GENERAL THEORY OF ALGEBRAS

DON PIGOZZI

1. Lattices

A notion of "order" plays an important role in the theory of algebraic structures. Many of the key results of the theory relate important properties of algebraic structures and classes of such strutures to questions of order, e.g., the ordering of substructures, congruence relations, etc. Order also plays an important role in the computational part of the theory; for example, recursion can conveniently be defined as the least fixed point of an interative procedure. The most important kind of ordering in the general theory of algebras is a lattice ordering, which turns out to be definable by identities in terms of of the least-upper-bound (the *join*) and greatest-lower-bound (the *meet*) operations.

Definition 1.1. A *lattice* is a nonempty set A with two binary operations $\vee\colon A \times A \to A$ (*join*) and $\wedge\colon A \times A \to A$ (*meet*) satisfying the following identities.

(L1)	$x \vee y = y \vee x$	$x \wedge y = y \wedge x$	(*commutative laws*)
(L2)	$(x \vee y) \vee z = x \vee (y \vee z)$	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	(*transitive laws*)
(L3)	$x \vee x = x$	$x \wedge x = x$	(*idempotent laws*)
(L4)	$x \vee (x \wedge y) = x$	$x \wedge (x \vee y) = x$	(*absorption laws*)

Examples. (1) (2-element) Boolean algebra: $A = \{\mathrm{T}, \mathrm{F}\}$.

a	b	$a \vee b$	$a \wedge b$
T	T	T	T
T	F	T	F
F	T	T	F
F	F	F	F

(2) Natural numbers: $A = \boldsymbol{\omega} = \{0, 1, 2, \ldots\}$. $a \vee b = \mathrm{LCM}(a, b)$, the *least common multiple* of a and b; $a \wedge b = \mathrm{GCD}(a, b)$, the *greatest common divisor* of a and b.

1.1. **Some Set Theory.** Sets will normally be represented by uppercase Roman letters: $A, B, C, \ldots$, and elements of sets by lowercase Roman letters $a, b, c, \ldots$. The set of all subsets of a set A is denoted by $\mathcal{P}(A)$.

$f\colon A \to B$: a function with *domain* A and *codomain* B. $f(A) = \{\, f(a) : a \in A \,\} \subseteq B$ is the *range* of f.

$\langle a_1, \ldots, a_n \rangle$: *ordered n-tuple*, for $n \in \omega$. $\langle a_1, \ldots, a_n \rangle = \langle b_1, \ldots, b_n \rangle$ iff (if and only if), for all $i \leq n$, $a_i = b_i$.

Date: first week.

$A_1 \times \cdots \times A_n = \{ \langle a_1, \ldots, a_n \rangle : \text{ for all } i \leq n,\ a_i \in A_i \}$: *Cartesian* (or *direct*) *product.*

$A_1 \times \cdots \times A_n = A^n$ if $A_i = A$ for all $i \leq n$: *n-th Cartesian power of A.*

An *n-ary operation on A* is a function f from the n-th Cartesian power of A to itself, i.e., $f\colon A^n \to A$. We write $f(a_1, \ldots, a_n)$ for $f(\langle a_1, \ldots, a_n \rangle)$. f is *binary* if $n = 2$. If f is binary we often write $a\, f\, b$ instead of $f(a, b)$; this is *infix notation.*

An *n-ary relation on A* is a subset R of the n-th Cartesian power of A, i.e., $R \subseteq A^n$. R is *binary* if $n = 2$. In this case $a\, R\, a'$ means the same as $\langle a, a' \rangle \in R$.

Definition 1.2. A *partially ordered set* (*poset*) is a nonempty set A with a binary relation $\leq \subset A \times A$ satisfying the following conditions

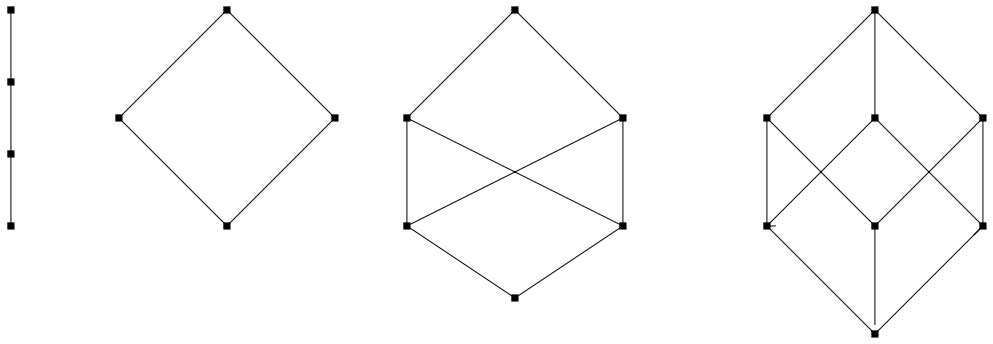
(P1)	$x \leq x$	(*reflexive law*)
(P2)	$x \leq y$ and $y \leq z$ implies $x \leq z$	(*transitive law*)
(P3)	$x \leq y$ and $y \leq x$ implies $x = y$.	(*antisymmetric law*)

A is a *linearly ordered set* or a *chain* if it satisfies

$$x \leq y \text{ or } y \leq x$$

$a \leq b \leq c$ means $a \leq b$ and $b \leq c$. $a < b$ means $a \leq b$ and $a \neq b$. $a \prec b$ means $a < b$ and, for all $c \in A$, $a \leq c \leq b$ implies $a = c$ or $c = b$; we say that b *covers* a in this case, and $\prec$ is called the *covering relation.* Note that, if A is finite, then $a \prec b$ iff there exist $c_0, \ldots, c_n \in A$ such that $a = c_0 \prec c_1 \prec \cdots \prec c_n = b$. So every finite poset is completely determined by its covering relation.

The *Hasse diagram* of a finite poset is a graphical representation of of its covering relation, where $a \prec b$ if there is a edge that goes up from a to b. Here are the Hasse diagrams of some posets. The set of natural numbers ω with the natural ordering, although infinite, is



also determined by its covering relation. But the set of real numbers $\mathbb{R}$ with the natural ordering is not; the covering relation is empty.

Let A be a poset with partial ordering $\leq$. Let X be a subset of elements of A. $\mathrm{UB}(X) = \{ y \in A : x \leq y \text{ for every } x \in X \}$; the set of *upper bounds of X*. The *least-upper-bound* of X, in symbols $\mathrm{LUB}(X)$, is the smallest element of $\mathrm{UB}(X)$, if it exists, i.e., $\mathrm{LUB}(X)$ is the unique element a of $\mathrm{UB}(X)$ such that $a \leq y$ for all $y \in \mathrm{UB}(X)$. The set of *lower bounds*, $\mathrm{LB}(X)$ and the *greatest-lower-bound*, $\mathrm{GLB}(X)$ are defined by interchanging $\leq$ and $\geq$.

Definition 1.3. A poset A is a *lattice ordered set* (a *loset*) if every pair of elements has a least-upper-bound (LUB) and a greatest-lower-bound (GLB).

Among the posets displayed above only the third fails to be a loset.

The lattice $\langle A, \vee, \wedge\rangle$ will be denoted by $\boldsymbol{A}$; in general boldface letters will be used to denote lattices and posets and the corresponding lowercase letter will denote the underlying set of the lattice or poset. The underlying set is also called the *universe* or *carrier* of the lattice or poset.

Theorem 1.4. (i) *If $\langle A, \leq\rangle$ is a loset, then $\langle A, \mathrm{LUB}, \mathrm{GLB}\rangle$ is a lattice.*

(ii) *Conversely, if $\langle A, \vee, \wedge\rangle$ is a lattice, then $\langle A, \leq\rangle$ is a loset where $a \leq b$ if $a \vee b = b$ (equivalently, $a \wedge b = a$).*

Proof. (i). The axioms (L1)–(L4) of lattices must be verified. (L4) says that $\mathrm{LUB}(a, \mathrm{GLB}(a, b)) = a$. But $\mathrm{GLB}(a, b) \leq a$ by definition so the above equality is obvious.

(L2). We must show that

$$\mathrm{LUB}(a, \mathrm{LUB}(b, c)) = \mathrm{LUB}(\mathrm{LUB}(a, b), c). \tag{1}$$

Let d be the left-hand side of this equation. $d \geq a$ and $d \geq \mathrm{LUB}(b, c)$. The second inequality implies $d \geq b$, $d \geq c$. From $d \geq a$ and $d \geq b$ we get $d \geq \mathrm{LUB}(a, b)$, which together with $d \geq c$ gives $d \geq \mathrm{LUB}(\mathrm{LUB}(a, b), c))$. This gives one of the two inclusions of (1). The proof of the other is similar. The verification of the remaining lattice axioms is left as an exercise.

(ii). We note first of all that, if $a \vee b = b$, then $a \wedge b = a \wedge (a \vee b) = a$ by (L4). Similarly, $a \wedge b = a$ implies $a \vee b = (a \wedge b) \vee b = b$ by (L1) and (L4). We verify (P1)–(P4).

(P1). $a \leq a$ iff $a \wedge a = a$.

(P2). We must verify that $a \vee b = b$ and $b \vee c = c$ implies $a \vee c = c$. $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$.

(P3). Suppose $a \vee b = b$ and $b \vee a = a$. Then $a = b$ by the commutativity of $\vee$. □

For any set A, $\langle \mathcal{P}(A), \subseteq\rangle$ is clearly a loset with $\mathrm{LUB}(X, Y) = X \cup Y$ and $\mathrm{GLB}(X, Y) = X \cap Y$. Thus by the theorem $\langle \mathcal{P}, \cup, \cap\rangle$ is a lattice.

If $\langle A, \leq\rangle$ is a loset, then $a \leq b$ iff $\mathrm{LUB}(a, b) = b$ (equivalently, $\mathrm{GLB}(a, b) = a$). Thus, if we start with a loset $\langle A, \leq\rangle$ and form a lattice $\langle A, \mathrm{LUB}, \mathrm{GLB}\rangle$ by (i) and then a loset by (ii) we get back the original loset. Conversely, the following lemma shows that if we start with a lattice, form a loset by (ii) and then a lattice by (i), we get back the original lattice.

Lemma 1.5. *Let $\langle A, \vee, \wedge\rangle$ be a lattice, and define $a \leq b$ and as in part* (ii) *of the theorem. Then, for all $a, b \in A$, $\mathrm{LUB}(a, b) = a \vee b$ and $\mathrm{GLB}(a, b) = a \wedge b$.*

Proof. $a \wedge (a \vee b) = a$. So $a \leq a \vee b$. $b \wedge (a \vee b) = b \wedge (b \vee c) = b$. So $b \leq a \vee b$. Suppose $a, b \leq c$. Then $a \vee c = c$ and $b \vee c = c$. Thus $(a \vee b) \vee c = a \vee (b \vee c) = a \vee c = c$. So $a \vee b \leq c$. Hence $\mathrm{LUB}(a, b) = a \vee b$. The proof that $\mathrm{GLB}(a, b) = a \vee b$ is obtain from the above by interchanging "$\leq$" and "$\geq$" and interchanging "$\vee$" and "$\wedge$". □

So the mappings between lattices and losets given in Theorem 1.4 are inverses on one another; the lattice $\langle A, \vee, \wedge\rangle$ and the loset $\langle A, \leq\rangle$ are essentially the same and we normally will not distinguish between them in the sequel.

Definition 1.6. An *isomorphism* between lattices $\boldsymbol{A} = \langle A, \vee, \wedge\rangle$ and $\boldsymbol{B} = \langle B, \vee, \wedge\rangle$ is a bijection (i.e., a one-one correspondence) $h\colon A \leftrightarrow B$ such that, for all $a, a' \in A$, $h(a \vee a') =$

$h(a) \vee h(a')$ and $h(a) \wedge a') = h(a) \wedge h(a')$. $\boldsymbol{A}$ and $\boldsymbol{B}$ are *isomorphic*, in symbols $\boldsymbol{A} \cong \boldsymbol{B}$, if there is an isomorphism h between them. We write $h\colon \boldsymbol{A} \cong \boldsymbol{B}$.

Definition 1.7. An *order-preserving map* between posets $\boldsymbol{A} = \langle A, \leq \rangle$ and $\boldsymbol{B} = \langle B, \leq \rangle$ is a function $h\colon A \to B$ such that, for all $a, a' \in A$, $a \leq a'$ implies $h(a) \leq h(a')$. A mapping h is *strictly order-preserving* if $a \leq a'$ iff $h(a) \leq h(a')$.

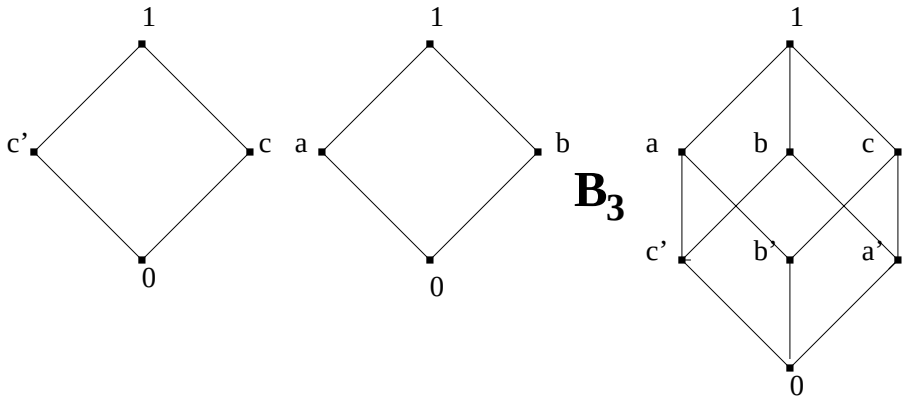
A mapping h is (*strictly*) *order-preserving map* between two lattices if it (strictly) preserves that lattice orderings.

Theorem 1.8. *Let $\boldsymbol{A} = \langle A, \vee, \wedge \rangle$ and $\boldsymbol{B} = \langle B, \vee, \wedge \rangle$ be lattices and Let $h\colon A \to B$. Then $h\colon \boldsymbol{A} \cong \boldsymbol{B}$ iff h is a strictly order-preserving bijection, i.e., h is a bijection and h and h^{-1} are both order-preserving.*

Proof. $\Longrightarrow$: Let $a, a' \in A$. We must show that $h(\mathrm{LUB}(a, a')) = \mathrm{LUB}(h(a), h(a'))$ and $h(\mathrm{GLB}(a, a')) = \mathrm{GLB}(h(a), h(a'))$. Let $a'' = \mathrm{LUB}(a, a')$. $a, a' \leq a''$. So $h(a), h(a') \leq h(a'')$. Suppose $h(a), h(a') \leq b \in B$. Then $a = h^{-1}(h(a)), b = h^{-1}(h(a')) \leq h^{-1}(b)$. So $a'' \leq h^{-1}(b)$ and $h(a'') \leq h^{-1}(h^{-1}(b)) = b$. The proof for GLB is similar.

$\Longleftarrow$: Exercise. □

Definition 1.9. Let $\boldsymbol{A} = \langle A, \vee^{\boldsymbol{A}}, \wedge^{\boldsymbol{A}} \rangle$, $\boldsymbol{B} = \langle B, \vee^{\boldsymbol{B}}, \wedge^{\boldsymbol{B}} \rangle$ be lattices. $\boldsymbol{A}$ is a *sublattice* of $\boldsymbol{B}$ if $A \subseteq B$ and $a \vee^{\boldsymbol{B}} a' = a \vee^{\boldsymbol{A}} a'$ and $a \wedge^{\boldsymbol{B}} a' = a \wedge^{\boldsymbol{A}} a'$ for all $a, a' \in A$.



The lattice on the left is a sublattice of $\boldsymbol{B}_3$ (the three-atom Boolean algebra).

Let $\boldsymbol{A} = \langle A, \leq^{\boldsymbol{A}} \rangle$, $\boldsymbol{B} = \langle B, \leq^{\boldsymbol{B}} \rangle$ be posets. $\boldsymbol{B}$ is a *subposet* of $\boldsymbol{A}$ if $B \subseteq A$ and, for all $b, b' \in B$, $b \leq^{\boldsymbol{B}} b'$ iff $b \leq^{\boldsymbol{A}} b'$.

Suppose $\boldsymbol{A}$ and $\boldsymbol{B}$ are losets. In general it is not true that $\boldsymbol{B}$ is a sublattice of $\boldsymbol{A}$ if $\boldsymbol{B}$ is a subposet of $\boldsymbol{A}$. For example, the second lattice in the above figure is a subposet of $\boldsymbol{B}_3$ but not a sublattice.

Let $\boldsymbol{G} = \langle G, \cdot, ^{-1}, e \rangle$ be a group, and let $\mathrm{Sub}(\boldsymbol{G}) = \{ H : H < G \}$ be the set of (underlying sets of) all subgroups of $\boldsymbol{G}$. $\langle \mathrm{Sub}(\boldsymbol{G}), \subseteq \rangle$ is a loset, where $H \wedge K = H \cap K$ and $H \vee K = \bigcap \{ L < G : H, K < G \}$. $\langle \mathrm{Sub}(\boldsymbol{G}), \subseteq \rangle$ is a subposet of $\langle \mathcal{P}(G), \subseteq \rangle$ but is not a sublattice. $H \vee K = H \cup K$ iff $H \subseteq K$ or $K \subseteq H$.

Definition 1.10. A lattice $\boldsymbol{A} = \langle A, \vee, \wedge \rangle$ is *distributive* each of join and meet distributives over the other, i.e.,

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z), \tag{D1}$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z). \tag{D2}$$

Theorem 1.11. *Either one of the two distributive laws is sufficient, i.e., in any lattice* $\boldsymbol{A}$, (D1) *implies* (D2) *and* (D2) *implies* (D1).

Also, in every lattice $\boldsymbol{A}$*, the following inidenitities hold*

$$x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z), \tag{2}$$

$$x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z). \tag{3}$$

Thus either of the two opposite inidentities is sufficient for distributivity.

Proof. (D1) $\Longrightarrow$ (D2).

$$\begin{aligned}
(x \vee y) \wedge (x \vee z) &= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z), && \text{(D1)} \\
&= x \vee ((x \wedge z) \vee (y \wedge z)), && \text{(L1), (L4) and (D1)} \\
&= (x \vee (x \wedge z)) \vee (y \wedge z), && \text{(L2)} \\
&= x \vee (y \wedge z), && \text{(L4).}
\end{aligned}$$

The proof of (D1) $\Longrightarrow$ (D2) is obtained from the above by interchanging "$\vee$" and "$\wedge$".

Proof of (2). $x \wedge y \leq x$ and $x \wedge z \leq x$ together imply

$$(x \wedge y) \vee (x \wedge z) \leq x. \tag{4}$$

$x \wedge y \leq y \leq y \vee z$ and $x \wedge z \leq z \leq y \vee z$ together imply

$$(x \wedge y) \vee (x \wedge z) \leq y \vee z. \tag{5}$$

(4) and (5) together together imply (2).

The proof of (3) is obtained by interchanging "$\vee$" and "$\wedge$" and "$\leq$" and "$\geq$". □

In every lattice, $x \leq y$ and $z \leq w$ together imply both $x \wedge z \leq y \wedge w$ and $x \vee z \leq y \vee w$. To see this we note that $x \wedge z \leq x \leq y$ and $x \wedge z \leq z \leq w$ together imply $x \wedge z \leq y \wedge w$. Proof of the other implication is obtained by the usual interchanges.

As an special case, we get that $x \leq y$ implies each of $x \wedge z \leq y \wedge z$, $z \wedge x \leq z \wedge y$, $x \vee z \leq y \vee z$, and $z \vee x \leq z \vee y$. Thus, for every lattice $\boldsymbol{A}$ and every $a \in A$, the mappings $x \mapsto x \wedge a, a \wedge x, x \vee a, a \vee x$ are all order preserving.

Department of Mathematics, Iowa State University, Ames, IA 50011, USA
E-mail address: dpigozzi@iastate.edu

Definition 1.12. A poset $\boldsymbol{A} = \langle A, \leq \rangle$ is *complete* if, for every $X \subseteq A$, $\mathrm{LUB}(X)$ and $\mathrm{GLB}(X)$ both exist.

We denote $\mathrm{LUB}(X)$ by $\bigvee X$ (if it exists) and $\mathrm{GLB}(X)$ by $\bigwedge X$.

If $\boldsymbol{A}$ is a lattice and $X = \{x_1, \ldots, x_n\}$ is finite, then $\mathrm{LUB}(X)$ and $\mathrm{GLB}(X)$ always exist and equal $x_1 \vee \cdots \vee x_n$ and $x_1 \wedge \cdots \wedge x_n$, respectively. Thus every finite lattice is complete.

$\langle \omega, \leq \rangle$, $\langle \mathbb{Q}, \leq \rangle$ ($\mathbb{Q}$ the rational numbers), and $\langle \mathbb{R}, \leq \rangle$ ($\mathbb{R}$ the real numbers) are not complete, but the natural numbers and the real numbers can be made complete by adjoining a largest element ∞ to the natural numbers and both a smallest element $-\infty$ and a largest element $+\infty$ to the reals. The rationals cannot be completed so easily; in fact, for every irrational number r, $\{\, q \in \mathbb{Q} : q < r \,\}$ fails to have a least upper bound. For any set A, $\langle \boldsymbol{\mathcal{P}}(A), \subseteq \rangle$ is a complete lattice. $\bigvee K = \bigcap K$ and $\bigwedge K = \bigcup K$ for every $K \subseteq \boldsymbol{\mathcal{P}}(A)$.

Theorem 1.13. *Let $\boldsymbol{A} = \langle A, \leq \rangle$ be a poset. For every $X \subseteq A$, $\bigvee X$ exists iff, for every $X \subseteq A$, $\bigwedge X$ exists. Thus a poset and in particular a lattice is complete iff every subset has a* LUB*, equivalently, iff every subset has a* GLB*.*

Proof. $\Longrightarrow$. Assume $\mathrm{LUB}(X)$ exists for every $X \subseteq A$. It suffices to show that, for every $X \subseteq A$, $\mathrm{GLB}(X) = \mathrm{LUB}(\mathrm{LB}(X))$; recall that $\mathrm{LB}(X) = \{\, y \in A : \text{for every } x \in X,\ y \leq x \,\}$, the set of lower bounds of X. Let $a = \mathrm{LUB}(\mathrm{LB}(X))$. For every $x \in X$, $x \in \mathrm{UB}(\mathrm{LB}(X))$. Thus, for every $x \in X$, $x \geq \mathrm{LUB}(\mathrm{LB}(X)) = a$. So $a \in \mathrm{LB}(X)$, and clearly, for every $y \in \mathrm{LB}(X)$, $a \geq y$.

$\Longleftarrow$. The proof is the dual of the one above, i.e., it is obtained by interchanging "$\leq$" and "$\geq$", "LUB" and "GLB", and "UB" and "LB". $\square$

For any group $\boldsymbol{G}$, $\mathbf{Sub}(\boldsymbol{G}) = \langle \mathrm{Sub}(\boldsymbol{G}), \subseteq \rangle$ is a complete lattice. For every $K \subseteq \mathrm{Sub}(\boldsymbol{G})$, $\bigvee K = \bigcap K$ and $\bigwedge K = \bigcap \{\, H \in \mathrm{Sub}(\boldsymbol{G}) : \bigcup K \subseteq H \,\}$.

Why doesn't $\langle \omega, \leq \rangle$ contradict the above theorem? Isn't the greatest lower bound of any set of natural numbers the smallest natural number in the set? This is true for any *nonempty* set, but $\emptyset$ has no GLB in ω. For any poset $\boldsymbol{A}$, $\mathrm{GLB}(\emptyset)$ (if it exists) is the largest element of $\boldsymbol{A}$, and $\mathrm{LUB}(\emptyset)$ is the smallest element of $\boldsymbol{A}$.

Let $\boldsymbol{A} = \langle \omega \cup \{a, b, \infty\}, \leq \rangle$, where $\leq$ is the natural order on ω, for every $n \in \omega$, $n < a, b, \infty$, and $a, b < \infty$. Every finite subset of A has a LUB (including $\emptyset$), but $\mathrm{GLB}(a, b)$ does not exist. So the requirement that X ranges over *all* subsets of A in the theorem is critical. But if $\boldsymbol{A}$ is a finite poset, and $\mathrm{LUB}(a, b)$ exists for every pair of elements of $\boldsymbol{A}$ and $\boldsymbol{A}$ has a smallest element, then $\boldsymbol{A}$ is a complete lattice.

Some notation: if $\boldsymbol{A}$ is a complete lattice, $1 = \bigvee A = \bigwedge \emptyset$ will denote the largest element of $\boldsymbol{A}$, and $0 = \bigwedge A = \bigvee \emptyset$ will denote the smallest element.

Definition 1.14. Let $\boldsymbol{A} = \langle A, \vee, \wedge \rangle$ and $\boldsymbol{B} = \langle B, \vee, \wedge \rangle$ be complete lattices. $\boldsymbol{B}$ is a *complete sublattice* of $\boldsymbol{A}$ if, for every $X \subseteq A$, $\bigvee^{\boldsymbol{B}} X = \bigvee^{\boldsymbol{A}} X$ and $\bigwedge^{\boldsymbol{B}} X = \bigwedge^{\boldsymbol{A}} X$.

$\langle \{-2\} \cup (-1, +1) \cup \{+2\}, \leq \rangle$ is a complete lattice and a sublattice of the complete lattice $\langle \{-\infty\} \cup \mathbb{R} \cup \{+\infty\}, \leq \rangle$ but not a complete sublattice.

Definition 1.15. Let A be a set. $E \subseteq A^2$ is an *equivalence relation* on A if

(E1) $$x \, R \, x,$$

(E2) $$x \, E \, y \text{ and } y \, E \, z \text{ imply } x \, E \, z,$$

(E3) $$x \, E \, y \text{ implies } y \, E \, x. \quad (\textit{symmetric law})$$

$\mathrm{Eq}(A)$ will denote the set of all equivalence relations on A. Let $K \subseteq \mathrm{Eq}(A)$.

(6) $$\bigcap K \in \mathrm{Eq}(A).$$

Check (E1)–(E3).

(E2). Assume $\langle a, b\rangle, \langle b, c\rangle \in \bigcap K$. For every $E \in K$, $\langle a, b\rangle, \langle b, c\rangle \in E$. Thus, for every $E \in K$, $\langle a, c\rangle \in E$. So $\langle a, c\rangle \in \bigcap K$. (E1) and (E3) are verified similarly.

So $\langle \mathrm{Eq}(A), \subseteq\rangle$ is a complete lattice with $\bigvee K = \bigcap K$ and

(7) $$\bigwedge K = \bigcap\{\, E \in \mathrm{Eq}(A) : \bigcup K \subset E \,\}.$$

The smallest equivalence relation on A is the *identity* or *diagonal relation*, $\Delta_A = \{\, \langle a, a\rangle : a \in A \,\}$, read "delta A". The largest equivalence relation is the *universal relation*, $\nabla_A = A \times A$, read "nabla A".

The description of the join operation in (7) is what can be called a "coinductive" or "from above" characterization; it is very useful for theoretical purposes, for example proving general propositions about the join, but it does not give much information about what the elements of the join of K look like in terms of the elements of the subgroups or the ordered pairs of the equivalence relations of K. For this we need an "inductive" or "from below" characterization.

Theorem 1.16. *Let H, K be subgroups of $\boldsymbol{G} = \langle G, \cdot, {}^{-1}, e\rangle$.*

$$H \vee K = HK \cup HKHK \cup HKHKHK \cup \cdots = \bigcup_{1 \le n \in \omega} (HK)^n,$$

where $(HK)^n = \{\, h_1 \cdot k_1 \cdots h_n \cdot k_n : h_1, \ldots, h_n \in H, k_1, \ldots, k_n \in K \,\}$.

Proof. Let $L = \bigcup_{1 \le n \in \omega} (HK)^n$. We must show three things.

(8) $$L \in \mathrm{Sub}(\boldsymbol{G}),$$

(9) $$H, K \subseteq L,$$

(10) $$\text{for all } M \in \mathrm{Sub}(\boldsymbol{G}),\ H, K \subseteq M \text{ implies } L \subseteq M.$$

Proof of (8). Clearly $L \neq \emptyset$. Let $a, b \in L$. We must show $ab \in L$ (following convention we often omit the "$\cdot$" when writing the product of elements of groups) and $a^{-1} \in L$. $a \in (HK)^n$ and $b \in (HK)^m$ for some $n, m \in \omega$. So $ab \in (HK)^{n+m} \subseteq L$, and $a^{-1} \in K^{-1}H^{-1} \cdots K^{-1}H^{-1} = (KH)^n = \{e\}(KH)^n\{e\} = H(KH)^nK = (HK)^{n+1} \subseteq L$.

(9). $H = H\{e\} \subseteq HK \subseteq L$ and $K \subseteq \{e\}K \subseteq HK \subseteq L$.

(10). Suppose $H, K \subseteq L \in \mathrm{Sub}(\boldsymbol{G})$. We prove by induction on n that $(HK)^n \subseteq M$. $HK \subseteq MM \subseteq M$. Assume $(HK)^n \subseteq M$. Then $(HK)^{n+1} \subseteq (HK)^nHK \subseteq MM \subseteq M$. $\square$

A similar argument gives a inductive characterization of the join of an arbitrary set of subgroups $\{ H_i : i \in I \}$. We leave as an exercise the proof that

$$\bigvee_{i\in I} H_i = \bigcup_{\langle h_1,\dots,h_n\rangle\in I^*} H_{i_1}\cdots H_{i_n},$$

where I^* is the set of all finite sequences of elements of I.

We next obtain a similar "inductive" characterization of the join of equivalence relations. For this purpose we need to explain some basic results in the "calculus of relations". Let A, B, C be arbitrary sets and $R \subseteq A \times B$ and $S \subseteq B \times C$. By the *relative product* of R and S, in symbols $R \circ S$, we mean the relation

$$\{ \langle a, c\rangle \in A \times C : \text{there exists a } b \in B \text{ such that } a\, R\, b\, S\, c \}.$$

The relative product is a binary operation on the set of all binary relations on any set A such that Δ_A acts as an identity (i.e., $\Delta_A \circ R = R \circ \Delta_A = R$). Also ∇_A acts like an infinity element on reflexive relations, i.e., $\Delta_A \subseteq A$ implies $\nabla_A \circ R = R \circ \nabla_A = \nabla_A$. We also have a unary *converse* operation that has some of the properties of the inverse of a group (but is not a group inverse). $\breve{R} = \{ \langle a, b\rangle : \langle b, a\rangle \in R \}$, i.e., $a\, \breve{R}\, b$ iff $b\, \breve{R}\, a$. $a\, (R \circ S)^\smile\, a'$ iff $a'\, (R \circ S)\, a$ iff there exists a b such that $a'\, R\, b\, S\, a$ iff there exists a b such that $a\, \breve{S}\, b\, \breve{R}\, a'$ iff $a\, \breve{S} \circ \breve{R}\, a'$. So $(R \circ S)^\smile = \breve{S} \circ \breve{R}$.

We note that the notation of the calculus of relations can be used to formulate the defining conditions of an equivalence relation in very simple terms. The reflexive law: $\Delta_A \subseteq E$; the transitive law: $E \circ E \subseteq E$; the symmetric law: $\breve{E} \subseteq E$.

Theorem 1.17. *Let $E, F \in \mathrm{Eq}(A)$.*

$$E \vee F = E \circ F \cup E \circ F \circ E \circ F \cup \cdots = \bigcup_{1\le n\in\omega} (E \circ F)^n.$$

Proof. Let $G = \bigcup_{1\le n\in\omega}(E \circ F)^n$. We show that $G \in \mathrm{Eq}(A)$. $\Delta_A = \Delta_A \circ \Delta_A \subseteq E \circ F \subseteq G$. Assume $\langle a, b\rangle, \langle b, c\rangle \in G$, i.e., that there exist $n, m \in \omega$ such that $a\, (E \circ F)^n\, b\, (E \circ F)^m\, c$. Then $\langle a, c\rangle \in (E \circ F)^n \circ (E \circ F)^m = (E \circ F)^{n+m} \subseteq G$. We also have that $\langle b, a\rangle \in \big((E \circ F)^n\big)^\smile = (\breve{F} \circ \breve{E})^n = (F \circ E)^n \subseteq (E \circ F)^{n+1} \subseteq G$. The proof that $G = E \vee F$ is left at an exercise. □

We also leave as an exercise the following inductive characterization of the join of an arbitrary set $\{ E_i : i \in I \}$ of equivalence relations on a set A.

$$\bigvee_{i\in I} E_i = \bigcup_{\langle h_1,\dots,h_n\rangle\in I^*} E_{i_1} \circ \cdots \circ E_{i_n}.$$

Exercise. Let $R \subseteq A^2$ be an arbitrary binary relation on A. Prove that $\bigcup_{1\le n\in\omega} R^n$, where $R^n = R \circ R \circ \cdots \circ R$ with n repetitions of R, is the smallest transitive relation that includes R. It is called the *transitive closure* of R.

Every equivalence relation is uniquely determined by its corresponding partition.

$\mathcal{P}$ is a *partition* of a set A if

- $\mathcal{P} \subseteq \boldsymbol{\mathcal{P}}(A) \setminus \{\emptyset\}$,
- $\bigcup \mathcal{P}$ $(= \bigcup\{ X : X \in \mathcal{P} \}) = A$,
- for all $X, Y \in \mathcal{P}$, $X \neq Y$ implies $X \cap Y = \emptyset$.

Let $E \in \mathrm{Eq}(A)$. For each $a \in A$, let $[a]_E = \{\, x \in A : x \,E\, a \,\}$, called the *equivalence class of* a (*over* E); $[a]_E$ is also denoted by a/E.

$\{\, [a]_E : a \in A \,\}$ is a partition of A (exercise). Conversely, if $\mathcal{P}$ is a partition of A, define $a \equiv_{\mathcal{P}}$ by the condition that there is an $X \in \mathcal{P}$ such that $a, b \in X$. Then $\equiv_{\mathcal{P}}$ is an equivalence relation whose partition is $\mathcal{P}$ (exercise). Moreover, for each equivalence relation E, $\equiv_{\{\, [a]_E : a \in A \,\}} = E$.

$\mathrm{Part}(A)$ denotes the set of partitions of A, and $\mathbf{Part}(A) = \langle \mathrm{Part}(A), \leq \rangle$, where $\leq$ is the partial ordering on $\mathrm{Part}(A)$ defined as follows: $\mathcal{P} \leq \mathcal{Q}$ if, for each $X \in \mathcal{P}$, there exists a $Y \in \mathcal{Q}$ such that $X \subseteq Y$, equivalently, each equivalence class of $\mathcal{Q}$ is a union of equivalence classes of $\mathcal{P}$. The mapping $\mathcal{P} \mapsto \equiv_{\mathcal{P}}$ is bijection between the posets $\mathbf{Eq}(A)$ and $\mathbf{Part}(A)$ that is strictly order-preserving (exercise). Thus $\mathbf{Part}(A)$ is a complete lattice and the above mapping is a lattice isomorphism.

