

THE BASIC CONCEPTS OF ALGEBRAIC LOGIC

PAUL R. HALMOS, University of Chicago

1. Introduction. It has often happened that a theory designed originally as a tool for the study of a physical problem came subsequently to have purely mathematical interest. When that happens, the theory is usually generalized way beyond the point needed for applications, the generalizations make contact with other theories (frequently in completely unexpected directions), and the subject becomes established as a new part of pure mathematics. The part of pure mathematics so created does not (and need not) pretend to solve the physical problem from which it arises; it must stand or fall on its own merits.

Physics is not the only external source of mathematical theories; other disciplines (such as economics and biology) can play a similar role. A recent (and possibly somewhat surprising) addition to the collection of mathematical catalysts is formal logic; the branch of pure mathematics that it has precipitated will here be called *algebraic logic*.

Algebraic logic starts from certain special logical considerations, abstracts from them, places them into a general algebraic context, and, *via* the generalization, makes contact with other branches of mathematics (such as topology and functional analysis). It cannot be overemphasized that algebraic logic is more algebra than logic. Algebraic logic does not claim to solve any of the vexing foundation problems that sometimes occupy logicians. All that is claimed for it is that it is a part of pure mathematics in which the concepts that constitute the skeleton of modern symbolic logic can be discussed in algebraic language. The discussion serves to illuminate and clarify those concepts and to indicate their connection with ordinary mathematics. Whether the subject as a whole will come to be considered sufficiently interesting and sufficiently deep to occupy a place among pure mathematical theories remains to be seen.

The literature of algebraic logic is not yet very extensive, and the few items that are available are highly technical. It is for that reason that this expository paper was written; its main purpose is to kindle interest in a young but promising subject. In such a context it does not seem to be appropriate to burden the reader with the usual scholarly references and assignments of credit. At the very least, however, the names of the principal contributors should be mentioned. Here they are: Curry, Henkin, Rasiowa, Sikorski, and Tarski. Many of the ideas of algebraic logic have been in the air for several years and were known, at least subconsciously, by most logicians. The greatest contributions are those of Tarski; especially relevant is his work (with Jónsson) on Boolean algebras with operators and his theory of cylindric algebras. (Most of the latter material is unfortunately unpublished.) The reader who wishes to study the details will find exact references in two papers on algebraic logic by the present author; the first is in *Compositio Mathematica* (1955), and the second is to appear in *Fundamenta Mathematicae* (1957).

2. Boolean algebras. The father of algebraic logic is George Boole; it is appropriate that a discussion of the subject begin with a quick review of the algebras that bear his name. The shortest definition of Boolean algebras is in terms of the theory of rings: a *Boolean algebra* is a ring with unit in which every element is idempotent (*i.e.*, if p is in the ring, then $p^2 = p$). The simplest example, and one that plays a vitally important role throughout the theory, is the field of integers modulo 2; this Boolean algebra will be denoted by \mathbf{O} .

Boolean algebras have an almost embarrassingly rich structure. It is, for instance, an easy consequence of the definition that a Boolean algebra always has characteristic 2 (*i.e.*, $p + p = 0$) and that as a ring it is always commutative (*i.e.*, $pq = qp$). In every Boolean algebra there is, moreover, a natural order relation; it is defined by writing $p \leq q$ if and only if $pq = p$. The algebraic structure and the order structure are as compatible as they can be. The algebraic zero is also the order zero (*i.e.*, the least element of the algebra), and the algebraic unit is also the order unit (*i.e.*, the greatest element of the algebra); in other words, $0 \leq p \leq 1$ for every p . With respect to the order, the algebra turns out to be a complemented lattice. The lattice operations can be expressed in terms of the given algebraic operations, as follows: the complement of p , denoted by p' , is $1 + p$; the infimum of p and q , denoted by $p \wedge q$, is pq ; and the supremum of p and q , denoted by $p \vee q$, is $p + q + pq$.

The process of defining many useful operations and relations in a Boolean algebra, in terms of addition and multiplication, is to a large extent reversible. This fact is responsible for the abundance of different axiomatic approaches to the subject. A Boolean algebra can be defined in terms of its partial order, or in terms of complements and suprema, or in terms of complements and infima, and so on and so forth *ad almost infinitum*. Thus, for instance, since sums and products can be expressed in terms of complements and infima ($pq = p \wedge q$ and $p + q = (p' \wedge q')' \wedge (p \wedge q)'$), it follows that if a set admits a unary operation and a binary operation satisfying the appropriate conditions, then that set is a Boolean algebra. (It isn't really, but it is close enough to make the distinction pedantic. What should be said is that if addition and multiplication are defined as indicated above, then the set, together with the defined operations, constitutes a Boolean algebra.) The appropriate conditions are simple to describe. They require that the underlying set contain at least two distinct elements, and that

$$(I\ 1) \qquad p \wedge (q \wedge r) = (p \wedge q) \wedge r,$$

$$(I\ 2) \qquad p \wedge q = q \wedge p,$$

$$(I\ 3) \qquad \text{if } p \wedge q' = r \wedge r', \text{ then } p \wedge q = p,$$

$$(I\ 4) \qquad \text{if } p \wedge q = p, \text{ then } p \wedge q' = r \wedge r',$$

for all elements p , q , and r . (Caution: (I 3) means that if $p \wedge q' = r \wedge r'$ for *some* r , then $p \wedge q = p$, and (I 4) means that if $p \wedge q = p$, then $p \wedge q' = r \wedge r'$ for *all* r .)

Since, inside a fixed non-empty set, set-theoretic complementation and the formation of set-theoretic intersections do satisfy these conditions, any class of sets that is closed under these two operations is a Boolean algebra. The class of all subsets of a non-empty set is the most easily described (but far from the only) example of a Boolean algebra obtained in this way.

[Terminological purists sometimes object to the Boolean use of the word "algebra." The objection is not really cogent. In the first place, the theory of Boolean algebras has not yet collided, and it is not likely to collide, with the theory of linear algebras. In the second place, a collision would not be catastrophic; a Boolean algebra is, after all, a linear algebra over the field of integers modulo 2. The last, but not the least, pertinent comment is a pragmatic one. While, to be sure, a shorter and more suggestive term than "Boolean algebra" might be desirable, the nomenclature is so thoroughly established that to change now would do more harm than good.]

It is amusing and instructive to compare the axiom system (I) with the following, somewhat unorthodox, system of axioms for groups. A group may be defined as a non-empty set with a unary operation ($p \rightarrow p^-$) and a binary operation ($(p, q) \rightarrow p \times q$) such that

$$(II\ 1) \quad p \times (q \times r) = (p \times q) \times r,$$

$$(II\ 2) \quad (p \times q)^- = q^- \times p^-,$$

$$(II\ 3) \quad \text{if } p \times q = r \times r^-, \text{ then } p = q^-,$$

$$(II\ 4) \quad \text{if } p = q^-, \text{ then } p \times q = r \times r^-,$$

for all elements p, q , and r . (Caution: (II 3) means that if $p \times q = r \times r^-$ for *some* r , then $p = q^-$, and (II 4) means that if $p = q^-$, then $p \times q = r \times r^-$ for *all* r .) It is clear that if, in a group, p^- is defined to be the inverse of p , and $p \times q$ is defined to be the product of p and q (in that order), then the conditions (II) are satisfied. The fact that, conversely, the conditions (II) are characteristic of inversion and multiplication in groups is an easy exercise in elementary axiomatics.

[One comment should be made on the independence of the axiom set (II). The fact is that the set is *not* independent; the first three axioms are sufficient to characterize groups, and, in particular, they imply the fourth. The reason (II) is offered in the present form is to emphasize its similarity with the axiom set (I) for Boolean algebras. Each of the axioms (II 1), (II 2), and (II 3) is independent of the other three axioms of the set (II).]

3. Propositional calculi. To understand the connection between Boolean algebra and logic, a good way to begin is to examine how sentences are combined by means of sentential connectives. To ensure an unprejudiced approach to the subject, it is desirable to proceed as abstractly as possible. Suppose, therefore, that there is given an arbitrary non-empty set S ; intuitively the elements of S are to be thought of as the basic sentences of some theory that is being studied. Suppose, moreover, that A and N are two distinct objects not contained in S ; intuitively A and N are to be thought of as the connectives "and" and "not."

(Warning: in other expositions, A is frequently used for the dual connective "or".) Consider finite sequences whose terms are either elements of S or else A or N . (The empty sequence is not included.) If s is a sequence of length n , say, so that s_0, \dots, s_{n-1} are elements of $S \cup \{A, N\}$, let Ns be the sequence defined by

$$(Ns)_0 = N, \quad (Ns)_i = s_{i-1} \quad (i = 1, \dots, n);$$

if s and t are sequences (of lengths n and m respectively), let Ast be the sequence defined by

$$(Ast)_0 = A, \quad (Ast)_i = s_{i-1} \quad (i = 1, \dots, n), \quad (Ast)_{n+j} = t_{j-1} \quad (j = 1, \dots, m).$$

Let S^* be the smallest set of sequences such that (1) if s is a sequence of length 1 whose unique term is in S , then $s \in S^*$, (2) if $s \in S^*$, then $Ns \in S^*$, and (3) if $s \in S^*$ and $t \in S^*$, then $Ast \in S^*$. In other words, S^* is the set of sequences generated from the one-term sequences of S by means of the operations of prefixing N to a sequence and prefixing A to the concatenation of two sequences. Intuitively S^* is to be thought of as the set of sentences generated from the basic sentences by the two basic connectives. The device of writing Ast instead of $s \ A \ t$ (an ingenious Polish invention) is designed to avoid the multiple layers of parentheses that the more intuitive infix notation necessitates.

