that if t is as above and if $\sigma_i(x_1, ..., x_n)$, $i = 0, 1$, are terms for $\mathcal{V}$, then $\tau = t(\sigma_0, \sigma_1)$ is a term whose interpretation in $\mathbf{A}_i$ agrees with that of σ_i if $\mathbf{A}_i \in \mathcal{V}_i, i = 0, 1$. From this it follows that $\mathcal{V}_0 \otimes \mathcal{V}_1$ defined above is equivalent (in the technical sense; see Taylor [**80**] p. 354) to $\mathcal{V}_0 \otimes \mathcal{V}_1$ as defined by Taylor.

The equation $\mathcal{V} = \mathcal{V}_0 \otimes \mathcal{V}_1$ has strong structural implications for $\mathcal{V}$: see Grätzer-Lakser-Plonka [**35**] and Taylor [**80**], pp. 357–8. In particular, each $\mathbf{A} \in \mathcal{V}$ can be decomposed as $\mathbf{A} = \mathbf{A}_0 \times \mathbf{A}_1$ with $\mathbf{A}_i \in \mathcal{V}_i$. Moreover $\mathbf{Con}(\mathbf{A}) \cong \mathbf{Con}(\mathbf{A}_0) \times \mathbf{Con}(\mathbf{A}_1)$. Any (weak) Mal'cev condition which holds for both $\mathcal{V}_0$ and $\mathcal{V}_1$ will hold for $\mathcal{V}_0 \otimes \mathcal{V}_1$.

THEOREM 11.3. *Let $\mathcal{V}$ be a modular variety. Let $\mathcal{V} = \mathcal{V}_0 \vee \mathcal{V}_1$, where $\mathcal{V}_1$ is solvable and $\mathcal{V}_0 \cap \mathcal{V}_1$ contains only the one-element algebras. Then $\mathcal{V} = \mathcal{V}_0 \otimes \mathcal{V}_1$.*

PROOF. First we will show that if $\mathbf{A} \in \mathcal{V}$ is a subdirect product of $\mathbf{A}_0$ and $\mathbf{A}_1$, with $\mathbf{A}_i \in \mathcal{V}_i$, then $\mathbf{A} = \mathbf{A}_0 \times \mathbf{A}_1$. To see this let $\eta_i \in \mathbf{Con}(\mathbf{A})$ be the projection kernel, $i = 0, 1$. Then $\eta_0 \wedge \eta_1 = 0$ and, since $\mathbf{A}/\eta_0 \vee \eta_1 \in \eta_0 \cap \eta_1$, $\eta_0 \vee \eta_1 = 1$. Since $\mathbf{A}_i$ is solvable, $[1]^k \leq \eta_1$ in $\mathbf{Con}(\mathbf{A})$ for some k. ($[1]^k$ is defined in Definition 6.1.) Hence $[\eta_0]^k \leq [1]^k \wedge \eta_0 \leq \eta_1 \wedge \eta_0 = 0$. Thus η_0 is solvable and so permutes with η_1 by Theorem 6.2, showing that $\mathbf{A} = \mathbf{A}_0 \times \mathbf{A}_1$.

Since $\mathcal{V} = \mathcal{V}_0 \vee \mathcal{V}_1$, $\mathbf{F}_{\mathcal{V}}(2)$ is a subdirect product of $\mathbf{F}_{\mathcal{V}_0}(2)$ and $\mathbf{F}_{\mathcal{V}_1}(2)$. Thus $\mathbf{F}_{\mathcal{V}}(2) = \mathbf{F}_{\mathcal{V}_0}(2) \times \mathbf{F}_{\mathcal{V}_1}(2)$. Let x and y be the free

generators of $\mathbf{F}_{\mathcal{V}}(2)$ and let η_i be the projection kernels. Since $\eta_0 \circ \eta_1 = 1$, $x\ \eta_0\ t(x,y)\ \eta_1\ y$ for some $t(x,y) \in \mathbf{F}_{\mathcal{V}}(2)$. Consequently $\mathcal{V}_0$ satisfies $x = t(x,y)$ and $\mathcal{V}_1$ satisfies $y = t(x,y)$, proving the theorem. □

Since a distributive variety and a solvable variety can have only the one-element algebra in common, the last theorem implies that *if* $\mathcal{D}$ *is a distributive variety and* $\mathcal{S}$ *is solvable variety and* $\mathcal{M} = \mathcal{D} \vee \mathcal{S}$ *then* $\mathcal{M} = \mathcal{D} \otimes \mathcal{S}$. Hence we have the following corollary, due to Herrmann [**45**].

COROLLARY 11.4. *Let* $\mathcal{M} = \mathcal{D} \vee \mathcal{A}$ *with* $\mathcal{M}$ *a modular variety,* $\mathcal{D}$ *a distributive variety and* $\mathcal{A}$ *an Abelian variety. Then* $\mathcal{M} = \mathcal{D} \otimes \mathcal{A}$. □

We remark that for each of the congruence identities ε considered in Chapter 8, if $\mathcal{V} = \mathcal{V}_0 \vee \mathcal{V}_1$ is modular, then $\mathcal{V}$ satisfies ε if and only both $\mathcal{V}_0$ and $\mathcal{V}_1$ satisfy ε. This is due to the fact that "hereditary ε" is a property preserved under the formation of subdirect products of two factors, and homomorphic images.

CHAPTER 12

Strictly Simple Algebras

We mean by a **strictly simple** algebra a finite simple algebra having more than one element, which is generated by any two of its distinct elements. (This last condition is equivalent to saying that any proper subalgebra has only one element.) A **minimal variety** is just an equationally complete variety, i.e., a variety possessing exactly two subvarieties, including itself. It is obvious that each locally finite minimal variety is generated by a strictly simple algebra. Surprisingly, the converse of this statement is very nearly true in the domain of modular varieties.

We shall also be concerned in this section with the spectrum sets and fine spectrum functions of varieties. We define

$$\begin{aligned} \mathrm{Spec}(\mathcal{V}) &= \{n < \omega : \text{for some } \mathbf{A} \in \mathcal{V},\ |\mathbf{A}| = n\} \\ n_{\mathcal{V}}(\kappa) &= (\text{the number of isomorphism types of algebras} \\ &\qquad \text{in } \mathcal{V} \text{ of cardinality } \kappa) \end{aligned}$$

Notice that $\mathrm{Spec}(\mathcal{V}) \subseteq \omega$, whereas $n_{\mathcal{V}}$ is a function defined on all cardinal numbers, finite and infinite.

The study of strictly simple algebras in modular varieties, and the spectra and fine spectra of modular varieties generated by strictly simple algebras, produced some interesting results. We collect them here and supply proofs which are relatively easy compared to those in the literature.

The following was first proved for permutable varieties in McKenzie [**62**] (but Smith [**79**], Chapter 5, came very close to proving it), and for modular varieties later by C. Herrmann. The **ternary discriminator operation** on a set $\mathbf{A}$ is operation $t : A^3 \to A$ given by $t(a, b, c) = a$ if $a \neq b$ and c if $a = b$. A variety $\mathcal{V}$ is called a **discriminator variety** if there is a term $t(x, y, z)$ for $\mathcal{V}$ such that the corresponding term operation is a ternary discriminator operation on each algebra in a generating set of $\mathcal{V}$. A finite algebra such that the ternary discriminator operation is a term operation is called **quasiprimal**.

THEOREM 12.1. (1) *Every strictly simple algebra in a modular variety generates either an Abelian or a distributive subvariety.*

(2) *If* $\mathbf{A}$ *is strictly simple and* $\boldsymbol{V}(\mathbf{A})$ *is permutable and non-Abelian, then* $\mathbf{A}$ *is a quasiprimal algebra.*

PROOF. Suppose first that $\mathbf{A}$ is strictly simple, $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$ is modular, and $\mathbf{A}$ is not affine. Obviously, $\mathbf{A}$ (and its subalgebras can have only one element) satisfies the congruence identity $[x, y] = x \cdot y$ (in fact $\mathbf{Con}\ \mathbf{A} = 0, 1$ and $[1, 1] = 1$). Thus $\mathbf{A}$ and its subalgebras are neutral. Since $\mathbf{A}$ is finite, $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(3)$ is a finite subdirectly power of $\mathbf{A}$. Now, by Exercise 8.2, $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(3)$ is neutral, which implies its congruence lattice is distributive by Exercise 8.1. Thus, by Jónsson's Theorem 2.1, $\boldsymbol{V}(\mathbf{A})$ is distributive.

For statement (2), suppose that $\mathbf{A}$ is strictly simple and non-Abelian and $\boldsymbol{V}(\mathbf{A})$ is permutable. Then by (1) $\boldsymbol{V}(\mathbf{A})$ is arithmetic (distributive and permutable), and by Jónsson's theorem every subdirectly irreducible algebra in the variety is isomorphic to $\mathbf{A}$, hence hereditarily simple. So (2) follows from Pixley's characterization of quasiprimal algebras [**72**] (or see Burris-Sankappanavar [**10**] p.173). □

COROLLARY 12.2. *Let* $\mathbf{F}$ *be a finite, simple, non-Abelian algebra in a modular variety and* $\mathbf{F}' = (\mathbf{F}, c)_{c \in F}$ *its inessential expansion by constants. Then we have*

(1) $\boldsymbol{V}(\mathbf{F}')$ *is distributive.*
(2) *If* $\boldsymbol{V}(\mathbf{F})$ *is permutable, then the ternary discriminator operation is a polynomial operation of* $\mathbf{F}$.

The following amazing result of R. Quackenbush [**76**], (but he discovered it in 1976) stood for four years with a difficult proof until an easy one was found in McKenzie [**63**]. Modularity is not implicitly assumed. The proofs lie outside commutator theory.

THEOREM 12.3. *The following are equivalent for any finite algebra* $\mathbf{A}$*, where* $|\mathbf{A}| = n > 1$.

(1) $\mathbf{A}$ *is strictly simple and* $\boldsymbol{V}(\mathbf{A})$ *is permutable.*
(2) $\mathrm{Spec}(\boldsymbol{V}(\mathbf{A})) = \{n^k : k < \omega\}$.

Quackenbush has used his theorem in [**77**] to give a relatively easy proof of I. Rosenberg's classification of pre-complete clones of operations on a finite set.

If $\mathbf{A}$ is strictly simple and $\boldsymbol{V}(\mathbf{A}) = \mathcal{V}$ is distributive, then $\mathcal{V}$ is minimal by Jónsson's Theorem. If $\mathcal{V}$ is also permutable, then $\mathrm{Spec}(\mathcal{V})$ is given by Theorem 12.3(ii), and $n_{\mathcal{V}}(m) = 1$ for finite m in the spectrum, since $\mathbf{A}$ is quasiprimal. On the other hand, if $\mathcal{V}$ is distributive but not permutable, then most of the obvious questions concerning $\mathrm{Spec}(\mathcal{V})$ and the finite values of $n_{\mathcal{V}}$ are completely open. [S. Burris proved in [**7**]

that for infinite λ, any distributive variety containing a simple algebra of cardinality at most λ, has $n_{\mathcal{V}}(\lambda) \geq 2^{(}\lambda)$ with equality, of course, if $\mathcal{V}$ has at most λ basic operations.]

On the Abelian side of Theorem 12.1, there are some interesting facts which we now proceed to derive under the rubric of theory developed in Chapter 9. It is easily seen, first of all, that any finite simple affine algebra is strictly simple, the condition on subalgebras being redundant. Let us recall the concept of the linearization, $\mathbf{A}_\nabla$, of an Abelian algebra $\mathbf{A}$, from Proposition 9.18. The history and contributors to the following theorem will be discussed after we prove it.

THEOREM 12.4. *Let $\mathbf{Q}$ be a finite, simple, Abelian algebra of n elements and let $\mathcal{V} = V(\mathbf{Q})$. Then n is a prime power. Furthermore*

(1) *If $\mathbf{Q}$ has an idempotent element, then*
   (i) *Every finite algebra in $\mathcal{V}$ is (isomorphic to) a power of $\mathbf{Q}$ and every infinite algebra in $\mathcal{V}$ is a Boolean power of $\mathbf{Q}$. Thus $\mathcal{V}$ is minimal.*
   (ii) *All algebras in $\mathcal{V}$ of size λ are isomorphic, for each λ.*

(2) *If $\mathbf{Q}$ has no idempotent element, then*
   (i) *Every finite algebra in $\mathcal{V}$ is a power of $\mathbf{Q}$ or of $\mathbf{Q}_\nabla$ and every algebra in $\mathcal{V}$ is a Boolean power of $\mathbf{Q}$ or of $\mathbf{Q}_\nabla$. $\boldsymbol{V}(\mathbf{Q}_\nabla)$ is the unique nontrivial proper subvariety of $\mathcal{V}$.*
   (ii) *$n_{\mathcal{V}}(\lambda) = 2$ if $\lambda = n^k$ $(k < \omega)$ and is 0 otherwise.*

PROOF. First we define the concept of isotopy. If $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ are algebras in a variety, we say $\mathbf{A}$ is **isotopic** to $\mathbf{B}$ via $\mathbf{C}$ provided $\mathbf{C} \times \mathbf{A}$ is isomorphic to $\mathbf{C} \times \mathbf{B}$ via an isomorphism which commutes with the first projection (i.e. $(c, a) \mapsto (c, a)$ for some $b \in B$). Notice that in a modular variety this is equivalent to

$(*)$ there is a $\beta \in \mathbf{Con}(\mathbf{C} \times \mathbf{A})$ with $(\mathbf{C} \times \mathbf{A})/\beta \cong \mathbf{B}$ and β a complement of η_0.

(Here we are using Gumm's result that every congruence of a direct product permutes with the factor congruences, see Exercise 5.4). Notice also that if $\mathbf{A}$ is isotopic to $\mathbf{B}$ via $\mathbf{C}$ and $\mathbf{C}$ has an idempotent element, then $\mathbf{A} \cong \mathbf{B}$.

Now $\mathbf{Q}_\nabla = (\mathbf{Q} \times \mathbf{Q})/\Delta_{1,1}$ and since $\Delta_{1,1}$ and η_0 are complements we have that $\mathbf{Q}$ and $\mathbf{Q}_\nabla$ are isotopic via $\mathbf{Q}$. In particular $\mathbf{Q} \times \mathbf{Q}_\nabla \cong \mathbf{Q} \times \mathbf{Q}$, and if $\mathbf{Q}$ has an idempotent $\mathbf{Q} \cong \mathbf{Q}_{nabla}$.

Now suppose $\mathbf{B} \in \boldsymbol{V}(\mathbf{Q})$ is finite and subdirectly irreducible. Since $\mathbf{Q}$ has no proper subalgebras and generates a permutable variety, its finitely generated free algebras are direct powers of $\mathbf{Q}$. Hence there is

a k with $\mathbf{Q}^k \to \mathbf{B}$ and we prove by induction on k that $\mathbf{B}$ is either $\mathbf{Q}$ or $\mathbf{Q}_\nabla$. Since $\mathbf{Q}$ is simple, $k = 1$ is easy. So assume $k > 1$. Then $\mathbf{Q}^k \cong \mathbf{Q} \times \mathbf{Q}^{k-1}$. Let $\theta \in \mathbf{Con}(\mathbf{Q}_\nabla \times Q^{k-1})$ be the kernel of the map onto $\mathbf{B}$. Since the coatoms of $\mathbf{Con}\mathbf{Q}^k$ meet to 0, $\mathbf{Con}\mathbf{Q}^k \cong \mathbf{Con}\mathbf{Q}_\nabla \times \mathbf{Q}^{k-1}$ is a complemented modular lattice and since θ is meet irreducible, this implies it is also a coatom. Let η_0' be the kernel of $\mathbf{Q}_\nabla \times \mathbf{Q}^{k-1} \to \mathbf{Q}^{k-1}$ and define $\gamma = (\eta_0 \wedge \theta) \vee \eta_0'$. By the minimality of k, $\theta \not\geq \eta_0'$ (and $\theta \neq \eta_0$) and so γ is a coatom above η_0'. By induction $\mathbf{C} = \mathbf{Q}_\nabla \times \mathbf{Q}^{k-1}/\gamma$ is either $\mathbf{Q}$ or $\mathbf{Q}_\nabla$. Also each pair from η_0, θ, and γ is complementary in the interval $1/\eta_0 \wedge \theta$. By (*) we see that $\mathbf{B}$ is isotopic to $\mathbf{C}$ via $\mathbf{Q}_\nabla$. But $\mathbf{Q}_\nabla$ has an idempotent. Hence $\mathbf{B} \cong \mathbf{C}$, proving that $\mathbf{Q}$ and $\mathbf{Q}_\nabla$ are the only subdirectly irreducible algebras in $\boldsymbol{V}(\mathbf{Q})$.

If $\mathbf{A} \in \boldsymbol{V}(Q)$ is finite, then it is a finite subdirect product of $\mathbf{Q}$ and $\mathbf{Q}_\nabla$. The minimality of $\mathbf{Q}$ and $\mathbf{Q}_\nabla$ and permutability imply that $\mathbf{A} \in \boldsymbol{P}\{\mathbf{Q}, \mathbf{Q}_\nabla\}$. Since $\mathbf{Q}_\nabla \times \mathbf{Q} \cong \mathbf{Q} \times \mathbf{Q}$. $\mathbf{A}$ is a direct power of $\mathbf{Q}$ or of $\mathbf{Q}_\nabla$.

Let $\mathbf{R} = \mathbf{R}(\boldsymbol{V}(\mathbf{Q}))$ and $\mathbf{M}_0 = \mathbf{M}(1_Q, 0) = \mathbf{M}(Q, 0)$ where 0 is a fixed but arbitrary element of $\mathbf{Q}$. Since $\mathbf{Con}\ \mathbf{Q} = \mathbf{Con}\ \mathbf{M}_0$ by Proposition 9.19(i), $\mathbf{M}_0$ is simple. It is a faithful $\mathbf{R}$-module because $\mathbf{Q}$ generates $\boldsymbol{V}(\mathbf{Q})$. Thus $\mathbf{R}$ is a finite simple ring, and hence isomorphic to the ring of m by m matrices over a finite field $\mathbf{GF}(p^r)$. Hence $n = |\mathbf{Q}| = |\mathbf{M}_0| = p^{rm}$.

By Jacobson [**52**], Theorem 4.4, p.208, every $\mathbf{R}$-module is isomorphic to a direct sum $\mathbf{M}_0^{(\lambda)}$ for some cardinal λ.

If $\mathbf{B} \in \boldsymbol{V}(\mathbf{Q})$ has an idempotent element e, then $\mathbf{M} = \mathbf{M}(B, e) \cong {\mathbf{M}_0}^{(\lambda)}$ and $\mathbf{B} = \mathbf{A}(\mathbf{M}, \varphi^{(e)}) \cong \mathbf{A}({\mathbf{M}_0}^{(\lambda)}, 0)$ by Theorem 9.16, so $\mathbf{B}$ is determined up to isomorphism by its cardinality. Notice that if $\mathbf{Q}$ has an idempotent element, then $\mathbf{F}_{\boldsymbol{V}(\mathbf{Q})}(1)$ does and hence every algebra in $\boldsymbol{V}(\mathbf{Q})$ does. This proves (1), since there are Boolean powers of every infinite cardinality.

To complete the proof we will show that if $\mathbf{B} \in \boldsymbol{V}(\mathbf{Q})$ has infinite cardinality λ and no idempotent element, then $\mathbf{B} \cong \mathbf{A}({\mathbf{M}_0}^{(\lambda)}, 0) \times \mathbf{Q}$. Indeed we have $\mathbf{B} \cong \mathbf{A}({\mathbf{M}_0}^{(\lambda)}, \psi)$ and we can assume the isomorphism is equality. The rang of ψ is a finite submodule of ${\mathbf{M}_0}^{(\lambda)}$, hence contained in a finite sum of the factors. So we can write $\mathbf{B} = \mathbf{A}({\mathbf{M}_0}^{(\lambda)} \times \mathbf{M}^{(k)}, \psi)$, with $k < \omega$ and the range of ψ contained in the second factor. Since the projection kernels are congruences of $\mathbf{B}$, this implies $\mathbf{B} \cong \mathbf{A}({\mathbf{M}_0}^{(\lambda)}, 0) \times \mathbf{A}(\mathbf{M}^{(k)}, \psi)$. The second factor is finite without idempotent hence isomorphic to $\mathbf{Q}^k$ by the above. Since $\mathbf{Q}^k \cong \mathbf{Q}^{k-1} \times \mathbf{Q}$, we obtain $\mathbf{B} \cong \mathbf{C} \times \mathbf{Q}$ where $\mathbf{C}$ has an idempotent. Hence $\mathbf{C} \cong \mathbf{A}({\mathbf{M}_0}^{(\lambda)}, 0)$, completing the proof. $\square$

Steven Givant in [**31, 32**] and E. A. Palyutin in [**70, 71**] described in detail all varieties of algebras of countable type which are categorical in some infinite power. The varieties $\boldsymbol{V}(\mathbf{Q}_\nabla)$ with $\mathbf{Q}$ strictly simple Abelian are precisely the modular varieties in Givant's classification. (The nonmodular ones can be constructed in a canonical way from permutational representations of finite groups.) Note that $\boldsymbol{V}(\mathbf{Q})$ is essentially of finite type, whatever its actual type, since every term is equal in $\mathbf{Q}$ to one obtained by composition from binary terms and d, by Theorem 9.16.

The conclusions in Theorem 12.4 which concern the finite algebras in $\boldsymbol{V}(\mathbf{Q})$ were proved in part by Smith [**79**], Chapter 5, and in full by Clark and Krauss [**12**], [**13**] and Quackenbush [**76**]. Categoricity of $\boldsymbol{V}(\mathbf{Q}_\nabla)$ in all powers was then proved by Clark-Krauss [**14**]. The fact that $n_{\mathcal{V}}(\lambda) = 2$ for all infinite λ when $\mathbf{Q}$ is not isomorphic to $\mathbf{Q}_\nabla$ follows from Corollary 2.8 and Lemma 2.9 of Clark-Krauss [**14**]. Our proof of Theorem 12.4 has not appeared before.

CHAPTER 13

Mal'cev Conditions for Lattice Equations

Theorems 2.1(2) and 2.2 give Jonsson's and Day's conditions on a variety equivalent to the variety having distributive or modular congruences. Both of these conditions assert the existence of terms in a fixed number of variables (3 for distributivity, 4 for modularity) which satisfy certain equations. Conditions of this form are known as Mal'cev conditions. In the light of Jonsson's and Day's results, it would be natural to conjecture that every lattice identity has such a Mal'cev condition. A. Pixley and R. Wille were able to prove that each lattice has a it weak Mal'cev condition. A it weak Mal'cev condition is the conjunction of Mal'cev conditions C_n, $n \in \omega$, where C_n implies C_m if $n \geq m$. See Taylor [**80**] for a precise discussion of these concepts. Several questions remain open. it Does every lattice identity correspond to a Mal'cev condition? Are there any nontrivial identities, other then distributivity and modularity, which have Mal'cev conditions? Certain identities were shown to have Mal'cev conditions, for example, Gedeonova [**30**] and Mederly [**66**], but Day [**20**], following Nation, shows that these identities were in fact equivalent to modularity for the congruence lattice of varieties of varieties algebras. In this section we shall answer the second question above. We use the commutator to sketch a proof that are infinitely many lattice identities each having a Mal'cev condition. Moreover, these identities are inequivalent in the strong since that for any two of them there is a modular variety whose congruence lattices satisfy one of these identities but not the other. In this chapter we assume the reader has some familiarity with Mal'cev conditions and the theory of modular lattices.

A subset $\{a_i : i = 1, \ldots, n\} \cup \{c_{ij} : 1 \leq i, j \leq n, i \neq j\}$ of a modular lattice is called a (von Neumann) n–**frame** provided.

$$a_i \wedge \bigvee_{j \neq i} a_j = \bigwedge_{k=1}^{n} a_k$$

$$(c_{ij} \vee c_{jk}) \wedge (a_i \vee a_k) = c_{ik}$$

$$c_{ij} = c_{ji}$$

for distinct i, j and k, and a_i, a_j, c_{ij} generates a copy of $\mathbf{M}_3$ for $i \neq j$. These n–frames play an important role in the theory of modular lattices. They are projective, i.e.,the free modular lattice generated by an n–frame is a projective lattice. This fact was first proved by Huhn [**48**]; see also Freese [**25**]. Moreover, if $\mathbf{L}$ is a modular lattice containing an n–frame, $n \geq 4$, we let $R = \{x \in L : x \vee a_2 = a_1 \vee a_2, x \wedge a_2 = a_1 \wedge a_2\}$ and define an addition $x \oplus y$ on R by

$$x \oplus y = [((x \vee c_{13}) \wedge (a_2 \vee a_3)) \vee ((y \vee a_3) \wedge (a_2 \vee c_{13}))] \wedge (a_1 \vee a_2)$$

Multiplication on R is defined by a similar formula. The details of these formulae are not important for our arguments here. Under these operations $\mathbf{R}$ is a ring with a_1 as its zero and c_{12} as its unit.

The next lemma is the key to our result.

LEMMA 13.1. *If $\theta_1, \ldots, \theta_n$, $\theta_{12}, \theta_{13}, \ldots, \theta_{n-1,n}$ is an n–frame in $Con\, A$ in a modular variety, then any two congruences in the interval between $\bigwedge \theta_i$ and $\bigvee \theta_i$ permute.*

PROOF. By additivity $[\bigvee \theta_i, \bigvee \theta_i] = \bigvee_{i,j} [\theta_i, \theta_j]$. If $i \neq j$, then $[\theta_i, \theta_j] \leq \theta_i \wedge \theta_j = \bigwedge \theta_k$. Since θ_i is part of an $\mathbf{M}_3$ with least element $\bigwedge \theta_k$, $[\theta_i, \theta_j] \leq \bigwedge \theta_k$. Thus $[\bigvee \theta_i, \bigvee \theta_i] \leq \bigwedge \theta_i$ and the lemma now follows easily from Theorem 6.2. □

Let $\mathbf{x} = (x_1, \ldots, x_n, x_{12}, \ldots, x_{n,n-1})$ be a vector of lattice variables. The fact that n–frames are projective implies that there are lattice terms $a_i(\mathbf{x})$, $c_{ij}(\mathbf{x})$, in these variables such that any interpretation of these terms into a modular lattice yields a (possibly degenerate) n–frame and if the variables x_i and x_{ij} are substituted into a frame a_i, c_{ij} the value of $a_i(\mathbf{x})$ is a_i and that of $c_{ij}(\mathbf{x})$ is c_{ij}. Let ε_p be the lattice equation which expresses the fact that the ring associated with the frame $\{a_i(\mathbf{x}), c_{ij}(\mathbf{x})\}$ satisfies $p \cdot 1 = 0$, where p is a prime. Here $p \cdot 1$ stands for the sum of p copies of 1. By the above formula for addition, this can be expressed as a lattice equation. If $\mathcal{V}$ is the variety of all vector spaces over a field $\mathbf{F}$, then using elementary linear algebra one can show that the ring associated with any n–frame in a congruence lattice (= subspace lattice) in $\mathcal{V}$ has the same characteristic as that of $\mathbf{F}$. Thus if p and q are distinct primes there is a modular variety (the variety of vector spaces over the field with p elements) which satisfies ε_p but fails ε_q. Hence the ε_p's are pairwise inequivalent even for congruences on varieties of algebras.

