Algebras, lattices, varieties

Charlotte Aten

CU Boulder

CU Boulder Graduate Algebra and Logic Seminar
2024 October 4

Commutator theory

Ralph Freese and Ralph McKenzie. *Commutator theory for congruence modular varieties*. Vol. 125. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1987, pp. iv+227. ISBN: 0-521-34832-3

- We'll be working through this text on commutator theory.
- I'll briefly give the idea of what it is commutator theory generalizes, and then talk at some length about the setting in which that generalization occurs.

Commutator theory

- Given a group $\mathbf{G}$, we can obtain a lot of information by looking at its subgroups, and in particular its normal subgroups.
- Even more information may be gained by studying the *commutator* of two normal subgroups.
- Given normal subgroups $\mathbf{M}$ and $\mathbf{N}$, their commutator $[\mathbf{M}, \mathbf{N}]$ is the normal subgroup of $\mathbf{G}$ which is generated by all elements of the form $m^{-1}n^{-1}mn$ where $m \in M$ and $n \in N$.

Commutator theory

- We can think of the commutator as an operation on the collection of normal subgroups of a group.
- It has a number of nice properties, which aid in its calculation.
- Since the commutator has been so useful in the study of groups, we would like to generalize it to other kinds of algebraic structures, such as rings or Boolean algebras.

Some history

- Universal algebra (or general algebra) is the appropriate general setting for discussing algebraic structures.
- Alfred North Whitehead's 1898 "A Treatise on Universal Algebra" noted the commonalities between groups and Boolean algebras.
- Richard Dedekind did some early work on lattices of subgroups around 1900.

Some history

- Lattice theory became an established discipline in its own right during the 1930s and 1940s.
- Garrett Birkhoff published "On the Structure of Abstract Algebras" in 1935, establishing universal algebra as a branch of mathematics.
- Birkhoff used lattice-theoretic ideas in his paper. In 1940 he published a book on lattice theory.
- Øystein Ore referred to lattices as "structures" and led a short-lived program during the 1930s where lattices were hailed as the single unifying concept for all of mathematics.
- During this period Saunders Mac Lane studied algebra under Ore's advisement. Mac Lane went on to become one of the founders of category theory.

Algebras

- Let $\omega = \{0, 1, 2, \dots\}$ be the set of natural numbers.
- An *operation* on a set A is a function $f\colon A^n \to A$.
- The *arity* of $f\colon A^n \to A$ is n.
- Given a sequence of operation symbols F_i for $i \in I$, we say that a function $\rho\colon I \to \omega$ is a *signature*.

Algebras

- An *algebra (of signature ρ)* consists of a set A along with a collection of operations $\overline{F}_i$ on A, where $\overline{F}_i$ has arity $\rho(i)$.
- We often denote such an algebra by

$$\mathbf{A} = \langle A, \{\overline{F}_i\}_{i \in I} \rangle$$

or

$$\mathbf{A} = \langle A, \{F_i^{\mathbf{A}}\}_{i \in I} \rangle.$$

Terms and polynomials

- There are two concepts which generalize polynomials from elementary algebra.
- Given a signature ρ and a set of variables $\{v_i\}_i \in \omega$, the *terms* for ρ constitute the smallest set T containing the v_i such that if $t_1, \ldots, t_n \in T$ and F_i is an operation symbol with $\rho(i) = n$, then $F_i(t_1, \ldots, t_n) \in T$.

Terms and polynomials

- For each term in T and each algebra $\mathbf{A}$ of signature ρ, we have a *term operation* $t^{\mathbf{A}}$ obtained by interpreting t in the context of $\mathbf{A}$ in the natural way.
- The *clone of term operations* for an algebra $\mathbf{A}$ is the smallest set of operations on A which contains all the basic operations of $\mathbf{A}$, is closed under composition, and which contains all the coordinate projections.

Terms and polynomials

- Similarly, the *clone of polynomial operations* for an algebra $\mathbf{A}$ is the smallest set of operations on A which contains all the basic operations of $\mathbf{A}$, is closed under composition, which contains all the coordinate projections, and which includes all the 0-ary constant operations on A.

Identities

- An *identity* (or *(universally quantified) equation*) is a formula

$$(\forall v_0, \ldots, v_{n-1})(s(v_0, \ldots, v_{n-1}) = t(v_0, \ldots, v_{n-1}))$$

  where $s, t \in T$ for some set of terms T.
- We abbreviate this by $s \approx t$.
- We write $\mathbf{A} \models s \approx t$ when

$$(\forall a_0, \ldots, a_{n-1} \in A)(s^{\mathbf{A}}(a_0, \ldots, a_{n-1}) = t^{\mathbf{A}}(a_0, \ldots, a_{n-1})).$$

Identities

- Given a class of algebras $\mathcal{K}$, we write $\mathcal{K} \models s \approx t$ when $\mathbf{A} \models s \approx t$ for each $\mathbf{A} \in \mathcal{K}$.
- Given a set of equations Σ in a signature ρ, we write

$$\mathrm{Mod}(\Sigma) = \{\, \mathbf{A} \mid \mathbf{A} \text{ has signature } \rho \text{ and } (\forall \epsilon \in \Sigma)(\mathbf{A} \models \epsilon) \,\}.$$

- Classes of the form $\mathrm{Mod}(\Sigma)$ are called *varieties* (or *equational classes*).