The set S^* by itself is not quite a proper object of logical study. The trouble is that if, for instance, s and t are in S^* , then Ast and Ats are distinct elements of S^* , whereas common sense seems to demand that if s and t are sentences, then " s and t " and " t and s " should be sentences that "say the same thing" in some sense. Sentences admit, in other words, a natural equivalence relation; such a relation should therefore be introduced into S^* . A little thought about the intuitive interpretation of the elements of S^* will suggest many conditions that equivalence should satisfy. If the assertion that the elements s and t of S^* are equivalent is denoted by $s \equiv t$, then, for all elements s, t , and u of S^* , it should at the very least be required that

$$(III \ 1) \quad AsAtu \equiv AAstu,$$

$$(III \ 2) \quad Ast \equiv Ats,$$

$$(III \ 3) \quad \text{if } AsNt \equiv AuNu, \quad \text{then} \quad Ast \equiv s,$$

$$(III \ 4) \quad \text{if } Ast \equiv s, \quad \text{then} \quad AsNt \equiv AuNu,$$

$$(III \ 5) \quad \text{if } s \equiv t, \quad \text{then} \quad Ns \equiv Nt,$$

$$(III \ 6) \quad \text{if } s \equiv t, \quad \text{then} \quad Asu \equiv Atu.$$

In addition, of course, it is necessary that the concept of equivalence used here be an honest equivalence, *i.e.*, that it be reflexive, symmetric, and transitive.

There are likely to be many equivalence relations satisfying the conditions (III); one such is defined by writing $s \equiv t$ for all s and t . In order to avoid this triviality (and for other reasons), it is desirable to consider the smallest possible

equivalence (*i.e.*, the one in which the fewest possible pairs turn out to be equivalent) satisfying these conditions. This makes sense. Indeed, if an equivalence relation is thought of as a certain set of ordered pairs, then the intersection of all the equivalence relations satisfying (III) is an equivalence relation satisfying (III). If, from now on, the symbol \equiv is used to denote this minimal equivalence, then the pair (S^*, \equiv) is one of the simplest non-trivial logical structures; it is usually known as the *propositional* (or *sentential*) *calculus*. There are really many propositional calculi; there is one corresponding to each non-empty set S . It is clear, however, that the only thing that matters (all other differences between the various propositional calculi being essentially notational matters) is the cardinal number of S . It is customary (but not particularly profitable) to assume that S is countably infinite.

4. Axioms and rules. The time has come to make the notation more transparent. While the symbols A and N are technically convenient (no parentheses), it is usually a cumbersome job to decode the sentences involving them and to recapture their intended intuitive content. Accordingly, in what follows, $(s)'$ will be used as an alternative symbol for Ns , and, similarly, $(s) \wedge (t)$ will be used as an alternative symbol for As . Thus, for instance, $AsNt$ can be denoted by $(s) \wedge ((t)')$; with the usual mathematical conventions about omitting superfluous parentheses, this becomes $s \wedge t'$. It should now be clear that the conditions (III 1)–(III 4) are only notationally different from (I 1)–(I 4); the conditions (III 5) and (III 6) assert, in customary mathematical language, that \equiv is a congruence relation with respect to the operations of attaching $'$ and infixing \wedge .

The equivalence relations that occur in algebra (*e.g.*, the congruence relations in a ring) are usually described by specifying a particular equivalence class (the kernel) and a particular operation (subtraction); it then turns out that two elements are congruent if and only if their difference belongs to the kernel. A similar procedure is available to define the equivalence \equiv described above. In order to motivate the choice of the kernel and the choice of the pertinent subtraction operation, consider first of all an element of S^* that has the form $s \wedge s'$. If the elements of S^* are interpreted as sentences, then there is something obviously undesirable about such an element; in some intuitive sense it is "false." By the same token, the result of attaching $'$ to such an element converts it into something quite laudable; sentences such as that are "true." The kernel that is usually considered is the equivalence class of any particular "true sentence" so obtained. It is pleasant to be able to report that this kernel is independent of the arbitrary choice of its generator. The equivalence class of any element of the form $(s \wedge s)'$ contains all other elements of that form, and, in fact, it consists exactly of all the elements that common sense would declare to be "true." An element of this kernel is called a *tautology* of the propositional calculus. The subtraction operation is the one that associates with two elements s and t of S^* the element $(s \wedge t')' \wedge (s' \wedge t)'$. (In the original notation this reads $ANAsNtNANst$.) The perceptive reader will note that if s and t are interpreted as sentences, then the intuitive interpretation of the proposed "difference" between s and t is the

sentence “ s if and only if t .” This subtraction does what it was tacitly promised it would do; it is true that a necessary and sufficient condition that s be equivalent to t is that the difference of s and t belong to the kernel. (In customary logical language: a necessary and sufficient condition for $s \equiv t$ is that the biconditional of s and t be a tautology. It is a happy circumstance that biconditioning is a commutative operation; the order of s and t is immaterial.)

In principle it is clear how the procedure used above could be reversed. The tautologies could be defined by making a complete list of them, and equivalence could then be defined in terms of tautologies and the formation of biconditionals. The list of tautologies would be infinite, to be sure, but a clever classifier might nevertheless succeed in describing it in a finite number of words. Something like this is what is usually done. In most text-book presentations of the propositional calculus one finds a small list of special tautologies, together with a few easy instructions for manufacturing others; a general tautology is then defined to be a member of the subset of S^* generated from the special tautologies by repeated applications of the instructions. The given special tautologies (whose particular choice is largely a matter of individual taste) are called *axioms*, and the instructions for manufacturing others are called *rules of inference*. This “axiomatic” procedure (which has become traditional) has no particular advantages (or disadvantages) in comparison with the one followed above; its final result is merely an alternative description of the propositional calculus.

[Here, for the sake of completeness, are the details of one of the popular axiomatic approaches to the propositional calculus. Let $s \vee t$ and $s \rightarrow t$ be abbreviations for $(s' \wedge t')'$ and $(s \wedge t')'$ respectively (or, in the original notation, for $NANsNt$ and $NAsNt$ respectively); the axioms are most conveniently, and most understandably, described by means of these abbreviations. The axioms consist of all those elements of S^* that are of one of the following four forms:

- (1) $(s \vee s) \rightarrow s,$
- (2) $s \rightarrow (s \vee t),$
- (3) $(s \vee t) \rightarrow (t \vee s),$
- (4) $(s \rightarrow t) \rightarrow ((u \vee s) \rightarrow (u \vee t)),$

where s , t , and u are arbitrary elements of S^* . There is only one rule of inference (called *modus ponens*). According to that rule, if s and t are elements of S^* such that both s and $s \rightarrow t$ are tautologies, then t is a tautology.]

5. Free Boolean algebras. By whatever method the pair (S^*, \equiv) is obtained, once it is at hand it is natural to form the set A^* of all equivalence classes. In analogy with calling an element of S^* a sentence, an element of A^* may be called a *proposition*. (The word “proposition” is not always defined this way. The intuitive reasons for using the definition are obvious, but, admittedly, they are not overwhelming.) The set A^* of propositions possesses, in a natural way, the structure of a Boolean algebra. If $p \in A^*$, let s be any element of the equivalence class p and write p' for the equivalence class of Ns (i.e., of s'). If both s_1 and s_2

belong to p , *i.e.*, if $s_1 \equiv s_2$, then, by (III 5), $Ns_1 \equiv Ns_2$, so that the definition of p' is unambiguous. If p and q are in \mathbf{A}^* , let s and t be corresponding representative elements (*i.e.*, $s \in p$ and $t \in q$) and write $p \wedge q$ for the equivalence class of Ast (*i.e.*, of $s \wedge t$). The necessary unambiguity argument is based on (III 6) this time. The fact that the conditions (I) are satisfied now follows immediately from a comparison of those conditions with the corresponding conditions (III).

The procedure for arriving at \mathbf{A}^* is familiar to anyone who ever heard of the theory of free groups; the Boolean algebra \mathbf{A}^* is, in fact, isomorphic to the free Boolean algebra generated by the originally given set S . In logical studies it is customary to describe the algebraic properties of \mathbf{A}^* by some rather specialized terminology. Thus, for instance, the fact that \mathbf{A}^* satisfies the first necessary condition for being a Boolean algebra (the possession of at least two distinct elements) is usually described by saying that the propositional calculus is consistent.