THEOREM 13.2. *For each prime p, the condition that the congruence lattice of a variety of algebras are modular and satisfy ε_p is definable by a Mal'cev condition.*

PROOF. In order to understand the proof we need to review the procedure for obtaining the weak Mal'cev condition associated with a lattice inequality. This is best done by way of example. We will illustrate this with the distributive law, the simplest nontrivial lattice equation. The distributive law is equivalent to the following inequality.

$$x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z) \tag{1}$$

Recall that a weak Mal'cev condition consists of the conjunction of stronger Mal'cev conditions C_n, $n < \omega$. To illustrate the procedure for obtaining C_n, let $\mathcal{V}$ be a distributive variety and let S be a set (whose size will be determinate later) of letters containing a and b, and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(S)$ be the free $\mathcal{V}$ algebra generated by S. In the first half of the procedure we associate congruences of $\mathbf{F}$ with the variables of (1) in such a way that $\langle a, b\rangle$ is in the left side of (1). Since we want $\langle a, b\rangle \in x \wedge (y \vee z)$, we must have $\langle a, b\rangle \in x$, and $\langle a, b\rangle \in y \vee z$. In order to insure that the latter occurs we include in S letters $a_1, \ldots, a_n$ such that $\langle a, a_1\rangle \in y$, $\langle a_i, a_{i+1}\rangle \in y$, if i is even $\langle a_i, a_{i+1}\rangle \in z$, if i is odd, and $\langle a_n, b\rangle$ is in y if n is even, in z if n is odd. (The n here is the same as the subscript of C_n.) Thus in order to insure that $\langle a, b\rangle$ is in the left side of (1) we take $S = a, b, a_1, \ldots, a_n$, and we take the following substitutions for x, y and z.

$$\begin{aligned} x &\mapsto \operatorname{Cg}(a, b) \\ y &\mapsto \bigvee_{i \text{ even}} \operatorname{Cg}(a_i, a_{i+1}) \\ z &\mapsto \bigvee_{i \text{ odd}} \operatorname{Cg}(a_i, a_{i+1}) \end{aligned} \tag{2}$$

Here we take $a_0 = a$ and $a_{n+1} = b$. This is the first half of the procedure for obtaining C_n.

The procedure for an arbitrary lattice inequality is similar. In the general step if we have $c, d \in S$ with $\langle c, d\rangle \in w$, where w is a subterm of the left side of the inequality, then if w is a meet, say $w = w_1 \wedge w_2$, then we put $\langle c, d\rangle$ in both w_1 and w_2. If $w = w_1 \vee w_2$ then we add $c_1, \ldots, c_n$ to S and put $\langle c_i, c_{i+1}\rangle$ into w_1 or w_2, depending on whether i is even or odd. The procedure stops when we reach the lattice generators. At this point, associated with each lattice generator is a list of pairs of elements of S. We then associate with this generator the congruence on $\mathbf{F}_{\mathcal{V}}(S)$ generated by this list of pairs. It is easy to see that, under this interpretation, $\langle a, b\rangle$ is in the left side of the inequality.

Now for the second half of the procedure. Let x, y and z denote the value of these letters under the substitution (2), i.e., let x denote $\mathrm{Cg}^{\mathbf{F}}(a,b)$, etc. Thus $\langle a,b\rangle \in x\wedge(y\vee z)$ and since we are assuming that $\mathcal{V}$ satisfies (1), we must have $\langle a,b\rangle \in (x\wedge y)\vee(x\wedge z)$. Hence there must be elements $t_0(a,a_1,\dots,a_n,b),\dots,t_m(a,a_1,\dots,a_n,b)$ of $\mathbf{F}_{\mathcal{V}}(S)$ such that $t_0 = a$, $t_m = b$, $\langle t_i, t_{i+1}\rangle \in x\wedge y$, if i is even, $\langle t_i,t_{i+1}\rangle \in x\wedge z$ if i is odd. Since $x = \mathrm{Cg}(a,b)$, for each i we have $t_i(a,a_1,\dots,a_n,a)\ x\ t_i(a,a_1,\dots,a_n,b)\ x\ t_{i+1}(a,a_1,\dots,a_n,b)\ x\ t_{i+1}(a,a_1,\dots,a_n,a)$. Since $\mathrm{Cg}(a,b)$ is the trivial relation on the subalgebra of $\mathbf{F}$ generated by $\{a,a_1,\dots,a_n\}$, we have

$$t_i(a,a_1,\dots,a_n,a) = t_{i+1}(a,a_1,\dots,a_n,a) \tag{3}$$

for $i = 0,\dots,m-1$. Similarly, assuming n is odd, we obtain for i even,

$$t_i(a,a,a_2,a_2,a_4,a_4,\dots,b) = t_{i+1}(a,a,a_2,a_2,a_4,a_4,\dots,b) \tag{4}$$

and for i odd

$$t_i(a,a_1,a_1,a_3,a_3,\dots,b,b) = t_{i+1}(a,a_1,a_1,a_3,a_3,\dots,b,b) \tag{5}$$

Now the Mal'cev condition C_n is the following assertion for a variety $\mathcal{V}$: for some $m < \omega$ there are $\mathcal{V}$-terms $t_0(a,a_1,\dots,a_n,b),\dots,t_m(a,a_1,\dots,a_n,b)$ such that $t_0 = a$, $t_m = b$ and $\mathcal{V}$ satisfies (3), (4), and (5). The above arguments show that if $\mathcal{V}$ is a distributive variety then $\mathcal{V}$ satisfies C_n for all n. It is not difficult to prove the converse: if $\mathcal{V}$ satisfies C_n for all n, then $\mathcal{V}$ is distributive. Jonsson's Mal'cev condition is C_1. His theorem (Theorem 2.1) is the much stronger result that $\mathcal{V}$ is distributive if and only if it satisfies C_1.

The same idea applies in the general case. Namely if we have a lattice inequality

$$v(x_1,\dots,x_k) \le u(x_1,\dots,x_k) \tag{6}$$

then following the first half of the procedure detailed above we obtain a set S, containing a and b, and a map, which we denote by τ, from each lattice variable x_i into a congruence on $\mathbf{F}_{\mathcal{V}}(S)$ generated by a partition on S, such that $\langle a,b\rangle$ is in the left side of (6). If $\mathcal{V}$ satisfies (6) then $\langle a,b\rangle$ is in the right side. Just as in the distributive case this implies that there are certain identities involving the variables S.

Thus $\mathcal{V}$ satisfies a lattice inequality, such as (6), if and only if $\mathcal{V}$ satisfies C_n for all n. An inequality such as (6) has a Mal'cev condition if there is a fixed n_0 such that $\mathcal{V}$ satisfies (6) if and only if it satisfies C_{n_0}. Since if $\mathcal{V}$ satisfies (6) it satisfies all C_n, to show that (6) has a Mal'cev condition it suffices to show that there is a fixed n_0 such that if $\mathcal{V}$ fails (6) then $\mathcal{V}$ fails C_{n_0}.

Now let $\mathcal{V}$ be a variety failing the conjunction of modularity and ε_p. If $\mathcal{V}$ is nonmodular then the C_2 of Day's Mal'cev condition fails in $\mathcal{V}$. Thus we may assume that $\mathcal{V}$ is modular and fails ε_p. We claim that the C_1 associated with ε_p fails in $\mathcal{V}$. Since ε_p fails there is an algebra $\mathbf{A}$ in $\mathcal{V}$ and congruences θ_i, θ_{ij} which fail ε_p. By the remarks above, $a_i(\theta)$, $c_{ij}(\theta)$ is a frame in $\mathbf{Con}(\mathbf{A})$ and if we substitute the variables of ε_p into this frame, instead of into the θ_i, θ_{ij}, the value of the two sides of ε_p remain the same. Thus, by changing notation, we may assume there is a substitution, $x_i \mapsto \theta_i$, $x_{ij} \mapsto \theta_{ij}$, of the variables into a frame $\{\theta_i, \theta_{ij}\}$ of $\mathbf{Con}(\mathbf{A})$ such that ε_p fails. Hence there are elements a, $b \in A$ with $\langle a, b\rangle$ in the left side of ε_p but not in the right. Now by Lemma 13.1 all of the subterms of the terms of ε permute. Now we build a subset $T \subseteq A$in a manner analogous to the procedure for forming S in the weak Mal'cev condition C_1 for ε_p described above. We start with a, $b \in T$. Let v be the left side of ε_p. Then $\langle a, b\rangle \in v$. Now suppose that c, $d \in T$, and $\langle c, d\rangle \in w = w_1 \vee w_2$, where w is a subterm of v. Since $w = w_1 \circ w_2$, there exists $e \in \mathbf{A}$ such that $c\ w_1\ e\ w_2\ d$. We add e to T. Since T is formed in a manner similar to S, there is a surjection $\sigma : S \to T$. Moreover if y is one of the lattice variables of v and if $\langle c, d\rangle$, $(c, d \in S)$ is in the congruence of $\mathbf{F}_{\mathcal{V}}(S)$ associated with y (see the description of C_1 above) then $\langle \sigma(c), \sigma(d)\rangle$ is in the congruence on $\mathbf{A}$ associated with y (θ_i if $y = x_i$, θ_{ij} if $y = x_{ij}$). That is, the image under σ of the partition on S associated with y lies in the congruence on $\mathbf{A}$ associated with y. If $\mathcal{V}$ satisfied C_1 it would follow from the construction of C_1 that $\langle a, b\rangle$ would be in the right side of ε_p, a contradiction. Thus C_1 fails in $\mathcal{V}$. □

The lattice equations satisfied by the lattice of submodules (= congruence lattice) of a variety of modules were extensively studied in Hutchinson-Czedli [**51**]. Using these ideas we can prove that *for each lattice equation ε there is another equation ε', which is equivalent to ε for varieties of modules, and such that the conjunction of ε' and modularity is definable by a Mal'cev condition.*

A recent paper of Day and Kiss defines a "canonical" n–frame in $\mathbf{F}_{\mathcal{V}}(n+1)$ when $\mathcal{V}$ is a modular variety. They show that the ring associated with this frame equals $\mathbf{R}(\mathcal{V})$. Thus the equations ε_p are significant for $\mathcal{V}$ in that $\mathcal{V}$ satisfies ε_p if and only if $p \cdot 1 = 0$ in $\mathbf{R}(\mathcal{V})$, for any p (not necessarily a prime). Thus our Mal'cev condition are closely connected to the characteristic of $\mathbf{R}(\mathcal{V})$. Some of these connections are developed in the exercises.

Exercises

1. (Jónsson, unpublished) Let $\mathcal{V}$ be a modular variety, $\mathbf{A} \in \mathcal{V}$ and α_i, $\gamma_{ij} \in \mathbf{Con}(\mathbf{A})$ be a n–frame, $n \geq 3$, such that $\alpha_1 \wedge \alpha_2 = 0$. Let β, δ be in the ring associated with this frame (i.e., $\beta \vee \alpha_2 = \alpha_1 \vee \alpha_2$ and $\beta \wedge \alpha_2 = \alpha_1 \wedge \alpha_2$ and the same for δ) and define an addition and multiplication $\dot{+}$ and $\times$ on the ring as follows:

$$\beta \dot{+} \delta = \{\langle x, y\rangle \in A^2 : \exists\, z,\, t \quad x\ \beta\ z\ \alpha_2\ y,\ x\ \alpha_2\ t\ \delta\ y,\ z\ \alpha_1\ T\}$$

$$\beta \times \delta = \{\langle x, y\rangle \in A^2 : \exists\, z,\, t \quad x\ \beta\ z\ \alpha_2\ y,\ x\ \alpha_1\ t\ \delta\ y, z\ \gamma_{12}\ t\}.$$

Prove that the addition given here is the same as the addition defined just above Lemma 13.1. (This exercise can be used to construct a fairly simple Mal'cev condition for ε_p.)

2. As mentioned at the end of the chapter, all the congruence lattice in $\mathcal{V}$ satisfy ε_n if and only if $\mathbf{R}(\mathcal{V})$ (and so also $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$) satisfies $n \cdot 1 = 0$. Prove this for $n = 3$. You may use that the satisfaction of ε_n is equivalent to the fact that the ring of every frame satisfies $n \cdot 1 = 0$.

CHAPTER 14

A Finite Basis Result

In this chapter we presents a generalization of Michael Vaughan-Lee's finite basis [**81**]. The result is that a finite nilpotent algebra of finite type which is the direct product of algebras of prime power orders has a finite basis for its identities. Vaughan-Lee proved this under the additional assumption that the algebra had an equationally defined constant.

Lemmas 7.3 through Corollary 7.7 prove some elementary facts about nilpotent algebras. The reader may want to quickly review them before proceeding. Recall from Chapter 6 that $(1,1]^0 = 1$ and that $(1,1]^{k+1} = [1,(1,1]^k]$. As in Chapter 7, we write $(1]_k$ for $(1,1]^k$. $\mathbf{A}$ is **nilpotent** if $(1]_k = 0$ for some k. For a (modular) variety $\mathcal{V}$ we let $\mathcal{V}_n$ be the subvariety consisting of all algebras in $\mathcal{V}$ satisfying $(1]_n = 0$.

We need to show that $\mathcal{V}_n$ is finitely based relative to $\mathcal{V}$. The next theorems prove this provided $\mathbf{F}_{\mathcal{V}}(2)$ is finite. We are interested in the case $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$, $\mathbf{A}$ finite, where this condition is of course true.

THEOREM 14.1. *$a\ \zeta_{\mathbf{A}}\ b$ if and only if*

$$(1)\quad f(d(r_1(a,b),r_1(b,b),c_1),\dots,d(r_n(a,b),r_n(b,b),c_n)) = d(f(r_1(a,b),\dots,r_n(a,b)),f(r_1(b,b),\dots,r_n(b,b)),f(c))$$

and

$$(2)\qquad d(r(a,b),r(b,b),r(b,b)) = r(a,b)$$

for all basic operations f, all $\mathbf{c} = \langle c_1,\dots,c_n\rangle \in \mathbf{A}^n$, and all binary term operations r and r_i.

PROOF. If $a\ \zeta\ b$ then (1) and (2) hold by Proposition 5.7. Now suppose that (1) and (2) hold. Then (1) holds whenever f is a term operation. (1) and (2) imply

$$(3)\qquad d(d(r(a,b),r(b,b),c),c,e) = d(r(a,b),r(b,b),e)$$

for all $c, e \in A$, and r a binary term operation. In fact,

$$\begin{aligned} &d(d(r(a,b), r(b,b), c, e) \\ &\quad = d(d(r(a,b), r(b,b), c), d(r(b,b), r(b,b), c), d(r(b,b), r(b,b), e) \\ &\quad = d(d(r(a,b), r(b,b), r(b,b)), r(b,b), e) \\ &\quad = d(r(a,b), r(b,b), e). \end{aligned}$$

Now define a relation θ on $\mathbf{A}$ by

$$u \;\theta\; v \leftrightarrow u = d(r(a,b), r(b,b), v) \tag{4}$$

for some binary term operation r.

Clearly $v \;\theta\; v$ (take $r(x,y) = y$). Suppose $u \;\theta\; v$ so that $u = d(r(a,b), r(b,b), v)$. Let $s(a,b) = d(r(b,b), r(a,b), r(b,b))$. Note that $s(b,b) = r(b,b)$. Now using (1) backwards and then (2),

$$\begin{aligned} &d(s(a,b), s(b,b), u) \\ &\quad = d(d(r(b,b), r(a,b), r(b,b)), d(r(b,b), r(b,b), r(b,b)), d(r(a,b), r(b,b), v)) \\ &\quad = d(d(r(b,b), r(b,b), r(a,b)), d(r(a,b), r(b,b), r(b,b)), d(r(b,b), r(b,b), v)) \\ &\quad = d(r(a,b), r(a,b), v) \\ &\quad = v. \end{aligned}$$

Thus $v \;\theta\; u$.

Suppose $u \;\theta\; v \;\theta\; w$. Then $u = d(r(a,b), r(b,b), v)$ and $v = d(s(a,b), s(b,b), w)$. Let $t(a,b) = d(r(a,b), r(b,b), s(a,b))$. Note $t(b,b) = s(b,b)$ and

$$\begin{aligned} &d(t(a,b), t(b,b), w) \\ &\quad = d(d(r(a,b), r(b,b), s(a,b)), d(r(b,b), r(b,b), s(b,b)), d(r(b,b), r(b,b), w)) \\ &\quad = d(d(r(a,b), r(b,b), r(b,b)), r(b,b), d(s(a,b), s(b,b), w)) \\ &\quad = d(r(a,b), r(b,b), v) \\ &\quad = u. \end{aligned}$$

If $u_i \;\theta\; v_i$, $i = 1, \ldots, n$ and f is an n-ary basic operation then (1) implies $f(u_1, \ldots, u_n) \;\theta\; f(v_1, \ldots, v_n)$. Thus θ is a congruence. Since (2) implies $d(a,b,b) = a$ (take $r(x,y) = x$), $a \;\theta\; b$. Hence, $\mathrm{Cg}\,(a,b) \leq \theta$. But if $u \;\theta\; v$ then $u = d(r(a,b), r(b,b), v)\ \mathrm{Cg}\,(a,b)\ d(r(b,b), r(b,b), v) = v$. Thus $\theta = \mathrm{Cg}\,(a,b)$.

Now if $\langle u_i, v_i\rangle \in \mathrm{Cg}\,(a,b)$, then $u_i = d(r_i(a,b), r_i(b,b), v_i)$. Hence, if f is an n–ary term operation and $\mathbf{c} = \langle c_1, \ldots, c_n\rangle \in A^n$, then using (3)

$$\begin{aligned}
&f(d(u_1, v_1, c_1), \ldots, d(u_n, v_n, c_n))\\
&\quad = f(d(d(r_1(a,b), r_1(b,b), v_1), v_1, c_1), \ldots, d(d(r_n(a,b), r_n(b,b), v_n), v_n, c_n))\\
&\quad = f(d(r_1(a,b), r_1(b,b), c_1), \ldots, d(r_n(a,b), r_n(b,b), c_n))\\
&\quad = d(f(r_1(a,b), \ldots, r_n(a,b)), f(r_1(b,b), \ldots, r_n(b,b)), f(\mathbf{c})).
\end{aligned}$$

Now using (3) again with $r(a,b) = f(r_1(a,b), \ldots, r_n(a,b))$

$$\begin{aligned}
&d(f(u_1, \ldots, u_n), f(v_1, \ldots, v_n), f(c_1, \ldots, c_n))\\
&\quad = d(f(d(r_1(a,b), r_1(b,b), v_1), \ldots, d(r_n(a,b), r_n(b,b), v_n)), f(v), f(\mathbf{c}))\\
&\quad = d(d(f(r_1(a,b), \ldots, r_n(a,b)), f(r_1(b,b), \ldots, r_n(b,b)), f(v)), f(v), f(\mathbf{c}))\\
&\quad = d(f(r_1(a,b), \ldots, r_n(a,b)), f(r_1(b,b), \ldots, r_n(b,b)), f(\mathbf{c}))
\end{aligned}$$

Hence, $f(d(u_1, v_1, c_1), \ldots, d(u_n, v_n, c_n) = d(f(u), f(v), f(\mathbf{c}))$ for all $\mathbf{c}$ and all $(u, v) \in \mathrm{Cg}\,(a,b)$. Thus, by Proposition 5.7, $[\mathrm{Cg}\,(a,b), 1] = 0$, and $a\ \zeta_{\mathbf{A}}\ b$, as claimed. □

As above let $\mathcal{V}$ be a modular variety and $\mathcal{V}_n = \{\mathbf{A} \in \mathcal{V} : (1]_n = 0 \text{ in } \mathbf{A}\}$. Define sets E_n of equations as follows. Let $E_0 = \{x \approx y\}$ and let E_{n+1} be the set of all equations of the form

$$\begin{aligned}
&f(d(r_1(s,t), r_1(t,t), z_1), \ldots, d(r_k(s,t), r_k(t,t), z_k))\\
&\qquad\qquad \approx d(f(r_1(s,t), \ldots, r_k(s,t)), f(r_1(t,t), \ldots, r_k(t,t)), f(z))
\end{aligned}$$

union the set of all equations of the form

$$d(r(s,t), r(t,t), r(t,t)) \approx r(s,t)$$

where f is a basic operation, r and r_i are binary terms, and $s \approx t \in E_n$, and the z_i are variables.

THEOREM 14.2. *Let* $\mathbf{A} \in \mathcal{V}$. *Then* $\mathbf{A}$ *satisfies* E_n *if and only if* $\mathbf{A} \in \mathcal{V}_n$.

PROOF. Suppose that $\mathbf{A} \in \mathcal{V}$. Then $\mathbf{A} \in \mathcal{V}_{n+1}$ if and only if $\mathbf{A}/\zeta \in \mathcal{V}_n$. By induction this holds if and only if $\mathbf{A}/\zeta$ satisfies E_n. This holds if and only if for all evaluations a and b of $s \approx t$ in E_n, $a\ \zeta\ b$. By the last theorem, this holds if and only if $\mathbf{A}$ satisfies E_{n+1}. □

When $\mathbf{F}_{\mathcal{V}}(2)$ is finite, then there is a finite set S of binary terms [namely a set of representative terms for the elements of $\mathbf{F}_{\mathcal{V}}(2)$] such that any binary term $r(x,y)$ for $\mathcal{V}$ is equivalent to a term in S, i.e., $r(x,y) \approx s(x,y)$ holds in $\mathcal{V}$ for some $s(x,y)$ in S. In this case, E_n can

be defined using only the binary terms of S, and so can be taken to be finite. Thus we have the following corollary.

COROLLARY 14.3. *In a modular variety $\mathcal{V}$ of finite type, if $\mathbf{F}_{\mathcal{V}}(2)$ is finite, then there is a finite set of laws which, together with the identities of $\mathcal{V}$, define $\mathcal{V}_n$.*

LEMMA 14.4. *Let $\mathbf{A} \in \mathcal{V}$ and let 0 be arbitrary in $\mathbf{A}$ and $S \subseteq A$ with $s\ \zeta_{\mathbf{A}}\ 0$ for all $s \in S$. Suppose $\langle a, 0\rangle \in \bigvee_S \operatorname{Cg}(s, 0)$. Then*

$$a = \sum_{k=1}^{m} r_k(s_k, 0)$$

for some $m \in \omega$, $s_k \in S$ and $r_k(x, z)$ binary idempotent terms for $\mathcal{V}$.

PROOF. Let $\theta = \bigvee_S \operatorname{Cg}(s, 0)$. Then $\theta \leq \zeta$ and hence $(0 : \theta) = 1$. By Theorem 9.9 (with $\beta = \theta$ and $\gamma = 1$) the interval $\theta/0$ of **Con A** is isomorphic to the lattice of submodules of the $\mathbf{R}(\mathcal{V}, 1)$–module $M(\theta, 0)$. Let $\mathbf{R} = R(\mathcal{V}, 1) = R(\mathcal{V})$. By Exercise 5 of Chapter 9 the image of $\operatorname{Cg}(s, 0)$ under this isomorphism is the submodule $\mathbf{R}s$. Thus $\mathbf{M}(\theta, 0) = \bigvee_{s\in S} Rs = \sum_{s\in S} Rs$. Since the elements of $\mathbf{R} = \mathbf{R}(\mathcal{V})$ can be represented by binary idempotent terms the result follows. □

By Theorem 6.2 a nilpotent variety is congruence permutable. Hence we assume that $\mathbf{A} \in \mathcal{U}$ where $\mathcal{U}$ is a permutable variety with Mal'cev term $d(x, y, z)$. Consider the free $\mathcal{U}$ algebra F generated by $X \cup z$. Define $u + v = d(u, z, v)$, $u, v \in \mathbf{F}$. For $x \in X$ let $\delta_x \in \mathbf{End}(\mathbf{F})$ be such that $x\delta_x = z$, $y\delta_x = y$, $y \in X - x$, $z\delta_x = z$. An element $w = w(x_1, \ldots, x_n, z)$ of $\mathbf{F}$ is a **commutator** if there is a set $x_1, \ldots, x_n \subseteq X$ such that w is in the subalgebra generated by this set and z and $w\delta = z$, $i = 1, \ldots, n$. A term corresponding to a commutator is a called a **commutator word**.

LEMMA 14.5. (Higman's Lemma) *Assume as above that $\mathbf{F}$ is the free algebra for $\mathcal{U}$ on $X \cup z$ and in addition that $\mathcal{U}$ is nilpotent. If u, $v \in \mathbf{F}$ then there is a finite set C of commutators such that*

(1) *the identity $u \approx v$, together with the identities of $\mathcal{U}$, implies the law $w(x, z) \approx z$ for all $w \in C$,*
(2) *$\langle u, v\rangle$ is contained in the congruence generated by $\{\langle w(x, z), z\rangle : w \in C\}$.*

PROOF. For $w \in F$ define $w\delta_x^* = d(w, w\delta_x, z)$. If $S \subseteq X$, δ_S is the endomorphism of F with $x\delta_S = z$, if $x \in S$, and fixing the other generators. Assume that X is linearly ordered. If $S \subseteq X$ is finite, δ_S^* is the composition of the ${\delta_S}^*$'s, $x \in S$ in the order of X.

Define

$$C = \{d(u,v,z)\delta_K\delta_L^* : \ K \cap L = \emptyset,\ K \cup L = X,\ L \text{ finite}\}$$

It is not hard to see and is in fact shown below that C is finite. If S, $T \subseteq X$ then, $\delta_S\delta_T = \delta_T\delta_S$, $\delta_S\delta_T^* = \delta_T^*\delta_S$, and, if $S \cap T \neq \emptyset$, then $w\delta_T^*\delta_S = z$. Now if $K \cap L = \emptyset$ and L is finite then $d(u,v,z)\delta_K\delta_L^*$ is in the subalgebra generated by $L \cup z$ and if $x \in L$, $d(u,v,z)\delta_K\delta_L^*\delta_X = z$ by the above. Thus C consists of commutators. Clearly the law $u \approx v$ implies the law $d(u,v,z) \approx z$, and hence the law $d(u,v,z)\delta_K\delta_L^* \approx z$.

