Universal algebra and lattice theory
Week 2
Congruences and quotients

Charlotte Aten

2020 September 10

Today's topics

- Relations
- Kernels
- Congruences
- Quotient algebras
- Kernels and groups
- The Homomorphism Theorem
- Generating congruences

Relations

- Given a set A and some $n \in \mathbb{N}$ we refer to a subset of A^n as a *relation* on A of *arity* n (or as an n-*ary relation* on A).
- In this talk we will focus on relations of arity 2, which are also called *binary relations*. We'll see more of the general relations on another day.
- There are a number of ways of getting new binary relations from old ones.
- Given binary relations θ and ψ on a set A we have that $\theta \cap \psi$ and $\theta \cup \psi$ are also binary relations on A.

Relations

- For binary relations θ and ψ on A we define the *relative product* of θ and ψ by

$$\theta \circ \psi := \{ (x, z) \in A^2 \mid (\exists y \in A)((x, y) \in \theta \text{ and } (y, z) \in \psi) \} .$$

- Note that while the relative product is similar to function composition, the order of the arguments is reversed.
- We also have a unary operation on binary relations on A. Given $\theta \subset A^2$ we define the *converse* of θ by

$$\theta^{\smile} = \{ (y, x) \in A^2 \mid (x, y) \in \theta \} .$$

- We often write $x \; \theta \; y$ instead of $(x, y) \in \theta$.

Relations

We are often concerned with the following type of binary relation.

Definition (Equivalence relation)

We say that a binary relation θ on a set A is an *equivalence relation* when for all $x, y, z \in A$ we have that

1. (reflexivity) $x \; \theta \; x$,
2. (symmetry) $x \; \theta \; y$ implies that $y \; \theta \; x$, and
3. (transitivity) if $x \; \theta \; y$ and $y \; \theta \; z$ then $x \; \theta \; z$.

Relations

- We denote by $\mathrm{Eq}(A)$ the set of all equivalence relations on the set A.
- We define $0_A := \{ (x, x) \in A^2 \mid x \in A \}$ and $1_A := A^2$. We have that 0_A and 1_A are equivalence relations on A.
- For any $\theta \in \mathrm{Eq}(A)$ we have that $0_A \subset \theta \subset 1_A$.
- When θ is an equivalence relation we may use the special notation

  $$x \equiv y \pmod{\theta} \text{ or } x \equiv_\theta y$$

  rather than $x \; \theta \; y$ or $(x, y) \in \theta$.

Relations

Now that we have some more notation we can rewrite our definition of an equivalence relation a little more symbolically.

Definition (Equivalence relation)

We say that a binary relation θ on a set A is an *equivalence relation* when

1. (reflexivity) $0_A \subset \theta$,
2. (symmetry) $\theta^{\smile} \subset \theta$, and
3. (transitivity) $\theta \circ \theta \subset \theta$.

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

$$\ker(f) := \{\, (x, y) \in A^2 \mid f(x) = f(y) \,\}\,.$$

We always have that $\ker(f)$ is an equivalence relation on A.
Is every equivalence relation the kernel of a function?

Kernels

- The answer is yes.
- Given an equivalence relation θ on a set A and some $a \in A$ we define the *equivalence class* of a modulo θ to be

$$a/\theta := \{\, x \in A \mid a \ \theta \ x \,\}.$$

- We have that $\{\, a/\theta \mid a \in A \,\}$ is a partition of A, which is another way you may have seen to think about equivalence relations on A.
- We refer to $A/\theta := \{\, a/\theta \mid a \in A \,\}$ as the *quotient* of A by θ.
- Define $q_\theta \colon A \to A/\theta$ by $q_\theta(a) := a/\theta$. We find that $\theta = \ker(q_\theta)$.

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

- The kernel of any homomorphism (indeed, any function) is an equivalence relation.
- 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 again 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 $f^{\mathbf{A}/\theta}$.

Quotient algebras

The algebras $\mathbf{A}/\theta$ given by the preceding construction are going to be very important to us, so we name them.

Definition (Quotient algebra)

Given an algebra $\mathbf{A}$ and a congruence θ of $\mathbf{A}$ the *quotient algebra* of $\mathbf{A}$ by θ is the algebra $\mathbf{A}/\theta$ similar to $\mathbf{A}$ with universe A/θ where for each basic n-ary operation symbol f and all $a_1, \ldots, a_n \in A$ we define

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

Quotient algebras

- We always have that 0_A and 1_A are congruences for any algebra $\mathbf{A}$.
- Moreover, $\mathbf{A}/0_A \cong \mathbf{A}$ and $\mathbf{A}/1_A$ is a trivial algebra.
- Many algebras have congruences other than 0 and 1.
- Trivial algebras have only one congruence, which is both 0 and 1.
- A nontrivial algebra with only the two congruences 0 and 1 is called *simple*.
- Simple algebras are special cases of more general «building blocks» for all algebraic structures. We'll come back to them later.