It is usually easier to picture the partition of a specific equivalence relation rather than the relation itself. The following characterizations of the join and meet operations in $\mathbf{Part}(A)$ are left as exercises. In the lattice $\mathbf{Part}(A)$,

$$\mathcal{P} \wedge \mathcal{Q} = \{\, X \cap Y : X \in \mathcal{P}, Y \in \mathcal{Q}, X \cap Y \neq \emptyset \,\}.$$

A finite sequence $X_1, Y_1, \ldots, X_n, Y_n$, where $X_1, \ldots, X_n \in \mathcal{P}$ and $Y_1, \ldots, Y_n \in \mathcal{P}$ is called *connected* if $X_i \cap Y_i \neq \emptyset$ for all $i \leq n$ and $Y_i \cap X_{i+1} \neq \emptyset$ for all $i < n$. Exercise: show that, for every $a \in A$, $b \in [a]_{\mathcal{P} \cup \mathcal{Q}}$ iff there exists a connected sequence $X_1, Y_1, \ldots, X_n, Y_n$ such that $a \in X_1$ and $b \in Y_n$.

Exercise. For each $n \in \omega \setminus \{0\}$, define $\equiv \pmod{n} \in \mathbb{Z}^2$ by $a \equiv b \pmod{n}$ if $a = b + kn$ for some $k \in \mathbb{Z}$, i.e., $n | a - b$. Show $\equiv \pmod{n} \in \mathrm{Eq}(\mathbb{Z})$. Describe the partition of $\equiv \pmod{n}$. Describe $\equiv \pmod{n} \wedge \equiv \pmod{m}$ and $\equiv \pmod{n} \vee \equiv \pmod{m}$.

The lattices of subgroups and equivalence relations have special properties. In the sequel we write $X' \subseteq_\omega X$ to mean that X' is a *finite* subset of X.

Definition 1.18. Let $\boldsymbol{A}$ be a lattice. An element c of $\boldsymbol{A}$ is *compact* if, for every $X \subseteq A$ such that $\bigvee X$ exists,

$$c \leq \bigvee X \text{ implies there exists a } X' \subseteq_\omega X \text{ such that } c \leq \bigvee X'.$$

The set of compact elements of $\boldsymbol{A}$ is denoted by $\mathrm{Comp}(\boldsymbol{A})$.

$\boldsymbol{A}$ is *compactly generated* if every element of $\boldsymbol{A}$ is the join of the compact elements less than or equal to it, i.e., for every $a \in A$,

$$a = \bigvee \{\, c \in \mathrm{Comp}\, \boldsymbol{A} : c \leq a \,\}.$$

A lattice is *algebraic* if it is complete and compactly generated.

We note that an element is compactly generated iff it is the join of some set of compact elements, since in this case it must be the join of all compact elements less than or equal to it.

Examples.

- Every finite lattice is algebraic.
- The lattice $\langle \omega \cup \{\infty\}, \leq \rangle$ is algebraic. ∞ is the only noncompact element and $\infty = \bigvee \omega$.

- $\langle [0,1], \leq \rangle$, where $[0,1] = \{ x \in \mathbb{R} : 0 \leq x \leq 1 \}$, is complete but not algebraic; 0 is the only compact element and hence the only element that is the join of compact elements.
- $\langle \mathrm{Sub}(\boldsymbol{G}), \subseteq \rangle$, for every group $\boldsymbol{G}$, and $\langle \mathrm{Eq}(A), \subseteq \rangle$, for every nonempty set A, are algebraic lattices, but this will be shown until later.

1.2. **Closed set systems and closure operators.** A family K of sets is said to be *upward directed by inclusion*, or *upward directed* for short, or even shorter, simply *directed*, if each pair of sets in K is included in a third member of K, i.e.,

$$\text{for all } X, Y \in K \text{ there exists a } Z \in K \text{ such that } X \vee Y \subseteq Z.$$

Definition 1.19. A *closed set system* consists of a nonempty set A and a $\mathcal{C} \subseteq \boldsymbol{\mathcal{P}}(A)$ such that $\mathcal{C}$ is closed under intersections of arbitrary subsets, i.e.,

$$\text{for every } K \subseteq \mathcal{C}, \bigcap K \in \mathcal{C}.$$

A closed set system $\langle A, \mathcal{C} \rangle$ is *algebraic* if $\mathcal{C}$ is closed under unions of upward directed subsets, i.e.,

$$\text{for every directed } K \subseteq \mathcal{C}, \bigcup K \in \mathcal{C}.$$

Note that by definition $\mathcal{C}$ always contains A since $A = \bigcap \emptyset$. Since $\mathrm{Sub}(\boldsymbol{G})$ and $\mathrm{Eq}(A)$ are closed under intersections of arbitrary subsets, to show they form algebraic closed-set systems it suffices to show they are closed under unions of directed subsets.

The union of any, not necessarily directed, $K \subseteq \mathrm{Sub}(\boldsymbol{G})$ contains the identity and is closed under inverse. Assume that K is directed. Let $a, b \in \bigcup K$, and let $H, L \in K$ such that $a \in H$ and $b \in L$. Choose $M \in K$ such that $K \cup L \subseteq M$. Then $ab \in M \subseteq \bigcup K$. So $\bigcup K \in \mathrm{Sub}(\boldsymbol{G})$.

The union of any, not necessarily directed, $K \subseteq \mathrm{Eq}(A)$ includes Δ_A and is closed under converse. Assume that K is directed. Let $\langle a, b \rangle, \langle b, c \rangle \in \bigcup K$, and let $H, L \in K$ such that $\langle a, b \rangle \in H$ and $\langle b, c \rangle \in L$. Choose $M \in K$ such that $K \cup L \subseteq M$. Then $\langle a, c \rangle \in M \subseteq \bigcup K$. So $\bigcup K \in \mathrm{Eq}(A)$.

Each of the defining conditions of a group involves only a finite number of group elements, and, similarly, each of the conditions that define equivalence relations involves only a finite number of ordered pairs. This is the common property that guarantees subgroups and equivalence relations form an algebraic lattice. This vague observation will be made more precise in the next chapter.

With each closed-set system we associate a closure operation.

Definition 1.20. Let $\langle A, \mathcal{C}\rangle$ be a closed-set system. Define $\mathrm{Cl}_{\mathcal{C}} : : \boldsymbol{\mathcal{P}}(A) \to \boldsymbol{\mathcal{P}}(A)$ as follows. For every $X \subseteq A$,

$$\mathrm{Cl}_{\mathcal{C}}(X) = \bigcap\{\, C \in \mathcal{C} : X \subseteq C \,\}.$$

$\mathrm{Cl}_{\mathcal{C}}(X)$ is called the *closure of* X.

Theorem 1.21. *Let $\langle A, \mathcal{C}\rangle$ be a closed-set system. Then for all $X, Y \subseteq A$,*

$$X \subseteq \mathrm{Cl}_{\mathcal{C}}(X), \tag{11}$$ (*extensivity*)

$$\mathrm{Cl}_{\mathcal{C}}\big(\mathrm{Cl}_{\mathcal{C}}(X)\big) = \mathrm{Cl}_{\mathcal{C}}(X), \tag{12}$$ (*idempotency*)

$$X \subseteq Y \quad \textit{implies} \quad \mathrm{Cl}_{\mathcal{C}}(X) \subseteq \mathrm{Cl}_{\mathcal{C}}(Y), \tag{13}$$ (*monotonicity*)

and if $\langle A, \mathcal{C}\rangle$ is algebraic,

$$\mathrm{Cl}_{\mathcal{C}}(X) = \bigcup\big\{\mathrm{Cl}_{\mathcal{C}}(X') : X' \subseteq_\omega X \,\big\}. \tag{14}$$ (*finitarity*).

Proof. Note that since $\mathcal{C}$ is closed under intersection, $\mathrm{Cl}_{\mathcal{C}}(X) \in \mathcal{C}$ and thus $\mathrm{Cl}_{\mathcal{C}}(X)$ is the smallest member of $\mathcal{C}$ that includes X, and that $X \in \mathcal{C}$ iff $\mathrm{Cl}_{\mathcal{C}}(X) = X$. The conditions (11) and (12) are immediate consequences of this fact, and, if $X \subseteq Y$, then every member of $\mathcal{C}$ that includes Y, in particular $\mathrm{Cl}_{\mathcal{C}}(Y)$, necessarily includes X and hence also $\mathrm{Cl}_{\mathcal{C}}(X)$. Thus (13) holds.

Assume $\langle A, \mathcal{C}\rangle$ is algebraic. By (11) $\{\, \mathrm{Cl}_{\mathcal{C}}(X') : X' \subseteq_\omega X \,\}$ is directed, because, for all $X', X'' \subseteq_\omega X$, $\mathrm{Cl}_{\mathcal{S}}(X') \cup \mathrm{Cl}_{\mathcal{S}}(X'') \subseteq \mathrm{Cl}_{\mathcal{S}}(X' \cup X'')$, and $X' \cup X'' \subseteq_\omega X$.

$$X = \bigcup\{\, X' : X' \subseteq X \,\} \underset{(11)}{\subseteq} \bigcup\big\{\, \mathrm{Cl}_{\mathcal{C}}(X') : X' \subseteq_\omega X \,\big\} \in \mathcal{C}.$$

So $\mathrm{Cl}_{\mathcal{C}}(X) \subseteq \bigcup\big\{\, \mathrm{Cl}_{\mathcal{C}}(X') : X' \subseteq_\omega X \,\big\}$. The opposite inclusion follows by monotonicity. Thus (14). □

Now suppose that a mapping $\mathrm{Cl} : \boldsymbol{\mathcal{P}}(A) \to \boldsymbol{\mathcal{P}}(A)$ satisfies (11)–(13). Let $\mathcal{C} = \{\, X \subseteq A : \mathrm{Cl}(X) = X \,\}$ (called the *closed sets* of Cl). Then $\mathcal{C}$ is a closed-set system (exercise). Moreover, $\mathcal{C}$ is algebraic if Cl satisfies (14). To see this let $K \subseteq \mathcal{C}$ be upward directed. We must show $\mathrm{Cl}(\bigcup K) \subseteq \bigcup K$. By (14) $\mathrm{Cl}(\bigcup K) = \bigcup\big\{\, \mathrm{Cl}(X) : X \subseteq_\omega \bigcup K \,\big\}$. Since K is directed, for every $X \subseteq_\omega \bigcup K$, there is a $C_X \in K$ such that $X \subseteq C_X$, and hence $\mathrm{Cl}(X) \subseteq C_X$, since C_X is closed. Thus

$$\bigcup\big\{\, \mathrm{Cl}(X) : X \subseteq_\omega \bigcup K \,\big\} \subseteq \bigcup\{\, C_X : X \subseteq_\omega K \,\} \subseteq \bigcup K.$$

Thus (algebraic) closed-set systems and (finitary) closure operators are equivalent in a natural sense, and we can go back-and-forth between them without hesitation. The next theorem shows that every (algebraic) closed-set system gives rise to an (algebraic) lattice.

Theorem 1.22. *Let $\langle A, \mathcal{C}\rangle$ be a closed-set system.*

(i) *$\langle \mathcal{C}, \subseteq\rangle$ is a complete lattice. For every $K \subseteq \mathcal{C}$, $\bigwedge K = \bigcap K$ and*

$$\bigvee K = \bigcap\{\, C \in \mathcal{C} : \bigcup K \subseteq C \,\} = \mathrm{Cl}_{\mathcal{C}}\big(\bigcup K\big).$$

(ii) *If* $\langle A, \mathcal{C}\rangle$ *is algebraic, then* $\langle \mathcal{C}, \subseteq\rangle$ *is an algebraic lattice. Moreover, the compact elements of* $\langle \mathcal{C}, \subseteq\rangle$ *are the closed sets of the form* $\mathrm{Cl}_{\mathcal{C}}(X)$ *with* $X \subseteq_\omega A$.

Proof. (i). Exercise. (The proof is just like the proofs that $\langle \mathrm{Sub}(\boldsymbol{G}), \subseteq\rangle$ and $\langle \mathrm{Eq}(A), \subseteq\rangle$ are complete lattices.)

(ii). Assume $\langle A, \mathcal{C}\rangle$ is algebraic. We first verify the claim that the compact elements are exactly those of the form $\mathrm{Cl}_{\mathcal{C}}(X)$ with $X \subseteq_\omega A$. Let $C = \mathrm{Cl}_{\mathcal{C}}(X)$ with $X \subseteq_\omega A$. Suppose

$$C \subseteq \bigvee K = \mathrm{Cl}_{\mathcal{C}}\big(\bigcup K\big) = \bigcup\{\mathrm{Cl}_{\mathcal{C}}(Y) : Y \subseteq_\omega \bigcup K\,\}.$$

Since X is finite and $\{\mathrm{Cl}_{\mathcal{C}}(Y) : Y \subseteq_\omega \bigcup K\,\}$ is directed, $X \subseteq \mathrm{Cl}_{\mathcal{C}}(Y)$ for some $Y \subseteq_\omega \bigcup K$. Thus there exist $D_1, \ldots, D_n \in K$ such that $Y \subseteq D_1 \cup \cdots \cup D_n \subseteq D_1 \vee \cdots \vee D_n$. Hence

$$C = \mathrm{Cl}_{\mathcal{C}}(X) \subseteq \mathrm{Cl}_{\mathcal{C}}(Y) \subseteq D_1 \vee \cdots \vee D_n.$$

So C is compact in the lattice $\langle \mathcal{C}, \subseteq\rangle$.

Conversely, assume C is compact in $\langle \mathcal{C}, \subseteq\rangle$. Then $C = \bigcup\{\,\mathrm{Cl}_{\mathcal{C}}(X) : X \subseteq_\omega C\,\} = \bigvee\{\,\mathrm{Cl}_{\mathcal{C}}(X) : X \subseteq_\omega C\,\}$. So there exist $X_1, \ldots, X_n \subseteq_\omega C$ such that $C = \mathrm{Cl}_{\mathcal{C}}(X_1) \vee \cdots \vee \mathrm{Cl}_{\mathcal{C}}(X_n) = \mathrm{Cl}_{\mathcal{C}}(X_1 \cup \cdots \cup X_n)$. Since $X_1 \cup \cdots \cup X_n$ is finite, we have, for every $C \in \mathcal{C}$,

For every $C \in \mathcal{C}$, $C = \bigcup\{\,\mathrm{Cl}_{\mathcal{C}}(X) : X' \subseteq X\,\} = \bigvee\{\,\mathrm{Cl}_{\mathcal{C}}(X) : X' \subseteq X\,\}$. So every $C \in \mathcal{C}$ is the join of compact elements. Hence $\langle \mathcal{C}, \subseteq\rangle$ is algebraic. □

For any group $\boldsymbol{G}$, $\mathrm{Cl}_{\mathrm{Sub}(\boldsymbol{G})}(X)$ the subgroup generated by X, which is usually denoted by $\langle X\rangle$. The finitely generated subgroups are the compact elements of $\mathbf{Sub}(\boldsymbol{G}) = \langle \mathrm{Sub}(\boldsymbol{G}), \subseteq\rangle$. The compact elements of $\mathbf{Eq}(A)$ are the equivalence relations "generated" by a finite set of ordered pairs.

The notion of a lattice was invented to abstract a number of difference phenomena in algebra, and other mathematical domains, that have to do with order. We have seen three levels of abstract so far: at the lowest level we have the lattices of subgroups and equivalence relations. At the next level the lattices of algebraic closed-set systems, and at the highest level the algebraic lattices in which all notions of set and subset have been abstracted away. The next theorem shows that in a real sense there is no loss in abstracting from algebraic closed-set systems to algebraic lattices.

Theorem 1.23. *Every algebraic lattice* $\boldsymbol{A} = \langle A, \leq\rangle$ *is isomorphic to the lattice of* $\langle \mathcal{C}, \subseteq\rangle$ *of closed sets for some algebraic closed-set system* $\langle B, \mathcal{C}\rangle$.

Proof. Let $B = \mathrm{Comp}(\boldsymbol{A})$, the set of compact elements of $\boldsymbol{A}$. For each $a \in A$, let $C_a = \{\, c \in \mathrm{Comp}(A) : c \leq a\,\}$. Let $\mathcal{C} = \{\, C_a : a \in A\,\}$. Because $\boldsymbol{A}$ is compactly generated, $a = \bigvee C_a$; hence the mapping $a \mapsto C_a$ is a bijection from A to $\mathcal{C}$. Moreover, the mapping is strictly order-preserving since, clearly, $a \leq b$ iff $C_a \subseteq C_b$. So by Theorem 1.8 $\langle \mathcal{C}, \subseteq\rangle$ is a complete lattice and the mapping $a \mapsto C_a$ is it is an isomorphism between the lattices $\langle A, \leq\rangle$ and $\langle \mathcal{C}, \subseteq\rangle$.

It only remains to show that $\langle \mathrm{Comp}(\boldsymbol{A}), \mathcal{C}\rangle$ is an algebraic closed-set system. Let $K \subseteq \mathcal{C}$; $K = \{\, C_x : x \in X\,\}$ for some $X \subseteq \mathrm{Comp}(\boldsymbol{A})$. Then

$$\bigcap\{\, C_x : x \in X\,\} = C_{\bigwedge X}.$$

To see this consider any $c \in \mathrm{Comp}(\boldsymbol{A})$. Then $c \in \bigcap\{\, C_x : x \in X\,\}$ iff, for all $x \in X$, $c \in C_x$ iff, for all $x \in X$, $c \leq x$ iff $c \in C_{\bigwedge X}$.

Assume now that K is upward directed. Since $x \leq y$ iff $C_x \subseteq C_y$, we see that X is also directed by the ordering $\leq$ of $\boldsymbol{A}$. We show that

$$\bigcup\{\, C_x : x \in X \,\} = C_{\bigvee X}.$$

Let $c \in \mathrm{Comp}(\boldsymbol{A})$.

$$\begin{aligned} c \in C_{\bigvee X} \quad &\text{iff} \quad c \leq \bigvee X \\ &\text{iff} \quad \text{for some } X' \subseteq_\omega X,\ c \leq \bigvee X', \quad \text{since } c \text{ is compact} \\ &\text{iff} \quad \text{for some } x \in X,\ c \leq x, \quad \text{since } X \text{ is directed} \\ &\text{iff} \quad \text{for some } x \in X,\ c \in C_x \\ &\text{iff} \quad c \in \bigcup\{\, C_x : x \in X \,\}. \end{aligned}$$

So $\bigvee\{\, C_x : x \in X \,\} = \bigcup\{\, C_x : x \in X \,\}$, and hence $\langle \mathcal{C}, \subseteq \rangle$ is algebraic. □

2. General Algebraic Structures

An algebraic structure is a simply a set with a possibly infinite set of operations on it of finite rank. For example a group is a set together with the binary operation of group multiplication, the inverse operation, which is of rank one, and what we call a "distinguished constant", the group identity. The latter can be viewed as as an operation of "rank zero". In order to compare two algebras of the same kind, it is useful to have some way of indexing the operations so that an operation on one algebra can matched with the corresponding operation of the other algebra. For instance, when we compare two rings we don't want to match addition on the first ring with multiplication on in the second ring. When one is dealing with only a few kinds of algebraic structures, like group, rings and vector spaces, this is not a problem. But in the general theory where a wide range of algebraic types are considered we have to be more precise. The custom now is to specify a the type of an algebraic structure by the formal language associated with it. This motivates the following definition.

Definition 2.1. A *signature* or *language type* is a set Σ together with a mapping $\rho\colon \Sigma \to \omega$. The elements of Σ are called *operations symbols*. For each $\sigma \in \Sigma$, $\rho(\sigma)$ is called the *arity* or *rank* of σ.

For simplicity we write Σ for $\langle \Sigma, \rho \rangle$, treating the rank function as implicit.

Definition 2.2. Let Σ be a signature. A Σ-*algebra* is a ordered couple $\boldsymbol{A} = \big\langle A, \langle \sigma^{\boldsymbol{A}} : \sigma \in \Sigma \rangle \big\rangle$, where A is a nonempty set and $\sigma^{\boldsymbol{A}}\colon A^{\rho(\sigma)} \to A$ for all $\sigma \in \Sigma$.

0-ary operations: if $\rho(\sigma) = 0$, $\sigma^{\boldsymbol{A}}\colon A^0 \to A$. But by definition $A^0 = \{\emptyset\}$. It is usual to identify the function $\sigma^{\boldsymbol{A}}$ with the unique element in its range, namely $\sigma^{\boldsymbol{A}}(\emptyset)$; the latter is called a *distinguished constant* of $\boldsymbol{A}$. In general the functions $\sigma^{\boldsymbol{A}}$ are called the *fundamental operations* of $\boldsymbol{A}$.

We give a number of examples of signatures and algebras. We consider two kinds of groups depending on the signature.

$\Sigma_1 = \{\cdot\}$; $\rho(\cdot) = 2$. $\Sigma_2 = \{\cdot, {}^{-1}, \mathrm{e}\}$; $\rho(\cdot) = 2$, $\rho({}^{-1}) = 1$, $\rho(\mathrm{e}) = 0$.

$\boldsymbol{G} = \langle G, \{\cdot^{\boldsymbol{G}}\}\rangle$ is a group of type I if it satisfies the following two conditions.

$$\forall x, y, z\big((x \cdot y) \cdot z \approx x \cdot (y \cdot z)\big) \tag{15}$$

$$\exists x\big(\forall y\big(x \cdot y \approx y \textbf{ and } y \cdot x \approx y\big) \textbf{ and } \forall y \exists z(y \cdot z \approx x \textbf{ and } z \cdot y \approx x)\big). \tag{16}$$

$\boldsymbol{G} = \langle G, \{\cdot^{\boldsymbol{G}}, {}^{-1^{\boldsymbol{G}}}, e^{\boldsymbol{G}}\}\rangle$ is a group of type II if (15) holds together with the following:

$$\forall x(e \cdot x \approx x \textbf{ and } x \cdot e \approx x) \tag{17}$$

$$\forall x(x \cdot x^{-1} \approx e \textbf{ and } x^{-1} \cdot x \approx e). \tag{18}$$

In the general theory of algebras we are careful to distinguish between the symbol for the equality symbol, $\approx$, the identity relation $\{\, \langle a, a\rangle : a \in A \,\}$ on a given set A, which is usually denoted by the symbol "=". One should think of the identity relation as the interpretation of the symbol $\approx$ in the set A in much the same way $\cdot^{\boldsymbol{G}}$ is the interpretation of the operation symbol $\cdot$ in the group $\boldsymbol{G}$. In the spirit of the notation of signatures and algebras we can write $\approx^A$ is $=$.

The two types of groups are equivalent in the sense that, if $\boldsymbol{G} = \langle G, \{\cdot^{\boldsymbol{G}}\}\rangle$ is a group of type I, then there is a unique $f\colon G \to G$ and $g \in G$ such that $\langle G, \cdot^{\boldsymbol{G}}, f, g\rangle$ is a group of type II. Conversely, if $\boldsymbol{G} = \langle G, \cdot^{\boldsymbol{G}}, {}^{-1^{\boldsymbol{G}}}, e^{\boldsymbol{G}}\rangle$ is a group of type II, then $\langle G, \cdot^{\boldsymbol{G}}\rangle$ is a group of type I.

However, from the viewpoint of the general theory of algebras, the two types of groups have very different properties. Note that the definition conditions (15), (17), and (18) are what we call *identities*: equations between terms with all the variables universally quantified. We note that although (17) is not strictly an identity, it is logically equivalent to the pair of identities $\forall x(e \cdot x \approx x)$ and $\forall x(x \cdot e \approx x)$.) (16) is not logically equivalent to any set of identities as we shall soon see. We mention also that is conventional to omit explicit reference to the universal quantifiers when writing an identity. Thus (15), the associative law, is nomally written simply "$(x \cdot y) \cdot z \approx x \cdot (y \cdot z)$"

We shall use the following simplifying notation. If Σ is finite we write $\boldsymbol{A} = \langle A, \sigma_1^{\boldsymbol{A}}, \sigma_2^{\boldsymbol{A}}, \ldots, \sigma_n^{\boldsymbol{A}}\rangle$, where $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$ and $\rho(\sigma_1) \geq \rho(\sigma_2) \geq \cdots \geq \rho(\sigma_n)$. We omit the superscripts "$^{\boldsymbol{A}}$" on the "$\sigma^{\boldsymbol{A}}$" when there is not chance of confusion.

More examples. $\boldsymbol{A} = \langle A, +, \cdot, -, 0\rangle$, where $+$ and $\cdot$ are binary, $-$ unary, and 0 nullary, is a *ring* if $\langle A, +, -, 0\rangle$ is *Abelian* group (of type II), i.e., it satisfies the identity $\forall x \forall y(x + y \approx y + x)$, and the $\cdot$ is associative and distributes over $+$, i.e.

$$\forall x, y(x \cdot (y + z) \approx (x \cdot y) + (x \cdot z) \textbf{ and } (y + z) \cdot x \approx (y \cdot x) + (z \cdot x)).$$

An *integral domain* is a ring satisfying

$$\forall x, y\big((x \cdot y \approx 0) \Longrightarrow (x \approx 0) \textbf{ or } (y \approx 0)\big).$$

Notice this is not an identity.

A *field* is an algebra $\langle A, +, \cdot, -, 0, 1\rangle$ such that $\langle A, +, \cdot, -, 0\rangle$ and the following conditions are satisfied.

$$\forall x(x \cdot y \approx y \cdot x)$$

$$\forall x(1 \cdot x \approx x)$$

$$\forall x\big(\textbf{not}(x \approx 0) \Longrightarrow \exists y(x \cdot y \approx 1)\big).$$

We cannot define a field as an algebra of type $\langle A, +, \cdot, -, ^{-1}, 0, 1\rangle$ because 0^{-1} is not defined and by definition every operation of an algebra must be defined for all elements of the algebra.

Lattices are Σ-algebras, with $\Sigma = \{\vee, \wedge\}$, defined by identities.

We now consider an algebra of quite different character, the algebra of *nondeterministic while programs*. Let $\Sigma = \{\mathbf{or}, ;, \mathbf{do}\}$, where **or** and ; are binary and **do** is unary. These operation symbols denote three different ways of controling the flow of a program. If P and Q are programs, then $P\,\mathbf{or}\,Q$ is the program that nondeterministically passes control to P or Q. $P;Q$ passes control first to P and when P terminates to Q. $\mathbf{do}\,P$ loops a nondeterministic number of times, possibly zero, through P. A set W of programs is said to be closed with respect to these control structures if $P, Q \in W$ imply $(P\ \mathbf{or}\ Q), (P\ ;\ Q), (\mathbf{do}\,P) \in W$. For any set S of "atomic programs", let $\mathrm{WP}(S)$ be the smallest closed set containing S. $\mathbf{WP}(S) = \langle \mathrm{WP}(S), \mathbf{or}, ;, \mathbf{do}\rangle$ is an algebra of *nondeterministic while programs*.

$\mathbf{WP}(S)$ is different from the other algebras we have considered in that we have not specificed any conditions that it must satisfy (other than its signature). It is typical of algebras that arise from programming languages in this regard; we will study this kind of algebra in more detail later.

A *vector space* over a field $\langle F, +, \cdot, -, 0, 1\rangle$ is an Abelian group $\langle A, +, -, 0\rangle$ with a scalar multiplication $F \times A \to A$ satisfying the following conditions, for all $r, r' \in F$ and $a, a' \in A$.

$$1a = a,$$
$$r(a + a') = ra + ra',$$
$$(r + r')a = ra + r'a,$$
$$(r \cdot r')b = r(r'a).$$

This is not an algebra in our sense but can be made into one by expanding the signature of Abelian groups by adjoining a new unary operation for each element of the field. Let $\Sigma = \{+, -, 0\} \cup \{\sigma_r : r \in F\}$, where $\rho(\sigma_r) = 1$ for every $r \in F$. (Note that Σ is infinite if F is infinite.) A vector space is a Σ-algebra $\boldsymbol{A} = \langle A, +^{\boldsymbol{A}}, -^{\boldsymbol{A}}, 0^{\boldsymbol{A}}, \sigma_r^{\boldsymbol{A}}\rangle_{r\in F}$ such that $\langle A, +^{\boldsymbol{A}}, -^{\boldsymbol{A}}, 0^{\boldsymbol{A}}\rangle$ is an Abelian group and, for every $r \in F$ and $a \in A$, $\sigma_r^{\boldsymbol{A}}(a) = ra$, the scalar product of a by r.

A vector space in this sense is defined by identities, but in general an infinite number. The properties of both the scalar multiplication the field must be expressed in terms of identities. For example, the last of the four defining condtions on scalar multiplication takes the form of a possibly infinite set of identities, namely, $\{\sigma_{r\cdot r'}(x) \approx \sigma_r(\sigma_{r'}(x) : r, r' \in F\}$, while the the commutativity of the ring multiplication is reflected in the set of identities $\{\sigma_r(\sigma_{r'}(x)) = \sigma_{r'}(\sigma_r(x)) : r, r' \in F\}$.

A more satisfactory treatment of vector spaces requires a generalization of the notion of a signature.

A *mult-sorted signature* consists of a nonempty set S of *sorts* together with a set Σ of *operation symbols* and, for each $\sigma \in \Sigma$, a nonempty sequence $\rho(\sigma) = \langle s_1, \ldots, s_n, t\rangle$ of sorts, called the *type* of σ. We usually write the type in the form $s_1, \ldots, s_n \to t$. The sequence of sorts $s_1, \ldots, s_n$ and the single sort t are called respectively the *arity* and *target sort* of σ.

A Σ-*algebra* is an ordered pair

$$\boldsymbol{A} = \big\langle \langle A_s : s \in S\rangle,\ \langle \sigma^{\boldsymbol{A}} : \sigma \in \Sigma\rangle \big\rangle,$$

where $\langle A_s : s \in S\rangle$, which is usually denoted by A, is a nonempty finite sequence of nonempty sets. For each $\sigma \in \Sigma$, if $s_1, \ldots, s_n \to t$ is the type of σ, then

$$\sigma^{\boldsymbol{A}} \colon A_{s_1} \times \cdots \times A_{s_n} \to A_t.$$

Vector spaces over a field can be most naturally viewed as multi-sorted algebras where $S = \{V, F\}$ and $\Sigma = \{+_V, -_V, 0_V, +_F, \cdot_F, -_F, 0_F, +_V, -_V, 0_V, 1_V, *\}$, where the types of the various operation symbols are given in the following table. $*$ denotes scalar multiplication. The defining identities are left to the reader.

operation	type	operation	type
$+_V$	$V, V \to V$	$+_F$	$F, F \to F$
$-_V$	$V \to V$	$-_F$	$F \to F$
0_V	$\to V$	0_F	$\to F$
		1_F	$\to F$
		$\cdot_F$	$F, F \to F$
$*$	$F, V \to V$		

We give an example of a multi-sorted algebra that arises in the algebraic theory of data types, the algebra of *lists of data*. $S = \{D, L\}$, $\Sigma = \{\mathtt{head}, \mathtt{tail}, \mathtt{append}, \mathtt{derror}, \mathtt{lerror}\}$. The type of each operation symbol is as follows: $\mathtt{head} : L \to D$; $\mathtt{tail} : L \to L$; $\mathtt{append} : D, L \to L$, $\mathtt{derror} : \to D$; $\mathtt{lerror} : \to L$.

The *algebra of lists* over a nonempty set A is

$$\mathbf{List}(A) = \langle \mathrm{List}(A), \mathtt{head}^{\mathbf{List}(A)}, \mathtt{tail}^{\mathbf{List}(A)}, \mathtt{append}^{\mathbf{List}(A)}, \mathtt{derror}^{\mathbf{List}(A)}, \mathtt{lerror}^{\mathbf{List}(A)} \rangle,$$

where $A^* = \{\langle a_1, \ldots, a_n\rangle : n \in \omega, a_1, \ldots, a_n \in A\}$, the set of all finite sequences of elements of A.

$$\begin{aligned}
\mathtt{head}^{\mathbf{List}(A)}(\langle a_1, \ldots, a_n\rangle) &= a_1 \quad \text{if } \langle a_1, \ldots, a_n\rangle \text{ is not empty,}\\
\mathtt{head}^{\mathbf{List}(A)}(\langle\rangle) &= \mathtt{derror},\\
\mathtt{head}^{\mathbf{List}(A)}(\langle a_1, \ldots, a_n\rangle) &= \langle a_2, \ldots, a_n\rangle \quad \text{if } \langle a_1, \ldots, a_n\rangle \text{ is not empty,}\\
\mathtt{head}^{\mathbf{List}(A)}(\langle\rangle) &= \mathtt{lerror},\\
\mathtt{append}^{\mathbf{List}(A)}(b, \langle a_1, \ldots, a_n\rangle) &= \langle b, a_1, \ldots, a_n\rangle,\\
\mathtt{derror}^{\mathbf{List}(A)} &= e_D,\\
\mathtt{lerror}^{\mathbf{List}(A)} &= e_L.
\end{aligned}$$

A signature is *unary* if $\rho(\sigma) \leq 1$ for every $\sigma \in \Sigma$; *mono-unary* if $\Sigma = \{\sigma\}$ and $\rho(\sigma) = 1$; a *groupoid* if $\Sigma = \{\sigma\}$ and $\rho(\sigma) = 2$. An algebra is *unary*, *mono-unary*, a *groupoid* if its signature is. In the sequel, for each $n \in \omega$, $\Sigma_n = \{\, \sigma \in \Sigma : \rho(\sigma) = n \,\}$.

2.1. **Subuniverses and subalgebras.**

Definition 2.3. Let $\boldsymbol{A}$ be a Σ-algebra and $B \subseteq A$. B is a *subuniverse* of $\boldsymbol{A}$ if, for all $n \in \omega$, $\sigma \in \Sigma_n$, and $b_1, \ldots, b_n \in B$, $\sigma^{\boldsymbol{a}}(b_1, \ldots, b_n) \in B$, i.e., B is *closed* under $\sigma^{\boldsymbol{A}}$ for each $\sigma \in \Sigma$. The set of all subuniverses of $\boldsymbol{A}$ will be denoted by $\mathrm{Sub}(\boldsymbol{A})$.

Note that this implies $\sigma^{\boldsymbol{A}} \in B$ for every $\sigma \in \Sigma_0$, and that the empty set is a subuniverse of $\boldsymbol{A}$ iff $\Sigma_0 = \emptyset$, i.e., $\boldsymbol{A}$ has no distinguished constants.

Theorem 2.4. $\langle A, \mathrm{Sub}(\boldsymbol{A})\rangle$ *is an algebraic closed-set system for every* Σ*-algebra* $\boldsymbol{A}$.

Proof. Let $\mathcal{K} \subseteq \mathrm{Sub}(\boldsymbol{A})$. Let $\sigma \in \Sigma$ and $a_1, \ldots, a_n \in \bigcap \mathcal{K}$, where $n = \rho(\sigma)$. Then for every $B \in \mathcal{K}$, $a_1, \ldots, a_n \in B$ and hence $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \in B$. So $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \in \bigcap \mathcal{K}$. So $\bigcap \mathcal{K} \in \mathrm{Sub}(\boldsymbol{A})$.