Let $c = d(u,v,z)$, and suppose that c lies in the subalgebra generated by $S = \{x_1, \ldots, x_n, z\}$. Then $c\delta_L^* = z$ unless $L \subseteq S$, and $c\delta_K\delta_L^* = c\delta_{K_1}\delta_L^*$ if $K \cap S = K_1 \cap S$. Hence $C = \{c\delta_K\delta_L^* : K \cup L = S\}$. Let $\theta = \bigvee_{w \in C} \operatorname{Cg}(w,z)$. We claim that $(c,z) \in \theta$. We show by induction on r that $(c\delta_K\delta_L^*, z) \in \theta$ when $K \cap L = \emptyset$, and $K \cup L = \{x_1, \ldots, x_{n-r}\}$. The case $r = 0$ is true by the definition of θ, and $r = n$ is the claim. Suppose the result is true for r. Let $K \cap L = \{x_1, \ldots, x_{n-r-1}\}$, $K \cup L = \{x_1, \ldots, x_{n-r-1}\}$, $K \cap L = \emptyset$. Let $M = K \cup \{x_{n-r}\}$. By induction, $(c\delta_M\delta_L^*, z)$ and $(c\delta_K\delta_N^*, z)$ are in θ. Now $c\delta_M\delta_L^* = c\delta_K\delta_L^*\delta_{x_{n-r}}$ and $c\delta_K\delta_N^* = c\delta_K\delta_L^*\delta_{x_{n-r}}^* = d(c\delta_K\delta_L^*, c\delta_K\delta_L^*\delta_{x_{n-r}}, z)$. Hence both of these elements are θ-related to z. So

$$\begin{aligned} z \ \theta \ & d(c\delta_K\delta_L^*, c\delta_K\delta_L^*\delta_{x_{n-r}}, z) \\ \theta \ & d(c\delta_K\delta_L^*, c\delta_M\delta_L^*, z) \\ \theta \ & d(c\delta_K\delta_L^*, z, z) \\ = \ & c\delta_K\delta_L^* \end{aligned}$$

proving the claim. Now since we are in a nilpotent variety, we can use Lemma 7.6 to see that $(u,v) \in \theta$, proving the lemma. □

LEMMA 14.6. *Let $\mathcal{U}$ be a permutable variety and $w(x_1, \ldots, x_k, z) \in \mathbf{F}_{\mathcal{U}_n}(X \cup z) = \mathbf{F}$. Then*

$$w(x,z) = w(z, \ldots, z) + c_1 + \cdots + c_m$$

where each c_i is a commutator (for $\mathcal{U}$) and the sum is associated left to right.

PROOF. Induct on n. The result is clear for $n = 0$. So we assume that $(1]_{n+1} = 0$ but $(1] \neq 0$ in **Con F**, and that the result is true for $\mathbf{F}/(1]_n$. Hence by Corollary 7.4.

$$w(x,z) = w(z, \ldots, z) + c_1 + \cdots + c_m + e(x,z)$$

where the c_i's are commutators for $\mathcal{U}$ and $e(1]_n z$. Setting each x_i to z we see that $w(z, \ldots, z) = w(z, \ldots, z) + e(z, \ldots, z)$. Thus $e(z, \ldots, z) = z$.

Suppose that e lies in the subalgebra generated by $\{x_1, \ldots, x_r, z\}$ and define

$$u(x,z) = \sum_{S \subseteq \{x_1,\ldots,x_r\}} (-1)^{|S|} e\delta_S.$$

Now a congruence α is said to be *fully invariant* if $\alpha\delta \subseteq \alpha$ for all endomorphisms δ. By Proposition 4.4(1) the commutator of two fully invariant congruences is again fully invariant. From this it follows that $(1]_n$ is fully invariant. Thus since $e\ (1]_n\ z$, $e\delta_S\ (1]_n\ z$ for each S. Thus $e\delta_S\ \zeta\ z$ and hence the order of the sum above is irrelevant. Clearly $u(x,z)$ is a commutator (one needs $e(z) = z$ for the case $r = 0$). Now

$$e = u - \sum_{\emptyset \neq S \subseteq \{x_1,\ldots,x_r\}} (-1)^{|S|} e\delta_S$$

By induction on r, each $e\delta_S$, $S \neq \emptyset$, is a sum of commutators which lie in z/ζ. Hence $e = e_1 + \cdots + e_t$, with e_i a commutator and $e_i\ \zeta\ z$. Hence $w(x,z) = (w(z,\ldots,z) + c_1 + \cdots + c_m) + (e_1 + \cdots + e_t)$. But since $e_i\ \zeta\ z$, $w(x,z) = w(z,\ldots,z) + c_1 + \cdots + c_m + e_1 + \cdots + e_t$, as desired. □

Let $\mathcal{U}$ be a permutable variety and let $\mathbf{A} \in \mathcal{U}$ be a nilpotent algebra. Let $0 \in A$ be fixed but arbitrary. For $a \in \mathbf{A}$, we let $\rho_a : \mathbf{A} \to \mathbf{A}$ be defined by $x\rho_a = x + a$, where $+$ is with respect to 0. By Corollary 7.4, ρ_a is a permutation of $\mathbf{A}$. Let $\mathbf{R}(\mathbf{A})$ be the subgroup of the full symmetric group, $\mathbf{Sym}(\mathbf{A})$, generated by $\{\rho_a : a \in \mathbf{A}\}$.

LEMMA 14.7. *If* $\mathbf{A}$ *is a finite nilpotent algebra then the order of* ρ_a *divides* $|\mathbf{A}|$.

PROOF. Induct on the nilpotency class of $\mathbf{A}$. The initial case is trivial. Let $c \in \mathbf{A}$, and let $n = |\mathbf{A}/\zeta|$, $m = |0/\zeta|$. Then $|\mathbf{A}| = nm$ by Corollary 7.5. By the inductive hypothesis, $c\rho_a^n\ \zeta\ c$. Hence, $c\rho_a^n = c + d$, for some $d \in 0/\zeta$. Since $d \in 0/\zeta$, $(b+d)\rho_a = (b+d) + a = (b+a) + d = b\rho_a + d$. Thus $c\rho_a^{2n} = (c+d)\rho_a^n = c + d + d$. Repeating this argument we obtain $c\rho_a^{nm} = c + md = c$, proving the lemma. □

LEMMA 14.8. *If* $\mathbf{A}$ *is a finite nilpotent algebra then* $\mathbf{R}(\mathbf{A})$ *is a solvable group and if* $\mathbf{A}$ *has prime power order then so does* $\mathbf{R}(\mathbf{A})$.

PROOF. We induct on the class of $\mathbf{A}$. The lemma is clear for the trivial algebra. As was proved in the last lemma, if $c \in 0/\zeta$ then $(x + c)\rho_a = x\rho_a + c$. Hence for any $\rho \in \mathbf{R}(\mathbf{A})$, $(x + c)\rho = x\rho + c$. Thus if $x'\ \zeta\ x$, then by Corollary 7.4 $x' = x + c$ for some $c \in 0/\zeta$, and $x'\rho = x\rho + c\ \zeta\ x\rho$. It follows that there is a natural homomorphism from $\mathbf{R}(\mathbf{A})$ onto $\mathbf{R}(\mathbf{A}/\zeta)$ which maps ρ_a to $\rho_{a/\zeta}$. If ρ is in the kernel K of this homomorphism then for all x there is a $c \in 0/\zeta$ such that

$x\rho = x + c$. Hence if ρ_1 and ρ_2 are in K and $x\rho_i = x + c_i$, then $x\rho_1\rho_2 = x + c_1 + c_2 = x + c_2 + c_1 = x\rho_2\rho_1$, i.e., K is an Abelian normal subgroup. If $\rho \in K$ then the order of ρ divides $|0/\zeta|$ since if $x\rho = x + c$ then $x\rho^k = x + kc$. By induction $\mathbf{R}(\mathbf{A}/\zeta)$ is solvable and so $\mathbf{R}(\mathbf{A})$ is solvable. If $\mathbf{A}$ has prime power order then by induction $R(\mathbf{A}/\zeta)$ has prime power order and so does K. Hence $\mathbf{R}(\mathbf{A})$ has prime power order and so is nilpotent. □

THEOREM 14.9. *Let $\mathcal{V}$ be a modular variety of finite type. If $\mathbf{A} \in \mathcal{V}$ is finite of prime power order and nilpotent then $\mathbf{A}$ is finitely based. In addition there is an integer M such that if $w(x, z)$ is a commutator in more then M variables then $\mathbf{A}$ satisfies $w(x, z) \approx z$.*

PROOF. By Theorem 2.1(1) there is a finitely based permutable variety $\mathcal{U}$ containing $\mathbf{A}$. We let $d(x, y, z)$ be a Mal'cev term for $\mathcal{U}$ will denote a finitely based variety containing $\mathbf{A}$. As the proof proceeds we will add identities to the axioms of $\mathcal{U}$ in such a way that $\mathcal{U}$ is always finitely based and $\mathbf{A} \in \mathcal{U}$.

We proceed by induction on the block size of $[1, 1]$. If this is 1 then $\mathbf{A}$ is a finite Abelian algebra of finite type. By Proposition 5.7 $\mathbf{A}$ satisfies the laws

$$f(d(x_1, y_1, z_1), \ldots, d(x_n, y_n, z_n)) \approx d(f(x), f(y), f(z))$$

for f a basic operation. These laws imply the corresponding laws for f an arbitrary term. In particular, d commutes with itself and so by Lemma 5.6 defines a ternary Abelian group, and any term can be written as a sum (using d) of one and two variable terms, see equation (8) of chapter 9. It follows that the above set of laws of $\mathbf{A}$ together with a finite basis for the two variable laws of $\mathbf{A}$, forms a finite basis for the laws of $\mathbf{A}$. We leave the details and the proof that the last statement of the theorem is true in this case with $M = 3$ to the reader.

Now suppose that $(1]_c = 0$ but $(1]_{c-1} \neq 0$. Of course there are finitely many identities of $\mathbf{A}$ which imply that $\mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(2)$ is finite. We assume that the laws of $\mathcal{U}$ include these laws. By Corollary 14.3 there is a finite set of laws which define $\mathcal{U}_c$ relative to $\mathcal{U}$. We assume that the laws of $\mathcal{U}$ also include these laws so that $\mathcal{U} = \mathcal{U}_c$.

Let $\theta \in \mathbf{Con}\ \mathbf{A}$ with $0 \prec \theta \leq (1]_{c-1} \leq \zeta$. Recall from chapter 4 that $\mathbf{A}(\theta)$ is θ viewed as a subalgebra of $\mathbf{A} \times \mathbf{A}$ and that $\Delta_{\theta,1}$ is the congruence on $\mathbf{A}(\theta)$ generated by $\{\langle\langle a, a\rangle, \langle b, b\rangle\rangle : a, b \in \mathbf{A}\}$. Let $\mathbf{C} = \mathbf{A}(\theta)/\Delta_{\theta,1}$ and $\mathbf{B} = \mathbf{C} \times \mathbf{A}/\theta$.

LEMMA 14.10. *$\mathbf{C}$ is Abelian. Moreover the block size of $[1_{\mathbf{B}}, 1_{\mathbf{B}}]$ is smaller than that of $[1_{\mathbf{A}}, 1_{\mathbf{A}}]$.*

PROOF. Let η_0 and η_1 be the projection congruences on $\mathbf{A}(\theta)$. Then easy calculations show that $\eta_0 + \Delta = \eta_1 + \Delta = 1$ for $\Delta = \Delta_{\theta,1}$. Hence in **Con** $\mathbf{A}(\theta)$, $[1,1] = [\eta_0 + \Delta, \eta_1 + \Delta] \leq \Delta + \eta_0\eta_1 = \Delta$. Thus $\mathbf{C}$ is Abelian.

By Proposition 4.5, $[1_{\mathbf{B}}, 1_{\mathbf{B}}] = [1_{\mathbf{C}} \times 1_{\mathbf{A}/\theta}, 1_{\mathbf{C}} \times 1_{\mathbf{A}/\theta}] = [1_{\mathbf{C}}, 1_{\mathbf{C}}] \times [1_{\mathbf{A}/\theta}, 1_{\mathbf{A}/\theta}] = 0_{\mathbf{C}} \times [1_{\mathbf{A}/\theta}, 1_{\mathbf{A}/\theta}]$. Hence the block size of $[1_{\mathbf{B}}, 1_{\mathbf{B}}]$ equals the block size of $[1_{\mathbf{A}/\theta}, 1_{\mathbf{A}/\theta}]$. Since $\theta \leq [1_{\mathbf{A}}, 1_{\mathbf{A}}]$ the block size of $[1_{\mathbf{A}/\theta}, 1_{\mathbf{A}/\theta}]$ is the block size of $[1_{\mathbf{A}}, 1_{\mathbf{A}}]$ divided by the block size of θ. □

Now by induction and Higman's Lemma, $\mathbf{B}$ has, relative to the laws of $\mathcal{U}$, a finite basis $w_1(x,z) \approx z, \ldots, w_m(x,z) \approx z$, where the w_i's are commutators. Moreover there is a $K \in \omega$ such that if $w(x,z)$ is a commutator in more then K variables then $\mathbf{B}$ satisfies $w(x,z) \approx z$.

LEMMA 14.11. *Let $\mathcal{V}$ be a modular variety and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(X)$ be the free algebra generated by an infinite set X. Then the center of $\mathbf{F}$ is a fully invariant congruence.*

PROOF. Let d be a Gumm difference term for $\mathcal{V}$ and let a, $b \in \mathbf{F}$ with $a\ \zeta_F\ b$. Then by Theorem 14.1, a and b satisfy (1) and (2) of Theorem 14.1 for any choice of the c_i's. There is a finite subset X_0 of X such that a and b are in the subalgebra generated by X_0. Let $x_1, \ldots, x_n$ be in $X - X_0$. Then (1) holds with $c_i = x_i$, $i = 1, \ldots, n$. Let δ be an endomorphism of F and let $c_1, \ldots, c_n \in F$ be arbitrary. Let δ' be the endomorphism of F that agrees with δ on $X - x_1, \ldots, x_n$ and $x_i\delta' = c_i$. Of course, $a\delta = a\delta'$ and $b\delta = b\delta'$. Now we have that (1) of Theorem 14.1 holds with a and b replaced by $a\delta$ and $b\delta$. It now follows from that theorem that $a\delta\ \zeta_F\ b\delta$, as desired. □

Continuing with Theorem 14.9, we let $\mathbf{F} = \mathbf{F}_{\mathcal{U}}(X \cup z)$ where X is a countably infinite set. Recall that 0 is a fixed but arbitrary element of $\mathbf{A}$. Since $\mathbf{B}$ satisfies $w_i(x,z) \approx z$ and $\mathbf{A}/\theta \in \boldsymbol{V}(\mathbf{B})$, for any substitution of the variables into $\mathbf{A}$ with $z \mapsto 0$ we have $w_i(a,0)\theta 0$. Since θ is Abelian and minimal it follows from Exercise 3 of Chapter 9 or from Lemma 14.4 that the group associated with each block of θ is an elementary Abelian p-group. Since $\theta \leq \zeta_{\mathbf{A}}$ we have, by Theorem 14.1, that there is a finite set of laws of $\mathbf{A}$ which imply that $w_i(x,z)\ \zeta_{\mathbf{F}}\ z$, $i = 1, \ldots, m$ and that $w_i(x,z)$ has order p in $\mathbf{F}$. We may assume $\mathcal{U}$ satisfies these laws.

Of course the laws of $\mathbf{B}$ are the elements in the fully invariant congruence generated by the pairs $\langle w_i(x,z), z\rangle$. By Lemma 7.6 this is the congruence

(5)
$$\bigvee (Cg(w_i(u_1, \ldots, u_n, u_0), u_0) : u_i \in F) = \bigvee Cg(d(w_i(u, u_0), u_0, z), z)$$

Let $\bar{w}_i(x_1, \ldots, x_n, x_0, z) = d(w_i(x, x_0), x_0, z)$. Since $w_i(x, z)\ \zeta_F\ z$, $w_i(x, x_0)\ \zeta_{\mathbf{F}}\ x_0$ by Lemma 14.11. Thus we have that $\bar{w}_i(x, x_0, z)\ \zeta_{\mathbf{F}}\ z$.

Now since $\mathbf{B}$ satisfies $w_i(x, z) \approx z$ and $w_i(x, z)$ is a commutator we have

$$b \text{ satisfies } \bar{w}_i(x, x_0, z) \approx z \tag{6}$$

$$\mathcal{U} \text{ satisfies } w_i(z, z, z) \approx z \tag{7}$$

LEMMA 14.12. *Suppose that B satisfies $u(x, z) \approx z$. Then there are idempotent terms $r_j(x, z)$ such that*

$$u(x, z) = \sum r_j(v_j, z) \tag{8}$$

where each v_j has the form $\bar{w}_i(s_1, \ldots, s_k, s_0, z)$ for some $s_0, \ldots, s_k \in F$. Moreover, $r_j(v_j, z)\ \zeta_{\mathbf{F}}\ z$.

PROOF. Since $u(x, z) \approx z$ holds in $\mathbf{B}$, $< u(x, z), z >$ is in the congruence given by (5), i.e., the congruence generated by the pairs $algorithm\bar{w}_i(s_1, \ldots, s_n, s_0, Z), z\rangle$ with $s_i \in \mathbf{F}$. Since $\bar{w}_i(x, x_0, z)\ \zeta_{\mathbf{F}}\ z$ and the center is a fully invariant congruence of $\mathbf{F}$, the first part of the result now follows from lemma 14.4. Since $v_i\ \zeta_{\mathbf{F}}\ z$ and r_j is idempotent the last statement is also true. □

LEMMA 14.13. *Suppose that $\mathbf{B}$ satisfies $u(x_1, \ldots, x_n, z) \approx z$ and $t_i(x, z) \approx z$, $i = 1, \ldots, n$. If $\mathbf{A}$ satisfies $u(z, \ldots, z) \approx z$ then it satisfies*

$$u(t_1(x, z), \ldots, t_n(x, z), z) \approx z.$$

PROOF. Let f be a homomorphism from $\mathbf{F}$ to $\mathbf{A}$ and let $f(x_i) = a_i$, $i = 1, \ldots, n$, and let $0 \in \mathbf{A}$ denote $f(z)$. Since $\mathbf{A}/\theta$ is in $\boldsymbol{V}(\mathbf{B})$ and $\mathbf{B}$ satisfies $t_i(x, z) \approx z$, $t_i(a, 0)\theta 0$. Let $c_i = t_i(a, 0)$, $i = 1, \ldots, n$, so that $c_i\ \theta\ 0$. Then, since $\mathbf{C} = \mathbf{A}(\theta)/\Delta_{\theta,1}$ satisfies $u(x, z) \approx z$, we have in $\mathbf{A}(\theta)$

$$\begin{aligned} \langle u(c_1, \ldots, c_n, 0), 0\rangle &= \langle u(c_1, \ldots, c_n, 0), u(0, \ldots, 0)\rangle \\ &= u(\langle c_1, 0\rangle, \ldots, \langle c_n, 0\rangle, \langle 0, 0\rangle) \\ &\equiv \langle 0, 0\rangle \mod \Delta_{\theta,1} \end{aligned}$$

By Theorem 4.9 this implies that $\langle u(c_1, \ldots, c_n, 0), 0\rangle \in [\theta, 1] = 0$. Hence $u(c_1, \ldots, c_n, 0) = 0$ in $\mathbf{A}$, proving the lemma. □

LEMMA 14.14. *There is a finite set of laws of $\mathbf{A}$ which imply*

$$u(a_1 + v(x, z), a_2, \ldots, a_n, z) = u(a_1, \ldots, a_n, z)$$

for all $a_i \in \mathbf{F}$ and for all $u(x, z)$ and $v(x, z)$ such that $\mathbf{B}$ satisfies $u(x, z) \approx z$, $v(x, z) \approx z$, and $\mathcal{U}$ satisfies $u(z, z) \approx z$.

PROOF. Assume that $\mathbf{B}$ satisfies $u(x,z) \approx z$, $v(x,z) \approx z$, and that $\mathcal{U}$ satisfies $u(z) \approx z$. Since $\langle v, z\rangle$ is in the fully invariant congruence generated by the $\langle w_i, z\rangle$, which are contained in $\zeta_{\mathbf{F}}$ by Lemma 14.11, $v\ \zeta_{\mathbf{F}}\ z$. Thus by Proposition 5.7 and the fact $u(z,z) = z$ we have

$$\begin{aligned} u(a_1 + v, a_2, \ldots, a_n, z) \\ &= u(d(v,z,a_1), d(z,z,a_2), \ldots, d(z,z,a_n), d(z,z,z)) \\ &= d(u(v,z,\ldots,z), u(z,\ldots,z), u(a_1,\ldots,a_n,z)) \\ &= d(u(v,z,\ldots,z), z, u(a_1,\ldots,a_n,z)) \\ &= u(a_1,\ldots,a_n,z) + u(v,z,\ldots,z,z) \end{aligned}$$

for all $a_i \in \mathbf{F}$. By Lemma 14.13, $u(v,z,\ldots,z) \approx z$ is an identity of $\mathbf{A}$. Hence it suffices to show there is a finite set of laws of $\mathbf{A}$ which imply all laws of the form $u(v,z,\ldots,z) \approx z$, where u and v satisfy the hypotheses of the lemma.

Since $\mathbf{B}$ satisfies $u(\mathbf{x},z) \approx z$, we can use Lemma 14.12 to write $u(\mathbf{x},z)$ in the form (8) as described in the lemma. Writing this out in full gives

$$u(\mathbf{x},z) = \sum r_j(\bar{w_{i_j}}(s_1^j(\mathbf{x},z),\ldots,s_n^j(\mathbf{x},z), s_0^j(\mathbf{x},z),z),z) \tag{9}$$

where the r_j are idempotent. If we apply the endomorphism which sends x_1 to v and the other generators to z, we have

$$\begin{aligned} u(v,z,\ldots,z) = \\ \sum_j (\bar{w_{i_j}}(s_1^j(v,z,\ldots,z),\ldots,s_n^j(v,z,\ldots,z), s_0^j(v,z,\ldots,z),z),z) \end{aligned}$$

Since $v\ \zeta_{\mathbf{F}}\ z$, $s_k^j(v,z)\ \zeta_{\mathbf{F}}\ s_k^j(z,z)$. Now in general by Proposition 5.7 if $a\ \zeta\ b$ then $d(d(a,b,c),c,e) = d(a,b,e)$ (see the proof of (3) above). Thus using Proposition 5.7 we obtain the following where, of course, $a - b = d(a,b,z)$ and $a + b = d(a,z,b)$

$$\begin{aligned} u(v,z,\ldots,z) = \sum r_j(\bar{w_{i_j}}(s_1^j(v,\mathbf{z}) - s_1^j(z,\mathbf{z}),\ldots,s_0^j(v,\mathbf{z}) - s_0^j(z,\mathbf{z}),z),z) \\ + \sum r_j(\bar{w_{i_j}}(s_1^j(z,\mathbf{z}),\ldots,s_0^j(z,\mathbf{z}),z),z) \end{aligned} \tag{10}$$

Applying to (9) the endomorphism which sends all the generators to z we obtain

$$z = u(z,\mathbf{z}) = \sum r_j(\bar{w_{i_j}}(s_1^j(z,\mathbf{z}),\ldots,s_0^j(z,\mathbf{z}),z),z)$$

From this and (10) we see that it suffices to show that there is a finite set of laws of $\mathbf{A}$ which imply the laws

$$\bar{w}_i(t_i(v,\mathbf{z}),\dots,t_n(v,\mathbf{z}),t_0(v,\mathbf{z}),z)\approx z \tag{11}$$

where $t_j(x_1,\dots,x_m)$ are idempotent.

Since $v\ \zeta_{\mathbf{F}}\ z$, $t_j(v,\mathbf{z})\ \zeta_{\mathbf{F}}\ t_j(z,\mathbf{z})=z$. Thus by equation (3) or (7) of chapter 9 (or by using Proposition 5.7) we have that the left side of (11) is the sum of elements of the form

$$\bar{w}_i(z,\dots,z,t_j(v,\mathbf{z}),z,\dots,z). \tag{12}$$

Since $\mathbf{B}$ satisfies $v(\mathbf{x},z)\approx z$, we have by Lemma 14.12 that $v(\mathbf{x},z)=\sum r_j(q_j,z)$ where r_j is idempotent and q_j has the form $\bar{w_{i_j}}(p_1,\dots,p_n,p_0,z)$, $p_i\in\mathbf{F}$. Since $r_j(q_j,z)\ \zeta_F\ z$ by Lemma 14.12, (12) can be expressed as a sum of elements of the form

$$\bar{w}_i(z,\dots,z,\overset{m^{\text{th}}}{t_m(r_j(q_j,z),z,\dots,z)},\dots,z)$$

It follows that (11) is a consequence of the laws

$$\bar{w}_i(z,\dots,\overset{m^{\text{th}}}{t_m(r_j(\bar{w_{i_j}}(x,y,z),z),\dots,z)},\dots,z)\approx z \tag{13}$$

Since both t_m and r_j are idempotent and $\mathbf{B}$ satisfies $\bar{w}_i(x,y,z)\approx z$ by (6), $\mathbf{B}$ satisfies

$$t_m(r_j(\bar{w_{i_j}}(\mathbf{x},y,z),z),z,\dots,z)\approx z$$

Thus by Lemma 14.13 equation (13) is a law of $\mathbf{A}$.

Since $t_m(r_j(x,z),z,\dots,z)$ is binary and there are only a fixed number of $\bar{w}_i$, there are only finitely many laws of the form (13). This completes the proof of the lemma. □

THEOREM 14.15. *There is an N and a finite set of laws of $\mathbf{A}$ such that if these laws are added to the axioms of $\mathfrak{U}$ then $b_j\in\mathbf{F}$ implies $\bar{w}_i(b_1,\dots,b_n,b_0,z)$ is a sum of elements of the form $\pm\bar{w}_i(a_1,\dots,a_n,a_0,z)$ where each a_j is a sum of at most N commutators and an element in the subalgebra generated by z.*

PROOF. Recall that by Lemma 14.8, $\mathbf{R}(\mathbf{A})$ is a finite p-group. Let $\mathbb{Z}_p(\mathbf{R}(\mathbf{A}))$ be the group ring of $\mathbf{R}(\mathbf{A})$ over the integers modulo p, i.e., $\mathbb{Z}_p(\mathbf{R}(\mathbf{A}))=\sum k_\rho\rho : k_\rho\in\mathbb{Z}_p$ with the multiplication induced from $\mathbf{R}(\mathbf{A})$. The Jacobson radical of this ring is the augmentation ideal: $\sum k_\rho\rho:\sum k_\rho=0$. For a proof of this fact see Satz 5.16 on page 484 of Huppert [**50**]. Hence $\rho-1$ is in the radical. Since the ring is finite, the radical is nilpotent, i.e., there is an N such that the product of any N elements of the radical is 0. Thus if $\rho_1,\dots,\rho_N\in\mathbf{R}(\mathbf{A})$ then

$$(\rho_1-1)(\rho_2-1)\dots(\rho_N-1)=0 \tag{14}$$

in $\mathbb{Z}_p(\mathbf{R}(\mathbf{A}))$. Fix $a, a_1, \ldots, a_n \in \mathbf{A}$. For $S = \{i < j < \cdots < k\}$ a subset of $\{1, .., N\}$ let $a_S = a_i + a_j + \cdots + a_k$ associated left to right. We claim that the number of even subsets S with $a = a_S$ equals modulo p the number of odd subsets with $a = a_S$. To see this let $\mathbf{V}$ be a vector space over $\mathbb{Z}_p$ with the set A as a basis (be careful to note that $0_{\mathbf{A}} \neq 0_{\mathbf{V}}$). Let $\mathbb{Z}_p(\mathbf{R}(\mathbf{A}))$ act on $\mathbf{V}$ by extending the natural action of $\mathbf{R}(\mathbf{A})$ on A. In (14) let $\rho_i = \rho_{a_i}$ then expanding out (14) we have

$$\sum_S (-1)^{|S|} \rho_{a_i} \rho_{a_j} \rho_{a_k} = 0$$

in $\mathbb{Z}_p(\mathbf{R}(\mathbf{A}))$. Applying this to the vector space element $0_{\mathbf{A}}$ (which, recall, is a basis element of $\mathbf{V}$) we obtain

$$0_{\mathbf{V}} = \sum_S (-1)^{|S|} 0_{\mathbf{A}} \rho_S, \tag{15}$$

where $0_{\mathbf{A}} \rho_S = 0_{\mathbf{A}} \rho_{a_i} \rho_{a_j} \ldots \rho_{a_k} = 0 + a_i + a_j + \cdots + a_k = a_i + a_j + \cdots + a_k$. Looking at the coefficient of a in (15) gives the claim.

