Chapter 9

Basic Concepts of Algebra

9.1 Definition of algebra

An *algebra* **A** is a set A together with one or more operations f_i. We may represent an algebra by writing

(9–1) $\mathbf{A} = \langle A, f_1, f_2, \ldots, f_n \rangle$

or by using particular symbols for the operations, such as

(9–2) $\mathbf{A} = \langle A, +, \times \rangle$

The set A may finite or infinite, and there may be either a finite or an infinite number of different operations. However, each operation must be *finitary*, i.e. unary, binary, ternary, ... Each n-ary operation must be a well-defined operation, i.e. defined for all n-tuples of elements of A and yielding a unique element of A as a value for each n-tuple (cf. the mapping condition for functions in Section 2.3).

These requirements on the operations can be stated in the form of two axioms which each operation in an algebra must satisfy. For simplicity, the axioms are stated in terms of a binary operation $\circ$; their generalization to arbitrary n-ary operations is straightforward.

Axiom 1. *Closure: A is closed under the operation $\circ$, i.e. for any $a, b \in A$ there is an element $c \in A$ such that $a \circ b = c$.*

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

Closure and uniqueness in appropriate sets are ordinarily considered the minimal requirements for well-behaved operations. Admitting partial operations in an algebra is common in universal algebra and category theory, which are beyond the introductory scope of this book. (See Goldblatt (1979), Grätzer (1971), MacLane and Birkhoff (1983) and for discussion in the context of Montague grammar especially Janssen (1983).) We shall not be concerned with operations that do not satisfy closure and uniqueness. Various kinds of algebras can be obtained by adding further axioms to these two basic requirements. We will study a number of such algebras in this chapter.

We have already encountered many structures which are algebras in this sense. The syntax of the logic of statements, for instance, can be represented as an algebra based on the set of well-formed statements (S) and the connectives as operations: $\mathbf{A} = \langle S, \sim, \&, \vee, \rightarrow, \leftrightarrow \rangle$. Similarly, the semantics of the logic of statements can be considered as an algebra, based on the set of truth values and the truth tables, interpreting the connectives as operations: $\mathbf{B} = \langle \{0,1\}, \sim, \&, \vee, \rightarrow, \leftrightarrow \rangle$, where the connectives are understood as operations on truth values, not as syntactic symbols. We will see below that there is an important connection between the syntactic algebra and the semantic algebra of such formal languages, which serve as models for the syntax and semantics of natural languages.

DEFINITION 9.1 *An algebra* $\mathbf{B}$ *is a* subalgebra *of an algebra* $\mathbf{A} = \langle A, f_1^A, f_2^A, \ldots, f_n^A \rangle$ *if* $\mathbf{B}$ *satisfies the following conditions:*
$\mathbf{B} = \langle B, f_1^B, f_2^B, \ldots, f_n^B \rangle$, *where*

(i) $B \subseteq A$

(ii) *For every* i, $f_i^B = f_i^A \restriction B$; *i.e.,* f_i^B *yields the same values as* f_i^A *when restricted to elements of* B.

(iii) B *is closed under all operations* f_i^B

■

9.2 Properties of operations

In Section 1.8 a number of properties of operations on sets were introduced. We repeat certain of these definitions here as properties of operations in

algebras for easy reference and add a number of properties of operations which are frequently encountered in algebraic operations

An operation $\circ$ from $A \times A$ to B is *associative* if and only if for all a, b, c in A, $(a \circ b) \circ c = a \circ (b \circ c)$. In an associative operation it is immaterial in what order repeated applications of it are made. Set-theoretic union and intersection and function composition are associative, as are logical conjunction and disjunction Examples of non-associative operations are set-theoretic difference and division of real numbers.

An operation $\circ$ from $A \times A$ to B is *commutative* if and only if for all a, b in A, $a \circ b = b \circ a$ Familiar commutative operations are logical conjunction and disjunction; set intersection and union; and addition and multiplication of real numbers Some non-commutative operations are subtraction, division and function composition

An operation $\circ$ from $A \times A$ to B is *idempotent* if and only if for all a in A, $a \circ a = a$. Set-theoretic union and intersection are idempotent, as are logical conjunction and disjunction. But most of the operations we have encountered are not: addition, multiplication, subtraction, division, relative complementation and function composition are not idempotent operations.