Suppose now that $\mathcal{K}$ is directed. Let $a_1, \ldots, a_n \in \bigcup \mathcal{K}$. Since there is only a finite number of the a_i, they are all contained in a single $B \in \mathcal{K}$. So $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \in B \in \bigcup \mathcal{K}$. Hence $\bigcup \mathcal{K} \in \mathrm{Sub}(\boldsymbol{A})$. □

Note that if Σ is unary, then $\bigcup \mathcal{K} \in \mathrm{Sub}(\boldsymbol{A})$ for every $\mathcal{K} \subseteq \mathrm{Sub}(\boldsymbol{A})$ because $a \in \bigcup \mathcal{K}$ implies $a \in B$ for some $B \in A$, and hence $\sigma^{\boldsymbol{A}}(a) \in B \subseteq \bigcup \mathcal{K}$.

Note also that $\mathrm{Sub}(\boldsymbol{A}) = \boldsymbol{\mathcal{P}}(A)$, i.e., every subset of A is a subuniverse of $\boldsymbol{A}$, iff, for every $n \in \Sigma$, every $\sigma \in \Sigma$, and all $a_1, \ldots, a_n \in A$, $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \in \{a_1, \ldots, a_n\}$.

The closure operator associated with the closed-set system $\langle A, \mathrm{Sub}(\boldsymbol{A})\rangle$ is denoted by $\mathrm{Sg}^{\boldsymbol{A}}$. Thus $\mathrm{Sg}^{\boldsymbol{A}} : \boldsymbol{\mathcal{P}}(A) \to \mathrm{Sub}(\boldsymbol{A})$ and $\mathrm{Sg}^{\boldsymbol{A}}(X) = \bigcap\{\, B \in \mathrm{Sub}(\boldsymbol{A}) : X \subseteq B \,\}$; this is called the *subuniverse generated* by X.

Theorem 2.5 (Birkhoff-Frink)**.** *Let* $\langle A, \mathcal{C}\rangle$ *be an algebraic closed-set system over* A*. There there exists a signature* Σ *and a* Σ*-algebra* $\boldsymbol{A}$ *such that* $\mathcal{C} = \mathrm{Sub}(\boldsymbol{A})$.

Proof. For every $X \subseteq_\omega A$ and every $b \in \mathrm{Cl}_{\mathcal{C}}(X)$, let $\sigma_{X,b}$ be an operation symbol of rank $|X|$, the cardinality of X. Let $\Sigma = \{\, \sigma_{X,b} : X \subseteq_\omega A, b \in \mathrm{Cl}_{\mathcal{C}}(X) \,\}$. Let $\boldsymbol{A}$ be the Σ-algebra with universe A such that, for every $\sigma_{X,b} \in \Sigma$ and all $a_1, \ldots, a_n \in A$, where $n = |X|$,

$$\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) = \begin{cases} b & \text{if } \{a_1, \ldots, a_n\} = X \\ a_1 & \text{otherwise.} \end{cases}$$

If $X = \emptyset$, $\sigma^{\boldsymbol{A}}_{X,b} = b$.

In order to establish the conclusion of the theorem it suffices to show that,

$$\text{for every } Y \subseteq A,\ \mathrm{Cl}_{\mathcal{C}}(Y) = \mathrm{Sg}^{\boldsymbol{A}}(Y).$$

$\supseteq$: We first show that $\mathrm{Cl}_{\mathcal{C}}(Y)$ is closed under the operations of $\boldsymbol{A}$. Let $X \subseteq_\omega A$ and $b \in \mathrm{Cl}_{\mathcal{C}}(X)$. Let $a_1, \ldots, a_n \in \mathrm{Cl}_{\mathcal{C}}(Y)$, were $n = |X|$. If $\{a_1, \ldots, a_n\} = X$, then $\sigma^{\boldsymbol{A}}_{X,b}(a_1, \ldots, a_n) = b \in \mathrm{Cl}_{\mathcal{C}}(X) \subseteq \mathrm{Cl}_{\mathcal{C}}(Y)$, since $X \subseteq \mathrm{Cl}_{\mathcal{C}}(Y)$; otherwise, $\sigma^{\boldsymbol{A}}_{X,b}(a_1, \ldots, a_n) = a_1 \in \mathrm{Cl}_{\mathcal{C}}(Y)$. So $Y \subseteq \mathrm{Cl}_{\mathcal{C}}(Y) \in \mathrm{Sub}(\boldsymbol{A})$, and hence $\mathrm{Sg}^{\boldsymbol{A}}(Y) \subseteq \mathrm{Cl}_{\mathcal{C}}(Y)$.

$\subseteq$. Let $b \in \mathrm{Cl}_{\mathcal{C}}(Y)$. Since $\langle A, \mathcal{C}\rangle$ is a algebraic by hypothesis, $\mathrm{Cl}_{\mathcal{C}}(Y) = \bigcup\{\, \mathrm{Cl}_{\mathcal{C}}(Y') : Y' \subseteq_\omega Y \,\}$. So there is a finite subset Y' of Y such that $b \in \mathrm{Cl}_{\mathcal{C}}(Y')$. If $Y' = \emptyset$, then b

is in every subuniverse of $\boldsymbol{A}$, in particular in $\mathrm{Sg}^{\boldsymbol{A}}(Y)$. So assume $Y \neq \emptyset$, and let $Y' = \{a_1, \ldots, a_n\}$, where the $a_1, \ldots, a_n$ are all distinct. Then $b = \sigma_{Y',b}(a_1, \ldots, a_n) \in \mathrm{Sg}^{\boldsymbol{A}}(Y)$. So $\mathrm{Cl}_{\mathcal{C}}(Y) \subseteq \mathrm{Sg}^{\boldsymbol{A}}(Y)$. □

We examine the subuniverse lattices of some familiar algebras. Let $\mathbb{Z} = \langle \mathbb{Z}, +, -, 0 \rangle$. We begin by showing that

$$\mathrm{Sub}(\mathbb{Z}) = \{\, n\mathbb{Z} : n \in \omega \,\}, \tag{19}$$

where $n\mathbb{Z} = \{n \cdot k : k \in \mathbb{Z}\}$ and $\cdot$ is integer multiplication.

Let $H \in \mathrm{Sub}(\mathbb{Z})$. If $H = \{0\}$, then $H = 0\mathbb{Z}$. Assume $H \neq \{0\}$. Then $H \cap \omega \neq \{0\}$, because if $k \in H$ and $h < 0$, then $-k \in H$. Let n be the least element of $H \cap (\omega \setminus \{0\})$. Let $k \in \mathbb{Z}$.

- If $k = 0$, $n \cdot k = 0 \in H$.
- If $k > 0$, $n \cdot k = \underbrace{n + n + \cdots + n}_{k} \in H$.
- If $k < 0$, $n \cdot k = \underbrace{-n + -n + \cdots + -n}_{-k} \in H$.

So $n\mathbb{Z} \subseteq H$.

Suppose $k \in H$. By the division algorithm, $k = qn + r$, where $0 \leq r < n$. $r = k - qn \in H \cap \omega$. So $r = 0$ by the minimality of n. Thus $k \in n\mathbb{Z}$, and $H \subseteq n\mathbb{Z}$. This verifies (19).

Let $\mathbf{Sub}(\mathbb{Z})$ be the complete lattice $\langle \mathrm{Sub}(\mathbb{Z}), \vee, \cap \rangle$. We note that $n\mathbb{Z} \vee m\mathbb{Z} = \{\, qn + pm : p, q \in \mathbb{Z} \,\} = \{\mathrm{GCD}(n, m)r : r \in \mathbb{Z}\,\}$. So

$$n\mathbb{Z} \vee n\mathbb{Z} = \mathrm{GCD}(n, m)\mathbb{Z}.$$

It is left as an exercise to show that $n\mathbb{Z} \wedge m\mathbb{Z} = \mathrm{LCM}(n, m)\mathbb{Z}$. Thus $\mathbf{Sub}(\mathbb{Z}) \cong \langle \omega, \mathrm{GCD}, \mathrm{LCM} \rangle$.

Note that $\mathrm{Sub}(\langle \omega, S \rangle = \{\, [n) : n \in \omega \,\} \cup \{\emptyset\}$, where S is the successor function, i.e., $S(n) = n + 1$, and $[n) = \{\, k \in \omega : n \leq k \,\}$. We have $[n) \vee [m) = [n) \cup [m) = [\mathrm{Min}(n, m))$ and $[n) \cap [m) = [\mathrm{Max}(n, m))$. Thus $\big\langle \mathrm{Sub}(\langle \omega, S \rangle), \vee, \cap \big\rangle \cong \langle \omega \cup \{\infty\}, \mathrm{Min}, \mathrm{Max} \rangle$. So $\big\langle \mathrm{Sub}(\langle \omega, S \rangle), \subseteq \big\rangle \cong \langle \omega \cup \{\infty\}, \geq \rangle$

$\mathrm{Sub}(\langle \omega, P \rangle = \{\, [0, n] : n \in \omega \,\} \cup \{\emptyset\}$, where P is the predecessor function, i.e., $P(n) = n - 1$ if $0 < n$; $P(0) = 0$. $\big\langle \mathrm{Sub}(\langle \omega, P \rangle), \vee, \cap \big\rangle \cong \langle \omega \cup \{\infty\}, \mathrm{Max}, \mathrm{Min} \rangle$. So $\big\langle \mathrm{Sub}(\langle \omega, P \rangle), \subseteq \big\rangle \cong \langle \omega \cup \infty, \leq \rangle$

If $\boldsymbol{A} = \langle A, \vee, \wedge \rangle$ is a lattice, $\langle A, \wedge, \vee \rangle$ is also a lattice, called the *dual* of $\boldsymbol{A}$. Its Hasse diagram is obtained by turning the Hasse diagram of $\boldsymbol{A}$ up-side-down. The lattices of subuniverses of $\langle \omega, S \rangle$ and $\langle \omega, P \rangle$ are duals of each other.

A lattice is *bounded* if it has a largest element, i.e., an element that is an upper bound of every element of the lattice, and also a smallest element. These elements are normally denoted by 1 and 0, respectively. The elements of the lattice that cover 0 (if any exist) are called *atoms*, and the elements that are covered by 1 are called *coatoms*. The coatoms of the lattice $\mathbf{Sub}(\boldsymbol{A})$ of subuniverses of a Σ-algebra $\boldsymbol{A}$ are called *maximal proper* subuniverses. Thus B is a maximal proper subuniverse of $\boldsymbol{A}$ if $B \neq A$ and there does not exist a $C \in \mathrm{Sub}(\boldsymbol{A})$ such that $B \subsetneq C \subsetneq A$.

The maximal proper subuniverses $\mathbb{Z}$ are of the form $p\mathbb{Z}$, p a prime. The only maximal proper subuniverse of $\langle \omega, S\rangle$ is [1), while $\langle \omega, P\rangle$ has no maximal proper subuniverse. This is a reflection of the fact that $\mathbb{Z}$ and $\langle \omega, S\rangle$ are both finitely generated, in fact by 1 and 0, respectively, while $\langle \omega, P\rangle$ is not finitely generated. This connection between the existence of maximal proper subuniverses and finite generation is a general phenomenon as the following theorem shows. Note that since every natural number greater than 1 has a prime factor, every proper subuniverse of $\mathbb{Z}$ is included in a maximal proper subuniverse, and trivially $\langle \omega, S\rangle$ has the same property.

Theorem 2.6. *Let $\boldsymbol{A}$ be a finitely generated Σ-algebra. Then every proper subuniverse of $\boldsymbol{A}$ is included in a maximal proper one.*

Let B be a proper subuniverse of $\boldsymbol{A}$. The theorem is obvious if $\boldsymbol{A}$ is finite: If B is not maximal, let B' be a proper subuniverse that is strictly larger than B. If B' is not maximal, let B'' be a proper subuniverse that is strictly larger than B'. Continue in this way. If $|A| = n$, this process cannot continue for more than n steps. If B is infinite, the process may continue ω steps (here we are thinking of ω as a ordinal number). In order to prove the theorem in general we need to be able to extend the process beyond ω steps to the transfinite. *Zorn's lemma*[1] allows us to do this. Let $\langle A, \leq\rangle$ be a (nonempty) poset with the property that every chain (i.e., linearly ordered subset) has an upper bound in A. Then Zorn's lemma asserts that $\langle P, \leq\rangle$ has a maximal element.

We are now ready to prove the theorem.

Proof. Let $A = \mathrm{Sg}^{\boldsymbol{A}}(X)$, $X \subseteq_\omega A$. Let $B \in \mathrm{Sub}(\boldsymbol{A})$, $B \neq A$. Let $\mathcal{K} = \{\, K \in \mathrm{Sub}(\boldsymbol{A}) : B \subseteq K \subsetneq A \,\}$. $\mathcal{K}$ is nonempty since it contains B. Let $\mathcal{C} \subseteq \mathcal{K}$ be any chain. $\mathcal{C}$ is directed, so $\bigcup \mathcal{C} \in \mathrm{Sub}(\boldsymbol{A})$. $\bigcup \mathcal{C}$ is a proper subuniverse, because if $\bigcup \mathcal{C} = A$, then $X \subseteq \bigcup \mathcal{C}$, and hence $X \subseteq K$ for some $K \in \mathcal{K}$, because X is finite and $\mathcal{C}$ is directed. But this is impossible since $X \subseteq K$ implies $K = A$ and hence $K \notin \mathcal{K}$. So every chain in $\mathcal{K}$ has an upper bound. By Zorn's lemma $\mathcal{K}$ has a maximal element. □

The converse of the theorem does not hold: there are algebras that are not finitely generated but which still have maximal proper subuniverses. For example, let $\boldsymbol{A} = \langle \omega \cup \{\infty\}, P\rangle$, where P is the usual predecessor function on ω and $P(\infty) = \infty$. $\boldsymbol{A}$ is clearly not finitely generated, but ω is a maximal proper subuniverse.

Theorem 2.7 (Principle of Structural Induction)**.** *Let $\boldsymbol{A}$ be a Σ-algebra generated by X. To prove that a property $\mathcal{P}$ holds for each element of $\boldsymbol{A}$ it suffices to show that*

(i) induction basis. *$\mathcal{P}$ holds for each element of X.*
(ii) induction step. *If $\mathcal{P}$ holds for each of the elements $a_1, \ldots, a_n \in A$ (the* induction hypothesis*), then $\mathcal{P}$ holds for $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n)$ for all $\sigma \in \Sigma_n$.*

Proof. Let $P = \{\, a \in A : \ \mathcal{P} \text{ holds for } a \,\}$. $X \subseteq P$ and P is closed under the operations of $\boldsymbol{A}$. So $P \in \mathrm{Sub}(\boldsymbol{A})$. Hence $A = \mathrm{Sg}^{\boldsymbol{A}}(X) \subseteq P$. □

Ordinary mathematical induction is the special case $\boldsymbol{A} = \langle \omega, S\rangle$. $\omega = \mathrm{Sg}^{\boldsymbol{A}}(\{0\})$. If 0 has the property $\mathcal{P}$ and n has $\mathcal{P}$ implies $S(n) = n + 1$ has $\mathcal{P}$, the every natural number has the property $\mathcal{P}$.

[1]Zorn's lemma is a theorem of set theory that is know to be equivalent to the Axiom of Choice, and hence independent of the usual axioms of set theory. It is of course highly nonconstructive.

We now show how the notion of subuniverse extends naturally for single-sorted to multi-sorted signatures. Let Σ be a multi-sorted signature with set S of sorts. Let $\boldsymbol{A} = \big\langle \langle\, A_s : s \in S \,\rangle, \sigma^{\boldsymbol{A}} \big\rangle_{\sigma\in\Sigma}$ be a Σ-algebra. A *subuniverse* of $\boldsymbol{A}$ is an S-sorted set $B = \langle\, B_s : s \in S \,\rangle$ such that $B_s \subseteq A_s$ for every $s \in S$, and, for every $\sigma \in \Sigma$ of type $s_1, \ldots, s_n \to t$, and all $a_1 \in A_{s_1}, \ldots, a_n \in A_{s_n}$, we have $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \in B_t$.

$\langle \mathrm{Sub}(\boldsymbol{A}), \leq \rangle$ is a complete lattice where $B = \langle B_s : s \in S\rangle \leq C = \langle C_s : s \in S\rangle$ iff $B_s \subseteq C_s$ for all $s \in S$. The (infinite) join and meet operations are:

$$\bigvee \mathcal{K} = \big\langle \bigcap \{\, B_s : B \in \mathcal{K} \,\} : s \in S \,\big\rangle,$$

$$\bigwedge \mathcal{K} = \big\langle \bigcap \{\, C_s : \ C \in \mathrm{Sub}(\boldsymbol{A}) \text{ such that, for all } B \in \mathcal{K},\ B \leq C \,\} : s \in S \,\big\rangle.$$

As an example consider the algebra

$$\mathbf{Lists}(\omega) = \big\langle \langle \omega \cup \{e_D\}, \omega^* \cup \{e_l\}\rangle, \mathtt{head}, \mathtt{tail}, \mathtt{append}, \mathtt{emptylist}, \mathtt{derror}, \mathtt{derror}\big\rangle.$$

We leave it as an exercise to show that every subuniverse is generated by a unique subset of the data set ω; more precisely, the subuniverses of **Lists** are exactly the S-sorted subsets of Lists of the form $\langle X_D \cup \{e_D\},\ X_D^* \cup \{e_L\}\rangle$ were X is an arbitrary subset of ω.

Hint: It is easy to check that this is a subuniverse. For the other direction it suffices to show that for any sorted set $X = \langle X_D, X_L\rangle \leq \langle \omega \cup \{e_D\}, \omega^* \cup \{e_l\}\rangle$, $\mathrm{Sg}^{\mathbf{Lists}(\omega)}(X) = \mathrm{Sg}^{\mathbf{Lists}(\omega)}(\langle Y, \emptyset\rangle)$, where $y = X \cup \bigcup \big\{\, \{a_1, \ldots, a_n\} : \langle a_1, \ldots, a_n\rangle \in X_L \,\big\}$. For this purpose it suffices to show that, if $\langle a_1, \ldots, a_n\rangle \in X_L$, then $\{a_1, \ldots, a_n\} \subseteq B_D$, where $B = \mathrm{Sg}^{\mathbf{Lists}(\omega)}(X)$. But, for all $i \leq n$, $a_i = \mathtt{head}(\mathtt{tail}^i(\langle a_1, \ldots, a_n\rangle) \in B_D$.

From this characterization of the subuniverses of **Lists** is follows easily that **Sub**(**Lists**) is isomorphic to the lattice of all subsets of ω and hence is distributive.

2.2. **The structure of mono-unary algebras.** Let $\boldsymbol{A} = \langle A, f\rangle$, where $f\colon A \to A$. By a *finite chain* in $\boldsymbol{A}$ we mean either a subset of A of the form $\{a, f^1(a), f^2(a), \ldots, f^n(a)\}$, for some $n \in \omega$, or of the form $\{a, f^1(a), f^2(a), \ldots\} = \{\, f^k(a) : k \in \omega \,\}$, where $f^i(a) \neq f^j(a)$ for all $i < j \leq n$ in the first case and for all $i < j < \omega$ in the second. Note that the finite chain is not a subuniverse of $\boldsymbol{A}$ unless $f^{n+1}(a) = f^i(a)$ for some $i \leq n$. The infinite chain is clearly a subuniverse and is isomorphic to the natural numbers under successor; we call it an *ω-chain*. By a *cycle* we mean a finite subset of $\boldsymbol{A}$ of the form $\{a, f^1(a), f^2(a), \ldots, f^{p-1}(a)\}$, where $f^p(a) = a$ but $f^i(a) \neq f^j(a)$ for all $i < j < p$. p is called the *period* the the cycle. A cycle is clearly a subuniverse.

We first consider the case where $\boldsymbol{A}$ is *cyclic*, i.e., $A = \mathrm{Sg}^{\boldsymbol{A}}(\{a\})$. It is easy to see that $A = \{\, f^n(a) : n \in \omega \,\}$. We show that if $\boldsymbol{A}$ is finite, then it must be in the form of a finite chain that is attached at the end to a cycle; see Figure 1.

Suppose $f^n(a) = f^m(a)$ for some $n < m$. Let l be the least n such that there exists an $m > n$ such that $f^n(a) = f^m(a)$. Then let p be the least $k > 0$ such that $f^{l+k}(a) = f^l(a)$. p is called the *period* of $\boldsymbol{A}$ (and of a) and l is called its *tail length*. $\boldsymbol{A}$ is finite. $\boldsymbol{A}$ thus consists of a finite chain of length l, called the *tail* of $\boldsymbol{A}$, that is attached to a cycle of period p, called the *cycle* of $\boldsymbol{A}$. If $f^n(a) \neq f^m(a)$ for all distinct $n, m \in \omega$, then $\boldsymbol{A}$ is an infinite

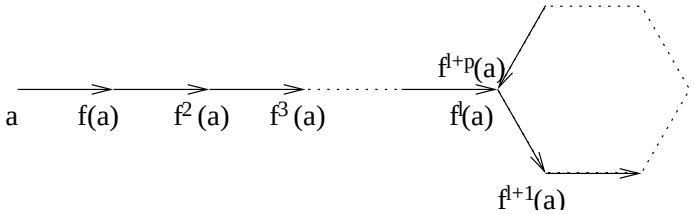


FIGURE 1

ω-chain.

Elements a, b of an arbitrary mono-unary algebra $\boldsymbol{A}$ are said to be *connected* if there exist $n, m \in \omega$ such that $f^n(a) = f^m(b)$. The relation of being connected is an equivalence relation. It is clearly reflexive and symmetric. Suppose $f^n(a) = f^m(b)$ and $f^k(b) = f^l(c)$. Then $f^{n+k}(a) = f^{m+k}(b) = f^{l+m}(c)$. The equivalence classes are called *connected components* of $\boldsymbol{A}$. Each connected component C of $\boldsymbol{A}$ is a subuniverse. For if $a \in C$, then $f(f(a) = f^2(a)$; hence $f(a)$ is connected to a and thus in C. $\boldsymbol{A}$ is the disjoint union of its connected components, and hence in order to fully understand the structure of mono-unary algebras it suffices to focus on connected algebras (those with a single connected component) Clearly any cyclic algebra is connected.

We now consider the proper 2-generated connected algebras, i.e., $A = \mathrm{Sg}^{\boldsymbol{A}}(\{a, b\})$ and $\boldsymbol{A}$ is not cyclic but is connected, i.e., there exist $n, m \in \omega$ such that $f^n(a) \neq f^m(b)$ but $f^{n+1}(a) = f^{m+1}(b)$. Since they are connected, $\mathrm{Sg}^{\boldsymbol{A}}(\{a\})$ is finite iff $\mathrm{Sg}^{\boldsymbol{A}}(\{b\})$ is, and in this case they have the same cycle. The tails either attach separately to the cycle or merge before the cycle, see Figure 2. $\boldsymbol{A}$ is infinite iff $\mathrm{Sg}^{\boldsymbol{A}}(\{a\})$ and $\mathrm{Sg}^{\boldsymbol{A}}(\{b\})$ are both infinite. It can be viewed either as the ω-chain $\mathrm{Sg}^{\boldsymbol{A}}(\{b\})$ with a finite chain beginning with b attached, or as the ω-chain $\mathrm{Sg}^{\boldsymbol{A}}(\{b\})$ with a finite chain beginning at a attached; see Figure 2

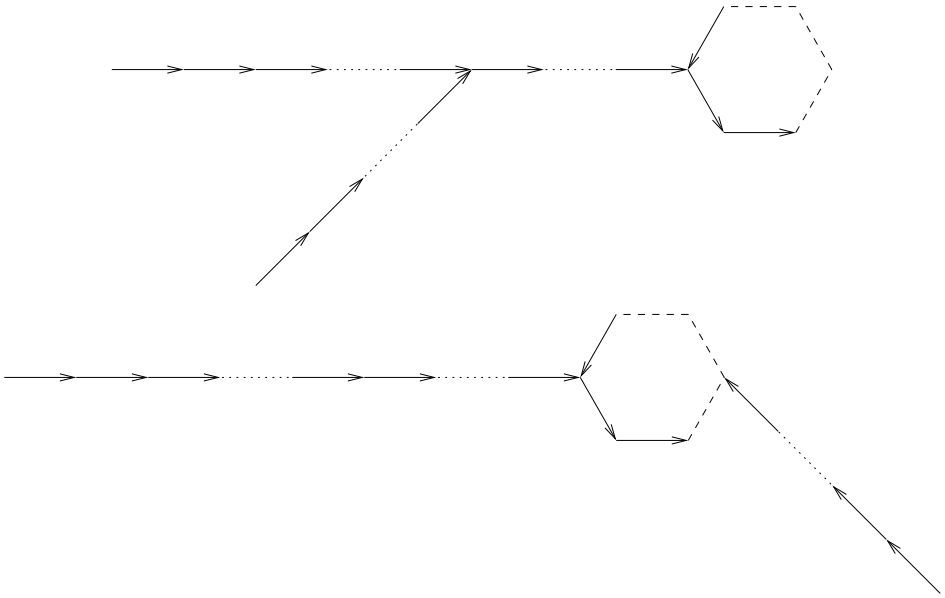


FIGURE 2

The proper 3-generated connected algebras are of the following form: three finite algebras, one with the three tails separately attached to the cycle; one with two of the tails merging before the cycle; and one with all three tails merging before the cycle. The one infinite form is an ω-chain with two finite chains attached to it. By a *finite reverse tree* we mean mean a finite chain with a finite number of finite chains attached to it. Every finite, finitely generated, connected mono-unary algebra is a cycle with a finite number of finite reverse trees attached to it. Every infinite, finitely generated, connected mono-unary algebra is an ω-chain with a finite number of reverse trees attached to it.

Examples of a nonfinitely generate mono-unary connected algebras are the natural numbers under the predecessor (a *reverse ω-chain*) attached to a cycle, and a ω-chain and a reverse ω-chain put together, i.e., the integers under successor. A full description of the nonfinitely generated mono-unary connected algebras is left to the reader.

2.3. **Subalgebras.** Roughly speaking a subalgebra of an algebra is a nonempty subuniverse with together with the algebraic structure it inherits from its parent.

Definition 2.8. Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be Σ-algebras. $\boldsymbol{B}$ is a *subalgebra* of $\boldsymbol{A}$, in symbols $\boldsymbol{B} \subseteq \boldsymbol{A}$, if $B \subseteq A$ and, for every $\sigma \in \Sigma$ and all $b_1, \ldots, b_n \in B$ (n is the rank of σ), $\sigma^{\boldsymbol{B}}(b_1, \ldots, b_n) = \sigma^{\boldsymbol{A}}(b_1, \ldots, b_n)$.

If $\boldsymbol{B} \subseteq \boldsymbol{A}$, then $B \in \mathrm{Sub}(\boldsymbol{A})$. Conversely, if $B \in \mathrm{Sub}(\boldsymbol{A})$ and $B \neq \emptyset$, then there is a unique $\boldsymbol{B} \subseteq \boldsymbol{A}$ such that B is the universe of $\boldsymbol{B}$.

Let $\mathsf{Alg}(\Sigma)$ be the class of all Σ-algebras. $\subseteq$ is a partial ordering of $\mathsf{Alg}(\Sigma)$. It is clearly reflexive and antisymmetric. If $\boldsymbol{C} \subseteq \boldsymbol{B}$ and $\boldsymbol{B} \subseteq \boldsymbol{A}$, then $C \subseteq B$ and $B \subseteq A$ so $C \subseteq A$, and for all $c_1, \ldots, c_n \in C$, $\sigma^{\boldsymbol{C}}(c_1, \ldots, c_n) = \sigma^{\boldsymbol{B}}(c_1, \ldots, c_n) = \sigma^{\boldsymbol{A}}(c_1, \ldots, c_n)$. $\langle \mathsf{Alg}(\Sigma), \subseteq \rangle$ is not a lattice ordering. If $A \cap B = \emptyset$, then $\boldsymbol{A}$ and $\boldsymbol{B}$ cannot have a GLB. Allowing empty

algebras would clearly not alter the situation for signatures with constants, and it is not hard to see that the the same is true even for signatures without constants. The problem becomes more interesting when we consider *isomorphism types* of algebras below.

For any class K of Σ-algebras we define

$$\mathbf{S}(\mathsf{K}) = \{\, \boldsymbol{A} \in \mathsf{Alg}(\Sigma) : \text{ there exists a } \boldsymbol{B} \in \mathsf{K} \text{ such that } \boldsymbol{A} \subseteq \boldsymbol{B} \,\}.$$

For simplicity we write $\mathbf{S}(\boldsymbol{A})$ for $\mathbf{S}(\{\boldsymbol{A}\})$.

$\mathbf{S}$ is an algebraic closure operator on $\mathsf{Alg}(\Sigma)$. Clearly $\mathsf{K} \subseteq \mathbf{S}(\mathsf{K})$ by the reflexivity of $\subseteq$, and and $\mathbf{S}\,\mathbf{S}(\mathsf{K}) = \mathbf{S}(K)$ because $\subseteq$ is transitive. Also $\mathsf{K} \subseteq \mathsf{L}$ implies $\mathbf{S}(\mathsf{K}) \subseteq \mathbf{S}(\mathsf{L})$. And $\mathbf{S}(\mathsf{K}) = \bigcup\{\, \mathbf{S}(\mathsf{K}') : \mathsf{K}' \subseteq_\omega \mathsf{K} \,\}$. In fact, $\mathbf{S}(\mathsf{K}) = \bigcup\{\, \mathbf{S}(\boldsymbol{A}) : \boldsymbol{A} \in \mathsf{K} \,\}$.

We should mention here that there are some set-theoretical difficulties in dealing with the class of all Σ-algebras because it is too large. Technically it is a *proper class* and not a set; a set can be an element of a class but a class cannot. Thus although the class $\mathsf{Alg}(\Sigma)$ of all algebras of signature Σ exists, the class $\{\mathsf{Alg}(\Sigma)\}$ whose only member is $\mathsf{Alg}(\Sigma)$ does not. In the sequel for purposes of simplicity and convenience we will use notation and terminology that in their normal set-theoretical interpretation implies that we are assuming the existence of classes that contain $\mathsf{Alg}(\Sigma)$ as an element. But the actual interpretation makes no assumption of this kind and is consistent with standard set-theory.

2.4. **Homomorphisms and quotient algebras.** Let $h\colon A \to B$ be a mapping between the sets A and B. h is *surjective* or *onto* if the range and codomain of h are the same, i.e., $h(A) = B$; we write $h\colon A \twoheadrightarrow B$ in this case. h is *injective* or *one-one* if, for all $a, a' \in A$, $a \neq a'$ implies $h(a) \neq h(a')$; we write $h\colon A \rightarrowtail B$. Finally, h is *bijective* or *one-one onto* if it is both surjective and injective, in symbols, $h\colon A \cong B$.

Definition 2.9. Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be Σ-algebras. A mapping $h\colon A \to B$ is a *homomorphism*, in symbols $h\colon \boldsymbol{A} \to \boldsymbol{B}$, if, for all $\sigma \in \Sigma$ and all $a_1, \dots, a_n \in A$, with $n = \rho(\sigma)$,

$$h\big(\sigma^{\boldsymbol{A}}(a_1, \dots, a_n)\big) = \sigma^{\boldsymbol{B}}(h(a_1), \dots, h(a_n)).$$

A surjective homomorphism is called an *epimorphism* ($h\colon \boldsymbol{A} \twoheadrightarrow \boldsymbol{B}$) and an injective homomorphism is called a *monomorphism* ($h\colon \boldsymbol{A} \rightarrowtail \boldsymbol{B}$). A bijective homomorphism is called an isomorphism and is written either $h\colon \boldsymbol{A} \cong \boldsymbol{B}$.

A homomorphism with the same domain and codomain, i.e., $h\colon \boldsymbol{A} \to \boldsymbol{A}$, is called and *endomorphism* of $\boldsymbol{A}$, and an isomorphism with the same domain and codomain, i.e., $h\colon \boldsymbol{A} \cong \boldsymbol{A}$, is an *automorphism* of $\boldsymbol{A}$.

$\mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B})$ will denote the set of all homomorphisms from $\boldsymbol{A}$ to $\boldsymbol{B}$. $\mathrm{Iso}(\boldsymbol{A}, \boldsymbol{B})$, $\mathrm{End}(\boldsymbol{A})$, and $\mathrm{Aut}(\boldsymbol{A})$ are defined accordingly.

Examples. The classic example is the homomorphism from the additive group of integers $\mathbb{Z} = \langle \mathbb{Z}, +, -, 0 \rangle$ to the group of integers $\pmod n$ $\mathbb{Z}_n = \langle \mathbb{Z}_n, + \pmod n, - \pmod n, 0 \pmod n \rangle$.

For $n \in \mathbb{Z}$, the mapping $h_n\colon \mathbb{Z} \to \mathbb{Z}$ defined by

$$h_n(x) = nx = \begin{cases} \underbrace{x + \cdots + x}_{n} & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ \underbrace{-x + - \cdots + -x}_{-n} & \text{if } n < 0 \end{cases}$$

is an endomorphism of $\mathbb{Z}$: $h(x+y) = n(x+y) = nx+ny$; $h(-x) = n(-x) = -(nx)$; $h(0) = n0 = 0$.

Theorem 2.10. *Let* $\boldsymbol{A} = \langle A, \cdot, ^{-1}, e\rangle$ *and* $\boldsymbol{B} = \langle B, \cdot, ^{-1}, e\rangle$ *be groups. Then* $\mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B}) = \mathrm{Hom}(\langle A, \cdot\rangle, \langle B, \cdot\rangle)$.

Proof. Clearly $\mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B}) \subseteq \mathrm{Hom}(\langle A, \cdot\rangle, \langle B, \cdot\rangle)$. Let $h \in \mathrm{Hom}(\langle A, \cdot\rangle, \langle B, \cdot\rangle)$. $h(e) \cdot h(e) = h(e \cdot e) = h(e) = e \cdot h(e)$. So $h(e) = e$ by cancellation. $h(a^{-1}) \cdot h(a) = h(a^{-1} \cdot a) = e = h(a)^{-1} \cdot h(a)$. So $h(a^{-1}) = h(a)^{-1}$ by cancellation. □

$\langle \mathbb{Z}, +\rangle$ is called a *reduct* of $\mathbb{Z}$. There is a useful general notion of reduct. Let $\langle \Sigma, \rho_\Sigma\rangle$ and $\langle \Delta, \rho_\Sigma\rangle$ be signatures. Δ is a *subsignature* of Σ if $\Delta \subseteq \Sigma$ and, for each $\delta \in \Delta$, $\rho_\Delta(\delta) = \rho_\Sigma(\delta)$.