Hence if $w(x, z)$ $\zeta_{\mathbf{F}}$ z and has order p then for all $b_2, \ldots, b_n \in \mathbf{A}$

$$\sum_S (-1)^{|S|} w(a_S, b_2, \ldots, b_n, 0) = 0$$

Thus $\mathbf{A}$ satisfies the finite set of laws of the form

$$\sum_S (-1)^{|S|} \bar{w}_i(x_1, \ldots, x_{j-1}, y_S, x_{j+1}, \ldots, x_n, x_0, z) \approx z$$

where $y_S = y_i + y_j + \cdots + y_k$. One term in this sum has $y_1 + \cdots + y_N$ in the j^{th} place and this law allows us to express this term as a sum of terms in which the j^{th} entry has fewer than N summands. The lemma now follows from Lemma 14.6. □

Now we are ready to complete the proof of Theorem 14.9. We assume that the finite set of laws which imply the conclusions of Lemma 14.14 and Theorem 14.15 is contained in the laws of $\mathcal{U}$. Let p be the maximum of the number of variables in the $\bar{w}_i$'s plus 2. Set $M = PNK$. Let $w(x_1, \ldots, x_n, z)$ be a commutator with $n > M$ and w actually depending on $x_1, \ldots, x_n$. Since $M \geq K$, $w(x, z) \approx z$ is a law of $\mathbf{B}$. By Lemma 14.12 and Lemma 14.6 $w(x, z)$ is a sum of terms of the form

$$r(\bar{w}_i(a_1, \ldots, a_k, a_0, z), z) \tag{16}$$

where $r(x, z)$ is an idempotent binary term and where each a_i is a sum of commutators and an element from the subalgebra generated by z. By Lemma 14.14 we may assume that no commutator in these sums involves more than K variables. Since r is a binary idempotent term it corresponds to an element of $\mathbf{R}(\mathcal{U})$ as defined in chapter 9. Since

$\bar{w}_i(a_1, \ldots, a_k, a_0, z)\ \zeta_{\mathbf{F}}\ z$, r will distribute across sums of such elements. (This fact can be derived directly from Proposition 5.7.) Thus using Theorem 14.15 we may assume that the a_i's are sums of an element of the subalgebra generated by z and at most N commutators. Since $k + 2 \leq P$ we see that w is a sum of terms each of which lies in a subalgebra of $\mathbf{F}$ generated by at most M of the variables, i.e.,

$$w(x, z) = u_1(x, z) + \cdots + u_r(x, z)$$

where $u_i(x, z)\ \zeta\ z$ and $u_i(x, z)$ is contained in a subalgebra generated by at most M of the variables. Let $w(x, z)$ involve variables in S and possibly z. Then, since each u_i is independent of at least one variable in S,

$$\begin{aligned} w &= w\delta_S^* \\ &= u_1\delta_S^* + \cdots + u_r\delta_S^* \\ &= z + \cdots + z \\ &= z \end{aligned}$$

in $\mathbf{F}$. This proves that there is a finite set of laws of $\mathbf{A}$ which imply that any commutator in more than M variables is trivial. Of course the second part of Theorem 14.9 follows from this. The first part follows from this and Higman's Lemma. □

THEOREM 14.16. *If $\mathbf{A}$ is a finite nilpotent algebra in a modular variety $\mathcal{V}$, which is a product of algebras of prime power order, then $\mathbf{A}$ has a finite basis for its laws. Moreover there is an integer M such that if $w(x, z)$ is a commutator in more then M variables, then $\mathbf{A}$ satisfies $w(x, z) \approx z$.*

PROOF. Let $\mathbf{A}$ be nilpotent of class c and suppose that $\mathbf{A}$ is a direct product of $\mathbf{A}_1, \ldots, \mathbf{A}_k$, where each $\mathbf{A}_i$ has prime power order. Then each $\mathbf{A}_i$ is nilpotent so by Theorem 14.9 there is an integer M such that if $w(x, z)$ is a commutator in more then M variables then $w(x, z) \approx z$ is a law of each $\mathbf{A}_i$. Hence $w(x, z) \approx z$ is a law of $\mathbf{A}$. The proof that $\mathbf{A}$ is finitely based is by induction on the block size of $[1, 1]$ as in the proof of Theorem 14.9. Again we choose $\theta \in \mathbf{Con}\ \mathbf{A}$ with $0 \prec \theta \leq (1]_{c-1} \leq \zeta$ and let $\mathbf{C} = \mathbf{A}(\theta)/\Delta_{\theta,1}$. Let $w_1, \ldots, w_m$ be a set of commutators such that $w_1(x, z) \approx z, \ldots, w_m(x, z) \approx z$ is a basis of $\mathbf{A}/\theta \times \mathbf{C}$. The only part of the proof of the previous theorem which required that $\mathbf{A}$ have prime power order was the proof of Theorem 14.15. However the conclusion of Theorem 14.15, with $N = M$, follows from the fact that

$$\sum_S (-1)^{|S|} \bar{w}_i(x_1, \ldots, x_{j-1}, y_S, x_{j+1}, \ldots, x_n, x_0, z) \approx z$$

(where the sum is over all $S \subseteq \{1, 2, \ldots, M+1\}$) is a law of $\mathbf{A}$, which it is since the left side is a commutator involving more that M variables. □

It is an open problem if every finite nilpotent algebra is finitely based. However M. Vaughan-Lee [**81**] has constructed a 12 element nilpotent loop such that there is no M such that commutators in more then M variables are trivial. Thus Theorem 14.9 and Theorem 14.16 are not true for arbitrary finite nilpotent algebras.

CHAPTER 15

Pure Lattice Congruence Identities

This chapter is being written.

In Chapter 8 we examined several serveral congruence identities; this is, equations in the language with three binary operations $\vee$, $\wedge$ and the commutator operation. We call such equations *congruence identities*. We examined the consequences of congruence identities in Chapters 8 and 10.

In this chapter we present some of the major results about congruence identities that only involve join and meet and not the commutator. We concentrate on results that were proved with the aid of, or whose proofs have been simplified by, the commutator. [Check that this is true in the end.] We let

$$\mathbf{Con}(\mathcal{V}) = \{\mathbf{Con}(\mathbf{A}) : \mathbf{A} \in \mathcal{V}\}$$

and define the **congruence variety** associated with a variety $\mathcal{V}$ to be the variety of lattices generated by all the congruence lattices of the members of $\mathcal{V}$; that is, $\boldsymbol{V}(\mathbf{Con}(\mathcal{V}))$.

THEOREM 15.1. *Let $\mathcal{V}$ be a modular variety and let $\mathcal{A}$ be its Abelian subvariety. Let $\mathbf{R} = \mathbf{R}(\mathcal{A})$ be the ring associated with $\mathcal{A}$ and let $\mathcal{M}$ be the variety of left $\mathbf{R}$–modules.*

(1) *The congruence variety of $\mathcal{V}$ contains that of $\mathcal{M}$.*
(2) *If $\mathcal{V}$ is Abelian, that is, $\mathcal{V} = \mathcal{A}$, then congruence variety of $\mathcal{V}$ equals that of $\mathcal{M}$.*

[better notation and terminology.]

PROOF. Of course the first statement follows from the second which follows from Proposition 9.19 and Lemma 9.14. □

[To be covered:

- the congruence variety of an Abelian variety is that of the variety of modules over its ring and the congruence variety of every modular variety contains that of its Abelian subvariety.
- Describe the congruence varieties assoc with modules.
- minimal modular congruence varieties
- Palfy Szabo thm, no proof.

- Day Kiss
- Freese Jonsson
- Haiman
- Freese Lipparini
- Freese
- Mal'cev condition for every lattice eq (Czedli, Lipparini, et al)
- Problem: Does Con(A) have a representation as a lattice of permuting equivalence relations?

[Describe all congruence varieties associated with modules, Hutchinson.]

So what are the congruence varieties of varieties of modules? For each function f defined on the set of prime numbers into $\omega \cup \{\infty\}$, we define $\mathbf{R}_f$ to be the ring $\mathbf{Z}[X]/I$ where $X = \{x_p : p \text{ a prime with } f(p) \neq \infty\}$ and I is the ideal generate by the elements $x_p p^{f(p)+1} - p^{f(p)}$.

For a ring $\mathbf{R}$ with 1 of characterisic 0, let $f_{\mathbf{R}}(p)$ be the least integer k such that there is an $a \in \mathbf{R}$ such that $ap^{k+1} = p^k$. If no such k exists, $f_{\mathbf{R}}(p) = \infty$. Let $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$ denote the ring of integers modulo n. The congruence varieties associated with varities of modules have been characterized by G. Hutchinson and G. Czedli [**51**] as follows:

THEOREM 15.2. *Let $\mathbf{R}$ be a ring with 1 and let $\mathcal{M}_{\mathbf{R}}$ be the variety of $\mathbf{R}$–modules. Let n be the characteristic of $\mathbf{R}$. Then*

1. *if $n > 0$ the congruence variety of $\mathcal{M}_{\mathbf{R}}$ is the same as the one associated with $\mathbf{Z}_n$,*
2. *if $n = 0$ the congruence variety of $\mathcal{M}_{\mathbf{R}}$ is the same as the one associated with $\mathbf{R}_{f_{\mathbf{R}}}$.*

[We may give a proof or a sketch or some exercises outlining the proof.]

One can easily check the order within the congruence varieties associated with modules:

THEOREM 15.3. *Let n and $m > 1$ be integers, p a prime, and suppose $n = p^e k$, where p does not divide k. Then*

1. $\boldsymbol{V}(\mathbf{Con}(\mathcal{M}_{\mathbf{Z}_n})) \subseteq \boldsymbol{V}(\mathbf{Con}(\mathcal{M}_{\mathbf{Z}_m}))$ *if and only if n divides m,*
2. $\boldsymbol{V}(\mathbf{Con}(\mathcal{M}_{\mathbf{Z}_n})) \subseteq \boldsymbol{V}(\mathbf{Con}(\mathcal{M}_{\mathbf{R}_f}))$ *if and only if $e \leq f(p)$,*
3. $\boldsymbol{V}(\mathbf{Con}(\mathcal{M}_{\mathbf{R}_f})) \subseteq \boldsymbol{V}(\mathbf{Con}(\mathcal{M}_{\mathbf{Z}_n}))$ *never holds,*
4. $\boldsymbol{V}(\mathbf{Con}(\mathcal{M}_{\mathbf{R}_f})) \subseteq \boldsymbol{V}(\mathbf{Con}(\mathcal{M}_{\mathbf{R}_g}))$ *if and only if $f(p) \leq g(p)$ for all primes.*

Using Theorems 15.1 and 15.3 we can show that the minimal modular congruence varieties are just those associated with the varieties of vector spaces over prime fields.

COROLLARY 15.4. *If $\mathcal{V}$ is a congruence modular, nondistributive variety of algebras then $\mathbf{V}(\mathbf{Con}(\mathcal{V}))$ contains either $\mathbf{V}(\mathbf{Con}(\mathcal{M}_{\mathbf{Z}_p}))$, for some prime p, or $\mathbf{V}(\mathbf{Con}(\mathcal{M}_{\mathbf{Q}}))$, where $\mathbf{Q}$ is the rationals.*[1]

Since, if α/β is an interval in $\mathbf{Con}(\mathbf{A})$ which contains a sublattice isomorphic to $\mathbf{M}_3$ with greatest element α and least element β, it is Abelian, there was hope that every modular congruence variety arises from a variety of modules. This is Problem 8.11 which was open at the time of the first edition of this book. But this difficult problem was refuted by P. P. Pálfy and C. Szabó in [**69**] and [**68**].

THEOREM 15.5. *Let $\mathcal{V}$ be the variety generated by $\mathbf{Q}$, the 8 element quaternion group. Then there is a lattice identity true in all lattices of subgroups of Abelian groups but which fails $\mathbf{Con}(\mathbf{F}_{\mathcal{V}}(5))$.*

We will not prove this here; the proof in [**68**] is quite readable. This result is much more subtle than one might suspect. See [**6**] for further discussion of this problem for group varieties. Incidentally $|\mathbf{Con}(\mathbf{F}_{\mathcal{V}}(5))| = 2^{20}$.

Despite this there are some positive results. A. Day and E. Kiss [**22**] give general conditions on a variety that do guarentee its congruence variety is the congruence variety of some variety of modules. The definition of $\mathbf{R}(\mathcal{V})$ is given in Definition 9.3.

THEOREM 15.6. *Let $\mathcal{V}$ be a congruence modular variety which is not congruence distributive. If $\mathcal{V}$ is residually small and locally finite (or residually small and solvable) then the congruence variety associated with $\mathcal{V}$ is the same as that of $\mathcal{M}$, the variety of modules over $\mathbf{R}(\mathcal{V})$.*

PROOF. By R. Wille [**82**] and A Pixley [**73**] pure lattice equation holding in the congruence lattices of a variety are definable by indempotent, weak Mal'cev conditions. This implies that the congruence variety associated with a variety is the same as the one associated with its idempotent reduct. Thus we may assume $\mathcal{V}$ is idempotent.

Checking the definition of $\mathbf{R}(\mathcal{V}) = \mathbf{R}(\mathcal{V}, 1)$ given in Defitions 9.2 and 9.3, we see that it only depends on $\mathbf{F}_{\mathcal{V}}(u, v_0)/[\theta_0, \theta_0]$, where $\theta_0 = \mathrm{Cg}(u, v_0)$. But since $\mathcal{V}$ is idempotent, $\theta_0 = 1$. Thus *if $\mathcal{V}$ is idempotent then $\mathbf{R}(\mathcal{V}) = \mathbf{R}(\mathcal{A})$, where $\mathcal{A}$ is the Abelian subvariety of $\mathcal{V}$.* Of course

[1]This result, due to Freese [**24**], has an easy direct modular-lattice theoretic proof. The result has been extended in two directions. First, Day and Freese [**23**] showed that Polin's variety, mentioned in Example 11.2, is contained in every non-modular congruence variety. Second, in as yet unpublished work, Paolo Lipparini and Freese show that *if $\mathcal{V}$ is a variety which is not congruence meet semidistributive, then the congruence variety associated with $\mathcal{V}$ contains one of the minimal modular congruence varieties of this corollary.*

the congruence variety of $\mathcal{A}$ is a subvariety of the congruence variety of $\mathcal{V}$. Hence by Theorem 15.1, the congruence variety of $\mathcal{M}$ is contained in the congruence variety of $\mathcal{V}$.

Suppose β is an Abelian congruence on $\mathbf{A} \in \mathcal{V}$. Then by Theorem 9.9 the direct sum $\sum_{i<\lambda} \mathbf{M}(\beta, z_i)$ of the blocks is a module over $\mathbf{R}(\mathcal{V}, \lambda)$ whose congruence lattice is isomorphic to the interval $\beta/0$. This module is of course a module over $\mathbf{R}(\mathcal{V})$ and thus $\beta/0$ is embedded into the congruence lattice (the submodule lattice) of an $\mathbf{R}(\mathcal{V})$–module.

The definition of a neutral element in a modular lattice with least and greatest element is given in Exercise 4 of Chaper 8. If u is such an element in $\mathbf{L}$ then $\mathbf{L}$ is a subdirect product of the intervals $1/u$ and $u/0$. It is also shown there that if **Con A** satisfies the congruence equation (C1) then $[1, 1]$ is neutral. The same argument shows that $[\alpha, \alpha]$ is neutral in the interval $\alpha/0$.

If $\mathcal{V}$ is residually small it satisfies equation (C1) by Theorem 10.14. If $\mathcal{V}$ is solvable then, for each $\mathbf{A} \in \mathcal{V}$, the solvable sequence of Defition 6.1 is eventually 0:

$$1 = [1]^0 \geq [1, 1] = [1]^1 \geq [[1, 1], [1, 1]] = [1]^2 \geq \cdots \geq [1]^k = 0$$

for some k. By the remarks above **Con A** is a subdirect product of the intervals $[1]^j/[1]^{j+1}$ each of which is embedded into the congruence lattice of an $\mathbf{R}(\mathcal{V})$–module, proving the theorem in this case.

Now suppose $\mathcal{V}$ is locally finite and residually small. Let $\mathbf{A}$ be a finitely generated (and thus finite) algebra in $\mathcal{V}$ and let $\theta \in$ **Con A**. Suppose $[\theta, \theta] = \theta$ and let α be a lower cover of θ. We claim α is neutral in the interval $\theta/0$. Otherwise there exist β and $\gamma \leq \theta$ such that

$$\alpha \leq \alpha \vee (\beta \wedge \gamma) < (\alpha \vee \beta) \wedge (\alpha \vee \gamma) \leq \theta$$

Since $\alpha \prec \theta$, this implies $\beta \wedge \gamma \leq \alpha$ and $\theta = \alpha \vee \beta = \alpha \vee \gamma$ and so $[\theta, \theta] = [\alpha \vee \beta, \alpha \vee \gamma] \leq \alpha \vee (\beta \wedge \gamma) = \alpha < \theta$, contradicting $[\theta, \theta] = \theta$.

Thus by choosing $\theta_0 = 1$ and θ_{j+1} to be $[\theta_j, \theta_j]$ if $[\theta_j, \theta_j] < \theta_j$ and to be any lower cover otherwise, we obtain a chain $1 = \theta_0 > \theta_1 > \cdots > \theta_k = 0$ such that θ_{j+1} is neutral in $\theta_j/0$. Hence **Con A** is a subdirect product of the intervals θ_j/θ_{j+1}, each of which is either embeddable in the congruence lattice of an $\mathbf{R}(\mathcal{V})$–module or the two element lattice, which of course can also be so ebedded. Hence **Con A** is embeddable in the congruence lattice of an $\mathbf{R}(\mathcal{V})$–module. □

There are several open problems some of which were presented in Chapter 8.

PROBLEM 15.7. *Is the congruence variety associated with loops (or with quasigroups) the largest modular congruence variety?*

PROBLEM 15.8. *Is there a largest modular congruence variety?*

PROBLEM 15.9. *Is the congruence variety associated with loops distinct from the one associated with groups?*

In [**47**] Hobby and McKenzie show that for each finite algebra $\mathbf{A}$ there is a finite loop with operators such that $\mathbf{Con\ A} \cong \mathbf{Con\ B}$. Thus the congruence variety associated with every locally finite, congruence modular variety is contained in the congruence variety associated with loops.

1. The Arguesian Equation

Recall from Definition 6.1 that $[\delta]^2 = [[\delta, \delta], [\delta, \delta]]$.

LEMMA 15.10. *Let* $\alpha_i,\ \beta_i \in \mathbf{Con\ A}$, $i = 0, 1, 2$ *where* $\mathbf{A}$ *is in a modular variety. Let*

$$\delta = (\alpha_0 \vee \beta_0) \wedge (\alpha_1 \vee \beta_1) \wedge (\alpha_2 \vee \beta_2)$$

Then

$$\delta = \big((\alpha_0 \circ \beta_0) \cap (\alpha_1 \circ \beta_1) \cap (\alpha_2 \circ \beta_2)\big) \circ [\delta]^2$$

PROOF. Of course δ contains the right side of the above equation. To see the other direction we let, for congruences α and β, $\alpha \circ_m \beta = \alpha \circ \beta \circ \alpha \cdots$ with $m - 1$ occurrences of $\circ$. We shall show that if $m > 2$ then

$$(1)\quad ((\alpha_0 \circ_m \beta_0) \cap (\alpha_1 \circ_m \beta_1) \cap (\alpha_2 \circ_m \beta_2)) \circ [\delta]^2 \subseteq ((\beta_0 \circ_{m-1} \alpha_0) \cap (\beta_1 \circ_{m-1} \alpha_1) \cap (\beta_2 \circ_{m-1} \alpha_2)) \circ [\delta]^2$$

Then if λ_m denotes the left side of (1) then we get $\lambda_m \subseteq \lambda_2$, at least if m is even. But if m is odd $\lambda_m \subseteq \lambda_{m+1} \subseteq \lambda_2$ so $\lambda_m \subseteq \lambda_2$ for all $m \geq 2$.

The lemma follows from $\lambda_m \subseteq \lambda_2$ since if $\langle a, b\rangle \in \delta$ then $\langle a, b\rangle \in (\alpha_0 \circ_m \beta_0) \cap (\alpha_1 \circ_m \beta_1) \cap (\alpha_2 \circ_m \beta_2)$ for some m, which is contained in the left side of (1).

So suppose

$$a\ (\alpha_0 \circ_m \beta_0) \cap (\alpha_1 \circ_m \beta_1) \cap (\alpha_2 \circ_m \beta_2)\ b\ [\delta]^2\ c$$

Then $a = a_{0i}\ \alpha_i\ a_{1i}\ \beta_i\ a_{2i}\ \alpha_i\ a_{3i}\ \beta_i\ a_{4i} \cdots a_{mi} = b$. Let $d_2(x, y, z)$ be the generalized Gumm difference term defined in Exercise 9 of Chapter 6. Then by that exercise we have

$$a = d_2(a_{1i}, a_{1i}, a)\ \beta_i\ d_2(a_{2i}, a_{1i}, a)\ \alpha_i\ d_2(a_{3i}, a, a)\ \beta_i\ d_2(a_{4i}, a, a)\ \alpha_i \cdots\ d_2(a_{mi}, a, a) = d_2(b, a, a)\ [\delta]^2\ b$$

Thus

$$a\ (\beta_0 \circ_{m-1} \alpha_0) \cap (\beta_1 \circ_{m-1} \alpha_1) \cap (\beta_2 \circ_{m-1} \alpha_2)\ d_2(b,a,a)\ [\delta]^2\ b\ [\delta]^2\ c$$

proving (1) and thus the lemma. □

THEOREM 15.11. *If* $\mathbf{A}$ *lies in a modular variety then* $\mathbf{Con\ A}$ *is arguesian. That is, if* α_i *and* $\beta_i \in \operatorname{Con}\mathbf{A}$, $i = 0, 1, 2$ *then*

(2) $(\alpha_0 \vee \beta_0) \wedge (\alpha_1 \vee \beta_1) \wedge (\alpha_2 \vee \beta_2) \leq (\alpha_1 \wedge ((\gamma_0 \wedge (\gamma_1 \vee \gamma_2)) \vee \alpha_2)) \vee \beta_1$

where $\gamma_0 = (\alpha_1 \vee \alpha_2) \wedge (\beta_1 \vee \beta_2)$ *and* γ_1 *and* γ_2 *are defined cyclically.*

PROOF. By Lemma 15.10 it suffices to show that both $[\delta]^2$ and

$$(\alpha_0 \circ \beta_0) \cap (\alpha_1 \circ \beta_1) \cap (\alpha_2 \circ \beta_2)$$

lie in the right side of (2). The latter is straightforward. For the former let ε be the expression obtained from δ using the distributive law:

$$\begin{aligned}\varepsilon = {} & (\alpha_0 \wedge \alpha_1 \wedge \alpha_2) \vee (\alpha_0 \wedge \alpha_1 \wedge \beta_2) \vee (\alpha_0 \wedge \beta_1 \wedge \alpha_2) \vee (\alpha_0 \wedge \beta_1 \wedge \beta_2) \\ & (\beta_0 \wedge \alpha_1 \wedge \alpha_2) \vee (\beta_0 \wedge \alpha_1 \wedge \beta_2) \vee (\beta_0 \wedge \beta_1 \wedge \alpha_2) \vee (\beta_0 \wedge \beta_1 \wedge \beta_2)\end{aligned}$$

Now

$$[\delta]^2 \leq [\delta, [\delta, \delta]] \leq [\alpha_0 \vee \beta_0, [\alpha_1 \vee \beta_1, \alpha_2 \vee \beta_2]] \leq \varepsilon$$

and clearly ε is contained in the right side, proving the theorem. □

Related Literature

Reading the first treatises on general commutator theory was, to many longtime enthusiasts of the subject of varieties, like opening a hidden door onto a bright new world of unsuspected possibilities. It appeared that many problems long solved (or partially solved) for distributive varieties and varieties of modules, could now be attacked directly in modular varieties. The high expectation has been realized, in many instances. We shall mention several areas, and papers, in which commutator theory has been exploited very successfully.

Smith [**79**] obtained new uniqueness theorems for direct decompositions of finite algebras in varieties with permuting congruences. Gumm and Herrmann [**42**] expanded these results to modular varieties and refined them. Two algebras $\mathbf{A}$ and $\mathbf{B}$ in a modular variety $\mathcal{V}$ are said to be it isotopic in $\mathcal{V}$ if there is an algebra $\mathbf{C}$ in $\mathcal{V}$ and an isomorphism between $\mathbf{A} \times \mathbf{C}$ and $\mathbf{B} \times \mathbf{C}$ which commutes with the projections onto $\mathbf{C}$. (Exercise: If $\mathbf{A}$ and $\mathbf{B}$ are isotopic in $\mathcal{V}$ then $\mathbf{C}$ can be taken to be an Abelian algebra in $\mathcal{V}$.) Let $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ be algebras in a modular variety $\mathcal{V}$ such that the congruences of $\mathbf{A}$ satisfy the ascending chain condition, and the congruences below the center of $\mathbf{A}$ satisfy the descending chain condition. The authors proved that if $\mathbf{A} \times \mathbf{B}$ and $\mathbf{A} \times \mathbf{C}$ are isomorphic (or merely isotopic in $\mathcal{V}$), then $\mathbf{B}$ and $\mathbf{C}$ are isotopic in $\mathcal{V}$. They also proved an isotopic refinement theorem for algebras which satisfy these chain conditions. (For finite algebras, these results were essentially proved by B. Jonsson in [**53**]).

