0. BASIC CONCEPTS AND NOTATION

This chapter can be quickly passed over by anyone familiar with modern universal algebra. The less familiar concepts and notations will be defined again in the text at their first occurrence. Occasionally, one may need to consult the index at the back of the book to find the place where a term has first been defined. For more complete treatments of the material of this chapter, one can consult the books by Grätzer, [14] and [15], for everything pertaining to algebras or lattices, and the book by Burris and Sankapalnavar [4] for varieties.

0.1 ALGEBRAS. An algebra consists of a nonvoid set and some finitary operations over that set. For example, a group is a set of elements and a binary operation on those elements (or sometimes, a binary operation and a unary operation are used). We shall deal with two kinds of algebras, the indexed and the non-indexed. An indexed algebra, written usually as $A = \langle A, f_i(i \in I) \rangle$, consists of a nonvoid set $A$ of elements (the base set or universe) and a function $\langle f_i : i \in I \rangle$ whose values, $f_i$, are operations on $A$. A non-indexed algebra is just a pair $A = \langle A, F \rangle$, consisting of a nonvoid set $A$ and a set $F$ of operations on $A$. Both kinds of algebras are called, simply "algebras". The operations given, either the $f_i(i \in I)$, or the members of $F$, are called the basic operations of the algebra. Indexed algebras are preferable to non-indexed in many instances. For example, in speaking of a homomorphism between two rings, one may need to refer to the "addition operations" of both rings. (In our general framework, rings can be construed as algebras $\langle A, f_+ , f_-, f_0 \rangle$, taking as index set for the operations $I = \{+,-,0\}$.) On the other hand, non-indexed algebras arise frequently in the theory we shall develop, in situations where it is both inconvenient and unnecessary to make a list of the operations.

The $n$th Cartesian power of a set $A$, where $n$ is a non-negative integer, is denoted $A^n$. Its elements are written as $\bar{x} = (x_0, \ldots , x_{n-1})$. By an $n$-ary operation on $A$, we mean any function $f : A^n \to A$. The only restriction we impose on an algebra is that its basic operations be finitary. This means that every basic operation $f$ of an algebra whose universe is $A$ must be an $n$-ary operation on $A$ for some non-negative integer $n$. It is common practice to use the word "unary" instead of "1-ary", and to use "binary" to replace "2-ary".
By composition of operations we mean the construction of an \( n \)-ary operation \( h \), from \( k \) given \( n \)-ary operations \( f_0, \ldots, f_{k-1} \) and a \( k \)-ary operation \( g \), through the defining formula \( h(\bar{x}) = g(f_0(\bar{x}), \ldots, f_{k-1}(\bar{x})) \). (All of these operations must be defined on the same set; while the non-negative integers \( k \) and \( n \) are arbitrary.) The projection operations on a set \( A \) are the trivial operations \( p^n_i \) satisfying \( p^n_i(x_0, \ldots, x_{n-1}) = x_i \). A clone on a set \( A \) is a set of operations on \( A \) that is closed under all compositions and contains the projections \( p^n_i \) (for all \( n \) and \( i \) satisfying \( 0 \leq i < n \)).

There are two important sets of derived operations in any algebra \( A \). One is the clone of polynomial operations of \( A \) denoted \( \text{Pol} A \). It is the close on \( A \) generated by the basic operations of \( A \) together with all of the constant 0-ary operations on \( A \) (and the projection operations, of course). The set of \( n \)-ary operations in this clone is denoted by \( \text{Pol}_n A \). The other is the clone of (so-called) term operations of \( A \), denoted \( \text{Clo} A \). It is the close on \( A \) generated by the basic operations of \( A \). To illustrate these definitions, let \( A = \langle \{0,1\}, + \rangle \) be the 2-element group, with \( 1 + 1 = 0 \). Here \( \text{Clo}_2 A \) consists of the four operations

\[
 f(x, y) = x, y, x + y, \quad \text{and} \quad 0 \quad (= x + x).
\]

\( \text{Pol}_2 A \) has eight operations, the term operations just listed, plus

\[
 f(x, y) = x + 1, \enspace y + 1, \enspace x + y + 1 \quad \text{and} \quad 1.
\]

If \( f \) is an \( m + n \)-ary term operation of \( A \) and \( \alpha = \langle \alpha_0, \ldots, \alpha_{m-1} \rangle \in A^m \), then the formula

\[
 g(\bar{x}) = f(\bar{\alpha}, \bar{x}) \quad (= f(\alpha_0, \ldots, \alpha_{m-1}, x_0, \ldots, x_{n-1}))
\]

defines an \( n \)-ary polynomial operation of \( A \). Conversely, every \( n \)-ary polynomial operation of \( A \) arises in this way, through substitution of constants for some of the variables in some term operation of \( A \). By a polynomial clone on \( A \), we mean a clone on \( A \) containing all the constant operations. Thus \( \text{Pol} A \) is the polynomial clone generated by \( \text{Clo} A \).