In view of what has already been said, it is not at all surprising that the construction of \mathbf{A}^* has a very near parallel in group theory. Given an arbitrary non-empty set S , form the set S^* exactly as before and introduce into S^* the smallest equivalence relation \equiv such that

$$(IV\ 1) \quad AsAtu \equiv AAstu,$$

$$(IV\ 2) \quad NAst \equiv ANtNs,$$

$$(IV\ 3) \quad \text{if } Ast \equiv AuNu, \text{ then } s \equiv Nt,$$

$$(IV\ 4) \quad \text{if } s \equiv Nt, \text{ then } Ast \equiv AuNu,$$

$$(IV\ 5) \quad \text{if } s \equiv t, \text{ then } Ns \equiv Nt,$$

$$(IV\ 6) \quad \text{if } s \equiv t, \text{ then } Asu \equiv Atu,$$

for all elements s, t , and u of S^* . The set of all equivalence classes possesses, in a natural way, the structure of a group. The obvious details may safely be omitted; suffice it to say that the proof depends on a comparison of (II) with (IV). The group so obtained is, in fact, isomorphic to the free group generated by the originally given set S .

[The method of sequences-*cum*-equivalence is essentially the only known way of constructing free groups. It is worth noting that for Boolean algebras the following much more elegant method is available. Given an arbitrary (possibly empty) set S , let X be the set of all subsets of S . For each s in S , let $p(s)$ be the set of all those elements of X that contain s . Let \mathbf{A}^* be the Boolean algebra generated by all the sets of the form $p(s)$ with s in S , so that \mathbf{A}^* is a Boolean subalgebra of the Boolean algebra of all subsets of X . Assertion: \mathbf{A}^* is isomorphic to the free Boolean algebra generated by S . The proof of the assertion is an easy exercise in set theory. Unfortunately this method of constructing \mathbf{A}^* is quite provincial; it works like a charm for Boolean algebras, but it does not work for very many algebraic systems, at least not without significant modifications.]

6. Quotients of free algebras. Since the algebraic end-product of the propositional calculus is a free Boolean algebra, that calculus, as it now stands, is too special for most logical purposes. (Freedom for an algebraic system means, roughly speaking, that the only relations among its elements are the trivial ones). The difficulty is visible in the starting point of the construction of the propositional calculus; its source is the fact that the generating set S is a set with no algebraic structure at all. In realistic situations the basic sentences of a theory are likely to be related to each other in various intricate ways, and, in fact, it is usually considered to be one of the chief functions of logic to study such relations and their consequences.

Suppose, for instance, that someone wants to undertake a logical examination of a fragment of the history of English literature. Among the basic sentences of the theory (*i.e.*, among the elements of S) there might occur "Shakespeare wrote Hamlet" and "Bacon wrote Macbeth"; call these sentences s_0 and t_0 respectively. ("Basic sentence" is not the same as "axiom." The sentences s_0 and t_0 need not, at first, be considered either "true" or "false"; they are just considered.) Under these circumstances the investigator would perhaps want to declare the sentence NAs_0t_0 to be an axiom. Since, however, NAs_0t_0 is not a tautology of the propositional calculus, the word "axiom" must be used here in a sense broader than the one discussed above. Such a broadening is perfectly feasible. One way to achieve it is to add another condition to the set (III); the new condition could, for instance, be

$$(III\ 7) \qquad As_0t_0 \equiv As_0Ns_0.$$

The effect of this adjunction is to enlarge the original equivalence relation; the new equivalence relation is not the smallest relation satisfying (III 1)–(III 6), but the smallest relation satisfying (III 1)–(III 7). The same purpose can be accomplished by adjoining to the axioms of the propositional calculus the *extra-logical axiom*

$$NAs_0t_0,$$

and then proceeding exactly as before. The result, with either approach, is that each new equivalence class is the union of several old ones. The tautologies, in particular, all belong to the same (new) equivalence class; an element of this equivalence class is usually called a *provable sentence* or a *theorem* of the modified propositional calculus. If there are at least two (new) equivalence classes (in logical language: if the adjoined axioms are consistent), the set \mathbf{A} of all such classes possesses in a natural way the structure of a Boolean algebra, which, in general, is not free.

The "free" procedure for constructing non-free Boolean algebras has its group-theoretic parallel. One way to ensure that the generators of a group satisfy certain prescribed relations is to build those relations into the equivalence by means of which the quotient system (S^* modulo \equiv) is formed. The disadvantage

of such a procedure is that it is repetitious; it uses the method of an earlier construction instead of its result. It is more usual, and algebraically more satisfactory, to apply the combinatorial method only once; thereafter, all groups defined by generators and relations are constructed by forming a quotient group of one of the free groups already obtained. This works very smoothly; the main reason it works is that every group is a quotient group of a free group.

Since, similarly, every Boolean algebra is a quotient algebra of a free Boolean algebra, the group-theoretic shortcut is available for Boolean algebras too. Just as in the theory of groups, moreover, the core of the idea is applicable to algebras that are not necessarily free. It makes sense (and it is often useful) to force the elements of a Boolean algebra (or group) to satisfy some relations, even if the algebra (or group) is not free to start with. A well-known example is the process of reducing a group by its commutator subgroup and thereby forcing it to become abelian.

7. Filters and ideals. From the point of view of logic, the reduction of Boolean algebras is connected with the theory of provability. It turns out that from the point of view of algebraic logic the most useful approach to that theory is not to ask "What is a proof?" or "How does one prove something?" but to ask about the structure of the set of provable propositions. Suppose, therefore, that \mathbf{A} is a Boolean algebra, whose elements are to be thought of, intuitively speaking, as the propositions of some theory, and suppose that a non-empty subset \mathbf{P} of \mathbf{A} has been singled out somehow; the elements of \mathbf{P} are to be thought of as the provable propositions of the theory. Common sense suggests that if s and t are provable sentences, then " s and t " is a provable sentence, and if s is a provable sentence, then " s or t " is a provable sentence, no matter what the sentence t may be. In order to meet these demands of common sense, the set \mathbf{P} cannot be arbitrary; it must be such that if both p and q belong to \mathbf{P} , then $p \wedge q$ belongs to \mathbf{P} , and if p belongs to \mathbf{P} , then $p \vee q$ belongs to \mathbf{P} for all q in \mathbf{A} . If a non-empty subset of a Boolean algebra satisfies these conditions, it is called a *filter*. An illuminating comment is this: a necessary and sufficient condition that a subset \mathbf{P} of a Boolean algebra be a filter is that $1 \in \mathbf{P}$ (i.e., all tautologies are provable), and that if $p \in \mathbf{P}$ and $(p \rightarrow q) \in \mathbf{P}$ (recall that $(p \rightarrow q) = (p' \vee q)$), then $q \in \mathbf{P}$ (i.e., *modus ponens* is a rule of inference).

A filter is not a commonly encountered mathematical object, but one of its first cousins (namely, an ideal) is known to every mathematician. A non-empty subset \mathbf{M} of a Boolean algebra is an *ideal* (for occasional emphasis, a *Boolean ideal*) if it contains $p \vee q$ whenever it contains both p and q and if it contains $p \wedge q$ whenever it contains p . Although it looks slightly different, this definition is, in fact, equivalent to the usual one; a Boolean algebra is, after all, a ring, and a Boolean ideal in the present sense is the same as an ordinary algebraic ideal.

Each of the two concepts (filter and ideal) is, in a certain sense, the Boolean dual of the other. (Some authors indicate this relation by using the term *dual-ideal* instead of filter.) Specifically, if \mathbf{P} is a filter in a Boolean algebra \mathbf{A} , and if

\mathbf{M} is the set of all those elements p of \mathbf{A} for which $p' \in \mathbf{P}$, then \mathbf{M} is an ideal in \mathbf{A} ; the reverse procedure (making a filter out of an ideal) works similarly. This comment indicates the logical role of the algebraically more common concept; just as filters arise in the theory of provability, ideals arise in the theory of refutability. (A proposition p is called refutable if its negation p' is provable.) Duality is so ubiquitous in Boolean theory that every development of that theory (unless it is exactly twice as long as it should be) must make an arbitrary choice between two possible approaches. Logic is usually studied from the “1” approach, *i.e.*, the emphasis is on truth and provability, and, consequently, on filters. Since the dual “0” approach uses the algebraically more natural concept of ideal, the remainder of this exposition (addressed to mathematicians, rather than to professional logicians) will be couched in terms of the logically less pleasant concepts of falsehood and refutability.

8. Boolean logics. The preceding discussion was intended to motivate the following definition. A *Boolean logic* is a pair (\mathbf{A}, \mathbf{M}) , where \mathbf{A} is a Boolean algebra and \mathbf{M} is a Boolean ideal in \mathbf{A} . The elements of \mathbf{A} will be called propositions; the elements of \mathbf{M} will be called refutable propositions. The group-theoretic analogue of this concept (the structure consisting of a group and a specified normal subgroup) has not received very much attention, but it would strike most algebraists as a perfectly reasonable object of study.

The concept of a Boolean logic (\mathbf{A}, \mathbf{M}) has many similarities with the earlier concept of the propositional calculus (S^*, \equiv) . Both objects consist of (1) a set already endowed with some structure, and (2) a congruence relation in that set. (In Boolean theory, as in the rest of algebra, there is a natural one-to-one correspondence between ideals and congruence relations.) It should not be surprising therefore that the “axiomatic” method is the most common way of converting a Boolean algebra into a Boolean logic. In algebraic terms the axiomatic method amounts simply to this: given \mathbf{A} , select an arbitrary subset \mathbf{M}_0 of \mathbf{A} , and let \mathbf{M} be the ideal generated by \mathbf{M}_0 . (Because \mathbf{M} consists of the refutable propositions, not the provable ones, the elements of \mathbf{M}_0 are “anti-axioms”; their negations are axioms in the usual sense.) Even this procedure has its group-theoretic analogue; for an example, recall the usual definition of the commutator subgroup of a group.