Definition 2.11. Let Σ be a signature and $\boldsymbol{A}$ a Σ-algebra. Then for every subsignature Δ of Σ, the Δ-algebra $\langle A, \delta^{\boldsymbol{A}}\rangle_{\delta\in\Delta}$ is called the *Δ-reduct* of $\boldsymbol{A}$. It is denoted by $\mathrm{Red}_\Delta(\boldsymbol{A})$.

Clearly, for all Σ-algebras $\boldsymbol{A}$ and $\boldsymbol{B}$ and every subsignature Δ of Σ, $\mathrm{Sub}(\boldsymbol{A}) \subseteq \mathrm{Sub}(\mathrm{Red}_\Delta(\boldsymbol{A}))$. We have seen that the equality fails to holds for the $\{+\}$-reduct of $\mathbb{Z}$. It does hold however for the $\{\cdot\}$-reduct of any finite group (exercise). Exercise: Is it true in general that $\mathbf{Sub}(\boldsymbol{A})$ is a sublattice of $\mathbf{Sub}(\mathrm{Red}_\Delta(\boldsymbol{A}))$?

It is also clear that $\mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B}) \subseteq \mathrm{Hom}(\mathrm{Red}_\Delta(\boldsymbol{A}), \mathrm{Red}_\Delta(\boldsymbol{B}))$, and we showed above that equality holds for the $\{\cdot\}$-reduct of any group (finite or infinite).

Every endomorphism of $\mathbb{Z}$ is of the form h_n for some $n \in \omega$. To see this consider any $g \in \mathrm{End}(\mathbb{Z})$, and let $n = g(1)$. If $x > 0$,

$$g(x) = g(\underbrace{1+\cdots+1}_{x}) = \underbrace{g(1)+\cdots+g(1)}_{x} = nx = h_n(x).$$

If $x = 0$, $g(x) = 0 = h_n(x)$, and if $x < 0$,

$$g(x) = g(\underbrace{-1+\cdots+-1}_{-x}) = \underbrace{-g(1)+\cdots+-g(1)}_{-x} = (-n)(-x) = nx = h_n(x).$$

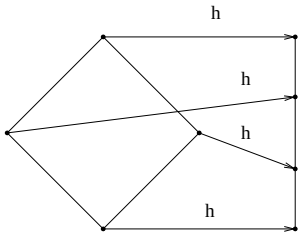
This result is a special case of a more general result which we now present.

Theorem 2.12. *Let* $\boldsymbol{A}, \boldsymbol{B}$ *be* Σ*-algebras, and assume* $\boldsymbol{A}$ *is a generated by* $X \subseteq A$*, i.e.,* $A = \mathrm{Sg}^{\boldsymbol{A}}(X)$*. Then every* $h \in \mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B})$ *is uniquely determined by its* restriction $h{\restriction}X$ *to* X*, i.e., for all* $h, h' \in \mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B})$*, if* $h{\restriction}X = h'{\restriction}X$*, then* $h = h'$*.*

Proof. The proof is by structural induction. Let $\mathcal{P}$ be the property of an element of $\boldsymbol{A}$ that its images under h and h' is the same; identifying a property with the set of all elements that have the property (this is called *extensionality*) we can say that $\mathcal{P} = \{\, a \in A : h(a) = h'(a) \,\}$. $X \subseteq \mathcal{P}$ by assumption. For every $\sigma \in \Sigma$ and all $a_1, \ldots, a_n \in \mathcal{P}$, $h\big(\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n)\big) = \sigma^{\boldsymbol{B}}\big(h(a_1), \ldots, h(a_n)\big) = \sigma^{\boldsymbol{B}}\big(h'(a_1), \ldots, h'(a_n)\big) = h'\big(\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n)\big)$. So $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \in \mathcal{P}$, and hence $\mathcal{P} \in \mathrm{Sub}(\boldsymbol{A})$. So $\mathcal{P} = A$ since X generates $\boldsymbol{A}$. □

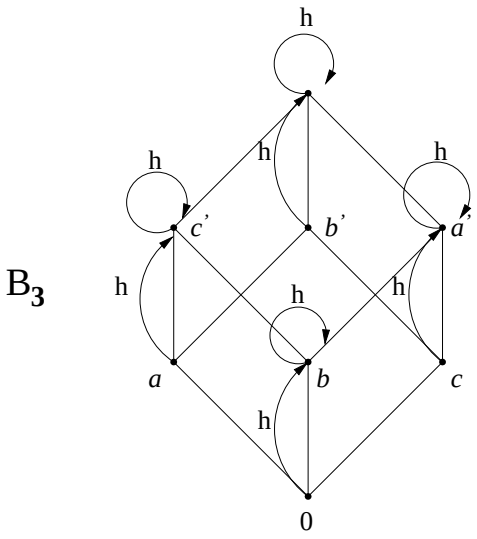
This theorem can be applied to give a easy proof that every endomorphism of $\mathbb{Z}$ is of the form h_n for some $n \in \mathbb{Z}$. Let $g \in \mathrm{End}(\mathbb{Z})$ and $n = g(1)$. Then $g(1) = h_n(1)$. Thus $g = h_n$ since $\mathbb{Z} = \mathrm{Sg}^{\mathbb{Z}}(\{1\})$.

Let $\boldsymbol{A} = \langle A, \vee, \wedge\rangle, \boldsymbol{B} = \langle B, \vee, \wedge\rangle$ be lattices. Then every $h \in \mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B})$ is order-preserving. In fact, $a \leq a'$ implies $a \wedge a' = a'$ which in turn implies that $h(a) \vee h(a') = h(a')$, i.e., $h(a) \leq h(a')$. The converse does not hold.



For example the mapping h in the figure above is order-preserving but is not a lattice homorphism. However recall that if if h is bijective and strictly order-preserving then it is a homorphism (Theorem 1.8).

Consider the function $h\colon B_3 \to B_3$ described pictorially in the following diagram, where $\boldsymbol{B}_3$ is the three-atom Boolean algebra, The claim is that h is endomorphism of $\boldsymbol{B}_3$. This



can be verified mechanically by considering each pair of elements x, y in turn and checking that $h(x \vee y) = h(x) \vee h(y)$ and $h(x \wedge y) = h(x) \wedge h(y)$, but this is a tedious process. For example, $h(c \vee b) = h(a') = a' = a' \vee b = h(a') \vee h(b)$. Here is a simpler way. Note first of all that, for all $x \in B_3$, $h(x) = x \vee b$. $\boldsymbol{B}_3$ is a distributive lattice. An easy way to see this is to observe that $\boldsymbol{B}_3$ is isomorphic to the $\langle \boldsymbol{\mathcal{P}}(\{1,2,3\}), \cup, \cap \rangle$, the lattice of all subsets of the three-element set $\{1,2,3\}$. The mapping $a \mapsto \{1\}$, $b \mapsto \{2\}$, $c \mapsto \{3\}$, $a' \mapsto \{2,3\}$, $b' \mapsto \{1,3\}$, $c' \mapsto \{1,2\}$, $0 \mapsto \emptyset$, $1 \mapsto \{1,2,3\}$ is an order-preserving bijection and hence a lattice isomorphism.

So $\boldsymbol{B}_3$ is distributive. We use this fact to verify h is a homomorphism: $h(x \vee y) = (x \vee y) \vee b = (x \vee y) \vee (b \vee b) = (x \vee b) \vee (y \vee b) = h(x) \vee h(y)$, and $h(x \wedge y) = (x \wedge y) \vee b = (x \vee b) \wedge (y \vee b) = h(x) \wedge h(y)$.

Exercise: Prove that for every lattice $\boldsymbol{L}$ the mapping $x \mapsto x \vee a$ is an endomorphism of $\boldsymbol{L}$ for all $a \in A$ iff $\boldsymbol{L}$ is distributive.

Theorem 2.13. *Let $\boldsymbol{A}, \boldsymbol{B}$ be Σ-algebras and $h \in \mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B})$.*

(i) *For every $K \in \mathrm{Sub}(\boldsymbol{A})$, $h(K) \in \mathrm{Sub}(\boldsymbol{B})$.*
(ii) *For every $L \in \mathrm{Sub}(\boldsymbol{B})$, $h^{-1}(L) := \{\, a \in A : h(a) \in L \,\} \in \mathrm{Sub}(\boldsymbol{A})$.*
(iii) *For every $X \subseteq A$, $h\big(\mathrm{Sg}^{\boldsymbol{A}}(X)\big) \in \mathrm{Sg}^{\boldsymbol{A}}\big(h(X)\big)$.*

Proof. (i). Let $\sigma \in \Sigma_n$ and $b_1, \dots, b_n \in h(K)$. Choose $a_1, \dots, a_n \in K$ such that $h(a_1) = b_1, \dots, h(a_n) = b_n$. Then $\sigma^{\boldsymbol{B}}(b_1, \dots, b_n) = \sigma^{\boldsymbol{B}}\big(h(a_1), \dots, h(a_n)\big) = h\big(\sigma^{\boldsymbol{A}}(a_1, \dots, a_n)\big) \in h(K)$.

(ii). Let $a_1, \dots, a_n \in h^{-1}(L)$, i.e., $h(a_1), \dots, h(a_n) \in L$. Then $h\big(\sigma^{\boldsymbol{A}}(a_1, \dots, a_n)\big) = \sigma^{\boldsymbol{B}}\big(h(a_1), \dots, h(a_n)\big) \in L$. So $\sigma^{\boldsymbol{A}}(a_1, \dots, a_n) \in h^{-1}(L)$.

(iii). $h(X) \subseteq h\big(\mathrm{Sg}^{\boldsymbol{A}}(X)\big) \in \mathrm{Sub}(\boldsymbol{B})$ by part (i). So $\mathrm{Sg}^{\boldsymbol{B}}\big(h(X)\big) \subseteq h\big(\mathrm{Sg}^{\boldsymbol{A}}(X)\big)$. For the reverse inclusion, $X \subseteq h^{-1}(h(X)) \subseteq h^{-1}\big(\mathrm{Sg}^{\boldsymbol{A}}(h(X)\big) \in \mathrm{Sub}(\boldsymbol{A})$ by part (ii). So $\mathrm{Sg}^{\boldsymbol{A}}(X) \subseteq h^{-1}\big(\mathrm{Sg}^{\boldsymbol{A}}(h(X))\big)$. □

$h(\boldsymbol{A})$ will denote the unique subalgebra of $\boldsymbol{B}$ with universe $h(A)$ and if $\boldsymbol{B'} \subseteq \boldsymbol{B}$, then $h^{-1}(\boldsymbol{B'})$ is the unique subalgebra of $\boldsymbol{A}$ with universe $h^{-1}(B')$.

Theorem 2.14. *Let $\boldsymbol{A} = \langle A, f \rangle$ be a finite, cyclic mono-unary algebra with period p and tail length l (see Figure 1). Let $h\colon \boldsymbol{A} \twoheadrightarrow \boldsymbol{A'}$ be a epimorphism. Then $\boldsymbol{A'}$ is finite, cyclic mono-unary algebra. Let p' be its period and l' its tail length. Then p' divides p and $l' \leq l$.*

Proof. By Theorem 2.13(iii), $\boldsymbol{A'}$ is a cyclic mono-unary algebra, and it is obviously finite. Let $A = \mathrm{Sg}^{\boldsymbol{A}}\big(\{a\}\big)$. Then $A' = \mathrm{Sg}^{\boldsymbol{A'}}(\{h(a)\})$ by Theorem 2.13(iii). By definition p is the smallest $m \in \omega \setminus \{0\}$ such that there is an $n \in \omega$ such that $f^{n+m}(a) = f^n(a)$, and l is the smallest $n \in \omega$ such that $f^{n+p}(a) = f^n(a)$. p' and l' are defined similarly. For every $n \geq l$ and every $q \in \omega$, we have

(20)
$$f^{n+qp}(a) = f^{n-l}\big(f^{l+qp}(a)\big) = f^{n-l}\big(\underbrace{f^p(f^p(\dots(f^p}_{q}(f^l(a)))\dots)\big)\big) = f^{n-l}\big(f^l(a)\big) = f^n(a).$$

We claim that, for all $n, m \in \omega$ with $m > 0$,

$$\text{if } f^{n+m}(a) = f^n(a) \text{ then } p \text{ divides } m.$$

For every $n' \geq n$, $f^{n'+m}(a) = f^{n'-n}\big(f^{n+m}(a)\big) = f^{n'-n}\big(f^n(a)\big) = f^{n'}(a)$. So without loss of generalization we assme $n \geq l$ By the division algorithm, $m = qp + r$ with $0 \leq r < p$. Then by (20), $f^{n+r}(a) = f^{n+r+qp}(a) = f^{n+m}(a) = f^n(a)$. By the minimality of p, $r = 0$; so $p \mid m$.

$f^{l+p}\big(h(a)\big) = h\big(f^{l+p}(a)\big) = h\big(f^l(a)\big) = f^l\big(h(a)\big)$. So by (20) (with $\boldsymbol{A'}$, $h(a)$, and p' in place of $\boldsymbol{A}$, a, and p, respectively), we get that p' divides p. Furthermore, choose q such that $l + qp \geq l'$. Then $f^{l+p'}\big(h(a)\big) = f^{p'}\big(f^l(h(a))\big) = f^{p'}\big(f^{l+qp}(h(a))\big) = f^{l+qp+p'}\big(h(a)\big) = f^{l+qp}\big(h(a)\big) = f^l\big(h(a)\big)$. So $l' \leq l$ by the minimality of l'. □

Define the binary relation $\preccurlyeq$ on $\mathsf{Alg}(\Sigma)$ by $\boldsymbol{A} \preccurlyeq \boldsymbol{B}$ (equivalently $\boldsymbol{B} \succcurlyeq \boldsymbol{A}$) if $\boldsymbol{A}$ is a *homomorphic image* of $\boldsymbol{B}$, i.e., there is an epimorphism $h\colon \boldsymbol{B} \twoheadrightarrow \boldsymbol{A}$. $\preccurlyeq$ is clearly reflexive and it is also transitive, for if $h\colon \boldsymbol{B} \twoheadrightarrow \boldsymbol{A}$ and $g\colon \boldsymbol{C} \twoheadrightarrow \boldsymbol{B}$, then $h \circ g\colon \boldsymbol{C} \twoheadrightarrow \boldsymbol{A}$. However, $\preccurlyeq$ fails to be antisymmetric in a strong way: in general,

$$\boldsymbol{A} \leq \boldsymbol{B} \text{ and } \boldsymbol{B} \leq \boldsymbol{C} \text{ does not imply } \boldsymbol{A} \cong \boldsymbol{B}.$$

For example, let $\boldsymbol{A} = \langle [0,3], \leq \rangle$ and $\boldsymbol{B} = \langle [0,1] \cup [2,3], \leq \rangle$. Define

$$h(x) = \begin{cases} x & \text{if } 0 \leq x \leq 1, \\ 2 & \text{if } 1 < x < 2, \\ x & \text{if } 2 \leq x \leq 3 \end{cases} \quad \text{and} \quad g(x) = \begin{cases} 3x & \text{if } 0 \leq x \leq 1, \\ 3 & \text{if } 1 < x \leq 3. \end{cases}$$

We leave it as an exercise to prove that h is an epimorphism from the lattice $\boldsymbol{A}$ to $\boldsymbol{B}$ and that g is an epimorphism in the opposite direction. However, $\boldsymbol{A} \ncong \boldsymbol{B}$. To see this note that an isomorphism preserves compact elements, but $\boldsymbol{A}$ had only one compact element, 0, while $\boldsymbol{B}$ has two, 0 and 2.

If $\boldsymbol{A}$ or $\boldsymbol{B}$ is finite, then $\boldsymbol{A} \preccurlyeq \boldsymbol{B}$ and $\boldsymbol{B} \preccurlyeq \boldsymbol{A}$ implies $\boldsymbol{A} \cong \boldsymbol{B}$. Because, $\boldsymbol{A} \preccurlyeq \boldsymbol{B}$ and $\boldsymbol{B} \preccurlyeq \boldsymbol{A}$ imply $|A| \leq |B|$ and $|B| \leq |A|$, i.e., $|A| = |B|$. So any surjective homomorphism from $\boldsymbol{A}$ onto $\boldsymbol{B}$ must be also injective by the pigeonhole principle. Thus $\boldsymbol{A} \cong \boldsymbol{B}$.

$\cong$ is an equivalence relation on $\mathsf{Alg}(\Sigma)$. ($\Delta_A \colon \boldsymbol{A} \cong \boldsymbol{A}$; if $h \colon \boldsymbol{A} \cong \boldsymbol{B}$ and $g \colon \boldsymbol{B} \cong \boldsymbol{C}$, then $g \circ h \colon \boldsymbol{A} \cong \boldsymbol{C}$; if $h \colon \boldsymbol{A} \cong \boldsymbol{B}$ then $h^{-1} \colon \boldsymbol{B} \cong \boldsymbol{A}$.) The equivalence class of $[\boldsymbol{A}]_{\cong}$ of $\boldsymbol{A}$ under $\cong$, which we normally write simply as $[\boldsymbol{A}]$, is called the *isomorphism type* of $\boldsymbol{A}$. ($[\boldsymbol{A}]$ is not a proper set, it's too big, but this problem can be disregarded for our purposes.) The class of all isomorphism types of Σ-algebras is denoted by $[\mathsf{Alg}(\Sigma)]$.

The relations of subalgebra and homomorphic image on $\mathsf{Alg}(\Sigma)$ induce corresponding relations on $[\mathsf{Alg}(\Sigma)]$.

- $[\boldsymbol{A}] \subseteq [\boldsymbol{B}]$ if $\boldsymbol{A} \cong \mathbin{;} \subseteq \boldsymbol{B}$, i.e., if $\exists \boldsymbol{C}(\boldsymbol{A} \cong \boldsymbol{C} \subseteq \boldsymbol{B})$.
- $[\boldsymbol{A} \preccurlyeq \boldsymbol{B}]$ if $\boldsymbol{A} \preccurlyeq \boldsymbol{B}$. (Note that because $\cong \subseteq \preccurlyeq$, $(\cong \mathbin{;} \preccurlyeq) \subseteq (\preccurlyeq \mathbin{;} \preccurlyeq) = \preccurlyeq$.)

$\subseteq$ and $\preccurlyeq$ are well defined in isomorphism types, i.e., if $\boldsymbol{A} \cong \boldsymbol{A}'$ and $\boldsymbol{B} \cong \boldsymbol{B}'$, then $\boldsymbol{A} \cong \mathbin{;} \subseteq \boldsymbol{B}$ iff $\boldsymbol{A}' \cong \mathbin{;} \subseteq \boldsymbol{B}'$ and $\boldsymbol{A} \preccurlyeq \boldsymbol{B}$ iff $\boldsymbol{A}' \preccurlyeq \boldsymbol{B}'$.

To see that these equivalences holds we observe that $\boldsymbol{A} \cong \mathbin{;} \subseteq \boldsymbol{B}$ implies $\boldsymbol{A}' \cong \mathbin{;} \cong \mathbin{;} \subseteq \mathbin{;} \cong \boldsymbol{B}'$, and $\boldsymbol{A} \preccurlyeq \boldsymbol{B}$ implies $\boldsymbol{A} \cong \mathbin{;} \preccurlyeq \mathbin{;} \cong \boldsymbol{B}$. The second implication holds because clearly $\cong \mathbin{;} \preccurlyeq \; = \; \preccurlyeq \mathbin{;} \cong \; = \; \preccurlyeq$. The first implication is an immediate consequence of the equality $\subseteq \mathbin{;} \cong \; = \; \cong \mathbin{;} \subseteq$, which is in turn a corollary of Thm. 2.15(i) below.

$\subseteq$ is a partial ordering of isomorphism types, and $\preccurlyeq$ is what is called a *quasi-ordering* or *pre-ordering*, i.e., it is reflexive and transitive but not symmetric. However, $\preccurlyeq$ is a partial ordering on *finite isomorphism types*, that is isomorphism types of finite algebras. Clearly, if $[\boldsymbol{A}] \preccurlyeq [\boldsymbol{B}]$ and $[\boldsymbol{B}] \preccurlyeq [\boldsymbol{C}]$ and $\boldsymbol{A}$ (equivalently $\boldsymbol{B}$) is finite, then $[\boldsymbol{A}] = [\boldsymbol{B}]$.

Let us consider the various relative products of $\subseteq$ and $\preccurlyeq$ and their converses:

$$\subseteq \mathbin{;} \preccurlyeq, \quad \preccurlyeq \mathbin{;} \subseteq, \quad \subseteq \mathbin{;} \succcurlyeq, \quad \succcurlyeq \mathbin{;} \subseteq .$$

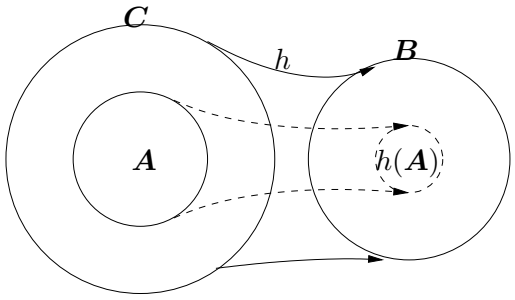
This gives half of the eight possible combinations, but each of the remaining four is a converse of one of these. For example, $(\supseteq \mathbin{;} \preccurlyeq) = (\breve{\subseteq} \mathbin{;} \breve{\succcurlyeq}) = (\subseteq \mathbin{;} \preccurlyeq)\breve{}$.

Theorem 2.15. *The following inclusions as relations be Σ-isomorphism types.*

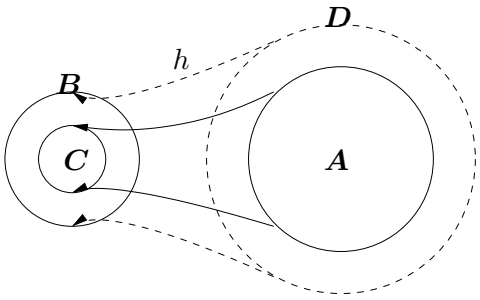
(i) $\subseteq \mathbin{;} \succcurlyeq \; = \; \succcurlyeq \mathbin{;} \subseteq$.
(ii) $\subseteq \mathbin{;} \preccurlyeq \; \subset \; \preccurlyeq \mathbin{;} \subseteq$.

Proof. (i) $\subseteq$. Assume $[\boldsymbol{A}] \subseteq \mathbin{;} \succcurlyeq [\boldsymbol{B}]$, i.e., there exists a $\boldsymbol{C}$ such that $\boldsymbol{A} \subseteq \boldsymbol{C} \succcurlyeq \boldsymbol{B}$. We need to show $[\boldsymbol{A}] \succcurlyeq \mathbin{;} \subseteq [\boldsymbol{B}]$, i.e., there exists a $\boldsymbol{D}$ such that $\boldsymbol{A} \succcurlyeq \boldsymbol{D} \subseteq \boldsymbol{B}$. Let $h \colon \boldsymbol{C} \twoheadrightarrow \boldsymbol{B}$. Then $\boldsymbol{A} \succcurlyeq h(\boldsymbol{A}) \subseteq \boldsymbol{B}$. See the following figure.

The inclusion $\supseteq$ of (i) is left as an exercise. See the following figure.



$\subseteq ; \succcurlyeq \subseteq \succcurlyeq ; \subseteq$



$\subseteq ; \succcurlyeq \supseteq \succcurlyeq ; \subseteq$

(ii) $\subseteq$. Assume $\boldsymbol{A} \subseteq \boldsymbol{C} \preccurlyeq \boldsymbol{B}$. Let $h\colon \boldsymbol{B} \twoheadrightarrow \boldsymbol{C}$. Then $\boldsymbol{A} \preccurlyeq h^{-1}(\boldsymbol{A}) \subseteq \boldsymbol{B}$.

We show by example that the inclusion of (ii) is proper. Let $\mathbb{Q} = \langle \mathbb{Q}, +, \cdot, -, 0, 1\rangle$ be the ring of rational numbers (a field). Recall that $\mathbb{Z} = \langle \mathbb{Z}, +, \cdot, -, 0, 1\rangle$ is the ring of integers and let $\mathbb{Z}_2 = \langle \mathbb{Z}_2, +, \cdot, -, 0, 1\rangle$ be the ring of integers (mod 2). We know that $\mathbb{Z}_2 \preccurlyeq \mathbb{Z} \subseteq \mathbb{Q}$, so $\mathbb{Z}_2 \preccurlyeq ; \subseteq \mathbb{Q}$. But it is not the case that $\mathbb{Z}_2 \subseteq ; \preccurlyeq \mathbb{Q}$. In fact, we show that

$$\mathbf{H}(\{\mathbb{Q}\}) = \mathbf{I}(\{\mathbb{Q}\}) \cup \{\, \boldsymbol{A} \in \mathsf{Alg}(\Sigma) : |A| = 1 \,\}, \tag{21}$$

i.e., the only nontrivial (two or more elements) homomorphic images of $\mathbb{Q}$ are its isomorphic images. Suppose $h\colon \mathbb{Q} \twoheadrightarrow \boldsymbol{A}$, and suppose h is not an isomorphism, i.e., it is not injective. Let a and b be distinct elements of $\mathbb{Q}$ such that $h(a) = h(b)$. $a - b \neq 0$ but $h(a - b) = h(a + -b) = h(a) + -h(b) = h(a) - h(b) = 0$. Thus $1 = h(1) = h((a - b) \cdot (a - b^{-1})) = h(a - b) \cdot h((a - b)^{-1}) = 0 \cdot h((a - b)^{-1}) = 0$. So for every $a \in A$, $a = 1 \cdot a = 0 \cdot a = 0$; i.e., $\boldsymbol{A}$ is trivial. This proves the claim.

Suppose now by way of contradiction that for some $\boldsymbol{A}$, $\mathbb{Z}_2 \subseteq \boldsymbol{A} \preccurlyeq \mathbb{Q}$. By the claim $\boldsymbol{A}$ must be either isomorphic to $\mathbb{Q}$ or a trivial one-element algebra. But $\mathbb{Z}_2$ is not isomorphic to an subalgebra of $\mathbb{Q}$. □

For any class K of Σ-algebras, we define

$$\mathbf{H}(\mathsf{K}) = \{\, \boldsymbol{A} \in \mathsf{Alg}(\Sigma) : \exists \boldsymbol{B} \in \mathsf{K}(\boldsymbol{A} \preccurlyeq \boldsymbol{B}) \,\},$$
$$\mathbf{I}(\mathsf{K}) = \{\, \boldsymbol{A} \in \mathsf{Alg}(\Sigma) : \exists \boldsymbol{B} \in \mathsf{K}(\boldsymbol{A} \cong \boldsymbol{B}) \,\},$$

the classes respectively of homomorphic and isomorphic images of algebras of K. $\mathbf{H}$ and $\mathbf{I}$ are algebraic closure operators on $\mathsf{Alg}(\Sigma)$. For example $\mathbf{H}\,\mathbf{H}(\mathsf{K}) = \mathbf{H}(\mathsf{K})$ because of the transitivity of $\preccurlyeq$. $\mathbf{H}$ is algebraic because $\mathbf{H}(\mathsf{K}) = \bigcup\{\, \mathbf{H}(\boldsymbol{A}) : \boldsymbol{A} \in \mathsf{K} \,\}$.

Theorem 2.16. *For any class* K *of* Σ*-algebras,*

(i) $\mathbf{S}\,\mathbf{H}(\mathsf{K}) \subseteq \mathbf{H}\,\mathbf{S}(\mathsf{K})$.

(ii) $\mathbf{H}\,\mathbf{S}$ *is an algebraic closure operator on* $\mathsf{Alg}(\Sigma)$.

Proof. (i). Suppose $\boldsymbol{A} \in \mathbf{S}\,\mathbf{H}(\mathsf{K})$. Then there exists a $\boldsymbol{B} \in \mathsf{K}$ such that $\boldsymbol{A} \subseteq ; \preccurlyeq \boldsymbol{B}$. Then by Thm. 2.15(ii), $\boldsymbol{A} \preccurlyeq ; \subseteq \boldsymbol{B}$. Thus $\boldsymbol{A} \in \mathbf{H}\,\mathbf{S}(\mathsf{K})$.

(ii) $\mathsf{K} \subseteq \mathbf{S}(\mathsf{K})$ by the extensivity of K, and hence by the extensivity and monotonicity of $\mathbf{H}$, $\mathsf{K} \subseteq \mathbf{H}(\mathsf{K}) \subseteq \mathbf{H}\,\mathbf{S}(\mathsf{K})$. So $\mathbf{H}\,\mathbf{S}$ is extensive. $\mathbf{H}\,\underline{\mathbf{S}\,\mathbf{H}}\,\mathbf{S}(\mathsf{K}) \overset{(i)}{\subseteq} \mathbf{H}\,\underline{\mathbf{H}\,\mathbf{S}}\,\mathbf{S}(\mathsf{K}) = \mathbf{H}\,\mathbf{S}(\mathsf{K})$. Since clearly $\mathbf{H}\,\mathbf{S}\,\mathbf{H}\,\mathbf{S}(\mathsf{K}) \subseteq \mathbf{H}\,\mathbf{S}(\mathsf{K})$, we get that $\mathbf{H}\,\mathbf{S}$ is idempotent. Finally, $\mathsf{K} \subseteq \mathsf{L}$ implies $\mathbf{S}(\mathsf{K}) \subseteq \mathbf{S}(\mathsf{L})$ which in turn implies $\mathbf{H}\,\mathbf{S}(\mathsf{K}) \subseteq \mathbf{H}\,\mathbf{S}(\mathsf{L})$. So $\mathbf{H}\,\mathbf{S}$ is monotonic. $\boldsymbol{A} \in \mathbf{H}\,\mathbf{S}(\mathsf{K})$ iff

there is a $\boldsymbol{B} \in \mathsf{K}$ such that $\boldsymbol{A} \preccurlyeq \boldsymbol{;} \subseteq \boldsymbol{B}$. Thus $\mathbf{HS}(\mathsf{K}) \subseteq \bigcup\{ \mathbf{HS}(\boldsymbol{B}) : \boldsymbol{B} \in \mathsf{K} \}$. Thus $\mathbf{HS}$ is algebraic. □

From Thm. 2.15(i) we see that the opposite inclusion of Thm. 2.16(i) does not in hold in general.

We also note the following obvious identities, which prove useful later. $\mathbf{I}(\mathsf{K}) = \mathbf{HI}(\mathsf{K}) = \mathbf{H}(\mathsf{K})$ and $\mathbf{IS}(\mathsf{K}) = \mathbf{SI}(\mathsf{K})$.

Let Σ be a multi-sorted signature with sort set S. Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be Σ-algebras. A *homomorphism* $h\colon \boldsymbol{A} \to \boldsymbol{B}$ is a *S-sorted map* $h = \langle h_s : s \in S \rangle$ such that, for all $s \in S$, $h_s\colon A_s \to B_s$, and for all $\sigma \in \Sigma$ of type $s_1, \dots, s_n \to s$ and for all $\langle a_1, \dots, a_n \rangle \in A_{s_1} \times \cdots \times A_{s_n}$, $h_s\big(\sigma^{\boldsymbol{A}}(a_1, \dots, a_n)\big) = \sigma^{\boldsymbol{B}}\big(h_{s_1}(a_1), \dots, h_{s_n}(a_n)\big)$.

Example. Let A and B be nonempty sets. Recall that

$$\mathbf{Lists}(A) = \big\langle \langle A \cup \{e_D\}, A^* \cup \{e_l\} \rangle, \mathtt{head}, \mathtt{tail}, \mathtt{append}, \mathtt{emptylist}, \mathtt{derror}, \mathtt{derror} \big\rangle.$$

Let $f\colon A \to B$ be any map. We define the S-sorted map $h = \langle h_D, h_L \rangle$ where $h_D \restriction A = f$ and $h_D(e_D) = e_D$, and, for all $a_1, \dots, a_n \in D$, $h_L(\langle a_1, \dots, a_n \rangle) = \langle f(a_1), \cdots, f(a_n) \rangle$, and $h_L(e_l) = e_l$. Then $h \in \mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B})$ and every homomorphism from $\boldsymbol{A}$ to $\boldsymbol{B}$ comes from some $f\colon A \to B$ in this way (Exercise).

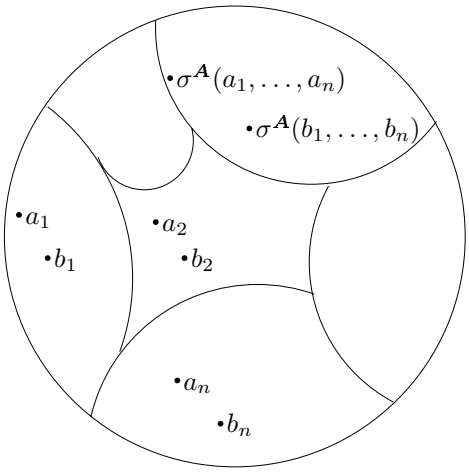
2.5. **Congruence relations and quotient algebras.**

Definition 2.17. Let $\boldsymbol{A}$ be a Σ-algebra. An equivalence relation E on A is called a *congruence relation* if, for all $n \in \boldsymbol{\omega}$, all $\sigma \in \Sigma_n$, and all $a_1, \dots, a_n, b_1, \dots, b_n \in A$,

$$a_1 \mathrel{E} b_1, \dots, a_n \mathrel{E} b_n \text{ imply } \sigma^{\boldsymbol{A}}(a_1, \dots, a_n) \mathrel{E} \sigma^{\boldsymbol{A}}(b_1, \dots, b_n). \tag{22}$$

The set of all congruences on $\boldsymbol{A}$ is denoted by $\mathrm{Co}(\boldsymbol{A})$.

(22) is called the *substitution property*. Intuitively, it asserts that the equivalence class of the result of applying any one of the fundamental operations of $\boldsymbol{A}$ depends only on the equivalence classes of the arguments. See the following figure.



We use lower case Greek letters, e.g., α, β, γ, etc., to represent congruence letters. The equivalence class $[a]_\alpha$ of a is called the *congruence class* of a and is normally denoted by

a/α. So $\alpha\,\alpha\,b$ iff $a/\alpha = b/\alpha$ iff $a \in b/\alpha$. The set of all congruence classes of α, i.e., the partition of α, is denoted by A/α.

Definition 2.18. Let $\boldsymbol{A}$ be a Σ-algebra and let $\alpha \in \mathrm{Co}(\boldsymbol{A})$. We define an Σ-algebra

$$\boldsymbol{A}/\alpha = \langle A/\alpha,\, \sigma^{\boldsymbol{A}/\alpha}\rangle_{\sigma\in\Sigma}$$

on the set of congruence classes of α as follows. For every $n \in \boldsymbol{\omega}$, every $\sigma \in \Sigma_n$, and for all $a_1/\alpha, \ldots, a_n/\alpha \in A/\alpha$,

$$\sigma^{\boldsymbol{A}/\alpha}(a_1/\alpha, \ldots, a_n/\alpha) = \sigma^{\boldsymbol{A}}(a_1, \ldots, a_n)/\alpha.$$

$\boldsymbol{A}/ga$ is called a *quotient algebra*, or more precisely, the *quotient of* $\boldsymbol{A}$ *by* α.