Let \( A \) be any algebra, \( U \) be a nonvoid subset of the universe of \( A \), and \( f \) be a polynomial operation of \( A \) such that \( U \) is closed under \( f \). Then the restriction of \( f \) to \( U \), or \( f|_U \), is obviously an operation on \( U \). By \( (\text{Pol} A)|_U \) we denote the set of all those \( f|_U \) where \( f \in \text{Pol} A \) and \( U \) is closed under \( f \). The non-indexed algebra \( (U, (\text{Pol} A)|_U) \) will be called the algebra induced by \( A \) on \( U \) and we shall denote it by \( A|_U \). These induced algebras play a cardinal role in this book. Notice that

\[
 \text{Clo} (A|_U) = \text{Pol} (A|_U) = (\text{Pol} A)|_U;
\]

i.e., every polynomial operation of this algebra is already a basic operation.

Indexed algebras \( A = \langle A, f_i (i \in I) \rangle \) and \( B = \langle B, g_i (i \in I) \rangle \) are called similar iff they have the same index set \( I \), and \( f_i \) and \( g_i \) are of equal arity for all \( i \in I \). For
indexed algebras, the basic notions of subalgebra of an algebra, of homomorphism or isomorphism between two similar algebras, and of (Cartesian) product of a system of similar algebras are so well known that we shall not bother to define them carefully. We write $A \subseteq B$ for "$A$ is a subalgebra of $B$", and $f : A \rightarrow B$ for "$f$ is a homomorphism of $A$ into $B$". The expression $\prod \{A_t : t \in T\}$ denotes the algebra which is the Cartesian product of a system $\langle A_t : t \in T \rangle$. To denote that $A$ is isomorphic to $B$ we write $A \cong B$. A subuniverse of $A$ is a subset closed under all the operations of $A$. We will sometimes confuse subalgebras with nonvoid subuniverses, when no ambiguity is likely to result.

For non-indexed algebras $A = (A, F)$ and $B = (B, G)$, the nomenclature and notation of homomorphism and isomorphism will be used with the following meanings. Let $f : A \rightarrow B$. We call $f$ a homomorphism (or isomorphism, respectively) iff the basic operations can be indexed, $F = \{f_i : i \in I\}$ and $G = \{g_i : i \in I\}$, in such a way that $\langle A, f_i(i \in I) \rangle$ and $\langle B, g_i(i \in I) \rangle$ are similar and $f$ is a homomorphism (an isomorphism) between these indexed algebras.

When $X$ is a subset of an algebra $A$ (i.e., a subset of the universe of $A$), then the smallest set containing $X$ and closed under the basic operations (i.e., the subuniverse of $A$ generated by $X$) is obtained by applying Clo$_n A$ to $X$. It is the set

$$X = \{f(x_0, \ldots, x_{n-1}) : f \in \text{Clo}_n A \text{ and } \{x_0, \ldots, x_{n-1}\} \subseteq X \text{ and } n \text{ is arbitrary} \}.$$

If $B = \prod \{A_t : t \in T\}$ with $A_t = \langle A_t, f_{it}(i \in I) \rangle$, and $B = \langle B, g_i(i \in I) \rangle$, then the operation $g_i$ of $B$ is the operation on $B$ which "acts coordinate-wise" and "acts like $f_{it}$ in the $t$-th coordinate," for all $t$. Of special interest is the case where $A_t = A = \langle A, f_i(i \in I) \rangle$ for all $t$, i.e., where $B = A^T$ is a Cartesian power of the algebra $A$. The universe of $A^T$ is of course the set $A^T$ of all functions from $T$ into the universe of $A$. Suppose that the $i$-th operation of $A$ is $n$-ary and that $h_0, \ldots, h_{n-1} \in A^T$. Then the $i$-th operation of $A^T$, when applied to $h_0, \ldots, h_{n-1}$, gives the result

$$g_i(h_0, \ldots, h_{n-1}) = h \in A^T$$

with $h$ defined by

$$h(t) = f_i(h_0(t), \ldots, h_{n-1}(t)) \ .$$

If, in the above, $T = A^n$ then Clo$_n A$ is a subset of $A^T$; and in fact it can easily be shown that Clo$_n A$ is identical with the subuniverse of $A^{A^n}$ generated by the $n$ projections. Similarly, Pol$_n A$ is identical with the subuniverse of $A^{A^n}$ generated by the projections and all the constant $n$-ary operations on $A$.

We adopt a convention used in logic and set theory, and identify each natural number $n$ with the set $\{0, \ldots, n-1\}$ of all smaller natural numbers. Then $A^n$ denotes
a set of functions \((n\)-tuples of elements of \(A\)), and \(A^n\) denotes the \(n\)th direct power of the algebra \(A\). We use the Greek letter \(\omega\) to denote the set of all natural numbers.

