XV
Universal Algebra

Universal algebra is the study of algebraic objects in general, also called *universal algebras*. These general objects were first considered by Whitehead [1898]. Birkhoff [1935], [1944] initiated their systematic study.

Varieties are classes of universal algebras defined by identities. Groups, rings, left R-modules, etc., constitute varieties, and many of their properties are in fact properties of varieties. The main results in this chapter are two theorems of Birkhoff, one that characterizes varieties, one about subdirect decompositions. The chapter draws examples from Chapters I, III, V, VIII, and XIV, and is otherwise independent of previous chapters.

1. Universal Algebras

A universal algebra is a set with any number of operations. This section gives basic properties, such as the homomorphism and factorization theorems.

Definitions. Let $n \geqq 0$ *be a nonnegative integer. An* n-ary operation ω *on a set* X *is a mapping of* X^n *into* X*, where* X^n *is the Cartesian product of* n *copies of* X*; the number* n *is the* arity *of* ω.

An operation of arity 2 is a *binary operation*. An operation of arity 1 or *unary* operation on a set X is simply a mapping of X into X. By convention, the empty cardinal product X^0 is your favorite one element set, for instance, $\{\emptyset\}$; hence an operation of arity 0 or *constant* operation on a set X merely selects one element of X. Binary operations predominate in previous chapters, but constant and unary operations were encountered occasionally.

There are operations of infinite arity (for instance, infimums and supremums in complete lattices), but many properties in this chapter require finite arity. Order relations and partial operations are excluded for the same reason (a *partial operation* on a set X is a mapping of a subset of X^n into X and need not be defined for all $(x_1, \ldots, x_n) \in X^n$).

Universal algebras are classified by their *type*, which specifies number of operations and arities:

Definitions. *A* type *of universal algebras is an ordered pair of a set* T *and a mapping* $\omega \longmapsto n_\omega$ *that assigns to each* $\omega \in T$ *a nonnegative integer* n_ω*, the formal* arity *of* ω*. A* universal algebra*, or just* algebra*,* of type T *is an ordered pair of a set* A *and a mapping, the* type-T algebra structure *on* A*, that assigns to each* $\omega \in T$ *an operation* ω_A *on* A *of arity* n_ω*.*

For clarity ω_A is often denoted by just ω. For example, rings and lattices are of the same type, which has two elements of arity 2. Sets are universal algebras of type $T = \emptyset$. Groups and semigroups are of the same type, which has one element of arity 2. Groups may also be viewed as universal algebras with one binary operation, one constant operation that selects the identity element, and one unary operation $x \longmapsto x^{-1}$; the corresponding type has one element of arity 0, one element of arity 1, and one element of arity 2. Left R-modules are universal algebras with one binary operation (addition) and one unary operation $x \longmapsto rx$ for every $r \in R$. These descriptions will be refined in Section 2 when we formally define identities.

On the other hand, partially ordered sets and topological spaces are not readily described as universal algebras. Section XVI.10 explains why, to some extent.

Subalgebras of an algebra are subsets that are closed under all operations:

Definition. *A* subalgebra *of a universal algebra* A *of type* T *is a subset* S *of* A *such that* $\omega(x_1, \ldots, x_n) \in S$ *for all* $\omega \in T$ *of arity* n *and* $x_1, \ldots, x_n \in S$*.*

Let S be a subalgebra of A. Every operation ω_A on A has a restriction ω_S to S (sends S^n into S, if ω has arity n). This makes S an algebra of the same type as A, which is also called a *subalgebra* of A.

Readers will verify that the definition of subalgebras encompasses subgroups, subrings, submodules, etc., provided that groups, rings, modules, etc. are defined as algebras of suitable types. Once started, they may as well prove the following:

Proposition **1.1.** *The intersection of subalgebras of a universal algebra* A *is a subalgebra of* A*.*

Proposition **1.2.** *The union of a nonempty directed family of subalgebras of a universal algebra* A *is a subalgebra of* A*. In particular, the union of a nonempty chain of subalgebras of a universal algebra* A *is a subalgebra of* A*.*

Proposition 1.2 becomes false if infinitary operations are allowed.

Homomorphisms are mappings that preserve all operations.

Definition. Let A *and* B *be universal algebras of the same type* T*.* *A* homomorphism *of* A *into* B *is a mapping* $\varphi : A \longrightarrow B$ *such that*

$$\varphi\left(\omega_A(x_1, \ldots, x_n)\right) = \omega_B\left(\varphi(x_1), \ldots, \varphi(x_n)\right)$$

for all $n \geqq 0$*, all* $\omega \in T$ *of arity* n*, and all* $x_1, \ldots, x_n \in A$*.*

Readers will see that this definition yields homomorphisms of groups, rings, R-modules, lattices, and so forth. In general, the identity mapping 1_A on a

universal algebra A is a homomorphism. If $\varphi : A \longrightarrow B$ and $\psi : B \longrightarrow C$ are homomorphisms of algebras of the same type, then so is $\psi \circ \varphi : A \longrightarrow C$.

An *isomorphism* of universal algebras of the same type is a bijective homomorphism; then the inverse bijection is also an isomorphism. If S is a subalgebra of A, then the inclusion mapping $S \longrightarrow A$ is a homomorphism, the *inclusion homomorphism* of S into A.

Quotient algebras. Universal algebras differ from groups, and from group based structures like rings and modules, in that quotient algebras must in general be constructed from equivalence relations, rather than from subalgebras. For example, this is the case with sets, semigroups, and lattices.

In the case of sets, every mapping $f : X \longrightarrow Y$ induces an equivalence relation $f(x) = f(y)$ on X, which we denote by $\ker f$. Conversely, when $\mathcal{E}$ is an equivalence relation on a set X, there is a *quotient set* $X/\mathcal{E}$, which is the set of all equivalence classes, and a *canonical projection* $\pi : X \longrightarrow X/\mathcal{E}$, which assigns to each $x \in X$ its equivalence class; and then $\mathcal{E} = \ker \pi$.

Algebra structures are inherited by quotient sets as follows.

Proposition **1.3.** *Let A be a universal algebra of type T. For an equivalence relation $\mathcal{E}$ on A the following conditions are equivalent:*

(1) *there exists a type-T algebra structure on $A/\mathcal{E}$ such that the canonical projection $\pi : A \longrightarrow A/\mathcal{E}$ is a homomorphism;*

(2) *there exists a homomorphism $\varphi : A \longrightarrow B$ of universal algebras of type T such that $\ker \varphi = \mathcal{E}$;*

(3) $x_1 \mathrel{\mathcal{E}} y_1, \ldots, x_n \mathrel{\mathcal{E}} y_n$ *implies* $\omega(x_1, \ldots, x_n) \mathrel{\mathcal{E}} \omega(y_1, \ldots, y_n)$, *for all* $n \geqq 0$, *all* $\omega \in T$ *of arity* n, *and all* $x_1, \ldots, x_n, y_1, \ldots, y_n \in A$.

Then the algebra structure in (1) *is unique.*

Proof. (1) implies (2); that (2) implies (3) follows from the definitions.

(3) implies (1). Let $Q = A/\mathcal{E}$ and let $\pi : A \longrightarrow Q$ be the projection. For every $\omega \in T$ of arity n and every equivalence classes $E_1, \ldots, E_n$, the set

$$\omega_A(E_1, \ldots, E_n) = \{\, \omega_A(x_1, \ldots, x_n) \mid x_1 \in E_1, \ldots, x_n \in E_n \,\}$$

is contained in a single equivalence class, by (3). This yields a mapping $\omega_Q : Q^n \longrightarrow Q$, which assigns to $(E_1, \ldots, E_n) \in Q^n$ the equivalence class $\omega_Q(E_1, \ldots, E_n)$ that contains $\omega_A(E_1, \ldots, E_n)$. Then

$$\pi\left(\omega_A(x_1, \ldots, x_n)\right) = \omega_Q\left(\pi(x_1), \ldots, \pi(x_n)\right)$$

for all $x_1, \ldots, x_n \in A$, by definition of $\omega_A(E_1, \ldots, E_n)$; equivalently, $\pi \circ \omega_A = \omega_Q \circ \pi^n$. Moreover, ω_Q is the only mapping with this property, since π^n is surjective. This constructs a type-T algebra structure on Q, which is the only structure such that π is a homomorphism. □

Definitions. *A* congruence *on a universal algebra A is an equivalence relation $\mathcal{E}$ on A that satisfies the equivalent conditions in Proposition* 1.3*; then the universal algebra $A/\mathcal{E}$ is the* quotient *of A by $\mathcal{E}$.*

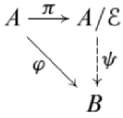
The quotient of a group G by a normal subgroup N is really the quotient of G by a congruence on G, namely, the partition of G into cosets of N, which is a congruence since $xN\,yN \subseteq xyN$ for all $x, y \in G$. In fact, all congruences on a group arise from normal subgroups (see the exercises). Readers will easily establish the following properties:

Proposition **1.4.** *The intersection of congruences on a universal algebra A is a congruence on A.*

Proposition **1.5.** *The union of a nonempty directed family of congruences on a universal algebra A is a congruence on A. In particular, the union of a nonempty chain of congruences on A is a congruence on A.*

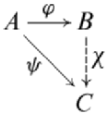
Quotient algebras have a universal property:

Theorem **1.6** (Factorization Theorem). *Let A be a universal algebra and let $\mathcal{E}$ be a congruence on A. Every homomorphism of universal algebras $\varphi : A \longrightarrow B$ such that* $\ker \varphi$ *contains $\mathcal{E}$ factors uniquely through the canonical projection $\pi : A \longrightarrow A/\mathcal{E}$ (there exists a homomorphism $\psi : A/\mathcal{E} \longrightarrow B$ unique such that $\varphi = \psi \circ \pi$):*