The next group of applications appeared in a sequence of five papers co-authored by McKenzie. The first paper, Freese-McKenzie [**29**], contained a characterization of finitely generated, residually small, modular varieties, proved here in Chapter 10, Section 3. The second, Burris-McKenzie [**8**] and [**9**],determined the structure of locally finite modular varieties with a decidable first order theory. It turned out that these varieties decompose as the product of an Abelian variety and a discriminator variety. This pointed up the desirability of determining which finite rings have a decidable theory of modules, a problem that is still open. the third, Baldwin-McKenzie [**1**], solved a counting problem

for modular varieties. The weak fine spectrum function of a variety $\mathcal{V}$ is the function $f(\kappa)$ which is defined to be ω plus the number of non-isomorphic κ-element members of $\mathcal{V}$, κ a cardinal. The authors proved that modular varieties of countable type have precisely six different weak fine spectrum functions. McKenzie [**64**] investigated residual smallness in varieties of rings. It turned out that for these varieties, (and for varieties of linear associative algebras over any commutative ring $\mathbf{K}$) the main theorem of the paper in this series does not require the hypothesis of finite generation. Thus a variety of $\mathbf{K}$-algebras is residually small if and only if it satisfies the congruence identity (C1) of chapter 8. McKenzie [**63**] used commutator theory to characterize the finitely generated varieties that have only finitely many finite directly indecomposable algebras, after first proving that a variety with this property has permuting congruences.

Some of the results from Freese's papers [**26**], [**27**], were proved here in Chapter 10. The results of Chapter 13 are his. The proof of the extension of M. Vaughan-Lee's finite basis theorem contained in Chapter 14 is his work. The structural relation between the module associated with an Abelian congruence and the algebra, Theorem 9.9, is his.

A sequence of important papers by E. Kiss deserve special mention. Kiss [**57**] proved that a modular variety has the property that principal congruences are always complemented if and only if it decomposes as $\mathcal{A} \otimes \mathcal{F}$ where $\mathcal{F}$ is a filtral variety (and therefore distributive), and $\mathcal{A}$ is an Abelian variety whose ring is semisimple Artinian. This extended the result of C. Herrmann [**46**] that a variety with complemented modular congruence lattices is Abelian, see exercise 11 of Chapter 5. Kiss [**55**] investigated the congruence extension property. He succeeded in relating it very closely to two special properties of the commutator. (See Theorem 8.3). This allowed him to prove, for example, that a locally finite modular variety has the congruence extension property if and only if the square of each of its subdirectly irreducible algebras has the property. Closely related to this work is a paper of B. A. Davey and L. G. Kovacs [**18**], which applies commutator theory to the study of injective hulls, and the existence of enough injectives, in modular varieties. Kiss [**58**] presented a short and elegant proof of a result of Burris and McKenzie: If $\mathcal{K}$ is a finite class if finite algebras such that every member of $\mathcal{V} = \boldsymbol{V}(\mathcal{K})$ is a Boolean product of algebras from $\mathcal{K}$,then $\mathcal{V}$ is the product of an Abelian variety and a discriminator variety.

In a very recent paper, [**56**], Emil Kiss gave a very nice generalization of Gumm's difference term. Recall that we defined a difference term to be a term $d(x, y, z)$ such that $d(x, x, z) = z$ and $d(x, z, z)$ $[\theta, \theta]$ x

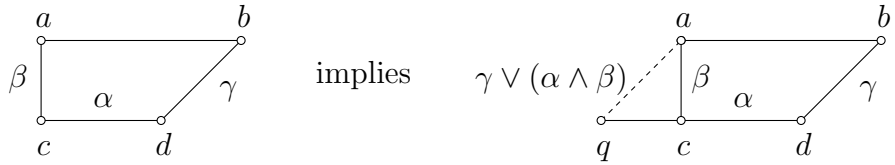
whenever $x \ \theta \ z$. Proposition 5.7 gave very useful necessary and sufficient conditions for $[\alpha, \beta] = 0$ in terms of this difference term when α and β are comparable. The hypothesis that α and β be comparable is necessary in that theorem. [However, see exercise 8 where it is shown that Proposition 5.7 does work in permutable varieties or if α is Abelian. See also McKenzie [**65**] for some related theorems using the Gumm terms constructed in Theorem 6.4] Kiss defines a **4-difference term** for $\mathcal{V}$ to be a term $q(x, y, u, v)$ satisfying $q(x, y, x, y) = x$ and $q(x, x, u, u) = u$, and if $\mathbf{A} \in \mathcal{V}$ and

$$(*) \qquad \begin{bmatrix} a & c \\ b & d \end{bmatrix}, \begin{bmatrix} a & c' \\ b & d \end{bmatrix} \in \mathbf{A}(\alpha, \beta)$$

(see Definition 4.7) then

$$q(a, b, c, d) \ [\alpha, \beta] \ q(a, b, c', d).$$

In a manner analogous to Theorem 5.5 and Proposition 5.7 he shows that every modular variety possess a 4-difference term, and that it can be used to complete diagrams as shown in the figure.



Compare this figure with the figure of Theorem 5.5. He then goes on to prove an analogue of Proposition 5.7, but without the assumption that the congruences are comparable. Namely, he shows that $[\alpha, \beta] = 0$ if and only if $q : \mathbf{A}(\alpha, \beta) \to \mathbf{A}$ is a homomorphism and if $(*)$ holds then

$$q(a, b, c, d) = q(a, b, c', d).$$

In a distributive variety one can take $q(x, y, u, v) = u$; in a permutable variety with Mal'cev term $p(x, y, z)$ one can take $q(x, y, u, v) = q(x, y, v)$. If q is a 4-difference term then $d(x, y, z) = q(x, y, z, z)$ is a difference term.

In this same paper Kiss answers a question raised by McKenzie in [**63**]. He shows that in a finitely directly representable variety every directly indecomposable algebra is either finite or Abelian.

Two recent papers of C. Bergman [**2**] and [**3**] studied the congruence extension property in modular varieties. Building on results presented there, Bergman and McKenzie have shown [unpublished] that a residually small modular variety γ with the amalgamation property also possesses the congruence extension property, provided that one of

these conditions is satisfied: (1) $\mathcal{V}$ is distributive; (2) $\mathcal{V}$ is a variety of groups; (3) $\mathbf{F}_{\mathcal{V}}(2)$ is finite.

The original *Overview* manuscript mentioned the problem of finding ring $\mathbf{R}(\mathcal{V}, 1, 0)$ when $\mathcal{V}$ is the variety of groups or of commutative rings. This problem was solved first by David Hobby, essentially before that manuscript was circulated. P. Zlatoš solved the problem independently and B. Sivák has calculated these rings for numerous varieties of groups. For the variety of groups the ring is $\mathbb{Z}[x, x^{-1}]$. Day and Kiss [**22**] show that for $\mathcal{V}$ the variety of groups, $R(\mathcal{V}, n, 0)$ is the group ring over the integers of the free group on n generators. L. G. Kovács in unpublished work clarified exactly how $\mathbb{Z}[x, x^{-1}]$ acts on an Abelian group congruence. Let $\mathbf{H}$ be an Abelian normal subgroup of $\mathbf{G}$ and let $z \in G$. Recall that if θ is the congruence associated with $\mathbf{H}$, then $\mathbf{M}(\theta, z)$ is the $\mathbf{H}$ coset containing z with addition defined by $a + b = d(a, z, b) = az^{-1}b$. It is easy to see that under this addition each coset is isomorphic to $\mathbf{H}$ as an Abelian group. Kovács showed that x (from $\mathbb{Z}[x, x^{-1}]$) acts on this coset by conjugation by z. In particular, the modules $\mathbf{M}(\theta, z_2)$ will not be isomorphic unless $z_1^{-1}z_2$ lies in the centralizer of $\mathbf{H}$.

The paper of A. Day and E. Kiss [**22**] has already been mentioned above and in connection with congruence identities of locally residually small varieties, in Chapter 8. The paper contains some suggestive results that may turn out to be very significant. For one example: the ring $\mathbf{R}(\mathcal{V}, 1, 0)$ of a variety is isomorphic to a ring produced via the classical von Neumann Coordinatization process from a natural it frame of congruence in a free algebra.

W. A. Lampe, who was one of the independent discoverers of the term condition, used it to show that certain compactly generated lattices can be represented as congruence lattices only by algebras with a large set of operations, see R. Freese, W. A. Lampe, and W. Taylor [**28**]. Recently he has solved an old problem by showing that $\mathbf{M}_3$ is never the lattice of subvarieties of a variety $\mathcal{V}$, Lampe [**60**]. $\mathcal{V}$ here is not assumed to be modular. If we let $\mathbf{F}$ be the free algebra $\mathbf{F}_{\mathcal{V}}(\omega)$ with the endomorphism adjoined as additional operations, then it is well known that the lattice of subvarieties of $\mathcal{V}$ is dually isomorphic to **Con F**. Lampe's proof shows that if $\mathcal{V}$ is modular then **Con F** satisfies $[1, 1] = 1$ (and hence **Con F** cannot have an $\mathbf{M}_3$ at the top).

A. Ursini has worked out a theory of it ideal determined varieties, having a constant 0 and the property that every it ideal is a congruence class of a unique congruence. (Examples: groups, rings, loops.) In Gumm-Ursini [**43**], the authors proved that every ideal determined

variety is congruence modular, and they sketched some details of a theory of commutators of ideals. This theory covers a range of varieties in which commutator theory is more directly accessible to the intuition than in the general modular varieties.

To conclude, let us address the question: Is viable commutator theory inherently restricted to modular varieties, or is it possible to extend usable fragments of it into some wider arena? The paper P. Zlatoš [**83**], is an attempt to provide axioms for a more general theory. In the book by D. Hobby and R. McKenzie [**47**], a theory of congruences in finite algebras is developed, called by the authors *tame congruence theory*, which reveals that the 'commutator' $C(\alpha, \beta)$, defined in Chapter 3, has interesting properties when restricted to locally finite algebras. If we define solvability in terms of this commutator, then the congruence lattice of a locally finite algebra $\mathbf{A}$ admits a congruence $\sim$ under which $\alpha \sim \beta$ (where $\alpha \geq \beta$) if and only if restricted to every finite subalgebra $\mathbf{B}$, $\beta|_{\mathbf{B}}$ is solvable over $\alpha|_{\mathbf{B}}$. Moreover, $(\mathbf{Con}\ \mathbf{A})/\sim$ satisfies the meet semidistributive law $(x \wedge y = x \wedge z \Rightarrow x \wedge (y \vee z) = x \wedge y)$. If $\mathbf{A}$ belongs to a locally finite variety that obeys a nontrivial pure congruence identity, then each equivalence class $\alpha/\sim$ is a modular lattice; moreover, Abelian congruences of $\mathbf{A}$ then have the expected structure, as if $\mathbf{A}$ belonged to a modular variety. In the first paragraph of Chapter 8, we remarked that there exist nonmodular varieties which satisfy a nontrivial pure congruence identity. Among the results of McKenzie and Hobby is the theorem that no locally finite variety of this kind can be residually small.

Solutions To The Exercises

Chapter 1

1.1. A term for $\mathcal{V}$ has the form $r_1x_1 + \cdots + r_nx_n$ where r_i is either an element of the ring or an integer. (We will usually only unitary $\mathbf{R}$-modules, in which case each r_i is in the ring.) From this description of terms it is easy to see that the term condition holds for all submodules $\mathbf{M}$ and $\mathbf{N}$. For the second part let $\mathbf{M}$ and $\mathbf{N}$ be submodules of a module $\mathbf{K}$. In $\mathbf{K} \times \mathbf{K}$ let $A = \{\langle m, 0\rangle : m \in M\}$ and $B = \{\langle 0, n\rangle : n \in N\}$ and let $\pi : \mathbf{K} \times \mathbf{K} \to \mathbf{K}$ be the homomorphism $\pi(x, y) = x + y$. Then $\pi(A) = M$ and $\pi(B) = N$. Since $A \cap B = 0$, (2) implies that $[\mathbf{M}, \mathbf{N}] = 0$.

Chapter 2

2.1. A quasigroup satisfies the cancellation law $a \cdot b = a \cdot c \Rightarrow b = c$, since $b = a \setminus (a \cdot b) = a \setminus (a \cdot c) = c$. Similarly $a \cdot c = b \cdot c \Rightarrow a = b$. Thus the map $b \to a \cdot b$ is one-one. Since $a \cdot (a \setminus b) = b$, it is onto as well. A universal algebraic proof of the last statement of the problem is this. Let $\mathbf{A}$ be a finite quasigroup and let $\mathbf{F} = \mathbf{F}_{\mathbf{V}(\mathbf{A})}(x, y)$ be the free algebra on two generators. Let B be the smallest subset of F containing x such if $b \in B$ then $b \cdot y \in B$. B inherits the cancellation and since $\mathbf{F}$ is finite, B is finite. Thus the map $b \to b \cdot y$, $b \in B$, is one-one. Since B is finite and the image is in B, it is onto so there is a $b \in B$ such that $b \cdot y = x$. Of course there is a term $t(x, y)$ using only $\cdot$ which represents b. Hence, $x = t(x, y) \cdot y$. Since $x = (x/y) \cdot y$ we have $t(x, y) = x/y$ by cancellation. Notice that we have actually proved a little more. Namely x/y is equivalent to a term of the form $(\cdots(x \cdot y) \cdot y) \cdots) \cdot y$.

2.2. We calculate

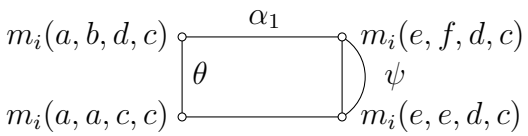
$$\begin{aligned} p(x, x, y) &= (x/(x \setminus x)) \cdot (x \setminus y) \\ &= ((x \cdot (x \setminus x))/(x \setminus x)) \cdot (x \setminus y) \\ &= x \cdot (x \setminus y) \\ &= y \end{aligned}$$

Similar calculations establish the other identities.

2.3. This is established with straightforward calculations; see Day [**19**].

2.4. Since $\langle b, d\rangle \in \gamma \leq \gamma \vee (\theta_0 \wedge \theta_1)$, this follows from the Shifting Lemma (2.4).

2.5. Clearly $m_i(e,e,c,c)\ \theta\ m_(e,f,d,c)$ and $m_i(e,e,c,c)\ \alpha_2\ m_i(e,e,e,e) = e = m_i(e,d,d,e)\ \alpha_2\ m_i(e,f,d,c)$. Thus since $\theta \wedge \alpha_2 \leq \psi$, we have $m_i(e,e,c,c)\ \psi\ m_i(e,f,d,c)$. Thus we have the relations indicated in the figure.



Thus $m_i(a,b,d,c)\ \psi\ m_i(a,a,c,c)$ by the Shifting Lemma (2.4) and so $a\ \psi\ c$ by Lemma 2.3.

Chapter 4

4.1. Note

$$\begin{bmatrix} p(p(x,b,y),b,b) & p(p(x,b,b),b,b) \\ p(p(b,b,y),b,x) & p(p(b,b,b),b,x) \end{bmatrix} = \begin{bmatrix} p(x,b,y) & x \\ p(y,b,x) & x \end{bmatrix}$$

is in $\mathrm{M}(\theta,\psi)$. Thus $p(x,b,y)[\theta,\psi]p(y,b,x)$. Since $[\theta,\psi] = 0$, $x + y = y + x$. Similarly

$$\begin{bmatrix} p(p(x,b,b),b,p(y,b,z)) & p(p(x,b,y),b,p(y,y,z)) \\ p(p(x,x,b),b,p(y,b,z)) & p(p(x,x,y),b,p(y,y,z)) \end{bmatrix}$$

$$= \begin{bmatrix} p(x,b,p(y,b,z)) & p(p(x,b,y),b,z) \\ p(y,b,z) & p(y,b,z) \end{bmatrix}$$

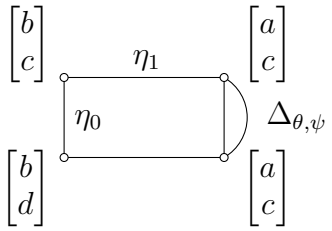
shows that $x + (y + z) = (x + y) + z$.

4.2. Both are the congruence on $\mathbf{A}(\psi)$ generated by $\{\langle\langle x,x\rangle, \langle y,y\rangle\rangle : x\ \theta\ y\}$. The statement $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Delta_{\psi,\theta}$ is equivalent to $\langle\langle a,b\rangle, \langle c,d\rangle\rangle$ being in this congruence which in turn is equivalent to $\begin{bmatrix} a & c \\ b & d \end{bmatrix} \in \Delta^{\theta,\psi}$.

4.3. Parts (i) and (ii) are obvious as is most of (iii). If $\begin{bmatrix} x & y \\ u & v \end{bmatrix} \in \Delta^{\theta,\psi}$ then $\begin{bmatrix} u & v \\ x & y \end{bmatrix} \in \Delta^{\theta,\psi}$ simply because $\Delta^{\theta,\psi}$ is symmetric. Clearly if $\begin{bmatrix} x & y \\ u & v \end{bmatrix} \in \mathrm{M}(\theta,\psi)$ then $\begin{bmatrix} u & v \\ x & y \end{bmatrix} \in \mathrm{M}(\theta,\psi)$. Now by Lemma 4.8, $\Delta_{\theta,\psi}$ is

the transitive closure of $\mathrm{M}(\theta, \psi)$ and it follows easily from this that the above implication holds for $\Delta_{\theta,\psi}$.

4.4. Since $\begin{bmatrix} a & a \\ c & d \end{bmatrix} \in \Delta_{\theta,\psi}$ and $\begin{bmatrix} a \\ b \end{bmatrix} \in \theta$, a, b, c, and d are θ-related. Now we have the relations indicated in the figure, where the η_i's are the projection kernels.



Since $\eta_0 \wedge \eta_1 = 0$, the result follows from the Shifting Lemma (2.4).

4.5. Let $\Delta = \Delta_{\theta,\psi}$ and suppose $\begin{bmatrix} x & y \\ u & v \end{bmatrix}$ and $\begin{bmatrix} u & v \\ r & s \end{bmatrix}$ are in Δ. We will apply Lemma 2.3 with $a = \begin{bmatrix} x \\ r \end{bmatrix}$, $b = \begin{bmatrix} x \\ u \end{bmatrix}$, $c = \begin{bmatrix} y \\ s \end{bmatrix}$, and $d = \begin{bmatrix} y \\ v \end{bmatrix}$. Now $\mathit{algorithm} b, d\rangle \in \Delta$ by assumption. Since $\begin{bmatrix} u \\ r \end{bmatrix} \Delta \begin{bmatrix} v \\ s \end{bmatrix}$ and $\begin{bmatrix} u \\ u \end{bmatrix} \Delta \begin{bmatrix} v \\ v \end{bmatrix}$ we have

$$\begin{bmatrix} m_i(u,u,v,v) \\ m_i(r,u,v,s) \end{bmatrix} = \left[\begin{bmatrix} u \\ r \end{bmatrix}, \begin{bmatrix} u \\ u \end{bmatrix}, \begin{bmatrix} v \\ v \end{bmatrix}, \begin{bmatrix} v \\ s \end{bmatrix} \right] \Delta \begin{bmatrix} u \\ r \end{bmatrix}$$

We also have

$$\begin{bmatrix} m_i(u,u,v,v) \\ m_i(r,r,s,s) \end{bmatrix} = m_i \left[\begin{bmatrix} u \\ r \end{bmatrix}, \begin{bmatrix} u \\ r \end{bmatrix}, \begin{bmatrix} v \\ s \end{bmatrix}, \begin{bmatrix} v \\ s \end{bmatrix} \right] \Delta \begin{bmatrix} u \\ r \end{bmatrix}$$

Hence by the previous exercise $\begin{bmatrix} m_i(x,x,y,y) \\ m_i(r,u,v,s) \end{bmatrix} \Delta \begin{bmatrix} m_i(x,x,y,y) \\ m_i(r,r,s,s) \end{bmatrix}$. This says $m_i(a,b,d,c) \ \Delta \ m_i(a,a,c,c)$ and so by Lemma 2.3 $a \ \Delta \ c$, i.e., $\begin{bmatrix} x & y \\ r & s \end{bmatrix} \in \Delta$. Thus $\Delta_{\theta,\psi}$ is a transitive relation on $\mathbf{A}(\psi)$ and it contains $\mathrm{M}(\theta, \psi)$. Hence by Lemma 4.8 $\Delta^{\theta,\psi} \subseteq \Delta_{\theta,\psi}$ and by symmetry they are equal.

4.6. Let $\gamma = (\bigwedge \alpha_i : \beta)$. Then $[\gamma, \beta] \leq \bigwedge \alpha_i$ and γ is the largest such congruence. Since $[\gamma, \beta] \leq \bigwedge \alpha_i \leq \alpha_i$, $\gamma \leq \bigwedge(\alpha_i : \beta)$. By monotonicity $[\bigwedge(\alpha_i : \beta), \beta] \leq \bigwedge[(\alpha_i : \beta), \beta] \leq \bigwedge \alpha_i$. Hence $\bigwedge(\alpha_i : \beta) \leq \gamma$.

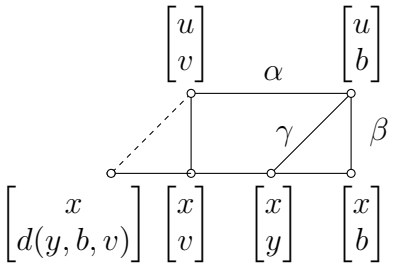
Chapter 5

5.1. Let α, β and γ be congruences which pairwise intersect to 0 and pairwise join to 1. Then $[1,1] = [\alpha \vee \beta, \alpha \vee \gamma] = [\alpha, \alpha] \vee [\alpha, \gamma] \vee [\beta, \alpha] \vee [\beta, \gamma] \leq \alpha \vee (\beta \wedge \gamma) = \alpha$. Similarly $[1,1] \leq \beta$ and so $[1,1] = 0$.

5.2. Clearly (ii) $\Rightarrow$ (i) $\Rightarrow$ (iii). Let $\mathbf{B}$ is a subdirect power of two copies of $\mathbf{A}$ such that $\mathbf{Con}\ \mathbf{B}$ has $\mathbf{M}_3$ as a 0, 1-sublattice. By the previous exercise $\mathbf{B}$ is Abelian. $\mathbf{A}$ is a homomorphic image of $\mathbf{B}$, so by Proposition 4.4(1) $\mathbf{A}$is Abelian. Hence (iii) $\Rightarrow$(iv). Suppose that $\mathbf{A}$ is Abelian and let $\Delta_{1,1}$ be the congruence in Definition 4.7. If follows directly from Theorem 4.9 (and Exercise 4.3(iii)) that $\eta_i \wedge \Delta_{1,1} = 0$, where η_i, $i = 0, 1$ are the projection kernels. Moreover it is shown in the proof of Theorem 4.11 that $\eta_i \vee \Delta_{11} = 1$. Hence (iv) $\Rightarrow$ (ii).

5.3. By Exercise 2, $\mathbf{B}$ is Abelian, and so affine by Herrmann's theorem. Thus $x - y + z$ is a term operation on $\mathbf{B}$. In particular, $\mathbf{B}$ has a Mal'cev term and thus has permutable congruences. Hence the projection kernels permute and join to 1 so the subdirect product is direct.

5.4. Suppose that $\begin{bmatrix} x \\ y \end{bmatrix} \gamma \circ \alpha \begin{bmatrix} u \\ v \end{bmatrix}$. Then there is a $b \in \mathbf{B}$ such that $\begin{bmatrix} x \\ y \end{bmatrix} \gamma \begin{bmatrix} u \\ b \end{bmatrix} \alpha \begin{bmatrix} u \\ v \end{bmatrix}$. Then we have



Hence $\begin{bmatrix} x \\ y \end{bmatrix} \alpha \begin{bmatrix} x \\ d(y,b,v) \end{bmatrix} \gamma \begin{bmatrix} u \\ v \end{bmatrix}$, showing that α and γ permute.

5.5. The inverse map is $y \mapsto d(y, v, u)$. To see this note that by Proposition 5.7

$$\begin{aligned} d(d(x,u,v),v,u) &= d(d(x,u,v), d(u,u,v), d(u,u,u)) \\ &= d(d(x,u,u), d(u,u,u), d(v,v,u)) \\ &= d(x,u,u) = x. \end{aligned}$$

It follows that the map is a bijection. Another application of Proposition 5.7 shows that it preserves addition.

5.6. To see that (i) holds apply condition (iii) with $x = y$, $z = u = u'$, $\alpha = \gamma = 0$, and $\beta = 1$. This gives $d(u, u, y) = y$. Now by taking $u = u'$ it is easy to derive the Shifting Lemma from condition (iii) (cf. Exercise 4 of Chapter 2). As pointed out in Chapter 2, this implies $\mathcal{V}$ is modular. Now suppose that $a\ \theta\ b$. Apply (iii) to $\mathbf{A}(\theta)$ with $x = z = \begin{bmatrix} b \\ b \end{bmatrix}$, $y = u' = \begin{bmatrix} a \\ b \end{bmatrix}$, $u = \begin{bmatrix} a \\ a \end{bmatrix}$, $\alpha = \eta_1$, $\beta = \eta_0$, and $\gamma = \Delta_{\theta,\theta}$ (the η_i's are the projection kernels). This gives $\begin{bmatrix} a \\ d(a,b,b) \end{bmatrix} = \begin{bmatrix} d(a,a,a) \\ d(a,b,b) \end{bmatrix}\ \Delta\ \begin{bmatrix} b \\ b \end{bmatrix}$, which by Theorem 4.9 implies $a\ [\theta, \theta]\ d(a, b, b)$, as desired.

5.7. $\begin{bmatrix} (x \cdot y)/(y \cdot x) & (1 \cdot y)/(y \cdot 1) \\ (x \cdot 1)/(1 \cdot x) & (1 \cdot 1)/(1 \cdot 1) \end{bmatrix} = \begin{bmatrix} (x \cdot y)/(y \cdot x) & 1 \\ 1 & 1 \end{bmatrix} \in \mathrm{M}(1, 1)$. Since $\mathbf{A}$ is Abelian, this gives $(x \cdot y)/(y \cdot x) = 1$ and so $x \cdot y = y \cdot x$. Starting with $((x \cdot y) \cdot z)/(x \cdot (y \cdot z))$ in the upper left corner of a matrix, a similar proof gives associativity.

5.8. Let $p(x, y, z)$ be either of the Mal'cev terms given in Exercise 2 of Chapter 2. Then p is a difference term and by Proposition 5.7 it suffices to show that p commutes with the basic operations. By Exercise 1 of Chapter 2 / and \ are equal on $\mathbf{G}$ to a term using only the multiplication. Thus it is enough to show that p commutes with multiplication, i.e.,

$$(*) \qquad p(x_1, y_1, z_1) \cdot p(x_2, y_2, z_2) = p(x_1 \cdot x_2, y_1 \cdot y_2, z_1 \cdot z_2).$$

Since G has 4 elements, there are only $4^6 = 4096$ cases to check. You may want to use a computer.

There is an easier solution to this problem. If $\mathbf{A}$ is an affine algebra with $\hat{\mathbf{A}} = \langle A, +, -, 0 \rangle$ as its Abelian group, then it is not hard to show that if $t(x, y)$ is a binary term operation on $\mathbf{A}$ then there are endomorphisms σ and τ of $\hat{\mathbf{A}}$ and $c \in \mathbf{A}$ such that $t(x, y) = \sigma(x) + \tau(y) + c$, see Chapter 9. Knowing what to look for, it is not hard to find such a representation for the multiplication in $\mathbf{G}$. Namely start with the four element group which is the direct product of two copies of the two element group, i.e., $\{0, 1, 2.3\}$ with $x + x = 0$, and $x + y = z$ if x and y are distinct members of $\{1, 2, 3\}$ and z is the remaining member. Let σ be the identity, τ transpose 2 and 3, and $c = 3$. Since τ is an automorphism of the group, the operation $x \cdot y = x + \tau(y) + 3$ defines an Abelian quasigroup which equals $\mathbf{G}$.