By an \(n\)-ary relation on a set \(A\), we mean a subset of \(A^n\). For binary relations \(\sigma\) and \(\rho\) on \(A\), the converse of \(\sigma\) is the relation

\[
\sigma^\to = \{(y, x) : (x, y) \in \sigma\}.
\]

and the relational product of \(\sigma\) and \(\rho\) is

\[
\sigma \circ \rho = \{(x, z) : \exists y((x, y) \in \sigma \text{ and } (y, z) \in \rho)\}.
\]

The relation \(\{(x, x) : x \in A\}\) is at once the identity function on \(A\), denoted \(\id_A\), and the least equivalence relation on \(A\) (see below). When it plays the second role, we denote it by \(0_A\). (The largest equivalence relation on \(A\) is \(1_A = A^2\).) A binary relation \(\sigma\) on \(A\) is called reflexive over \(A\) iff \(\sigma \supseteq \id_A\); symmetric iff \(\sigma = \sigma^\to\); transitive iff \(\sigma \supseteq \sigma \circ \sigma\). The transitive closure of a binary relation \(\sigma\) is the smallest transitive relation including \(\sigma\); it is identical with the set \(\bigcup\{\sigma^n : n \geq 1\}\), where \(\sigma^1 = \sigma\) and, inductively, \(\sigma^{k+1} = \sigma^k \circ \sigma\).

By an \(n\)-ary admissible relation of an indexed algebra \(A\) we mean a subuniverse of \(A^n\). Thus an \(n\)-ary relation \(\rho\) is admissible for \(A\) iff \(\rho \subseteq A^n\) and \(\rho\) is closed (or admissible) under all the operations of \(A\) acting co-ordinatewise. (For “operation” read either “basic operation” or “term operation”; it will not change the concept defined.) Phrased in this way, the concept of admissible relation makes sense for both kinds of algebra, indexed and non-indexed. Note that an admissible binary relation of \(A\) is reflexive over \(A\) iff it is admissible for the polynomial operations, as well as for the term operations, of \(A\).

Two types of admissible relations play a large role in this book. A tolerance of \(A\) is an admissible binary relation that is symmetric and reflexive over the universe of \(A\). A congruence of \(A\) is a transitive tolerance of \(A\), i.e., an admissible equivalence relation.

**Notation for equivalence relations:** \(\Pi_A\) denotes the set of all equivalence relations (reflexive, symmetric, transitive binary relations) on \(A\). If \(\sigma \in \Pi_A\) and \(x, y \in A\), then \(x \equiv y\) (mod \(\sigma\)) means that \((x, y) \in \sigma\). We put \(x/\sigma = \{z : (x, z) \in \sigma\}\). Given an equivalence relation \(\sigma\), the set \(A/\sigma = \{x/\sigma : x \in A\}\) is a partition of \(A\); that is, \(A = \bigcup\{x/\sigma : x \in A\}\) and for all \(x, y\) we have \(x/\sigma \cap y/\sigma = \emptyset\) or \(x/\sigma = y/\sigma\). The elements of \(A/\sigma\) are called equivalence classes (sometimes, blocks) of \(\sigma\).

**Quotient algebras:** If an \(n\)-ary operation \(f\) on \(A\) preserves an equivalence relation \(\sigma \in \Pi_A\), i.e., if \(\sigma\) is a congruence of the algebra \((A, f)\), then an operation \(f_\sigma\) is defined on \(A_\sigma\) by the formula

\[
f_\sigma(x_0/\sigma, \ldots, x_{n-1}/\sigma) = f(x_0, \ldots, x_{n-1})/\sigma.
\]
Thus if $\mathbf{A} = \langle A, f_i (i \in I) \rangle$ (or $\mathbf{A} = \langle A, F \rangle$) is an algebra and $\sigma$ is a congruence of $\mathbf{A}$, then we have an algebra $A/\sigma = \langle A/\sigma, f_{i\sigma} (i \in I) \rangle$ (or $A/\sigma = \langle A/\sigma, \{f_\sigma : f \in F\} \rangle$).

The mapping $\pi_\sigma$ that takes $x$ to $x/\sigma$ is a homomorphism of $\mathbf{A}$ onto $A/\sigma$ in either case. $A/\sigma$ is called the quotient of $\mathbf{A}$ by the congruence $\sigma$. Whenever we have a homomorphism $\pi : \mathbf{A} \to \mathbf{B}$, then $\ker \pi = \{(x, y) \in A^2 : \pi x = \pi y\}$ is a congruence of $\mathbf{A}$. This congruence is called the kernel of $\pi$, and we have $\mathbf{B} \cong A/\ker \pi$ if $\pi$ is onto $\mathbf{B}$. The congruences of $\mathbf{A}$ are the same as the kernels of the homomorphisms from $\mathbf{A}$.

Two algebras, $\mathbf{A} = \langle A, \ldots \rangle$ and $\mathbf{B} = \langle B, \ldots \rangle$, are called polynomially equivalent iff they have the same universe and precisely the same polynomial operations, i.e., $A = B$ and $\text{Pol } A = \text{Pol } B$. It is easy to show that the algebras $\langle A, \text{Clo } A \rangle$, $\langle A, \text{Pol } A \rangle$, and $\langle A, \text{Pol}_1 A \rangle$, have the property that any $\theta \in \Pi_A$ is a congruence of one of these algebras iff it is a congruence of all of them. (This is true for every $\mathbf{A}$.) Each of the first three of these algebras is polynomially equivalent to $\mathbf{A}$.