For two operations $\circ_1$ and $\circ_2$ both from $A \times A$ to B, $\circ_1$ *distributes over* $\circ_2$ if and only if for all a, b, c in A, $a \circ_1 (b \circ_2 c) = (a \circ_1 b) \circ_2 (a \circ_1 c)$. We have seen that set-theoretic union distributes over intersection and vice versa. But, although arithmetic multiplication distributes over addition ($a \times (b + c) = (a \times b) + (a \times c)$), addition does not distribute over multiplication, since in general $a + (b \times c) \neq (a + b) \times (a + c)$.

9.3 Special elements

The next three notions are special properties which certain members of a set may have with respect to some operation defined on the set.

Given an operation $\circ$ from $A \times A$ to B, an element e_l is a *left identity element* of $\circ$ if and only if for all a in A, $e_l \circ a = a$. Similarly, e_r in A is a *right identity element* of $\circ$ if and only if for all a in A, $a \circ e_r = a$. As we saw in Section 2 4, for a function $F : A \to B$, if the operation $\circ$ denotes function composition, then $id_B \circ F = F$ and $F \circ id_A = F$. Thus for the operation of composition of functions the identity functions id_B and id_A are respectively a left and right identity element. Subtraction defined on the set of integers and zero has a right identity element, namely zero itself, since

for all n, $n - 0 = n$. But there is no left identity element; i.e., there is no element m in the set such that for all n, $m - n = n$

For commutative operations, every left identity element is also a right identity element, and vice versa. To see this, consider a left identity e_l. By definition $(\forall a \in A)(e_l \circ a = a)$. Because the operation is commutative, $e_l \circ a = a \circ e_l = a$, for all $a \in A$, and so e_l is also a right identity element. Similarly, every right identity is also a left identity for commutative operations. An element that is both a right and left identity element is called a *two-sided identity* or simply an *identity element*. While commutativity of an operation is a sufficient condition for every right or left identity to be two-sided, it is not a necessary condition; a two-sided identity may exist for some operations that are not commutative. An example of this is found in the operations of composition of functions defined on some set of functions $\mathbf{F} = \{F, G, H, \ldots\}$, each being a function in A. If id_A is one of these function, it is a two-sided identity, since for each $x \in F$, $id_A \circ x = x \circ id_A = x$, but the operation of composition of functions is not in general commutative. For addition the two-sided identity is 0, but for arithmetic multiplication it is 1, since for all n, $n + 0 = 0 + n = n$ and $n \times 1 = 1 \times n = n$. Given some collection of sets, the identity element for intersection is U, the universal set, and for union it is the empty set (verify!). Relative complementation has $\emptyset$ as a right identity but in general it has no left identity. It is provable that if for a given operation a two-sided identity exists, then this element is unique

Given an operation $\circ$ from $A \times A$ to B with a two-sided identity element e, a given element a in A is said to have a *right inverse* a_r if and only if $a \circ a_r = e$. A given element a in A is said to have a *left inverse* a_l if and only if $a_l \circ a = e$. If a^{-1} is both a left and a right inverse of a, i e. $a^{-1} \circ a = a \circ a^{-1} = e$, then a^{-1} is called a *two-sided inverse* of a. When the term 'inverse' is used without further qualification, we mean that it is two-sided. Note that inverses are always paired in the following way: b is a right inverse of a if and only if a is a left inverse of b, since both statements follow from $a \circ b = e$. One should observe also that the question of the existence of an inverse can be raised with respect to *each* element in the set on which the operation is defined. In contrast, an identity element, if it exists, is defined for the operation as a whole. To illustrate, let addition be defined in the set Z of all positive and negative integers and zero. As we have seen, 0 is the two-sided identity element for this operation. Consider now the number 3, and let us ask if it has an inverse in Z. Is there an element z in Z that when added to 3 yields 0? The number -3 is such an element, and, furthermore, it is both a right and a left inverse, since $3 + (-3) = (-3) + 3 = 0$. From this it

also follows that 3 is a two-sided inverse of -3. For addition, every member of Z has an inverse, since to each integer z, except 0, there corresponds a negative integer $-z$, such that $z+(-z) = 0$. The number 0 is its own inverse, since $0 + 0 = 0$.

Given an operation $\circ$ from $A \times A$ to B, an element 0_l is called a *left zero of* $\circ$ if and only if for all a in A, $0_l \circ a = 0_l$. Similarly, 0_r is called a *right zero of* $\circ$ if and only if for all a in A, $a \circ 0_r = 0_r$. An element that is both a left and a right zero is called a *two-sided zero*, or simply a *zero*. This terminology derives from the fact that the number zero functions as a zero element in arithmetic multiplication. There is no zero element for subtraction or division. The empty set is a zero element for set intersection and the universal set U is the zero element for set union.

