Lectures on Universal Algebra

Matt Valeriote
McMaster University

November 8, 1999

1 Algebras

In this first section we will consider some common features of familiar algebraic structures such as groups, rings, lattices, and boolean algebras to arrive at a definition of a general algebraic structure.

Recall that a group **G** consists of a nonempty set G, along with a binary operation $\cdot : G \to G$, a unary operation $^{-1} : G \to G$, and a constant 1_G such that

- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all x, y, $z \in G$,
- $x \cdot x^{-1} = 1_G$ and $x^{-1} \cdot x = 1_G$ for all $x \in G$,
- $1_G \cdot x = x$ and $x \cdot 1_G = x$ for all $x \in G$.

A group is abelian if it additionally satisfies:

$x \cdot y = y \cdot x$ for all x, $y \in G$.

A ring **R** is a nonempty set R along with binary operations $+$, $\cdot$, a unary operation $-$, and constants 0_R and 1_R which satisfy

- R, along with $+$, $-$, and 0_R is an abelian group.
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all x, y, $z \in G$.
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ and $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$ for all x, y, $z \in G$.

- $1_G \cdot x = x$ and $x \cdot 1_G = x$ for all $x \in G$.

Lattices are algebras of a different nature, they are essentially an algebraic encoding of partially ordered sets which have the property that any pair of elements of the ordered set has a least upper bound and a greatest lower bound. A lattice $\mathbf{L}$ consists of a nonempty set L, equipped with two binary operations $\wedge$ and $\vee$ which satisfy:

- $x \wedge x = x$ and $x \vee x = x$ for all $x \in L$,
- $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$ for all x, $y \in L$,
- $x \wedge (y \vee x) = x$ and $x \vee (y \wedge x) = x$ for all x, $y \in L$.

It follows from the above equations, that if we define the relation $\leq$ on L by: $x \leq y$ if and only if $x = x \wedge y$ then $\leq$ is a partial order on L. Furthermore, for x, $y \in L$, the element $x \wedge y$ is the greatest lower bound of x and y, and $x \vee y$ is the least upper bound of x and y with respect to the order $\leq$.

Conversely, if $\langle P, \leq \rangle$ is a partially ordered set, with the property that each pair from P has a greatest lower bound and least upper bound, then by defining $x \wedge y$ and $x \vee y$ to be the greatest lower bound and least upper bound of x and y respectively, P, equipped with these operations is a lattice.

Sometimes lattices have a smallest element and a largest element with respect to its partial order. When this is the case, we use the constant symbols 0 and 1 to denote these elements. Such a lattice is called a bounded lattice and satisfies the equations:

$$x \wedge 1 = x \text{ and } x \vee 0 = x \text{ for all } x \in L.$$

A lattice is distributive if it satisfies the distributive laws:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

and

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

One last important class of algebras to mention is the class of boolean algebras. A boolean algebra is an algebra of the form $\langle B, \wedge, \vee, ', 0, 1 \rangle$ where $\langle B, \wedge, \vee, 0, 1 \rangle$ is a bounded distributive lattice and $'$ is a unary operation such that

- $(x')' = x$ for all $x \in B$.

- $(x \wedge y)' = x' \vee y'$ for all $x, y \in B$.
- $(x \vee y)' = x' \wedge y'$ for all $x, y \in B$.
- $x' \vee x = 1$ and $x' \wedge x = 0$ for all $x \in B$.

The set of all subsets of a set X, with the operations of intersection, union and complementation forms a boolean algebra called a field of sets. It turns out that every boolean algebra can be embedded into some field of sets.

Definition 1 *An algebra* $\mathbf{A}$ *is a pair* $\langle A, F \rangle$*, with* A *a nonempty set, called the universe of* $\mathbf{A}$*, and* $F = \langle f_i : i \in I \rangle$*, a sequence of finitary operations on* A*. The operations in* F *are called the basic operations of* $\mathbf{A}$ *and the set* I *is called the index set of* $\mathbf{A}$*. The type of* $\mathbf{A}$ *is the function* $\tau : I \to \mathbb{N}$*, where* $\tau(i)$ *is equal to the arity of the function* f_i*. (The arity of an operation* f *on* A *is* n*, if and only if the domain of* f *is* A^n*.)*

Two algebras are said to be similar if and only if they have the same type.

We often call the elements of the index set I of an algebra $\mathbf{A}$ the operation symbols of $\mathbf{A}$, and for $f \in I$, the basic operation of $\mathbf{A}$ corresponding to f is denoted by $f^{\mathbf{A}}$.

Following this convention then, the index set of the ring of integers is $\{\cdot, +, -, 0, 1\}$, while the operation of multiplication is denoted by $\cdot^{\mathbb{Z}}$. If the context is clear, we usually dispense with the superscript.

Note that all of the examples presented earlier are algebras in the above sense.

Those familiar with groups and rings will undoubtably be familiar with the concepts of subgroups and subrings, as well as with homomorphisms, isomorphisms, and direct products. All of these things have natural extensions to the class of all algebras.

Definition 2 *A subuniverse of the algebra* $\mathbf{A}$ *is a subset (possibly empty) of* A *which is closed under all of the basic operations of* $\mathbf{A}$*.* $\mathbf{B}$ *is a subalgebra of* $\mathbf{A}$ *if* $\mathbf{B}$ *is similar to* $\mathbf{A}$*,* B *is a nonempty subuniverse of* $\mathbf{A}$*, and for each* f *in the index of* $\mathbf{A}$*, the operation* $f^{\mathbf{B}}$ *is the restriction to* B *of the operation* $f^{\mathbf{A}}$*.*

Let $\mathrm{Sub}\,(\mathbf{A})$ be the set of all subuniverses of the algebra $\mathbf{A}$. This set is naturally ordered by inclusion. It turns out that this ordered set is a lattice.

Proposition 3 *Let* $\mathbf{A}$ *be an algebra.*

1. *The intersection of a set* S *of subuniverses of* $\mathbf{A}$ *is a subuniverse of* $\mathbf{A}$*, and is the greatest lower bound of* S*.*

2. *Let* $\mathbf{A}$ *be an algebra. Then* $\mathrm{Sub}\,(\mathbf{A})$*, ordered by inclusion is a lattice.*

From this proposition, we see that intersection is the meet operation of the subuniverse lattice. It also follows that for $X \subseteq A$, the intersection of the set of all subuniverses of $\mathbf{A}$ which contain X is a subuniverse of X. Clearly, this subuniverse is the smallest one which contains X, and is denoted by $\mathrm{Sg}^{\mathbf{A}}(X)$. If $B = \mathrm{Sg}^{\mathbf{A}}(X)$, then X is called a generating set for B. If B is generated by a finite set, then B is said to be a finitely generated subuniverse. The algebra $\mathbf{A}$ is called finitely generated if A is a finitely generated subuniverse of $\mathbf{A}$.

With a little effort, it can be shown that the join of two subuniverses U and V of $\mathbf{A}$ is equal to $\mathrm{Sg}^{\mathbf{A}}(U \cup V)$.

A homomorphism from the group $\mathbf{G}$ to the group $\mathbf{H}$ can be described as a map from G to H which is compatible with the operations of the groups. Lifting this to arbitrary algebras yields the following definition:

Definition 4 *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be similar algebras, of type* $\tau : I \to \mathbb{N}$*. A function* $h : A \to B$ *is a homomorphism from* $\mathbf{A}$ *to* $\mathbf{B}$ *if* h *is compatible with the basic operations of* $\mathbf{A}$ *and* $\mathbf{B}$*, i.e., for all* $f \in I$*, if* $\tau(f) = n$*, then for all* $a_1, \ldots, a_n \in A$*,* $h(f^{\mathbf{A}}(a_1, \ldots, a_n)) = f^{\mathbf{B}}(h(a_1), \ldots, h(a_n))$*.*

If $h : A \to B$ is a surjective homomorphism from $\mathbf{A}$ to $\mathbf{B}$, then $\mathbf{B}$ is called a homomorphic image of $\mathbf{A}$. An isomorphism between two similar algebras $\mathbf{A}$ and $\mathbf{B}$ is a homomorphism which is also injective and surjective. In this case, the algebras $\mathbf{A}$ and $\mathbf{B}$ are said to be isomorphic.