Most logical concepts have an algebraic alter-ego definable within the theory of Boolean logics. Two concepts of special importance (consistency and completeness) will be used to illustrate this point.

A Boolean logic (\mathbf{A}, \mathbf{M}) is called *consistent* if for no proposition p in \mathbf{A} are both p and p' provable, or, equivalently, if for no p in \mathbf{A} do both p and p' belong to \mathbf{M} . Since \mathbf{M} is an ideal, it follows that (\mathbf{A}, \mathbf{M}) is consistent if and only if the ideal \mathbf{M} is proper. To say that a Boolean logic is consistent is to say, roughly speaking, that the set of propositions that are refutable in it is not too large.

On intuitive (pragmatic) grounds it is desirable that the set of refutable propositions be not too small. (Recall that there is a natural one-to-one correspondence between refutable propositions and provable propositions.) The

simplest way to ensure that the set of refutable propositions is large enough is to insist that, for every proposition p , either p or p' be refutable. A Boolean logic satisfying this condition is called *complete*. In other words, (\mathbf{A}, \mathbf{M}) is complete if and only if, for every p in \mathbf{A} , either $p \in \mathbf{M}$ or $p' \in \mathbf{M}$.

Inconsistent Boolean logics, *i.e.*, logics of the form (\mathbf{A}, \mathbf{A}) are not very interesting from either the algebraic or the logical point of view. For a consistent logic (\mathbf{A}, \mathbf{M}) , the concept of completeness has an elegant algebraic formulation: the logic is complete if and only if the ideal \mathbf{M} is maximal in the algebra \mathbf{A} . ("Maximal ideal" in such contexts always means "maximal proper ideal.")

If (\mathbf{A}, \mathbf{M}) is a Boolean logic, it is natural to form the quotient system \mathbf{A}/\mathbf{M} . A necessary and sufficient condition that \mathbf{A}/\mathbf{M} be a Boolean algebra is that it have at least two distinct elements, and a necessary and sufficient condition for that is exactly that \mathbf{M} be a proper ideal in \mathbf{A} . On the other hand, a necessary and sufficient condition that (\mathbf{A}, \mathbf{M}) be complete is that \mathbf{A}/\mathbf{M} have at most two distinct elements; if this is so, and if $\mathbf{M} \neq \mathbf{A}$, then $\mathbf{A}/\mathbf{M} = \mathbf{O}$. (Recall that $\mathbf{O} = \{0, 1\}$. On universal algebraic grounds, the condition that a proper ideal \mathbf{M} be maximal in an algebra \mathbf{A} is equivalent to the condition that the quotient algebra \mathbf{A}/\mathbf{M} be *simple*, *i.e.*, that \mathbf{A}/\mathbf{M} have no non-trivial proper ideals. The only simple Boolean algebra is \mathbf{O} .) Conclusion: a necessary and sufficient condition that a Boolean logic (\mathbf{A}, \mathbf{M}) be both consistent and complete is that $\mathbf{A}/\mathbf{M} = \mathbf{O}$.

For a deeper study of concepts such as consistency and completeness additional logical apparatus is needed; some of it is described below. First, a terminological warning. Consistency and completeness, as defined above, are usually called *simple consistency* and *simple completeness*; perhaps *syntactic* would be a more suggestive adjective here than *simple*. The point is that the propositional calculus, for instance, is usually considered to be a "language," and (simple) consistency and completeness are defined in terms of the intrinsic structure (syntax) of that language. Two related concepts, to be discussed below, are defined in terms of a possible external interpretation (meaning) of the language, and are therefore appropriately called *semantic*. The group-theoretic analog of a semantic concept is one that depends on constructions reaching outside the given group, *i.e.*, typically, on representations of the group. Thus, for instance, "characteristic subgroup" is a syntactic concept, while "character" is a semantic one.

In most of what follows it will be simpler to forget about Boolean logics and to consider Boolean algebras instead. The point is that if (\mathbf{A}, \mathbf{M}) is a consistent Boolean logic, then the quotient algebra \mathbf{A}/\mathbf{M} can be formed and can be used to study virtually all the logically important properties of (\mathbf{A}, \mathbf{M}) . Note that if a proposition in \mathbf{A} is refutable, then its image in \mathbf{A}/\mathbf{M} (its equivalence class modulo \mathbf{M}) is equal to 0, and, similarly, if a proposition in \mathbf{A} is provable, then its image in \mathbf{A}/\mathbf{M} is equal to 1. It is, accordingly, convenient to agree that if p is an element of a Boolean algebra, then " p is refutable" shall be a long way of saying " $p=0$," and, similarly, " p is provable" shall be a long way of saying " $p=1$."

9. Quantifiers. Within the framework of Boolean algebras (or logics) it is easy to give an algebraic formulation of the inference from the premises "Some Greeks are men" and "All men are mortal" to the conclusion "Some Greeks are men." This is not a misprint. Within the framework of Boolean algebras alone it is not possible to formulate the inference that allows, from the same premises, the conclusion "Some Greeks are mortal." The desired inference is justified not by manipulating with propositions as a whole, but by the intrinsic structure of its constituents, and, in particular, by a study of what "some" and "all" mean.

The clue is in the consideration of propositional functions. As their name indicates, propositional functions are functions whose values are propositions. If, for instance, for every natural number x , $p(x)$ is the sentence " x is even" and $q(x)$ is the sentence " $2x = 1$," then p and q are propositional functions. (The present discussion is only heuristic, of course, but even so the contrasting use of "sentence" and "proposition" needs a little justification. The justification is a very common one in mathematics; it is convenient, though incorrect, to identify an equivalence class with a representative element. Recall that a proposition was defined above as an equivalence class of sentences. The solecism is the same as the one every analyst commits when he speaks of an element of L_2 as a function.) From the algebraic point of view, a propositional function is a function defined on an arbitrary non-empty set with values in a Boolean algebra.

To single out a particular theory for logical examination means, algebraically, to fix a Boolean algebra \mathbf{B} . If, in addition, a certain non-empty set X is selected, then the ground is prepared for a discussion of propositional functions. (Intuitively the elements of X may be thought of as the objects that the propositions of the theory talk about.) The set \mathbf{A} of all functions from X to \mathbf{B} is in a natural way a Boolean algebra (pointwise operations), and the same is true of many of its subsets. The constant functions (*i.e.*, the functions p obtained by selecting an element p_0 in \mathbf{B} and writing $p(x) = p_0$ for every x in X) constitute a subalgebra of the algebra \mathbf{A} ; that subalgebra is obviously isomorphic to \mathbf{B} . In other words, the propositions of a theory are (or, rather, may be identified with) particular propositional functions of that theory.

What is the effect of "some" in a sentence such as "for some x , x is even"? (It is understood here that the underlying set X is the set of natural numbers; the value-algebra \mathbf{B} has not been, and need not be, specified). The most striking effect it has is to convert a propositional function into a constant, or, *via* the identification convention of the preceding paragraph, into a constant function. This effect is analogous to the effect of "sup" in " $\sup_x f(x)$ " and to the effect of " $\int_0^1 \dots dx$ " in " $\int_0^1 f(x)dx$ " (where the function f is, say, a real-valued continuous function defined on the closed unit interval). Accordingly, the algebraic analogue of "some" ought to be a mapping that sends a certain Boolean algebra (propositional functions) into a certain subalgebra (constant functions). Such a mapping (usually denoted by \exists) is indeed at the basis of the theory of propositional functions.

It is now wise to abstract from the motivation. Consider a perfectly arbitrary Boolean algebra \mathbf{A} , and let \exists be a mapping of \mathbf{A} into itself. If \mathbf{A} were an algebra of propositional functions, and if \exists were the operator "some," then, presumably, \exists would satisfy some rather special conditions; the problem now is to find a reasonable list of conditions that characterize such a special \exists . This is easy; here are some of them:

- (Q 1) $\exists 0 = 0,$
 (Q 2) $p \leq \exists p,$
 (Q 3) $\exists(p \vee q) = \exists p \vee \exists q,$
 (Q 4) $\exists \exists p = \exists p.$

(In these conditions, and also in (Q 5) below, p and q are arbitrary elements of \mathbf{A}). The intuitive grounds for the conditions are easy to see. Suppose, for instance, that $q(x)$ is " $2x = 1$ "; here, once more, \mathbf{A} is to be thought of as an algebra of propositional functions whose domain is the set of natural numbers. Since in all reasonable theories of the arithmetic of natural numbers the sentence " $2x = 1$ " is refutable, each value of the propositional function q is refutable, and therefore (in accordance with the agreement concerning the reduction of Boolean logics to Boolean algebras) the propositional function q is equal to the constant function 0. The same considerations apply to the sentence "for some x , $2x = 1$ " and thus serve to complete the illustration of (Q 1). The remaining conditions (Q 2), (Q 3), and (Q 4) are illustrated similarly. In intuitive terms, (Q 2) says that each value of p implies that "for some x , $p(x)$ "; the construction of analogous readings of (Q 3) and (Q 4) is left as an exercise to the reader.