Note that $\sigma^{\boldsymbol{A}/\alpha}$ is well defined by the substitution property.

Examples. (1) $\Delta_A, \nabla_A \in \mathrm{Co}(\boldsymbol{A})$. $\boldsymbol{A}/\Delta_A \cong \boldsymbol{A}$ and $\boldsymbol{A}/\nabla_A$ is a trivial one-element algebra.

(2) Let $\boldsymbol{G} = \langle G, \cdot, {}^{-1}, e\rangle$ be a group. A subuniverse N of $\boldsymbol{G}$ is called *normal* if it is closed under *conjugation* by arbitrary elements of G, i.e., if $a \in N$ implies $x \cdot a \cdot x^{-1} \in N$ for every $x \in G$. Define $a\,\alpha\,b$ if $a \cdot b^{-1} \in N$. Then α is a congruence relation. Furthermore, for each congruence α on $\boldsymbol{G}$, e/α is a normal subuniverse of Γ. The mapping $\alpha \mapsto e/\alpha$ is a bijection between $\mathrm{Co}(\boldsymbol{G})$ and the normal subuniverses of $\boldsymbol{G}$. We leave the verification of all these facts to the reader but will give the details of a similar verification for rings.

(3) Let $\boldsymbol{R} = \langle R, +, \cdot, -, 0\rangle$ be a ring, and let I be an *ideal* subuniverse of $\boldsymbol{R}$: if $a \in I$ then $x \cdot a, a \cdot x \in I$ for every $x \in R$. Define $a\,\alpha\,b$ if $a - b$ $(= a + {-b})$ is in I. We show α is an equivalence relation. $a - a = 0 \in I$. $a - b, b - c \in I$ imply $a - c = (a - b) + (b - c) \in I$. $a - b \in I$ implies $b - a = -(a - b) \in I$. We now verify the substitution property. Suppose $a_1\,\alpha\,b_1$ and $a_2\,\alpha\,b_2$, i.e., $a_1 - b_1, a_2 - b_2 \in I$. Then $(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \in I$. So $(a_1 + a_2)\,\alpha\,(b_1 + b_2)$. $-a_1 - (-b_1) = -(a_1 - b_1) \in I$. So $-a_1\,\alpha\,-b_1$. Finally, $\big((a_1 - b_1)\cdot a_2\big) + (b_1 \cdot (a_2 - b_2)\big) \in I$. But $\big((a_1 - b_1)\cdot a_2\big) + (b_1 \cdot (a_2 - b_2)\big) = a_1 \cdot a_2 - b_1 \cdot a_2 + b_1 \cdot a_2 - b_1 \cdot b_2 = a_1 \cdot a_2 - b_1 \cdot b_2$. So $(a_1 \cdot a_2)\,\alpha\,(b_1 \cdot b_2)$. Thus α is a congruence on $\boldsymbol{G}$.

Now let $\alpha \in \mathrm{Co}(\boldsymbol{G})$. We check that $0/\alpha$ is an ideal. Let $a, a' \in 0/\alpha$, i.e., $a\,\alpha\,a'\,\alpha\,0$. Then $(a + a')\,\alpha\,(0 + 0) = 0$, $-a\;\alpha\;-0 = 0$, $(a \cdot a')\,\alpha\,(0 \cdot 0) = 0$. So $0/\alpha$ is a subuniverse. Moreover, for every $x \in R$, $(x \cdot a)\,\alpha\,(x \cdot 0) = 0$ and $(a \cdot x)\,\alpha\,(0 \cdot x) = 0$. So $0/\alpha$ is an ideal. Furthermore, $(a - b) \in 0/\alpha$ iff $(a - b)\,\alpha\,0$ iff $a = ((a - b) + b)\,\alpha\,(0 + b) = b$. So α is the congruence determined as in the first part by the ideal $0/\alpha$. Conversely, if one starts with an ideal I, constructs the congruence α as in the first part, then forms its ideal $0/\alpha$ one gets back I, because $a \in 0/\alpha$ iff $a\,\alpha\,0$ iff $a = (a - 0) \in I$. So for any ring $\boldsymbol{R}$ the mapping $\alpha \to 0/\alpha$ is a bijection between $\mathrm{Co}(\boldsymbol{R})$ and the set of ideals of $\boldsymbol{R}$.

(4) Let $\boldsymbol{L} = \langle L, \vee, \wedge, 0, 1\rangle$ be a bounded chain. Let $\alpha \in \mathrm{Co}(\boldsymbol{L})$. If $a \,\alpha\, b$ then, for every $c \in [a, b]$ $(= \{\, x \in L : a \leq x \leq b \,\})$ we have $c = (a \vee c)\,\alpha\,(b \vee c) = b$. So, if any two elements of $\boldsymbol{L}$ are identified, so are all the elements in the interval between the two. This implies that A/α is a partition of L into intervals, either closed, open, or half-open, and it is easy to check that every such partition is the partition of a congruence. For example $\{[0, 1/2),\ [1/2, 3/4],\ (3/4, 4/5),\ [4/5, 1]\}$ is the partition of a congruence of $\langle [0, 1], \leq\rangle$.

Theorem 2.20. *Let $\boldsymbol{A}$ be a Σ-algebra and let $\alpha \in \mathrm{Co}(\boldsymbol{A})$. The mapping $\Delta_\alpha : A \to A/\alpha$ such that, for all $a \in A$, $\Delta_\alpha(a) = a/\alpha$ is an epimorphism from $\boldsymbol{A}$ onto $\boldsymbol{A}/\alpha$ called the* ***natural map****.*

Proof.

$$\begin{aligned}\Delta_\alpha\big(\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n)\big) &= \sigma^{\boldsymbol{A}}(a_1, \ldots, a_n)/\alpha \\ &= \sigma^{\boldsymbol{A}/\alpha}(a_1/\alpha, \ldots, a_n/\alpha) \\ &= \sigma^{\boldsymbol{A}/\alpha}\big(\Delta_\alpha(a_1), \ldots, \Delta_\alpha(a_n)\big).\end{aligned}$$

Δ_α is obviously surjective. □

Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be Σ-algebras and $h \in \mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B})$. Thinking of h as is graph, a binary relation between A and B, we can form its converse $\breve{h} = \{\, \langle b, a\rangle \in B \times A : h(a) = b \,\}$. Note that $h\,;\breve{h} \subseteq A^2$ and that $a\,(h\,;\breve{h})\,a'$ iff there is a $b \in B$ such that $a\,h\,b\,\breve{h}\,a'$ iff there is a $b \in B$ such that $h(a) = b = h(a')$. Thus

$$h\,;\breve{h} = \{\, \langle a, a'\rangle \in A^2 : h(a) = h(a') \,\}.$$

We call this the *relation kernel of* h, in symbols $\mathrm{rker}(h)$. It is easy to check that $\mathrm{rker}(h)$ is an equivalence relation on A; its associated partition is $\{\, h^{-1}(b) : b \in h(A) \,\}$, where $h^{-1}(b) = \{\, a \in A : h(a) = b \,\}$. The substitution property also holds. In fact, if $h(a_i) = h(a_i')$, $i \leq n$, then $h\big(\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n)\big) = \sigma^{\boldsymbol{B}}\big(h(a_1), \ldots, h(a_n)\big) = \sigma^{\boldsymbol{B}}\big(h(a_1'), \ldots, h(a_n')\big) = h\big(\sigma^{\boldsymbol{A}}(a_1', \ldots, a_n')\big)$. So $\mathrm{rker}(h) \in \mathrm{Co}(\boldsymbol{A})$ for every Σ-algebra $\boldsymbol{B}$ and every $h \in \mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B})$.

The following observation is helpful in understanding the following Homomorphism Theorem. If $\alpha, \beta \in \mathrm{Co}(\boldsymbol{A})$, then $\alpha \subseteq \beta$ iff, for every $a \in A$, $a/\alpha \subseteq a/\beta$; see Figure 3.

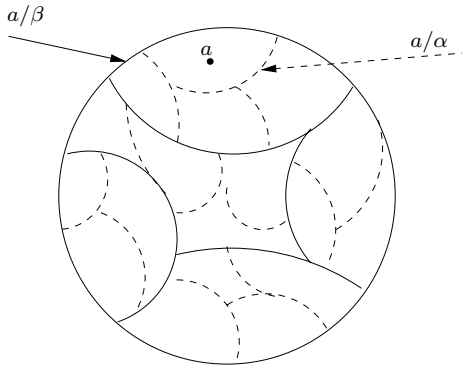


FIGURE 3

Theorem 2.21 (Homomorphism Theorem)**.** *Assume $\boldsymbol{A}$ and $\boldsymbol{B}$ are Σ-algebras. Let $h \in \mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B})$. If $\alpha \in \mathrm{Co}(\boldsymbol{A})$ and $\alpha \subseteq \mathrm{rker}(h)$, then the map $h_\alpha \colon A/\alpha \to B$ defined by $h_\alpha(a/\alpha) = h(a)$ for all $a \in A$ is well-defined and $h_\alpha \in \mathrm{Hom}(\boldsymbol{A}/\alpha, \boldsymbol{B})$. Furthermore, $h_\alpha \circ \Delta_\alpha = h$, i.e., the diagram in Figure 4 "commutes" in the sense that either of the two possible paths from $\boldsymbol{A}$ to $\boldsymbol{B}$ give the same result.*

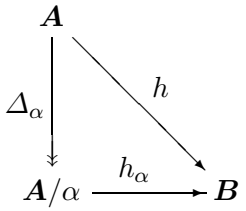


FIGURE 4

Proof. Let $a, a' \in A$ such that $a/\alpha = a'/\alpha$. Then $a/\mathrm{rker}(h) = a'/rker(h)$ since $\alpha \subseteq \mathrm{rker}(h)$. Thus $h(a) = h(a')$. So h_α is well-defined.

$$\begin{aligned}
h_\alpha\big(\sigma^{\boldsymbol{A}/\alpha}(a_1/\alpha, \ldots, a_n/\alpha)\big) &= h_\alpha(\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n)/\alpha\big), && \text{by defn. of } \boldsymbol{A}/\alpha \\
&= h\big(\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n)\big), && \text{by defn. of } h \\
&= \sigma^{\boldsymbol{B}}\big(h(a_1), \ldots, h(a_n)\big), && \text{since } h \text{ is a homomorphism} \\
&= \sigma^{\boldsymbol{B}}\big(h_\alpha(a_1/\alpha), \ldots, h_\alpha(a_n/\alpha)\big), && \text{by defn. of } h.
\end{aligned}$$

Thus $h_\alpha \in \mathrm{Hom}(\boldsymbol{A}/\alpha, \boldsymbol{B})$.

Finally we have $(h_\alpha \circ \Delta_\alpha)(a) = h_\alpha\big(\Delta_\alpha(a)\big) = h_\alpha(a/\alpha) = h(a)$. See Figure 5.

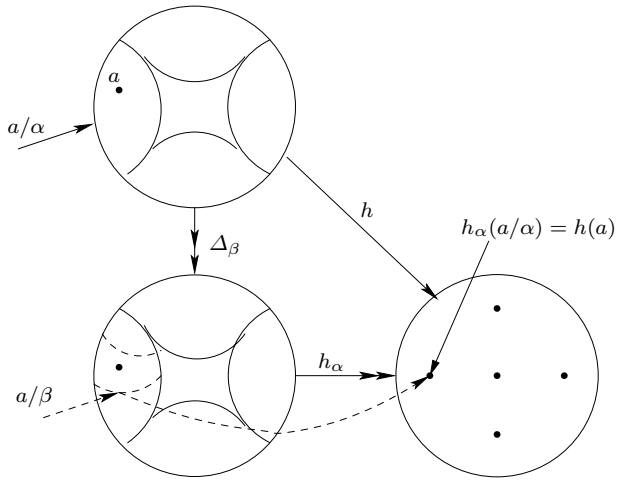


FIGURE 5

Thus Figure 4 commutes. □

On paraphases the conclusion of the theorem by saying that h "factors through" the natural map Δ_α.

Corollary 2.22 (First Isomorphism Theorem)**.** *$\boldsymbol{A} \succcurlyeq B$ iff there exists an $\alpha \in \mathrm{Co}(\boldsymbol{A})$ such that $\boldsymbol{A}/\alpha \cong \boldsymbol{B}$. In particular, if $h\colon \boldsymbol{A} \twoheadrightarrow \boldsymbol{B}$, then $\boldsymbol{A}/\operatorname{rker}(h) \cong \boldsymbol{B}$.*

Proof. Let $h\colon \boldsymbol{A} \twoheadrightarrow \boldsymbol{B}$, and let $\alpha = \operatorname{rker}(h)$. See Figure 6. $h_\alpha(a/\alpha) = h_\alpha(a'/\alpha)$ iff $h(a) =$

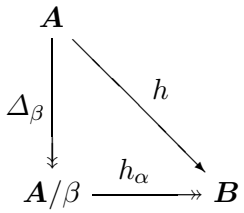


FIGURE 6

$h(a')$ iff $a/\operatorname{rker}(h) = a'/\operatorname{rker}(h)$ iff $a/\alpha = a'/\alpha$. So h_α is injective. Since it is clearly surjective we have $h_\alpha\colon \boldsymbol{A}/\alpha \cong \boldsymbol{B}$. □

Corollary 2.23. *Let $\alpha, \beta \in \mathrm{Co}(\boldsymbol{A})$. $\alpha \subseteq \beta$ implies $\boldsymbol{A}/\alpha/ \succcurlyeq \boldsymbol{A}/gb$.*

Proof. Exercise. □

Theorem 2.24 (Second Isomorphism Theorem)**.** *Let $\boldsymbol{A}$ be a Σ-algebra, and let $\alpha, \beta \in \mathrm{Co}(\boldsymbol{A})$ with $\alpha \subseteq \beta$. Let $\beta/\alpha = \{\, \langle a/\alpha, a'/\alpha\rangle : a \,\alpha\, a' \,\}$. Then $\beta/\alpha \in \mathrm{Co}(\boldsymbol{A}/\alpha)$ and $(\boldsymbol{A}/\alpha)/(\beta/\alpha) \cong \boldsymbol{A}/\beta$.*

Proof. By the Homomorphism Theorem $(\Delta_\beta)_\alpha\colon \boldsymbol{A}/\alpha \twoheadrightarrow \boldsymbol{A}/\beta$ where $(\Delta_\beta)_\alpha(a/\alpha) = \Delta_\beta(a) = a/\beta$. See Figure 7.

$$\begin{aligned} \langle a/\alpha,\, a'/\alpha\rangle \in \operatorname{rker}\big((\Delta_\beta)_\alpha\big) \quad &\text{iff} \quad (\Delta_\beta)_\alpha(a/\alpha) = (\Delta_\beta)_\alpha(a'/\alpha) \\ &\text{iff} \quad a/\beta = a'/\beta \\ &\text{iff} \quad a\,\beta\,a' \\ &\text{iff} \quad \langle a/\alpha,\, a'/\alpha\rangle \in \beta/\alpha. \end{aligned}$$

So $\operatorname{rker}\big((\Delta_\beta)_\alpha\big) = \beta/\alpha$ and hence $(\boldsymbol{A}/\alpha)/(\beta/\alpha) \cong \boldsymbol{A}/\beta$ by the First Isomorphism Theorem. □

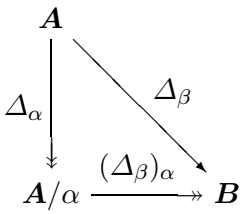


FIGURE 7

Let us recall the Third Isomorphism Theorem for groups. Let H be a subuniverse of a group $\boldsymbol{G}$ and let N be a normal subuniverse of $\boldsymbol{G}$. Let $\boldsymbol{H}\,N$ be the subgroup with universe $H\,N = \{\, h \cdot n : h \in H, n \in N \,\}$. Then $(\boldsymbol{H}\,N)/N \cong \boldsymbol{H}/(H \cap N)$ under the map $h/(H \cap N) \mapsto h/H$.

Let $\boldsymbol{A}$ be a Σ-algebra and let $\boldsymbol{B} \subseteq \boldsymbol{A}$. Let $\alpha \in \mathrm{Co}(\boldsymbol{A})$. Define $B\,\alpha = \bigcup\big(\, b/\alpha : b \in B \,\} = \{\, a/\alpha \in A/\alpha : \exists\, b \in B (a\,\alpha\,b \,\}$. Some simple observations:

(1) $\alpha \cap B^2 \in \mathrm{Co}(\boldsymbol{B})$. (exercise)

(2) $B \subseteq B\,\alpha \in \mathrm{Sub}(\boldsymbol{A})$. To see that $B\,\alpha$ is a subuniverse of $\boldsymbol{A}$, we note that $a_1\,\alpha\,b_1, \cdots, a_n\,\alpha\,b_n$ with $b_1, \ldots, b_n \in B$ imply $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n)\ \alpha\ \sigma^{\boldsymbol{A}}(b_1, \ldots, b_n)$ with $\sigma^{\boldsymbol{A}}(b_1, \ldots, b_n) \in B$.

Let $\boldsymbol{B}\,\alpha$ be the unique subalgebra of $\boldsymbol{A}$ with universe $B\,\alpha$. Then $\boldsymbol{B} \subseteq \boldsymbol{B}\,\alpha \subseteq \boldsymbol{A}$. See Figure 8

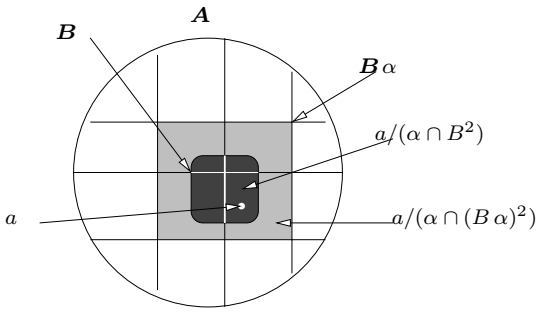


FIGURE 8

Theorem 2.25 (Third Isomorphism Theorem)**.** *Let $\boldsymbol{A}$ be a Σ-algebra, $\boldsymbol{B} \subseteq \boldsymbol{A}$, and $\alpha \in \mathrm{Co}(\boldsymbol{A})$. Then*

$$\boldsymbol{B}\,\alpha\big/(\alpha \cap (B\,\alpha)^2 \cong \boldsymbol{B}\big/(\alpha \cap B^2).$$

Proof. Define $h\colon B \to B\,\alpha\big/\big(\alpha \cap (B\,\alpha)^2\big)$ by $h(b) = b\big/\big(\alpha \cap (B\,\alpha)^2\big)$. h is surjective. Let $\beta = \alpha \cap (B\,\alpha)^2$.

$$\begin{aligned} h\big(\sigma^{\boldsymbol{B}}(b_1, \ldots, b_n)\big) &= \sigma^{\boldsymbol{B}}(b_1, \ldots, b_n)/\beta \\ &= \sigma^{\boldsymbol{B}\,\alpha}(b_1, \ldots, b_n)/\beta \\ &= \sigma^{\boldsymbol{B}\,\alpha/\beta}(b_1/\beta, \ldots, b_n/\beta) \\ &= \sigma^{\boldsymbol{B}\,\alpha/\beta}\big(h(b_1), \ldots, h(b_n)\big). \end{aligned}$$

So $h\colon \boldsymbol{B} \twoheadrightarrow \boldsymbol{B}\,\alpha/\beta$. For all $b, b' \in B$, $h(b) = h(b')$ iff $b/\beta = b'/\beta$ iff $b\,\beta\,b'$ iff $b\ \big(\alpha \cap (B\,\alpha)^2\big)\ b'$ iff $b\ (\alpha \cap B^2)\ b'$ since $b, b' \in B$. So $\mathrm{rker}(h) = \alpha \cap B^2$. Now apply the First Isomorphism Theorem. □

2.6. **The lattice of congruences.** *Notation:* Let $\alpha \in \mathrm{Co}(A)$, more generally, let $\alpha \in \mathrm{Eq}(A)$, i.e., an equivalence relation on A. Then for all $a, b \in A$ the following all mean the same thing. $\langle a, b\rangle \in \alpha$, $a\,\alpha\,\beta$, $a \equiv b \pmod{\alpha}$, $a \equiv b\,(\alpha)$, $a \equiv_\alpha b$.

Theorem 2.26. *$\langle A \times A, \mathrm{Co}(\boldsymbol{A})\rangle$ is an algebraic closed-set system for every Σ-algebra $\boldsymbol{A}$.*

Proof. Let $\mathcal{K} \subseteq \mathrm{Co}(\boldsymbol{A})$. $\mathcal{K} \subseteq \mathrm{Eq}(A)$, so $\bigcap \mathcal{K} \in \mathrm{Eq}(A)$. We must verify the substitution property. Let $\beta = \bigcap \mathcal{K}$ and assume that $a_i \equiv_\beta b_i$ for all $i \leq n$. Then $a_i \equiv_\alpha b_i$ for all $i \leq n$ and all $\alpha \in \mathcal{K}$. Thus $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \equiv_\alpha \sigma^{\boldsymbol{A}}(b_1, \ldots, b_n)$ for all $\alpha \in \mathcal{K}$, and hence $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \equiv_\beta \sigma^{\boldsymbol{A}}(b_1, \ldots, b_n)$. So $\beta \in \mathrm{Co}(\boldsymbol{A})$.

Assume now that $\mathcal{K}$ is directed, and let $\beta = \bigcup \mathcal{K}$. Then $\beta \in \mathrm{Eq}(A)$. Assume $a_i \equiv_\beta b_i$ for all $i \leq n$. Then for each $i \leq n$ there exists a $\alpha_i \in \mathcal{K}$ such that $a_i \equiv_{\alpha_i} b_i$. Take α to be an upper bound in $\mathcal{K}$ for all the α_i, $i \leq n$. α exists because $\mathcal{K}$ is directed. Then $a_i \equiv_\alpha b_i$ for all $i \leq n$. Thus $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \equiv_\alpha \sigma^{\boldsymbol{A}}(b_1, \ldots, b_n)$, and hence $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \equiv_\beta \sigma^{\boldsymbol{A}}(b_1, \ldots, b_n)$. So $\bigcup \mathcal{K} \in \mathrm{Co}(\boldsymbol{A})$. □

So $\mathbf{Co}(\boldsymbol{A}) = \langle \mathrm{Co}(\boldsymbol{A}), \bigvee^{\mathrm{Co}(\boldsymbol{A})}, \cap \rangle$ is a complete lattice where

$$\bigvee^{\mathbf{Co}(\boldsymbol{A})} \mathcal{K} = \bigcap \{ \beta \in \mathrm{Co}(\boldsymbol{A}) : \forall\, \alpha \in \mathcal{K}\, (\alpha \subseteq \beta) \}.$$

The associated closure operator $\mathrm{Cl}_{\mathrm{Co}(\boldsymbol{A})}$ gives congruence generation. Thus, for every $X \subseteq A^2$,

$$\mathrm{Cl}_{\mathrm{Co}(\boldsymbol{A})}(X) = \bigcap \{ \alpha \in \mathrm{Co}(\boldsymbol{A}) : X \subseteq \alpha \}$$

is the *congruence generated by* X. The traditional notation for this is $\Theta_{\boldsymbol{A}}(X)$, or just $\Theta(X)$ if $\boldsymbol{A}$ is clear from context. If X consists of a single ordered pair, say $X = \{\langle a, b \rangle\}$, then we write $\Theta_{\boldsymbol{A}}(a, b)$ for $\Theta_{\boldsymbol{A}}(X)$. Such a congruence, i.e., one generated by a single ordered pair, is called a *principal congruence*. Principal congruences are the congruence analogs of cyclic subuniverses.

Congruences are special kinds of equivalence relations and both form complete lattices. It is natural to ask about the relationship between the two lattices, in particular if the congruences form a sublattice of the equivalence relations. In fact they form a complete sublattice. In order to prove this the following lemmas about binary relations in general prove useful. We only considered the substitution property for equivalence relations, but the property makes sense for any binary relation on the universe of a Σ-algebra. Let $\boldsymbol{A}$ be a Σ-algebra and let $R \subseteq A^2$. R has the *substitution property* if $\langle a_i, b_i \rangle \in R$ for all $i \leq n$ implies $\langle \sigma^{\boldsymbol{A}}(a_1, \ldots, a_n), \sigma^{\boldsymbol{A}}(b_1, \ldots, b_n) \rangle \in R$.

Lemma 2.27. *Let $\boldsymbol{A}$ be a Σ-algebra. If $R, S \subseteq A^2$ both have the substitution property, then so does their relative product $R \,;\, S$.*

Proof. Suppose $a_i \; (R \,;\, S) \, b_i$ for all $i \leq n$. Then for each $i \leq n$ there is a $c_i \in A$ such that $a_i \, R \, c_i \, S \, b_i$. Thus $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \, R \, \sigma^{\boldsymbol{A}}(c_1, \ldots, c_n) \, S \, \sigma^{\boldsymbol{A}}(b_1, \ldots, b_n)$. Hence $\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \, R ; S \, \sigma^{\boldsymbol{A}}(b_1, \ldots, b_n)$. □

Lemma 2.28. *Let $\boldsymbol{A}$ be a Σ-algebra and let $\mathcal{R}$ be a directed set of binary relations on A. If each $R \in \mathcal{R}$ has the substitution property, then so does $\bigcup \mathcal{R}$.*

The proof is straightforward and is left as an exercise.

Theorem 2.29. *Let $\boldsymbol{A}$ be a Σ-algebra. $\mathbf{Co}(\boldsymbol{A})$ is a complete sublattice of $\mathbf{Eq}(A)$, i.e., for every $\mathcal{K} \subseteq \mathrm{Co}(\boldsymbol{A})$,*

$$\bigvee^{\mathbf{Co}(\boldsymbol{A})} \mathcal{K} = \bigvee^{\mathbf{Eq}(A)} \mathcal{K}.$$

Proof. The inclusion from right to left holds because $\bigvee^{\mathbf{Co}(\boldsymbol{A})} \mathcal{K}$ is an equivalence relation that includes each congruence in $\mathcal{K}$. For the inclusion in the opposite direction it suffices to show that $\bigvee^{\mathbf{Eq}(A)} \mathcal{K}$ has the substitution property. Let

$$\mathcal{R} = \big\{\, \alpha_1 \,;\, \alpha_2 \,;\, \cdots \,;\, \alpha_n : n \in \omega, \alpha_1, \dots, \alpha_n \in \mathcal{K} \,\big\}.$$

$\bigvee^{\mathbf{Eq}(A)} \mathcal{K} = \bigcup \mathcal{R}$ by Thm 1.17 and the exercise following it. Each relation in $\mathcal{R}$ has the substitution property by Lem. 2.27, and hence $\bigvee^{\mathbf{Eq}(A)} \mathcal{K}$ has the substitution property by Lem. 2.28. □

We next prove the analog for congruences of Theorem 2.14 that describes the behavior of subuniverses under homomorphisms and inverse homomorphisms. The situation is more complicated in the case of congruences however. For one thing nice results are obtained only for surjective homomorphisms.

Theorem 2.30. *Let $h\colon \boldsymbol{A} \twoheadrightarrow \boldsymbol{B}$ be an epimorphism between Σ-algebras.*

(i) *For every $\beta \in \mathrm{Co}(\boldsymbol{B})$, $h^{-1}(\beta) := \{\, \langle a, a' \rangle \in A : h(a) \equiv_\beta h(a') \,\} \in \mathrm{Co}(\boldsymbol{A})$, and* $\mathrm{rker}(h) \subseteq h^{-1}(\beta)$.

(ii) *For every $\alpha \in \mathrm{Co}(\boldsymbol{A})$, if* $\mathrm{rker}(h) \subseteq \alpha$, *then*

$$h(\alpha) := \{\, \langle h(a), h(b,) \rangle : a, a' \in A, a \equiv_\alpha a' \,\} \in \mathrm{Co}(\boldsymbol{B}).$$

(iii) *For every $X \subseteq A^2$, if* $\mathrm{rker}(h) \subseteq \Theta_{\boldsymbol{A}}(X)$, *then* $h\big(\Theta_{\boldsymbol{A}}(X)\big) = \Theta_{\boldsymbol{B}}\big(h(X)\big)$.

Proof. (i). We have $\boldsymbol{A} \overset{h}{\twoheadrightarrow} \boldsymbol{B} \overset{\Delta_\beta}{\twoheadrightarrow} \boldsymbol{B}/\beta$. Thus $(\Delta_\beta \circ h)\colon \boldsymbol{A} \twoheadrightarrow \boldsymbol{B}/\beta$. $h(a) \equiv_\beta h(a')$ iff $h(a)/\beta = h(a)/\beta$ iff $(\Delta_\beta \circ h)(a) = (\Delta_\beta) \circ h)(a')$. Thus $h^{-1}(\beta) = \mathrm{rker}(\Delta_\beta \circ h) \in \mathrm{Co}(\boldsymbol{A})$. If $h(a) = h(a')$ then obviously $(\Delta_\beta \circ h)(a) = (\Delta_\beta \circ h)(a')$. So $\mathrm{rker}(h) \subseteq \mathrm{rker}(\Delta_\beta \circ h)$ and hence $\mathrm{rker}(\Delta_\beta) \subseteq h^{-1}(\beta)$.

(ii) Assume $\mathrm{rker}(h) \subseteq \alpha$. $h(\Delta_A) = \big\{\, \langle h(a), h(a) \rangle : a \in A \,\big\} = \{\, \langle b, b \rangle : b \in h(A) \,\} = \Delta_{h(A)}$. So $h(\Delta_A) = \Delta_B$ since h is surjective, and hence $\Delta_A \subseteq \alpha$ implies $\Delta_B \subseteq h(\alpha)$. So $h(\alpha)$ is reflexive.

$b \equiv_{h(\alpha)} b'$ implies the existence of $a, a' \in A$ such that $a \equiv_\alpha a'$ and $h(a) = b, h(a') = b'$. But $a' \equiv_\alpha a$, so $b' \equiv_{h(\alpha)} b$. So $h(\alpha)$ is symmetric.

Transitivity requires the assumption $\mathrm{rker}(h) \subseteq \alpha$. Suppose $b_0 \equiv_{h(\alpha)} b_1 \equiv_{h(\alpha)} b_2$. Then there exist $a_0, a_1 \in A$ such that $a_0 \equiv_\alpha a_1$ and $h(a_0) = b_0$ and $h(a_1) = b_1$. There also exist $a_1', a_2 \in A$ such that $a_1' \equiv_\alpha a_2$ and $h(a_1') = b_1$ and $h(a_2) = b_2$. Thus

$$a_0 \equiv_\alpha a_1 \equiv_{\mathrm{rker}(h)} a_1' \equiv_\alpha a_2.$$

Since $\mathrm{rker}(h) \subseteq \alpha$, $a_0 \equiv_\alpha a_2$, and hence $b_0 = h(a_0) \equiv_{h(\alpha)} h(a_2) = b_2$. So $h(\alpha)$ is transitive and hence an equivalence relation.

The proof of the substitution property follows a familar pattern and is represented diagramatically. Assume that for each $i \leq n$ we have

$$\begin{array}{ccc} a_i & \equiv_\alpha & a_i' \\ \big\downarrow h & & \big\downarrow h \\ b_i & \equiv_{h(\alpha)} & b_i'. \end{array}$$

Then we have

$$\begin{array}{ccc}
\sigma^{\boldsymbol{A}}(a_1,\dots,a_n) & \equiv_\alpha & \sigma^{\boldsymbol{A}}(a'_1,\dots,a'_n) \\
\Big\downarrow h & & \Big\downarrow h \\
h\big(\sigma^{\boldsymbol{A}}(a_1,\dots,a_n)\big) & \equiv_{h(\alpha)} & h\big(\sigma^{\boldsymbol{A}}(a'_1,\dots,a'_n)\big) \\
\| & & \| \\
\sigma^{\boldsymbol{B}}(b_1,\dots,b_n) & \equiv_{h(\alpha)} & \sigma^{\boldsymbol{B}}(b'_1,\dots,b'_n).
\end{array}$$

Thus $h(\alpha) \in \mathrm{Co}(\boldsymbol{B})$.

(iii) $h(X) \subseteq h\big(\Theta_{\boldsymbol{A}}(X)\big) \underset{(ii)}{\in} \mathrm{Co}(\boldsymbol{B})$. So $\Theta_{\boldsymbol{B}}\big(h(X)\big) \subseteq h\big(\Theta_{\boldsymbol{A}}(X)\big)$. $X \subseteq h^{-1}\big(\Theta_{\boldsymbol{B}}(h(X))\big) \underset{(i)}{\in} \mathrm{Co}(\boldsymbol{A})$. So $\Theta_{\boldsymbol{A}}(X) \subseteq h^{-1}\big(\Theta_{\boldsymbol{B}}(h(X))\big)$, and hence

$$h\big(\Theta_{\boldsymbol{A}}(X)\big) \subseteq hh^{-1}\big(\Theta_{\boldsymbol{B}}(h(x))\big) \subseteq \Theta_{\boldsymbol{B}}\big(h(X)\big).$$

□

The Correspondence Theorem, which we next prove, shows that the congruence lattice of every homomorphic image of a Σ-algebra is isomorphically embeddable as a special kind of sublattice of the congruence lattice of the algebra itself. To prepare for the theorem we must describe the special kind of sublattices that are involved.

Let $\boldsymbol{L} = \langle L, \wedge, \vee \rangle$ be a lattice. A subset X of $\boldsymbol{L}$ is a *lower segment* $x \in X$ implies $y \in X$ for every $y \leq x$. An lower segment is an *ideal* of $\boldsymbol{L}$ if it is closed under join, i.e., $x, y \in X$ implies $x \vee y \in X$. An ideal is obviously a subuniverse of $\boldsymbol{L}$, in fact, if $x \in X$ then $x \wedge y \in X$ for every $y \in L$. A *dual ideal* of $\boldsymbol{L}$ is an ideal of the dual lattice, i.e., X is a dual ideal if $x \in X$ implies $y \in X$ for every $y \geq x$ (X is an *upper segment*), and X is closed under meet. A dual ideal of $\boldsymbol{L}$ is also a subuniverse.