For h a homomorphism between a pair of groups or rings, we are able to associate a subalgebra, called the kernel of h, by setting the kernel to be the set of elements in the domain of h which are mapped to the identity element of the range. Besides being a subalgebra, the kernel has other special properties. Since a general algebra doesn't usually come equipped with an identity element, then we can't naturally associate a subalgebra with a homomorphism. Instead, we define the kernel of a homomorphism $h : A \to B$, denoted by $\ker(h)$, to be the following equivalence relation:

$$\ker(h) = \{(a, b) \in A \times A \,:\, h(a) = h(b)\}.$$

The fact that h is compatible with the basic operations of $\mathbf{A}$ and $\mathbf{B}$ carries over to the kernel. Namely, if $(a_i, b_i) \in \ker(h)$ for $i \leq n$ and f is an n-ary basic operation of $\mathbf{A}$, then $(f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)) \in \ker(h)$.

As with groups and rings, the kernel can be used to detect when a homomorphism is injective. Namely,

Proposition 5 *Let $h : A \to B$ be a homomorphism from $\mathbf{A}$ to $\mathbf{B}$. Then h is injective if and only if $\ker(h) = \{(a, a) : a \in A\}$.*

Note that for h a group homomorphism, the kernel of h in the above sense is equal to the equivalence relation induced by the partitioning of the domain by the cosets of the kernel in the usual sense.

Definition 6 *A binary relation θ on an algebra $\mathbf{A}$ is called a congruence relation on $\mathbf{A}$ if it is an equivalence relation on $\mathbf{A}$ which is compatible with the basic operations of $\mathbf{A}$. The set of all congruences on an algebra $\mathbf{A}$ will be denoted by $\mathrm{Con}\,(\mathbf{A})$.*

So, every kernel of a homomorphism from $\mathbf{A}$ to some other algebra is a congruence relation on $\mathbf{A}$.

As with the set of subuniverses of an algebra, we can partially order $\mathrm{Con}\,(\mathbf{A})$ by inclusion.

Proposition 7 *Let $\mathbf{A}$ be an algebra.*

1. *The intersection of a set S of congruences on $\mathbf{A}$ is a congruence on $\mathbf{A}$ and is the least upper bound of S with respect to inclusion.*

2. *Under inclusion, $\mathrm{Con}\,(\mathbf{A})$ is a lattice.*

The congruence lattice of an algebra $\mathbf{A}$ is in fact a bounded lattice, with the least element 0_A being the identity relation $\{(a, a) : a \in A\}$ and the largest element 1_A being $A \times A$.

For X a collection of ordered pairs on A, the smallest congruence which contains X, called the congruence of $\mathbf{A}$ generated by X, and denoted by $\mathrm{Cg}^{\mathbf{A}}(X)$, is equal to the intersection of the set of congruences on $\mathbf{A}$ which contain X. A congruence θ is finitely generated if $\theta = \mathrm{Cg}^{\mathbf{A}}(X)$ for some finite set X.

As with groups and rings, there is a close connection between homomorphic images, kernels and congruences for arbitrary algebras. The connections arise by considering quotient algebras.

Recall that if N is a normal subgroup of the group G, then G/N is equal to the set of equivalence classes of the equivalence relation

$$\{(a, b) : aN = bN\}.$$

The fact that N is normal allows us to define a natural group structure on G/N by setting $aN \cdot bN = abN$ and $(aN)^{-1} = (a^{-1})N$.

Replacing G and N by an algebra $\mathbf{A}$ and congruence θ, and mimicking this construction, we can define the quotient of $\mathbf{A}$ by θ.

Definition 8 *Let $\mathbf{A}$ be an algebra and θ a congruence on $\mathbf{A}$. For $a \in A$, let $a/\theta = \{b \in A : (a, b) \in \theta\}$, the congruence class of θ which contains a. Let $A/\theta = \{a/\theta : a \in A\}$.*

Since θ is an equivalence class, then the congruence classes of θ partition the set A. It is an easy exercise to check that for N a normal subgroup of the group G, the equivalence relation corresponding to the partitioning of G by the left cosets of N is a congruence on G.

Let τ and I be the type and index set, respectively, of $\mathbf{A}$. We define the algebra $\mathbf{A}/\theta$ of type τ to be the algebra with universe A/θ and such that for each $f \in I$, say with $\tau(f) = n$,

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

The compatibility of the congruence θ with the basic operations of $\mathbf{A}$ ensures that this function is well defined. $\mathbf{A}/\theta$ is called the quotient of $\mathbf{A}$ by the congruence θ.

As the above is a generalization of the quotient construction from groups and rings, many of the familiar features of quotient groups and quotient rings hold for arbitrary quotients.

Theorem 9 *Let $\mathbf{A}$ and $\mathbf{B}$ be similar algebras, let h be a homomorphism from $\mathbf{A}$ onto $\mathbf{B}$, and let θ be a congruence relation on $\mathbf{A}$. Then*

1. *The map $g : A \to A/\theta$ defined by $g(a) = a/\theta$ is a surjective homomorphism from $\mathbf{A}$ to $\mathbf{A}/\theta$ whose kernel is θ.*

2. *There is a unique isomorphism f from $\mathbf{A}/\theta$ to $\mathbf{B}$ which satisfies $h = f \circ g$.*

The proof of this theorem is essentially the same as the corresponding result for groups and rings. It shows that congruences and kernels are one and the same thing, and also shows that, up to isomorphism, the collection of quotients of an algebra $\mathbf{A}$ is the same as the collection of homomorphic images of $\mathbf{A}$.

The final topic in this first section has to do with a construction which produces, from a system of algebras, an algebra which is larger and apparently more complicated than the individual algebras in the system. This is in contrast to the earlier constructions.

Let $\langle \mathbf{A}_i : i \in I \rangle$ be a sequence of algebras of type τ. We define the direct product of this sequence to be the algebra $\prod_{i\in I} \mathbf{A}_i$ of type τ with universe $\prod_{i\in I} A_i$ and such that if f is an n-ary function symbol of τ, then $f^{\prod_{i\in I}\mathbf{A}_i}(\alpha_1, \ldots, \alpha_n)$ is the element of $\prod_{i\in I} A_i$ whose jth component is the element $f^{\mathbf{A}_j}(\alpha_1(j), \ldots, \alpha_n(j))$, for all $j \in I$. Recall that $\prod_{i\in I} A_i$ consists of all sequences indexed by I whose jth component is a member of A_j, for all $j \in I$.

An algebra which is isomorphic to a nontrivial direct product of a sequence of algebras is said to be directly decomposable. If it can't be so represented it is called directly indecomposable. The following proposition shows that indecomposability can be detected by looking for certain pairs of congruences of the algebra in question.

The relational product of two binary relations α and β on a set A is defined to be the binary relation

$$\alpha \circ \beta = \{(a, c) : (a, b) \in \alpha \text{ and } (b, c) \in \beta \text{ for some } b \in A\}.$$

As an exercise, check that if α and β are equivalence relations or congruences then so is their product. Congruences α and β are said to permute if $\alpha \circ \beta = \beta \circ \alpha$.

Proposition 10 *An algebra $\mathbf{A}$ is directly decomposable if and only if there are permuting congruences α and β with $\alpha \wedge \beta = 0_A$ and $\alpha \vee \beta = 1_A$ and with $\{\alpha, \beta\} \neq \{0_A, 1_A\}$.*

Proof. $\mathbf{A}$ is isomorphic to a nontrivial direct product of a sequence of algebras, if and only if $\mathbf{A}$ is isomorphic to $\mathbf{B} \times \mathbf{C}$ for some nontrivial algebras

$\mathbf{B}$ and $\mathbf{C}$. If $\mathbf{A} = \mathbf{B} \times \mathbf{C}$ then the projection maps $\pi_1 : B \times C \to B$ and $\pi_2 : B \times C \to C$ defined by $\pi_1(b, c) = b$ and $\pi_2(b, c) = c$ for all $(b, c) \in B \times C$ are surjective homomorphisms. It can be shown that the kernels of π_1 and π_2 satisfy the conditions of the proposition.

Conversely, if $\mathbf{A}$ has a pair of congruences α and β which satisfy the conditions of the proposition, then the map $f : A \to A/\alpha \times A/\beta$ defined by $f(a) = (a/\alpha, a/\beta)$ is an isomorphism between $\mathbf{A}$ and $\mathbf{A}/\alpha \times \mathbf{A}/\beta$. ∎

Exercises:

1. If S is a set of subuniverses of the algebra $\mathbf{A}$, then the intersection of S is the greatest lower bound of S in the lattice Sub $(\mathbf{A})$.

2. If α and β are equivalence relations on the set A, then $\alpha \circ \beta$ is an equivalence relation on A. If α and β are congruences on $\mathbf{A}$, then $\alpha \circ \beta$ is a congruence on $\mathbf{A}$.

3. Let $h : \mathbf{A} \to \mathbf{B}$ be a homomorphism. If U is a subuniverse of $\mathbf{A}$ then $h(U)$ is a subuniverse of $\mathbf{B}$. If V is a subuniverse of $\mathbf{B}$ then $h^{-1}(V)$ is a subuniverse of $\mathbf{A}$.