5.9. Take the cyclic group of order four, $\{0, 1, 2, 3\}$, and let σ interchange 2 and 3. Then the multiplication of the given quasigroup is $x \cdot y = \sigma(x) + y$. Since σ is not a group automorphism, $\mathbf{A}$ is not Abelian. In fact $(*)$ of the previous solution fails with $y_1 = 1$ and all other

variables 0. However, it is possible to show that $p(x, y, z) = x - y + z$ and thus $x +_c y = p(x, c, y)$ is an Abelian group operation.

5.10. It is routine to verify that $\mathbf{G}$ is a loop with $\langle 0, 0\rangle$ as its identity element and that the second projection is a homomorphism. It is also easy to see that $\mathbf{H} \cong \mathbb{Z}_4$. Suppose that $[\theta, \theta] = 0$. Then for all $z \in \mathbf{H}$, and all x, y, y' with $y\theta y'$

$$(*) \qquad (x + (y + z))/(x + y) = (x + (y' + z))/(x + y').$$

To see this just note that the following matrix is in $\mathrm{M}(\theta, \theta)$.

$$\begin{bmatrix} (x + (y + z))/(x + y) & (x + (y + 0))/(x + y) \\ (x + (y' + z))/(x + y) & (x + (y' + 0))/(x + y') \end{bmatrix}$$

$$= \begin{bmatrix} (x + (y + z))/(x + y) & 0 \\ (x + (y' + z))/(x + y') & 0 \end{bmatrix}$$

Now if we let $z = \langle 1, 0\rangle$, $x = \langle 0, 1\rangle$, $y = \langle 1, 1\rangle$, and $y' = \langle 2, 1\rangle$ then the left side of $(*)$ evaluates to $\langle 2, 2\rangle/\langle 0, 2\rangle = \langle 2, 0\rangle$ and the right side evaluates to $\langle 3, 2\rangle/\langle 2, 2\rangle = \langle 1, 0\rangle$. Thus $(*)$ fails in $\mathbf{G}$ and hence $[\theta, \theta] \neq 0$.

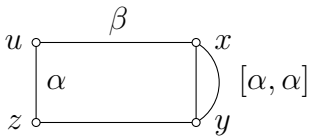
5.11. Since the congruence lattices are complemented, every subdirectly irreducible algebra in $\mathcal{V}$ is simple. If all of these subdirectly irreducible algebras are Abelian then $\mathcal{V}$ is Abelian. Thus let $\mathbf{A}$ be a simple, non-Abelian algebra in $\mathcal{V}$. Let I be an infinite set and let $\mathbf{B}$ the direct product of $|I|$ copies of $\mathbf{A}$. Define $\lambda \in \mathbf{Con}\ \mathbf{B}$ by $x\lambda y$ if and only if $x_i = y_i$ for all but finitely many i. Let λ' be a complement of λ in $\mathbf{Con}\ \mathbf{B}$, and let η_i be the kernel of the projection onto the i^{th} coordinate. Clearly $\eta_i \not\geq \lambda$. If $\lambda' \leq \eta_i$ for all i, then $\lambda' = 0$. But then $\lambda = 1$, which is false. Thus, for some i, $\lambda' \not\leq eta_i$. From this and the fact that η_i is a coatom it follows that $\eta_i \wedge (\lambda \vee \lambda')$, η_i, $\eta_i \wedge (\lambda' \vee \lambda)$ generates an $\mathbf{M}_3$ with greatest element 1. But then $[1, 1] \leq \eta_i$, which implies $\mathbf{A}$ is Abelian by Proposition 4.4(1). This contradiction proves that $\mathcal{V}$ is Abelian.

Chapter 6

6.1. By reversing the roles of α and β in Theorem 6.2 we obtain $\beta \circ \alpha \subseteq [\beta]^k \circ \alpha \circ \beta$. Now if $\langle x, y\rangle \in \alpha \circ \beta$ then $\langle y, x\rangle \in \beta \circ \alpha \subseteq [\beta]^k \circ \alpha \circ \beta$. Hence $\langle x, y\rangle \in \beta \circ \alpha \circ [\beta]^k$, as desired.

6.2. By the last exercise $\alpha \circ \beta \subseteq \beta \circ \alpha \circ [\beta]^n$. By Theorem 6.2 $\alpha \circ [\beta]^n \subseteq [\alpha]^m \circ [\beta]^n \circ \alpha$ and hence $\alpha \circ \beta \subseteq \beta \circ [\alpha]^m \circ [\beta]^n \circ \alpha$. Of course if $[\alpha]^m$ and $[\beta]^n$ permute for some m and n, then $\alpha \circ \beta \subseteq \beta \circ \alpha$ as $[\alpha]^m \subseteq \alpha$ and $[\beta]^n \subseteq \beta$.

6.3. Clearly it suffices to show that if α and β permute then $[\alpha, \alpha]$ and β permute. Suppose that $x\ [\alpha, \alpha]\ y\ \beta\ z$. Then since α and β permute there is some u such that $x\ \beta\ u\ \alpha\ z$. Thus we have the relations indicated in the figure.



By the shifting lemma $u\ [\alpha, \alpha] \vee (\alpha \wedge \beta)\ z$. We will show that $[\alpha, \alpha]$ and $\alpha \wedge \beta$ permute. From this it follows that for some v we have $x\ \beta\ u\ \alpha \wedge \beta\ v\ [\alpha, \alpha]\ z$, i.e., $x\ \beta\ v\ [\alpha, \alpha]\ z$, showing that $[\alpha, \alpha]$ and β permute. To see that $[\alpha, \alpha]$ and $\alpha \wedge \beta$ permute observe by the previous exercise, with $n = m = 1$,

$$\begin{aligned}(\alpha \wedge \beta) \circ [\alpha, \alpha] &\subseteq [\alpha, \alpha] \circ [\alpha, \beta]^1 \circ [[\alpha, \alpha]]^1 \circ (\alpha \wedge \beta) \\ &= [\alpha, \alpha] \circ (\alpha \wedge \beta)\end{aligned}$$

since both $[\alpha \wedge \beta]^1$ and $[[\alpha, \alpha]]^1$ are contained in $[\alpha, \alpha]$.

6.4. Suppose that $(\alpha, \alpha]^m = 0 = (\beta, \beta]^n$. We claim that $(\alpha \vee \beta, \alpha \vee \beta]^{m+n} = 0$. Now $(\alpha \vee \beta, \alpha \vee \beta]^{m+n}$ is the commutator of $m + n + 1$ copies of $\alpha \vee \beta$, associated right to left. If we expand this using the commutator, we obtain a sum of terms of the form

$$[\gamma_0, [\gamma_1, \dots [\gamma_{m+n-1}, \gamma_{m+n}] \dots],$$

where each γ_i is either α or β. Now either there are at least $m + 1$ γ's equal to α or $n + 1$ γ's equal to β. Thus each term in our sum is either less then or equal to $(\alpha]^m$ or $(\beta]^n$, and hence 0.

6.5. Let $x, y \in \mathbf{A} \in \mathcal{V}$ and suppose that $x\ \theta\ y$. We must show that $x\ [\theta, \theta]\ p(x, y, y)$. Since $p(x, y, y) = q_n(x, y, y)$, and $q_0 = x$, it suffices to show that, for each i, $q_i(x, y, y)\ [\theta, \theta]\ q_{i+1}(x, y, y)$. For i even the two sides are actually equal by Theorem 6.4(3). For i odd first we need to show that for all i, $q_i(x, y, y)\ [\theta, \theta]\ q_i(x, x, y)$. The following matrix is in $\mathrm{M}(\theta, \theta)$:

$$\begin{bmatrix} q_i(x,y,y) & q_i(x,x,y) \\ q_i(x,y,x) & q_i(x,x,x) \end{bmatrix} = \begin{bmatrix} q_i(x,y,y) & q_i(x,x,y) \\ x & x \end{bmatrix}.$$

Hence $q_i(x, y, y)\ [\theta, \theta]\ q_i(x, x, y)$, as desired. Now for i odd, $q_i(x, y, y)\ [\theta, \theta]$ $q_i(x, x, y) = q_{i+1}(x, x, y)\ [\theta, \theta]\ q_{i+1}(x, y, y)$, proving the result.

6.6. Each of (1) to (8) is either obvious or can be verified by straightforward calculations. For example, to see that (3) holds, suppose that $K(a, b, c, d)$ holds and that $s(c, a, \mathbf{e}) = s(c, b, \mathbf{e})$. Let $u =$

$s(d,a,\mathbf{e})$, $v = s(d,b,\mathbf{e})$, and $w = s(c,a,\mathbf{e}) = s(c,b,\mathbf{e})$. We need to show that $u = v$. Using $K(a,b,c,d)$ (with the $s(a,\mathbf{e}) = s(a,e_0,\dots,e_k)$ from the definition of $K(a,b,c,d)$ taken to be $s(e_0,a,e_1,\dots,e_k)$ from the present context) we have

$$\begin{aligned} q_i(u,w,v) &= q_i(s(d,a,\mathbf{e}), s(c,b,\mathbf{e}), s(d,b,\mathbf{e})) \\ &= q_i(s(d,a,\mathbf{e}), s(d,b,\mathbf{e}), s(d,b,\mathbf{e})) \\ &= q_i(u,v,v). \end{aligned}$$

Similarly $q_i(u,w,v) = q_i(u,u,v)$. Hence $q_i(u,v,v) = q_i(u,u,v)$. Thus, by Theorem 6.4, $u = p(u,v,v)$. But $K(a,b,c,d)$ also implies that $p(u,v,v) = p(w,w,v) = v$. Hence $u = v$, as desired.

To see (4) use (2) and (3) repeatedly: $H(a,b,c,d) \to K(a,b,c,d)$ $\to H(c,d,a,b) \to K(c,d,a,b) \to H(a,b,c,d)$.

Let $\theta = \mathrm{Cg}(a,b)$ and $\psi = \mathrm{Cg}(c,d)$ and assume that $K(a,b,c,d)$ holds. Then it follows from (4) to (8) that $K(a,b) = \{\langle x,y\rangle : K(a,b,x,y)\}$ is a congruence and $\langle c,d\rangle$ is in this congruence. Hence $\psi \subseteq K(a,b)$ and so if $\langle u,v\rangle \in \psi$ then $K(a,b,u,v)$ holds. Repeating this argument we get that $K(x,y,u,v)$ [and hence $H(x,y,u,v)$] holds whenever $\langle x,y\rangle \in \theta$ and $\langle u,v\rangle \in \psi$. We want to show that $C(a,b,c,d)$ holds, i.e., $[\theta,\psi] = 0$. We show this by showing the θ, ψ term condition holds. So let t be a term operation and $x_i\ \theta\ y_i$, $i = 0,\dots,m-1$ and $u_i\ \psi\ v_j$, $j = 0,\dots,k-1$. Then $\begin{bmatrix} t(\mathbf{x},\mathbf{u}) & t(\mathbf{x},\mathbf{v}) \\ t(\mathbf{y},\mathbf{u}) & t(\mathbf{y},\mathbf{v}) \end{bmatrix} \in \mathrm{M}(\theta,\psi)$. Suppose $t(\mathbf{x},\mathbf{u}) = t(\mathbf{x},\mathbf{v})$. We want $t(\mathbf{y},\mathbf{u}) = t(\mathbf{y},\mathbf{v})$. First observe that we may assume that $m = 1$, i.e., $\mathbf{x} = (x)$ and $\mathbf{y} = (y)$, since the general case of the term condition can be derived from this. Let $w = t(x,\mathbf{u}) = t(x,\mathbf{v})$ and $u = t(y,\mathbf{u})$ and $v = t(y,\mathbf{v})$. Just as in the argument above, it will suffice to show that $q_i(u,u,v) = q_i(u,w.v) = q_i(u,v,v)$, for $i = 0,\dots,n$, and $p(u,v,v) = p(w,w,v)$. By Theorem 6.4(2), we have

$$q_i(t(y,\mathbf{u}), t(x,\mathbf{u}), t(y,\mathbf{u})) = q_i(t(y,\mathbf{u}), t(y,\mathbf{u}), t(y,\mathbf{u}))$$

By the symmetry in (4) we have $H(u_j,v_j,x,y)$, $j = 0,\dots,k-1$. Applying this k times to (the last $\mathbf{u}$ in) the above equation we obtain:

$$q_i(t(y,\mathbf{u}), t(x,\mathbf{u}), t(y,\mathbf{v})) = q_i(t(y,\mathbf{u}), t(y,\mathbf{u}), t(y,\mathbf{v})).$$

Thus $q_i(u,w,v) = q_i(u,u,v)$. Similarly $q_i(u,w,v) = q_i(u,v,v)$ and $p(w,w,v) = p(u,v,v)$, as desired. Hence $[\theta,\psi] = 0$, i.e., $K(a,b,c,d) \to C(a,b,c,d)$. Now by (1) they are equivalent.

6.7. By Gumm's result, in every case we have that $p(x,y,y) = x$ whenever $\langle x,y\rangle \in \alpha$. Let $\mathbf{D} = \langle x,y,z\rangle : x\ \alpha\ y\ \beta\ z \subseteq \mathbf{A}^3$. First, suppose that $p : \mathbf{D} \to A$ is a homomorphism. We wish to prove that

$[\alpha, \beta] = 0$. By the result of the previous exercise, it will suffice to prove that $H(a, b, c, d)$ holds for all $\langle a, b\rangle \in \alpha$ and $\langle c, d\rangle \in \beta$. To do this, suppose that $s(x, y, z)$ is a $k + 2$-ary term, that $\mathbf{e} \in \mathbf{A}^k$, and that $s(a, c, \mathbf{e}) = s(a, d, \mathbf{e})$. We apply our assumption to the elements $\langle b, a, a\rangle$, $\langle c, c, d\rangle$, $\langle e_i, e_i, e_i\rangle$ of $\mathbf{D}$. Thus we get

$$\begin{aligned} p(s(b, c, \mathbf{e}), s(a, c, \mathbf{e}), s(a, d, \mathbf{e})) \\ &= s(p(b, a, a), p(c, c, d), \ldots, p(e_i, e_i, e_i), \ldots) \\ &= s(b, d, \mathbf{e}). \end{aligned}$$

Since $s(b, c, \mathbf{e}) = s(b, d, \mathbf{e})$, the displayed equations yield $s(b, c, \mathbf{e}) = s(b, d, \mathbf{e})$ as desired. This completes the proof that $[\alpha, \beta] = 0$ if $p : \mathbf{D} \to \mathbf{A}$ is a homomorphism.

Now suppose that $[\alpha, \beta] = 0$. Thus $C(\alpha, \beta; 0)$ (see Definition 3.2). To prove that $p|_{\mathbf{D}}$ is a homomorphism let f be a basic k-ary operation of $\mathbf{A}$ and let $\mathbf{x}\ \alpha\ \mathbf{y}\ \beta\ \mathbf{z}$ with $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z} \in \mathbf{A}^k$. It must be show that $p(f(\mathbf{x}), f(\mathbf{y}), f(\mathbf{z})) = f(p(\mathbf{x}, \mathbf{y}, \mathbf{z}))$ where $p(\mathbf{x}, \mathbf{y}, \mathbf{z})$ denotes the obvious k-tuple of elements of $\mathbf{A}$. This desired equation can be rewritten as

$$p(f(\mathbf{x}), f(\mathbf{y}), f(p(\mathbf{y}, \mathbf{y}, \mathbf{z}))) = p(f(\mathbf{y}), f(\mathbf{y}), f(p(\mathbf{x}, \mathbf{y}, \mathbf{z}))).$$

If we replace the z_i by y_i, we do obtain a true equation, with both sides equal to $f(\mathbf{x})$. The desired equation now follows from $C(\beta, \alpha; 0)$.

6.8. Let $\mathbf{C} = \mathbf{A} \times \mathbf{B}$ and η_0, η_1 be the projection congruences on $\mathbf{C}$, where each of $\mathbf{A}$ and $\mathbf{B}$ has permuting congruences. According to Exercise 4 in Chapter 5, η_i permutes with all congruences of $\mathbf{C}$. Note that whenever a congruence β permutes with each of δ_0 and δ_1 then β permutes with $\delta_0 + \delta_1$. Now suppose that β permutes with $[\alpha, \eta_0]$ and with $[\alpha, \eta_1]$. Then by Theorem 6.2,

$$\begin{aligned} \alpha \circ \beta &\subseteq [\alpha, \alpha] \circ \beta \circ \alpha \\ &\subseteq ([\alpha, \eta_0] \vee [\alpha, \eta_1]) \circ \beta \circ \alpha \\ &= \beta \circ ([\alpha, \eta_0] \vee [\alpha, \eta_1]) \circ \alpha \\ &= \beta \circ \alpha, \end{aligned}$$

so that β permutes with α. By two applications of this observation we reduce our work to showing that congruences permute if each of them lies below one of the η_i. Of course, two congruences lying above η_i (for fixed i) must permute, since the congruences of $\mathbf{C}/\eta_i$ permute. Consider first the case $\alpha \vee \beta \leq \eta_0$. The congruences $\alpha \vee \eta_1 = \alpha \circ \eta_1$

and $\beta \vee \eta_1 = \beta \circ \eta_1$ permute. Thus

$$\begin{aligned}\alpha \circ \beta &\subseteq (\beta \vee \eta_1) \circ (\alpha \vee \eta_1) \\ &= \beta \circ \eta_1 \circ \alpha \circ \eta_1 \\ &= \beta \circ \alpha \circ \eta_1.\end{aligned}$$

giving

$$\begin{aligned}\alpha \circ \beta &\subseteq \eta_0 \cap ((\beta \circ \alpha) \cap \eta_0) \circ \eta_1) \\ &= \beta \circ \alpha.\end{aligned}$$

Consider now the case $\alpha \leq \eta_0$, $\beta \leq \eta_1$. Note that $\alpha = \alpha \vee (\eta_0 \cap \beta) = \eta_0 \cap (\beta \vee \alpha)$. Note also that $\alpha \circ \beta \subseteq \eta_0 \circ \beta = \beta \circ \eta_0$. Thus we have

$$\alpha \circ \beta \subseteq \beta \circ (\eta_0 \cap (\beta \vee \alpha)) = \beta \circ \alpha.$$

this completes the proof that all congruences of $\mathbf{C}$ permute.

Chapter 7

7.1. Let $\mathbf{B} = \{0, 1, 2\}$ with addition modulo 3. Define a transfer function $T : \mathbf{B}^2 \to \mathbf{B}$ for addition by $T(1, 1) = 1$ and $T(x, y) = 0$ for all $\langle x, y\rangle \neq \langle 1, 1\rangle$. Let $\mathbf{A} = \mathbf{B} \otimes^T \mathbf{B}$. It is easy to see that $\mathbf{A}$ is a loop with identity $\langle 0, 0\rangle$. Let η be the kernel of the projection onto the second coordinate. As in the proof of Corollary 7.2, η is a congruence such that $\eta \leq \zeta_{\mathbf{A}}$ and $\mathbf{A}/\eta$ is Abelian. Since $\mathbf{B}$ is simple, either $\zeta_{\mathbf{A}} = \eta$ or $\zeta_{\mathbf{A}} = 1$. In the latter case $\mathbf{A}$ would be Abelian. To see that this cannot happen, Let $x \cdot y$ denote the operation on $\mathbf{A}$, so that $\langle x_0, x_1\rangle \cdot \langle y_0, y_1\rangle = \langle x_0 + y_0, x_1 + y_1\rangle$ unless $x_1 = y_1 = 1$ in which case it is $\langle x_0 + y_0 + 1, x_1 + y_1\rangle$. Let $p(x, y, z) = x \cdot (y \backslash z)$. Then p is a Mal'cev term for $\mathbf{A}$ and if we let $x = x' = \langle 0, 1\rangle$, $y = y' = \langle 0, 0\rangle$, and $z = z' = \langle 0, 2\rangle$ then $p(x \cdot x', y \cdot y', z \cdot z') = \langle 1, 0\rangle$ but $p(x, y, z) \cdot p(x', y', z') = \langle 0, 0\rangle$. Hence $\mathbf{A}$ is not Abelian and thus $\eta = \zeta_{\mathbf{A}}$, which implies that $\mathbf{A}/\zeta_{\mathbf{A}} \cong \mathbb{Z}/3$, as desired.

7.2. Let $\mathbf{A}$ be a nilpotent loop having four elements. If it is not Abelian then by Corollary 7.5 it must be class two and by Corollary 7.2 it must have the form $\mathbf{B} \otimes^T \mathbf{C}$ where $\mathbf{B}$ and $\mathbf{C}$ are two element loops. Up to isomorphism there is only one loop of order 2, the integers modulo 2. Thus $\mathbf{B} \cong \mathbf{C}$. Now $\mathbf{B} \otimes^T \mathbf{B}$ must have an identity element and this must be either $\langle 0, 0\rangle$ or $\langle 1, 0\rangle$. For the former to be the identity we must have $T(x, y) = 0$ if either x or y is 0. However one can easily check that if $T(1, 1) = 1$ then $\mathbf{B} \otimes^T \mathbf{B}$ is isomorphic to $\mathbb{Z}/4$ and of course if $T(1, 1) = 0$ then it is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$. A similar argument works when $\langle 1, 0\rangle$ is the identity.

Showing that an arbitrary loop of order four is Abelian involves looking at the various cases for the multiplication table but is not difficult.

7.3. Let $\theta_0 = \theta$ and $\theta_{k+1} = [1, \theta_k]$. Since $\mathbf{A}$ is nilpotent and $\theta \neq 0$, there is a positive integer r such that $\theta_r = 0$ and $\theta_{r-1} \neq 0$. Then $[1, \theta_{r-1}] = \theta_r = 0$. Hence $0 < \theta_{r-1} \leq \theta \wedge \zeta$.

7.4. We prove this by induction on $|\mathbf{A}|$. Let $\theta = \zeta \cap B^2 \in \mathbf{Con}\ \mathbf{B}$. Since $\mathbf{B}$ is nilpotent, θ is uniform by Corollary 7.5. Since $\mathbf{B}/\theta$ is a subalgebra of $\mathbf{A}/\zeta$, $|\mathbf{B}/\theta|$ divides $|\mathbf{A}/\zeta|$ by induction. Now let $b \in \mathbf{B}$. By the uniformity $|\mathbf{B}/\theta| = |\mathbf{B}|/|b/\theta|$ and $|\mathbf{A}/\zeta| = |\mathbf{A}|/|b/\zeta|$. Hence $\frac{|b/\zeta|}{|b/\theta|}|\mathbf{B}|$ divides $|\mathbf{A}|$. But b/ζ is a ternary group and b/θ is a ternary subgroup. Thus $|b/\theta|$ divides $|b/\zeta|$. Hence $|\mathbf{B}|$ divides $|\mathbf{A}|$.

7.5. Let $\mathbf{Z} = 1/\zeta$ and choose $b \in A - Z$. Let $\mathbf{B}$ be the subalgebra generated by b. Then $|\mathbf{B}|$ is either 1 or p or p^2. The first case is out because 1 is the only idempotent element of a loop. Suppose that $|\mathbf{B}| = p$. Since $\mathbf{B}$ is a subalgebra of $\mathbf{A}$, $\mathbf{B}$ is nilpotent. Since $|\mathbf{B}| = p$, $\mathbf{B}$ is an Abelian loop. By Exercise 7 of Chapter 5, $\mathbf{B}$ is a cyclic group of order p. Since $B \cap Z = 1$ and every element of $\mathbf{Z}$ commutes and associates with all elements of $\mathbf{A}$, it is not hard to see that every element of $\mathbf{A}$ has the form $b^i c$ for some i, $0 \leq i < p$, and $c \in Z$. Using this it follows that every element of $\mathbf{A}$ commutes and associates with all elements of $\mathbf{A}$. This implies $\mathbf{A}$ is Abelian, contradicting $|\mathbf{A}/\zeta| = p$. Thus we must have $|\mathbf{B}| = p^2$, i.e., $\mathbf{A} = \mathbf{B}$ and so $\mathbf{A}$ is generated by b.

7.6. Using the first relation of Lemma 7.3 we have

$$q(a, b, b) = f_n(a, b, b) = f_n(p(a, b, b), b, b) = a$$

and

$$q(b, b, a) = f_n(b, a, b) = f_n(p(a, a, b), a, b) = a.$$

7.7. Clearly p is a Mal'cev term for $\mathbf{A}$. Let θ be the equivalence relation on $\mathbf{A}$ with two blocks, G and H. It is easy to verify that θ is a congruence relation on $\mathbf{A}$ and that $\mathbf{A}/\theta$ is isomorphic to the two-element ternary group. Thus $[1, 1] \leq \theta$. By Proposition 5.7 to show that $[\theta, \theta] = 0$ we need to show that p commutes with itself on the block of θ. Since $p(x, y, z) = x - y + z$ on these blocks, this is clear. Hence A is solvable.

Now it is easy to use this algebra to construct a solvable algebra which fails to satisfy the conclusions of Lemma 7.3-Corollary 7.7. For Lemma 7.6, if a, $b \in G$ and $c \in H$ with $a \neq b$ then $\mathrm{Cg}(a, b) \neq 0$ but $\mathrm{Cg}(p(a, b, c), c) = \mathrm{Cg}(c, c) = 0$. For Corollary 7.7, let $\beta \in \mathbf{Con}\ \mathbf{A}$ be

defined by $\langle x, y\rangle \in \beta$ if $x, y \in G$ or $x = y$. Then β and θ have a block in common but are not equal. So $\mathbf{A}$ does not have regular congruences.

7.8. Assume that the relation holds for n and let $x' = f_n(p(x, b, c), b, c)$ so that $x'\ (1]_n\ x$ by assumption. Then

$$f_{n+1}(p(x, b, c), b, c) = p(b, p(b, p(x, b, c), p(x', b, c)), x').$$

Now the following matrix is in $\mathrm{M}((1]_n, 1)$

$$\begin{bmatrix} p(b, p(b, p(x, b, c), p(x', b, c)), x') & p(b, p(b, p(x, x, b), p(x', b, b)), x') \\ p(b, p(b, p(x, b, c), p(x, b, c), x) & p(b, p(b, p(x, x, b), p(x, b, b)), x) \end{bmatrix}$$

$$= \begin{bmatrix} p(b, p(b, p(x, b, c), p(x', b, c)), x') & b \\ b & b \end{bmatrix}$$

Thus by Definition 3.2(2), $f_{n+1}(p(x, b, c), b, c)\ (1]_{n+1}\ x$, as desired.

7.9. If α and β are congruences on $\mathbf{A}$ which have a common block then $\alpha \vee \beta$ and β have the same common block. So if $\mathbf{A}$ is not regular then it has congruences $\alpha > \beta$ which share a block. In $\mathbf{A}/\beta$ the congruence α/β is nontrivial but has a block with one element. This contradicts the hypothesis that all the homomorphic images of $\mathbf{A}$ have uniform congruences.