Readers will prove a more general property:

Theorem **1.7** (Factorization Theorem). *Let $\varphi : A \longrightarrow B$ be a homomorphism of universal algebras. If φ is surjective, then every homomorphism $\psi : A \longrightarrow C$ of universal algebras such that* $\ker \psi$ *contains* $\ker \varphi$ *factors uniquely through φ (there exists a homomorphism $\chi : B \longrightarrow C$ unique such that $\psi = \chi \circ \varphi$):*

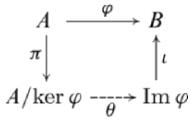


The homomorphism theorem for universal algebras reads as follows:

Theorem **1.8** (Homomorphism Theorem). *If $\varphi : A \longrightarrow B$ is a homomorphism of universal algebras, then* $\ker \varphi$ *is a congruence on A,* $\operatorname{Im} \varphi$ *is a subalgebra of B, and*

$$A/\ker \varphi \;\cong\; \operatorname{Im} \varphi;$$

in fact, there is an isomorphism $\theta : A/\ker f \longrightarrow \operatorname{Im} f$ unique such that $\varphi = \iota \circ \theta \circ \pi$, where $\iota : \operatorname{Im} f \longrightarrow B$ is the inclusion homomorphism and $\pi : A \longrightarrow A/\ker f$ is the canonical projection:



Proof. First, $\ker \varphi$ is a congruence on A by definition, and it is clear that $\operatorname{Im} \varphi$ is a subalgebra of B. Let $\theta : A/\ker \varphi \longrightarrow \operatorname{Im} \varphi$ be the bijection that sends an equivalence class E of $\ker \varphi$ to the sole element of $\varphi(E)$. Then $\iota \circ \theta \circ \pi = \varphi$, and θ is the only mapping of $A/\ker \varphi$ into $\operatorname{Im} \varphi$ with this property. We show that θ is a homomorphism. If $\omega \in T$ has arity n and $x_1, \ldots, x_n \in A$, then

$$\begin{aligned}\iota\big(\theta\big(\omega\,(\pi(x_1),\ \ldots,\ \pi(x_n))\big)\big) &= \iota\big(\theta\big(\pi\,(\omega(x_1,\ \ldots,\ x_n))\big)\big)\\ = \omega\big(\iota\big(\theta\,(\pi(x_1))\big),\ \ldots,\ \iota\big(\theta\,(\pi(x_n))\big)\big) &= \iota\big(\omega\big(\theta\,(\pi(x_1)),\ \ldots,\ \theta\,(\pi(x_n))\big)\big),\end{aligned}$$

since π, $\varphi = \iota \circ \theta \circ \pi$, and ι are homomorphisms. Hence

$$\theta\,\big(\omega\,(y_1,\ \ldots,\ y_n)\big) = \omega\,\big(\theta(y_1),\ \ldots,\ \varphi(y_n)\big)$$

for all $y_1, \ldots, y_n \in A/\ker \varphi$, since ι is injective and π is surjective. □

The isomorphism theorems extend to universal algebras.

Proposition **1.9.** *Let $\varphi : A \longrightarrow B$ be a homomorphism of universal algebras. If $\mathcal{E}$ is a congruence on B, then $\varphi^{-1}(\mathcal{E})$, defined by*

$$x\ \varphi^{-1}(\mathcal{E})\ y \text{ if and only if } \varphi(x)\ \mathcal{E}\ \varphi(y),$$

is a congruence on A. If φ is surjective, then $A/\varphi^{-1}(\mathcal{E}) \cong B/\mathcal{E}$, and the above defines a one-to-one correspondence between congruences on B and congruences on A that contain $\ker \varphi$.

The proof is an exercise; so is the second isomorphism theorem.

Exercises

1. Show that the intersection of subalgebras of an algebra A is a subalgebra of A.

2. Show that the union of a nonempty directed family of subalgebras of an algebra A is a subalgebra of A.

3. Let $A = \mathbb{R} \cup \{\infty\}$ be the algebra with one infinitary operation that assigns to each infinite sequence its least upper bound in A. Show that a directed union of subalgebras of A need not be a subalgebra of A.

4. Let $\varphi : A \longrightarrow B$ be a homomorphism of universal algebras, and let S be a subalgebra of A. Show that $\varphi(S) = \{\, \varphi(x) \mid x \in S \,\}$ is a subalgebra of B.

5. Let $\varphi : A \longrightarrow B$ be a homomorphism of universal algebras, and let T be a subalgebra of B. Show that $\varphi^{-1}(T) = \{\, x \in A \mid \varphi(x) \in T \,\}$ is a subalgebra of A.

6. Use the previous two exercises to produce a one-to-one correspondence between certain subalgebras of A and certain subalgebras of B.

7. Show that every congruence on a group is the partition into cosets of a unique normal subgroup; this defines a one-to-one correspondence between normal subgroups and congruences.

8. Produce a one-to-one correspondence between the ideals of a ring and its congruences.

9. Let S be a semigroup in which $xy = x$ for all $x, y \in S$. Show that every equivalence relation on S is a congruence. If S has five elements, then show that S has more congruences than subsets (hence there cannot be a one-to-one correspondence between suitable subsets of S and congruences on S).

10. Show that an equivalence relation on an algebra A is a congruence on A if and only if it is a subalgebra of $A \times A$.

11. Show that the intersection of congruences on an algebra A is a congruence on A.

12. Show that the union of a nonempty directed family of congruences on an algebra A is a congruence on A.

13. Let $\varphi : A \longrightarrow B$ be a surjective homomorphism. Show that every homomorphism $\psi : A \longrightarrow C$ such that $\ker \psi$ contains $\ker \varphi$ factors uniquely through φ.

14. Let $\varphi : A \longrightarrow B$ be a homomorphism and let $\mathcal{E}$ be a congruence on B. Show that $\varphi^{-1}(\mathcal{E})$ is a congruence on A.

15. If φ is surjective, then show that the previous exercise defines a one-to-one correspondence between congruences on B, and congruences on A that contain $\ker \varphi$; and that $A/\varphi^{-1}(\mathcal{E}) \cong B/\mathcal{E}$.

16. Let A be a universal algebra, let S be a subalgebra of A, and let $\mathcal{E}$ be a congruence on A. Show that $T = \{ x \in A \mid x \mathcal{E} s \text{ for some } s \in S \}$ is a subalgebra of A. Show that $\mathcal{E}$ induces congruences $\mathcal{A}$ on S and $\mathcal{B}$ on T, and that $T/\mathcal{B} \cong S/\mathcal{A}$.

2. Word Algebras

Word algebras are free universal algebras of a given type, and lead to a formal definition of identities.

Generators. Since every intersection of subalgebras of a universal algebra A is a subalgebra of A, there is, for every subset X of A, a subalgebra of A *generated by* X, which is the least subalgebra of A that contains X, and is the intersection of all subalgebras of A that contain X. The following is an exercise:

Proposition **2.1.** *Let X be a subset of a universal algebra A of type T. Define $S_k \subseteq A$ for every integer $k \geqq 0$ by $S_0 = X$; if $k > 0$, then S_k is the set of all $\omega(w_1, \ldots, w_n)$ in which $\omega \in T$ has arity n and $w_1 \in S_{k_1}, \ldots, w_n \in S_{k_n}$, with $k_1, \ldots, k_n \geqq 0$ and $1 + k_1 + \cdots + k_n = k$. The subalgebra $\langle X \rangle$ of A generated by X is $\langle X \rangle = \bigcup_{k \geqq 0} S_k$.*

By 2.1, every element of $\langle X \rangle$ can be calculated in finitely many steps from elements of X and operations on A (using k operations when $x \in S_k$). In general, this calculation can be performed in several different ways. The simplest

way to construct an algebra of type T that is generated by X is to ensure that different calculations yield different results. This is precisely what happens in the word algebra. Thus, word algebras are similar to free groups, except that, in word algebras, words like $x\,(yz)$ and $(xy)\,z$ are distinct, and words like xx^{-1} need not be omitted. Indeed, free groups must satisfy certain identities; word algebras are exempt from this requirement.

Construction. Given a type T of universal algebras and a set X, define a set W_k as follows: let $W_0 = X$; if $k > 0$, then W_k is the set of all sequences $(\omega, w_1, \ldots, w_n)$ in which $\omega \in T$ has arity n and $w_1 \in W_{k_1}, \ldots, w_n \in W_{k_n}$, where $k_1, \ldots, k_n \geqq 0$ and $1 + k_1 + \cdots + k_n = k$. This classifies words by the number k of operations $\omega \in T$ that appear in them.

For instance, if T consists of a single element μ of arity 2, then $W_0 = X$; the elements of W_1 are all (μ, x, y) with $x, y \in X$; the elements of W_2 are all $(\mu, x, \mu(y, z))$ and $(\mu, \mu(x, y), z)$ with $x, y, z, t \in X$; and so forth.