0.2 LATTICES. A po-set (partially ordered set) is a nonvoid set $A$ together with a binary relation $\rho$ on $A$ satisfying $\rho \rho \subseteq \rho$, $\rho \cap \rho^\downarrow = \text{id}_A$. The binary relation (partial ordering) of a po-set is usually denoted as $\leq$. We use the notation $x < y \ (x \leq y$ and $x \neq y)$, and $x \prec y \ (y$ covers $x$, which means that $x < y$ and for n.c. $z$ does $x < z < y$ hold). Finite po-sets can be pictured in Hasse diagrams, with the elements depicted as points on a plane, larger elements corresponding to higher points, and the covering relation represented by ascending straight line segments. Here are some Hasse diagrams.

![Figure 0](image-url)

The rule for decoding Hasse diagrams is that $x \leq y$ iff one can get from point $x$ to point $y$ by following ascending line segments between points. Turns of direction are allowed only at the points. Thus in the last diagram of the figure, $u \nleq v$. The elements $u$ and $v$ in the diagram are incomparable, that is, neither $u \leq v$ nor $v \leq u$ holds. In the second diagram of Figure 0, $a \prec b \prec c$ and thus $a \prec c$. 
A lattice is an algebra \( \langle A, \lor, \land \rangle \) with two binary operations such that for some partial ordering \( \leq \) of \( A \), the formulas \((x \lor y \leq z) \iff (x \leq z \text{ and } y \leq z)\) and \((z \leq x \land y) \iff (z \leq x \text{ and } z \leq y)\) are valid for all elements \( x, y, \text{ and } z \). Each of the operations of a lattice, \( \lor \) (called \textit{join}) and \( \land \) (called \textit{meet}), determines \( \leq \) uniquely, and thus each operation determines the other. A po-set \( \langle A, \leq \rangle \) is correlated with a lattice in this fashion if and only if every pair of elements of \( A \) have a least upper bound and a greatest lower bound in \( A \) (with respect to \( \leq \)).

The final three diagrams in Figure 0 are Hasse diagrams of lattices, the first two are not. \( \text{Su}(3) \) is our name for the lattice of subsets of a three-element set.

Lattices are algebras, and so we can speak of their subalgebras, homomorphisms and congruences. The \textit{modular law} is the equation \( x \land ((x \land y) \lor z) = (x \land y) \lor (x \land z) \). A lattice which satisfies this as an identity, i.e., for all choices of elements \( x, y, \text{ and } z \), is called \textit{modular}. A lattice \( L \) is modular iff in \( L \), \( y \leq x \) implies \( x \land (y \lor z) = y \lor (x \land z) \). The lattice \( N_5 \) is nonmodular (Figure 0), and every lattice having a sublattice isomorphic to \( N_5 \) is nonmodular. Conversely, if \( L \) is nonmodular then it has a sublattice isomorphic to \( N_5 \). For suppose \( y < x \) and \( x \land (y \lor z) \neq y \lor (x \land z) \). It is then easily verified that this is a sublattice of \( L \) isomorphic to \( N_5 \):

\[ y \lor z \]
\[ \downarrow \]
\[ z = x \land (y \lor z) \]
\[ \land \]
\[ x \land z \]
\[ y \lor (x \land z) \]

The \textit{distributive law} for lattices is the equation \( x \land (y \lor z) = (x \land y) \lor (x \land z) \). Lattices satisfying this as an identity are called \textit{distributive}. (Exercise: A modular lattice is distributive iff it has no sublattice isomorphic to \( M_3 \) in Figure 0.)

Set inclusion is a lattice ordering of the set \( \Pi_A \) of all equivalence relations on a set \( A \). In the lattice \( \Pi_A = \langle \Pi_A, \lor, \land \rangle \), called the \textit{full partition lattice} over \( A \), the join of two equivalence relations is the transitive closure of their set union, and the meet of two equivalence relations is simply their intersection.

\textbf{Congruence lattices:} For any algebra \( A \), \( \text{Con} \ A \) denotes the set of all congruence relations of \( A \). It is closed under the join and meet in \( \Pi_A \), and so we have a lattice \( \text{Con} \ A = \langle \text{Con} \ A, \lor, \land \rangle \), called the \textit{congruence lattice of} \( A \). This lattice is \textit{complete}, in fact, it is a \textit{complete sublattice} of \( \Pi_A \). That is to say, for any set \( X \) of congruences on \( A \), the join or least upper bound of \( X \), and the meet or greatest lower bound of
$X$, exist in $\text{Con } A$, and these joins and meets are the same as in $\Pi A$. The join and meet of $X$ are written as $\vee X$ and $\wedge X$.