It is amusing to observe that (except for notation) the conditions (Q 1)–(Q 4) are well-known to most mathematicians (but in a very different context). They are, all but verbatim, the Kuratowski axioms for a closure operator on a topological space. They do not, however, serve to characterize the "some" operator; in technical language, the theory of closure algebras is not co-extensive with the monadic functional calculus. Another glance at the conditions as they now stand should arouse the suspicion that something is missing; the trouble is that they relate \exists to \vee only (0 and \leq can be defined in terms of \vee), and say nothing about the relation of \exists to either \wedge or $'$. The missing condition is this:

$$(Q 5) \quad \exists(\exists p)' = (\exists p)'.$$

In intuitive terms, (Q 5) serves as at least a partial reminder of the fact that the constant functions form a Boolean algebra (so that, in particular, they are closed under complementation), and that "some" applied to a constant function has no effect.

[Two remarks are in order. (1) The conditions (Q 1)–(Q 5) are equivalent to a shorter set, namely to (Q 1), (Q 2), and

$$(Q 6) \quad \exists(p \wedge \exists q) = \exists p \wedge \exists q.$$

The proof of this equivalence is just axiom-chopping. The longer set was selected for presentation here because of its greater intuitive content. (2) The motivation of (Q 1)–(Q 5), and also of (Q 6), could have been, and sometimes is, based on quasi-geometric considerations, involving the formation of (possibly infinite) Boolean suprema. The didactic danger of this motivation is its emphasis on the intuitive idea that “some” is just an infinite “or.” The idea is not wholly unsound, but real progress in algebraic logic was achieved only after the realization that \exists is really a unary operation, not an infinitary one.]

The way is now clear to a precise definition: an *existential quantifier* is a mapping \exists of a Boolean algebra into itself satisfying the conditions (Q 1)–(Q 5). Dually, a *universal quantifier* is a mapping \forall of a Boolean algebra into itself satisfying the conditions

- (Q' 1) $\forall 1 = 1,$
 (Q' 2) $\forall p = p,$
 (Q' 3) $\forall(p \wedge q) = \forall p \wedge \forall q,$
 (Q' 4) $\forall \forall p = \forall p,$
 (Q' 5) $\forall(\forall p)' = (\forall p)'.$

It is easy to see that \forall bears the same relation to the intuitive “all” as \exists bears to “some.”

There is a very close connection between existential quantifiers and universal ones: if \exists is an existential quantifier on, say, a Boolean algebra \mathbf{A} , and if a mapping \forall of \mathbf{A} into itself is defined by

$$\forall p = (\exists p')',$$

then \forall is a universal quantifier on \mathbf{A} ; if, in reverse, a universal quantifier \forall is given, and if \exists is defined by

$$\exists p = (\forall p')',$$

then \exists is an existential quantifier. (“Always p ” is the same as “not sometimes not p ,” and “sometimes p ” is the same as “not always not p ”). The thoroughgoing symmetry of this situation justifies an asymmetric treatment; anything that can be said about an \exists has an obvious dual about an \forall , and it is therefore sufficient to discuss in detail only one of these two objects. In what follows \exists will be given preferred treatment, and, in fact, the word “quantifier” will be used from now on in the sense of “existential quantifier.” (This is in line with the algebraists preference for ideals instead of filters; the dual of an algebraist would select \forall for preferred treatment.) Universal quantifiers, whenever they must be considered, will always be given their full name.

10. Monadic algebras. Once the concept of a quantifier is at hand, it is immediately possible to generalize the concept of a Boolean algebra in a manner adapted to an algebraic answer to the question of why some Greeks are mortal. Technically the generalized algebras (called monadic algebras) play an inter-

mediate role; they are slightly more useful than Boolean algebras, but not nearly so useful as certain even more general algebras (the polyadic algebras that will be described a little later). Psychologically and historically, however, the intermediate generalization has some value. Its psychological value is that it exhibits in a simplified form some of the curious properties of its generalized version; its historical value is that it puts into a modern algebraic context the oldest known systematic treatment of logic, namely Aristotle's syllogistics.

A *monadic* (Boolean) *algebra* is a pair (\mathbf{A}, \exists) , where \mathbf{A} is a Boolean algebra and \exists is a quantifier on \mathbf{A} . (The word "monadic" serves as a reminder of the one additional operation that distinguishes monadic algebras from Boolean algebras.) The elementary theory of monadic algebras is a routine matter; subalgebras, homomorphisms, ideals, and similar universal algebraic concepts (with a qualifying "monadic" when clarity demands it) are defined in a completely unsurprising manner. Free monadic algebras can be defined and studied (if desired) by the techniques used in the study of free Boolean algebras; the analogue of the propositional calculus is called the *monadic functional calculus*.

The concept of a monadic logic arises naturally in connection with the theory of provability and refutability in the monadic functional calculus: a *monadic logic* is a pair (\mathbf{A}, \mathbf{M}) , where \mathbf{A} is a monadic algebra (with quantifier \exists , say) and \mathbf{M} is a monadic ideal in \mathbf{A} . (It is convenient here, as in other parts of algebra, to be mildly forgetful of the completely rigorous definitions, and, accordingly, to identify a monadic algebra with the underlying Boolean algebra. If this were not done, a monadic logic would have to be denoted by a symbol such as $((\mathbf{A}, \exists), \mathbf{M})$.) The fact that a monadic ideal is a Boolean ideal invariant under the application of \exists corresponds to the logical fact that if p is a refutable propositional function, then $\exists p$ is also refutable.

To discuss the (simple, or syntactic) consistency and completeness of Boolean logics, it is desirable to introduce a new term: an element p of a monadic algebra will be called *closed* if $\exists p = p$. Intuitively, closed propositions correspond to what were called constant functions before, or, in other words, to propositions instead of propositional functions. There is a natural way of associating a Boolean logic $(\mathbf{A}_0, \mathbf{M}_0)$ with every monadic logic (\mathbf{A}, \mathbf{M}) ; the algebra \mathbf{A}_0 is the set of all closed elements of \mathbf{A} and the ideal \mathbf{M}_0 is the intersection of \mathbf{M} with \mathbf{A}_0 . A monadic logic (\mathbf{A}, \mathbf{M}) is called syntactically consistent (or complete) if the associated Boolean logic $(\mathbf{A}_0, \mathbf{M}_0)$ is consistent (or complete).

Why is it necessary to modify the Boolean definitions of consistency and of completeness for the monadic situation? Consistency could conceivably be defined by the requirement that for no p in \mathbf{A} should both p and p' belong to \mathbf{M} , and, similarly, completeness could be defined by the requirement that for every p in \mathbf{A} either p or p' should belong to \mathbf{M} . What is wrong with these definitions? The answer is that there is nothing wrong as far as consistency is concerned, and very much is wrong as far as completeness is concerned. The alternative definition of consistency is equivalent to the one officially adopted above, but the alternative definition of completeness is out of harmony with both the official

definition and common sense. If, as in some previous examples, $p(x)$ is “ x is even,” then it is not at all reasonable to demand of a logic sufficient power to settle the provability or refutability of the propositional function p . The sentences “for some x , x is even” and “for all x , x is even” are closed; a reasonable logical theory of arithmetic should declare each of them to be either provable or refutable. The function p , however, is not a sentence; common sense demands that both it and its negation should fail to be either provable or refutable.

11. Syllogisms. The discussion of monadic algebras and logics up to this point was merely an adaptation of the corresponding discussion of Boolean facts. Some progress has been made, nevertheless; monadic logics (unlike Boolean logics) contain the general theory of syllogisms. For an example, consider again the premises “Some Greeks are men” and “All men are mortal,” and consider the desired conclusion “Some Greeks are mortal.” To make an algebraic model of the situation, let X be an appropriate set and let \mathbf{B} be an appropriate Boolean algebra of propositions about the elements of X . The set X , for instance, could be the set of all animals, and \mathbf{B} could be an algebra containing, for each x in X , the propositions “ x is Greek,” “ x is a man,” and “ x is mortal.” (This description is, of course, much too colloquial for complete precision, but there is no difficulty at all in converting it into honest mathematics.) If these propositions are denoted by $p(x)$, $q(x)$, and $r(x)$, respectively, and if \mathbf{A} is the algebra of all propositional functions such as p , q , and r , then \mathbf{A} (with the intuitively obvious “some” quantifier in the role of \exists) is a monadic algebra suitable for the study of the inference described above. The first premise is $\exists(p \wedge q)$, the second premise is $\forall(q \rightarrow r)$, and the conclusion is $\exists(p \wedge r)$. (The universal quantifier \forall here is the natural dual of the given existential quantifier \exists .) The algebraic justification of the inference is that if \mathbf{A} is the monadic algebra of a monadic logic such that both premises belong to the filter of provable propositions, then the conclusion also belongs to that filter.