Definition. The word algebra *of type T on the set X is the union $W = W_X^T = \bigcup_{k \geqq 0} W_k$, with operations defined as follows: if $\omega \in T$ has arity n and $w_1 \in W_{k_1}, \ldots, w_n \in W_{k_n}$, then $\omega_W(w_1, \ldots, w_n) = (\omega, w_1, \ldots, w_n) \in W_k$, where $k = 1 + k_1 + \cdots + k_n$.*

Proposition **2.2.** *If $w \in W_X^T$, then $w \in W_Y^T$ for some finite subset Y of X.*

Proof. We have $w \in W_k$ for some k and prove the result by induction on k. If $w \in W_0$, then $w \in X$ and $Y = \{w\}$ serves. If $k > 0$ and $w \in W_k$, then $w = (\omega, w_1, \ldots, w_n)$, where $\omega \in T$ has arity n and $w_1 \in W_{k_1}, \ldots, w_n \in W_{k_n}$ for some $k_1, \ldots, k_n < k$. By the induction hypothesis, $w_i \in W_{Y_i}^T$ for some finite subset Y_i of X. Then $w_1, \ldots, w_n \in W_Y^T$, where $Y = Y_1 \cup \cdots \cup Y_n$ is a finite subset of X, and $w = (\omega, w_1, \ldots, w_n) \in W_Y^T$. □

Word algebras are blessed with a universal property:

Proposition **2.3.** *The word algebra W_X^T of type T on a set X is generated by X. Moreover, every mapping of X into a universal algebra of type T extends uniquely to a homomorphism of W_X^T into A.*

Proof. $W = W_X^T$ is generated by X, by 2.1. Let f be a mapping of X into a universal algebra A of type T. If $\varphi : W \longrightarrow A$ is a homomorphism that extends f, then necessarily $\varphi(x) = f(x)$ for all $x \in X$ and $\varphi(\omega, w_1, \ldots, w_n) = \omega_A\big(\varphi(w_1), \ldots, \varphi(x_n)\big)$ for all $(\omega, w_1, \ldots, w_n) \in W_k$. These conditions define (recursively) a unique mapping of W into A; therefore φ is unique; and we see that our mapping is a homomorphism. □

Identities. Word algebras yield precise definitions of relations and identities, which resemble the definition of group relations in Section I.7, except that an identity that holds in an algebra must hold for all elements of that algebra.

Formally, a *relation* of type T between the elements of a set X is a pair

(u, v), often written as an equality $u = v$, of elements of the word algebra W_X^T of type T; the relation (u, v) *holds* in a universal algebra A of type T *via* a mapping $f : X \longrightarrow A$ when $\varphi(u) = \varphi(v)$, where $\varphi : W_X^T \longrightarrow A$ is the homomorphism that extends f.

An *identity* is a relation that holds via every mapping. Since identities involve only finitely many elements at a time, the set X needs only arbitrarily large finite subsets and could be any infinite set. In the formal definition, X is your favorite countable infinite set (for instance, $\mathbb{N}$).

Definitions. Let X be a countable infinite set. An identity *of type T is a pair (u, v), often written as an equality $u = v$, of elements of the word algebra W_X^T of type T on the set X. An identity (u, v)* holds *in a universal algebra A of type T when $\varphi(u) = \varphi(v)$ for every homomorphism $\varphi : W_X^T \longrightarrow A$; then A* satisfies *the identity (u, v).*

In this definition, the choice of X is irrelevant in the following sense. Between any two countable infinite sets X and Y, there is a bijection $X \longrightarrow Y$, which induces an isomorphism $\theta : W_X^T \cong W_Y^T$. If $u, v \in W_X^T$, then the identity (u, v) holds in A if and only if the identity $(\theta(u), \theta(v))$ holds in A. In this sense the identities that hold in A do not depend on the choice of X.

For example, *associativity* for a binary operation μ is the identity

$$\big((\mu,\ x,\ \mu(y, z)),\ (\mu,\ \mu(x, y),\ z)\big),$$

where x, y, z are any three distinct elements of X. This identity holds in a universal algebra A if and only if

$$\begin{aligned}\mu_A\big(\varphi(x),\ \mu_A(\varphi(y), \varphi(z))\big) &= \varphi\big((\mu,\ x,\ \mu(y, z)\big) \\ &= \varphi\big(\mu,\ \mu(x, y),\ z\big) = \mu_A\big(\mu_A(\varphi(x),\ \varphi(y)),\ \varphi(z)\big)\end{aligned}$$

for every homomorphism $\varphi : W_X^T \longrightarrow A$. By 2.3, there is for every $a, b, c \in A$ a homomorphism $\varphi : W_X^T \longrightarrow A$ that sends x, y, z to a, b, c; hence the associativity identity holds in A if and only if $\mu_A(a,\ \mu_A(b, c)) = \mu_A(\mu_A(a, b),\ c)$ for all $a, b, c \in A$, if and only if μ_A is associative in the usual sense.

Exercises

1. Let X be a subset of a universal algebra A of type T. Show that the subalgebra $\langle X \rangle$ of A generated by X is $\langle X \rangle = \bigcup_{k \geqq 0} S_k$, where $S_k \subseteq A$ is defined by: $S_0 = X$; if $k > 0$, then S_k is the set of all $\omega(w_1, \ldots, w_n)$ in which $\omega \in T$ has arity n and $w_1 \in S_{k_1}, \ldots, w_n \in S_{k_n}$, with $k_1, \ldots, k_n \geqq 0$ and $1 + k_1 + \cdots + k_n = k$.

2. Show that every mapping $f : X \longrightarrow Y$ induces a homomorphism $W_f^T : W_X^T \longrightarrow W_Y^T$ of word algebras of type T, so that W_-^T becomes a functor from sets to universal algebras of type T.

3. Show that every universal algebra of type T is a homomorphic image of a word algebra of type T.

4. Let $T = \{\varepsilon, \iota, \mu\}$, where ε has arity 0, ι has arity 1, and μ has arity 2. Describe all elements of $W_0 \cup W_1 \cup W_2 \subseteq W_X^T$.

5. Let $T = \{\alpha\} \cup R$, where α has arity 2 and every $r \in R$ has arity 1. Describe all elements of $W_0 \cup W_1 \cup W_2 \subseteq W_X^T$.

6. Write commutativity as a formal identity.

7. Write distributivity in a ring as a formal identity.

8. Given a countable infinite set X, show that the set of all identities that hold in a universal algebra A of type T is a congruence on W_X^T.

3. Varieties

A variety consists of all algebras of the same type that satisfy a given set of identities. Most of the algebraic objects in this book (groups, rings, modules, etc.) constitute varieties. Many of their properties extend to all varieties. This section contains general characterizations and properties of varieties. Additional properties will be found in Section XVI.10.

Definition. Let T be a type of universal algebras and let X be a given countable infinite set. Every set $\mathfrak{I} \subseteq W_X^T \times W_X^T$ of identities of type T defines a class $\mathrm{V}(\mathfrak{I})$, which consists of all universal algebras of type T that satisfy every identity $(u, v) \in \mathfrak{I}$.

Definition. Let X be a given countable infinite set. A variety *of type T is a class $\mathcal{V} = \mathrm{V}(\mathfrak{I})$, which consists of all universal algebras of type T that satisfy some set $\mathfrak{I} \subseteq W_X^T \times W_X^T$ of identities of type T.*

The class of all universal algebras of type T is a variety, namely $\mathrm{V}(\emptyset)$. At the other extreme is the *trivial* variety $\mathcal{T}$ of type T, which consists of all universal algebras of type T with at most one element, and is characterized by the single identity $x = y$, where $x \neq y$; $\mathcal{T}$ is contained in every variety of type T.

Groups constitute a variety. The definition of groups as algebras with one binary operation is not suitable for this, since the existence of an identity element, or the existence of inverses, is not an identity. But we may regard groups as algebras with one binary operation, one constant "identity element" operation 1, and one unary operation $x \longmapsto x^{-1}$. An algebra of this type is a group if and only if $1x = x$ for all $x \in G$, $x1 = x$ for all $x \in G$, $xx^{-1} = 1$ for all $x \in G$, $x^{-1}x = 1$ for all $x \in G$, and $x(yz) = (xy)z$ for all $x, y, z \in G$; these five conditions are identities. (Dedicated readers will write them as formal identities.)

Abelian groups constitute a variety (of algebras with one binary operation, one constant "identity element" operation 0, and one unary operation $x \longmapsto -x$) defined by the five identities above and one additional commutativity identity $x + y = y + x$. Readers will verify that rings, R-modules, R-algebras, lattices,

etc., constitute varieties, when suitably defined. But fields do not constitute a variety; this follows from Proposition 3.1 below.

Properties. Every variety is closed under certain constructions.

A *homomorphic image* of a universal algebra A is a universal algebra B of the same type such that there exists a surjective homomorphism of A onto B; equivalently, that is isomorphic to the quotient of A by a congruence on A.

The *direct product* of a family $(A_i)_{i\in I}$ of algebras of the same type T is the Cartesian product $\prod_{i\in I} A_i$, equipped with componentwise operations,

$$\omega\big((x_{1i})_{i\in I},\ \ldots,\ (x_{ni})_{i\in I}\big),\ =\ \big(\omega\,(x_{1i},\ \ldots,\ x_{ni})\big)_{i\in I}$$

for all $(x_{1i})_{i\in I}, \ldots, (x_{ni})_{i\in I} \in \prod_{i\in I} A_i$ and $\omega \in T$ of arity n. The direct product comes with a *projection* $\pi_j : \prod_{i\in I} A_i \longrightarrow A_j$ for each $j \in J$, which sends $(x_i)_{i\in I} \in \prod_{i\in I} A_i$ to its j component x_j. The operations on $\prod_{i\in I} A_i$ are the only operations such that every projection is a homomorphism.

A *directed family* of algebras is a family $(A_i)_{i\in I}$ of algebras of the same type T, such that for every $i, j \in I$ there exists $k \in I$ such that A_i and A_j are subalgebras of A_k. A *directed union* of algebras of the same type T is the union $A = \bigcup_{i\in I} A_i$ of a directed family $(A_i)_{i\in I}$ of algebras of type T. Readers will verify that there is unique type T algebra structure on A such that every A_i is a subalgebra of A. Directed unions are particular cases of direct limits.