We write $\Theta(T)$ for the congruence generated by a set $T \subseteq A^2$. If $T = \{(a, b)\}$, we write instead $\Theta(a, b)$. $\Theta(T)$ is the transitive closure of the relation

$$\text{id}_A \cup \{(f(a), f(b)) : f \in \text{Pol}_1 A \text{ and } \langle a, b \rangle \in T \text{ or } \langle b, a \rangle \in T\}.$$ 

The finitely generated congruences of $A$ are those of the form $\Theta(T)$ where $T$ is a finite subset of $A^2$. By a compact element of a complete lattice $L$ is meant an element $c$ for which $c \leq \bigvee X$ always implies the existence of a finite set $X' \subseteq X$ with $c \leq \bigvee X'$. It is easy to see that the compact elements of $\text{Con } A$ are precisely the finitely generated congruences.

A lattice $L$ is called algebraic if and only if $L$ is complete and every element of $L$ is the join of a set of compact elements of $L$. The nomenclature is justified by a classical theorem of G. Grätzer and E.T. Schmidt: A lattice $L$ is algebraic iff for some algebra $A$, $L \cong \text{Con } A$. Every finite lattice is algebraic. The Grätzer-Schmidt proof produces in nearly every case an infinite algebra; and it is not known if every finite lattice is isomorphic to $\text{Con } A$ for some finite algebra $A$.

**Simple and subdirectly irreducible algebras:** An algebra $A$ is called simple iff $\text{Con } A$ is a two-element lattice. This holds iff $A$ has at least two elements and every homomorphism $f : A \to B$ is one-to-one or constant. (Exercise: The lattice $M_3$ of Figure 0 is a simple algebra.) An algebra $A$ is called subdirectly irreducible iff $\text{Con } A$ has an element $\beta \neq 0_A$ such that every congruence $\delta$ satisfies $\delta \geq \beta \iff \delta \neq 0_A$. Thus $A$ is subdirectly irreducible iff it has elements $a \neq b$ such that every homomorphism $f : A \to B$ is either one-to-one or has $f(a) = f(b)$. The least non-zero congruence $\beta$ of a subdirectly irreducible algebra $A$ is called the monolith of $A$.

We say that $A$ is a subdirect product of a system of algebras $(B_i : i \in I)$, symbolically $A \leq \text{sd} \prod\{B_i : i \in I\}$, if $A$ is a subalgebra of the product and the coordinate homomorphism $p_i : A \to B_i$ is onto $B_i$ for each and every $i$. It is not hard to see that an algebra $A$ is subdirectly irreducible iff for every one-to-one homomorphism $\varphi : A \to \prod\{B_i : i \in I\}$ of $A$ into a product, there exists $i$ for which $p_i \varphi : A \to B_i$ is injective—in other words, iff $A$ is not isomorphic in a non-trivial way to a subdirect product.

For any two elements $a \leq b$ in a lattice $L$, we have the interval

$$I[a, b] = \{x \in L : a \leq x \leq b\},$$

which is a sublattice of $L$. If $\varphi : A \to B$ is onto $B$, and $\theta = \ker \varphi$, then we have an isomorphism $\varphi^{-1}$ of $\text{Con } B$ with the interval sublattice $I[\theta, 1_A]$ in $\text{Con } A$, defined by $\varphi^{-1}(\alpha) = \{(x, y) \in A^2 : (\varphi(x), \varphi(y)) \in \alpha\}$. Thus, in fact, for any congruence $\delta$ of $A$, $\text{Con } (A/\delta) \cong I[\delta, 1_A]$. This is a generalization of one of the isomorphism theorems.
of group theory. Using this fact, one may prove G. Birkhoff's subdirect representation theorem, which states that for any algebra $A$, there is a set $\{\theta_i : i \in I\} \subseteq \text{Con } A$ (with $I$ empty if $A$ has only one element) such that $A/\theta_i$ is subdirectly irreducible for each $i$, and $x \mapsto (x/\theta_i : i \in I)$ is an isomorphism of $A$ with a subdirect product of $(A/\theta_i : i \in I)$. (Let $I = A^2 - \text{id}_A$ and for each $i = (a, b) \in I$, let $\theta_i$ be a maximal member of the set $\{\delta \in \text{Con } A : (a, b) \notin \delta\}$.)

0.3 VARIETIES. To come to terms with the wild diversity of form and character exhibited by algebras, it is desirable to group them into classes according to some scheme. One way to do this has proved so fruitful that it has no serious competitor. That is to group algebras into classes defined by equations. The basic classes in this scheme are called varieties. It is probably no accident that the first really broad classes of algebras to be studied systematically were varieties such as the class of groups, the class of rings, and the class of Lie algebras.

To give a completely adequate and precise introduction to the elementary theory of varieties would require more space than we are willing to commit here. We shall discuss varieties briefly and depend on the reader to supplement our remarks by a reading of Chapters II, §§9-11 in [4], if this subject has not been met before.