Chapter 8

8.1. Let $[\alpha, \beta] = \alpha \wedge \beta$ for all congruence α and β of $\mathbf{A}$. Then for congruences χ, ϕ, ψ we have $\chi \wedge (\phi \vee \psi) = [\chi, \phi \vee \psi] = [\chi, \phi] \vee [\chi, \psi] = (\chi \wedge \phi) \vee (\chi \wedge \psi)$ showing that $\mathbf{Con}\ \mathbf{A}$ is a distributive lattice.

8.2. It suffices to prove the result for subdirect product of two factors. So suppose that $\mathbf{A}$ and $\mathbf{B}$ are neutral and that $\mathbf{C} \subseteq A \times B$ with $p_0(C) = A$ and $p_1(C) = B$. Let η_i $(i = 0, 1)$ be the kernels of p_i. Let ν, μ be any two congruences of $\mathbf{C}$. Using the assumption about $\mathbf{A}$ and $\mathbf{B}$ and Remark 4.6, we find that $[\nu, \mu] \vee \eta_i = (\nu \vee \eta_i) \wedge (\mu \vee \eta_i)$, implying that $\nu \wedge \mu \leq [\nu, \mu] \vee \eta_i$ and so

$$\nu \wedge \mu = [\nu, \mu] \vee (\nu \wedge \mu \wedge \eta_i).$$

This is true also when we replace ν by $\nu \wedge \eta_i$ and mu by $\mu \wedge \eta_i$. Thus we obtain

$$\begin{aligned} \nu \wedge \mu \wedge \eta_i &= [\nu \wedge \eta_i, \mu \wedge \eta_i] \vee (\nu \wedge \eta_i \wedge \mu \wedge \eta_i \wedge \eta_{1-i}) \\ &= [\nu \wedge \eta_i, \mu \wedge \eta_i]. \end{aligned}$$

Putting the two displayed equations together gives $\nu \wedge \mu = [\nu, \mu]$, as desired.

If $\mathcal{V} = \mathcal{V}_0 \vee \mathcal{V}_1$, where $\mathcal{V}$ is modular and $\mathcal{V}_0$ and $\mathcal{V}_1$ are distributive, then $\mathbf{F}_{\mathcal{V}}(3)$ is a subdirect product of $\mathbf{F}_{\mathcal{V}_0}(3)$ and $\mathbf{F}_{\mathcal{V}_1}(3)$. Hence $\mathbf{F}_{\mathcal{V}}(3)$

is neutral and so by the previous exercise, **Con** $\mathbf{F}_{\mathcal{V}}(3)$ is distributive. Now by Jónsson's Theorem 2.1, $\mathcal{V}$ is distributive.

8.3. The exercise is to prove that a variety $\mathcal{V}$ is distributive if and only if it satisfies (C3) if and only if its finite subdirect products possess no skew congruences. According to the result of Exercise 1, $\mathcal{V} \models$ (C3) implies $\mathcal{V}$ is distributive. If $\mathcal{V}$ is distributive and $\mathbf{C}$ is a subdirect product of $\mathbf{A}$ and $\mathbf{B}$ in $\mathcal{V}$ with projection congruences η_i, and if ψ is any congruence of $\mathbf{C}$, then $\psi = \psi \vee (\eta_0 \wedge \eta_1) = (\psi \vee \eta_0) \wedge (\psi \vee \eta_1)$; hence ψ is not skew. Finally, suppose that $\mathcal{V}$ has no skew congruence on finite subdirect products. We shall show that this implies $\mathcal{V} \models$ (C3). If (C3) fails, then there is $\mathbf{A}$ in $\mathcal{V}$ with a nonzero Abelian congruence β. The algebra $\mathbf{A}(\beta)$ (see Definition 4.7 and the proof of Theorem 4.10) has congruences $\Delta_{\beta,\beta}$, η_0, η_1 forming an $\mathbf{M}_3$. Thus $\mathbf{A}(\beta)$ is the subdirect product of $\mathbf{A}(\beta)/\eta_0$ and $\mathbf{A}(\beta)/\eta_1$, and it is clear that $\Delta_{\beta,\beta}$ is skew.

8.4. Suppose that a is an element in a modular lattice $\mathbf{L}$ satisfying $a \wedge (x \vee y) = (a \wedge x) \vee (a \wedge y)$ for all elements x and y. By joining x to both sides of the equation we obtain $(a \vee x) \wedge (x \vee y) = x \vee (a \wedge y)$. Then meet with y we obtain $(a \vee x) \wedge y = (x \wedge y) \vee (a \wedge y)$. Finally, joining with a we obtain $(a \vee x) \wedge (a \vee y) = a \vee (x \wedge y)$. The proof of the equivalence of the conditions $a \wedge (x \vee y) = (a \wedge x) \vee (a \wedge y)$ (for all x, y) and $(a \vee x) \wedge (a \vee y) = a \vee (x \wedge y)$ (for all x, y) is now concluded by dualizing the above argument. Now if a satisfies these equations then it is clear that $x \mapsto \langle a \vee x, a \wedge x \rangle$ is a homomorphism of $\mathbf{L}$ onto a subdirect product of the interval lattice $1/a$ and $a/0$. To see that the function is injective, suppose that $a \vee x = a \vee y$ and $a \wedge x = a \wedge y$. Then $x = x \wedge (a \vee x) \wedge (a \vee y) = x \wedge (a \vee (x \wedge y)) = (x \wedge a) \vee (x \wedge y) = (y \wedge a) \vee (x \wedge y) \leq y$, and the same argument shows that $y \leq x$, so $x = y$. Now suppose that **Con** $\mathbf{A} \models$ (C1). According to the discussion preceding Theorem 8.1, the element $a = [1_{\mathbf{A}}, 1_{\mathbf{A}}]$ of **Con** $\mathbf{A}$ satisfies the above conditions, i.e. is neutral. Thus **Con** $\mathbf{A}$ is embeddable subdirectly into the product of the interval lattices $1/a$ and $a/0$.

8.5. Let **Con** $\mathbf{A} \models$ (C1). Suppose that α and β are Abelian congruences of $\mathbf{A}$. Observe that $[\alpha, \beta] \leq [\alpha \vee \beta, \alpha \vee \beta]$, so that by (C1) $[\alpha, \beta] = [[\alpha, \beta], \alpha \vee \beta] = [[\alpha, \beta], \alpha] \vee [[\alpha, \beta], \beta] \leq [\alpha, \alpha] \vee [\beta, \beta] = 0_{\mathbf{A}}$. Thus α, β Abelian implies $[\alpha, \alpha] = [\alpha, \beta] = [\beta, \beta] = 0_A$. Now let $\alpha = \bigvee\{\alpha_i : i \in I\}$ where $\{\alpha_i : i \in I\}$ is the set of all the Abelian congruences of $\mathbf{A}$. Since the commutator is completely additive and, as we just showed, $[\alpha_i, \alpha_j] = 0_{\mathbf{A}}$ for all i and j then it follows readily that α is Abelian. Clearly α is the largest Abelian congruence of $\mathbf{A}$.

8.6. We prove the harder of the two statements of the exercise. Let ε be a congruence equation such that $\mathcal{V} \models$ (Ci) implies $\mathcal{V} \models \varepsilon$ $(i = 3, 4)$

for all modular varieties $\mathcal{V}$. We are to show that this implication is valid also for $i = 2$. So let $\mathcal{V}$ be a modular variety that satisfies (C2). Let $\mathcal{A}$ be the variety of Abelian algebras in $\mathcal{V}$. Choose any algebra $\mathbf{A}$ in $\mathcal{V}$, and set $\mathbf{L} = \mathbf{Con}\ \mathbf{A}$. Let $u = [1_{\mathbf{A}}, 1_{\mathbf{A}}]$. Now we also have that $\mathcal{V} \models$ (C1) (in fact, (C2) implies (C1)). So by the result of Exercise 4, $\mathbf{L}$ is a subdirect of the intervals $1/u$ and $u/0$. It is easy to see that this subdirect representation preserves commutators. Hence the commutation lattice $\langle L, x \wedge y, x \vee y, [x, y], 0, 1\rangle$ is a subdirect product of commutation lattices $\mathbf{L}_0$ and $\mathbf{L}_1$ whose universes are the intervals $1/u$ and $u/0$, respectively. To see that $\mathbf{L} \models \varepsilon$, which is the point of the exercise, one is thus reduced to a consideration of the commutation lattices $\mathbf{L}_i$. Now $\mathbf{L}_0$ is naturally isomorphic to the commutation lattice of the algebra $\mathbf{A}/u$, which belongs to $\mathcal{A}$. Since $\mathcal{A} \models$ (C4), it follows that $\mathbf{L}_0 \models \varepsilon$. On the other hand, $\mathbf{L}_1 = \langle u/0, x \wedge y, x \vee y, x \wedge y\rangle$, a distributive lattice with trivial commutator (equal to the meet). The proof can be concluded by showing that $\mathbf{L}_1$ can be embedded into the commutation lattice of an algebra in a distributive variety (in fact we can choose the variety of lattices), for this will imply that $\mathbf{L}_1 \models \varepsilon$. This is very easy to do. We can ignore the commutator since it is trivial, and regard $\mathbf{L}_1$ simply as a distributive lattice with 0 and 1. $\mathbf{L}_1$ is a sublattice of some Boolean lattice, which in turn is isomorphic to a sublattice of its own congruence lattice.

8.7. Let $\mathbf{R}$ be a ring with unit. For any ideal $\mathbf{J}$ of $\mathbf{R}$, $\mathbf{J} \cdot \mathbf{R} = \mathbf{R} \cdot \mathbf{J} = \mathbf{J}$, due to the presence of a unit element. Equivalently, for any congruence θ of $\mathbf{R}$, $[\theta, 1_{\mathbf{R}}] = \theta$.

8.8. Suppose that $\mathbf{L} = \mathbf{Con}\ \mathbf{A}$ satisfies (C8) and $\alpha, \beta \in L$ satisfy $\alpha \vee \beta = 1$, $\alpha \wedge \beta = 0$, $\alpha \circ \beta = \beta \circ \alpha$. Then the natural homomorphism $\mathbf{A}$ to $\mathbf{A}/\alpha \times \mathbf{A}/\beta$ is an isomorphism. Thus we can assume that α and β are the projection congruences on a product algebra $\mathbf{A} = \mathbf{C} \times \mathbf{D}$. Now by the proof in Theorem 8.5 that (1) $\Rightarrow$ (5), it follows that α and β are neutral in $\mathbf{L}$ and that $\pi(\lambda) = \langle \alpha \vee \lambda, \beta \vee \lambda\rangle$ defines an isomorphism between $\mathbf{L}$ and $(1/\alpha) \times (1/\beta)$, where the interval lattices $1/\alpha$ and $1/\beta$ are complete and isomorphic to $\mathbf{Con}\ \mathbf{C}$ and $\mathbf{Con}\ \mathbf{D}$, respectively. From this it follows that $f(\bigwedge\{\lambda_t : t \in T\}) = \bigwedge\{f(\lambda_t) : t \in T\}$ for every family $\{\lambda_t : t \in T\} \subseteq L$, and this implies that f is a complete endomorphism of $\mathbf{L}$, as asserted. (Note that f trivially preserves infinite joins.)

8.9. The algebra $\mathbf{A}$ is actually simple and non-Abelian, from which its neutrality follows trivially. To see this, let θ be any nonzero congruence of $\mathbf{A}$. We can choose $a_0 \neq 0$ with $\langle 0, a_0\rangle \in \theta$, then choose $k-1$ more elements forming a vector space basis $a_0, a_1, \ldots, a_{k-1}$ of $\mathbf{V}$. Now

for all x, $y \in A$.

$$\begin{aligned} x \cdot y &= f(a_0, \ldots, a_{k-1}, x, y) \\ &\equiv f(0, a_1, \ldots, a_{k-1}, x, y) \pmod{\theta} \\ &= 0 \\ &= g(0, a_1, \ldots, a_{k-1}, x, y) \\ &\equiv g(a_0, a_1, \ldots, a_{k-1}, x, y) \pmod{\theta} \\ &= x \oplus y. \end{aligned}$$

The calculation shows that $x \cdot y \equiv x \oplus y \pmod{\theta}$, implying that $\langle x, y \rangle \in \theta$. Thus θ is $1_{\mathbf{A}}$. The calculation also displays the fact that the lattice operations $x \cdot y$ and $x \oplus y$ are polynomial operations of $\mathbf{A}$, and this implies $\mathbf{A}$ is non-Abelian. Now to show that every algebra in $\boldsymbol{V}(\mathbf{A})$ generated by $k-1$ or fewer elements is Abelian, it suffices to prove this for the subalgebras of $\mathbf{A}$ that are generated by $k-1$ or fewer elements, because the free algebra $\mathbf{F} = \mathbf{F}_{\boldsymbol{V}(\mathbf{A})}(k-1)$ is a subdirect product of these algebras. So let $\mathbf{B}$ be the subalgebra of $\mathbf{A}$ generated by elements $b_0, \ldots, b_{k-2}$. Let $\mathbf{W}$ be the vector subspace of $\mathbf{V}$ subspace by $b_0, \ldots, b_{k-2}$. On $\mathbf{W}$ the operations f and g are constant, giving only the value 0. (This follows from the definition of f and g.) Thus, clearly, W is a subuniverse of $\mathbf{A}$, and we must have $W = B$. Then $\langle B, +, -, f, g \rangle = \langle B, +, -, 0, 0 \rangle$ and so $\mathbf{B}$ is Abelian.

8.10. Every subgroup of an Abelian group is a normal subgroup. That Abelian groups have the congruence extension property follows easily from this. Now suppose that $\mathcal{V}$ is a variety of groups in which congruences can always be extended. Thus, by Theorem 8.4, whenever $\mathbf{A}$ is a group in $\mathcal{V}$ and $\mathbf{B}$, $\mathbf{H}$, $\mathbf{K}$ are subgroups of $\mathbf{A}$ with $\mathbf{H}$ and $\mathbf{K}$ normal in $\mathbf{A}$, then $[\mathbf{H} \cap \mathbf{B}, \mathbf{K} \cap \mathbf{B}] = [\mathbf{H}, \mathbf{K}] \cap \mathbf{B}$. Suppose that $\mathbf{A}$ is non-Abelian. Then there exists a nontrivial cyclic subgroup $\mathbf{B} \subseteq [\mathbf{A}, \mathbf{A}]$. Taking $\mathbf{H} = \mathbf{K} = \mathbf{A}$ in the above formula leads to an immediate contradiction.

Chapter 9

9.1.. Suppose $\mathbf{A}$ is Abelian and $\mathbf{R} = \mathbf{R}(\boldsymbol{V}(\mathbf{A}))$ is commutative. Using equation (10) we see that $x \cdot y = rx + sy + c$ for some r, $s \in R$ and $c \in A$. Then $(x \cdot y) \cdot (u \cdot v) = (rx + sy + c) \cdot (ru + sv + c) = r^2x + rsy + rc + sry + s^2v + sc + c$. Also $(x \cdot y) \cdot * y \cdot v) = r^2x + rsy + rc + sry + s^2v + sc + c$, and so $(x \cdot y) \cdot (u \cdot v) = (x \cdot u) \cdot y \cdot v)$ follows from the commutativity of $\mathbf{R}$.

Now suppose that the identity holds. It says that $\cdot$ commutes with itself. From this we can show that each of $\cdot$, $/$, and $\backslash$ commute with

each other and with themselves. For example, to see that / commutes with itself we calculate

$$\begin{aligned} x &= [((x/y)/(u/v)) \cdot (u/v)] \cdot [(y/v) \cdot v] \\ &= [((x/y)/(u/v)) \cdot (y/v)] \cdot [(u/v) \cdot v] \\ &= [((x/y)/(u/v)) \cdot (y/v)] \cdot u. \end{aligned}$$

Hence $((x/y)/(u/v)) \cdot (y/v) = x/u$. But $[(x/u)/(y/v)] \cdot (y/v) = x/u$ also. Thus $(x/y)/(u/v) = (x/u)/(y/v)$, as desired. To see that $\cdot$ and / commute, calculate

$$[(x/y) \cdot (u/v)] \cdot (y \cdot v) = [(x/y) \cdot y] \cdot [(u/v) \cdot v] = x \cdot u$$

Since $[(x \cdot u)]/(y \cdot v)] \cdot (y \cdot v) = x \cdot u$ also, we have $(x \backslash y) \cdot (u \backslash) = (x \cdot u)/(y \cdot v)$. Which shows $\cdot$ and $\backslash$ commute.

Thus the basic operations and hence all term operations commute with each other. By Proposition 5.7, $\mathbf{A}$ is Abelian. If $r, s \in R$ then $rs = r(s(u,v),v) = r(s(u,v),s(v,v)) = s(r(u,v),r(v,v)) = s(r(u,v),v) = sr$.

To see the second statement first suppose that $\boldsymbol{V}(\mathbf{A})$ is permutable and every basic operation of $\mathbf{A}$ commutes with every idempotent term operation of $\mathbf{A}$. Then every idempotent term operation commutes with every other idempotent term operation. By Proposition 5.7, $\mathbf{A}$ is Abelian and since the elements of $\mathbf{R}(\boldsymbol{V}(\mathbf{A}))$ are idempotent terms, it is commutative as above.

Now suppose that $\mathbf{A}$ is Abelian and $\mathbf{R} = \mathbf{R}(\boldsymbol{V}(\mathbf{A}))$ is commutative. Choose an arbitrary element 0 in A and let $\mathbf{R}$ act on $\mathbf{A}$ by $r \cdot a = r(a, 0)$, as usual. If f is an n-ary term operation on $\mathbf{A}$ then since $\mathbf{A}$ is Abelian there are elements $r_{f1}, \ldots, r_{fn} \in R$ and $c_f \in A$

$$(*) \qquad f(x_1, \ldots, x_n) = r_{f1} \cdot x_1 + \cdots + r_{fn} \cdot x_n + c_f.$$

If g is an m-ary term operation then it has a similar representation

$$g(x_1, \ldots, x_m) = r_{g1} \cdot x_1 + \cdots + r_{gm} \cdot x_m + c_g.$$

If one writes out both $f(g(x_{11}, \ldots, x_{1m}), \ldots, g(x_{n1}, \ldots, x_{nm}))$ and also $g(f(x_{11}, \ldots, x_{n1}), \ldots, f(x_{1m}, \ldots, x_{nm}))$ in terms of the above representations and uses the fact that $\mathbf{R}$ is commutative, one sees that f and g commute if and only if

$$(**) \qquad (r_{f1} + \cdots + r_{fn} - 1) \cdot c_g = (r_{g1} + \cdots + r_{gm} - 1) \cdot c_f$$

holds in $\mathbf{A}$. Now suppose that f is idempotent. Then it follows from the representation $(*)$ with $x_1 = \cdots = x_n = 0$, that $c_f = 0$. If we let $x_1 = \cdots = x_n = x$ in $(*)$ we see that $(r_{f1} + \cdots + r_{fn}) \cdot x = x$ for all

$x \in A$. Now by $(**)$ it is clear that f then commutes with every term operation.

9.2. Let $\mathbf{G}$ be the group on $\{0,1,2,3\}$ isomorphic to the direct of two copies of the group with two elements. Thus, in $\mathbf{G}$, $x + x = 0$ and $x + y = z$ if $\{x, y, z\} = \{1, 2, 3\}$. Let $\sigma = (12)$ and $\tau = (23)$ be permutations of $\{0, 1, 2, 3\}$. Then σ, $\tau \in \mathbf{Aut}(\mathbf{G})$. Let $\mathbf{A}$ be the quasigroup on $\{0, 1, 2, 3\}$ defined by $x \cdot y = \sigma(x) + \tau(y)$. Then $\mathbf{A}$ is an Abelian quasigroup (by Corollary 5.9). Let p be a Mal'cev term for quasigroups. (Two such are given in Exercise 2 of Chapter 2.) Clearly, $r(u, v) = p(u \cdot v, v \cdot v, v)$ and $s(u, v) = p(v \cdot u, v \cdot v, v)$ are both in $\mathbf{R}(\boldsymbol{V}(\mathbf{A}))$; see (9) of Chapter 9. If we take $0 \in A$ as our zero element, then $r \cdot a = \sigma(a)$ and $s \cdot a = \tau(a)$ for $a \in A$. Since σ and τ do not commute, r and s do not commute, and so $\mathbf{R}(\boldsymbol{V}(\mathbf{A}))$ is not commutative. Hence, by Proposition 9.6, the ring $\mathbf{R}(\mathcal{V})$ is not commutative for the variety $\mathcal{V}$ of quasigroups.

9.3. $\mathbf{D}$ is a division ring by Schur's lemma. Namely if $\delta \in D$ then both the range of δ and the kernel $(= \{\mathbf{a} \in \mathbf{M}(\beta) : \delta(\mathbf{a}) = 0\})$ are submodules of $\mathbf{M}(\beta)$ as an $\mathbf{R}$-module. Since $\mathbf{M}(\beta)$ is simple, it has no nontrivial submodules. Thus either $\delta = 0$ or the kernel of δ is 0 and the range is $\mathbf{M}(\beta)$, i.e., δ is an automorphism and so invertible. Hence $\mathbf{D}$ is a division ring.

Recall that $\mathbf{a} \in \iota_i\mathbf{M}(\beta, z_i)$, means that $a_j = z_j$ for all $j \neq i$. Let $\mathbf{m} \in R$ have all entries 0 except $m_{ii} = 1$ (that is, $m_{ii} = u$). Then $\mathbf{a} \in \iota_i\mathbf{M}(\beta, z_i)$ if and only if $\mathbf{m} \cdot \mathbf{a} = \mathbf{a}$. If δ is an endomorphism and $\mathbf{m} \cdot \mathbf{a} = \mathbf{a}$ then $\delta(\mathbf{a}) = \delta(\mathbf{m} \cdot \mathbf{a}) = \mathbf{m} \cdot \delta(\mathbf{a})$, showing $\iota_i\mathbf{M}(\beta, z_i)$ is a $\mathbf{D}$-subspace.

Suppose that $a_1, \ldots, a_n \in \mathbf{M}(\beta, z_i)$ are such that $\iota_i a_1, \ldots, \iota_i a_n$ are $\mathbf{D}$-linearly independent and that $b_1, \ldots, b_n \in \mathbf{M}(\beta, z_j)$. By the Jacobson Density Theorem (Theorem 1.12 of Chapter 9 of Hungerford [**49**]) there is an $\mathbf{m} \in R$ such that $\mathbf{m} \cdot (\iota_i a_k) = \iota_i b_k$. Let $m_{ji} = \phi_j(r(u, v))$ with $r(u, v) \in H_{ij}$ and let $g(x) = r(x, z)$. Then $g(a_k) = b_k$, of course.

If $\mathbf{A}$ is finite then $\mathbf{D}$ is finite and hence its prime subfield has characteristic p for some prime p. Each block is a finite vector space over the prime subfield and thus has order p^i for some i.

9.4. To prove the first it clearly suffice to prove it in the case that $\alpha/\beta \nearrow \gamma/\delta$, i.e., $\gamma = \alpha \vee \delta$ and $\beta = \alpha \wedge \delta$. Suppose that $[\varphi, \alpha] \leq \beta$. Then $[\varphi, \gamma] = [\varphi, \alpha \vee \delta] = [\varphi, \alpha] \vee [\varphi, \delta] \leq \beta \vee \delta = \delta$. If $[\theta, \gamma] \leq \delta$, then $[\theta, \alpha] \leq [\theta, \gamma] \wedge \alpha \leq \delta \wedge \alpha = \beta$. Hence $(\beta : \alpha) = (\delta : \gamma)$.

For the second part we may again assume that $\alpha/\beta \nearrow \gamma/\delta$. Moreover we may assume that $\beta = 0$. Since $[\alpha, \alpha] \leq \beta \leq \delta$, α and δ permute by Theorem 6.2. Define a map $\tau_i : \mathbf{M}(\gamma/\delta, z_i) \to \mathbf{M}(\alpha, z_i)$ as follows.

If $x\ \gamma\ z_i$ then, since $\gamma = \delta \circ \alpha$, there is a y such that $x\ \delta\ y\ \alpha\ z_i$. Moreover, since $\alpha \wedge \delta = \beta = 0$, y is unique. Let $\tau_i(x/\delta) = y$. To see that this is well defined suppose $x\ \delta\ x'$ and that $x\ \delta\ y\ \alpha\ z_i$ and $x'\ \delta\ y'\ \alpha\ z_i$. Then $y\ \delta \wedge \alpha\ y'$, i.e., $y = y'$ and so τ_i is well defined. Now let $\tau : \mathbf{M}(\gamma/\delta) \to \mathbf{M}(\alpha)$ be defined by $\tau(a)_i = \tau_i(a_i)$.

To see that each τ_i, and hence τ, is one-to-one suppose that x, $x'\ \gamma\ z_i$ and $\tau_i(x/\delta) = \tau_i(x'/\delta) = y$. Then $x\ \delta\ y\ \alpha\ z_i$ and $x'\ \delta\ y\ \alpha\ z_i$. This implies that $x\ \delta\ x'$ so $x/\delta = x'/\delta$. Now if $y\ \alpha\ z_i$ then certainly $y\ \delta\ y\ \alpha\ z_i$ and $y\ \gamma\ z_i$. Hence $\tau_i(y/\delta) = y$, and thus τ_i is onto.

To see that τ_i, and hence τ, preserves addition let x, $x' \in z_i/\gamma$ and let $y = \tau_i(x/\delta)$ and $y' = \tau_i(x'/\delta)$. Then $x\ \delta\ y\ \alpha\ z_i$ and $x'\ \delta\ y'\ \alpha\ z_i$. It follows that $d(x, z_i, x')\ \delta\ d(y, z_i, y')\ \alpha\ d(z_i, z_i, z_i) = z_i$. So $\tau_i(d(x, z_i, x')) = d(y, z_i, y')$ which shows that τ_i preserves addition.

To see that τ respect multiplication by elements of $\mathbf{R}$ we need to show that if $r(u, v) \in \mathrm{H}_{ij}$ and $x \in z_i/\gamma$ then $r_j(r(x, z)) = r(\tau_i(x), z)$. Let $y = \tau_i(x)$ so that $x\delta y\alpha z_i$. Then $r(x, z)\ \delta\ r(y, z)\ \alpha\ r(z_i, z) = z_i$, which implies that $\tau_j(r(x, z)) = r(y, z) = r(\tau_i(x), z)$, completing the proof.