Proposition **3.1.** *Every variety is closed under subalgebras, homomorphic images, direct products, and directed unions.*

Proof. Let $\mathcal{V} = \mathrm{V}(\mathcal{I})$ be the variety of all universal algebras A of type T that satisfy a set $\mathcal{I} \subseteq W_X^T \times W_X^T$ of identities. An algebra A of type T belongs to $\mathcal{V}$ if and only if $\varphi(u) = \varphi(v)$ for every $(u, v) \in \mathcal{I}$ and homomorphism $\varphi : W_X^T \longrightarrow A$. Readers will verify that $\mathcal{V}$ contains every subalgebra of every $A \in \mathcal{V}$, and every direct product of algebras $A_i \in \mathcal{V}$.

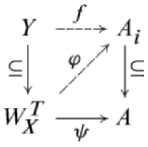
Let $A \in \mathcal{V}$ and let $\sigma : A \longrightarrow B$ be a surjective homomorphism. Let $\psi : W_X^T \longrightarrow B$ be a homomorphism. Since σ is surjective one can choose for each $x \in X$ one $f(x) \in A$ such that $\sigma\big(f(x)\big) = \psi(x)$. By 2.3, f extends to a homomorphism $\varphi : W_X^T \longrightarrow A$:

$$\begin{array}{ccc} X & \xrightarrow{\ f\ } & A \\ {\scriptstyle\subseteq}\downarrow & \nearrow_{\varphi} & \downarrow{\scriptstyle\sigma} \\ W_X^T & \xrightarrow[\ \psi\ ]{} & B \end{array}$$

Then $\psi = \sigma \circ \varphi$, since both agree on X. If now $(u, v) \in \mathcal{I}$, then $\varphi(u) = \varphi(v)$ and $\psi(u) = \sigma\big(\varphi(u)\big) = \sigma\big(\varphi(v)\big) = \psi(v)$. Therefore $B \in \mathcal{V}$.

Let $A = \bigcup_{i\in I} A_i$ be a directed union of universal algebras $A_i \in \mathcal{V}$. Let $(u, v) \in \mathcal{I}$ and let $\psi : W_X^T \longrightarrow A$ be a homomorphism. By 2.2, $u, v \in$

W_Y^T for some finite subset Y of X. Since Y is finite, some A_i contains all $\psi(y) \in \psi(Y)$. By 2.3, the restriction of ψ to Y extends to a homomorphism $\varphi : W_Y^T \longrightarrow A_i$:

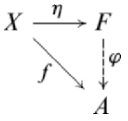


Then $\varphi(w) = \psi(w)$ for all $w \in W_Y^T$, since φ and ψ agree on Y. Hence $\psi(u) = \varphi(u) = \varphi(v) = \psi(v)$. Therefore $A \in \mathcal{V}$. □

By 3.1, fields do not constitute a variety (of any type), since, say, the direct product of two fields is not a field.

Free algebras. Free algebras are defined by their universal property:

Definition. Let X be a set and let $\mathcal{C}$ be a class of universal algebras of type T. A universal algebra F is free *on the set X in the class $\mathcal{C}$ when $F \in \mathcal{C}$ and there exists a mapping $\eta : X \longrightarrow F$ such that, for every mapping f of X into a universal algebra $A \in \mathcal{C}$, there exists a unique homomorphism $\varphi : F \longrightarrow A$ such that $\varphi \circ \eta = f$.*



For example, free groups are free in this sense in the class of all groups; W_X^T is free on X in the class of all universal algebras of type T, by Proposition 2.3. Some definitions of free algebras require the mapping η to be injective; readers will verify that this property holds when $\mathcal{C}$ is not trivial (when some $A \in \mathcal{C}$ has at least two elements). Readers will also prove the following:

Proposition **3.2.** *Let X be a set and let $\mathcal{C}$ be a class of universal algebras of the same type. If there exists a universal algebra F that is free on X in the class $\mathcal{C}$, then F and the mapping $\eta : X \longrightarrow F$ are unique up to isomorphism; moreover, F is generated by $\eta(X)$.*

Existence of free algebras is a main property of varieties. More generally:

Theorem **3.3.** *Let $\mathcal{C}$ be a class of universal algebras of the same type, that is closed under isomorphisms, direct products, and subalgebras (for instance, a variety). For every set X there exists a universal algebra that is free on X in the class $\mathcal{C}$.*

Proof. We give a direct proof; a better proof will be found in Section XVI.10. Given a set X, let $(\mathcal{E}_i)_{i\in I}$ be the set of all congruences $\mathcal{E}_i$ on W_X^T such that $W_X^T/\mathcal{E}_i \in \mathcal{C}$; let $C_i = W_X^T/\mathcal{E}_i$ and $\pi_i : W_X^T \longrightarrow C_i$ be the projection. Then $P = \prod_{i\in I} C_i \in \mathcal{C}$. Define a mapping $\eta : X \longrightarrow P$ by $\eta(x) = \big(\pi_i(x)\big)_{i\in I}$.

If $C \in \mathcal{C}$, then every mapping $f : X \longrightarrow C$ extends to a homomorphism φ of W_X^T into C. Then $\operatorname{Im}\varphi$ is a subalgebra of $C \in \mathcal{C}$, $W_X^T/\ker\varphi \cong \operatorname{Im}\varphi \in \mathcal{C}$, and $\ker\varphi = \mathcal{E}_i$ for some i. Composing $\pi_i : W_X^T \longrightarrow C_i = W_X^T/\ker\varphi$ and $W_X^T/\ker\varphi \cong \operatorname{Im}\varphi \subseteq C$ yields a homomorphism $\psi : P \longrightarrow C$ such that $\psi \circ \eta = f$. But ψ need not be unique with this property.

Let F be the set of all $p \in P$ such that $\zeta(p) = p$ for every endomorphism ζ of P such that $\zeta\big(\eta(x)\big) = \eta(x)$ for all $x \in X$. Then $\eta(X) \subseteq F$, F is a subalgebra of P, and $F \in \mathcal{C}$. If $C \in \mathcal{C}$ and $f : X \longrightarrow C$ is a mapping, then the above yields a homomorphism ψ of $F \subseteq P$ into C such that $\psi \circ \eta = f$. We show that ψ is unique, so that F is free on X in the class $\mathcal{C}$.

Let $\varphi, \psi : F \longrightarrow C$ be homomorphisms such that $\varphi \circ \eta = \psi \circ \eta$. Then $E = \{\, p \in F \mid \varphi(p) = \psi(p) \,\}$ contains $\eta(X)$ and is a subalgebra of F. Since $\eta : X \longrightarrow E$ and $E \in \mathcal{C}$, there is a homomorphism $\zeta : P \longrightarrow E$ such that $\zeta \circ \eta = \eta$. Then ζ is an endomorphism of P, $\zeta\big(\eta(x)\big) = \eta(x)$ for all $x \in X$, $p = \zeta(p) \in E$ for every $p \in F$, $\varphi(p) = \psi(p)$ for every $p \in F$, and $\varphi = \psi$. □

Birkhoff's theorem on varieties is the converse of Proposition 3.1:

Theorem **3.4** (Birkhoff [1935]). *A nonempty class of universal algebras of the same type is a variety if and only if it is closed under direct products, subalgebras, and homomorphic images.*

Proof. First we prove the following: when F is free in a class $\mathcal{C}$ on an infinite set, relations that hold in F yield identities that hold in every $C \in \mathcal{C}$:

Lemma **3.5.** *Let X be a given infinite countable set, let Y be an infinite set, and let $p, q \in W_Y^T$.*

(1) *There exist homomorphisms $\sigma : W_Y^T \longrightarrow W_X^T$ and $\mu : W_X^T \longrightarrow W_Y^T$ such that $\sigma \circ \mu$ is the identity on W_X^T and $\mu\big(\sigma(p)\big) = p$, $\mu\big(\sigma(q)\big) = q$.*

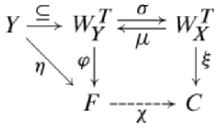
(2) *Let F be free on Y in a class $\mathcal{C}$ of universal algebras of type T and let $\varphi : W_Y^T \longrightarrow F$ be the homomorphism that extends $\eta : Y \longrightarrow F$. If $\varphi(p) = \varphi(q)$, then the identity $\sigma(p) = \sigma(q)$ holds in every algebra $C \in \mathcal{C}$.*

Proof. (1). By 2.2, $p, q \in W_Z^T$ for some finite subset Z of Y. There is an injection $h : X \longrightarrow Y$ such that $h(X)$ contains Z. The inverse bijection $h(X) \longrightarrow X$ can be extended to a surjection $g : Y \longrightarrow X$; then $g \circ h$ is the identity on X and $h\big(g(z)\big) = z$ for all $z \in Z$. By 2.3, $g : Y \longrightarrow W_X^T$ and $h : X \longrightarrow W_Y^T$ extend to homomorphisms σ and μ such that $\sigma \circ \mu$ is the identity on W_X^T and $\mu\big(\sigma(z)\big) = z$ for all $z \in Z$:

$$\begin{array}{ccc} X & \xrightarrow{\subseteq} & W_X^T \\ {\scriptstyle g}\big\downarrow\big\uparrow{\scriptstyle h} & & {\scriptstyle \sigma}\big\uparrow\big\downarrow{\scriptstyle \mu} \\ Y & \xrightarrow[\subseteq]{} & W_Y^T \end{array}$$

Then $\mu\big(\sigma(w)\big) = w$ for all $w \in W_Z^T$, and $\mu\big(\sigma(p)\big) = p$, $\mu\big(\sigma(q)\big) = q$.

