Universal algebra and lattice theory
Week 1
Examples of algebras

Charlotte Aten

2020 September 3

Today's topics

- Quick review of the definition of an algebra
- Magmas
- Semigroups
- Monoids
- Groups
- Rings
- Modules
- Quasigroups
- Semilattices
- Lattices
- n-ary magmas

Definition of an algebra

Operations are rules for combining elements of a set together to obtain another element of the same set.

Definition (Operation, arity)

Given a set A and some $n \in \mathbb{W}$ we refer to a function $f\colon A^n \to A$ as an *n-ary operation* on A. When f is an n-ary operation on A we say that f has *arity* n.

Algebras are sets with an indexed sequence of operations.

Definition (Algebra)

An *algebra* (A, F) consists of a set A and a sequence $F = \{f_i\}_{i \in I}$ of operations on A, indexed by some set I.

Magmas

- An algebra $\mathbf{A} := (A, f)$ with a single binary operation is called a *magma*.
- This is the Bourbaki terminology. These algebras are also known as *groupoids* and *binars*, but the term «groupoid» has also become attached to a different concept in category theory.
- When the set A is finite we can represent the basic operation $f\colon A^2 \to A$ as a finite table, called a *Cayley table* or *operation table* for f.

Magmas

f	r	p	s
r	r	p	r
p	p	p	s
s	r	s	s

Figure: A Cayley table for a binary operation f

The above table defines a binary operation $f\colon A^2 \to A$ where $A \coloneqq \{r, p, s\}$. For example, $f(r, p) = p$. The magma $\mathbf{A} \coloneqq (A, f)$ is the *rock-paper-scissors magma*.

Magmas

$\cdot$	r	p	s
r	r	p	r
p	p	p	s
s	r	s	s

Figure: A Cayley table for a binary operation $\cdot$

We usually use *infix notation* for binary operations. For example, instead of $f(x, y)$ we write $x \cdot y$. Any other symbol, such as $+$, $*$, or $\circ$, will work as well, but some have special connotations, such as $+$ usually referring to a commutative operation.

Magmas

	r	p	s
r	r	p	r
p	p	p	s
s	r	s	s

Figure: A Cayley table for a binary operation

Going even further, we often use *concatenation notation* when there is only a single operation under consideration. We may write $\mathbf{A} := (A, f)$ or $\mathbf{A} := (A, \cdot)$ to define the rock-paper-scissors magma, then just write $rp = p$ rather than $f(r, p) = p$ or $r \cdot p = p$. (Naturally concatenation notation is my favorite, since it contains a version of my name.)

Magmas

- When the universe A of a magma $\mathbf{A} := (A, f)$ is infinite (or even just very large) it is easier to specify f by way of some rule rather than writing out its Cayley table.
- For example, we can take $A := \mathrm{Mat}_2(\mathbb{F}_{27})$ to be the set of 2×2 matrices over the field with 27 elements. We can then define an operation $f\colon A^2 \to A$ by $f(\alpha, \beta) := \alpha\beta - \beta\alpha$. This operation f has a finite Cayley table, but writing it out would take a lot of space. The algebra (A, f) is a magma.
- For an infinite example, take the magma $(\mathbb{N}, +)$ where $+$ is defined in the usual way for natural numbers.

Semigroups

- A *semigroup* is a magma $(S, \cdot)$ which satisfies the associative law
$$x \cdot (y \cdot z) \approx (x \cdot y) \cdot z.$$
- We write $\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$ to indicate the set of integers.
- We have that $(\mathbb{N}, +)$, $(\mathbb{W}, +)$, and $(\mathbb{Z}, +)$ are all semigroups. Also, $(\mathbb{N}, +)$ is a subalgebra of $(\mathbb{W}, +)$ and $(\mathbb{W}, +)$ is a subalgebra of $(\mathbb{Z}, +)$.
- We have that $(\mathbb{N}, \cdot)$ is a semigroup, but it is not a subalgebra of $(\mathbb{W}, +)$.

Monoids

- A *monoid* is an algebra $\mathbf{M} := (M, \cdot, e)$ such that $(M, \cdot)$ is a semigroup and $e\colon M^0 \to M$ is a nullary operation such that $\mathbf{M}$ satisfies the laws

$$x \cdot e \approx x \text{ and } e \cdot x \approx x.$$

- We have that $(\mathbb{W}, +, 0)$ is a monoid, as is $(\mathbb{N}, \cdot, 1)$.
- An important example is the *full transformation monoid* $(A^A, \circ, \mathrm{id}_A)$ whose universe A^A consists of the set of all functions from a given set A to itself, whose binary operation $\circ$ is function composition, and whose constant operation «is» the identity map $\mathrm{id}_A\colon A \to A$ given by $\mathrm{id}_A(a) := a$ for each $a \in A$.

