Lecture 20: Introduction to Algebra and Algebras

Read: Chapter 9.
Do: Homework 19.

9.1. What is an algebra?

The first thing to realize is that "algebra" can be a count noun, and not only a proper noun. We will look at various kinds of algebras and at some fundamental notions used in algebra in general. Why is the study of algebra(s) useful? (1) Different kinds of algebras, which are defined by specific sets of axioms, give very nice examples of formal systems and their models. Changing one axiom can make the difference between one kind of algebra and another. So we can see model theory at work here, very vividly. (2) Algebras schematize various kinds of *structures*, and that's what linguists study. (3) Some particular kinds of algebras turn out to be highly relevant to the study of some parts of linguistics: Boolean algebras to the study of semantics, unification algebras to the study of feature structures, lattices both to semantics and to Optimality Theory.

What is an algebra? An algebra is a set together with a collection of operations on this set. For example, the set of natural numbers and operations of addition and multiplication forms an algebra.

An algebra **A** consists of a set A, called the *carrier* of **A,** together with one or more operations f_i defined on A.

$\mathbf{A} = \langle A, f_1, f_1, \ldots, f_n \rangle$

For example, $\mathbf{A} = \langle Rat, +, \times \rangle$: the rational numbers with addition and multiplication.

The set A may be finite or infinite.

The number of operations may be finite or infinite.

Each operation must be n-ary for some finite n.

Each operation must be well-defined on set A (Axiom 1 below) and must yield a unique element of A as value for each n-tuple of elements of A as argument (Axiom 2).

Two axioms that all algebras must obey:

Axiom 1: Closure. The set A must be closed under each operation f_i.

What does that mean? Suppose f_i is $\bullet$. Then a set A is *closed under* $\bullet$ iff for every a ,b ,*in* A, there is a c in A *such that* $a \bullet b = c$.

Practice: Are the integers closed under addition? Multiplication? Subtraction? Division?

Axiom 2: Uniqueness. If $a = a'$ and $b = b'$, *then* $a \bullet b = a' \bullet b'$.

Different kinds of algebras can be obtained by adding further axioms to these two.

Example: The syntax of statement logic can be represented by taking the set of statements as the set and conceiving of the rules for forming new statements as operations &, ~, etc.

$\mathbf{A} = \langle S, \sim, \&, \vee, \rightarrow, \leftrightarrow \rangle$. And the semantics of statement logic can be conceived of as an algebra whose set contains just the two truth values, and whose operations are defined by the familiar truth-tables. $\mathbf{B} = \langle \{0,1\}, \sim, \&, \vee, \rightarrow, \leftrightarrow \rangle$, where the connectives now are understood as operations on truth values, not as syntactic symbols.

Definition of *subalgebra*.

Given two algebras, $\mathbf{A} = \langle A, f_1^A, f_1^A, \ldots, f_n^A \rangle$ and $\mathbf{B} = \langle A, f_1^B, f_1^B, \ldots, f_n^B \rangle$, we say that **B** is a *subalgebra* of **A** if

1) **Subset**: $B \subseteq A$;

2) **Restriction:** for every i, $f_i^B = f_i^A | B$, i.e. f_i^B gives the same values as f_i^A when restricted to elements of B.

3) **Closure:** *B is closed under all operations f_i^B.*

9.2. Properties of operations.

For characterizing various kinds of algebras, the most important properties are properties of their *operations* (Section 9.2) and properties of various *special elements* (Section 9.3) such as 0 in the case of addition.

As we go through the properties, think about which of them apply to various familiar operations such as +, -, ×, ÷, ∪, ∩, set difference $A - B$, and the operation of function composition. We'll use the symbol • to stand for an arbitrary operation.

Associativity. An operation • from $A \times A$ to B is *associative* if and only if for all a, b, c in A, $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.

Commutativity. An operation • from $A \times A$ to B is *commutative* if and only if for all a, b in A, $a \bullet b = b \bullet a$.

Idempotence. An operation • from $A \times A$ to B is *idempotent* if and only if for all a in A, $a \bullet a = a$.

Distributivity. An operation $\bullet_1$ from $A \times A$ to B *distributes over* an operation $\bullet_2$ from $A \times A$ to B if and only if for all a, b, c in A, $a \bullet_1 (b \bullet_2 c) = (a \bullet_1 b) \bullet_2 (a \bullet_1 c)$

9.3. Special elements

Identity elements. Given an operation • from $A \times A$ to A:

e_L is a *left identity* for • iff $e_L \bullet a = a$ for all a in A.

e_R is a *right identity* for • iff $a \bullet e_R = a$ for all a in A.

e is a *two-sided identity*, or simply an *identity*, for • iff $a \bullet e = e \bullet a = a$, for all a in A.

It can be proven that if • is commutative, then every e_L or e_R is a two-sided identity.

Examples: most simple examples are two-sided identities. (Find them for +, ×, ∪). But for relative complement *A – B,* the empty set ∅ is e_R; there is no e_L and hence no e.

Inverses. (See book for left and right inverse; we'll only define *two-sided inverse*, or *inverse*).

An element *b* is an *inverse* of *a* with respect to an operation • iff $a \bullet b = b \bullet a = e$.

Notation: a^{-1} is the *inverse of a.*

For addition on the integers, a^{-1} is $-a$.

For addition on the positive integers, there are no inverses.

9.4. Maps and morphisms.

In this section we consider properties of functions that map one algebra to another:

F: $\mathbf{A} \rightarrow \mathbf{B}$; properties that indirectly relate to whether the two algebras have structures that are the same in important respects.

Such maps may be *one-to-one* (*"injective"*), *onto* ("surjective"), or both ("bijective").

Homomorphism

Given algebras **A** and **B** with carriers *A* and *B* respectively and a mapping

$F: A \rightarrow B$, we say that *F* is a *homomorphism* from *A* to *B*, if for every f_i we have

$$F(f_i^A\,(a_1, ..., a_n)) = f_i^B\,(F\,(a_1), ..., F\,(a_n)).$$

In words: the result of applying corresponding operations to corresponding elements are corresponding elements. (But the formula is more accurate than the words.)

Example: The mapping from the *syntactic algebra* of propositional logic to its *semantic algebra* is a homomorphism. (Check out this claim.)

Isomorphism

Algebras **A** and **B** are *isomorphic* iff there is an *isomorphism* between them. An *isomorphism* is a homomorphism which is also a one-to-one mapping.

(So an isomorphism must be one-one; a homomorphism can be many-one.)

If two algebras are isomorphic, they are basically identical in the relevant structure, and one can be transformed into the other just by relabeling the elements.

Automorphism

An *automorphism* is an isomorphism of an algebra with *itself.*