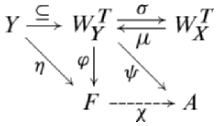
(2). Let $\xi : W_X^T \longrightarrow C$ be any homomorphism. Since $C \in \mathcal{C}$, the restriction of $\xi \circ \sigma$ to Y factors through η: there is a homomorphism $\chi : F \longrightarrow A$ such that $\chi\big(\eta(y)\big) = \xi\big(\sigma(y)\big)$ for all $y \in Y$:



Then uniqueness in Proposition 2.3 yields $\chi \circ \varphi = \xi \circ \sigma$. Hence $\varphi(p) = \varphi(q)$ implies $\xi\big(\sigma(p)\big) = \xi\big(\sigma(q)\big)$. Thus, the identity $\sigma(p) = \sigma(q)$ holds in C. □

Lemma **3.6.** *Let $\mathcal{C}$ be a class of universal algebras of the same type T, that is closed under isomorphisms, direct products, and subalgebras. Let A be a nonempty universal algebra of type T such that every identity that holds in every $C \in \mathcal{C}$ also holds in A. Then A is a homomorphic image of some $C \in \mathcal{C}$.*

Proof. There is an infinite set Y and a mapping f of Y into A such that A is generated by $f(Y)$: indeed, A is generated by some subset S; if S is infinite, then $Y = S$ serves; otherwise, construct Y by adding new elements to S, which f sends anywhere in A. Then 2.3 yields a homomorphism $\psi : W_Y^T \longrightarrow A$ that extends f. Since W_Y^T is generated by Y, $\operatorname{Im}\psi$ is generated by $\psi(Y)$, $\operatorname{Im}\psi = A$, and ψ is surjective. By 3.3 there exists an algebra F that is free on Y in $\mathcal{C}$. The homomorphism $\varphi : W_Y^T \longrightarrow F$ that extends $\eta : Y \longrightarrow F$ is surjective: since W_Y^T is generated by Y, $\operatorname{Im}\varphi$ is generated by $\varphi(Y) = \eta(Y)$ and $\operatorname{Im}\varphi = F$ by 3.2. We show that $\ker\varphi \subseteq \ker\psi$: if $\varphi(p) = \varphi(q)$, then 3.5 yields homomorphisms μ and σ such that $\sigma \circ \mu$ is the identity on W_X^T and the identity $\sigma(p) = \sigma(q)$ holds in every $C \in \mathcal{C}$; then the identity $\sigma(p) = \sigma(q)$ holds in A, $\psi\big(\mu(\sigma(p))\big) = \psi\big(\mu(\sigma(q))\big)$, and $\psi(p) = \psi(q)$. Therefore $\psi = \chi \circ \varphi$ for some homomorphism $\chi : F \longrightarrow A$; then χ is surjective, like ψ: □



Now, let $\mathcal{C}$ be a class of universal algebras of the same type T, that is closed under direct products, subalgebras, and homomorphic images (hence, closed under isomorphisms). Let X be any given countable infinite set and let $\mathcal{I} \subseteq W_X^T \times W_X^T$ be the set of all identities that hold in every algebra $C \in \mathcal{C}$. Then $\mathcal{C} \subseteq \mathrm{V}(\mathcal{I})$. Conversely, let $A \in \mathrm{V}(\mathcal{I})$. If $A = \emptyset$, then A is isomorphic to the empty subalgebra of some $C \in \mathcal{C}$ and $A \in \mathcal{C}$. If $A \neq \emptyset$, then A is a homomorphic image of some $C \in \mathcal{C}$, by 3.6, and again $A \in \mathcal{C}$. Thus $\mathcal{C} = \mathrm{V}(\mathcal{I})$ is a variety. □

We note some consequences of Birkhoff's theorem and its proof. First, every intersection of varieties is a variety: indeed, let $(\mathcal{V}_i)_{i\in I}$ be varieties of universal algebras of type T; then $\bigcap_{i\in I}\mathcal{V}_i$ is, like every $\mathcal{V}_i$, closed under direct products, subalgebras, and homomorphic images, and is therefore a variety. Consequently, every class $\mathcal{C}$ of algebras of type T *generates* a variety, which is the smallest variety of type T that contains $\mathcal{C}$.

Proposition **3.7.** *Let $\mathcal{C}$ be a class of universal algebras of type T. The variety generated by $\mathcal{C}$ consists of all homomorphic images of subalgebras of direct products of members of $\mathcal{C}$.*

Proof. For any class $\mathcal{C}$ of universal algebras of type T:

(1) a homomorphic image of a homomorphic image of a member of $\mathcal{C}$ is a homomorphic image of a member of $\mathcal{C}$; symbolically, $\mathrm{HH}\mathcal{C} \subseteq \mathrm{H}\mathcal{C}$;
(2) a subalgebra of a subalgebra of a member of $\mathcal{C}$ is a subalgebra of a member of $\mathcal{C}$; symbolically, $\mathrm{SS}\mathcal{C} \subseteq \mathrm{S}\mathcal{C}$;
(3) a direct product of direct products of members of $\mathcal{C}$ is a direct product of members of $\mathcal{C}$; symbolically, $\mathrm{PP}\mathcal{C} \subseteq \mathrm{P}\mathcal{C}$;
(4) a subalgebra of a homomorphic image of a member of $\mathcal{C}$ is a homomorphic image of a subalgebra of a member of $\mathcal{C}$; symbolically, $\mathrm{SH}\mathcal{C} \subseteq \mathrm{HS}\mathcal{C}$;
(5) a direct product of subalgebras of members of $\mathcal{C}$ is a subalgebra of a direct product of members of $\mathcal{C}$; symbolically, $\mathrm{PS}\mathcal{C} \subseteq \mathrm{SP}\mathcal{C}$;
(6) a direct product of homomorphic images of members of $\mathcal{C}$ is a homomorphic image of a direct product of members of $\mathcal{C}$; symbolically, $\mathrm{PH}\mathcal{C} \subseteq \mathrm{HP}\mathcal{C}$.

Now, every variety $\mathcal{V}$ that contains $\mathcal{C}$ also contains all homomorphic images of subalgebras of direct products of members of $\mathcal{C}$: symbolically, $\mathrm{HSP}\mathcal{C} \subseteq \mathcal{V}$. Conversely, $\mathrm{HSP}\mathcal{C}$ is closed under homomorphic images, subalgebras, and direct products: by the above, $\mathrm{HHSP}\mathcal{C} \subseteq \mathrm{HSP}\mathcal{C}$, $\mathrm{SHSP}\mathcal{C} \subseteq \mathrm{HSSP}\mathcal{C} \subseteq \mathrm{HSP}\mathcal{C}$, and $\mathrm{PHSP}\mathcal{C} \subseteq \mathrm{HPSP}\mathcal{C} \subseteq \mathrm{HSPP}\mathcal{C} \subseteq \mathrm{HSP}\mathcal{C}$; therefore $\mathrm{HSP}\mathcal{C}$ is a variety. □

Once generators are found for a variety, Proposition 3.7 provides very loose descriptions of all members of that variety. This is useful for structures like semigroups or lattices, that are difficult to describe precisely.

Another consequence of the above is a one-to-one correspondence between varieties of type T and certain congruences on W_X^T. A congruence $\mathcal{E}$ on a universal algebra A is *fully invariant* when $a\ \mathcal{E}\ b$ implies $\zeta(a)\ \mathcal{E}\ \zeta(b)$, for every $a, b \in A$ and endomorphism ζ of A.

Proposition **3.8.** *Let X be a given infinite countable set. There is a one-to-one, order reversing correspondence between varieties of type T and fully invariant congruences on W_X^T.*

Proof. For each variety $\mathcal{V}$, let $\mathrm{I}(\mathcal{V}) \subseteq W_X^T \times W_X^T$ be the set of all identities that hold in every $A \in \mathcal{V}$: the set of all $(u, v) \in W_X^T \times W_X^T$ such that $\xi(u) = \xi(v)$ for every homomorphism $\xi : W_X^T \longrightarrow A$ such that $A \in \mathcal{V}$. If $(u, v) \in \mathrm{I}(\mathcal{V})$ and ζ is an endomorphism of W_X^T, then $\xi\big(\zeta(u)\big) = \xi\big(\zeta(v)\big)$ for every homo-

morphism $\xi : W_X^T \longrightarrow A$ such that $A \in \mathcal{V}$, since $\xi \circ \zeta$ is another such homomorphism, and $(\zeta(u),\ \zeta(v)) \in \mathrm{I}(\mathcal{V})$. Moreover, $\mathrm{I}(\mathcal{V})$ is the intersection of congruences $\ker \xi$ and is a congruence on W_X^T. Hence $\mathrm{I}(\mathcal{V})$ is a fully invariant congruence on W_X^T.

Conversely, a fully invariant congruence $\mathcal{E}$ on W_X^T is a set of identities and determines a variety $\mathrm{V}(\mathcal{E})$ of type T. The constructions I and V are order reversing; we show that $\mathrm{I}\big(\mathrm{V}(\mathcal{E})\big) = \mathcal{E}$ and $\mathrm{V}\big(\mathrm{I}(\mathcal{V})\big) = \mathcal{V}$ for every fully invariant congruence $\mathcal{E}$ and variety $\mathcal{V}$, so that I and V induce the one-to-one correspondence in the statement.