HSP Theorem

- Given a class of algebras $\mathcal{K}$, we write $\mathbf{H}(\mathcal{K})$, $\mathbf{S}(\mathcal{K})$, and $\mathbf{P}(\mathcal{K})$ to denote the classes of (isomorphic copies of) homomorphic images, subalgebras, and products, respectively, of algebras from $\mathcal{K}$.

HSP Theorem

Theorem (HSP Theorem (Birkhoff, 1935))

A class of similar algebras $\mathcal{V}$ is a variety if and only if $\mathcal{V}$ is closed under forming homomorphic images, subalgebras, and products.

- That is, $\mathcal{V}$ is a variety exactly when $\mathcal{V} = \mathbf{HSP}(\mathcal{V})$.

Homomorphisms

Definition (Homomorphism)

Given algebras $\mathbf{A} = \langle A, \{F_i^{\mathbf{A}}\}_{i \in I} \rangle$ and $\mathbf{B} = \langle B, \{F_i^{\mathbf{B}}\}_{i \in I} \rangle$ of the same similarity type $\rho \colon I \to \omega$ we say that a function $h \colon A \to B$ is a *homomorphism* from $\mathbf{A}$ to $\mathbf{B}$ when for each $i \in I$ and all $a_1, \ldots, a_{\rho(i)} \in A$ we have that

$$h(F_i^{\mathbf{A}}(a_1, \ldots, a_{\rho(i)})) = F_i^{\mathbf{B}}(h(a_1), \ldots, h(a_{\rho(i)})).$$

Kernels

To each function we associate a binary relation as follows.

Definition (Kernel)

Given a function $f\colon A \to B$ the *kernel* of f is the binary relation

$$\operatorname{Ker}(f) \coloneqq \left\{ (x, y) \in A^2 \mid f(x) = f(y) \right\}.$$

We always have that $\operatorname{Ker}(f)$ is an equivalence relation on A.

Congruences

It turns out that the kernels of homomorphisms of algebras always have additional structure.

Definition (Substitution property, congruence)

Given an algebra $\mathbf{A}$ and a binary relation θ on A we say that

1. θ has the *substitution property* (with respect to $\mathbf{A}$) when for each n-ary basic operation f of $\mathbf{A}$ and all $x_1, \ldots, x_n, y_1, \ldots, y_n \in A$ such that $x_i \,\theta\, y_i$ for each $i \in \{1, 2, \ldots, n\}$ we have that $f(x_1, \ldots, x_n) \,\theta\, f(y_1, \ldots, y_n)$ and
2. θ is a *congruence* of $\mathbf{A}$ when θ has the substitution property and is an equivalence relation on A.

Congruences

- Using the definition of a homomorphism we see that the kernel of each homomorphism has the substitution property and is thus a congruence.
- Is every congruence the kernel of a homomorphism?

Congruences

- The answer is yes.
- We can show this by turning the map $q_\theta \colon A \to A/\theta$ into a homomorphism.
- In order to do that we need to define an algebra $\mathbf{A}/\theta$ with universe A/θ such that $q_\theta \colon \mathbf{A} \to \mathbf{A}/\theta$ becomes a homomorphism.
- Given a basic n-ary operation symbol f and some $a_1, \ldots, a_n \in A$ we need that

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

- This means we require

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

  which we take as our definition of $f^{\mathbf{A}/\theta}$.

Congruences

- Congruences generalize normal subgroups for groups and two-sided ideals for rings.
- For each normal subgroup **N** of a group **G** we have that the relation

$$\{ (x, y) \in G \mid x^{-1}y \in N \}$$

  is a congruence on **G**.
- For each two-sided ideal I of a ring **R** we have that the relation

$$\{ (x, y) \in R \mid x - y \in I \}$$

  is a congruence on **R**.

Congruences

- The congruences of an algebra $\mathbf{A}$ form a lattice under the inclusion ordering, which we denote by $\mathbf{Con}(\mathbf{A})$.
- An algebra is *simple* when it has exactly two congruences, and *subdirectly irreducible* when its congruence lattice has exactly one atom which lies below every nonzero congruence.
- Simple groups include $\mathbb{Z}/p\mathbb{Z}$ for a prime p or the alternating groups $\mathbf{A}_n$ for $n \geq 5$.
- Subdirectly irreducible groups include the Abelian p-groups $\mathbb{Z}/p^n\mathbb{Z}$ and the Prüfer groups $\mathbb{Z}(p^\infty)$.