9.5. Let $\theta = \mathrm{Cg}(a, b) \leq \beta$ so that $a\ \beta\ b$. Let $c = d(a, b, z_i)$ where a, $b \in z_i/\gamma$. Then $c = d(a, b, z_i)\ \theta\ d(a, a, z_i) = z_i$. Let $g(x) = d(x, z_i, b)$. Then $g(z_i) = b$ and

$$\begin{aligned} g(c) &= d(d(a, b, z_i), z_i, b) \\ &= d(d(a, b, z_i), d(b, b, z_i), d(b, b, b)) \\ &= d(d(a, b, b), d(b, b, b), d(z_i, z_i, b)) \\ &= d(a, b, b) = a \end{aligned}$$

Hence $\mathrm{Cg}(a, b) = \mathrm{Cg}(c, z_i)$ $(= \theta)$. Let $\mathbf{c} \in \mathbf{M} = \sum \mathbf{M}(\beta, z_j)$ denote the vector with all 0's except with c in the i^{th} coordinate. Let $\mathbf{N} = \mathbf{Rc}$ be the cyclic module generated by $\mathbf{c}$. Now $x\ \alpha_N\ y$ if and only if $x\ \beta\ y$ and if x, $y \in z_j/\gamma$ and we let $\mathbf{v} \in \mathbf{M}$ be the vector whose i^{th} coordinate is $d(x, y, z_j)$ and whose other coordinates are 0, then $\mathbf{v} \in \mathbf{N}$. But then $\mathbf{v} = \mathbf{m} \cdot \mathbf{c}$ for some $\mathbf{m} \in \mathbf{R}$. This implies that there is an $r \in \mathrm{H}_{ij}$ such that $r(c, \mathbf{z}) = d(x, y, z_j)$. Since $r(z_i, \mathbf{z}) = z_j$, we have that $\langle d(x, y, z_j), z_j \rangle \in \mathrm{Cg}(c, z_i) = \mathrm{Cg}(a, b)$, i.e., $\alpha_N \leq \mathrm{Cg}(a, b)$. But clearly $c\ \alpha_N\ z_i$; so that $\mathrm{Cg}(a, b) = \alpha_N$. Hence $\mathrm{Cg}(a, b)$ corresponds to a cyclic submodule. Thus we have shown that in the isomorphism of $\beta/0$ onto $\mathbf{L}(\mathbf{M})$ the image of a principal congruence is a cyclic submodule. Hence the image of an n-generated congruence is an n-generated submodule. Of course, an element is compact in $\beta/0$ if and only if it is compact in **Con A** by upper continuity, and thus the isomorphism maps the set of compact element onto the set of finitely generated submodules.

9.6. As in the proof of Proposition 9.4, if $r_{ij}(u, \mathbf{v}, \mathbf{y}) \in \mathrm{H}_{ji}$, the maps $r_{ij}(u, \mathbf{v}, \mathbf{y}) \mapsto r_{ij}(u, \mathbf{v}, \sigma(\mathbf{y}))$ can be combined into a homomorphism, which we again denote by σ, from $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$ onto $\mathbf{R}(\mathcal{V}, \lambda)$. Let $\mathbf{m} = (m_{ij})$ be in $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$ and let $\mathbf{a}$ be in $\sum \mathbf{M}(\beta, z_i)$. Then, by Theorem 9.7, $\mathbf{m} \cdot \mathbf{a} = (\sigma\mathbf{m}) \cdot \mathbf{a}$. Hence, if $\mathbf{m}$ is in the kernel of σ, $\mathbf{m} \cdot \mathbf{a} = (\sigma\mathbf{m}) \cdot \mathbf{a} = 0$ for all $\mathbf{a}$ in $\sum \mathbf{M}(\beta, z_i)$ and thus $\mathbf{m}$ is in the kernel of the action of $\mathbf{R}(\mathcal{V}, \lambda, \kappa)$ on $\sum \mathbf{M}(\beta, z_i)$.

9.7. The maps $\psi : \mathbf{M}(\beta, z_i) \to \mathbf{M}(\beta, z_i)$ given by $\psi(x) = d(x, z_i, z_i)$ can be combined in an obvious way to give a map $\psi : \sum \mathbf{M}(\beta, z_i) \to \sum M(\beta, z_i')$. To see that ψ_i, and hence ψ, preserves addition let x, $x' \in \mathbf{M}(\beta, z_i)$. Then

$$\begin{aligned}
\psi_i(d(x, z_i, x')) &= d(d(x, z_i, x'), z_i, z_i') \\
&= d(d(x, z_i, x'), d(z_i, z_i, z_i), d(z_i', z_i', z_i')) \\
&= d(d(x, z_i, z_i'), d(z_i, z_i, z_i'), d(x', z_i, z_i')) \\
&= d(\psi_i(x), z_i', \psi_i(x'))
\end{aligned}$$

as desired.

The proof that ψ preserves $\mathbf{R}$-multiplication and is a bijection is similar to the proof of Proposition 9.11.

Chapter 10

10.1. Let $\beta \prec \alpha$ in **Con C** and let δ be a completely meet irreducible element with $\delta \geq \beta$ and $\delta \not\geq \alpha$. Let $\gamma = \delta^* = \alpha \vee \delta$ be the unique cover of δ. By Exercise 4 of Chapter 9. $(\beta : \alpha) = (\delta : \gamma)$. Let $\eta_i' = \bigwedge_{j \neq i} \eta_j$. If $\delta \geq \eta_i'$ then we can use induction on n to show that $(\delta : \gamma) \geq \eta_j$ for some j. Thus we may assume that η_i, $\eta_i' \not\leq \delta$. Hence by the implication displayed in the proof of Theorem 10.1 we have that $\eta_i \leq (\delta : \gamma)$, as desired. The second part follows by letting $\theta = \bigwedge_{\beta \prec \alpha} (\beta : \alpha) \in$ **Con B**. As in Theorem 10.5, θ is nilpotent and by the first part $\theta = \bigwedge_{i=1}^{n} (\theta \vee \eta_i)$.

Chapter 13

13.1. First we will show that $\beta \dot{+} \gamma \subseteq \beta \oplus \gamma$. So suppose that $\langle x, y \rangle \in \beta \dot{+} \gamma$ so that there is a z and t such that $x \; \beta \; z \; \alpha_2 \; y$, $x \; \alpha_2 \; t \; \gamma \; y$ and $z \; \alpha_1 \; t$. Then $x \; \alpha_2 \; t \; \alpha_1 \; z \; \alpha_2 \; y$, so $\langle x, y \rangle \in \alpha_1 \vee \alpha_2$. Since $\alpha_1 \leq \alpha_1 \vee \alpha_3 = \gamma_{13} \vee \alpha_3$ and $z \; \alpha_1 \; t$, there is a $w \in A$ such that $z \; \gamma_{13} \; w \; \alpha_3 \; t$. Now we have that $x \; \beta \; z \; \gamma_{13} \; w$ and

$$x \; \alpha_2 \; t \; \alpha_3 \; w.$$

so that $\langle x, w\rangle \in (\beta \vee \gamma_{13}) \wedge (\alpha_2 \vee \alpha_3)$. Similarly $\langle w, y\rangle \in (\gamma \vee \alpha_3) \wedge (\alpha_2 \vee \gamma_{13})$. Hence $\langle x, y\rangle \in (\beta \vee \gamma_{13}) \wedge (\alpha_2 \vee \alpha_3) \vee (\gamma \vee \alpha_3) \wedge (\alpha_2 \vee \gamma_{13})$, proving that $\langle x, y\rangle \in \beta \oplus \gamma$.

Next we observe that $\beta \dot{+} \gamma$ is a congruence. To see symmetry suppose that $\langle x, y\rangle \in \beta \dot{+} \gamma$ and that z and t are as above. Then $\langle y, x\rangle \in \beta \dot{+} \gamma$ with $z' = d(x, z, y)$ and $t' = d(x, t, y)$. Similarly $\beta \dot{+} \gamma$ is transitive and it obviously respects the operations. Moreover $\alpha_1 \leq \alpha_2 \vee (\beta \dot{+} \gamma)$. To see this let $\langle u, v\rangle \in \alpha_1$. By hypothesis $\alpha_1 \leq \beta \vee \alpha_2$ and $\alpha_1 \leq \gamma \vee \alpha_2$. Hence there are elements r and s with $u\ \beta\ r\ \alpha_2\ v$, and $u\ \alpha_2\ s\ \gamma\ v$. By definition this implies that $\langle r, s\rangle \in \beta \dot{+} \gamma$. Now $u\ \alpha_2\ s\ \beta \dot{+} \gamma\ r\ \alpha_2\ v$, showing that $\alpha_1 \leq \alpha_2 \vee (\beta \dot{+} \gamma)$. Since $\alpha_2 \wedge (\beta \oplus \gamma) = 0$, $\alpha_2 \wedge (\beta \dot{+} \gamma) = 0$. Since in a modular lattice comparable complements are equal, $\beta \oplus \gamma = \beta \dot{+} \gamma$.

13.2. First suppose that $\mathcal{V}$ satisfies ε_3, that $\{\alpha_i, \gamma_{ij}\}$ is an n-frame, $n \geq 3$, in **Con C**, $\mathbf{C} \in \mathcal{V}$ and that $\alpha_1 \wedge \alpha_2 = 0$. Let $x\ \gamma_{12}\ z$. Since $\gamma_{12} \leq \alpha_1 \vee \alpha_2$ there is a t with $x\ \alpha_1\ t\ \alpha_2\ z$. Since $\alpha_1 \leq \alpha_2 \vee \gamma_{12}$ there is a y with $x\ \alpha_2\ y\ \gamma_{12}\ t$. We have the situation indicated in Figure 1.

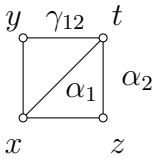


FIGURE 1.

Now we can apply Theorem 5.5(iii) with z for u' and x for both y and u. By that theorem we have the relationships indicated in Figure 2.

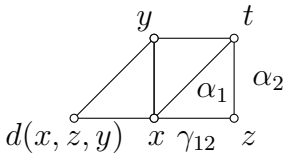


FIGURE 2.

Since $\gamma_{12} \leq \alpha_1 \vee \alpha_2$ there is an element t_2 such that $y\ \alpha_1\ t_2\ \alpha_2\ t$. Similarly there is a y_2 such that $y\ \alpha_2\ y_2\ \gamma_{12}\ t_2$. By Theorem 5.5(iii) $d(y, t, y)$ and the other elements satisfy the relations indicated in Figure 3.

Clearly $d(x, z, x)\ \alpha_2\ d(y, t, y)$. Hence we can apply Theorem 5.5(iii) again to obtain the following relationships indicated in Figure 4, where $3 \cdot x = d(x, z, d(x, z, x))$.

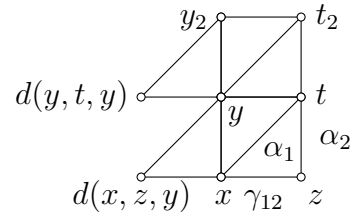


FIGURE 3.

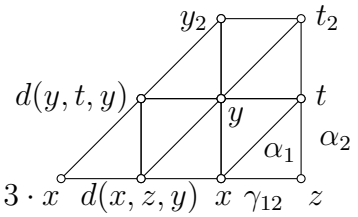


FIGURE 4.

Recall the definition of $\gamma_{12} \dot{+} \gamma_{12}$ from the previous exercise. Now $\langle y, z\rangle \in \gamma_{12} \dot{+} \gamma_{12}$ by taking x and t as the two auxiliary points required in that definition. From this it follows that $\langle z, y_2\rangle \in \gamma_{12} \dot{+} \gamma_{12} \dot{+} \gamma_{12}$ by taking y and t_2 as auxiliary points. Since we are assuming ε_3, $\gamma_{12} \dot{+} \gamma_{12} \dot{+} \gamma_{12} = \alpha_1$. Thus $y_2 \ \alpha_1 \ z$, and hence $3 \cdot x \ \alpha_1 \wedge \gamma_{12} \ z$; see Figure 4. Since $\alpha_1 \wedge \gamma_{12} = 0$, $z = 3 \cdot x$. Thus we have shown that the Abelian group $\mathbf{M}(\gamma_{12}, z)$ has exponent 3 or is trivial. Now suppose that θ is an arbitrary Abelian congruence on an algebra $\mathbf{A}$, and let $\mathbf{B} = \mathbf{A}(\theta) = \{\langle x, y\rangle \in \mathbf{A}^2 : x \ \theta \ y\}$. Then since θ is Abelian, the set $\{0, \eta_0, \eta_1, \Delta_{\theta,\theta}, \theta_0 = \theta_1\}$ is isomorphic to $\mathbf{M}_3$. Let $\mathbf{C} = \{\langle a_0, \dots, a_{n-1}\rangle \in \mathbf{A}^n : a_0 \ \theta \ a_1 \ \theta \ \cdots \ \theta \ a_{n-1}\}$. Then it is not hard to verify that $\alpha_i = \bigwedge_{j \neq i} \eta_j$, $\gamma_{ij} = \Delta_{ij} \wedge (\alpha_i \vee \alpha_j)$ is an n-frame (with 0 for its index base) in $\mathbf{Con}\ \mathbf{C}$, where $\Delta_{ij} = \{\langle\langle a_0, \dots, a_{n-1}\rangle, \langle b_0, \dots, b_{n-1}\rangle\rangle : \langle a_i, a_j\rangle \ \Delta_{\theta,\theta} \ \langle b_i, b_j\rangle\}$. Now since θ_0/η_0 and $\gamma_{12}/0$ are projective intervals, we have

$$\begin{aligned} \mathbf{M}_{\mathbf{A}}(\theta, z) &\cong \mathbf{M}_{\mathbf{C}}(\theta_0/\eta_0, \langle z, \dots, z\rangle/\eta_0) \\ &\cong \mathbf{M}_{\mathbf{C}}(\gamma_{12}, \langle z, \dots, z\rangle) \end{aligned}$$

by (the solution to) Exercise 4 of Chapter 9. Thus we have shown that $\mathbf{M}(\theta, z)$ has exponent 3 for every (nontrivial) Abelian congruence θ. Now the elements of $\mathbf{R}(\mathcal{V})$ lie in an Abelian congruence (in the notation of Chapter 9, $\theta_0/[\theta_0, \theta_0]$) and their addition is inherited from the addition on $\mathbf{M}(\theta/[\theta, \theta], v)$ (suppressing the zeros). Thus $\mathbf{R}(\mathcal{V})$ satisfies $1 + 1 + 1 = 0$, as desired.

For the converse suppose that $\mathbf{R}(\mathcal{V})$ has characteristic 3 and let $\{\alpha_i, \gamma_{ij}\}$ be an n-frame in **Con A**, where $\mathbf{A}$ is in $\mathcal{V}$. Let $\langle z, y_2\rangle \in \gamma_{12} \dot{+} \gamma_{12} \dot{+} \gamma_{12}$. Then there exist y, $t_2 \in A$ such that the relations in Figure 4 hold for the four elements, z, y, y_2, t_2. By Lemma 13.1 and Theorem 6.2, α_1, α_2, and γ_{12} pairwise permute. From this it follows that there exists elements x and t as in Figure 4. Applying Theorem 5.5(iii) three times we have the full situation indicated in Figure 4.

Of course $\gamma_{12}/[\gamma_{12}, \gamma_{12}]$ is an Abelian congruence and so has exponent 3 since $\mathbf{R}(\mathcal{V})$ has characteristic 3. Thus $3 \cdot x \; [\gamma_{12}, \gamma_{12}] \; z$, and since $[\gamma_{12}, \gamma_{12}] \leq \alpha_1$ we have that $3 \cdot z \; \alpha_1 \; z$. Now we have that $y_2 \; \alpha_1 \; z$; see Figure 4. Thus we have shown that $\gamma_{12} \dot{+} \gamma_{12} \dot{+} \gamma_{12} \leq \alpha_1$ which implies that they are equal as above. Since $\gamma_{12} \dot{+} \gamma_{12} \dot{+} \gamma_{12} = \gamma_{12} \oplus \gamma_{12} \oplus \gamma_{12}$ by the previous exercise, the characteristic of the ring of the frame is 3. Thus ε_3 holds.

Bibliography

[1] J. Baldwin and R. McKenzie, *Counting models in universal horn classes*, Algebra Universalis **15** (1982), 359–384.

[2] C. Bergman, *On the relationship of AP, RS and CEP in modular varieties*, Algebra Universalis **22** (1986), 164–171.

[3] Clifford Bergman, *Another consequence of AP in residually small, congruence modular varieties*, Houston J. Math. **14** (1988), no. 4, 451–464.

[4] G. Birkhoff, *On the structure of abstract algebras*, Proc. Cambridge Phil. Soc. **31** (1935), 433–454.

[5] G. Birkhoff, *Lattice theory*, Amer. Math. Soc., 1967, 3rd ed., Colloquium Publications.

[6] R. G. Burns and S. Oates-Williams, *Varieties of groups and normal-subgroup lattices—a survey*, Algebra Universalis **32** (1994), 145–152.

[7] S. Burris, *Boolean powers*, Algebra Universalis **5** (1976), 341–360.

[8] S. Burris and R. McKenzie, *Decidability and boolean representations*, Memoirs Amer. Math. Soc. **246** (1981).

[9] S. Burris and R. McKenzie, *Decidable varieties with modular congruence lattices*, Bull. Amer. Math. Soc. (N.S.) **4** (1981), 350–352.

[10] S. Burris and H. P. Sankappanavar, *A course in universal algebra*, Springer-Verlag, New York, 1981.

[11] C. C. Chang, B. Jónsson, and A. Tarski, *Refinement properties for relational structures*, Fund. Math. **55** (1964), 249–281.

[12] D. M. Clark and P. H. Krauss, *Para-primal algebras*, Algebra Universalis **6** (1976), 165–192.

[13] D. M. Clark and P. H. Krauss, *Varieties generated by para-primal algebras*, Algebra Universalis **7** (1977), 93–114.

[14] D. M. Clark and P. H. Krauss, *Plain para primal algebras*, Algebra Universalis **11** (1980), 365–388.

[15] P. Crawley and R. P. Dilworth, *Algebraic theory of lattices*, Prentice-Hall, Englewood Cliffs, New Jersey, 1973.

[16] B. Csákány, *Varieties of affine modules*, Acta Sci. Math. (Szeged) **37** (1975), 3–10.

[17] B. Csákány, *Varieties of modules and affine modules*, Acta Math. Acad. Sci. Hungar. **26** (1975), 263–266.

[18] B. A. Davey and L. G. Kovács, *Absolute subretracts and weak injectives in congruence-modular varieties*, Trans. Amer. Math. Soc. **297** (1986), 181–196.

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

[20] A. Day, *p–modularity implies modularity in equational classes*, Algebra Universalis **3** (1973), 398–399.

[21] A. Day, *Splitting lattices generate all lattices*, Algebra Universalis **7** (1977), 163–170.
[22] A. Day and E. Kiss, *Frames and rings in congruence modular varieties*, J. Algebra **109** (1987), 479–507.
[23] Alan Day and Ralph Freese, *A characterization of identities implying congruence modularity, I*, Canad. J. Math. **32** (1980), 1140–1167.
[24] Ralph Freese, *Minimal modular congruence varieties*, Notices Amer. Math. Soc. **23** (1976), #76T–A181.
[25] Ralph Freese, *Planar sublattices of* **FM**(4), Algebra Universalis **6** (1976), 69–72.
[26] Ralph Freese, *Subdirectly irreducible algebras in modular varieties*, Universal Algebra and Lattice Theory (R. Freese and O. Garcia, eds.), Springer-Verlag, New York, 1983, Lecture notes in Mathematics, vol. **1004**, pp. 142–152.
[27] Ralph Freese, *On jónsson's theorem*, Algebra Universalis **18** (1984), 70–76.
[28] Ralph Freese, William Lampe, and Walter Taylor, *Congruence lattices of algebras of fixed similarity type, i*, Pacific J. Math. **82** (1979), 59–68.
[29] Ralph Freese and Ralph McKenzie, *Residually small varieties with modular congruence lattices*, Trans. Amer. Math. Soc. **264** (1981), 419–430.
[30] E. Gedeonová, *Jordan-hölder theorem for lines*, Mat. Časopis Sloven. Akad. Vied. **22** (1972), 177–198.
[31] Steven Givant, *Universal Horn classes categorical or free in power*, Ann. Math. Logic **15** (1978), no. 1, 1–53.
[32] Steven Givant, *A representation theorem for universal Horn classes categorical in power*, Ann. Math. Logic **17** (1979), no. 1-2, 91–116.
[33] G. Grätzer, *General lattice theory*, Academic Press, New York, 1978.
[34] G. Grätzer, *Universal algebra*, second ed., Springer-Verlag, New York, 1979.
[35] G. Grätzer, H. Lakser, and J. Płonka, *Joins and direct products of equational classes*, Canad. Math. Bull. **12** (1969), 741–744.
[36] H. P. Gumm, *über die lösungsmengen von gleichungsystemen über allgemeinen algebren*, Math. Z. **162** (1978), 51–62.
[37] H. P. Gumm, *Algebras in congruence permutable varieties: Geometrical properties of affine algebras*, Algebra Universalis **9** (1979), 8–34.
[38] H. P. Gumm, *An easy way to the commutator in modular varieties*, Arch. Math. **34** (1980), 220–228.
[39] H. P. Gumm, *The little desarquesian theorem for algebras in modular varieties*, Proc. Amer. Math. Soc. **80** (1980), 393–397.
[40] H. P. Gumm, *Congruence modularity is permutability composed with distributiveity*, Arhc. Math. (Basel) **36** (1981), 569–576.
[41] H. P. Gumm, *Geometrical methods in congruence modular algebras*, 1983, Memoirs Amer. Math. Soc.
[42] H. P. Gumm and Ch. Herrmann, *Algebras in modular varieties: Baer refinements, cancellation and isotopy*, Houston J. Math. **5** (1979), 503–523.
[43] H. P. Gumm and A. Ursini, *Ideals in universal algebras*, Algebra Universalis **19** (1984), 45–54.
[44] 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.

[45] C. Herrmann, *Affine algebras in congruence modular varieties*, Acta Sci. Math. (Szeged) **41** (1979), 119–125.
[46] C. Herrmann, *On varieties of algebras having complemented modular lattices of congruences*, Algebra Universalis **16** (1983), 129–130.
[47] D. Hobby and R. McKenzie, *The structure of finite algebras (tame congruence theory)*, Contemporary Mathematics, American Mathematical Society, Providence, RI, 1988.
[48] A. P. Huhn, *Schwach distributive verbände, I*, Acta Sci. Math. (Szeged) **33** (1972), 297–305.
[49] T. W. Hungerford, *Algebra*, Holt, Reinhart and Winston, Inc., New York, 1974.
[50] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967.
[51] G. Hutchinson and G. Czédli, *A test for identities satisfied in lattices of submodules*, Algebra Universalis **8** (1978), 269–309.
[52] Nathan Jacobson, *Basic algebra. II*, second ed., W. H. Freeman and Company, New York, 1989.
[53] B. Jónsson, *The unique factorization problem for finite relational structures*, Colloq. Math. **14** (1966), 1–32.
[54] B. Jónsson, *Algebras whose congruence lattices are distributive*, Math. Scand. **21** (1967), 110–121.
[55] E. Kiss, *Injectivity and related concepts in modular varieties: I–II*, Bull. Aust. Math. Soc. **32** (1985), 35–53.
[56] E. Kiss, *Three remarks on the modular commutator*, Algebra Universalis **29** (1992), 455–476.
[57] E. W. Kiss, *Complemented and skew congruences*, Ann. Univ. Ferrara Sez. VII(N.S.) **29** (1983), 111–127.
[58] E. W. Kiss, *Finitely boolean representable varieties*, Proc. Amer. Math. Soc. **89** (1983), 579–582.
[59] H. Lakser, W. Taylor, and S. Tschantz, *A new proof of gumm's theorem*, Algebra Universalis **20** (1985), 115–122.
[60] W. A. Lampe, *A property of the lattice of equational theories*, Algebra Universalis **23** (1986), 61–69.
[61] A. I. Maltsev, *On the general theory of algebraic systems*, Mat. Sbornik **77** (1954), 3–20 (Russian).
[62] R. McKenzie, *On minimal locally finite varieties with permuting congruence relations*, never published, 1978.
[63] R. McKenzie, *Narrowness implies uniformity*, Algebra Universalis **15** (1982), 67–85.
[64] R. McKenzie, *Residually small varieties of* $\mathbf{K}$*-algebras*, Algebra Universalis **14** (1982), 181–196.
[65] R. McKenzie, *Finite equational bases for congruence modular varieties*, Algebra Universalis **24** (1987), 224–250.
[66] Peter Mederly, *Three Mal'cev type theorems and their application*, Math. Časopis Sloven. Akad. Vied. **25** (1975), 83–95.
[67] F. Osterman and J. Schmidt, *Der baryzentrische Kalkul als axiomatische Grundlage der affinen Geometrie*, J. Reine Angew. Math. **224** (1966), 44–57.

[68] P. P. Pálfy and C. Szabó, *Congruence varieties of groups and abelian groups*, Lattice Theory and its Applications (K. A. Baker and R. Wille, eds.), Heldermann Verlag, Lemgo, Germany, 1995, Darmstadt, Germany, June 13–17, 1991, pp. 163–184.

[69] P. P. Pálfy and C. Szabó, *An identity for subgroup lattices of abelian groups*, Algebra Universalis **33** (1995), 191–195.

[70] E. A. Palyutin, *Models with enumerably categorical universal theories*, Algebra i Logika **10** (1971), 23–32.

[71] E. A. Palyutin, *Description of categorical quasivarieties*, Algebra i Logika **14** (1975), no. 2, 145–185, 240.

[72] A. F. Pixley, *Completeness in arithmetical algebras*, Algebra Universalis **2** (1972), 179–196.

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

[74] S. V. Polin, *Identities in congruence lattices of universal algebras*, Mat. Zametki **22** (1977), 443–451 (Russian), transl. Math. Notes, **22**(1977), 737–742.

[75] R. W. Quackenbush, *Demi-semi-primal algebras and mal'cev-type conditions*, Math. Z. **122** (1971), 166–176.

[76] R. W. Quackenbush, *Algebras with minimum spectrum*, Algebra Universalis **10** (1980), 117–129.

[77] R. W. Quackenbush, *A new proof of rosenberg's primal algebra characterization theorem*, Finite algebra and Multiple-valued logic (Szeged,1979), 1981, Colloq. Math. Soc. János Bolyai, pp. 603–634.

[78] A. Rosenberg and D. Zelinsky, *Finiteness of the injective hull*, Math. Z. **70** (1959), 372–380.

[79] J. D. H. Smith, *Mal'cev varieties*, vol. 554, Lecture Notes in Mathematics, Berlin, 1976.

[80] W. Taylor, *Characterizing mal'cev conditions*, Algebra Universalis **3** (1973), 351–397.

[81] M. R. Vaughan-Lee, *Nilpotence in permutable varieties*, Universal Algebra and Lattice Theory (R. Freese and O. Garcia, eds.), Springer-Verlag, New York, 1983, Lecture notes in Mathematics, vol. **1004**, pp. 293–308.

[82] R. Wille, *Primitive subsets of lattices*, Algebra Universalis **2** (1972), 95–98.

[83] Pavol Zlatoš, *Unitary congruence adjunctions*, Lectures in universal algebra (Szeged, 1983), Colloq. Math. Soc. János Bolyai, vol. 43, North-Holland, Amsterdam, 1986, pp. 587–647.

Index