By a language we shall mean an ordered triple $L = (I, F, \sigma)$ consisting of a set $I$, a one-to-one function $F = \{f_i : i \in I\}$ (whose values, $f_i$, will be called operation symbols), and a function $\sigma = \{\sigma_i : i \in I\}$ whose values are non-negative integers. A model of $L$, or $L$-algebra, is any algebra $A = (A, f_i^A (i \in I))$ in which $f_i^A$ is a $\sigma_i$-ary operation on $A$ for each $i$. For any nonvoid set $X$, there is an $L$-algebra $F_L(X)$, generated by $X$, having the property that every mapping $\varphi$ of $X$ into any $L$-algebra $A$ has a unique extension $\hat{\varphi}$ which is a homomorphism of $F_L(X)$ into $A$. $F_L(X)$ is called the free $L$-algebra, freely generated by $X$. It is determined up to isomorphism by $X$; in fact, if $F_L(X)$ and $F_L'(X)$ both satisfy the conditions laid down above, then these algebras are isomorphic by an isomorphism which leaves fixed each element of $X$.

A term in the language $L$, or $L$-term, is simply a member of $F_L(X)$ for some finite set $X$. Terms belonging to $F_L(x_1, \ldots, x_k)$ (where $x_1, \ldots, x_k$ are assumed distinct) will be written as $t(x_1, \ldots, x_k)$. Let $t = t(x_1, \ldots, x_k)$ be such a term. Given elements $a_1, \ldots, a_k$ in an $L$-algebra $A$, we define $t^A(a_1, \ldots, a_k)$ to be the element $\varphi(t)$ where $\varphi$ is the homomorphism of $F_L(x_1, \ldots, x_k)$ into $A$ with $\varphi(x_i) = a_1, \ldots, \varphi(x_k) = a_k$. This defines a $k$-ary operation $t^A$ on the universe of $A$, corresponding to the term $t(x_1, \ldots, x_k)$. (A fixed ordered list of the free generators $x_1, \ldots, x_k$ is required, in order to determine $t^A$ precisely.) An operation in the algebra $A$ that can be defined in this way, from some $L$-term, is called a term operation of $A$. It is not hard to see that the set of all term operations of $A$ is identical with the clone Clo $A$ which we defined earlier.
A formal equation in the language \( L \), or \( L \)-equation, is an ordered pair of terms, both of which are members of the same free algebra. Formal equations are written in the form \( s(x_1, \ldots, x_k) \approx t(x_1, \ldots, x_k) \). Such an equation is said to be an identity of an \( L \)-algebra \( A \) iff \( s^A = t^A \). (Equivalent expressions: "\( A \) obeys \( s \approx t \)" \( (x_1, \ldots, x_k \) are understood). "\( A \) satisfies \( s \approx t \) identically", "\( s \approx t \) holds in \( A \)", "\( A \models s \approx t \)."

When speaking of equations, the free generators \( x_1, \ldots, x_k \) are called variables.

If \( \Sigma \) is any set of \( L \)-equations (in various finite sets of variables), the class of all algebras in which every member of \( \Sigma \) is an identity will be denoted by \( \text{Mod}(\Sigma) \) (the class of models of \( \Sigma \)). Classes of the form \( \text{Mod}(\Sigma) \) are called varieties. Every variety comes with a language attached; its members are similar algebras—all of them models for that language.

It is quite clear that the class of all groups, construed as models of a language with one binary operation symbol, \( \cdot \), and one unary operation symbol, \( ^{-1} \), is a variety. The class of all lattices is a variety. We choose a language \( L \) with two binary operation symbols, \( \lor \) and \( \land \), and write some equations using terms in \( F_L(x, y, z) \):

\[
\begin{align*}
  x \lor x & \approx x, \\
  x \lor y & \approx y \lor x, \\
  (x \lor y) \lor z & \approx x \lor (y \lor z) \\
  [\text{the equations obtained by replacing } \lor \text{ by } \land \text{ in the above}] \\
  x \lor (x \land y) & \approx x, \\
  x \land (x \lor y) & \approx x.
\end{align*}
\]

It is not hard to see that these equations define the class of lattices; i.e., an algebra \( \langle A, \lor, \land \rangle \) is a lattice if and only if it obeys the above equations. For any ring \( R \) with unit, the class of left unitary \( R \)-modules can be construed as a variety in a rather obvious fashion. The language should have a binary and a unary operation symbol, \( + \) and \( - \), and one unary symbol \( f_\lambda \) for scalar multiplication, for each \( \lambda \in R \).

For any class \( K \) of similar algebras (models of one language), \( H K \), \( S K \), and \( P K \) denote the class of all algebras that are, respectively, homomorphic images of algebras in \( K \), isomorphic to a subalgebra of an algebra in \( K \), or isomorphic to a product of algebras in \( K \). According to the HSP-theorem of G. Birkhoff, a class \( K \) of similar algebras is a variety iff \( K = HSPK \); and the smallest variety containing a class \( K \) of similar algebras is \( V(K) = HSPK \).