4. If $\mathbf{A}$ and $\mathbf{B}$ are isomorphic then Sub $(\mathbf{A})$ is isomorphic to Sub $(\mathbf{B})$ and Con $(\mathbf{A})$ is isomorphic to Con $(\mathbf{B})$. Show that the converse need not hold by finding two similar non-isomorphic algebras whose subuniverse and congruence lattices are isomorphic.

5. If $h : \mathbf{A} \to \mathbf{B}$ and $g : \mathbf{B} \to \mathbf{C}$ are homomorphisms then $g \circ h$ is a homomorphism. Show that if h is an isomorphism, then h^{-1} is an isomorphism too.

6. If X generates the algebra $\mathbf{A}$ and $f : X \to B$ is any map then there is at most one homomorphism from $\mathbf{A}$ to $\mathbf{B}$ which extends f.

7. Let $\mathbf{A}$ be an algebra. Show that there is some algebra $\mathbf{B}$ such that Sub $(\mathbf{B})$ = Con $(\mathbf{A})$.

8. If α and β are permuting congruences of the algebra $\mathbf{A}$ then $\alpha \vee \beta$ equals $\alpha \circ \beta$ in Con $(\mathbf{A})$.

9. Show that the set of equivalence relations on a set A is a lattice. Show that Con $(\mathbf{A})$ is a sublattice of this lattice.

10. Show that the lattice of normal subgroups of a group $\mathbf{G}$ is isomorphic to Con ($\mathbf{G}$).

11. Let $f : \mathbf{A} \to \mathbf{B}$ and $g : \mathbf{A} \to \mathbf{C}$ be homomorphisms with $\ker(f) \subseteq \ker(g)$ and with f surjective. Then there is a homomorphism $h : \mathbf{B} \to \mathbf{C}$ with $g = h \circ f$.

2 Varieties

The reader may have noticed that the examples of algebras presented in the first section were all defined via equations. In this section I will discuss the classification of algebraic structures according to the equations which they satisfy. Equationally defined collections of algebras are called varieties and are central objects of study in universal algebra.

Equations in the type τ are expressions which equate terms of type τ. The set of terms of type τ in the variables X is the smallest collection $T(X)$ of finite strings which satisfies:

- $X \subseteq T(X)$.
- If $c \in I$ and $\tau(c) = 0$ (i.e., c is a constant symbol) then $c \in T(X)$.
- If $t_1, \ldots, t_n \in T(X)$ and $f \in I$ has arity n then $f(t_1, \ldots, t_n) \in T(X)$

For convenience, we will assume that throughout this discussion, the set of variables X is disjoint from the symbols associated with τ and that X is nonempty if the set of constant symbols of τ is empty. For $\mathbf{A}$ an algebra of type τ and $t(x_1, \ldots, x_n)$ a term of type τ in the variables $\{x_1, \ldots, x_n\}$, we define the n-ary operation $t^{\mathbf{A}}$ on A by induction on the length of t as follows:

- If $t = x_i$ for some $i \leq n$, then for $\bar{a} \in A$, $t^{\mathbf{A}}(\bar{a}) = a_i$.
- If $t = c$ for some constant symbol c of τ, then for $\bar{a} \in A$, $t^{\mathbf{A}}(\bar{a}) = c^{\mathbf{A}}$, the interpretation of c in the algebra $\mathbf{A}$.
- If $t = f(t_1, \ldots, t_k)$, then for $\bar{a} \in A$, $t^{\mathbf{A}}(\bar{a}) = f^{\mathbf{A}}(t_1^{\mathbf{A}}(\bar{a}), \ldots, t_k^{\mathbf{A}}(\bar{a}))$.

An equation of type τ is a string of the form $s \approx t$, where s and t are terms of type τ. If $\mathbf{A}$ is an algebra of type τ and s and t are terms in the variables $\{x_1, \ldots, x_n\}$, then the n-tuple $\bar{a}$ from A satisfies the equation $s \approx t$

if $s^{\mathbf{A}}(\bar{a}) = t^{\mathbf{A}}(\bar{a})$. The equation $s \approx t$ is true in $\mathbf{A}$ if $\bar{a}$ satisfies the equation for all $\bar{a}$ from A. We denote this by $\mathbf{A} \models s \approx t$.

Let Σ be a set of equations of type τ. The class of all algebras of type τ which satisfy all of the equations in Σ is denoted by $\mathrm{Mod}\,(\Sigma)$ (the class of models of Σ). Such a class of algebras is called an equational class and we say that Σ axiomatizes it.

Given a class $\mathcal{K}$ of algebras of type τ, we let $\Theta(\mathcal{K})$ be the set of equations of type τ in the variables $\{x_i : i \in \mathbb{N}\}$ which are satisfied by all algebras in $\mathcal{K}$. A set of equations of the form $\Theta(\mathcal{K})$ for some class $\mathcal{K}$ is called an **equational theory**.

There is a close connection between equational classes and the algebraic operations introduced in the first section. To set this up I need to define some special class operators.

Definition 11 *Let $\mathcal{K}$ be a class of similar algebras.*

- *$I(\mathcal{K})$ is the class of all algebras which are isomorphic to some member of $\mathcal{K}$.*
- *$H(\mathcal{K})$ is the class of all algebras which are a homomorphic image of some algebra in $\mathcal{K}$.*
- *$S(\mathcal{K})$ is the class of all algebras which are isomorphic to a subalgebra of some algebra in $\mathcal{K}$.*
- *$P(\mathcal{K})$ is the class of all algebras which are isomorphic to a direct product of a sequence of algebras from $\mathcal{K}$.*

The class $\mathcal{K}$ is said to be closed under a class operator O if $O(\mathcal{K})$ is contained in $\mathcal{K}$.

Anyone familiar with groups and rings will readily see that the class of groups and the class of rings are both closed under the class operators H, S, and P. A class of similar algebras with this closure property is called a variety. So, a class $\mathcal{K}$ is a variety if and only if $H(\mathcal{K}) = S(\mathcal{K}) = P(\mathcal{K}) = \mathcal{K}$.

For $\mathcal{K}$ a class of similar algebras, we can close it, as necessary, under the operators H, S and P to obtain the variety generated by $\mathcal{K}$. We denote this variety by $\mathsf{V}(\mathcal{K})$. It turns out that $\mathsf{V}(\mathcal{K}) = HSP(\mathcal{K})$. A variety $\mathcal{V}$ is finitely generated if $\mathcal{V} = \mathsf{V}(\mathcal{F})$ for some finite set $\mathcal{F}$ of finite algebras.

Theorem 12 *Let $\mathcal{V}$ be a equational class. Then $\mathcal{V}$ is a variety.*

PROOF. Proving this theorem amounts to showing that equations are preserved under the taking of subalgebras, homomorphic images and direct products. The verification of this is left to the reader. ∎

I will now set out to prove the converse to this theorem, commonly referred to as Birkhoff's Theorem. What I will show is that for $\mathcal{K}$ a class of similar algebras, $\mathsf{V}(\mathcal{K}) = \operatorname{Mod}\Theta(\mathcal{K})$. Since the class on the righthand side of this equality is an equational class, then when $\mathcal{K}$ happens to be a variety, it implies that $\mathcal{K}$ is also an equational class.

It was noted earlier that the class operators H, S, and P preserve equations and so it follows that if $\mathbf{A} \in \mathsf{V}(\mathcal{K})$ then $\mathbf{A}$ satisfies all of the equations which hold for $\mathcal{K}$. More concisely, $\mathsf{V}(\mathcal{K}) \subseteq \operatorname{Mod}\Theta(\mathcal{K})$.

Apparently the challenging part of Birkhoff's Theorem is to show that $\operatorname{Mod}\Theta(\mathcal{K}) \subseteq \mathsf{V}(\mathcal{K})$. To do this, we need to show that if $\mathbf{A}$ is an algebra which satisfies $\Theta(\mathcal{K})$ then $\mathbf{A}$ is equal to a homomorphic image of some algebra in $SP(\mathcal{K})$. The algebra from $SP(\mathcal{K})$ which we will use is called a free algebra for $\mathcal{K}$.

The set $T(X)$ of terms of type τ in the variables X can be enriched to produce an algebra of type τ, called the term algebra of type τ in the variables X in the following way: for f an n-ary operation symbol of τ, define $f^{\mathbf{T}(X)}$ by

$$f^{\mathbf{T}(X)}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n),$$

for all term $t_1, \ldots, t_n \in T(X)$.