First we show that $F = W_X^T/\mathcal{E} \in \mathrm{V}(\mathcal{E})$ when $\mathcal{E}$ is fully invariant. Let $\pi : W_X^T \longrightarrow F$ be the projection and let $\xi : W_X^T \longrightarrow F$ be any homomorphism. For every $x \in X$ choose $g(x) \in W_X^T$ such that $\pi\big(g(x)\big) = \xi(x)$. By 2.3, $g : X \longrightarrow W_X^T$ extends to an endomorphism ζ of W_X^T; then $\pi \circ \zeta = \xi$, since they agree on X. Hence $(u, v) \in \mathcal{E}$ implies $(\zeta(u),\ \zeta(v)) \in \mathcal{E}$ and $\xi(u) = \pi\big(\zeta(u)\big) = \pi\big(\zeta(v)\big) = \xi(v)$. Thus $F \in \mathrm{V}(\mathcal{E})$. (Readers will verify that F is the free algebra on X in $\mathrm{V}(\mathcal{E})$, and generates $\mathrm{V}(\mathcal{E})$.)

Now, $\mathcal{E} \subseteq \mathrm{I}\big(\mathrm{V}(\mathcal{E})\big)$, since every $(u, v) \in \mathcal{E}$ holds in every $A \in \mathrm{V}(\mathcal{E})$. Conversely, if $(u, v) \in \mathrm{I}\big(\mathrm{V}(\mathcal{E})\big)$ holds in every $A \in \mathrm{V}(\mathcal{E})$, then (u, v) holds in $F \in \mathrm{V}(\mathcal{E})$, $\pi(u) = \pi(v)$, and $(u, v) \in \mathcal{E}$. Thus $\mathrm{I}\big(\mathrm{V}(\mathcal{E})\big) = \mathcal{E}$.

Conversely, let $\mathcal{V}$ be a variety of type T. Then $\mathcal{V} \subseteq \mathrm{V}\big(\mathrm{I}(\mathcal{V})\big)$, since every member of $\mathcal{V}$ satisfies every identity in $\mathrm{I}(\mathcal{V})$. Conversely, let $A \in \mathrm{V}\big(\mathrm{I}(\mathcal{V})\big)$. If $A = \emptyset$, then A is isomorphic to the empty subalgebra of some $C \in \mathcal{V}$ and $A \in \mathcal{V}$. If $A \neq \emptyset$, then A is a homomorphic image of some $C \in \mathcal{V}$, by 3.6, and again $A \in \mathcal{V}$. Thus $\mathcal{V} = \mathrm{V}\big(\mathrm{I}(\mathcal{V})\big)$. □

Exercises

1. Write a set of formal identities that characterize groups.

2. Write a set of formal identities that characterizes rings [with identity elements].

3. Show that lattices constitute a variety (of universal algebras with two binary operations).

4. Show that modular lattices constitute a variety (of universal algebras with two binary operations).

5. Show that Boolean lattices constitute a variety.

6. Show that the direct product $\prod_{i\in I} A_i$ of universal algebras $(A_i)_{i\in I}$ of type T, and its projections $\pi_j : \prod_{i\in I} A_i \longrightarrow A_j$, have the following universal property: for every universal algebra A of type T and homomorphisms $\varphi_i : A \longrightarrow A_i$, there is a unique homomorphism $\varphi : A \longrightarrow \prod_{i\in I} A_i$ such that $\pi_i \circ \varphi = \varphi_i$ for all $i \in I$.

7. Let $A = \bigcup_{i\in I} A_i$ be the directed union $A = \bigcup_{i\in I} A_i$ of a directed family $(A_i)_{i\in I}$ of universal algebras of the same type T. Show that there is unique type-T algebra structure on A such that every A_i is a subalgebra of A.

8. Define and construct direct limits of universal algebras of type T; verify that the direct limit is a directed union of homomorphic images.

9. Define and construct inverse limits of universal algebras of type T.

Prove the following:

10. Every variety is closed under subalgebras and closed under direct products.

11. If F is free on a set X in a class $\mathcal{C}$ that contains an algebra with more than one element, then $\eta : X \longrightarrow F$ is injective.

12. Let $\mathcal{C}$ be a class of universal algebras of the same type. The free algebra F on a set X in the class $\mathcal{C}$ and the corresponding mapping $\eta : X \longrightarrow F$, if they exist, are unique up to isomorphism.

13. Let $\mathcal{C}$ be a class of universal algebras of the same type. If F is free on a set X in the class $\mathcal{C}$, then F is generated by $\eta(X)$.

14. Let $\mathcal{C}$ be a class of universal algebras of the same type. If F is free in $\mathcal{C}$ on an infinite set X, then every identity that holds in F holds in every member of $\mathcal{C}$.

15. If $\mathcal{V}$ is a variety, and F is free in $\mathcal{V}$ on an infinite set, then $\mathcal{V}$ is generated by F (so that every member of $\mathcal{V}$ is a homomorphic image of a subalgebra of a direct product of copies of F). (Use the previous exercice.)

16. The variety of all abelian groups is generated by $\mathbb{Z}$.

17. The variety of all commutative semigroups is generated by $\mathbb{N}$.

18. Given a countable infinite set X, when $\mathcal{E}$ is a fully invariant congruence on W_X^T, then $W_X^T/\mathcal{E}$ is free on X in the variety $\mathrm{V}(\mathcal{E})$.

19. There are no more than $\left|\mathbb{R}\right|$ varieties of groups.

4. Subdirect Products

Subdirect products were introduced by Birkhoff [1944]. They provide loose but useful descriptions of structures that are difficult to describe more precisely; examples in this section include distributive lattices and commutative semigroups.

Definition. *A* subdirect product *of a family* $(A_i)_{i\in I}$ *of universal algebras of the same type* T *is a subalgebra* P *of the Cartesian product* $\prod_{i\in I} A_i$ *such that* $\pi_i(P) = A_i$ *for all* $i \in I$, *where* $\pi_j : \prod_{i\in I} A_i \longrightarrow A_j$ *is the projection.*

For example, in the vector space $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$, a straight line $x = at$, $y = bt$, $z = ct$ is a subdirect product of $\mathbb{R}$, $\mathbb{R}$, and $\mathbb{R}$ if and only if $a, b, c \neq 0$. Thus, a subdirect product of algebras may be very thinly spread in their direct product. Only the conditions $\pi_i(P) = A_i$ prevent subdirect products from being too dangerously thin.

Proposition **4.1.** *Let* $(A_i)_{i\in I}$ *be universal algebras of type* T. *A universal algebra* A *of type* T *is isomorphic to a subdirect product of* $(A_i)_{i\in I}$ *if and only*

if there exist surjective homomorphisms $\varphi_i : A \longrightarrow A_i$ *such that* $\bigcap_{i\in I} \ker \varphi_i$ *is the equality on* A.

Here, $\bigcap_{i\in I} \ker \varphi_i$ is the equality on A if and only if $\varphi_i(x) = \varphi_i(y)$ for all $i \in I$ implies $x = y$, if and only if $x \neq y$ in A implies $\varphi_i(x) \neq \varphi_i(y)$ for some $i \in I$. Homomorphisms with this property are said to *separate* the elements of A.

Proof. Let P be a subdirect product of $(A_i)_{i\in I}$. The inclusion homomorphism $\iota : P \longrightarrow \prod_{i\in I} A_i$ and projections $\pi_j : \prod_{i\in I} A_i \longrightarrow A_j$ yield surjective homomorphisms $\rho_i = \pi_i \circ \iota : P \longrightarrow A_i$ that separate the elements of P, since elements of the product that have the same components must be equal. If now $\theta : A \longrightarrow P$ is an isomorphism, then the homomorphisms $\varphi_i = \rho_i \circ \theta$ are surjective and separate the elements of A.

Conversely, assume that there exist surjective homomorphisms $\varphi_i : A \longrightarrow A_i$ that separate the elements of A. Then $\varphi : x \longmapsto \big(\varphi_i(x)\big)_{i\in I}$ is an injective homomorphism of A into $\prod_{i\in I} A_i$. Hence $A \cong \operatorname{Im}\varphi$; moreover, $\operatorname{Im}\varphi$ is a subdirect product of $(A_i)_{i\in I}$, since $\pi_i(\operatorname{Im}\varphi) = \varphi_i(A) = A_i$ for all i. □

Direct products are associative: if $I = \bigcup_{j\in J} I_j$ is a partition of I, then $\prod_{i\in I} A_i \cong \prod_{j\in J} \big(\prod_{i\in I_j} A_i\big)$. So are subdirect products, as readers will deduce from Proposition 4.1:

Proposition **4.2.** *Let* $(A_i)_{i\in I}$ *be universal algebras of type* T *and let* $I = \bigcup_{j\in J} I_j$ *be a partition of* I. *An algebra* A *of type* T *is isomorphic to a subdirect product of* $(A_i)_{i\in I}$ *if and only if* A *is isomorphic to a subdirect product of algebras* $(P_j)_{j\in J}$ *in which each* P_j *is a subdirect product of* $(A_i)_{i\in I_j}$.

Subdirect decompositions. A *subdirect decomposition* of A into algebras $(A_i)_{i\in I}$ of the same type is an isomorphism of A onto a subdirect product of $(A_i)_{i\in I}$. By 4.1, subdirect decompositions of A can be set up from within A from suitable families of congruences on A. They are inherited by every variety $\mathcal{V}$: when A has a subdirect decomposition into algebras $(A_i)_{i\in I}$, then $A \in \mathcal{V}$ if and only if $A_i \in \mathcal{V}$ for all i, by 3.1.

Subdirect decompositions of A give loose descriptions of A in terms of presumably simpler components $(A_i)_{i\in I}$. The simplest possible components are called *subdirectly irreducible*:

Definition. A universal algebra A *is* subdirectly irreducible *when* A *has more than one element and, whenever* A *is isomorphic to a subdirect product of* $(A_i)_{i\in I}$, *at least one of the projections* $A \longrightarrow A_i$ *is an isomorphism.*

Proposition **4.3.** *A universal algebra* A *is subdirectly irreducible if and only if* A *has more than one element and the equality on* A *is not the intersection of congruences on* A *that are different from the equality.*

The proof is an exercise in further deduction from Proposition 4.1.