**Free algebras in varieties:** Let \( L \) be a language and let \( K \) be a nontrivial class of \( L \)-algebras (one which contains an algebra with at least two elements). For any nonvoid set \( X \) there exists an algebra, \( F_K(X) \), generated by \( X \), such that \( F_K(X) \in SPK \) and every mapping of \( X \) into an algebra of \( K \) (or of \( SPK \)) extends to a homomorphism of \( F_K(X) \) into that algebra. Where \( \phi \) is the homomorphism of \( F_L(X) \) onto \( F_K(X) \) extending the identity map on \( X \), the kernel of \( \phi \) is

\[
\theta_K = \bigcap \{ \ker f \mid f : F_L(X) \to A \text{ for some } A \in K \},
\]
and $F_K(X) \cong F_L(X)/\theta_K$. One proof of Birkhoff’s theorem proceeds by noting that if $A$ obeys all of the equations that hold in $K$, then for large $X$ there is a homomorphism $f$ of $F_L(X)$ onto $A$ and $\ker f \cong \theta_K$; thus $A \in H(F_K(X)) \subseteq HSPK$.

Now let $V$ be a nontrivial variety of $L$-algebras. For each nonvoid set $X$, $F_V(X)$ belongs to $V$; it is called the free algebra in $V$, freely generated by $X$. Elements of the finitely generated free algebras in $V$ are called $V$-terms. Every $V$-term $t(x_1, \ldots, x_n)$ gives rise to a term operation $t^A$ in each algebra $A$ of $V$. The kernel of the homomorphism $F_L(x_1, \ldots, x_n) \to F_V(x_1, \ldots, x_n)$ is equal to the set of equations in the variables $x_1, \ldots, x_n$ that hold as identities in $V$. If $C$ is an algebra such that $V = V(C)$, then the map $t(x_1, \ldots, x_n) \to t^C$ is an isomorphism between $F_V(x_1, \ldots, x_n)$ and the subalgebra of $C^{x_n}$ whose universe is $C_{\text{fin}}C$.

We close this chapter by proving three simple but important theorems about varieties. An algebra $A$ is said to be locally finite iff every subalgebra of $A$ generated by finitely many elements is finite. We call a variety $V$ locally finite iff every algebra in $V$ is locally finite, or equivalently, every finitely generated algebra in $V$ is finite. We say that $V$ is finitely generated iff it has the form $V(A_1, \ldots, A_n) (= V(A_1 \times \cdots \times A_n))$ where $n$ is some positive integer and each of $A_1, \ldots, A_n$ is a finite algebra. The free algebra $F_V(x_1, \ldots, x_k)$ in $V$, freely generated by $k$ distinct elements, will be denoted simply by $F_V(k)$.

**Theorem 0.1.** Let $V$ be any variety.

1. $V$ is locally finite iff $F_V(k)$ is finite for all $1 \leq k < \omega$.
2. If $V$ is finitely generated than it is locally finite. In fact, if $V = V(A)$ for a finite algebra $A$ then, for each $k < \omega$, $F_V(k) \in S(A^n)$ for some $n < \omega$.

**Proof.** To prove (1) we simply note that $F_V(k)$ is finitely generated (if $k$ is finite) and every finitely generated algebra in $V$ is in $H(F_V(k))$ for some $k < \omega$.

To prove (2), let $V = V(A)$ where $|A| = m$. Given any $k, 1 \leq k < \omega$, we recall that $t(x_1, \ldots, x_k) \mapsto t^A$ is an isomorphism of $F_V(k)$ onto the subalgebra of $A^{x_k}$ with universe $C_{\text{fin}}A$. Thus $F_V(k) \in S(A^n)$, where $n = m^k$. 

For any class $K, P_{\text{fin}}K$ denotes the class of algebras isomorphic to a product $A_1 \times \cdots \times A_n$ for some finite $n$, where $\{A_1, \ldots, A_n\} \subseteq K$.

**Theorem 0.2.** If $V = V(A_1, \ldots, A_m)$ and $A_1, \ldots, A_m$ are finite, then every finite algebra in $V$ belongs to the class $HSP_{\text{fin}}(A_1, \ldots, A_m)$.

**Proof.** Let $A = A_1 \times \cdots \times A_m$. Let $B$ be any finite algebra in $V = V(A)$, say $|B| = k$. By Theorem 0.1 (2), $F_V(k) \in SP_{\text{fin}}(A) \subseteq SP_{\text{fin}}(A_1, \ldots, A_m)$. Since $B \in H(F_V(k))$, the proof is finished. 

$\square$
The third statement in the next theorem was proved by A. I. Mal’cev around 1954.

Two equivalence relations, $\sigma$ and $\tau$, on a set $A$ are said to be permuting iff $\sigma \circ \tau = \tau \circ \sigma$.

**THEOREM 0.3.**

1. If $\sigma$ and $\tau$ are permuting equivalence relations on a set $A$ then $\sigma \circ \tau = \sigma \lor \tau$ (the join in $\Pi_A$).
2. If $A$ is an algebra with permuting congruences (every two congruences permute) then $\text{Con} \ A$ is a modular lattice.
3. A variety $\mathcal{V}$ has permuting congruences (every algebra in $\mathcal{V}$ has permuting congruences) iff there is a ternary term $t(x, y, z)$ in the language of $\mathcal{V}$ such that the equations $t(x, x, y) \approx y$, $t(x, y, y) \approx x$ are identities in $\mathcal{V}$ (Mal’cev’s equations).