Proposition 13 *Let τ be a type of algebras and let X be a set of variables. Then $\mathbf{T}(X)$ is generated by X and, if $\mathbf{A}$ is any algebra of type τ and f any map from X to A then there is a unique homomorphism $g : \mathbf{T}(X) \to \mathbf{A}$ which extends the map f.*

PROOF. That X generates $\mathbf{T}(X)$ follows pretty much from the definition of $\mathbf{T}(X)$. Now, let $f : X \to A$. We'll define $g : T(X) \to A$ by setting $g(t) = t^{\mathbf{A}}(a_1, \ldots, a_n)$, for t a term in the variables $x_1, \ldots, x_n$ where $f(x_i) = a_i$, for $i \leq n$. It is an elementary exercise to check that g is a homomorphism which extends f. Since X generates $\mathbf{T}(X)$, it follows that there is at most one homomorphism into $\mathbf{A}$ which extends f. ∎

An algebra which satisfies the properties listed in this proposition is said to have the universal mapping property for the class of all τ-algebras over X. Such an algebra is also said to be absolutely free.

More generally, if $\mathcal{K}$ is a class of algebras of type τ, then the algebra $\mathbf{F}$ of type τ is said to have the universal mapping property with respect to $\mathcal{K}$ over X if for every $\mathbf{A} \in \mathcal{K}$ and every map $f : X \to A$, there is a homomorphism $g : \mathbf{F} \to \mathbf{A}$ which extends f. If in addition, X generates $\mathbf{F}$, then $\mathbf{F}$ is said to be free for $\mathcal{K}$ over X.

It follows from the proposition that if $\mathbf{A}$ is an algebra of type τ, then $\mathbf{A}$ is a homomorphic image of the term algebra $\mathbf{T}(A)$ generated by A, since the extension of the identity map on A to a homomorphism from $\mathbf{T}(A)$ to $\mathbf{A}$ is surjective.

Proposition 14 *Let $\mathcal{K}$ be a class of algebras of type τ and let X be a set of variables. Define θ to be the intersection of the set*

$$\{\alpha \in \mathrm{Con}\,(\mathbf{T}(X)) \,:\, \mathbf{T}(X)/\alpha \in S(\mathcal{K})\}.$$

Then $\mathbf{T}(X)/\theta \in SP(\mathcal{K})$ and is free for $\bigvee(\mathcal{K})$ over the set X/θ.

Proof. By an earlier result, θ is a congruence on $\mathbf{T}(X)$. To show that $\mathbf{T}(X)/\theta$ is in $SP(\mathcal{K})$ it suffices to produce an embedding h from $\mathbf{T}(X)/\theta$ into a direct product of algebras from $\mathcal{K}$. Let $\mathbf{B} = \prod_{\alpha \in S} \mathbf{T}(X)/\alpha$, where $S = \{\alpha \,:\, \mathbf{T}(X)/\alpha \in S(\mathcal{K})\}$. I claim, without proof, that the following definition for h works:

$$h(t/\theta)(\alpha) = t/\alpha$$

for all $\alpha \in S$ and $t \in T(X)$.

Let's first show that this algebra is free for $\mathcal{K}$ over X/θ. Let $\pi : \mathbf{T}(X) \to \mathbf{T}(X)/\theta$ be the homomorphism which maps t to t/θ for all terms t. Take $\mathbf{A} \in \mathcal{K}$ and let $f : X/\theta \to A$ be any map. Since $\mathbf{T}(X)$ is absolutely free, then there is a unique homomorphism $g : \mathbf{T}(X) \to \mathbf{A}$ which extends the map $f \circ \pi$ on X.

As $\mathbf{T}(X)/\ker(g)$ is isomorphic to a subalgebra of $\mathbf{A}$, then $\theta \subseteq \ker(g)$. From this it follows that the map $h : \mathbf{T}(X)/\theta \to \mathbf{A}$ defined by $h(t/\theta) = g(t)$ is a well defined homomorphism with $h \circ \pi = g$. Clearly, h extends the map f.

It is left as an exercise to show that $\mathbf{T}(X)/\theta$ must be free for $HSP(\mathcal{K})$ as well. ∎

If $\mathcal{K}$ consists of only 1 element algebras, then the congruence θ from the previous proposition is the largest congruence on $\mathbf{T}(X)$ and so $\mathbf{T}(X)/\theta$ is also trivial. On the other hand, if $\mathcal{K}$ contains some nontrivial algebras, then the set X/θ is in one-to-one correspondence with X and so we can find an algebra which is isomorphic to $\mathbf{T}(X)/\theta$ and which is free for $\mathsf{V}(\mathcal{K})$ over X. Thus we have:

Corollary 15 *If $\mathcal{K}$ contains a nontrivial algebra, then if X is any set, $SP(\mathcal{K})$ contains an algebra which is free for $\mathsf{V}(\mathcal{K})$ over X.*

We denote a free algebra for the class $\mathcal{K}$ over X by $\mathbf{F}_{\mathcal{K}}(X)$. It follows that if a free algebra exists, then it is determined up to isomorphism by the cardinality of the set X.

Theorem 16 *Let $\mathcal{K}$ be a class of similar algebras. Then $\mathcal{K}$ is a variety if and only if it is an equational class.*

Proof. From the preceding discussion, we need only verify that if $\mathbf{A}$ is an algebra in $\operatorname{Mod}\Theta(\mathcal{K})$ then $\mathbf{A}$ is a homomorphic image of some algebra in $SP(\mathcal{K})$. The case in which $\mathcal{K}$ consists only of trivial algebras is not interesting, and so we will assume that $\mathcal{K}$ contains some nontrivial algebras. By the previous corollary, $SP(\mathcal{K})$ contains an algebra $\mathbf{F}_{\mathcal{K}}(A)$ which is free for $\mathsf{V}(\mathcal{K})$ over the set A.

Let $f : \mathbf{T}(A) \to \mathbf{A}$ be a homomorphism with $f(a) = a$ for all $a \in A$ and let $g : \mathbf{T}(A) \to \mathbf{F}_{\mathcal{K}}(A)$ be the homomorphism which extends the identity map on A. If we can show that the kernel of g is contained in the kernel of f, then it will follow that there is a surjective homomorphism $h : \mathbf{F}_{\mathcal{K}}(A) \to \mathbf{A}$. This of course places $\mathbf{A}$ in $\mathsf{V}(\mathcal{K})$, as required.

So, suppose that $(s(\bar{a}), t(\bar{a}))$ is in the kernel of g. Then the equation $s \approx t$ holds for all algebras in $\mathcal{K}$ (this requires some justification) and so, in particular, $s \approx t$ holds in $\mathbf{A}$, since $\mathbf{A}$ satisfies all of the equations which hold in $\mathcal{K}$. But then, $s^{\mathbf{A}}(\bar{a}) = t^{\mathbf{A}}(\bar{a})$, which implies that $(s(\bar{a}), t(\bar{a}))$ is in the kernel of f. ∎

Exercises

1. Show that for a class of similar algebras $\mathcal{K}$, $HS(\mathcal{K}) \subseteq SH(\mathcal{K})$, $SP(\mathcal{K}) \subseteq PS(\mathcal{K})$ and $PH(\mathcal{K}) \subseteq HP(\mathcal{K})$.

2. An operator O is idempotent if $OO = O$. Show that the class operators H, S, and P are idempotent.

3. Show that for $\mathcal{K}$ a class of similar algebras, $HSP(\mathcal{K})$ is closed under H, S, and P and so is equal to the variety generated by $\mathcal{K}$.

4. Let $\mathcal{K}$ be a class of algebras of type τ and Σ a set of equations of type τ. Show that

   (a) $\mathcal{K} \subseteq \operatorname{Mod} \Theta(\mathcal{K})$.

   (b) $\Theta(\mathcal{K}) = \Theta(\mathsf{V}(\mathcal{K}))$.

   (c) $\Sigma \subseteq \Theta\operatorname{Mod}(\Sigma)$.

5. For $\mathcal{K}$ a class of algebras of type τ, and X a set of variables, the relation $\{(s,t) : s,t \in T(X) \text{ and } \mathcal{K} \models s \approx t\}$ is a congruence of $\mathbf{T}(X)$.

6. Show that if S is a subset of the algebra $\mathbf{A}$, then the subalgebra generated by S has subuniverse

$$\{t^{\mathbf{A}}(s_1, \ldots, s_n) : \text{for some } n \geq 0,\ s_i \in S \text{ and term } t(x_1, \ldots, x_n)\}.$$

7. Let $\mathbf{A}$ and $\mathbf{B}$ be two algebras of type τ which have the universal mapping property with respect to the class of all τ-algebras over the set X. Show that $\mathbf{A}$ and $\mathbf{B}$ are isomorphic.