Theorem **4.4** (Birkhoff [1944]). *Every nonempty universal algebra is isomorphic to a subdirect product of subdirectly irreducible universal algebras. In any variety $\mathcal{V}$, every nonempty universal algebra $A \in \mathcal{V}$ is isomorphic to a subdirect product of subdirectly irreducible universal algebras $A_i \in \mathcal{V}$.*

Proof. Let A be a nonempty algebra of type T. By 1.5, the union of a chain of congruences on A is a congruence on A. Let $a, b \in A$, $a \neq b$ of A. If $(\mathcal{C}_i)_{i\in I}$ is a chain of congruences on A, none of which contains the pair (a, b), then the union $\mathcal{C} = \bigcup_{i\in I} \mathcal{C}_i$ is a congruence on A that does not contain the pair (a, b). By Zorn's lemma, there is a congruence $\mathcal{M}_{a,b}$ on A that is maximal such that $(a, b) \notin \mathcal{M}_{a,b}$. The intersection $\bigcap_{a,b\in A,\, a\neq b} \mathcal{M}_{a,b}$ cannot contain any pair (a, b) with $a \neq b$ and is the equality on A. By 4.1, A is isomorphic to a subdirect product of the quotient algebras $A/\mathcal{M}_{a,b}$.

The algebra $A/\mathcal{M}_{a,b}$ has at least two elements, since $\mathcal{M}_{a,b}$ does not contain the pair (a, b). Let $(\mathcal{C}_i)_{i\in I}$ be congruences on $A/\mathcal{M}_{a,b}$, none of which is the equality. Under the projection $\pi : A \longrightarrow A/\mathcal{M}_{a,b}$, the inverse image $\pi^{-1}(\mathcal{C}_i)$ is, by 1.9, a congruence on A, which properly contains $\ker \pi = \mathcal{M}_{a,b}$, hence contains the pair (a, b), by the maximality of $\mathcal{M}_{a,b}$. Hence $\big(\pi(a),\ \pi(b)\big) \in \mathcal{C}_i$ for every i, and $\bigcap_{i\in I} \mathcal{C}_i$ is not the equality on $A/\mathcal{M}_{a,b}$. Thus $A/\mathcal{M}_{a,b}$ is subdirectly irreducible, by 4.3. □

Abelian groups. Abelian groups can be used to illustrate these results.

Congruences on an abelian group are induced by its subgroups. Hence an abelian group A (written additively) is isomorphic to a subdirect product of abelian groups $(A_i)_{i\in I}$ if and only if there exist surjective homomorphisms $\varphi_i : A \longrightarrow A_i$ such that $\bigcap_{i\in I} \operatorname{Ker} \varphi_i = 0$; an abelian group A is subdirectly irreducible if and only if A has more than one element and 0 is not the intersection of nonzero subgroups of A.

By Theorem 4.4, every abelian group is isomorphic to a subdirect product of subdirectly irreducible abelian groups. The latter are readily determined.

Proposition **4.5.** *An abelian group is subdirectly irreducible if and only if it is isomorphic to $\mathbb{Z}_{p^\infty}$ or to $\mathbb{Z}_{p^n}$ for some $n > 0$.*

Proof. Readers will verify that $\mathbb{Z}_{p^\infty}$ and $\mathbb{Z}_{p^n}$ (where $n > 0$) are subdirectly irreducible. Conversely, every abelian group A can, by X.4.9 and X.4.10, be embedded into a direct product of copies of $\mathbb{Q}$ and $\mathbb{Z}_{p^\infty}$ for various primes p. Hence A is isomorphic to a subdirect product of subgroups of $\mathbb{Q}$ and $\mathbb{Z}_{p^\infty}$.

Now, $\mathbb{Q}$ has subgroups $\mathbb{Z}$, $2\mathbb{Z}$, …, $2^k\mathbb{Z}$, …, whose intersection is 0; since $\mathbb{Q}/2^k\mathbb{Z} \cong \mathbb{Q}/\mathbb{Z}$, $\mathbb{Q}$ is isomorphic to a subdirect product of subgroups of $\mathbb{Q}/\mathbb{Z}$. Readers will verify that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to a direct sum of $\mathbb{Z}_{p^\infty}$'s (for various primes p). By 4.2, $\mathbb{Q}$ is isomorphic to a subdirect product of subgroups of $\mathbb{Z}_{p^\infty}$ (for various primes p). Then every abelian group A is isomorphic

to a subdirect product of subgroups of $\mathbb{Z}_{p^\infty}$ (for various primes p). If A is subdirectly irreducible, then A is isomorphic to a subgroup of some $\mathbb{Z}_{p^\infty}$. □

Distributive lattices. Birkhoff's earlier theorem, XIV.4.8, states that every distributive lattice is isomorphic to a sublattice of the lattice of all subsets 2^X of some set X. We give another proof of this result, using subdirect products.

Since distributive lattices constitute a variety, every distributive lattice is isomorphic to a subdirect product of subdirectly irreducible distributive lattices, by 4.4. One such lattice is the two-element lattice $L_2 = \{0, 1\}$, which has only two congruences and is subdirectly irreducible by 4.3.

Proposition **4.6.** *Every distributive lattice is isomorphic to a subdirect product of two-element lattices. A distributive lattice is subdirectly irreducible if and only if it has just two elements.*

Proof. To each prime ideal $P \neq \emptyset, L$ of a distributive lattice L there corresponds a lattice homomorphism φ_P of L onto L_2, defined by $\varphi_P(x) = 0$ if $x \in P$, $\varphi_P(x) = 1$ if $x \notin P$. The homomorphisms φ_P separate the elements of L: if $a, b \in L$ and $a \neq b$, then, say, $a \nleqq b$, and Lemma XIV.4.7 provides a prime ideal P of L that contains the ideal $I = \{ x \in L \mid x \leqq b \}$ but does not contain $a \notin I$, so that $\varphi_P(b) \neq \varphi_P(a)$. By 4.1, L is isomorphic to a subdirect product of copies of L_2. If L is subdirectly irreducible, then some φ_P is an isomorphism and $L \cong L_2$ has just two elements. □

A direct product $\prod_{i \in I} L_2$ of copies of L_2 is isomorphic to the lattice 2^I of all subsets of the index set I; the isomorphism sends $(x_i)_{i \in I} \in \prod_{i \in I} L_2$ to $\{ i \in I \mid x_i = 1 \}$. Hence a subdirect product of copies of L_2 is, in particular, isomorphic to a sublattice of some 2^I; thus, Theorem XIV.4.8 follows from 4.6.

Commutative semigroups include abelian groups but can be much more complex; for instance, there are about 11.5 million nonisomorphic commutative semigroups of order 9. We use subdirect products to assemble finitely generated commutative semigroups from the following kinds of semigroups.

Definitions. A semigroup S is cancellative *when $ac = bc$ implies $b = c$, and $ca = cb$ implies $a = b$, for all $a, b, c \in S$. A* nilsemigroup *is a semigroup S with a zero element z (such that $sz = z = zs$ for all $s \in S$) in which every element is* nilpotent *($s^m = z$ for some $m > 0$).*

Finitely generated commutative semigroups are related to ideals of polynomial rings. By Proposition 1.3, a congruence $\mathcal{E}$ on a commutative semigroup S is an equivalence relation $\mathcal{E}$ on S such that $a \mathcal{E} b$ and $c \mathcal{E} d$ implies $ac \mathcal{E} bd$. We saw in Section I.1 that the free commutative semigroup with generators $x_1, \ldots, x_n$ consists of all nonconstant monomials $X^a = X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n} \in R[X_1, \ldots, X_n]$, where R is any commutative ring [with identity]. Every ideal $\mathfrak{E}$ of $R[X_1, \ldots, X_n]$ *induces* a congruence $\mathcal{E}$ on F, in which $X^a \mathcal{E} X^b$ if and only if $X^a - X^b \in \mathfrak{E}$; then $\mathfrak{E}$ *determines* a commutative semigroup $F/\mathcal{E}$ and,

by extension, every commutative semigroup $S \cong F/\mathcal{E}$.

Lemma **4.7.** *Let F be the free commutative semigroup on $X_1, \ldots, X_n$. Every congruence $\mathcal{E}$ on F is induced by an ideal of $\mathbb{Z}[X_1, ..., X_n]$. Every commutative semigroup with n generators is determined by an ideal of $\mathbb{Z}[X_1, ..., X_n]$.*

Proof. Let $\mathfrak{E}$ be the ideal of $\mathbb{Z}[X_1, ..., X_n]$ generated by all binomials $X^a - X^b$ such that $X^a \mathrel{\mathcal{E}} X^b$ in F. The ideal $\mathfrak{E}$ induces a congruence $\overline{\mathcal{E}}$ on F, in which $X^a \mathrel{\overline{\mathcal{E}}} X^b$ if and only if $X^a - X^b \in \mathfrak{E}$. Then $\mathcal{E} \subseteq \overline{\mathcal{E}}$. We prove the converse inclusion. Since $X^a \mathrel{\mathcal{E}} X^b$ implies $X^a X^c \mathrel{\mathcal{E}} X^b X^c$, the ideal $\mathfrak{E}$ consists of all finite sums $\sum_i n_i(X^{a_i} - X^{b_i})$ in which $n_i \in \mathbb{Z}$ and $X^{a_i} \mathrel{\mathcal{E}} X^{b_i}$ for all i. Since $\mathcal{E}$ is symmetric we may further assume that $n_i > 0$ for all i. Hence $X^a \mathrel{\overline{\mathcal{E}}} X^b$ if and only if there is an equality

$$X^a - X^b = \textstyle\sum_i n_i(X^{a_i} - X^{b_i}) \tag{1}$$

in which $n_i > 0$ and $X^{a_i} \mathrel{\mathcal{E}} X^{b_i}$ for all i.