There is a special aspect of the theory of syllogisms that still remains to be converted into algebra; it is exemplified by the classical premises “Socrates is a man” and “All men are mortal,” together with the conclusion “Socrates is mortal.” In highly informal language, the trouble with this syllogism is that the algebraic theory (so far) is equipped to deal with generalities only, and is unable to say anything concrete; Socrates, however, is a concrete individual entity. The preceding paragraph shows that a monadic algebra can be taught to say “All men are mortal.” The reason is that “manhood” can easily be thought of as an element of a monadic algebra, since it is the obvious abstraction of the propositional function whose value at each point x of some set is “ x is a man.” Socrates, on the other hand, is a “constant,” and there is no immediately apparent way of pointing to him. (The use of the word “constant” here and below is quite different from its earlier use in the phrase “constant function.” The important concept now is what logicians call an individual constant.) A classical artifice, designed to deal with just this difficulty, is to promote Socrates to a propositional function, *i.e.*, to identify him with the function whose value at x is

" x is Socrates." This procedure is both intuitively and algebraically artificial; Socrates should not be a propositional function but a possible argument of such functions.

To find the proper algebraization of the concept of a constant it is necessary only to recall that the elements of a monadic algebra are abstractions of the concept of a propositional function, and to determine the algebraic effect of replacing the argument of such a function by some fixed element of its domain. If p is a propositional function with domain X , and if $x_0 \in X$, then $p(x_0)$ is a proposition, or, *via* the obvious identification convention, a propositional function with only one value. The mapping $p \rightarrow p(x_0)$ (the evaluation map induced by x_0) clearly preserves the Boolean operations (*i.e.*, suprema, infima, and complements). If the function p itself has only one value (equivalently, if $p = \exists q$ for some q), then that value is $p(x_0)$, *i.e.*, the mapping leaves the range of \exists element-wise fixed. If, on the other hand, \exists is applied to the (constant) function $p(x_0)$, the result is the same function, *i.e.*, \exists leaves the range of the mapping element-wise fixed. These considerations motivate the following general definition: a *constant* of a monadic algebra \mathbf{A} is a Boolean endomorphism c of \mathbf{A} such that

$$c\exists = \exists \quad \text{and} \quad \exists c = c.$$

This definition is applicable to the mortality of Socrates. If, as before, q is manhood and r is mortality, and if Socrates is taken to be a constant, say c , of a monadic algebra containing q and r , then the algebraic justification of the classical syllogism is this: if \mathbf{A} is the monadic algebra of a monadic logic such that both $\forall(q \rightarrow r)$ and cq belong to the filter of provable propositions, then cr also belongs to that filter.

Constants are much more important than their more or less casual introduction above might indicate; the concept of a constant (suitably generalized to the polyadic situation) is probably the most important single concept in algebraic logic. This should not be too surprising; in the intuitive interpretation, the constants of a theory constitute, after all, the subject matter that the propositions of the theory talk about. Algebraically constants play a crucial role in the representation theory of monadic (and polyadic) algebras.

12. Quantifier algebras. The theory of propositional functions of only one variable (and of their abstract algebraic counterparts) is as insufficient for the understanding of logic and its applications as the theory of ordinary numerical functions of one variable is insufficient for the understanding of calculus. Mathematics contains not only sentences of the form " x is positive," but also sentences such as " x is less than y " and " x is between y and z ." Although a mathematician with no training in modern logic is likely to be suspicious when he is told that syllogisms are not enough for mathematics, the basis of that assertion is nothing more profound or esoteric than the need to consider propositional functions of several variables. This is all that DeMorgan meant when he said that the scholastics, after two millennia of Aristotelean tradition, were still unable to prove that if a horse is an animal, then a horse's tail is an animal's tail.

Suppose, to begin modestly, that one wants to study propositional functions of three variables. The most immediately apparent new phenomenon is the possibility of partial quantification: the theory must be able to treat sentences of the form "there is an x_1 and there is an x_3 , such that $p(x_1, x_2, x_3)$." (Here, as before, it is enough to discuss existential quantifiers; the corresponding theory of universal quantifiers is obtained by a simple dualization.) Another way of expressing the phenomenon is to say that the appropriate algebraic system must possess not one quantifier but many. What appears to be going on is this: if I is the set of relevant indices, so that $I = \{1, 2, 3\}$ in the present example, then there is a quantifier (*i.e.*, an existential quantifier) corresponding to each subset (*e.g.*, to $\{1, 3\}$) of the set I . If $\exists(J)$ is the quantifier corresponding to the subset J of I , then, of course, the way that $\exists(J)$ depends on J should be specified. The example shows the way. If J is empty, then prefixing $\exists(J)$ to p should produce no change in p , and if both J and K are subsets of I , then prefixing $\exists(J)$ and $\exists(K)$ to p , in either order, should have the same effect as prefixing the quantifier corresponding to the union of J and K .

The preceding paragraph suggests the definition of an algebraic system, which, however, turns out to fall far short of what is needed. It is worth a brief look anyway. Call a *quantifier algebra* a triple (\mathbf{A}, I, \exists) , where \mathbf{A} is a Boolean algebra, I is a set, and \exists is a function from subsets of I to quantifiers on \mathbf{A} such that

$$(\exists 1) \quad \exists(\emptyset)p = p$$

whenever $p \in \mathbf{A}$, and

$$(\exists 2) \quad \exists(J)\exists(K) = \exists(J \cup K)$$

whenever J and K are subsets of I . In analogy with logical usage, an element of the set I will be called a *variable* (or, in more detail, an *individual variable*) of the quantifier algebra (\mathbf{A}, I, \exists) . Caution: a variable, in this sense, does not vary at all; it merely serves as a reminder of the place into which a "variable," in the intuitive sense, could be substituted, if, that is, the elements of \mathbf{A} were propositional functions and not elements of a quite abstract Boolean algebra.

The concept of a quantifier algebra is a proper generalization of the concept of a monadic algebra; a quantifier algebra (\mathbf{A}, I, \exists) for which the set I of variables consists of exactly one element may be identified with the monadic algebra $(\mathbf{A}, \exists(I))$. The *degree* of a quantifier algebra is defined to be the cardinal number of the set of its variables; the last comment says that quantifier algebras of degree 1 are essentially the same as monadic algebras. It is crucial for applications to permit the consideration of quantifier algebras of infinite degree. While, to be sure, each particular propositional function that is likely to arise has only finitely many arguments, the number of arguments in a reasonably extensive theory (*e.g.*, in mathematics) is not likely to be bounded. To keep the generalization from running away with itself, it is often advisable to restrict the study of quantifier algebras to the locally finite case. The quantifier algebra (\mathbf{A}, I, \exists) is

called *locally finite* if to every element p of \mathbf{A} there corresponds a finite subset J of I such that $\exists(I - J)p = p$; this is the abstract formulation of the concrete promise that no propositional function under consideration will actually depend on infinitely many variables.

13. Polyadic algebras. The reason that quantifier algebras are an inefficient logical tool is that they do not allow the discussion of transformations of variables. Consider, for instance, a sentence of the form "if $p(x_1, x_2)$ and $p(x_2, x_1)$, then $x_1 = x_2$." Such sentences usually occur in the definition of a partial order; they indicate the need for discussing the passage from $p(x_1, x_2)$ to $p(x_2, x_1)$. For a more complicated example of the same type consider the problem of converting $p(x_1, x_2, x_3, x_4)$ into $p(x_4, x_4, x_1, x_3)$. There is no way of describing such conversions in terms of Boolean operations and quantifications alone; the best way of incorporating them into the general theory is by postulating them outright. What appears to be going on is this: to every transformation τ on I (i.e., to every mapping of the set I into itself) there corresponds a mapping, say $\mathbf{S}(\tau)$, of the set of propositional functions under consideration into itself. The mappings $\mathbf{S}(\tau)$ preserve the Boolean operations (i.e., they are Boolean endomorphisms). If τ is the identity transformation on I (to be denoted by δ), then $\mathbf{S}(\tau)$ leaves every p invariant; if both σ and τ are transformations on I , then the effect of $\mathbf{S}(\sigma)$ on $\mathbf{S}(\tau)p$ is the same as the effect of $\mathbf{S}(\sigma\tau)$ on p .

In analogy with quantifier algebras, it is possible to define a *transformation algebra* as a triple $(\mathbf{A}, I, \mathbf{S})$, where \mathbf{A} is a Boolean algebra, I is a set, and \mathbf{S} is a function from transformations on I to Boolean endomorphisms on \mathbf{A} , such that

$$(\mathbf{S} \ 1) \qquad \mathbf{S}(\delta)p = p$$

whenever $p \in \mathbf{A}$, and

$$(\mathbf{S} \ 2) \qquad \mathbf{S}(\sigma)\mathbf{S}(\tau) = \mathbf{S}(\sigma\tau)$$

whenever σ and τ are transformations on I .