8. Let $\mathbf{F}$ be free for the class $\mathcal{K}$ over X. Show that $\mathbf{F}$ is free for $\mathsf{V}(\mathcal{K})$ over X. Hint: Show that it is free for each of the classes $H(\mathcal{K})$, $S(\mathcal{K})$, and $P(\mathcal{K})$ over X.

9. Let $\mathcal{K}$ be a class of similar algebras and let X be an infinite set. Then $\mathsf{V}(\mathcal{K}) = \mathsf{V}(\mathbf{F}_{\mathcal{K}}(X))$. Also, show that $\mathsf{V}(\mathcal{K})$ is generated by the set $\{\mathbf{F}_{\mathcal{K}}(n) : n \geq 1\}$.

3 More on Varieties

It can be shown that a variety $\mathcal{V}$ is generated by $\mathbf{F}_{\mathcal{V}}(X)$ for any infinite set X. It is also the case that $\mathcal{V}$ is generated by $\{\mathbf{F}_{\mathcal{K}}(n) : n \geq 1\}$. In this section, I would like to identify another class of algebras which can be used to generate varieties. These algebras are called subdirectly irreducible and can be regarded as the building blocks of algebras and varieties.

Earlier I mentioned directly indecomposable algebras. An easy inductive argument shows that any finite algebra is isomorphic to a direct product

of directly indecomposable algebras. Unfortunately, this does not hold for arbitrary algebras. To remedy this, we consider algebras which are indecomposable with respect to a different sort of product.

Definition 17 *A subdirect product of the algebras* $\{\mathbf{A}_i : i \in I\}$ *is a subalgebra* $\mathbf{B}$ *of the direct product* $\prod_{i\in I} \mathbf{A}_i$ *such that for all* $j \in I$, $\pi_j(B) = A_j$, *where* $\pi_j : \prod_{i\in I} A_i \to A_j$ *is the projection map.*

A subdirect representation of $\mathbf{A}$ *by the algebras* $\{\mathbf{A}_i : i \in I\}$ *is an embedding* $f : \mathbf{A} \to \prod_{i\in I} \mathbf{A}_i$ *with* $f(\mathbf{A})$ *a subdirect product of the* $\mathbf{A}_i$*s.*

An algebra $\mathbf{A}$ *is subdirectly irreducible if* $|A| > 1$ *and for every subdirect embedding* $f : \mathbf{A} \to \prod_{i\in I} \mathbf{A}_i$, *there is some* $i \in I$ *with* $\pi_i \circ f$ *an isomorphism.*

As with direct indecomposibility, one can test for subdirect irreducibility by looking at the congruence lattice of the algebra.

Proposition 18 *A nontrivial algebra* $\mathbf{A}$ *is subdirectly irreducible if and only if there is a congruence* μ *of* $\mathbf{A}$ *with* $\mu \neq 0_A$ *and with* $\mu \leq \alpha$ *for all nonzero congruences* α *of* $\mathbf{A}$.

Proof. Suppose that $\mathbf{A}$ has a congruence μ with the above properties and let $f : \mathbf{A} \to \prod_{i\in I} \mathbf{A}_i$ be a subdirect embedding of $\mathbf{A}$. Since f is one-to-one then its kernel is 0_A. But, the kernel of f is equal to the intersection of the congruences $\ker(\pi_i \circ f)$ for $i \in I$ and so $\bigcap_{i\in I}\{\ker(\pi_i \circ f) : i \in I\} = 0_A$. As μ is contained in every nontrivial congruence of $\mathbf{A}$ it follows that $\ker(\pi_i \circ f) = 0_A$ for some $i \in I$. This means that $\pi_i \circ f$ is an isomorphism, and so $\mathbf{A}$ is subdirectly irreducible.

Conversely, suppose that $\mathbf{A}$ is subdirectly irreducible and define $f : \mathbf{A} \to \prod\{\mathbf{A}/\theta : \theta \in \mathrm{Con}(\mathbf{A}) \text{ and } \theta \neq 0_A\}$ by $f(a)(\theta) = a/\theta$. Then f is a homomorphism with the property that $\pi_\theta \circ f$ is surjective, but not injective, for all nonzero congruences θ. Since $\mathbf{A}$ is irreducible, then f cannot be an embedding, and so $\ker(f) \neq 0_A$. But, $\ker(f) \subseteq \theta$ for all nonzero congruences θ, and so $\ker(f)$ is the congruence we are in search of. ∎

The congruence μ from the proposition is sometimes called the monolith of $\mathbf{A}$. In this case, the congruence 0_A is a completely meet irreducible element of the lattice $\mathrm{Con}(\mathbf{A})$, which means that it cannot be written as the intersection of any set of congruences, unless that set includes 0_A.

The following theorem, due to Birkhoff, shows that every algebra is isomorphic to a subdirect product of subdirectly irreducible algebras.

Theorem 19 *Let* $\mathbf{A}$ *be a nontrivial algebra. Then* $\mathbf{A}$ *is isomorphic to a subdirect product of subdirectly irreducible quotients of* $\mathbf{A}$.

PROOF. From the previous proposition, it follows that if α is a congruence of $\mathbf{A}$ which is completely meet irreducible, then $\mathbf{A}/\alpha$ is subdirectly irreducible. If we can find a set I of completely meet irreducible congruences of $\mathbf{A}$ whose intersection is 0_A then the homomorphism $f : \mathbf{A} \to \prod_{\alpha \in I} \mathbf{A}/\alpha$ defined by $f(a)(\alpha) = a/\alpha$ for $\alpha \in I$ will be a subdirect embedding of $\mathbf{A}$ into the subdirectly irreducible algebras $\mathbf{A}/\alpha$, $\alpha \in I$.

To find such a set of congruences, it will suffice to show that for any set of distinct elements $\{a, b\}$ of A, there is a completely meet irreducible congruence $\theta_{\{a,b\}}$ with $(a, b) \neq \theta_{\{a,b\}}$. By Zorn's lemma, it follows that there is a congruence $\theta_{\{a,b\}}$ of $\mathbf{A}$ which is maximal with respect to the property that $(a, b) \neq \theta_{\{a,b\}}$. It is an elementary exercise to show that this congruence is completely meet irreducible, since every congruence which properly contains it must contain the pair (a, b). ∎

For $\mathcal{K}$ a class of algebras, we denote the class of irreducible algebras in $\mathcal{K}$ by $\mathcal{K}_{SI}$. From the above theorem, it follows that if $\mathcal{V}$ is a variety, then $\mathcal{V} = \mathbf{V}(\mathcal{V}_{SI})$, and so it is of interest to determine the class of irreducible algebras in a variety. Recent research in this area by McKenzie and others points out that this task is inherently difficult.

For certain kinds of varieties, the class of irreducible members can be found fairly easily. A notable result of this kind is due to Jónsson, and will be discussed later. Let's consider a special case of this, due to Stone, by investigating the variety of boolean algebras.

Theorem 20 *Up to isomorphism, the 2 element boolean algebra* $\mathbf{2}$ *is the only nontrivial directly indecomposable boolean algebra.*

PROOF. Let $\mathbf{B}$ be a boolean algebra with more than 2 elements. Then there is an element $a \in B$ with $a \notin \{0_B, 1_B\}$. Using the element a we can define two nontrivial boolean algebras via the following construction.

If $b \in B$ let $B|_b = \{x \in B : x \leq b\}$ and let $\wedge_b$ and $\vee_b$ be the restriction of $\wedge$ and $\vee$ on $\mathbf{B}$ to $B|_b$. If we define x^* on $B|_b$ by $x' \wedge b$, then it turns out that $B|_b$ with these operations is a boolean algebra.

I claim that $\mathbf{B}$ is isomorphic to the direct product $\mathbf{B}|_a \times \mathbf{B}_{a'}$ via the homomorphism which sends the element x in B to the pair $(x \wedge a, x \wedge a')$. ∎

Corollary 21 *The two element boolean algebra is, up to isomorphism, the only subdirectly irreducible boolean algebra.*

Corollary 22 *If* $\mathbf{B}$ *is a boolean algebra, then* $\mathbf{B}$ *is isomorphic to a subalgebra of* $\mathbf{2}^X$ *for some set* X*.*

One successful scheme for classifying varieties is based on the nature of the congruence lattices which arise from the members of the variety.

An algebra $\mathbf{A}$ is said to have permuting congruences (or is congruence permutable) if for all congruences $\alpha, \beta \in \mathrm{Con}(\mathbf{A})$, $\alpha \circ \beta = \beta \circ \alpha$. A variety is congruence permutable if each of its members is congruence permutable.