Hold on a minute

What's the deal with that «squiggly equals sign» $\approx$?

Is something being approximated?

What's the deal with that «squiggly equals sign» $\approx$?

Is something being approximated?

An expression like $x(yz) \approx (xy)z$ stands for an *identity*, which is shorthand for the statement «For all possible values of x, y, and z we have that $x(yz) = (xy)z$.». This statement is true in some magmas (the semigroups), but is false in other ones, like the rock-paper-scissors magma. We won't get too technical about it until much later, so don't dwell on it for now.

An aside about signatures

- We gave a strict definition for the notation $(A, f_1, \ldots, f_k)$ last time. We said that this was shorthand for (A, F) where $F := \{f_i\}_{i \in I}$ where $I = \{1, 2, \ldots, k\}$.
- The signature of such an algebra is the function $\rho\colon I \to \mathbb{W}$ taking each $i \in \{1, 2, \ldots, k\}$ to the arity of $\rho(i)$.
- Since a function $\rho\colon \{1, 2, \ldots, k\} \to \mathbb{W}$ is a k-tuple of whole numbers, we say that the signature of $(A, f_1, \ldots, f_k)$ is $(\rho(1), \rho(2), \ldots, \rho(k))$.
- We will introduce algebras by saying things like «Consider an algebra $\mathbf{A} := (A, f, g, \star, +, u, 1)$ of signature $(25, 7, 2, 2, 1, 0)$.».

Groups

- A *group* is an algebra $\mathbf{G} := (G, \cdot, \_^{-1}, e)$ such that $(G, \cdot, e)$ is a monoid and $\_^{-1} \colon G \to G$ is a unary operation such that $\mathbf{G}$ satisfies
$$x \cdot x^{-1} \approx x^{-1} \cdot x \approx e.$$
- We have that $(\mathbb{Z}, +, -, 0)$ is a group. According to our definition here $(\mathbb{Z}, +)$ is actually neither a group nor a monoid because it doesn't have the right signature, although it is a semigroup (and hence a special kind of magma).
- An important example is the *permutation group* $\mathbf{Perm}(A) := (\mathrm{Perm}(A), \circ, \_^{-1}, \mathrm{id}_A)$ whose universe $\mathrm{Perm}(A)$ consists of the set of all bijections from a given set A to itself, whose binary operation $\circ$ is function composition, whose unary operation $\_^{-1}$ is given by taking the inverse function, and whose nullary operation «is» the identity map id_A.

Rings

- A *ring* is an algebra $\mathbf{R} := (R, +, \cdot, -, 0)$ such that $(R, +, -, 0)$ is an abelian group, $(R, \cdot)$ is a semigroup, and the identities
$$x \cdot (y + z) \approx (x \cdot y) + (x \cdot z)$$
and
$$(y + z) \cdot x \approx (y \cdot x) + (z \cdot x)$$
hold.
- The algebra $(\mathbb{Z}, +, \cdot, -, 0)$ with the usual definition of $\cdot$ for $\mathbb{Z}$ is a ring.
- A point we haven't stressed too much until now is that the order of the basic operations matters. The algebra $(\mathbb{Z}, \cdot, +, -, 0)$ is different from $(\mathbb{Z}, +, \cdot, -, 0)$ and is not a ring according to our definition, even though both of these algebras have the signature $(2, 2, 1, 0)$.

Modules

- Given a ring $\mathbf{R}$ a *(left)* $\mathbf{R}$*-module* is an algebra

$$\mathbf{M} \coloneqq (M, +, -, 0, \{\lambda_r\}_{r \in R})$$

such that $(M, +, -, 0)$ is an abelian group, for each $r \in R$ we have that λ_r is unary, and for each $r, s \in R$ we have that the laws

$$\lambda_r(x + y) \approx \lambda_r(x) + \lambda_r(y),$$

$$\lambda_{r+s}(x) \approx \lambda_r(x) + \lambda_s(x),$$

and

$$\lambda_r(\lambda_s(x)) \approx \lambda_{rs}(x)$$

hold.

Modules

- We didn't follow either of our existing rules for specifying the sequence of basic operations for an algebra in the preceding definition. It is a little tedious, but not difficult, to carefully formalize what we just did.
- The similarity type of an $\mathbf{R}$-module depends on the ring $\mathbf{R}$, in contrast with the previous examples. If R is an infinite set then an $\mathbf{R}$-module has infinitely many basic operations.