9.4 Maps and morphisms

Relations between algebras may be described by functions mapping one algebra in another; $F : \mathbf{A} \rightarrow \mathbf{B}$. Such a map is *injective* if some function $F : \mathbf{A} \rightarrow \mathbf{B}$ is one-to-one, i.e. $F(a) = F(b)$ implies $a = b$. $F : \mathbf{A} \rightarrow \mathbf{B}$ is *surjective* (or *onto*) if $\{F(a) \mid a \in A\} = B$. And $F : \mathbf{A} \rightarrow \mathbf{B}$ is *bijective* if F is both injective and surjective (or one-to-one and onto). A *morphism* is a mapping $F : \mathbf{A} \rightarrow \mathbf{B}$ conceived of dynamically as a transformation process of $\mathbf{A}$ into $\mathbf{B}$. If $\mathbf{A} = \langle A, f_1, \ldots, f_n \rangle$ and $\mathbf{B} = \langle B, g_1, \ldots, g_n \rangle$ then $\mathbf{A}$ and $\mathbf{B}$ are *isomorphic* if and only if there is a one-to-one correspondence between their operations (we will assume for simplicity that the correspondence is $f_i \leftrightarrow g_i$) and a one-to-one and onto function φ mapping A onto B such that for all $x, y, z, \ldots$, in A and all $i \leq n$

$$g_i(\varphi(x), \varphi(y), \varphi(z), \ldots) = \varphi(f_i(x, y, z, \ldots)).$$

A *homomorphism* is a correspondence between algebras with all the properties of an isomorphism except that the mapping from A to B may be *many-to-one*; the set B may be smaller than the set A.

An *automorphism* of an algebra $\mathbf{A}$ is an isomorphism of $\mathbf{A}$ with itself. The identity mapping ($\varphi(x) = x$) always provides an automorphism for any algebra (the "trivial" automorphism); the question generally asked of a given algebra is whether it has any other ("non-trivial") automorphisms.

For instance, let $\mathbf{A} = \langle S, \sim, \&, \vee, \rightarrow, \leftrightarrow \rangle$, and $\mathbf{B} = \langle \{0, 1\}, \sim, \&, \vee, \rightarrow, \leftrightarrow \rangle$, as defined above in 9.1.

Any assignment of truth-values to the statements in S is a homomorphism $F : \mathbf{A} \rightarrow \mathbf{B}$. *i.e* distinct statements p, q may be mapped to the same truth-value, but

$$\begin{aligned} F(p \,\&\, q) &= F(p) \,\&\, F(q) \\ F(p \vee q) &= F(p) \vee F(q) \\ F(p \rightarrow q) &= F(p) \rightarrow F(q) \\ F(p \leftrightarrow q) &= F(p) \leftrightarrow F(q) \\ F(\sim p) &= \sim F(p) \end{aligned}$$

Construction of truth tables for complex statements can now be understood as based on the fact that, given an assignment to the atomic statements, the composition preserves the homomorphism from the syntactic algebra to the semantic one. This can be considered to be the algebraic counterpart of the Principle of Compositionality, often also espoused in one form or another for the syntax and semantics of natural languages. The principle requires the meaning of a complex expression to be a function of the meaning of its constituent parts and the way in which they are put together (See also Ch 13). Homomorphisms can, of course, relate semantic algebras, e g. by embedding a given interpretation into an extension of that interpretation. Extensive applications are made of these embeddings, for instance, in semantic theories based on dynamic interpretations and in Kripke semantics (see Ch 12).

A simple example of an algebra A' which is isomorphic to A is a syntax of the statment logic which uses instead of p, q, r etc for statements, a different alphabet, say the Greek letters ϕ, ψ, χ etc , and possibly alternative symbols for the connectives If alphabetic variance is the only difference between two logical systems they are isomorphic from an algebraic point of view.

Throughout the remainder of this part of the book we will encounter more interesting mathematical examples of homomorphisms and isomorphisms.

Category theory, a relatively recent and flourishing development of algebra, studies properties of algebras that can be expressed in terms of morphisms. It provides a very abstract and universal perspective on the foundations of set theory, algebra and logic, in which cross-fertilization yields many new insights and results. The interested reader is referred to Goldblatt (1979) for an introduction.

Exercises

1. Consider the operation of intersection defined on some arbitrary collection of sets.

   (a) Is there a two-sided identity element?

   (b) Which sets have an inverse element?

2. Given an arbitrary collection of sets, what elements, if any, have inverses with respect to the operation of a) union and b) symmetric difference?

3. If for a given operation in an algebra a two-sided identity exists, it is unique Prove this for the operation of set-theoretic union.