We can use the next theorem, due to Mal'cev, to show that many classical algebraic structures generate congruence permutable varieties.

Theorem 23 *A variety* $\mathcal{V}$ *is congruence permutable if and only if there is a term* $p(x, y, z)$ *in the language of* $\mathcal{V}$ *such that* $\mathcal{V}$ *satisfies the equations:* $p(x, x, y) \approx y$ *and* $p(x, y, y) \approx x$*.*

Proof. Let p be a term as in the statement of the theorem and let $\mathbf{A} \in \mathcal{V}$. If $\alpha, \beta \in \mathrm{Con}(\mathbf{A})$, then we need only show, by symmetry, that if $(a, c) \in \alpha \circ \beta$, then $(a, c) \in \beta \circ \alpha$.

If $b \in A$ with $(a, b) \in \alpha$ and $(b, c) \in \beta$, then consider the element $d = p^{\mathbf{A}}(a, b, c)$. We have that

$$a = p(a, b, b) \beta p(a, b, c) \alpha p(b, b, c) = c$$

and so $(a, d) \in \beta$ and $(d, c) \in \alpha$. Thus $(a, c) \in \beta \circ \alpha$.

Conversely, suppose that $\mathcal{V}$ is congruence permutable, and to avoid a trivial situation, assume that $\mathcal{V}$ doesn't satisfy the equation $x \approx y$. We need to show that $\mathcal{V}$ has a ternary term p which satisfies $p(x, x, y) \approx y$ and $p(x, y, y) \approx x$.

Let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z)$, the 3 generated free algebra for $\mathcal{V}$ and let $\alpha = \mathrm{Cg}^{\mathbf{F}}(x, y)$ and $\beta = \mathrm{Cg}^{\mathbf{F}}(y, z)$. By assumption, these congruences commute, and since $(x, z) \in \alpha \circ \beta$, it follows that there is some $b \in F$ with $(x, b) \in \beta$ and $(b, z) \in \alpha$. Since $\mathbf{F}$ is generated by $\{x, y, z\}$ then there is a ternary term p such that $b = p^{\mathbf{F}}(x, y, z)$.

To show that $p(x, x, y) \approx y$ holds in $\mathcal{V}$, let $\mathbf{A} \in \mathcal{V}$ and let $u, v \in A$. Since $\mathbf{F}$ is free for $\mathcal{V}$ over $\{x, y, z\}$ then there is a homomorphism $f : \mathbf{F} \to \mathbf{A}$ with

$f(x) = u$, $f(y) = u$ and $f(z) = v$ and so, $f(p^{\mathbf{F}}(x, y, z)) = p^{\mathbf{A}}(u, u, v)$. As (x, y) generates the congruence α, and $(x, y) \in \ker(f)$, then $\alpha \subseteq \ker(f)$. This implies that $(b, z) \in \ker(f)$ and so $v = f(z) = f(p^{\mathbf{F}}(x, y, z)) = p^{\mathbf{A}}(u, u, v)$. Since u and v are arbitrary elements of A it follows that $\mathbf{A} \models p(x, x, y) \approx y$. Similarly, it can be shown that $\mathbf{A} \models p(x, y, y) \approx x$. ∎

A term of a variety $\mathcal{V}$ for which the above equations holds is called a Mal'cev term. Using this characterization of congruence permutability, it is easy to show that, for example, the class of groups is congruence permutable. The group term $x - y + z$ is a Mal'cev term.

Not all familiar algebraic structures are congruence permutable, for example in general, lattices are not congruence permutable. In spite of this, the variety of lattices has some very nice features, and many of them are due to another property of congruence lattices.

For ϵ an equation in the language of lattices, a variety $\mathcal{V}$ is said to be congruence-ϵ if the congruence lattice of every algebra in $\mathcal{V}$ satisfies the equation ϵ.

Two important equations which we will briefly consider are modularity and distributivity. The modular equation is equivalent to the statement:

If $x \leq y$ then $x \vee (y \wedge z) \approx y \wedge (x \vee z)$.

Distributivity is equivalent to one of the equations:

$$x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z)$$

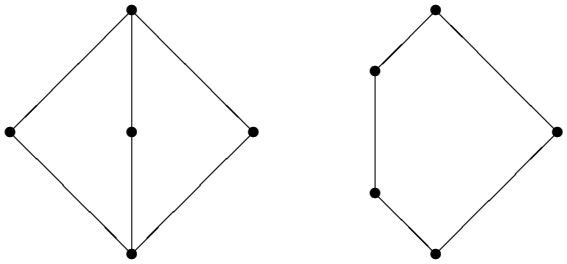
or

$$x \vee (y \wedge z) \approx (x \vee y) \wedge (x \vee z).$$

The following proposition lists some elementary facts about these equations:

Proposition 24 *Let* $\mathbf{L}$ *be a lattice.*

1. *If* $\mathbf{L}$ *is distributive then it is modular.*
2. $\mathbf{L}$ *is nonmodular if and only if the lattice* $\mathbf{N}_5$ *can be embedded into* $\mathbf{L}$.
3. $\mathbf{L}$ *is nondistributive if and only if* $\mathbf{M}_5$ *or* $\mathbf{N}_5$ *can be embedded into* $\mathbf{L}$.
4. *If* $\mathbf{A}$ *is permutable, then* $\mathrm{Con}(\mathbf{A})$ *is modular.*



$\mathbf{M}_5$ $\mathbf{N}_5$

Jónsson and Day have proved theorems similar to Mal'cev's which characterize congruence distributivity and congruence modularity in terms of the existence of terms which satisfy certain equations. Here is Jónsson's theorem on congruence distributivity:

Theorem 25 *A variety $\mathcal{V}$ is congruence distributive if and only if there are ternary terms $d_0, \ldots, d_n$ for some n such that the following equations hold in $\mathcal{V}$:*

- $d_0(x, y, z) \approx x$.
- $d_i(x, y, x) \approx x$ *for* $i \leq n$.
- $d_i(x, y, y) \approx d_{i+1}(x, y, y)$ *for all even* $i < n$.
- $d_i(x, x, y) \approx d_{i+1}(x, x, y)$ *for all odd* $i < n$.
- $d_n(x, y, z) \approx z$.

We leave it as an exercise to show that the variety of lattices is congruence distributive. Conditions having the above form are commonly referred to as Mal'cev conditions. Classifying varieties according to the Mal'cev conditions they satisfy has turned out to be a very successful classification scheme.

I would like to conclude this section by mentioning a highlight of the theory of congruence distributive varieties. The following result is a special case of a theorem of Jónsson's.

Theorem 26 *Let $\mathcal{V} = \mathsf{V}(\mathcal{K})$ be congruence distributive. If $\mathcal{K}$ is a finite set of finite algebras, then $\mathcal{V}_{SI}$ is contained in the class $HS(\mathcal{K})$.*

Note that, if $\mathcal{K}$ is a finite set of finite algebras, then up to isomorphism, so is $HS(\mathcal{K})$. So, a consequence of Jónsson's result is that a finitely generated congruence distributive variety has, up to isomorphism, a finite set of irreducible algebras, and they are all finite.

Exercises:

1. Find an infinite algebra which cannot be written as the direct product of a sequence of directly indecomposable algebras.
2. Let $f : \mathbf{A} \to \prod_{i\in I} \mathbf{A}_i$ be a homomorphism. Then $\ker(f) = \bigcap_{i\in I}\{\ker(\pi_i \circ f) : i \in I\}$.
3. $\mathbf{A}$ is subdirectly irreducible if and only if there are distinct elements a, $b \in A$ with $\mathrm{Cg}^{\mathbf{A}}(a, b)$ contained in all nonzero congruences of $\mathbf{A}$.
4. If $\mathbf{A}$ is subdirectly irreducible, then $\mathbf{A}$ is directly indecomposable.
5. Show that the variety of lattices is not congruence permutable but is congruence distributive.
6. Show that the variety of boolean algebras is both congruence permutable and congruence distributive.
7. Show that a lattice satisfies both $x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z)$ and $x \vee (y \wedge z) \approx (x \vee y) \wedge (x \vee z)$ if and only if it satisfies one of these equations.
8. Show that the modular law is equivalent to the lattice equation

$$(x \wedge y) \vee (y \wedge z) \approx y \wedge ((x \wedge y) \vee z).$$

4 Finite Algebras

In this last section, I will discuss a novel way of dealing with finite algebras which has lead to some fairly significant results over the past decade or so. The theory of finite algebras that I will describe is called tame congruence theory, whose rather cryptic name time does not permit me to explain. The rough idea of the theory is that much information about an algebra and the variety it generates can be obtained by examining the algebra locally.