Kernels and groups

The preceding definitions of a kernel and a congruence do actually generalize those of a kernel and normal subgroup in group theory.

Theorem

Take $\mathbf{G}$ to be a group.

1. *Given a normal subgroup $\mathbf{N}$ of $\mathbf{G}$ we have that*

$$\theta_{\mathbf{N}} := \{\, (x, y) \in G^2 \mid y^{-1}x \in N \,\}$$

   is a congruence of $\mathbf{G}$. For each $x \in G$ we have that $xN = x/\theta_{\mathbf{N}}$.

2. *Given a congruence θ of $\mathbf{G}$ we have that e/θ is (the universe of) a normal subgroup of $\mathbf{G}$.*
3. *The map $\mathbf{N} \mapsto \theta_{\mathbf{N}}$ is an order-preserving bijection from normal subgroups of $\mathbf{G}$ to congruences of $\mathbf{G}$.*

The Homomorphism Theorem

We can finally start formulating the Isomorphism Theorems for all algebras.

Theorem (The Homomorphism Theorem)

Given a homomorphism $h\colon \mathbf{A} \to \mathbf{B}$ *with kernel* θ *we have that there exists a unique embedding* $\bar{h}\colon \mathbf{A}/\theta \to \mathbf{B}$ *such that* $\bar{h} \circ q_\theta = h$. *When* h *is surjective we have that* $\bar{h}$ *is an isomorphism.*

$$\begin{tikzcd}
\mathbf{A} \arrow[r, "h"] \arrow[d, two heads, "q_\theta"'] & \mathbf{B} \\
\mathbf{A}/\theta \arrow[ur, hook, dotted, "\bar{h}"'] &
\end{tikzcd}$$

Generating congruences

Just as we discussed the subuniverse generated by a set previously, we can also examine congruences generated by a set.

Proposition

Given an algebra $\mathbf{A}$ *and a collection* Θ *of congruences of* $\mathbf{A}$ *we have that* $\bigcap \Theta$ *is a congruence of* $\mathbf{A}$.

The proof of this statement is quite similar to that of the corresponding proposition for subuniverses.

Generating congruences

We can consider the smallest congruence of $\mathbf{A}$ containing a set of pairs. We denote by $\mathrm{Con}(\mathbf{A})$ the set of all congruences of $\mathbf{A}$.

Definition (Congruence generated by a set)

Given an algebra $\mathbf{A}$ and $\nu \subset A^2$ we define the congruence of $\mathbf{A}$ generated by ν to be

$$\mathrm{Cg}^{\mathbf{A}}(\nu) := \bigcap \{\, \theta \in \mathrm{Con}(\mathbf{A}) \mid \nu \subset \theta \,\}\,.$$

The previous proposition tells us that $\mathrm{Cg}(\nu)$ is indeed a congruence of $\mathbf{A}$. Note that $\mathrm{Cg}(\nu)$ must contain ν.

Generating congruences

- Instead of taking this «top-down» viewpoint using intersections we can give a «bottom-up» description of $\mathrm{Sg}^{\mathbf{A}}(X)$ by taking unions.
- It will be very convenient to have some more notation before we proceed. We will write $\mathbf{a} \in A^n$ to indicate that $\mathbf{a} = (a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in A$.
- Given some $\nu \subset A^2$ we write $\mathbf{a} \ \nu \ \mathbf{b}$ to indicate that $a_i \ \nu \ b_i$ for each $i \in \{1, 2, \ldots, n\}$.
- Note that we can reformulate the substitution property as saying that $\mathbf{a} \ \theta \ \mathbf{b}$ implies that $f(\mathbf{a}) \ \theta \ f(\mathbf{b})$ for any tuples $\mathbf{a}$ and $\mathbf{b}$ and any basic operation f.

Generating congruences

We can now give our «bottom-up» description of $\mathrm{Cg}^{\mathbf{A}}(\nu)$.

Theorem

Given an algebra $\mathbf{A} := (A, F)$ *and* $\nu \subset A^2$ *we define* $\nu_0 := \nu \cup \nu^{\smile} \cup 0_A$ *and for each* $n \in \mathbb{N}$ *we define* ν_n *to be*

$$(\nu_{n-1} \circ \nu_{n-1}) \cup \left\{ (f(\mathbf{a}), f(\mathbf{b})) \in A^2 \;\middle|\; f \in F \text{ and } \mathbf{a} \;\nu_{n-1}\; \mathbf{b} \right\}.$$

We have that $\mathrm{Cg}^{\mathbf{A}}(\nu) = \bigcup_{n \in \mathbb{W}} \nu_n$.

Generating congruences

- Congruences which can be written as $\mathrm{Cg}(\nu)$ where ν is finite are called *finitely generated*.
- We will be particularly interested in congruences of the form $\mathrm{Cg}(\{(x, y)\})$, which are called *principal congruences*.
- We usually indicate principal congruences by $\mathrm{Cg}(x, y)$ rather than $\mathrm{Cg}(\{(x, y)\})$.