Neither quantifier algebras nor transformation algebras are of much logical significance; the important concept is one that possesses both structures at the same time. It is a matter of universal algebraic experience, however, that it is not enough to impose two different structures on the same set; in order to get a usable theory, it is necessary to describe the compatibility conditions that relate the two structures to each other. (A topological group is not merely a set that is simultaneously a group and a topological space.) The appropriate conditions are discovered by experimentation with the special structures that the theory is intended to generalize; their final justification is their success. To examine here the experimentation that led to the definition of polyadic algebras would be more boring than profitable; suffice it to report the results. A *polyadic (Boolean) algebra* is a quadruple $(\mathbf{A}, I, \mathbf{S}, \exists)$ subject to the following conditions: (i) $(\exists \ 1)$ and $(\exists \ 2)$ hold, or, more precisely, (\mathbf{A}, I, \exists) is a quantifier algebra, (ii) $(\mathbf{S} \ 1)$ and $(\mathbf{S} \ 2)$ hold, or, more precisely, $(\mathbf{A}, I, \mathbf{S})$ is a transformation algebra, and (iii)

$$(3S\ 1) \quad \mathbf{S}(\sigma)\mathfrak{I}(J) = \mathbf{S}(\tau)\mathfrak{I}(J)$$

whenever J is a subset of I and σ and τ are transformations on I such that $\sigma i = \tau i$ for all i in $I - J$, and

$$(3S\ 2) \quad \mathfrak{I}(J)\mathbf{S}(\tau) = \mathbf{S}(\tau)\mathfrak{I}(\tau^{-1}J)$$

whenever J is a subset of I and τ is a transformation on I such that two distinct elements of I are never mapped by τ onto the same element of J .

The conditions (3S 1) and (3S 2) were recorded here for the sake of completeness only; no technical use will be made of them in this merely descriptive report. It is perhaps worth remarking though that they (or, rather, the provisos that accompany them) are not so complicated as they seem on first sight. What they amount to is a condensation of the usual and intuitively obvious relations between quantifications and transformations. Suppose, for example, that i and j are distinct elements of I ; let J be the singleton $\{i\}$ and let τ be the transformation that maps i onto j and everything else (including j itself) onto itself. Since τ agrees with δ outside J , it follows from (3S 1) that $\mathbf{S}(\tau)\mathfrak{I}(J) = \mathfrak{I}(J)$; this equation corresponds to the familiar fact that once a variable has been quantified, the replacement of that variable by another one has no further effect. To get another example, note, for the same τ and J , that $\tau^{-1}J = \emptyset$. It follows from (3S 2) that $\mathfrak{I}(J)\mathbf{S}(\tau) = \mathbf{S}(\tau)$; this equation corresponds to the familiar fact that once a variable has been replaced by another one, a quantification on the replaced variable has no further effect.

[Polyadic algebras stand in the same relation to the so-called *pure* first-order functional calculus as do Boolean algebras to the propositional calculus. The simplest example of an *applied* functional calculus is one that is equipped to discuss the concept of equality. By a suitable adaptation of standard logical methods, such applied calculi can be treated within the framework of polyadic algebras; the details are of no relevance here. What should be mentioned, however, is that there is another way of algebraizing the functional calculus with equality, namely, *via* Tarski's concept of a cylindric algebra. Roughly speaking, a cylindric algebra is a quantifier algebra together with certain distinguished elements; the distinguished elements play the role of sentences that assert equations among variables. The theory of cylindric algebras is an efficient algebraic tool for studying calculi with equality. The exact relations between polyadic algebras and cylindric algebras are of considerable technical interest; they are still in the process of being clarified. It is already known, however, that in most important cases the two concepts are equivalent. The way that transformations enter into the theory of cylindric algebras is an ingenious trick; the idea is that to say " $p(x_1, x_1)$ " is the same as to say "there is an x_2 such that $p(x_1, x_2)$ and $x_2 = x_1$."]

14. Semantic concepts. The discussion of polyadic logics and their syntactic consistency and completeness proceeds in a straightforward manner. A *polyadic logic* is a pair (\mathbf{A}, \mathbf{M}) , where \mathbf{A} is a polyadic algebra and \mathbf{M} is a polyadic ideal in

A. An element p of a polyadic algebra \mathbf{A} is called *closed* if $\exists(I)p = p$ (where I , of course, is the set of variables of \mathbf{A}). Just as for monadic logics, there is a natural way of associating a Boolean logic $(\mathbf{A}_0, \mathbf{M}_0)$ with every polyadic logic (\mathbf{A}, \mathbf{M}) ; the algebra \mathbf{A}_0 is the set of all closed elements of \mathbf{A} and the ideal \mathbf{M}_0 is the intersection of \mathbf{M} with \mathbf{A}_0 . A polyadic logic (\mathbf{A}, \mathbf{M}) is called syntactically consistent (or complete) if the associated Boolean logic $(\mathbf{A}_0, \mathbf{M}_0)$ is consistent (or complete).

All this is pretty routine stuff by now. The element of novelty is in the study of the "semantic" theory of polyadic logics, *i.e.*, in the study of "interpretations" of a logic in a "model" and in the study of "truth" and "validity." (It must be admitted that these concepts could have been introduced in connection with Boolean logics and monadic logics also. Since, however, in those simple situations, they exhibit the deceptive simplicity of a degenerate case, their premature study would have been more confusing than helpful.) The natural habitat of semantic theories is situated somewhere near a polyadic *logic*, but the machinery for examining such a theory is easier for a polyadic *algebra*. The reduction of (syntactically consistent) logics to algebras is an easy step: if $\mathbf{M} \neq \mathbf{A}$, then \mathbf{A}/\mathbf{M} can be formed and can be used to study (\mathbf{A}, \mathbf{M}) . (This kind of thing was done before; *cf.* the corresponding discussion in the Boolean case.) Some concepts disappear in the passage from (\mathbf{A}, \mathbf{M}) to \mathbf{A}/\mathbf{M} and others take on an interesting new guise. Thus, for instance, to say that a polyadic algebra is (syntactically) consistent is to say merely that it is there; on the other hand, to say that a polyadic algebra is (syntactically) complete is to say that it is simple. (Just as for Boolean logics, it turns out that a polyadic logic (\mathbf{A}, \mathbf{M}) , with $\mathbf{M} \neq \mathbf{A}$, is syntactically complete if and only if the polyadic ideal \mathbf{M} is a maximal ideal in the polyadic algebra \mathbf{A} .)

The usual way to describe a model is this: take a non-empty set X , interpret the variables (*i.e.*, the elements of I) as variables (in the intuitive sense) varying over X , and interpret the elements of \mathbf{A} as propositional functions on an appropriate Cartesian power of X with values that are either true or false. This is somewhat vague; a slight change in language converts it, however, into an algebraically precise and clean definition. If X is a non-empty set and if I is an arbitrary set, the set of all functions from the Cartesian product X^I into the Boolean algebra \mathbf{O} possesses in a natural way the structure of a polyadic Boolean algebra; a *model* is, by definition, a polyadic subalgebra of such a total functional algebra.

Once the concept of a model is known, the definitions of the remaining semantic concepts are automatic. The purpose of the following paragraphs is first to define the usual semantic concepts and then to examine their algebraic significance.

An *interpretation* of a polyadic algebra $(\mathbf{A}, I, \mathbf{S}, \exists)$ in a model is a polyadic homomorphism from \mathbf{A} onto the model. An element p of \mathbf{A} is *true* in an interpretation f if $fp = 1$; if $fp = 0$, then p is *false* in the interpretation. (Caution: fp is a function from X^I into \mathbf{O} and is therefore not necessarily either 0 or 1. To say that p is true for f means that the image fp of p under f is the constant function

whose value is 1.) An element p of \mathbf{A} is *valid* if it is true in every interpretation; if p is false in every interpretation, then p is called *contravalid*. An element p of \mathbf{A} is *satisfiable* if there is an interpretation for which it is not false (i.e., if p is not contravalid).

The algebra \mathbf{A} is *semantically consistent* if it has an interpretation in a model. The definition of semantic completeness requires a little more motivation. It is a trivial consequence of the definition of Boolean homomorphism (sometimes even built in as part of the definition) that the unit element of \mathbf{A} is always valid, and, dually, that the zero element is always contravalid; in logical terms this says that provable propositions are valid, and refutable ones are contravalid. (The assumption of syntactic consistency is usually, and quite properly, made explicit at this point. In the present discussion, dealing with algebras instead of logics, the role of that assumption is played by the fact that \mathbf{A} is an algebra at all, or, in more detail, that \mathbf{A} has a unit element distinct from zero.) Semantic completeness requires the converse assertions; the algebra \mathbf{A} is *semantically complete* if the unit is the only valid element, or, equivalently, if every non-zero element is satisfiable. In logical terms these requirements say that everything valid is provable, or, equivalently, that everything that is not refutable is satisfiable.

All the preceding definitions are based on one of them, namely, on the definition of a model. The situation can be better understood if it is first generalized and then specialized in a new direction. A model was defined as an element of a certain particular class of polyadic algebras, but, in the subsequent definitions, no special properties of that class were used. Those definitions, in other words, are relative to the prescribed class \mathfrak{M} of models, and to nothing else; a significant generalization of them is obtained if \mathfrak{M} is replaced by an arbitrary class \mathcal{C} of algebras. The concepts so obtained may be referred to by using \mathcal{C} as a prefix, so that expressions such as “ \mathcal{C} -interpretation” and “ \mathcal{C} -valid” now make sense. (Only in case $\mathcal{C} = \mathfrak{M}$ may the prefix be omitted.) An interesting specialization is obtained by letting the class \mathcal{S} of all simple algebras play the role of \mathcal{C} . The discussion that follows will be in terms of \mathcal{S} rather than \mathfrak{M} ; the vitally important relation between \mathcal{S} and \mathfrak{M} will be treated afterward.