I will spend the next hour talking about what is meant by the local structure of a finite algebra. To set things up, I need to make a few definitions and to alter an earlier one. For this theory, the underlying language of an algebra is not important, and so for this lecture, we will think of algebras as consisting of a nonempty universe equipped with a set of finitary operations. These operations aren't necessarily indexed and so we won't be able to speak of the type or the language of such an algebra.

Definition 27 *An (non-indexed) algebra* $\mathbf{A}$ *is a pair of the form* $\langle A, \mathcal{F} \rangle$*, where* A *is a nonempty set and* $\mathcal{F}$ *is a set of finitary operations on* A*.*

The clone of term operations on $\mathbf{A}$*, denoted* $\mathrm{Clo}(\mathbf{A})$*, is the smallest collection of operations on* A *which contains the set* $\mathcal{F}$*, the projection maps and is closed under composition. An element of* $\mathrm{Clo}(\mathbf{A})$ *is called a term operation of* $\mathbf{A}$*. The set of* n*-ary term operations is denoted by* $\mathrm{Clo}_n(\mathbf{A})$*.*

The polynomial clone of $\mathbf{A}$*, denoted* $\mathrm{Pol}(\mathbf{A})$ *is the smallest collection of operations on* A *which contains* $\mathrm{Clo}(\mathbf{A})$ *and the constant functions on* $\mathbf{A}$ *and which is closed under composition. An element of* $\mathrm{Pol}(\mathbf{A})$ *is called a polynomial of* $\mathbf{A}$*. The set of* n*-ary polynomials of* $\mathbf{A}$ *is denoted by* $\mathrm{Pol}_n(\mathbf{A})$*.*

We say that two algebras $\mathbf{A}$ and $\mathbf{B}$ which have the same universe are polynomially equivalent if $\mathrm{Pol}(\mathbf{A}) = \mathrm{Pol}(\mathbf{B})$. In some sense, this is the fundamental notion of equivalence in tame congruence theory.

As mentioned earlier, we want to consider a finite algebra locally. The small pieces of an algebra which we will deal with are called minimal sets. As we will see, certain kinds of minimal sets are very well behaved.

Definition 28 *Let* $\mathbf{A}$ *be a finite algebra. A subset* M *of* A *is called a minimal set of* $\mathbf{A}$ *if* M *is the range of some nonconstant polynomial of* $\mathbf{A}$ *and no proper subset of* M *has this property.*

$\mathbf{A}$ *is called a minimal algebra if it is finite and* A *is a minimal set of* $\mathbf{A}$*.*

It is easy to check that a finite algebra $\mathbf{A}$ is minimal if every unary polynomial of $\mathbf{A}$ is either constant or is a permutation. Also, any 2 element algebra is minimal.

The next result is due to Pálfy, and provides a classification of minimal algebras.

Theorem 29 *Let* $\mathbf{A}$ *be a minimal algebra having at least 3 elements. Then either* $\mathbf{A}$ *is essentially unary, or* $\mathbf{A}$ *is polynomially equivalent to a vector space.*

An algebra is essentially unary if each of its basic operations depends on at most one variable. Every basic operation of an essentially unary minimal algebra then must be either constant or a permutation. While the proof of Pálfy's Theorem is elementary, it would take too much time to present here.

Corollary 30 *Let* $\mathbf{A}$ *be a minimal algebra. Then* $\mathbf{A}$ *is polynomially equivalent to one of the following 5 kinds of algebras:*

1. *a unary algebra whose basic operations are all permutations*
2. *a vector space*
3. *the 2 element boolean algebra*
4. *the 2 element lattice*
5. *the 2 element semi-lattice*

PROOF. A proof of this amounts to showing that if $\mathbf{A}$ has 2 elements, then it is polynomially equivalent to an algebra in the above list, since by Pálfy's theorem, all other algebras are either unary or vector spaces (up to polynomial equivalence). ∎

Using the corollary, we can assign a type to each minimal algebra. We set the type of $\mathbf{A}$ to be i, if $\mathbf{A}$ is polynomially equivalent to an algebra which occurs in the ith element of the above list. We denote the type of $\mathbf{A}$ by $\mathrm{typ}\,(\mathbf{A})$.

Subuniverses of an algebra $\mathbf{A}$ are subsets of A which are, in some sense, compatible with the basic operations of $\mathbf{A}$. By definition, they are the subsets which are closed under the basic operations. In general, as subuniverses of an algebra aren't closed under polynomial operations, they will not be adequate vehicles for studying the local structure of a finite algebra.

Definition 31 *A subset* U *of an algebra* $\mathbf{A}$ *is called a neighbourhood of* $\mathbf{A}$ *if* $U = e(A)$ *for some idempotent polynomial* e *of* $\mathbf{A}$. *e idempotent means that* $e(e(x)) = x$ *for all* $x \in A$.

For S *a subset of* A, *the localization of* $\mathbf{A}$ *to* S, *denoted by* $\mathbf{A}|_S$ *is the algebra*

$$\langle S, \{f(\bar{x})|_S \,:\, f \in \mathrm{Pol}\,(\mathbf{A}) \text{ and } S \text{ is closed under } f\}\rangle.$$

Note that even if the original algebra $\mathbf{A}$ has an associated language, the localizations do not. If we localize $\mathbf{A}$ to a minimal set U, it is the case that $\mathbf{A}|_U$ is a minimal algebra and so can be assigned one of the 5 types defined above.

Localizing an algebra $\mathbf{A}$ to a neighbourhood preserves the local polynomial structure of the algebra, since if N is a neighbourhood of $\mathbf{A}$, $\bar{n} \in N$ and p is a polynomial of $\mathbf{A}$ with $p(\bar{n}) \in N$, then there is a polynomial of $\mathbf{A}|_N$ which maps the tuple $\bar{n}$ to $p(\bar{n})$. This property does not hold in general if we localize to arbitrary subsets of an algebra.

A crucial result of the theory shows that under certain conditions the minimal sets of an algebra are well behaved. What I will show is that if the algebra $\mathbf{A}$ is simple, then the minimal sets of $\mathbf{A}$ are very well behaved (tame). An algebra is simple if it has exactly two congruences, 0_A and 1_A.

Proposition 32 *Let $\mathbf{A}$ be a finite simple algebra and let U be a minimal set of $\mathbf{A}$. Then U is a neighbourhood of $\mathbf{A}$.*

PROOF. Let K be the set of unary polynomials of $\mathbf{A}$ whose range is contained in U and let $\mu = \{(x, y) \in A^2 : f(x) = f(y) \text{ for all } f \in K\}$. I claim that μ is a congruence of $\mathbf{A}$, and so by the simplicity of $\mathbf{A}$ is either 0_A or 1_A.

Since U is a minimal set then there is a nonconstant polynomial f of $\mathbf{A}$ whose range is equal to U. Using f, it is easy to show that $\mu \neq 1_A$ and so $\mu = 0_A$ since there are distinct a and b with $f(a) \neq f(b)$. Then $(f(a), f(b)) \notin \mu$ and so there is some $g \in K$ with $gf(a) \neq gf(b)$. If we consider the polynomial $p(x) = gf(x)$ then we have that the range of p is contained in U and p is not constant. By the minimality of U it follows that $p(A) = U$. Since $f(A) = U$ we conclude that $g(U) = U$ and by taking a suitable iterate of g, we arrive at a polynomial e with range U and such that $e(x) = x$ for all $x \in U$. Then e is idempotent, and so U is a neighbourhood of $\mathbf{A}$. ∎

Two subsets U and V of a finite algebra $\mathbf{A}$ are said to be polynomially isomorphic if there are polynomials f and g of $\mathbf{A}$ with $gf(u) = u$ and $fg(v) = v$ for all $u \in U$ and $v \in V$.

Theorem 33 *Let $\mathbf{A}$ be a finite simple algebra. Then*

1. *If U and V are minimal sets then U and V are polynomially isomorphic.*

2. *If U is a minimal set and f is a unary polynomial with $f|_U$ nonconstant then $f(U)$ is a minimal set.*

3. *If U is a minimal set and a and b are distinct elements of A then there is a polynomial f of $\mathbf{A}$ with range equal to U and with $f(a) \neq f(b)$.*

4. *If a and b are elements of A then they can be connected by a chain of overlapping minimal sets.*

PROOF. I will prove only part of this theorem. For part 3, let U be minimal and let e be an idempotent polynomial with range U. Let

$$\theta = \{(x, y) \in A^2 : ef(x) = ef(y) \text{ for all unary polynomials } f\}.$$

Then θ is a congruence of $\mathbf{A}$ and so is either 0_A or 1_A. Since any pair from U is not in θ it follows that $\theta \neq 1_A$ and so $\theta = 0_A$.