For every $a \in L$ we define:

$$L(a] = \{\, x \in L : x \leq a \,\} \quad \text{and} \quad L[a) = \{\, x \in L : a \leq x \,\}.$$

It is easy to see that $L(a]$ is an ideal of $\boldsymbol{L}$ and $L[a)$ is a dual ideal. $L[a)$ and $L(a]$ are subuniverses of $\boldsymbol{L}$ and the corresponding sublattices are denoted by $\boldsymbol{L}[a)$ and $\boldsymbol{L}(a]$, respectively. If $\boldsymbol{L}$ is a complete lattice, then $\boldsymbol{L}[a)$ and $\boldsymbol{L}(a]$ are complete sublattices (exercise). $\boldsymbol{L}(a]$ is called the *principal ideal generated by* a and $\boldsymbol{L}(a]$ is the *principal dual ideal generated by* a. See Figure 9

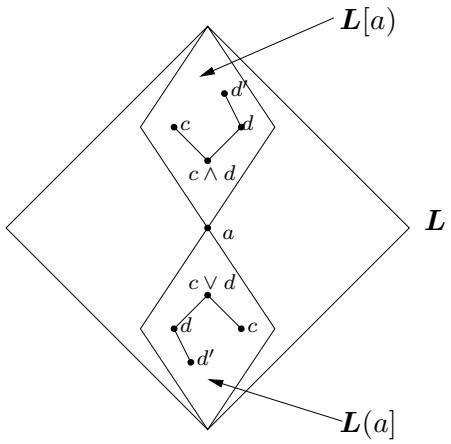


FIGURE 9

For example, in the chain lattice $\langle \mathbb{R}, \vee, \wedge \rangle$ of real numbers under the natural ordering, the principal ideals are the lower infinite closed intervals $(-\infty, a]$ and the principal dual ideals are the upper infinite closed intervals $[a, \infty)$.

Theorem 2.31 (Correspondence Theorem)**.** *Let $\boldsymbol{A}$ be a Σ-algebra and γ a congruence on $\boldsymbol{A}$. Then $\mathbf{Co}(\boldsymbol{A}/\gamma) \cong \mathbf{Co}(\boldsymbol{A})[\gamma)$. In particular, the mapping $\alpha \mapsto \alpha/\gamma$ is an isomorphism from $\mathbf{Co}(\boldsymbol{A})[\gamma)$ to $\mathbf{Co}(\boldsymbol{A}/\gamma)$, where $\alpha/\gamma = \{\, \langle a/\gamma, a'/\gamma \rangle : a \,\alpha\, a' \,\}$.*

Proof. For $\alpha \in \mathrm{Co}[\gamma)$ we have $\alpha/\gamma = \{\, \langle \Delta_\gamma(a), \Delta_\gamma(a) \rangle : a \,\alpha\, a' \,\} = \Delta_\gamma(\alpha)$, where $\Delta_\gamma \colon \boldsymbol{A} \twoheadrightarrow \boldsymbol{A}/\gamma$ is the natural map. So we must show that $\Delta_\gamma \colon \mathbf{Co}(\boldsymbol{A})[\gamma) \to \mathbf{Co}(\boldsymbol{A}/\gamma)$ is a lattice isomorphism. Note that $\mathrm{rker}(\Delta_\gamma) = \gamma$, because $\Delta_\gamma(a) = \Delta_\gamma(a')$ iff $a/\gamma = a'/\gamma$ iff $a \equiv_\gamma a'$.

Let $\beta \in \mathrm{Co}(\boldsymbol{A}/\gamma)$. By Lem. 2.30(i) we have $\gamma \subseteq \Delta_\gamma^{-1}(\beta) \in \mathrm{Co}(\boldsymbol{A})$, i.e., $\Delta_\gamma^{-1}(\beta) \in \mathrm{Co}(\boldsymbol{A})[\gamma]$. $\Delta_\gamma\Delta_\gamma^{-1}(\beta) = \beta$ by set theory since the mapping $\langle a, a'\rangle \mapsto \langle a/\gamma, a'/\gamma\rangle$ from A^2 to $(A/\gamma)^2$ is surjective.

Let $\alpha \in \mathrm{Co}(\boldsymbol{A})[\gamma]$, i.e., $\gamma \subseteq \alpha \in \mathrm{Co}(\boldsymbol{A})$. Then $\Delta_\gamma(\alpha) \in \mathrm{Co}(\boldsymbol{A}/\gamma)$ by Lem. 2.30(ii) because the relation kernel of Δ_γ, namely γ, is included in α. We claim that $\Delta_\gamma^{-1}\Delta_\gamma(\alpha) = \alpha$. By set theory $\alpha \subseteq \Delta_\gamma^{-1}\Delta_\gamma(\alpha)$. For the opposite inclusion, suppose $a \equiv a' \left(\Delta_\gamma^{-1}\Delta_\gamma(\alpha)\right)$. Then $\Delta_\gamma(a) \equiv \Delta_\gamma(a') \left(\Delta_\gamma\Delta_\gamma^{-1}\Delta_\gamma(\alpha)\right)$. But $\Delta_\gamma(a) = a/\gamma$ and $\Delta_\gamma(a') = a/\gamma$, and $\Delta_\gamma\Delta_\gamma^{-1}\Delta_\gamma(\alpha) \subseteq \Delta_\gamma(\alpha)$ by set theory. So $a/\gamma \equiv_{\Delta_\gamma(\alpha)} a'/\gamma$. Thus there exist $a_0, a_0' \in A$ such that $a/\gamma = a_0/\gamma$ and $a'/\gamma = a_0'/\gamma$ (i.e., $a_0 \equiv_\gamma a$ and $a_0' \equiv_\gamma a'$) and $a_0 \equiv_\alpha a_0'$. Since $\gamma \subseteq \alpha$ we have $a \equiv_\alpha a'$. Thus $\Delta_\gamma^{-1}\Delta_\gamma(\alpha) = \alpha$. Hence Δ_γ: $\mathrm{Co}(\boldsymbol{A})[\gamma] \twoheadrightarrow \mathrm{Co}(\boldsymbol{A}/\gamma)$ is a bijection with inverse Δ_γ^{-1}. $\alpha \subseteq \alpha'$ implies $\Delta_\gamma(\alpha) \subseteq \Delta_\gamma(\alpha')$ which in turn implies $\alpha = \Delta_\gamma^{-1}\Delta_\gamma(\alpha) \subseteq \Delta_\gamma^{-1}\Delta_\gamma(\alpha') = \alpha'$. So Δ_γ is strictly order-preserving and hence a lattice isomorphism by Thm. 1.8. □

As an example we consider the 3-atom Boolean algebra $\boldsymbol{B}_3$ (or more precisely its lattice reduct). Let h be the endomorphism of $\boldsymbol{B}_3$ indicated by the arrows in Figure 10 and let α be its relation kernel.

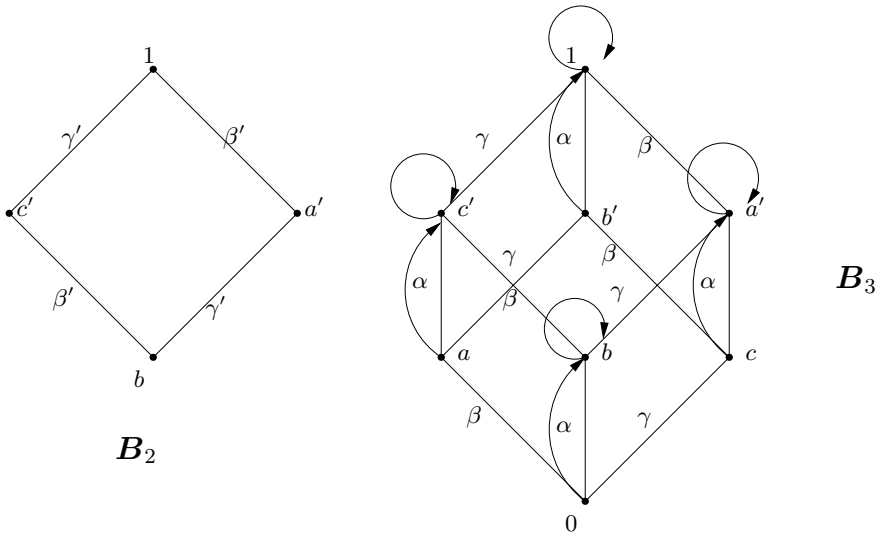


FIGURE 10

α is indicated on the Hasse diagram for $\boldsymbol{B}_3$ by labeling the edge between every pair of elements congruent mod α with "α". The two proper congruences β and γ that properly include α are also indicated on the diagram. β and γ are respectively he relation kernels of the endomorphisms that push the right front face onto the back left face, and the left front face onto the back right face. The quotient lattice $\boldsymbol{B}_3/\alpha$ is isomorphic to the image of $\boldsymbol{B}_3$ under h which is the 2-atom Boolean algebra $\boldsymbol{B}_2$. As guaranteed by the Correspondence Theorem there are just two proper congruences of $\boldsymbol{B}_2$ corresponding respectively to the β and γ; moreover $\mathbf{Co}(\boldsymbol{B}_2)$ and $\mathbf{Co}(\boldsymbol{B}_3)[\alpha]$ are isomorphic. See Figure 11.

In general, to form the join of a pair of congruences in the lattice of congruences (and also in the lattice of equivalence relations) one has to take arbitrary long alternating relative products of the two congruences (see Theorem 1.17, and the exercise immediately following

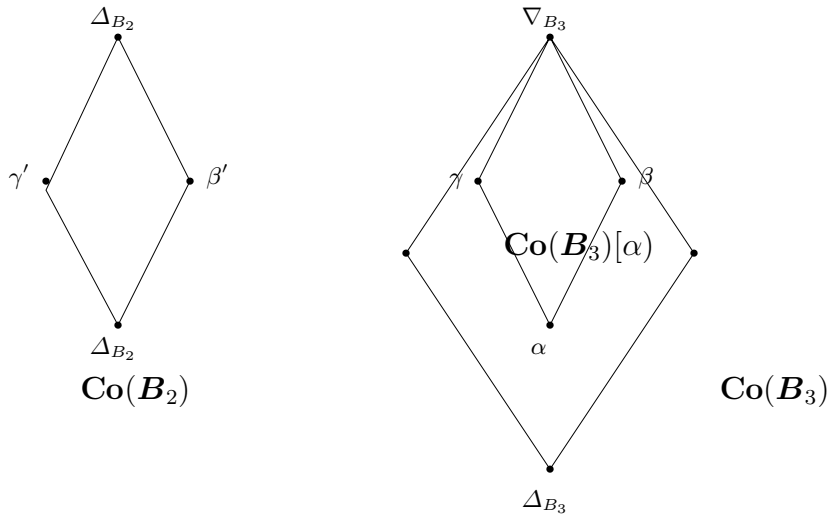


FIGURE 11

it, together with Theorem 2.29). For an important class of algebras only one iteration of the relative product is needed.

Theorem 2.32. *Let $\boldsymbol{A}$ be a Σ-algebra and let $\alpha, \beta \in \mathrm{Co}(\boldsymbol{A})$. The following are equivalent.*

(i) $\alpha \,;\, \beta \subseteq \beta \,;\, \alpha$.
(ii) $\alpha \,;\, \beta = \beta \,;\, \alpha$.
(iii) $\alpha \,;\, \beta \in \mathrm{Co}(\boldsymbol{A})$.
(iv) $\alpha \,;\, \beta = \alpha \vee^{\mathbf{Co}(\boldsymbol{A})} \beta$.

Proof. Here is the chain of implications we will prove: (i) $\iff$ (ii) $\implies$ (iv) $\iff$ (iii) $\implies$ (ii).

(i) $\iff$ (ii). The implication from right to left is trivial. Assume $\alpha;\beta \subseteq \beta;\alpha$. Since α and β are symmetric, $\breve{\alpha} = \alpha$ and $\breve{\beta} = \beta$. Thus $\beta \,;\, \alpha = \breve{\beta} \,;\, \breve{\alpha} = (\alpha \,;\, \beta)^{\smile} \subseteq (\beta \,;\, \alpha)^{\smile} = \breve{\alpha} \,;\, \breve{\beta} = \alpha \,;\, \beta$.

(i) $\implies$ (iv). Assume $\alpha \,;\, \beta = \beta \,;\, \alpha$. By Theorems 1.17 and 2.29 we have

$$\alpha \vee^{\mathbf{Co}(\boldsymbol{A})} \beta = \alpha \vee^{\mathbf{Eq}(\boldsymbol{A})} \beta = \alpha \,;\, \beta \cup \alpha \,;\, \beta \,;\, \alpha \,;\, \beta \cup \cdots \cup (\alpha \,;\, \beta)^n \cup \cdots .$$

The claim is that $(\alpha \,;\, \beta)^n = \alpha \,;\, \beta$ for all $n \in \omega$. This is trivial if $n = 1$. $(\alpha \,;\, \beta)^{n+1} = (\alpha \,;\, \beta)^n \alpha \,;\, \beta \underset{\text{ind. hyp.}}{=} \alpha \,;\, \beta \,;\, \alpha \,;\, \beta \underset{(ii)}{=} \alpha \,;\, \alpha \,;\, \beta \,;\, \beta = \alpha \,;\, \beta$. So $\alpha \vee^{\mathbf{Co}(\boldsymbol{A})} \beta = \alpha \,;\, \beta$.

(iii) $\iff$ (iv). Obvious.

(iii) $\implies$ (ii). Assume $\alpha \,;\, \beta \in \mathrm{Co}(\boldsymbol{A})$. Then $\alpha \,;\, \beta = (\alpha \,;\, \beta)^{\smile} = \breve{\beta} \,;\, \breve{\alpha} = \beta \,;\, \alpha$. □

Definition 2.33. A Σ-algebra $\boldsymbol{A}$ has *permutable congruence relations* if, for all $\alpha, \beta \in \mathrm{Co}(\boldsymbol{A})$, $\alpha \,;\, \beta = \beta \,;\, \alpha$.

Theorem 2.34. *Every group has permutable congruence relations.*

Proof. Let $\boldsymbol{G} = \langle G, \cdot, -1, e \rangle$ be a group and $\alpha, \beta \in \mathrm{Co}(\boldsymbol{G})$. Suppose $\langle a, b \rangle \in \alpha \,;\, \beta$. Then there is a $c \in G$ such that $a \,\alpha\, c \,\beta\, b$. The claim is that

$$a = ac^{-1}c \equiv_\beta ac^{-1}b \equiv_\alpha cc^{-1}b = b.$$

$ac^{-1} \equiv_\beta ac^{-1}$ and $c \equiv_\beta b$ imply $(ac^{-1})c \equiv_\beta (ac^{-1})b$, and $a \equiv_\alpha c$ and $c^{-1}b \equiv_\alpha c^{-1}b$ imply $a(c^{-1}b) \equiv_\alpha c(c^{-1}b)$. So $\langle a, b\rangle \in \beta\,;\,\alpha$. Hence $\alpha\,;\,\beta \subseteq \beta\,;\,\alpha$. □

The permutability of congruence relations on groups is a reflection of the fact that normal subuniverses permute under complex product, and hence that the relative product of two normal subuniverses is a normal subuniverse (recall the correspondence between congruences and normal subuniverses). This property of normal subgroups implies the following important property of groups. For all normal subuniverses N, M, and Q of a group $\boldsymbol{G}$,

$$N \subseteq M \text{ implies } N(M \cap Q) = M \cap (NQ).$$

This is the modular law for the lattice of normal subuniverses.

Definition 2.35. A lattice is *modular* if it satisfies the quasi-identity

$$\forall\, x, y \big(x \leq y \to x \vee (y \wedge z) \approx y \wedge (x \vee z)\big). \tag{23}$$

Remarks:

(1) The inclusion $x \vee (y \wedge z) \leq y \wedge (x \vee z)$ always holds if $x \leq y$ because $x \leq y$ and $x \leq x \vee z$ imply $x \leq y \wedge (x \vee z)$, and $y \wedge z \leq y$ and $y \wedge z \leq z \leq x \vee z$ imply $y \wedge z \leq y \wedge (x \vee z)$. And $x \leq y \wedge (x \vee z)$ and $y \wedge z \leq y \wedge (x \vee z)$ together imply $x \vee (y \wedge z) \leq y \wedge (x \vee z)$.

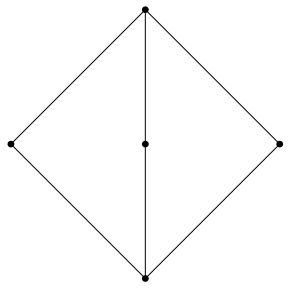
(2) The quasi-identity (23) is equivalent to the quasi-identity (by custom we omit the explicit quantifier)

$$(x \wedge y) \approx x \to x \vee (y \wedge z) \approx y \wedge (x \vee z)\big),$$

and hence to the identity obtained by substituting $x \wedge y$ for x in the right-hand side of this quasi-identity:

$$(x \wedge y) \vee (y \wedge z) \approx \big(\underbrace{(x \wedge y) \vee y}_{y}\big) \wedge \big((x \wedge y) \vee z\big).$$

So every distributive lattice is modular, but not conversely. The 3-atom distributive lattice $\boldsymbol{M}_3$ (see Figure 12) is modular but not conversely.



$\boldsymbol{M}_3$

FIGURE 12

There is easy way to see that a lattice is modular from its Hasse diagram. Let $\boldsymbol{L}$ be an arbitrary lattice and let x, y, z be arbitrary elements such that $x \leq y$. If the equation on the right side of (23) fails to hold, it is a easy to see that sub-poset of $\boldsymbol{L}$ with elements $x, y, z, x \vee z, y \wedge z$, $y \wedge (x \vee z)$, and $x \vee (y \wedge z)$ has the Hasse diagram given in Figure 13. Hence if a lattice fails to satisfy the modular law, then it must contain the lattice in Figure 14 as a sublattice.

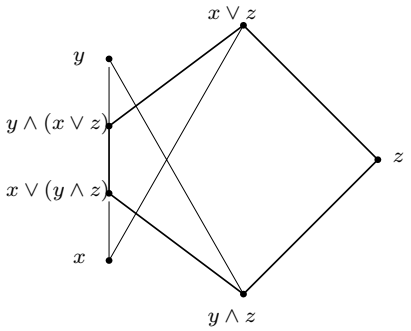
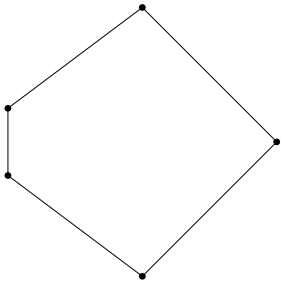


FIGURE 13



$\boldsymbol{N}_5$

FIGURE 14

This is the lattice $\boldsymbol{N}_5$. It is clearly nonmodular and from the above analysis we see that an arbitrary lattice is nonmodular iff it includes $\boldsymbol{N}_5$ as a sublattice. This simple characterization of nonmodular lattices is due to Dedekind. It follows immediately from this that $\boldsymbol{D}_3$ is modular.

Dedekind was also the one to show that the lattice of normal subgroups of a a lattice is modular. We will generalize this result to show that any congruence-permutable Σ-algebra has a modular congruence lattice. It turns our that there is more general form of the modular law that holds for the binary relations on any set.

Lemma 2.36 (Generalized Modular Law for Relations)**.** *Let A be any nonempty set and let $\alpha \in \mathrm{Eq}(A)$ and $\beta, \gamma \subseteq A \times A$.*

$$\beta \subseteq \alpha \text{ implies } \beta \,;\, (\alpha \cap \beta) \,;\, \beta = \alpha \cap (\beta \,;\, \gamma \,;\, \beta). \tag{24}$$

Proof. Assume $\beta \subseteq \alpha$. Then $\beta;(\alpha\cap\gamma);\beta \subseteq \alpha;\alpha;\alpha = \alpha$. Since the inclusion $\beta;(\alpha\cap\gamma);\beta \subseteq \beta \,;\, \gamma \,;\, \beta$ is obvious, we have the inclusion from left to right on the right-hand side of (24). So it suffices to prove

$$\alpha \cap (\beta \,;\, \gamma \,;\, \beta) \subseteq \beta \,;\, (\alpha \cap \beta) \,;\, \beta.$$

Let $\langle x, y\rangle \in \alpha \cap (\beta \,;\, \gamma \,;\, \beta)$, and let $a, b \in A$ such that $x \,\beta\, a \,\gamma\, b \,\beta\, y$. Consider the diagram in Figure 15.

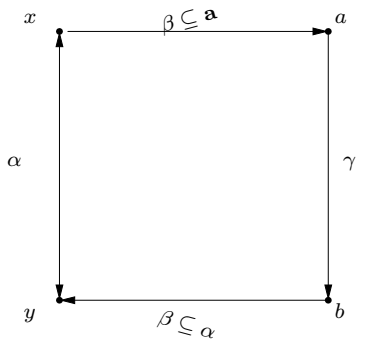


FIGURE 15

There are two ways to get from a to b. One is directly along the γ-arrow. The other is back along the reverse of the β-arrow to x and and then along the α-arrow to y and then along the reverse of the β-arrow to b. This gives $a\,(\breve{\beta}\,;\alpha\,;\breve{\beta})\,b$. But $\breve{\beta}\,;\alpha\,;\breve{\beta} \underset{\beta\subseteq\alpha}{\subseteq} \breve{\alpha}\,;\alpha\,;\breve{\alpha} = \alpha$, since α is assumed to be an equivalence relation. So $a\,(\alpha\cap\gamma)\,b$, and hence $x\,\beta\,a\,(\alpha\cap\gamma)\,b\,\beta\,y$. So $\langle x, y\rangle \in \beta\,;(\alpha\cap\gamma)\,\beta$. □

Theorem 2.37. *Let $\boldsymbol{A}$ be a Σ-algebra. If $\boldsymbol{A}$ has permutable congruence relations, then* $\mathbf{Co}(\boldsymbol{A})$ *is modular.*

Proof. Let $\alpha, \beta, \gamma \in \mathrm{Co}(\boldsymbol{A})$. $\beta\,;\gamma\,;\beta = \beta\,;\beta\,;\gamma = \beta\,;\gamma = \beta \vee \alpha$. And $\beta\,;(\alpha\cap\gamma)\,;\beta = \beta\,;\beta\,;(\alpha\cap\gamma) = \beta\,;(\alpha\cap\gamma) = \beta \vee (\alpha\cap\gamma)$. Thus, by Lem. 2.36,

$$\beta \subseteq \alpha \text{ implies } \beta \vee (\alpha\cap\gamma) = \alpha\cap(\beta\vee)\gamma).$$

□

2.7. **Simple algebras.** A common theme in algebra is to analyze the structure of a complex algebra by attempting to decompose it in some regular way into simpler algebras. The simplest groups from this point of groups are the groups that have no nonisomorphic nontrivial homomorphic images. These are the so-called simple groups and they have natural generalization to arbitrary Σ-algebras.

Definition 2.38. A Σ-algebra $\boldsymbol{A}$ is *simple* if it is nontrivial ($|A| \geq 2$) and $\mathrm{Co}\,\boldsymbol{A} = \{\Delta_A, \nabla_A\}$. Equivalently, $\boldsymbol{A}$ is *simple* if it is nontrivial and, for every Σ-algebra $\boldsymbol{B}$ and every epimorphism from $\boldsymbol{A}$ to $\boldsymbol{B}$, either $|B| = 1$ or $h\colon \boldsymbol{A} \cong \boldsymbol{B}$.

Remarks:

(1) Let $\alpha \in \mathrm{Co}(\boldsymbol{A})$. By the Correspondence Theorem $\boldsymbol{A}/\alpha$ is simple iff α is a coatom of the congruence lattice $\mathbf{Co}(\boldsymbol{A})$, i.e., α is a maximal proper congruence.

(2) $\boldsymbol{A}$ is simple iff $|A| \geq 2$ and $\Theta_{\boldsymbol{A}}(a, b) = \nabla_A$ every pair a, b of distinct elements of $\boldsymbol{A}$.

Examples:

(1) A group is simple iff it has no normal subuniverses. The alternating group A_n is simple for every $n \geq 5$.

(2) The only simple Abelian groups are $\mathbb{Z}_p$ for each prime p.

(3) Every field $\langle R, +, \cdot, -, 0, 1\rangle$ is simple.

(4) The n-atom modular lattice $\boldsymbol{M}_n$ is simple for every $n \geq 3$. See Figure 16.

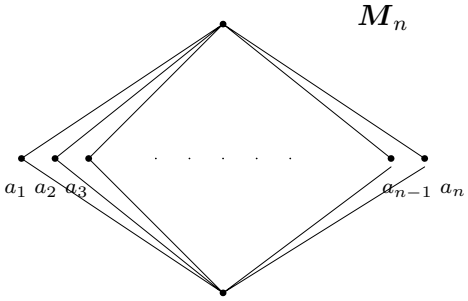


FIGURE 16

To see this first let $\alpha = \Theta_{\boldsymbol{M}_n}(a_i, a_j)$ with $i \neq j$. $1 = a_i \vee a_j \equiv_\alpha a_i \vee a_i = a_i = a_i \wedge a_i \equiv_\alpha a_i \wedge a_j = 0$. So $\Theta_{\boldsymbol{M}_n}(a_i, a_j) = \nabla_{M_n}$. Now let $\alpha = \Theta_{\boldsymbol{M}_n}(a_i, 0)$ and choose any $j \neq i$. $1 = a_i \vee a_j \equiv_\alpha 0 \vee a_j = a_j$. So $\Theta_{\boldsymbol{M}_n}(a_j, 1) \subseteq \Theta_{\boldsymbol{M}_n}(a_i, 0)$ for all $j \neq i$. If i, j, k are all distinct, then $a_j \equiv_\alpha 1 \equiv_\alpha a_k$, and hence $\nabla_{M_n} = \Theta_{\boldsymbol{M}_n}(a_j, a_k) \subseteq \Theta_{\boldsymbol{M}_n}(a_i, 0)$. Similarly $\Theta_{\boldsymbol{M}_n}(a_i, 1) = \nabla_{M_n}$.

(5) The only simple mono-unary algebras are cycles of prime order (exercise).

The proof of the following theorem is also left as an exercise.

Theorem 2.39. *Let $\boldsymbol{A}$ be a nontrivial Σ-algebra.*

(i) *If Δ_A finitely generated as a congruence of $\boldsymbol{A}$, then there exists a simple Σ-algebra $\boldsymbol{B}$ such that $\boldsymbol{B} \preccurlyeq \boldsymbol{A}$.*

(ii) *If Σ is finite (i.e., it has only a finite number of operation symbols) and A is finitely generated as a subuniverse of itself, then there exists a simple Σ-algebra $\boldsymbol{B}$ such that $\boldsymbol{B} \preccurlyeq \boldsymbol{A}$.*

Under the hypotheses of (ii) it can be shown that Δ_A is finitely generated.

As a corollary of this theorem every finite nontrivial Σ-algebra has a simple homomorphic image.

Lemma 2.40. *Let $\boldsymbol{A}$ be a nontrivial Σ-algebra. If $\boldsymbol{A}$ is nonsimple, then $\boldsymbol{A}$ has a nonsimple subalgebra that is generated by at most four elements.*

Proof. Suppose $\boldsymbol{A}$ is nonsimple. Then there exist $a, b \in A$, $a \neq b$, such that $\Theta_{\boldsymbol{A}}(a, b) \neq \nabla_A$. Let $c, d \in A$ such that $\langle c, d\rangle \notin \Theta_{\boldsymbol{A}}(a, b)$, and let $\boldsymbol{B} = \mathbf{Sg}^{\boldsymbol{A}}\{(a, b, c, d\}$ and $\alpha = \Theta_{\boldsymbol{A}}(a, b) \cap B^2$. $\alpha \in \mathrm{Co}(\boldsymbol{B})$, $\langle a, b\rangle \in \alpha$, and $\langle c, d\rangle \neq \alpha$. So $\alpha \neq \Delta_B, \nabla_B$. Hence $\boldsymbol{B}$ is not simple. □

As an immediate consequence of the lemma we have:

Theorem 2.41. *If every finitely generated subalgebra of a Σ-algebra $\boldsymbol{A}$ is simple, then so is $\boldsymbol{A}$.* □

Let Σ be a multi-sorted signature with sort set S, and let $\boldsymbol{A}$ and $\boldsymbol{B}$ be Σ-algebras. A *homomorphism* h for $\boldsymbol{A}$ to $\boldsymbol{B}$ is a S-sorted set $\langle\, h_s : s \in S \,\rangle$ such that $h_s \colon A_s \to B_s$ for every $s \in S$ and such that, for every $\sigma \in \Sigma$ with type $s_1, \ldots, s_n \to s$ and all $\langle a_1, \ldots, a_n\rangle \in A_{s_1} \times \cdots \times A_{s_n}$,

$$h_s\big(\sigma^{\boldsymbol{A}}(a_1, \ldots, a_n)\big) = \sigma^{\boldsymbol{B}}\big(h_{s_1}(a_1), \ldots, h_{s_n}(a_n)\big).$$

A *congruence* α on $\boldsymbol{A}$ is an S-sorted set $\langle\, \alpha_s : s \in S \,\rangle$ such that $\alpha_s \in \mathrm{Eq}(A_s)$ for each $s \in S$, and for every $\sigma \in \Sigma$ with type $s_1, \ldots, s_n \to s$ and all $\langle a_1, \ldots, a_n \rangle, \langle b_1, \ldots, b_n \rangle \in A_{s_1} \times \cdots \times A_{s_n}$,

$$\forall\, i \leq n\, (a_i \equiv_{\alpha_{s_i}} b_i) \Longrightarrow \sigma^{\boldsymbol{A}}(a_1, \ldots, a_n) \equiv_{\alpha_s} \sigma^{\boldsymbol{A}}(b_1, \ldots, b_n).$$

2.8. **Direct products.** Of the three basic ways of constructing new Σ-algebras from old ones, the direct product is the only one that increases complexity, or at least the size of the algebras. It is also distinct in that it is a way of combining system of many algebras into a single one.

Let I be a set (possibly empty) and let $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ be an I-indexed system of nonempty sets. We recall that the *direct* or *Cartesian product* of the system is

$$\prod_{i\in I} A_i = \big\{\, \vec{a} : \vec{a}\colon I \to \bigcup_{i\in I} A_i, \forall\, i \in I\, (\vec{a}(i) \in A_i) \,\big\}.$$

Intuitively, $\prod_{i\in I} A_i$ is the set of all "I-dimensional vectors", that is I-indexed systems of elements, such that the i-component is a member of A_i for each $i \in I$. We will often write a_i for the i-th component of $\vec{a}$, i.e., $a_i = \vec{a}(i)$, so that $\vec{a} = \langle\, a_i : i \in I \,\rangle$,

Definition 2.42. Let be a set (possibly empty) and let $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ be an I-indexed system of Σ-algebras. By the *direct* or *Cartesian product* of $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ we mean the Σ-algebra

$$\prod_{i\in I} \boldsymbol{A}_i = \big\langle \prod_{i\in I} A_i,\ \sigma^{\prod_i A_i} \big\rangle_{\sigma\in\Sigma},$$

where $\sigma^{\prod_i A_i}(\vec{a}_1, \ldots, \vec{a}_n) = \big\langle\, \sigma^{\boldsymbol{A}_i}\big(\vec{a}_1(i), \ldots, \vec{a}_n(i)\big) : i \in I \,\big\rangle$ for each $\sigma \in \Sigma_n$ and all $\vec{a}_1, \ldots, \vec{a}_n \in \prod_{i\in I} A_i$. The algebras $\boldsymbol{A}_i$ are called (*direct*) *factors* of $\prod_{i\in I} \boldsymbol{A}_i$.

By the *I-th direct*, or *I-th Cartesian, product* of a Σ-algebra $\boldsymbol{A}$ we mean $\boldsymbol{A}^I = \prod_{i\in I} \boldsymbol{A}_i$ were $\boldsymbol{A}_i = \boldsymbol{A}$ for every $i \in I$.

Remarks:

(1) We normally write $\boldsymbol{A}_1 \times \cdots \times \boldsymbol{A}_n$ for $\prod_{i\in\{1,2,\ldots,n\}} \boldsymbol{A}_i$.

(2) If the index set I is empty, then

$$\prod_{i\in I} A_i = \big\{\, \vec{a} : \vec{a}\colon I \to \bigcup, \forall\, i \in I\, (\vec{a}(i) \in A_i) \,\big\} = \{\, \vec{a} : \vec{a}\colon \emptyset \to \emptyset \,\} = \{\emptyset\},$$

where $\emptyset$ is the empty function, the function with empty domain. Thus $\prod_{i\in\emptyset} \boldsymbol{A}_i$ is a one-element Σ-algebra. All one-element Σ-algebras are isomorphic; they are called *trivial Σ-algebras*. They all have the form $\langle\, \{a\}, \sigma^{\boldsymbol{A}} \rangle_{\sigma\in\Sigma}$, where $\sigma^{\boldsymbol{A}}(a, \cdots, a) = a$ for all $\sigma \in \Sigma$.

Let $\boldsymbol{A} = \langle A, \vee^{\boldsymbol{A}}, \wedge^{\boldsymbol{A}}, 0^{\boldsymbol{A}}, 1^{\boldsymbol{A}} \rangle$ and $\boldsymbol{B} = \langle B, \vee^{\boldsymbol{B}}, \wedge^{\boldsymbol{B}}, 0^{\boldsymbol{B}}, 1^{\boldsymbol{B}} \rangle$ be bounded lattices.

$$\boldsymbol{A} \times \boldsymbol{B} = \langle A \times B, \vee^{\boldsymbol{A}\times\boldsymbol{B}}, \wedge^{\boldsymbol{A}\times\boldsymbol{B}}, 0^{\boldsymbol{A}\times\boldsymbol{B}}, 1^{\boldsymbol{A}\times\boldsymbol{B}} \rangle,$$

where $\langle a, b\rangle \vee^{\boldsymbol{A}\times\boldsymbol{B}} \langle a', b'\rangle = \langle a \vee^{\boldsymbol{A}} a',\, b \vee^{\boldsymbol{B}} b'\rangle$ and $\langle a, b\rangle \wedge^{\boldsymbol{A}\times\boldsymbol{B}} \langle a', b'\rangle = \langle a \wedge^{\boldsymbol{A}} a',\, b \wedge^{\boldsymbol{B}} b'\rangle$ and $0^{\boldsymbol{A}\times\boldsymbol{B}} = \langle 0^{\boldsymbol{A}},\, 0^{\boldsymbol{B}}\rangle$ and $1^{\boldsymbol{A}\times\boldsymbol{B}} = \langle 1^{\boldsymbol{A}},\, 1^{\boldsymbol{B}}\rangle$.

We note that

$$\langle a, b\rangle \leq^{\boldsymbol{A}\times\boldsymbol{B}} \langle a', b'\rangle \quad \text{iff} \quad a \leq^{\boldsymbol{A}} a' \text{ and } b \leq^{\boldsymbol{B}} b'.$$

This follows from the following simple computation. $\langle a, b\rangle \leq^{\boldsymbol{A}\times\boldsymbol{B}} \langle a', b'\rangle$ iff $\langle a, b\rangle \wedge^{\boldsymbol{A}\times\boldsymbol{B}} \langle a', b'\rangle = \langle a, b\rangle$ iff $\langle a \wedge^{\boldsymbol{A}} a',\, b \wedge^{\boldsymbol{B}} b'\rangle = \langle a', b'\rangle$ iff $a \wedge^{\boldsymbol{A}} a' = a$ and $b \wedge^{\boldsymbol{B}} b' = b$ iff $a \leq^{\boldsymbol{A}} a'$ and $b \leq^{\boldsymbol{B}} b'$. See Figure 17.