Congruences

- Another early result of Birkhoff is that every algebra $\mathbf{A}$ is isomorphic to a subalgebra $\mathbf{C}$ of a product $\prod_{i \in I} \mathbf{A}_i$ where
  1. each $\mathbf{A}_i$ is subdirectly irreducible,
  2. each $\mathbf{A}_i$ is a homomorphic image of $\mathbf{A}$, and
  3. the projection of $\mathbf{C}$ onto coordinate i yields all of A_i.
- Such an algebra $\mathbf{C}$ is said to be a *subdirect product* of the $\mathbf{A}_i$.

Congruences

- We say that two congruences $\theta, \psi \in \mathbf{Con}(\mathbf{A})$ *commute* when $\theta \circ \psi = \psi \circ \theta$.
- This necessarily means that $\theta \circ \psi = \theta \vee \psi$.
- An algebra $\mathbf{A}$ is *permutable* when every pair of congruences of $\mathbf{A}$ commute.
- A variety is *permutable* when each algebra in that variety is permutable.

Congruences

Theorem (Mal'cev)

A variety $\mathbf{V}$ *is permutable if and only if there is a term* $p(x, y, z)$ *in the language of* $\mathcal{V}$ *such that*

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

holds in $\mathcal{V}$.

- Such a term is called a *Mal'cev term*.
- For groups, we can take $p(x, y, z) = xy^{-1}z$.

Free algebras

- For each variety $\mathcal{V}$ and each set X, there exists a *free algebra* $\mathbf{F} \in \mathcal{V}$ where
  1. $X \subset F$,
  2. X generates $\mathbf{F}$, and
  3. for each algebra $\mathbf{A} \in \mathcal{V}$ and each function $f\colon X \to A$ we have that there exists a unique homomorphism $\hat{f}\colon \mathbf{F} \to \mathbf{A}$ with $\hat{f}(x) = f(x)$ for each $x \in X$.

Free algebras

- We often use notation such as $\mathbf{F}(X)$ or $\mathbf{F}_{\mathcal{V}}(X)$ to indicate the free algebra described previously.
- If we write Ab for the variety of Abelian groups, we have free algebras like $\mathbf{F}_{\mathsf{Ab}}$.

Free algebras

- Every algebra is a quotient of a free algebra.
- Every variety has $\mathcal{V} = \mathbf{HSP}(\mathbf{F}_{\mathcal{V}}(X))$ where $X = \{x_i\}_{i \in \omega}$.

Distributive lattices

Definition (Distributive lattice)

We say that a lattice $\mathbf{L}$ is *distributive* when $\mathbf{L}$ satisfies

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

- We actually always have

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

  so if we want to check that a lattice is distributive it suffices to show that

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

Distributive lattices

- An algebra $\mathbf{A}$ is *distributive* when $\mathbf{Con}(\mathbf{A})$ is distributive.
- A variety is *distributive* when each of its members is distributive.
- The variety of lattices is distributive.
- The variety of (Abelian) groups is not distributive. Consider the Klein 4-group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Distributive lattices

Theorem (Jónsson)

A variety $\mathcal{V}$ 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

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

Modular lattices

Definition (Modular lattice)

We say that a lattice $\mathbf{L}$ is *modular* when for all $y \in L$ we have that

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

- We actually always have that $z \leq x$ implies

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

so if we want to check that a lattice is modular it suffices to show that $z \leq x$ implies

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

Modular lattices

- An algebra $\mathbf{A}$ is *modular* when $\mathbf{Con}(\mathbf{A})$ is modular.
- A variety is *modular* when each of its members is modular.
- Every distributive lattice is modular.
- The variety of groups is modular.

Modular lattices

- We are going to study the generalization of the commutator operation on normal subgroups to a commutator operation on the congruence lattices of algebras in congruence modular varieties.

Some textbooks

- Clifford Bergman. *Universal Algebra: Fundamentals and Selected Topics*. Chapman and Hall/CRC, 2011. ISBN: 978-1-4398-5129-6
- George M. Bergman. *An invitation to general algebra and universal constructions*. Second. Universitext. Springer, Cham, 2015, pp. x+572. ISBN: 978-3-319-11477-4; 978-3-319-11478-1. DOI: 10.1007/978-3-319-11478-1
- Jonathan D. H. Smith and Anna B. Romanowska. *Post-Modern Algebra*. 1st ed. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley-Interscience, 1999. ISBN: 0471127388,9780471127383