**PROOF.** To prove (1) we simply note that

$$\sigma \lor \tau = \bigcup \{(\sigma \cup \tau)^n : 1 \leq n < \omega \} = \bigcup \{\sigma \circ \tau^n : 1 \leq n < \omega \}.$$  

Thus if $\sigma \circ \tau = \tau \circ \sigma$, we have

$$(\sigma \circ \tau)^2 = \sigma \circ \tau \circ \sigma \circ \tau = \sigma \circ \sigma \circ \tau \circ \tau = \sigma \circ \tau,$$

and so $(\sigma \circ \tau)^n = \sigma \circ \tau$ for all $n$.

To prove (2), suppose that the congruences of $A$ permute, and let $\alpha, \beta, \delta \in \text{Con} \ A$ with $\beta \leq \alpha$. It must be shown that $\alpha \land (\beta \lor \delta) = \beta \lor (\alpha \land \delta)$, or equivalently, that $\alpha \land (\beta \lor \delta) \leq \beta \lor (\alpha \land \delta)$. Let $(a, c) \in \alpha \land (\beta \lor \delta)$. Since $(a, c) \in \beta \lor \delta$, by (1) there is $b \in A$ with $(a, b) \in \beta$, $(b, c) \in \delta$.

Since $\beta \leq \alpha = \alpha \circ \alpha$, we have $(b, c) \in \alpha$. Thus $(b, c) \in \alpha \land \delta$; consequently $(a, c) \in \beta \circ (\alpha \land \delta) = \beta \lor (\alpha \land \delta)$ as desired.

The proof of (3) is a slightly more substantial enterprise. Suppose first that there is a term $t(x, y, z)$ for which Mal’cev’s equations hold in $\mathcal{V}$. Let $A \in \mathcal{V}$, $\alpha, \beta \in \text{Con} \ A$, $(a, b) \in \alpha, (b, c) \in \beta$. Now $\alpha$ and $\beta$ are congruences and thus are preserved by all term operations of $A$. Therefore $t^A(a, b, b) \equiv t^A(a, b, c) \pmod{\beta}$ and $t^A(a, b, c) \equiv t^A(b, b, c) \pmod{\alpha}$. Now $t^A(a, b, b) = a$ and $t^A(b, b, c) = c$ since $A$ satisfies Mal’cev’s equations. So we have the following picture, showing that $\alpha \circ \beta \subseteq \beta \circ \alpha$. 

![Diagram](image.png)
We can take converses, and conclude that $\beta \circ \alpha = (\beta \circ \alpha)^{\dagger} = (\alpha \circ \beta)^{\dagger} \subseteq (\beta \circ \alpha)^{\dagger} = \alpha \circ \beta$; thus $\alpha \circ \beta = \beta \circ \alpha$.

Now suppose that $\mathcal{V}$ does have permuting congruences. On $F = F_\mathcal{V}(x, y, z)$ define the congruences $\alpha = \Theta(x, y)$, $\beta = \Theta(y, z)$. We have $(x, y) \in \alpha$, $(y, z) \in \beta$. Therefore for some $s = s^F(x, y, z)$ in $F$ we have $(s, s) \in \beta$ and $(s, z) \in \alpha$. Let $\pi_\alpha$ be the endomorphism of $F$ satisfying $\pi_\alpha(x) = \pi_\alpha(y) = x$, $\pi_\alpha(z) = y$; and let $\pi_\beta$ be the endomorphism satisfying $\pi_\beta(x) = x$, $\pi_\beta(y) = \pi_\beta(z) = y$. Since $(x, y) \in \ker \pi_\alpha$, we have $\alpha \subseteq \ker \pi_\alpha$, similarly $\beta \subseteq \ker \pi_\beta$. (Exercise: Show that $\ker \pi_\alpha = \alpha$ and $\ker \pi_\beta = \beta$.) Therefore $(x, s) \in \ker \pi_\beta$, $s = s^F(x, y, z)$, implying

$$x = \pi_\beta(x) = \pi_\beta(s) = s^F(\pi_\beta x, \pi_\beta y, \pi_\beta z) = s^F(x, y, y).$$

Similarly, we have $y = s^F(x, x, y)$. There is a term $t(x, y, z) \in F_L(x, y, z)$ with $\varphi(t(x, y, z)) = s$ where $\varphi : F_L(x, y, z) \to F_\mathcal{V}(x, y, z)$ with $\varphi(x) = x$, $\varphi(y) = y$, $\varphi(z) = z$. It follows that $t^F(x, y, z) = s$ and then, arguing as above, $t^F(x, x, y) = x$ and $t^F(x, x, y) = y$. Thus $\varphi(t(x, y, y)) = \varphi(x)$, implying that $t(x, y, y) \approx x$ is an identity of $\mathcal{V}$. Similarly, $t(x, x, y) \approx y$ is an identity of $\mathcal{V}$. This ends the proof. $\square$