In general, for any system $\langle\, \boldsymbol{L}_i : i \in I \,\rangle$ of lattices, $\vec{a} \leq \vec{b}$ iff, for all $i \in I$, $\vec{a}(i) \leq \vec{b}(i)$ (exercise).

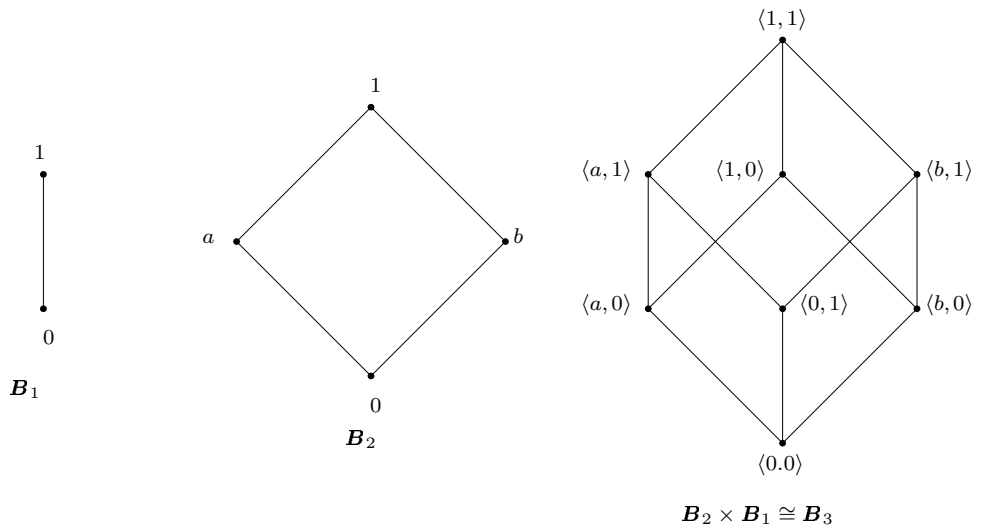


FIGURE 17

Theorem 2.43 (Generalized Communitive Law)**.** *Let* $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ *be a system of* Σ*-algebras and let* $h\colon I \rightarrowtail\!\!\!\!\twoheadrightarrow I$ *be a bijection between* I *and itself, i.e., a* permutation*. Then* $\prod_{i\in I} \boldsymbol{A}_i \cong \prod_{i\in I} \boldsymbol{A}_{h(i)}$.

Proof. The map $\vec{a} \mapsto \langle\, \vec{a}\big(h(i)\big) : i \in I \,\rangle$ is an isomorphism. This is left as an exercise. □

Corollary 2.44. (i) $\boldsymbol{A} \times \boldsymbol{B} \cong \boldsymbol{B} \times \boldsymbol{A}$.
(ii) $\boldsymbol{A} \times \boldsymbol{B} \times \boldsymbol{C} \cong \boldsymbol{A} \times \boldsymbol{C} \times \boldsymbol{B} \cong \boldsymbol{B} \times \boldsymbol{A} \times \boldsymbol{C} \cong \boldsymbol{B} \times \boldsymbol{C} \times \boldsymbol{A} \cong \boldsymbol{C} \times \boldsymbol{A} \times \boldsymbol{B} \cong \boldsymbol{C} \times \boldsymbol{B} \times \boldsymbol{A}$.

Proof. For example: Let $\boldsymbol{D}_1 = \boldsymbol{A}$, $\boldsymbol{D}_2 = \boldsymbol{B}$, and $\boldsymbol{D}_3 = \boldsymbol{C}$, and let $h(1) = 2$, $h(2) = 3$, and $h(3) = 1$. Then $\boldsymbol{A} \times \boldsymbol{B} \times \boldsymbol{C} = \prod_{i\in\{1,2,3\}} \boldsymbol{D}_i$ and $\boldsymbol{B} \times \boldsymbol{C} \times \boldsymbol{A} = \prod_{i\in\{1,2,3\}} \boldsymbol{A}_{h(i)}$. □

Theorem 2.45 (Generalized Associative Law)**.** *Let* $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$*, and let* $\{\, I_j : j \in J \,\}$ *be a partition of* I *then*

$$\prod_{j\in J}\Big(\prod_{i\in I_j} \boldsymbol{A}_i\Big) \cong \prod_{i\in I} \boldsymbol{A}_i.$$

Proof. The map $\vec{a} \mapsto \big\langle\, \langle \vec{a}(i) : i \in I_j \,\rangle : j \in J \,\big\rangle$ is an isomorphism (exercise). □

Corollary 2.46. $(\boldsymbol{A} \times \boldsymbol{B}) \times \boldsymbol{C} \cong \boldsymbol{A} \times (\boldsymbol{B} \times \boldsymbol{C}) \cong \boldsymbol{A} \times \boldsymbol{B} \times \boldsymbol{C}$. □

In the sequel, unless explicitly stated otherwise, $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ will be an I-indexed system of Σ-algebras, and $\vec{a}, \vec{b}, \vec{c}$ will represent arbitrary elements of $\prod_{i\in I} A_i$. $\prod_{i\in I} \boldsymbol{A}_i$ will often be written in the simpler form $\prod_i \boldsymbol{A}_i$ or, even more simply, $\prod \boldsymbol{A}_i$.

Definition 2.47. For each $i \in I$, $\pi\colon \prod_{i\in I} A_i \twoheadrightarrow A_i$ is defined by $\pi_i(\vec{a}) = \vec{a}(i)$ for each $i \in I$. φ_i is called the *i-th projection.*

Special case: $\pi_1\colon A \times B \twoheadrightarrow A$ and $\pi_2\colon A \times B \twoheadrightarrow B$.

Note that $\vec{a} = \vec{b}$ iff, for all $i \in I$, $\pi_i(\vec{a}) = \pi_i(\vec{b})$.

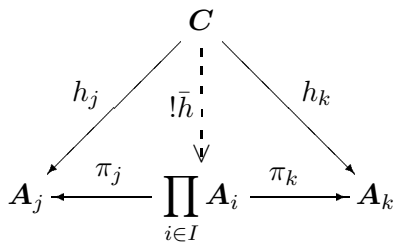


FIGURE 18

$\pi_i\colon \prod_{i\in I} \boldsymbol{A}_i \twoheadrightarrow \boldsymbol{A}_i$ is an epimorphism. We check this. $\pi_i\big(\sigma^{\prod_i \boldsymbol{A}_i}(\vec{a}_1,\dots,\vec{a}_n)\big) = \pi_i\big(\langle\, \sigma^{\boldsymbol{A}_j}(\vec{a}_1(j),\dots,\vec{a}_n(j)) : j \in J\,\rangle\big) = \sigma^{\boldsymbol{A}_i}\big(\vec{a}_1(i),\dots,\vec{a}_n(i) = \sigma^{\boldsymbol{A}_i}\big(\pi_i(\vec{a}_i),\dots,\pi_i(\vec{a}_n)\big)$.

Theorem 2.48 (Categorical Product Property)**.** *Let $\langle\, \boldsymbol{A}_i : i \in I\,\rangle$ be a system of Σ-algebras. For every Σ-algebra $\boldsymbol{C}$ and every system $\vec{h} = \langle\, h_i : i \in I\,\rangle \in \prod_{i\in I} \mathrm{Hom}(\boldsymbol{C}, \boldsymbol{A}_i)$ of homomorphisms of $\boldsymbol{C}$ into the $\boldsymbol{A}_i$, there exists a unique $\bar{h} \in \mathrm{Hom}\big(\boldsymbol{C}, \prod_{i\in I} \boldsymbol{A}_i\big)$ such that $h_i = \pi_i \circ \bar{h}$ for every $i \in I$, i.e., such that the diagram in Figure* 18 *is commutative.*

Proof. Define $\bar{h}$ by $\bar{h}(c) = \langle\, h_i(c) : i \in I\,\rangle$.

$$\begin{aligned}
\bar{h}\big(\sigma^{\boldsymbol{C}}(c_1,\dots,c_n)\big) &= \langle h_i\big(\sigma^{\boldsymbol{C}}(c_1,\dots,c_n)\big) : i \in I\,\rangle \\
&= \big\langle \sigma^{\boldsymbol{A}_i}\big(h_i(c_1),\dots,h_i(c_n)\big) : i \in I\,\big\rangle \\
&= \big\langle\, \sigma^{\boldsymbol{A}_i}\big(\bar{h}(c_1)(i),\dots,\bar{h}(c_n)(i)\big) : i \in I\,\big\rangle \\
&= \sigma^{\prod \boldsymbol{A}_i}\big(\bar{h}(c_1),\dots,\bar{h}(c_n)\big).
\end{aligned}$$

So $\bar{h}$ is a homomorphism.

For every $c \in C$ and every $j \in I$, $(\pi_j \circ \bar{h})(c) = \pi_j\big(\bar{h}(c)\big) = \pi_j\big(\langle\, h_i(c) : i \in I\,\rangle\big) = h_j(c)$. So $\pi_i \circ \bar{h} = h_i$ for each $i \in I$. □

Corollary 2.49. *$\boldsymbol{C} \succcurlyeq \mathbf{;} \subseteq \prod_{i\in I} \boldsymbol{A}_i$ iff, for every $i \in I$, $\boldsymbol{C} \succcurlyeq \mathbf{;} \subseteq \boldsymbol{A}_i$.*

Proof.

$$\begin{aligned}
\forall\, i \in I\,(\boldsymbol{C} \succcurlyeq \mathbf{;} \subseteq \boldsymbol{A}_i) &\iff \forall\, i \in I\,\exists\, h_i\colon \boldsymbol{C} \to \boldsymbol{A}_i) \\
&\iff \exists\, \bar{h}\,(\bar{h}\colon \boldsymbol{C} \to \prod_{i\in I} \boldsymbol{A}_i) \\
&\iff \boldsymbol{C} \succcurlyeq \mathbf{;} \prod_{i\in I} \boldsymbol{A}_i.
\end{aligned}$$

□

Corollary 2.50. *Let $j \in I$. Then $\boldsymbol{A}_j \cong \mathbf{;} \subseteq \prod_{i\in I} \boldsymbol{A}_i$ iff, for each $i \in I \setminus \{j\}$, $\boldsymbol{A}_j \succcurlyeq \mathbf{;} \subseteq \boldsymbol{A}_i$.*

Proof. $\implies$ Assume $\boldsymbol{A}_j \overset{h}{\cong} \boldsymbol{B} \subseteq \prod_{i\in I} \boldsymbol{A}_i$. Then $\pi_i \circ h\colon \boldsymbol{A}_j \to \boldsymbol{A}_i$ for each $i \in I \setminus \{j\}$.

$\impliedby$ Assume $h_i\colon \boldsymbol{A}_j \to \boldsymbol{A}_i$ for each $i \in I \setminus \{j\}$. Let $h_j = \Delta_{A_j}\colon \boldsymbol{A}_j \cong \boldsymbol{A}_j$. By the Categorical Product Property, there is a $\bar{h}\colon \boldsymbol{A}_j \to \prod_{i\in I} \boldsymbol{A}_i$ such that $\pi_i \circ \bar{h} = h_i$ for each

$i \in I$. For every $a \in A_j$, $\pi_j\big(\bar{h}(a)\big) = (\pi_j \circ \bar{h})(a) = h_j(a) = a$. Thus $\bar{h}$ is injective and hence $\boldsymbol{A}_j \overset{\bar{h}}{\cong} \bar{h}(\boldsymbol{A}_j) \subseteq \prod_{i\in I} \boldsymbol{A}_i$. So $\boldsymbol{A}_j \cong \mathbf{;} \subseteq \prod_{i\in I} \boldsymbol{A}_i$. □

In particular, if every $\boldsymbol{A}_i$ has a trivial subalgebra, then, for every $j \in I$, $\boldsymbol{A}_j$ is isomorphic to a subalgebra of $\prod_{i\in I} \boldsymbol{A}_i$. This is so because the function that maps all of A_j to the unique element of the trivial subalgebra of $\boldsymbol{A}_i$ for each $i \in I \setminus \{j\}$ is a homomorphism. For this reason every group is isomorphic to a subgroup of any direct product of groups which includes it as one of its direct factors.

Definition 2.51. Let $\boldsymbol{A}$ be a Σ-algebra. A system $\vec{\alpha} = \langle\, \alpha_i : i \in I \,\rangle$ of congruence relations of $\boldsymbol{A}$ is called a *factor congruence system* (FAC) *for* $\boldsymbol{A}$ if

(i) $\bigcap_{i\in I} \alpha_i = \Delta_A$, and,
(ii) for every $\vec{a} = \langle\, a_i : i \in I \,\rangle \in A^I$, $\bigcap_{i\in I}(a_i/\alpha_i) \neq \emptyset$.

Notice that $b \in \bigcap_{i\in I} a_i/\alpha_i$ iff b is a solution of the system of congruence equations

$$\forall\, i \in I\, (x \equiv a_i \pmod{\alpha_i}). \tag{25}$$

Notice further that condition (i) implies that any solution of this system of congruence equations is unique.

Thus condition (ii) in the above definition is equivalent to the requirement that the system (25) of congruence equations has a solution. For this reason condition (ii) is called the *Chinese Remainder Property*, the CRP for short. If $\langle n_1, \ldots, n_k\rangle$ is a finite system of pairwise relatively prime integers, and if for each $i \leq k$, α_i is the congruence on the ring of integers $\mathbb{Z}$ defined by $\langle a, b\rangle \in \alpha_i$ if $a \equiv b \pmod{n_i}$, then the classical Chinese Remainder Theorem says that $\langle \alpha_1, \ldots, \alpha_k\rangle$ has the CRP.

The following theorem characterizes those Σ-algebras $\boldsymbol{B}$ that are isomorphic to a given direct product in terms of the congruences of $\boldsymbol{B}$.

Theorem 2.52. *$\boldsymbol{B} \cong \prod_{i\in I} \boldsymbol{A}_i$ iff there exists a factor congruence system $\vec{\alpha} = \langle\, \alpha_i : i \in I \,\rangle$ such that, for all $i \in I$, $\boldsymbol{A}_i \cong \boldsymbol{B}/\alpha_i$.*

Proof. Suppose that $h\colon \boldsymbol{B} \cong \boldsymbol{C}$ and $\vec{\alpha} = \langle\, a_i : i \in I \,\rangle$ is a FCS for $\boldsymbol{C}$ such that $\boldsymbol{C}/\alpha_i \cong \boldsymbol{A}_i$ for each $i \in I$. Then we claim that $h^{-1}(\vec{\alpha}) := \langle\, h^{-1}(\alpha_i) : i \in I \,\rangle$ is a FCS for $\boldsymbol{B}$ such that $\boldsymbol{B}/h^{-1}(\alpha_i) \cong \boldsymbol{A}_i$ for each $i \in I$. (Recall that $h^{-1}(\alpha_i) = \{\, \langle b, b'\rangle \in B^2 : \langle h(b), h(b')\rangle \in \alpha_i \,\}$.) By set theory, $\bigcap_{i\in I} a_i/\alpha_i = h^{-1}\big(\bigcap_{i\in I} \alpha_i\big) = h^{-1}(\Delta_C) = \Delta_B$ (since h is a bijection). Also, consider any $\langle\, b_i : i \in I \,\rangle \in B^I$, and let $c \in C$ such that $c \equiv h(b_i) \pmod{\alpha_i}$ for each $i \in I$, i.e., $hh^{-1}(c) \equiv h(b_i) \pmod{\alpha_i}$ for each $i \in I$. Thus $h^{-1}(c)$ is a solution of the system of congruence equations $x \equiv b_i \pmod{h^{-1}(\alpha_i)}$, $i \in I$. Finally, the mapping from B to A/α_i such that $b \mapsto h(b)/\alpha_i$ is a surjective homomorphism with relation kernel $h^{-1}(\alpha_i)$. Thus $\boldsymbol{B}/h^{-1}(\alpha_i) \cong \boldsymbol{A}_i$ by the First Isomorphism Theorem. This establishes the claim.

We now verify the conclusion of the theorem.

$\Longrightarrow$ Assume $\boldsymbol{B} \cong \prod_{i\in I} \boldsymbol{A}_i$. By the above claim we can assume without loss of generality that $\boldsymbol{B} = \prod_{i\in I} \boldsymbol{A}_i$. Let $\alpha_i = \operatorname{rker}(\pi_i)$ for each $i \in I$. Note that,for each $i \in I$, $\vec{a}\,\alpha_i\,\vec{b}$ iff $\pi_i(\vec{a}) = \pi_i(\vec{b})$ iff $\vec{a}(i) = \vec{b}(i)$. So $\vec{a}\ \bigcap_{i\in I} \alpha\ \vec{b}$ iff $\forall\, i \in I\, (\vec{a}\,\alpha_i\,\vec{b})$ iff $\forall\, i \in I\, \big(\vec{a}(i) = \vec{b}(i)\big)$ iff $\vec{a} = \vec{b}$. So $\bigcap_{i\in I} \vec{a}_i = \Delta_A$.

Consider any $\langle\, \vec{a}_i : i \in I \,\rangle \in \left(\prod_{i\in I} A_i\right)^I$, and let $\vec{b} = \langle\, \vec{a}_i(i) : i \in I \,\rangle$. Then $\vec{a}_i(i) = \vec{b}(i)$ for all $i \in I$. So $\vec{a}_i \,\alpha_i\, \vec{b}$ for all $i \in I$, i.e., $\vec{b} = \bigcap_{i\in I} \vec{a}_i/\alpha_i$. And $\left(\prod_{i\in I} \boldsymbol{A}_i\right)/\alpha_i \cong \boldsymbol{A}_i$ by the First Isomorphism Theorem.

$\Longleftarrow$ Assume α is a factor congruence system for $\boldsymbol{B}$ such that $\boldsymbol{B}/\alpha_i \cong \boldsymbol{A}_i$ for all $i \in I$. Let $h_i\colon \boldsymbol{B} \twoheadrightarrow \boldsymbol{A}_i$ such that $\alpha_i = \operatorname{rker}(h_i)$. By the Categorical Product Property there exists a unique $\bar{h}\colon \boldsymbol{B} \to \prod_{i\in I} \boldsymbol{A}_i$ such that $\pi_i \circ \bar{h} = h_i$ for all $i \in I$, i.e., $\bar{h}(b)(i) = h_i(b)$ for each $b \in B$ and all $i \in I$. Thus, for all $b, b' \in B$,

$$\begin{aligned} \bar{h}(b) = \bar{h}(b') \quad &\text{iff} \quad \forall\, i \in I \left(h_i(b) = h_i(b')\right) \\ &\text{iff} \quad \forall\, i \in I \,(b \,\alpha_i\, b') \\ &\text{iff} \quad b \bigcap_{i\in I} \alpha_i \; b' \\ &\text{iff} \quad b = b'. \end{aligned}$$

So $\bar{h}$ is injective. Consider any $\vec{a} = \langle\, a_i : i \in I \,\rangle \in \prod_{i\in I} A_i$. For each $i \in I$ choose $b_i \in B$ such that $h_i(b_i) = a_i$. By the Chinese Remainder Property, there is a $b \in B$ such that, for every $i \in I$, $b \equiv_{\alpha_i} a_i$, i.e., $h_i(b) = a_i$ for every $i \in I$. So $\bar{h}(b) = \langle\, h_i(b) : i \in I \,\rangle = \langle\, a_i : i \in I \,\rangle = \vec{a}$. Thus $\bar{h}$ is surjective. □

Theorem 2.53. *let $\vec{\alpha} = \langle\, \alpha_i : i \in I \,\rangle$ be a factor congruence system for $\boldsymbol{A}$, and let $\{\, I_j : j \in J \,\}$ be a partition of I. Let $\beta_j = \bigcap_{i\in I_j} \alpha_i$, for all $j \in J$. Then $\vec{\beta} = \langle\, \beta_j : j \in J \,\rangle$ is also a factor congruence system for $\boldsymbol{A}$. In particular, for each $j \in I$, let $\hat{\alpha}_j = \bigcap_{i\in I\setminus\{j\}} \alpha_i$. Then $\langle\, \alpha_j, \hat{\alpha}_j \,\rangle$ is a factor congruence system for $\boldsymbol{A}$.*

Proof. $\bigcap_{j\in J} \beta_j = \bigcap_{j\in J} \bigcap_{i\in I_j} \alpha_i = \bigcap_{i\in I} \alpha_i = \Delta_A$. Let $\langle\, a_j : j \in J \,\rangle \in A^J$. By the CRP for $\vec{\alpha}$ there is a $b \in A$ such that $\forall\, j \in J \,\forall\, i \in I_j \,(b \equiv_{\alpha_i} a_j)$. Thus $\forall\, j \in J \left(b \equiv_{\bigcap_{i\in I_j} \alpha_i} a_j\right)$. I.e., $b \equiv_{\beta_i} a_j$. So, $\vec{\beta}$ has the Chinese Remainder Property. □

Definition 2.54. $\alpha \in \operatorname{Co}(\boldsymbol{A})$ is a *factor congruence of $\boldsymbol{A}$* if there exists a factor congruence system $\langle\, \beta_i : i \in I \,\rangle$ with $|I| \geq 2$ such that $\alpha = \beta_i$ for some $i \in I$.

Equivalently, by Thm. 2.53, α is a factor congruence if there is a $\hat{\alpha} \in \operatorname{Co}(\boldsymbol{A})$ such that $\langle \alpha, \hat{\alpha} \rangle$ is a factor congruence. α and $\hat{\alpha}$ are *complementary factor congruences of $\boldsymbol{A}$*.

Theorem 2.55. *Let $\alpha, \hat{\alpha} \in \operatorname{Co} \boldsymbol{A}$. α and $\hat{\alpha}$ are* complementary factor congruences *iff $\alpha \cap \hat{\alpha} = \Delta_A$ and $\alpha \,;\, \hat{\alpha} = \nabla_A$.*

Proof.

$$\begin{aligned} \alpha \,;\, \hat{\alpha} = \nabla_A \quad &\text{iff} \quad \forall\, \langle a_1, a_2 \rangle \in A^2 \,(a_1 \,(\alpha \,;\, \hat{\alpha})\, a_2) \\ &\text{iff} \quad \forall\, \langle a_1, a_2 \rangle \in A^2 \,\exists\, b \in A \,(b \,\alpha\, a_1 \text{ and } b \,\hat{\alpha}\, a_2) \\ &\text{iff} \quad \langle \alpha, \hat{\alpha} \rangle \text{ has the CRP.} \end{aligned}$$

□

Definition 2.56. A Σ algebra $\boldsymbol{A}$ is *directly indecomposable* or *directly irreducible* (DI) if, for every system of Σ-algebras $\langle\, \boldsymbol{B}_i : i \in I \,\rangle$, $\boldsymbol{A} \cong \prod_{i\in I} \boldsymbol{B}_i$ implies $\boldsymbol{B}_k$ is nontrivial for at exactly one $k \in I$.

If $\boldsymbol{A}$ is directly indecomposable, then $\boldsymbol{A} \cong \prod_{I \in i} \boldsymbol{B}_I$ implies that $\boldsymbol{A}$ is isomorphic to one of the $\boldsymbol{B}_i$, namely the one such that all the other direct factors are trivial. We see in Cor. 2.58 below that this is also a sufficient condition for direct idecomposability if $\boldsymbol{A}$ is finite.

Theorem 2.57. *Let $\boldsymbol{A}$ be a nontrivial Σ-algebra. The following three conditions are equivalent.*

(i) *$\boldsymbol{A}$ is directly indecomposable.*
(ii) *$\boldsymbol{A} \cong \boldsymbol{B} \times \boldsymbol{C}$ implies either $\boldsymbol{B}$ or $\boldsymbol{C}$ is trivial.*
(iii) *$\boldsymbol{A}$ has exactly two factor congruence relations, more precisely, the only two factor congruences of $\boldsymbol{A}$ are Δ_A and ∇_A.*

Proof. (i) $\Longrightarrow$ (ii): trivial

(ii) $\Longrightarrow$ (iii). Let α and $\hat{\alpha}$ be complementary congruences of $\boldsymbol{A}$. Then $\boldsymbol{A} \cong \boldsymbol{A}/\alpha \times \boldsymbol{A}/\hat{\alpha}$. By assumption $\boldsymbol{A}/\alpha$ or $\boldsymbol{A}/\hat{\alpha}$ is trivial. In the first case we have $\alpha = \nabla_A$ and hence $\hat{\alpha} = \nabla_A \cap \hat{\alpha} = \alpha \cap \hat{\alpha} = \Delta_A$. If $\boldsymbol{A}/\hat{\alpha}$ is trivial, then $\hat{\alpha} = \nabla_A$ and $\alpha = \Delta_A$. So Δ_A and ∇_A are the only factor congruences of $\boldsymbol{A}$.

(iii) $\Longrightarrow$ (i). Suppose $\boldsymbol{A} \cong \prod_{i \in I} \boldsymbol{B}_i$. Let $\langle\, \alpha_i : i \in I \,\rangle$ be a factor congruence system such that $\boldsymbol{B}_i \cong \boldsymbol{A}/\alpha_i$ for each $i \in I$. By assumption each α_i is either Δ_A or ∇_A. They all cannot be ∇_A since otherwise each $\boldsymbol{B}_i$ is trivial which is impossible since $\boldsymbol{A}$ is nontrivial. So $\alpha_k = \Delta_A$ for at least one $k \in I$. For each $i \in I$ let $\hat{\alpha}_i = \bigcap_{j \in I \setminus \{i\}} \alpha_j$. Note that, for each $i \in I \setminus \{k\}$, $\hat{\alpha}_i \subseteq \alpha_k = \Delta_A$ and hence $\hat{\alpha}_i = \Delta_A$. But by Thm. 2.53 α_i and $\hat{\alpha}_i$ are complementary congruences. So $\alpha_i = \nabla_A$ and hence $\boldsymbol{B}_i$ is trivial for all $i \in I \setminus \{k\}$. □

Every simple algebra is directly indecomposable. An example of a nonsimple algebra that is directly indecomposable is the Abelian group $\mathbb{Z}_{p^n} = \mathbb{Z}/\equiv (\mathrm{mod}\ p^n)$ for each prime p and positive integer n. The only (normal) subgroups are $p^k\mathbb{Z}_{p^n}$ for $k \leq n$ and hence the only congruence relations are $\equiv (\mathrm{mod}\ p^k)/\equiv (\mathrm{mod}\ p^n)$ for $k \leq n$. So the lattice of congruence relations is linearly ordered and hence the only factor congruences are

$$\Delta_{\mathbb{Z}_{p^n}} = \equiv (\mathrm{mod}\ p^n)/\equiv (\mathrm{mod}\ p^n) \quad \text{and} \quad \nabla_{\mathbb{Z}_{p^n}} = \equiv (\mathrm{mod}\ p^0)/\equiv (\mathrm{mod}\ p^n).$$

The fact that the $\mathbb{Z}_{p^n}$ are directly indecomposable, and in fact the only directly indecomposable finitely generated Abelian groups, can also be obtained from the Fundamental Theorem of Abelian Groups.

Corollary 2.58. *Let $\boldsymbol{A}$ be a finite, nontrivial Σ-algebra. The following three conditions are equivalent.*

(i) *$\boldsymbol{A}$ is directly indecomposable.*
(ii) *For every system of Σ-algebras $\langle\, \boldsymbol{B}_i : i \in I \,\rangle$, $\boldsymbol{A} \cong \prod_{i \in I} \boldsymbol{B}_i$ implies $\boldsymbol{B}_k \cong \boldsymbol{A}$ for some $k \in I$.*
(iii) *$\boldsymbol{A} \cong \boldsymbol{B} \times \boldsymbol{C}$ implies either $\boldsymbol{B} \cong \boldsymbol{A}$ or $\boldsymbol{C} \cong \boldsymbol{A}$.*

Proof. Suppose $\boldsymbol{A} \cong \prod_{i \in I} \boldsymbol{B}_i$. If $\boldsymbol{A} \cong \boldsymbol{B}_k$ for some $k \in I$, then $|B_k| = |A|$ and hence, since $\boldsymbol{A}$ is finite, $|B_i| = 1$ for all $i \in I \setminus \{k\}$. Conversely, if $|B_i| = 1$ for all $i \in I \setminus \{k\}$, then $|B_k| = |A|$, and hence the projection function π_k is an isomorphism between $\boldsymbol{A}$ and $\boldsymbol{B}_k$ by the pigeon-hole principle, because $\boldsymbol{A}$ is finite. So the conditions (i) and (ii) are equivalent.

By essentially the same argument, if $\boldsymbol{A} \cong \boldsymbol{B} \times \boldsymbol{C}$, then $\boldsymbol{B}$ is trivial iff $\boldsymbol{A} \cong \boldsymbol{C}$, and $\boldsymbol{C}$ is trivial iff $\boldsymbol{A} \cong \boldsymbol{B}$. So condition (iii) is equivalent to Thm 2.57(ii). □

Neither of the conditions (ii) or (iii) of the corollary is equivalen to direct indecomposability for arbitrary Σ-algebras. In particular, it follows from the remarks at the end of the chapter that every countably infinite left-trivial semigroup satisfies both (ii) and (iii), but none of these algebras is directly irreducible.

We prove in Thm. 2.61 below that every finite Σ-algebra is a direct product of directly indecomposable algebras. But it is shown in subsequent remarks that this is not the case for all infinite Σ-algebras.

For any class K of Σ-algebras define

$$\mathbf{P}(\mathsf{K}) := \{\, \boldsymbol{B} : \exists \langle\, \boldsymbol{A}_i : i \in I \,\rangle \in \mathsf{K}^I \left(\boldsymbol{B} \cong \prod_{i\in I} \boldsymbol{A}_i\right) \}.$$

We show that $\mathbf{P}$ is a closure operator on $\mathsf{Alg}(\Sigma)$. For each $\boldsymbol{A} \in \mathsf{K}$, $\boldsymbol{A} \cong \prod_{i\in I} \boldsymbol{A}_i$ where $I = \{0\}$ and $\boldsymbol{A}_0 = \boldsymbol{A}$. So $\mathsf{K} \subseteq \mathbf{P}(\mathsf{K})$. By the generalized associative law

$$\prod_{j\in J}\Big(\prod_{i\in I_j} \boldsymbol{A}_{ij}\Big) = \prod_{\langle i,j\rangle \in \bigcup_{j\in J}(I_j\times\{j\}} \boldsymbol{A}_{ij}.$$

So $\mathbf{P}\,\mathbf{P}(\mathsf{K}) = \mathbf{P}(\mathsf{K})$. Finally, it is obvious that $\mathsf{K} \subseteq \mathsf{L}$ implies $\mathbf{P}(\mathsf{K}) \subseteq \mathbf{P}(\mathsf{L})$. $\mathbf{P}$ is not algebraic (exercise).

Theorem 2.59. *Let* K *be any class of* Σ*-algebras.*

(i) $\mathbf{P}\,\mathbf{H}(\mathsf{K}) \subseteq \mathbf{H}\,\mathbf{P}(\mathsf{K})$.
(ii) $\mathbf{P}\,\mathbf{S}(\mathsf{K}) \subseteq \mathbf{S}\,\mathbf{P}(\mathsf{K})$.
(iii) $\mathbf{H}\,\mathbf{P}$, $\mathbf{S}\,\mathbf{P}$, *and* $\mathbf{H}\,\mathbf{S}\,\mathbf{P}$ *are closure operators on* $\mathsf{Alg}(\Sigma)$.

Proof. (i) Assume $\boldsymbol{A} \in \mathbf{P}\,\mathbf{H}(\mathsf{K})$. Then there is a $\langle\, \boldsymbol{B}_i : i \in I \,\rangle \in \mathbf{H}(\mathsf{K})^I$ such that $\boldsymbol{A} \cong \prod_{i\in I} \boldsymbol{B}_i$. Let $\langle\, \boldsymbol{C}_i : i \in I \,\rangle \in \mathsf{K}^I$ such that $\boldsymbol{C}_i \succcurlyeq \boldsymbol{B}_i$ for all $i \in I$. For each $i \in I$ let $h_i\colon \boldsymbol{C}_i \twoheadrightarrow \boldsymbol{B}_i$. Then $h_i \circ \pi_i\colon \prod_{i\in I} \boldsymbol{C}_i \twoheadrightarrow \boldsymbol{B}_i$ for each $i \in I$. By the Categorical Product Property there is a unique homomorphism $\bar{h}\colon \prod_{i\in I} \boldsymbol{C}_i \to \prod_{i\in I} \boldsymbol{B}_i$ such that $\pi_i \circ \bar{h} = h_i \circ \pi_i\colon \prod_{i\in I} \boldsymbol{C}_i \to \boldsymbol{B}_i$ for every $i \in I$. We denote $\bar{h}$ by $\prod_{i\in I} h_i$ and refer to it as the *natural map*.

Let $\vec{b} = \langle\, b_i : i \in I \,\rangle \in \prod_{i\in I} \boldsymbol{B}_i$. Choose $\vec{c} = \langle\, c_i : i \in I \,\rangle \in \prod_{i\in I} \boldsymbol{C}_i$ such that $h_i(c_i) = b_i$ for every $i \in I$. Then $\big(\prod_{i\in I} h_i\big)(\vec{c}) = \langle\, h_i(c_i)\colon i \in I \,\rangle = \vec{b}$. Hence $\prod_{i\in I} h_i$ is surjective and thus $\boldsymbol{A} \in \mathbf{I}\,\mathbf{H}\,\mathbf{P}(\mathsf{K}) = \mathbf{H}\,\mathbf{P}(\mathsf{K})$.

(ii) Assume $\boldsymbol{A} \in \mathbf{P}\,\mathbf{S}(\mathsf{K})$. There is a $\langle\, \boldsymbol{B}_i : i \in I \,\rangle \in \mathsf{K}^I$ and a $\langle\, \boldsymbol{C}_i : i \in I \,\rangle \in \mathbf{S}(\mathsf{K})^I$ such that, for every $i \in I$, $\boldsymbol{C}_i \subseteq \boldsymbol{B}_i$ and $\boldsymbol{A} \cong \prod_{i\in I} \boldsymbol{C}_i$. But $\prod_{i\in I} \boldsymbol{C}_i \subseteq \prod_{i\in I} \boldsymbol{B}_i$ (exercise). So $\boldsymbol{A} \in \mathbf{I}\,\mathbf{S}\,\mathbf{P}(\mathsf{K}) = \mathbf{S}\,\mathbf{P}(\mathsf{K})$.