Quasigroups

- A *quasigroup* is an algebra $\mathbf{Q} := (Q, \cdot, /, \backslash)$ of signature $(2, 2, 2)$ which satisfies the laws

$$x\backslash(x \cdot y) \approx y,$$

$$(x \cdot y)/y \approx x,$$

$$x \cdot (x\backslash y) \approx y,$$

and

$$(x/y) \cdot y \approx x.$$

Quasigroups

- Given a group $\mathbf{G} := (G, \cdot, \_^{-1}, e)$ the algebra $(G, \cdot, /, \backslash)$ where $x/y := x \cdot y^{-1}$ and $x \backslash y := x^{-1} \cdot y$ is a quasigroup.
- Just as we often think of groups as being magmas with a particular type of binary operation (from which we can obtain the unary and nullary operations of the group), so too can we think of quasigroups as magmas with a particular type of binary operation (from which we can obtain the other two).
- A *Latin square* $\mathbf{Q} := (Q, \cdot)$ is a magma such that for all $a, b \in Q$ the equations

  $$a \cdot x = b \text{ and } y \cdot a = b$$

  have unique solutions.
- Quasigroups and Latin squares are in bijective correspondence, as we can take $x = a \backslash b$ and $y = b/a$ in the preceding equations.

Quasigroups

- Not all quasigroups come from the previous construction using groups.
- The algebra $(\mathbb{Z}, -)$ is a Latin square whose corresponding quasigroup does not arise from a group operation in this way.
- We denote by $\mathbb{R}$ the set of *real numbers*. Fixing some $n \in \mathbb{N}$ we define $x \cdot y$ to be the midpoint of the segment joining x and y for any $x, y \in \mathbb{R}^n$. The algebra $(\mathbb{R}^n, \cdot)$ is a Latin square.
- Quasigroup operations are typically not associative. Quasigroups are «nonassociative groups».
- Quasigroups with an identity element are called *loops*.

Semilattices

- A *semilattice* is a commutative semigroup $\mathbf{S} := (S, \cdot)$ which satisfies the identity
$$x \cdot x \approx x.$$
- Given $a, b \in \mathbb{Z}$ let $\min(a, b)$ and $\max(a, b)$ be the minimum and maximum of $\{a, b\}$, respectively. Both $(\mathbb{Z}, \min)$ and $(\mathbb{Z}, \max)$ are semilattices.
- Given $a, b \in \mathbb{N}$ let $\gcd(a, b)$ and $\mathrm{lcm}(a, b)$ be the greatest common divisor and least common multiple of $\{a, b\}$, respectively. Both $(\mathbb{N}, \gcd)$ and $(\mathbb{N}, \mathrm{lcm})$ are semilattices.
- Both $(\mathrm{Sb}(A), \cap)$ and $(\mathrm{Sb}(A), \cup)$ are semilattices for any given set A.

Lattices

- A *lattice* is an algebra $\mathbf{L} := (L, \wedge, \vee)$ such that $(L, \wedge)$ and $(L, \vee)$ are semilattices and the identities

$$x \wedge (x \vee y) \approx x \text{ and } x \vee (x \wedge y) \approx x$$

  hold.
- We have that $(\mathbb{Z}, \min, \max)$, $(\mathbb{N}, \gcd, \mathrm{lcm})$, and $(\mathrm{Sb}(A), \cap, \cup)$ are lattices.
- In some of the earliest work which laid the foundations for lattice theory, Dedekind considered the lattice of subgroups of an abelian group $\mathbf{A}$ under the operations of intersection and internal direct sum.

n-ary magmas

- Weren't we going to see algebras with all sorts of crazy n-ary operations for $n > 2$? Where are those?
- Historically people seem to more frequently produce and study binary operations.
- An algebra $\mathbf{A} := (A, f)$ of signature (n) is called an *n-ary magma*.

n-ary magmas

- An algebra $\mathbf{A} := (A, f)$ of signature (n) is called an *n-ary magma*.
- Fix an $n \in \mathbb{N}$. Given vectors $x_1, \ldots, x_{n-1} \in \mathbb{R}^n$ define $f(x_1, \ldots, x_{n-1})$ to be the determinant of

$$\begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ \vdots & \ddots & \vdots \\ x_{n-1,1} & \cdots & x_{n-1,n} \\ e_1 & \cdots & e_n \end{bmatrix}$$

where the e_i are standard basis vectors. The operation f is the *n-dimensional cross product* and $(\mathbb{R}^n, f)$ is an $(n-1)$-ary magma.

n-ary magmas

- An algebra $\mathbf{A} := (A, f)$ of signature (n) is called an *n-ary magma*.
- There are also n-ary analogues of groups and quasigroups which have received quite a bit of study.