If $a \neq b$ in A then $(a, b) \notin \theta$ and so there is a polynomial f with $ef(a) \neq ef(b)$. But then the polynomial ef has range equal to U (by minimality) and separates a and b.

Assuming that 2 holds we can prove 4 by showing that the transitive closure of the relation

$$\gamma = \{(g(x), g(y)) \in A^2 : \ (x, y) \in U^2 \text{ and } g \text{ is a polynomial}\}$$

is a congruence. If it is a congruence then it is not 0_A and so must be 1_A. This implies that any pair of elements from A are in γ and so can be connected up by pairs of the form $(g(x), g(y))$ for some polynomial g which is nonconstant on U and x, $y \in U$. By 2 we know that $g(U)$ is minimal and so we get that any pair can be connected by a chain of overlapping minimal sets.

We need only show that γ is reflexive, symmetric and compatible with the unary polynomials of $\mathbf{A}$ to conclude that its transitive closure is a congruence. We leave this as an exercise. ∎

This theorem shows that if $\mathbf{A}$ is a finite simple algebra, then it is populated by a number of isomorphic minimal algebras. These minimal algebras cover the entire universe of $\mathbf{A}$ and are such that the set of unary polynomials of $\mathbf{A}$ which map into a given minimal set separate the points of A. Since all of the minimal sets of $\mathbf{A}$ have the same type, then we can assign this type to the algebra $\mathbf{A}$.

The next step in the development of a local theory of finite algebras is to relativize the above to a pair of congruences $\alpha \prec \beta$ on a finite algebra $\mathbf{A}$.

The relation $\prec$ holds between two congruences α and β if and only if $\alpha < \beta$ and there is no congruence of $\mathbf{A}$ which lies strictly between α and β.

If we consider the algebra $\mathbf{A}' = \mathbf{A}/\alpha$, then the image of β under the quotient map is a congruence β' which covers the congruence $0_{\mathbf{A}'}$. If C is a nontrivial congruence class of β' then the induced algebra $\mathbf{A}'|_C$ is a finite simple algebra.

We have just seen that a type can be assigned to any simple algebra, and so the algebra $\mathbf{A}'|_C$ has some type i. It is the case that if D is any other nontrivial congruence class of β' then the type of $\mathbf{A}'|_D$ is the same as that of $\mathbf{A}'|_C$. This allows us to assign a type to the pair (α, β). We define typ (α, β) to be the type of the simple algebra $\mathbf{A}'|_C$.

So, to assert that the type of the pair (α, β) is 2 means that modulo α, the β congruence classes behave locally as vector spaces. The fact that this sort of local uniform behaviour exists for all finite algebras has far reaching consequences. I will end this section by listing a few highlights of the theory.

Definition 34 *Let* $\mathbf{A}$ *be a finite algebra and* $\mathcal{K}$ *a class of similar algebras. The type set of* $\mathbf{A}$*, denoted by* typ $(\mathbf{A})$ *is the set*

$$\{\text{typ}\,(\alpha, \beta) \,:\, \alpha \prec \beta \text{ in } \text{Con}\,(\mathbf{A})\}.$$

The type set of the class $\mathcal{K}$*, denoted by* typ $(\mathcal{K})$ *is the set*

$$\bigcup\{\text{typ}\,(\mathbf{A}) \,:\, \mathbf{A} \in \mathcal{K} \text{ and } \mathbf{A} \text{ finite}\}.$$

Since there are only 5 types, then there are at most 32 possible typesets for algebras and varieties.

Hobby and McKenzie established a strong connection between omitting certain types and the satisfaction of nontrivial congruence identities. Combining their result with a recent theorem of Kearnes provides:

Theorem 35 *Let* $\mathcal{V}$ *be a finitely generated variety. Then* $\mathcal{V}$ *satisfies a nontrivial congruence identity if and only if* typ $(\mathcal{V}) \subseteq \{2, 3, 4\}$.

So, the congruence lattices of the algebras in a finitely generated variety will satisfy some equation which fails to hold in all lattices if and only if the local behaviour of the finite algebras in the variety excludes the unary and semi-lattice types.

An early application of tame congruence theory was to the study of the class of subdirectly irreducible algebras in a finitely generated variety. A variety $\mathcal{V}$ is said to be residually small if there is some cardinal κ such that each subdirectly irreducible in $\mathcal{V}$ has size bounded by κ. Hobby and McKenzie proved the following:

Theorem 36 *Let $\mathcal{V}$ be a finitely generated variety which is residually small. If* typ $(\mathcal{V}) \subseteq \{2, 3, 4\}$ *then $\mathcal{V}$ is congruence modular.*

Others successes in the study of residual smallness have been obtained using tame congruence theory, and it seems possible that a characterization of residual smallness for finitely generated varieties may be expressible in the language of tame congruence theory.

A variety $\mathcal{V}$ is said to be decidable if the set of all first order sentences which are satisfied by $\mathcal{V}$ is recursive. So, decidability of $\mathcal{V}$ means that there is an algorithmic way to settle which first order sentences in the language of $\mathcal{V}$ are satisfied by all members of $\mathcal{V}$.

Burris and McKenzie provided a characterization of finitely generated, decidable, congruence modular varieties using a generalization of the commutator operation for groups. Using tame congruence theory, their theorem was extended to arbitrary finitely generated varieties by McKenzie and Valeriote. A precursor to this theorem appeared in the book by Hobby and McKenzie:

Theorem 37 *Let $\mathcal{V}$ be a finitely generated decidable variety. Then* typ $(\mathcal{V}) \subseteq \{1, 2, 3\}$.

Exercises

1. Show that $p(\bar{x})$ is a polynomial of an algebra $\mathbf{A}$ if and only if there is some term operation $t(\bar{x}, \bar{y})$ of $\mathbf{A}$ and some elements $\bar{a}$ from A with $p(\bar{x}) = t(\bar{x}, \bar{a})$.

2. Show that an equivalence relation on a set A is a congruence of the algebra $\mathbf{A}$ if and only if it is compatible with the unary polynomials of $\mathbf{A}$.

3. Show that the relation μ in the proof of Proposition 32 is a congruence of $\mathbf{A}$.

4. Show that the 2 element boolean algebra on $\{0,1\}$ is polynomially equivalent to the algebra $\mathbf{A} = \langle \{0,1\}; d(x,y,z) \rangle$, where

$$d(x,y,z) = \begin{cases} z, & \text{if } x = y \\ x, & \text{otherwise} \end{cases}$$

5. Show that a vector space is a minimal algebra. The language of a vector space over the field $\mathbb{F}$ consists of the language of abelian groups, along with the set $\{f_\lambda : \lambda \in \mathbb{F}\}$ of unary operation symbols. The unary symbol f_λ is interpreted as multiplication by the scalar λ.

6. Show that a function $f : A \to A$ is idempotent if and only if its restriction to its range is the identity map.

7. Determine the 2 element neighbourhoods of the ring $\mathbb{Z}_4$ and determine their types as minimal algebras.

8. Let N be a neighbourhood of the algebra $\mathbf{A}$, let $\bar{n}$ be a tuple from N and p a polynomial of $\mathbf{A}$ with $p(\bar{n}) \in N$. Show that there is a polynomial of $\mathbf{A}|_N$ which maps $\bar{n}$ to $p(\bar{n})$. Hint: Let e be an idempotent polynomial with range N and consider the function ep.

9. Show that if U is a minimal set of the finite algebra $\mathbf{A}$ then the algebra $\mathbf{A}|_U$ is a minimal algebra.

10. Let A be finite, and $f : A \to A$. There is some $n > 0$ such that f^n is an idempotent map.

11. Prove that the transitive closure of γ from Theorem 33 is a congruence of $\mathbf{A}$.

12. Let $\mathbf{A}$ be a finite algebra and α a minimal nonzero congruence. Show that if C is a nontrivial congruence class of α then $\mathbf{A}|_C$ is a simple algebra.

5 References

For further reading on this subject, I recommend the following books:

1. *A Course in Universal Algebra*, S. Burris and H.P. Sankappanavar, Springer-Verlag, 1981.

2. *Algebras, Lattices, Varieties, Volume I*, R. McKenzie, G. McNulty, and W. Taylor, Wadsworth & Brooks/Cole, 1987.

3. *The Structure of Finite Algebras*, D. Hobby and R. McKenzie, Contemporary Mathematics, Volume 76, 1988.

4. *Algebraic Model Theory*, Edited by B. Hart, A. Lachlan, and M. Valeriote, NATO ASI Series Volume 496, Kluwer, 1997.