If $\mathcal{E} \subsetneqq \overline{\mathcal{E}}$, then there is an equality (1) in which $X^a \mathrel{\mathcal{E}} X^b$ does not hold, and in which $\sum_i n_i$ is as small as possible. Since X^a appears in the left hand side of (1), it must also appear in the right hand side, and $X^{a_k} = X^a$ for some k. Subtracting $X^{a_k} - X^{b_k}$ from both sides of (1) then yields an equality

$$X^{b_k} - X^b = \textstyle\sum_i m_i(X^{a_i} - X^{b_i})$$

in which $X^b \mathrel{\mathcal{E}} X^{b_k}$ does not hold (otherwise, $X^a \mathrel{\mathcal{E}} X^b$) and $\sum_i m_i = \left(\sum_i n_i\right) - 1$, an intolerable contradiction. Therefore $\mathcal{E} = \overline{\mathcal{E}}$ is induced by $\mathfrak{E}$.

Now, let S be a commutative semigroup with n generators $x_1, \ldots, x_n$. There is a homomorphism $\pi : F \longrightarrow S$ that sends X_i to x_i, defined by $\pi\left(X_1^{a_1} \cdots X_n^{a_n}\right) = x_1^{a_1} \cdots x_n^{a_n}$; π is surjective, since S is generated by $x_1, \ldots, x_n$. The congruence $\mathcal{E} = \ker \pi$ on F is induced by an ideal $\mathfrak{E}$ of $\mathbb{Z}[X_1, ..., X_n]$; hence $S \cong F/\mathcal{E}$ is determined by $\mathfrak{E}$. □

Proposition **4.8.** *Every commutative semigroup with n generators has a subdirect decomposition into finitely many commutative semigroups determined by primary ideals of $\mathbb{Z}[X_1, ..., X_n]$.*

Proof. Let S be a commutative semigroup with n generators $x_1, \ldots, x_n$. By 4.7, $S \cong F/\mathcal{E}$, where $\mathcal{E}$ is induced by an ideal $\mathfrak{E}$ of $\mathbb{Z}[X_1, ..., X_n]$. In the Noetherian ring $\mathbb{Z}[X_1, ..., X_n]$, the ideal $\mathfrak{E}$ is the intersection of finitely many primary ideals $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r$. Hence $\mathcal{E}$ is the intersection of the congruences $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$ induced by $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r$. By 1.9, $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$ are the inverse images under $\pi : F \longrightarrow S$ of congruences $\mathcal{C}_1, \ldots, \mathcal{C}_r$ on S such that $S/\mathcal{C}_i \cong F/\mathcal{Q}_i$. Since $\mathcal{E} = \mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_r$, the equality on S is the intersection of $\mathcal{C}_1, \ldots, \mathcal{C}_r$, and S is isomorphic to a subdirect product of the semigroups $S/\mathcal{C}_1, \ldots, S/\mathcal{C}_r$ determined by $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r$. □

Now, let S be determined by a primary ideal $\mathfrak{Q}$ of $\mathbb{Z}[X_1, ..., X_n]$, so that

$\pi(X^a) = \pi(X^b)$ if and only if $X^a - X^b \in \mathfrak{Q}$, where $\pi : F \longrightarrow S$ is the projection. The radical $\mathfrak{P}$ of $\mathfrak{Q}$ is a prime ideal of $\mathbb{Z}[X_1, ..., X_n]$. Moreover:

(1) If $X^c \in \mathfrak{Q}$, then $z = \pi(X^c)$ is a zero element of S: indeed, $X^a X^c - X^c \in \mathfrak{Q}$ for all $X^a \in F$, hence $sz = z$ for all $s = \pi(X^a) \in S$.

(2) If $X^c \in \mathfrak{P}$, then $(X^c)^m \in \mathfrak{Q}$ for some $m > 0$; hence S has a zero element z, and $s = \pi(X^c) \in S$ is nilpotent ($s^m = z$). Since $\mathfrak{P}$ is an ideal of $\mathbb{Z}[X_1, ..., X_n]$, the elements $s = \pi(X^c)$ such that $X^c \in \mathfrak{P}$ constitute an *ideal* N of S ($s \in N$ implies $st \in N$ for all $t \in S$).

(3) If $X^c \notin \mathfrak{P}$, then $X^c(X^a - X^b) \in \mathfrak{Q}$ implies $X^a - X^b \in \mathfrak{Q}$; hence $s = \pi(X^c) \in S$ is *cancellative in* S ($st = su$ implies $t = u$, when $t, u \in S$). Since $\mathfrak{P}$ is a prime ideal of $\mathbb{Z}[X_1, ..., X_n]$, X^c, $X^d \notin \mathfrak{P}$ implies $X^c X^d \notin \mathfrak{P}$; hence the elements $s = \pi(X^c)$ such that $X^c \notin \mathfrak{P}$ constitute a *subsemigroup* C of S ($s, t \in C$ implies $st \in C$).

By (2) and (3), a semigroup that is determined by a primary ideal $\mathfrak{Q}$ of $\mathbb{Z}[X_1, ..., X_n]$ is either a nilsemigroup (if $\mathfrak{P}$ contains every $X^c \in F$), or cancellative (if $\mathfrak{P}$ contains no $X^c \in F$), or *subelementary* in the following sense:

Definition. A subelementary *semigroup is a commutative semigroup that is the disjoint union $S = N \cup C$ of an ideal N and a nonempty subsemigroup C, such that N is a nilsemigroup and every element of C is cancellative in S.*

Subelementary semigroups are named for their relationship, detailed in the exercises, to previously defined "elementary" semigroups.

Every finitely generated commutative semigroup is now a subdirect product of finitely many nilsemigroups, cancellative semigroups, and subelementary semigroups. Readers will verify that a subdirect product of finitely many nilsemigroups is a nilsemigroup, and that a subdirect product of cancellative semigroups is cancellative. Subdirect decompositions need only one of each; hence we have:

Theorem **4.9** (Grillet [1975]). *Every finitely generated commutative semigroup is isomorphic to a subdirect product of a nilsemigroup, a cancellative semigroup, and finitely many subelementary semigroups.*

Exercises

1. Let $(A_i)_{i \in I}$ be universal algebras of type T and let $I = \bigcup_{j \in J} I_j$ be a partition of I. Show that a universal algebra A of type T is isomorphic to a subdirect product of $(A_i)_{i \in I}$ if and only if A is isomorphic to a subdirect product of algebras $(P_j)_{j \in J}$ in which each P_j is a subdirect product of $(A_i)_{i \in I_j}$.

2. Let $\mathcal{C}$ be a class of universal algebras of type T. If every A_i is a subdirect product of members of $\mathcal{C}$, then show that every subdirect product of $(A_i)_{i \in I}$ is a subdirect product of members of $\mathcal{C}$.

3. Let $\mathcal{C}$ be a class of universal algebras of type T. Show that every subalgebra of a subdirect product of members of $\mathcal{C}$ is a subdirect product of subalgebras of members of $\mathcal{C}$.

4. Prove that an algebra A is subdirectly irreducible if and only if A has more than one element and the equality on A is not the intersection of congruences that are different from the equality.

5. Show that $\mathbb{Z}_{p^\infty}$ and $\mathbb{Z}_{p^n}$ are subdirectly irreducible (when $n > 0$).

6. Show that $\mathbb{Z}$ is isomorphic to a subdirect product of cyclic groups of prime order p, one for each prime p.

Readers who are allergic to semigroups should avoid the remaining exercises.

7. Show that the zero element of a semigroup, if it exists, is unique.

8. Show that a finitely generated commutative nilsemigroup is finite.

9. Prove *Rédei's theorem* [1956]: the congruences on a finitely generated commutative semigroup satisfy the ascending chain condition.

10. Verify that a subdirect product of finitely many nilsemigroups is a nilsemigroup.

11. Verify that a subdirect product of cancellative semigroups is cancellative.

12. What can you say of a commutative semigroup that is determined by a prime ideal of $\mathbb{Z}[X_1, ..., X_n]$? by a semiprime ideal of $\mathbb{Z}[X_1, ..., X_n]$?

13. Show that a finite cancellative semigroup is a group.

14. Show that a cancellative commutative semigroup has a group of fractions, in which it can be embedded.

15. Show that a cancellative commutative semigroup is subdirectly irreducible if and only if its group of fractions is subdirectly irreducible.

16. Prove the following: if a subelementary semigroup $S = N \cup C$ is subdirectly irreducible, then its cancellative part C is subdirectly irreducible, or has just one element.

17. Prove *Malcev's theorem* [1958]: every subdirectly irreducible, finitely generated commutative semigroup is finite; hence every finitely generated commutative semigroup is isomorphic to a subdirect product of of finite semigroups. (Use the previous two exercises.)

18. A commutative semigroup S is *elementary* when it is the disjoint union $S = N \cup G$ of an ideal N and an abelian group G, such that N is a nilsemigroup, G is a group, and every element of G is cancellative in S. Show that a subelementary semigroup $S = N \cup C$ can be embedded into an elementary semigroup (e.g., a semigroup of fractions s/c).

19. Show that every finite semigroup is isomorphic to a subdirect product of a nilsemigroup, a group, and finitely many elementary semigroups.