To say that an algebra \mathbf{A} is *semantically \mathcal{S} -consistent* means, by definition, that there exists a homomorphism from \mathbf{A} onto a simple algebra. This, in turn, is equivalent, on universal algebraic grounds, to the existence of a maximal ideal in \mathbf{A} . The problem of the existence of maximal ideals is well known in algebra; the cases in which the solution is affirmative can usually be settled by a straightforward application of Zorn's lemma. The theory of polyadic algebras is one of these pleasant cases; Zorn's lemma applies and proves that maximal ideals always do exist. In other words, every polyadic algebra is (semantically) \mathcal{S} -consistent. The situation is reminiscent of syntactic consistency, and, in fact, it turns out that the two concepts are the same. It is profitable to return (but just for a moment) to logics instead of algebras. Recall that a logic (\mathbf{A}, \mathbf{M}) is syntactically consistent if and only if \mathbf{M} is a proper ideal in \mathbf{A} . The general definition

of semantic \mathcal{C} -consistency for a logic (\mathbf{A}, \mathbf{M}) requires the existence of an algebra \mathbf{C} in the class \mathcal{C} and the existence of a homomorphism f from \mathbf{A} onto \mathbf{C} such that $fp = 0$ whenever $p \in \mathbf{M}$. If \mathcal{C} is \mathcal{S} , then this is equivalent to the requirement that \mathbf{M} be included in some maximal ideal. Since Zorn's lemma can be used to show not only that maximal ideals exist, but that, in fact, every proper ideal is included in some maximal ideal, syntactic consistency and semantic \mathcal{S} -consistency are the same whether they are approached *via* logics (\mathbf{M} is a proper ideal) or *via* algebras (\mathbf{A} is a non-degenerate algebra).

To say that an algebra \mathbf{A} is semantically \mathcal{C} -complete means, by definition, that for every non-zero element p of \mathbf{A} there exists an algebra \mathbf{C} in the class \mathcal{C} and there exists a homomorphism f from \mathbf{A} onto \mathbf{C} such that $fp \neq 0$. In this formulation \mathcal{C} -completeness may not look familiar even to a professional algebraist; an easy argument serves, however, to prove that the definition is equivalent to one that is very well known indeed. The fact is that \mathbf{A} is \mathcal{C} -complete if and only if \mathbf{A} is a *subdirect sum* of algebras belonging to the class \mathcal{C} . The argument (and even the definition of subdirect sum) will be omitted here; they are mentioned only to show that the concept (\mathcal{C} -completeness for an arbitrary \mathcal{C}) does fit into the framework of algebra.

In view of the relation between maximal ideals on the one hand and homomorphisms onto simple algebras on the other hand, the definition of semantic \mathcal{S} -completeness for an algebra \mathbf{A} reduces to this: to every non-zero element of \mathbf{A} there corresponds a maximal ideal not containing it. Equivalently: the intersection of all the maximal ideals of \mathbf{A} is the singleton $\{0\}$. This too is a well-known algebraic phenomenon. In analogy with some other parts of algebra, a polyadic algebra will be called *semisimple* if the intersection of all its maximal ideals is trivial; the result is that a polyadic algebra is \mathcal{S} -complete if and only if it is semisimple, or, equivalently, if and only if it is a subdirect sum of simple algebras.

15. The Gödel theorems. The title of this paper promised a discussion of the basic concepts of algebraic logic, and indeed the definitions of the basic *concepts* were emphasized much more than the basic *results* concerning them. As a partial rectification of this unbalanced state of affairs the present (concluding) section is devoted to the statement of two of the deepest theorems of the field. The original formulations and proofs of these justly celebrated theorems are due to Gödel; the results are known as the Gödel completeness theorem and the Gödel incompleteness theorem.

The word "completeness" in "completeness theorem" refers to semantic completeness. The algebraic statement of the theorem is short and elegant: *every locally finite polyadic algebra of infinite degree is semantically complete* (or, equivalently, \mathfrak{M} -complete). The crux of the proof is a characterization of simple polyadic algebras. It is very easy to see that every model is a simple algebra; the hard thing to prove is that, conversely, every simple, locally finite polyadic algebra of infinite degree is (isomorphic to) a model. The proof makes use of the polyadic generalization of what was called a "constant" of a monadic algebra.

In terms of the symbols used above, the easy fact is that $\mathfrak{M} \subset \mathfrak{S}$ and the hard one is that (in the presence of local finiteness and infinite degree) $\mathfrak{S} \subset \mathfrak{M}$. In view of the equation $\mathfrak{S} = \mathfrak{M}$, semantic completeness (*i.e.*, \mathfrak{M} -completeness) is the same as \mathfrak{S} -completeness, and, consequently, the Gödel completeness theorem implies that every locally finite polyadic algebra of infinite degree is semisimple. In fact, *every* polyadic algebra is semisimple, and this assertion is sometimes taken to be the algebraic version of the Gödel completeness theorem. The proof of semisimplicity is quite easy; the crucial fact is not that something is semisimple but that in the most important cases semisimplicity is the same as semantic completeness.

The word "incompleteness" in "incompleteness theorem" refers to syntactic incompleteness. The result here is not so general as the completeness theorem; the subject matter is not all polyadic algebras, but only relatively few of them. The algebras covered by the theorem are usually described by saying that they are adequate for elementary arithmetic. Because a precise explanation of what this means would involve a rather long and technical detour, no such explanation will be presented here, and, consequently, the incompleteness theorem will be described rather than stated. The striking qualities of the theorem are sufficiently great to remain visible even under such cavalier treatment.

Even if the definition of the class of algebras under consideration is not made explicit, it is convenient to have a short phrase in which to refer to them; in what follows "Peano algebra" will be used instead of "polyadic algebra that is adequate for elementary arithmetic." The Gödel incompleteness theorem asserts the existence of "undecidable propositions." Since in the passage from logics to algebras the statement that an element p is refutable (or provable) was identified with the statement that $p=0$ (or $p=1$), and since "undecidable" means "neither refutable nor provable," the assertion reduces to the existence of a (closed) element different from both 0 and 1. The ideal generated by such an element is a non-trivial proper ideal. Conversely, every non-trivial proper ideal contains an undecidable (closed) element. These facts indicate that the Gödel incompleteness theorem asserts the existence, in Peano algebras, of non-trivial proper ideals; the definition of syntactic completeness shows now that the theorem does indeed assert that something is (syntactically) incomplete. The usual, logical, formulation explicitly makes the assumption that the underlying logic is consistent; the treatment of algebras instead of logics makes it unnecessary to mention such an assumption here.

The Gödel theorem does not assert that every Peano algebra is syntactically incomplete. It asserts, instead, that the definition of Peano algebras is not a faithful algebraic transcription of all intuitive facts about elementary arithmetic. In algebraic terms this means that while some Peano algebras may be syntactically complete, there definitely exist others that are not. The situation is analogous to the one in the theory of groups. A class of polyadic algebras could be defined that is adequate for a discussion of elementary group theory. For this class the assertion that every two elements of a group commute would be un-

decidable, in the obvious sense that the assertion is true for some groups (and, therefore, corresponds to the unit element of some of the polyadic algebras under consideration) and false for others.

What has been said so far makes the Gödel incompleteness theorem take the following form: not every Peano algebra is syntactically complete. In view of the algebraic characterization of syntactic completeness this can be rephrased thus: not every Peano algebra is a simple polyadic algebra. This is the description that was promised above. What follows is another rephrasing of this description; the rephrasing, possibly of some mnemonic value, makes its point by making a pun. Consider one of the systems of axiomatic set theory that is commonly accepted as a foundation for all extant mathematics. There is no difficulty in constructing polyadic algebras with sufficiently rich structure to mirror that axiomatic system in all detail. Since set theory is, in particular, an adequate foundation for elementary arithmetic, each such algebra is a Peano algebra. The elements of such a Peano algebra correspond in a natural way to the propositions considered in mathematics; it is stretching a point, but not very far, to identify such an algebra with mathematics itself. Some of these "mathematics" may turn out to possess no non-trivial proper ideals, *i.e.*, to be syntactically complete; the Gödel theorem implies that some of them will certainly be syntactically incomplete. The conclusion is that the crowning glory of modern logic (algebraic or not) is the assertion: *mathematics is not necessarily simple*.

ZERO INTEGRAL HOMOGENEOUS SYMMETRIC FUNCTIONS IN CERTAIN RINGS*

MILO WEAVER, University of Texas

In this paper †, we shall discuss a type of function which we shall define at the start. If $f(c_0, c_1, \dots, c_n)$ is a function with the c 's in a ring, then f is called an *integral homogeneous symmetric function of degree n* , written IHSF, of degree n provided it satisfies:

- (i) f is a polynomial in the c 's which is unchanged by any permutation of the c 's.
- (ii) $f(tc_0, tc_1, \dots, tc_n) = t^n f(c_0, c_1, \dots, c_n)$.

Each elementary symmetric function is an IHSF. It is well known that in the field of real numbers each elementary symmetric function of the n th roots of unity is zero except the one of highest degree. More generally if

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n = 0$$

has a decomposition in a field, then in this field, $a_i = S_i(-1)^i$, where S_i is the

* This paper was supported in part by National Science Foundation Grant G1397.

† The author wishes to thank the referee for valuable suggestions relative to this paper.