(iii) For every $\mathsf{K} \subseteq \mathsf{Alg}(\Sigma)$, $\mathsf{K} \subseteq \mathbf{P}(\mathsf{K})$, which implies $\mathsf{K} \subseteq \mathbf{S}(\mathsf{K}) \subseteq \mathbf{S}\,\mathbf{P}(\mathsf{K})$, which in turn implies that $\mathsf{K} \subseteq \mathbf{H}(\mathsf{K}) \subseteq \mathbf{H}\,\mathbf{S}(\mathsf{K}) \subseteq \mathbf{H}\,\mathbf{S}\,\mathbf{P}(\mathsf{K})$. Thus

$$\begin{aligned}
\mathbf{H}\,\mathbf{S}\,\underline{\mathbf{P}\,\mathbf{H}}\,\mathbf{S}\,\mathbf{P}(\mathsf{K}) &\subseteq \mathbf{H}\,\mathbf{S}\,\underline{\mathbf{H}\,\mathbf{P}}\,\mathbf{S}\,\mathbf{P}(\mathsf{K}) \\
&= \mathbf{H}\,\underline{\mathbf{S}\,\mathbf{H}}\,\mathbf{P}\,\mathbf{S}\,\mathbf{P}(\mathsf{K}) \\
&\subseteq \mathbf{H}\,\underline{\mathbf{H}\,\mathbf{S}}\,\mathbf{P}\,\mathbf{S}\,\mathbf{P}(\mathsf{K}) \\
&= \mathbf{H}\,\mathbf{H}\,\mathbf{S}\,\underline{\mathbf{P}\,\mathbf{S}}\,\mathbf{P}(\mathsf{K}) \\
&= \mathbf{H}\,\mathbf{H}\,\mathbf{S}\,\underline{\mathbf{S}\,\mathbf{P}}\,\mathbf{P}(\mathsf{K}) \\
&= \mathbf{H}\,\mathbf{S}\,\mathbf{P}(\mathsf{K}).
\end{aligned}$$

So $\mathbf{HSPHSP}(\mathsf{K}) \subseteq \mathbf{HSP}(\mathsf{K})$; the inclusion in the opposite direction is immediate.
Clearly $\mathsf{K} \subseteq \mathsf{L}$ implies $\mathbf{HSP}(\mathsf{K}) \subseteq \mathbf{HSP}(\mathsf{K})$. □

Corollary 2.60. *Let* K *be any class of* Σ*-algebras. The following conditions are equivalent.*

(i) $\mathbf{H}(\mathsf{K}) \subseteq \mathsf{K}$, $\mathbf{S}(\mathsf{K}) \subseteq \mathsf{K}$, $\mathbf{P}(\mathsf{K}) \subseteq \mathsf{K}$, *i.e.,* K *is closed under the formation of homomorphic images, subalgebras, and isomorphic images of direct products.*

(ii) $\mathbf{HSP}(\mathsf{K}) = \mathsf{K}$.

Proof. (i) $\Longrightarrow$ (ii). $\mathbf{HSP}(\mathsf{K}) \subseteq \mathbf{HS}(\mathsf{K}) \subseteq \mathbf{H}(\mathsf{K}) \subseteq \mathsf{K}$; $\mathsf{K} \subseteq \mathbf{HSP}(\mathsf{K})$ always holds.

(ii) $\Longrightarrow$ (i). $\mathbf{H}(\mathsf{K}) = \mathbf{HHSP}(\mathsf{K}) = \mathbf{HSP}(\mathsf{K}) = \mathsf{K}$. $\mathbf{S}(\mathsf{K}) = \mathbf{SHSP}(\mathsf{K}) \subseteq \mathbf{HSSP}(\mathsf{K}) = \mathbf{HSP}(\mathsf{K}) = \mathsf{K}$. $\mathbf{P}(\mathsf{K}) = \mathbf{PHSP}(\mathsf{K}) \subseteq \mathbf{HPSP}(\mathsf{K}) \subseteq \mathbf{HSPP}(\mathsf{K}) = \mathbf{HSP}(\mathsf{K}) = \mathsf{K}$. □

2.9. **Subdirect products.** We give two standard homomorphism constructions involving direct products that are used often in the sequel.

(I) Let $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ and $\langle\, \boldsymbol{B}_i : i \in I \,\rangle$ be I-indexed systems of Σ-algebras. Let $\vec{h} = \langle\, h_i : i \in I \,\rangle \in \prod_{i\in I} \mathrm{Hom}(\boldsymbol{A}_i, \boldsymbol{B}_i)$. We denote by $\prod_{i\in I} h_i$ or simply by $\prod \vec{h}$ the homomorphism from $\prod_{i\in I} \boldsymbol{A}_i$ into $\prod_{i\in I} \boldsymbol{B}_i$ such that, for every $\langle\, a_i : i \in I \,\rangle \in \prod_{i\in I} A_i$,

$$\big(\prod_{i\in I} h_i\big)(\langle\, a_i : i \in I \,\rangle) = \langle\, h_i(a_i) : i \in I \,\rangle.$$

That $\prod \vec{h}$ is a homomorphism is an immediate consequence of the categorical product property, but it can also be easily verified directly. $\prod \vec{h}$ is called the *product* of the system $\vec{h}$. It is easily checked that $\prod \vec{h}$ is an epimorphism, a monomorphism, or an isomorphism if, for each $i \in I$, h_i has the respective property.

(II) Let $\boldsymbol{A}$ be a Σ-algebra and let $\vec{\alpha} = \langle\, \alpha_i : i \in I \,\rangle \in \mathrm{Co}(\boldsymbol{A})^I$. We denote by $\Delta_{\vec{\alpha}}$ the homomorphism from $\boldsymbol{A}$ to $\prod_{i\in I} \boldsymbol{A}/\alpha_i$ such that, for every $a \in A$,

$$\Delta_{\vec{\alpha}}(a) = \langle\, a/\alpha_i : i \in I \,\rangle.$$

As in the case of a product of a system of homomorphisms, that $\Delta_{\vec{\alpha}}$ is a homomorphism can be obtained from the categorical product property or verified directly. $\Delta_{\vec{\alpha}}$ is called the *natural map* from $\boldsymbol{A}$ into $\prod_{i\in I} \boldsymbol{A}/\alpha_i$.

Definition 2.61 (Subdirect Product)**.** Let $\langle\, \boldsymbol{B}_i : i \in I \,\rangle$ be a system of Σ-algebras. A subalgebra $\boldsymbol{A}$ of $\prod_{i\in I} \boldsymbol{B}_i$ is called a *subdirect product* of the system $\langle\, \boldsymbol{B}_i : i \in I \,\rangle$, in symbols $\boldsymbol{A} \subseteq_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$, if the projection of $\boldsymbol{A}$ onto each of the components $\boldsymbol{B}_i$ is surjective, i.e., for all $i \in I$, $\pi_i(A) = B_i$.

If all of the components $\boldsymbol{B}_i$ of $\langle\, B_i : i \in I \,\rangle$ are the same algebra, say $\boldsymbol{B}$, then $\boldsymbol{A}$ is called a *subdirect power* of $\boldsymbol{B}$ and we write $\boldsymbol{A} \subseteq_{\mathrm{SD}} \boldsymbol{B}^I$.

It is helpful to note that $\boldsymbol{A} \subseteq_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$ iff for every $i \in I$ and every $b \in B_i$, b appears as the i-th component of at least one element of $\boldsymbol{A}$.

The direct product itself $\prod_{i\in I} \boldsymbol{B}_i$ is obviously a subdirect product of $\langle\, \boldsymbol{B}_i : i \in I \,\rangle$, and is the largest one. Given any algebra $\boldsymbol{B}$ and any index set I, let D be the set of all constant functions from I into B, i.e., $D = \{\, \langle b, b, \ldots, b\rangle : b \in B \,\}$. Note that

$$\begin{aligned}\sigma^{\boldsymbol{B}^I}\big(\langle b_1, b_1, \ldots, b_n\rangle, \ldots, \langle b_n, b_n, \ldots, b_n\rangle\big)\\ = \langle \sigma^{\boldsymbol{B}}(b_1, b_2, \ldots, b_n), \sigma^{\boldsymbol{B}}(b_1, b_2, \ldots, b_n), \ldots, \sigma^{\boldsymbol{B}}(b_1, b_2, \ldots, b_n)\big).\end{aligned}$$

So D is a nonempty subuniverse of $\boldsymbol{B}^I$. Clearly for every $i \in I$ and every $b \in B$, b is the i-component of some (in this case unique) element of D. So $\boldsymbol{D}$, the subalgebra of $\boldsymbol{B}^I$ with universe D, is a subdirect power of $\boldsymbol{B}$. $\boldsymbol{D}$ is called the *I-th diagonal subdirect power* of $\boldsymbol{B}$ for obvious reasons; it is isomorphic to $\boldsymbol{B}$. In general it is not the smallest I-th subdirect power of $\boldsymbol{B}$. To show this we apply the following lemma, which often proves useful in verifying subdirect products.

Lemma 2.62. *Let $\langle\, \boldsymbol{B}_i : i \in I \,\rangle$ be a system of Σ-algebras, and let $X \subseteq \prod_{i\in I} B_i$. Let $\boldsymbol{A} = \mathbf{Sg}^{\prod \boldsymbol{B}_i}(X)$, the subalgebra of $\prod_{i\in I} \boldsymbol{B}_i$ generated by X. Then $\boldsymbol{A}$ is a subdirect product of $\langle\, \boldsymbol{B}_i : i \in I \,\rangle$ iff, for each $i \in I$, $B_i = \mathrm{Sg}^{\boldsymbol{B}_i}\big(\pi_i(X)\big)$.*

Proof. By Thm 2.14(iii) $\pi_i\big(\mathrm{Sg}^{\prod \boldsymbol{B}_i}(X)\big) = \mathrm{Sg}^{\boldsymbol{B}}\big(\sigma_i(X)\big)$, for each $i \in I$. □

Let $\langle 1, 3\rangle \in \mathbb{Z}_8 \times \mathbb{Z}_8$. Since $\mathbf{Z}_8$ is generated by both 1 and 3, the cyclic subgroup of $\mathbf{Z}_8 \times \mathbf{Z}_8$ is a subdirect power of $\mathbf{Z}_8$ by the lemma. But it clearly does not include the diagonal subdirect power.

Definition 2.63 (Subdirect Irreducibility)**.** A Σ-algebra $\boldsymbol{A}$ is *subdirectly irreducible* (SI) if, for every system $\langle\, \boldsymbol{B}_i : i \in I \,\rangle$ of Σ-algebras, $\boldsymbol{A} \cong \mathbf{;} \subseteq_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$ implies $\boldsymbol{A} \cong \boldsymbol{B}_i$ for some $i \in I$.

Our goal is to prove the so-called Birkhoff subdirect product theorem that says that every Σ-algebra is a subdirect product of a system of subdirectly irreducible algebras. This is one of the major results in the early development of universal algebra. For this purpose it is useful to consider a characterization of subdirect irreducibility that explicitly involves the monomorphism that gives the subirect embedding. We begin with some preliminary definitions.

A monomorphism $h\colon \boldsymbol{A} \rightarrowtail \boldsymbol{B}$, i.e., an injective homomorphism, is also called an *embedding* of $\boldsymbol{A}$ in $\boldsymbol{B}$. Note that h is an embedding iff

$$\boldsymbol{A} \overset{h}{\cong} h(\boldsymbol{A}) \subseteq \boldsymbol{B}.$$

A homomorphism $h\colon \boldsymbol{A} \to \prod_{i\in I} \boldsymbol{B}_i$ is said to be *subdirect* if, for every $i \in I$, $\pi_i\big(h(\boldsymbol{A})\big) = \boldsymbol{B}_i$, i.e., the homomorphism $\pi_i \circ h\colon \boldsymbol{A} \to \boldsymbol{B}_i$ is surjective. Note that h is subdirect iff

$$\boldsymbol{A} \overset{h}{\twoheadrightarrow} h(\boldsymbol{A}) \subseteq_{\mathrm{SD}} \boldsymbol{B}.$$

Finally, a homomorphism $h\colon \boldsymbol{A} \to \prod_{i\in I} \boldsymbol{B}_i$ is a *subdirect embedding* if it is both an embedding and subdirect, i.e.,

$$\boldsymbol{A} \overset{h}{\cong} h(\boldsymbol{A}) \subseteq_{\mathrm{SD}} \boldsymbol{B}.$$

In this case we write $h\colon \boldsymbol{A} \rightarrowtail_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$. Clearly, $\boldsymbol{A} \cong \mathbf{;} \subseteq_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$ iff there exists a subdirect embedding $h\colon \boldsymbol{A} \rightarrowtail_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$.

Lemma 2.64. *Let $h\colon \boldsymbol{A} \to \prod_{i\in I} \boldsymbol{B}_i$ be an arbitrary homomorphism. Then* $\mathrm{rker}(h) = \bigcap_{i\in I} \mathrm{rker}(\pi_i \circ h)$.

Proof.

$$\begin{aligned}
\langle b, b'\rangle \in \bigcap_{i\in I} \mathrm{rker}(\pi_i \circ h) &\Leftrightarrow \forall i \in I\big(\langle b, b'\rangle \in \mathrm{rker}(\pi_i \circ h)\big)\\
&\Leftrightarrow \forall i \in I\big(h(b)(i) = h(b')(i)\big)\\
&\Leftrightarrow h(b) = h(b')\\
&\Leftrightarrow \langle b, b'\rangle \in \mathrm{rker}(h).
\end{aligned}$$

□

Corollary 2.65. (i) *A homomorphism $h\colon \boldsymbol{A} \to \prod_{i\in I} \boldsymbol{B}_i$ is is an embedding iff $\bigcap_{i\in I} \mathrm{rker}(\pi_i \circ h) = \Delta_A$.*

(ii) *For every $\vec{\alpha} = \langle\, \alpha_i : i \in I \,\rangle \in \mathrm{Co}(\boldsymbol{A})$, the natural map $\Delta_{\vec{\alpha}}\colon \boldsymbol{A} \to \prod_{i\in I} \boldsymbol{A}/\alpha_i$ is a subdirect embedding iff $\bigcap_{i\in I} \alpha_i = \Delta_A$.*

Proof. (i). By definition of relation kernel we have that h is an embedding iff $\mathrm{rker}(h) = \Delta_A$.

(ii). We first note that the natural map $\Delta_{\vec{\alpha}}$ of a system of congruences $\vec{\alpha}$ is always subdirect because $\pi_i \circ \Delta_{\vec{\alpha}} = \Delta_{\alpha_i}$, and the natural map Δ_{α_i} is always surjective. Thus $\Delta_{\vec{\alpha}}$ is a subdirect embedding iff it is an embedding, which by the lemma is true iff $\bigcap_{i\in I} \alpha_i = \Delta_A$ since $\mathrm{rker}(\pi_i \circ \Delta_{\vec{\alpha}}) = \alpha_i$ for each $i \in I$. □

In the next theorem we characterize in terms of congruences the systems of algebras in which a given algebra can be subdirectly embeddable. Notice that the characterization differs from the corresponding characterization of those systems for which the given algebra is isomorphic to the direct product only in the absence of the Chinese remainder property.

Theorem 2.66. *Let $\boldsymbol{A}$ be a Σ-algebra and let $\langle\, \boldsymbol{B}_i : i \in I \,\rangle$ be a system of Σ-algebras. Then $\boldsymbol{A} \cong \mathbf{;} \subseteq_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$ iff there exists a system $\vec{\alpha} = \langle\, \alpha_i : i \in I \,\rangle \in \mathrm{Co}(\boldsymbol{A})^I$ such that*

(i) $\bigcap_{i\in I} \alpha_i = \Delta_A$, *and*

(ii) *for every $i \in I$, $\boldsymbol{A}/\alpha_i \cong \boldsymbol{B}_i$.*

Proof. $\Longleftarrow$. Assume (i) and (ii) hold. By (i) and Cor. 2.65(ii), there is a subdirect embedding $\vec{\alpha}\colon \boldsymbol{A} \rightarrowtail_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$. Let $\vec{h} = \langle\, h_i : i \in I \,\rangle \in \prod_{i\in I} \mathrm{Iso}(\boldsymbol{A}/\alpha_i, \boldsymbol{B}_i)$. Then $\boldsymbol{A} \overset{\Delta_{\vec{\alpha}}}{\rightarrowtail}_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i \overset{\prod \vec{h}}{\cong} \prod_{i\in I} \boldsymbol{B}_i$. Thus $\left(\prod \vec{h}\right) \circ \Delta_{\vec{\alpha}}\colon \boldsymbol{A} \rightarrowtail_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$.

$\Longrightarrow$. Suppose $\boldsymbol{A} \cong \mathbf{;} \subseteq_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$. Let h be a subdirect embedding. Let $\alpha_i = \mathrm{rker}(\pi_i \circ h)$ for each $i \in I$. Then $\bigcap_{i\in I} \alpha_i = \Delta_A$ by Cor. 2.65(i). Since h is subdirect, for each $i \in I$, $\pi_i \circ h\colon \boldsymbol{A} \twoheadrightarrow \boldsymbol{B}_i$ and hence $\boldsymbol{A}/\alpha_i \cong \boldsymbol{B}_i$ by the First Isomorphism Theorem. □

Definition 2.67. A Σ-algebra is *subdirectly embedding irreducible* (SDEI) if, for every subdirect embedding $h \rightarrowtail_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$, there is an $i \in I$ such that $\alpha_i\colon h\colon \boldsymbol{A} \cong \boldsymbol{B}_i$.

Subdirect embedding irreducibility trivially implies subdirect irreducibility. For suppose $\boldsymbol{A}$ is SDEI and $\boldsymbol{A} \cong \mathbf{;} \subseteq_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$. Let $h\colon \boldsymbol{A} \rightarrowtail_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{B}_i$ be a subdirect embedding. Then $\alpha_i \circ h\colon \boldsymbol{A} \cong \boldsymbol{B}_i$ for some i; in particular $\boldsymbol{A} \cong \boldsymbol{B}_i$. So $\boldsymbol{A}$ is SDI.

Theorem 2.68. *An algebra $\boldsymbol{A}$ is* SDEI *iff for every $\vec{\alpha} = \langle\, \alpha_i : i \in I \,\rangle \in \mathrm{Co}(\boldsymbol{A})^I$, we have $\bigcap_{i\in I} \alpha_i = \Delta_A$ only if there is an $i \in I$ such that $\alpha_i = \Delta_A$.*

Proof. $\Longrightarrow$. Suppose $\bigcap_{i\in I} \alpha_i = \Delta_A$. Then by Cor. 2.65(ii), $\Delta_{\vec{\alpha}}\colon \boldsymbol{A} \rightarrowtail_{\mathrm{SD}} \prod_{i\in I} \boldsymbol{A}/\alpha_i$. So there exists an i such that $\pi_i \circ \Delta_{\vec{\alpha}}\colon \boldsymbol{A} \cong \boldsymbol{A}/\alpha_i$. But $\pi_i \circ \Delta_{\vec{\alpha}} = \Delta_A$. So $\alpha_i = \Delta_A$.

$\Longleftarrow$. Let $h\colon \boldsymbol{A} \rightarrowtail_{\mathrm{SD}} \boldsymbol{B}Ii$ be a subdirect embedding. For each $i \in I$ let $\alpha_i = \mathrm{rker}(\pi_i\colon h)$. We have $\bigcap_{i\in I} \alpha_i \Delta_A$ by Cor.2.65(i) because h is an embedding. So, for some i, $\alpha_i = \Delta_A$. Thus $\pi_i \circ h\colon \boldsymbol{A} \cong \boldsymbol{B}_i$. □

Corollary 2.69. *A Σ-algebra $\boldsymbol{A}$ is a SDEI iff the set $\mathrm{Co}(\boldsymbol{A}) \setminus \{\Delta_A\}$ of congruences of $\boldsymbol{A}$ strictly larger than Δ_A has a smallest element μ, i.e., $\Delta_A \subset \mu$ and, for every $\alpha \in \mathrm{Co}(\boldsymbol{A})$ such that $\Delta_A \subset \alpha$, we have $\mu \subseteq \alpha$. A graphical representation of the lattice $\mathbf{Co}(\boldsymbol{A})$ of congruences of $\boldsymbol{A}$ is given in Figure* 19. *μ is called the* ***monolith*** *of $\boldsymbol{A}$.*

Proof. $\Longrightarrow$. $\bigcap\{\, \alpha \in \mathrm{Co}(\boldsymbol{A}) \setminus \{\Delta_A\} \,\} \neq \Delta_A$ since $\boldsymbol{A}$ is SDEI. This is the monolith μ of $\boldsymbol{A}$.

$\Longleftarrow$. Suppose $\langle\, \alpha_i : i \in I \,\rangle \in \mathrm{Co}(\boldsymbol{A})^I$ and, for each $i \in I$, $\alpha_i \neq \Delta_A$. Then, for every $i \in I$, $\mu \subseteq \alpha_i$. Hence $\Delta_A \subset \mu \subseteq \bigcap_{i\in I} \alpha_i$. □

Using the Correspondence Theorem we can relativize this result to obtain a useful characterization of the quotients of an algebra that are SDEI.

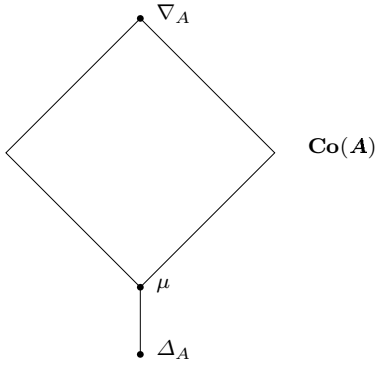


FIGURE 19

Corollary 2.70. *Let $\boldsymbol{A}$ be a Σ-algebra and let $\alpha \in \mathrm{Co}(\boldsymbol{A})$. Then the quotient $\boldsymbol{A}/\alpha$ is* SDEI *iff the set $\{\, \beta \in \mathrm{Co}(\boldsymbol{A}) : \alpha \subset \beta \,\} = \mathrm{Co}(\boldsymbol{A})[\alpha] \setminus \{\alpha\}$ of all congruences of $\boldsymbol{A}$ strictly including α has a smallest element μ_α, i.e., $\alpha \subset \mu_\alpha$ and, for every $\beta \in \mathrm{Co}(\boldsymbol{A})$ such that $\alpha \subset \beta$ we have $\mu_\alpha \subseteq \beta$. A graphical representation of the principal filter of $\mathbf{Co}(\boldsymbol{A})$ generated by α is given in the left-hand side of Figure* 20*.*

Proof. By the Correspondence Theorem, Thm. 2.26, the map $\beta \mapsto \beta/\alpha$ is an isomorphism between the lattices $\mathbf{Co}(\boldsymbol{A})[\alpha]$ and $\mathbf{Co}(\boldsymbol{A}/\alpha)$. See Figure 20

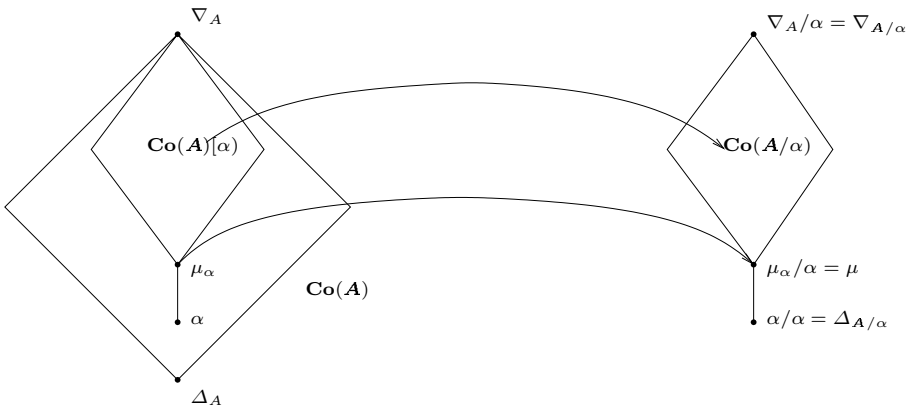


FIGURE 20

If $\boldsymbol{A}/\alpha$ is SDEI, then $\boldsymbol{A}/\alpha$ has a monolith μ. Let μ_α be the unique congruence in $\mathrm{Co}(\boldsymbol{A})[\alpha]$ such that $\mu_\alpha/\alpha = \mu$. Then μ_α is the smallest element of $\mathrm{Co}(\boldsymbol{A})[\alpha] \setminus \{\alpha\}$. Conversely, if μ_α is the smallest element of $\mathrm{Co}(\boldsymbol{A})[\alpha] \setminus \{\alpha\}$, then μ_α/α is the monolith of $\boldsymbol{A}/\alpha$ and hence $\boldsymbol{A}/\alpha$ is SDEI. □

Let $\boldsymbol{L}$ be a complete lattice. An element $a \in A$ is *strictly meet irreducible* (SMI) if, for every $X \subseteq L$, we have that $a = \bigwedge X$ only if $a = x$ for some $x \in X$ Clearly a is SMI iff $a < \bigwedge\{\, x \in L : a < x \,\}$. $\boldsymbol{A}$ is SDEI iff Δ_A is SMI in the lattice $\mathbf{Co}(\boldsymbol{A})$; more generally, for every $\alpha \in \mathrm{Co}(\boldsymbol{A})$, $\boldsymbol{A}/\alpha$ is SDEI iff α is SMI.

Theorem 2.71 (Birkhoff Sudirect Product Theorem)**.** *Every nontrivial Σ-algebra is isomorphic to a subdirect product of* SDEI *algebras.*

Proof. For all distinct $a, b \in A$ let $K(a,b) = \{\, \alpha \in \mathrm{Co}(\boldsymbol{A}) : \langle a,b\rangle \notin \alpha \,\}$. $K(a,b) \neq \emptyset$ since it contains Δ_A. Let $C \subseteq K(a,b)$ be a chain, i.e., a set of congruences in $K(a,b)$ linearly ordered under inclusion. Then $\langle a,b\rangle \notin \bigcup C \in \mathrm{Co}(\boldsymbol{A})$. So $\bigcup C \in K(a,b)$. By Zorn's lemma $K(a,b)$ has a maximal element $\alpha(a,b)$ (it is not in general unique). The claim is that $\alpha(a,b)$ is strictly meet irreducible. For each $\beta \in \mathrm{Co}(\boldsymbol{A})$ such that $\alpha(a,b) \subset \beta$ we have $\langle a,b\rangle \in \beta$ by the maximality of $\alpha(a,b)$. So $\langle a,b\rangle \in \bigcap\{\, \beta \in \mathrm{Co}(\boldsymbol{A}) : \alpha(a,b) \subset \beta \,\}$. Thus $\alpha(a,b) \subset \bigcap\{\, \beta \in \mathrm{Co}(\boldsymbol{A}) : \alpha(a,b) \subset \beta \,\}$. So $\alpha(a,b)$ is SMI and hence $\boldsymbol{A}/\alpha(a,b)$ is SDEI for all $\langle a,b\rangle \in A^2 \setminus \Delta_A$ by Cor. 2.70. Moreover, $\bigcap\{\, \alpha(a,b) : \langle a,b\rangle \in A^2 \setminus \Delta_A \,\} = \Delta_A$. So by Thm. 2.65(ii),

$$\boldsymbol{A} \cong \mathbf{;} \subseteq_{\mathrm{SD}} \prod_{\langle a,b\rangle \in A^2 \setminus \Delta_A} \boldsymbol{A}/\alpha(a,b).$$

□

Corollary 2.72. *Let $\boldsymbol{A}$ be a nontrivial Σ-algebra. Then $\boldsymbol{A}$ is subdirectly irreducible* (SDI) *iff $\boldsymbol{A}$ is subdirectly embedding irreducible* (SDEI)*.*

Proof. We have already observed that SDEI implies SDI trivially. For the implication in the other direction suppose $\boldsymbol{A}$ is SDI. By the Birkhoff Subdirect Product Theorem $\boldsymbol{A} \cong \mathbf{;} \subseteq_{\text{SD}} \prod_{i\in I} \boldsymbol{B}_i$ with $\boldsymbol{B}_i$ SDEI for every $i \in I$. Since $\boldsymbol{A}$ is SDI, there is an $i \in I$ such that $\boldsymbol{A} \cong \boldsymbol{B}_i$. Hence $\boldsymbol{A}$ is SDEI and thus SDI. □

As an application of the Birkhoff Subdirect Product Theorem we that every distributive lattice is isomorphic to a lattice of sets. Recall that a *bounded* lattice has the form $\langle L, \wedge, \vee, 0, 1\rangle$ where 0 and 1 are the smallest and largest elements of L, respectively.

Theorem 2.73. *The only* SDI *distributive lattice is the* 2*-element lattice $\boldsymbol{D}_2$.*

Proof. Let $\boldsymbol{L}$ be a bounded distributive lattice, and let $\mathrm{Co}(\boldsymbol{L})^+ = \mathrm{Co}(\boldsymbol{L}) \setminus \{\Delta_L\}$, the set of congruences of $\boldsymbol{A}$ strictly larger than Δ_L. If $\boldsymbol{L} \cong \boldsymbol{D}_2$, then $\mathrm{Co}(\boldsymbol{A}) = \{\Delta_L, \nabla_L\}$ and $\boldsymbol{L}$ is SDI with monolith ∇_L. We assume now that $|L| > 2$ and show that $\boldsymbol{L}$ fails to be SDI by showing

$$\bigcap \mathrm{Co}(\boldsymbol{L})^+ = \Delta_A. \tag{26}$$

For each $a \in L$ we define binary relations $\equiv_a^\vee, \equiv_a^\wedge \subseteq A^2$ as follows. For all $x, y \in L$,

$$x \equiv_a^\vee y \text{ if } x \vee a = y \vee a \quad \text{and} \quad x \equiv_a^\wedge y \text{ if } x \wedge a = y \wedge a.$$

We claim that $\equiv_a^\vee$ and $\equiv_a^\wedge$ are both congruences of $\boldsymbol{L}$. The best way to see this is to show they are relation kernels of homomorphisms.

Define $h_a^\vee \colon L \to L$ by setting $h_a^\vee(x) = x \vee a$. $h_a^\vee(x \vee y) = (x \vee y) \vee a = (x \vee a) \vee (y \vee a) = h_a^\vee(x) \vee h_a^\vee(y)$ and $h_a^\vee(x \wedge y) = (x \wedge y) \vee a = (x \vee a) \wedge (y \vee a) = h_a^\vee(x) \wedge h_a^\vee(y)$. So $h_a^\vee \in \mathrm{End}(\boldsymbol{L}, \boldsymbol{L})$, and hence $\equiv_a^\vee = \mathrm{rker}(h_a^\vee) \in \mathrm{Co}(\boldsymbol{L})$. $\equiv_a^\wedge \in \mathrm{Co}(\boldsymbol{L})$ by duality.

Note that $x \leq a$ iff $x \vee a = a = a \vee a$ iff $x \equiv_a^\vee a$. So $0/\equiv_a^\vee (= a/\equiv_a^\vee) = L(a]$, the principal ideal of $\boldsymbol{L}$ generated by a, and dually $1/\equiv_a^\wedge = L[a)$, the principal filter generated by a. In particular, this gives us that

$$0 < a \text{ implies } \equiv_a^\vee \in \mathrm{Co}(\boldsymbol{L})^+ \quad \text{and} \quad a < 1 \text{ implies } \equiv_a^\wedge \in \mathrm{Co}(\boldsymbol{L})^+.$$

Suppose there exist nonzero a and b in $\boldsymbol{L}$ such that $a \wedge b = 0$. Then $\equiv_a^\vee, \equiv_b^\vee \in \mathrm{Co}(\boldsymbol{L})^+$. If $\langle x, y\rangle \in \equiv_a^\vee \cap \equiv_b^\vee$, then $x \vee a = y \vee a$ and $x \vee b = y \vee b$. So $(x \vee a) \wedge (x \vee b) = (y \vee a) \wedge (y \vee b)$. But by distributivity, $(x \vee a) \wedge (x \vee b) = (x \wedge x) \vee (a \wedge x) \vee (x \wedge b) \vee (a \wedge b) = x$ since $a \wedge b = 0$. Similarly, $(y \vee a) \wedge (y \vee b) = y$. So $\langle x, y\rangle \in \equiv_a^\vee \cap \equiv_b^\vee$ implies $x = y$, i.e., $\bigcap \mathrm{Co}(\boldsymbol{L})^+ \subseteq \equiv_a^\vee \cap \equiv_b^\vee = \Delta_L$.

So in the case $\boldsymbol{L}$ contains nonzero a, b such that $a \wedge b = 0$ we conclude that $\boldsymbol{L}$ is not SDI. So we now assume that $a \wedge b \neq 0$ for all nonzero a and b. Then for all such a, b we have $\equiv_{a\wedge b}^\vee \in \mathrm{Co}(\boldsymbol{L})^+$. But $a = a \vee (a \wedge b)$ and $b = b \vee (a \wedge b)$ by absorption. So, if $a \neq b$ and both are different from 0 we have $\langle a, b\rangle \notin \equiv_{a\wedge b}^\vee$ and hence $\langle a, b\rangle \notin \bigcap \mathrm{Co}(\boldsymbol{A})^+$. By duality, the same is true if $a \neq b$ and both are different from 1. It remains only to consider the case $a = 0$ and $b = 1$. Since $\boldsymbol{L} \neq \boldsymbol{D}_2$, there is a $c \in L$ such that $0 < c < 1$. $\langle 0, 1\rangle \notin \equiv_c^\vee \in \mathrm{Co}(\boldsymbol{L})^+$. Thus (26) holds and $\boldsymbol{L}$ is not SDI. □

Theorem 2.74 (Birkhoff Representation Theorem)**.** *Every distributive lattice is isomorphic to a lattice of sets. More precisely, for every distributive lattice $\boldsymbol{L}$ there exists a set I and an embedding $h \colon \boldsymbol{L} \rightarrowtail \langle \boldsymbol{\mathcal{P}}(I), \cup, \cap\rangle$.*

Proof. Without loss of generality we can assume $\boldsymbol{L}$ is bounded. For if not, then we can adjoin new elements 0 and 1 to $\boldsymbol{L}$ and set $0 < x$ for every $x \in L \cup \{1\}$ and $x < 1$ for every $x \in L \cup \{0\}$. It is easily checked that the extended po-set obtained this way is a bounded distributive lattice $\boldsymbol{L}'$ and that $\boldsymbol{L}$ is a sublattice (strictly speaking, a sublattice of the $\{\wedge, \vee\}$-reduct of $\boldsymbol{L}'$). Any embedding of $\boldsymbol{L}'$ into a lattice of sets restricts to an embedding of $\boldsymbol{L}$ into the same lattice of sets.

By the Birkhoff Sudirect Product Theorem and Thm 2.73 there is a set I such that $\boldsymbol{L} \cong \mathbf{;} \subseteq_{\text{SD}} \boldsymbol{D}_2^I$. Let $g\colon \boldsymbol{L} \rightarrowtail_{\text{SD}} \boldsymbol{D}_2^I$ be a subdirect embedding. Define $h\colon L \rightarrowtail \boldsymbol{\mathcal{P}}(I)$ by $h(a) = \{\, i \in I : g(a)(i) = 1 \,\}$. Note that $g(a)\colon I \to \{0,1\}$ is the characteristic function of $h(a)$. For all $a, b \in L$ we have

$$\begin{aligned} a \neq b \quad &\iff g(a) \neq g(b) \\ &\iff \quad \exists i \in I\big(g(a)(i) \neq g(b)(i)\big) \\ &\iff \quad \exists i \in I\big(i \in h(a) \setminus h(b) \text{ or } i \in h(b) \setminus h(a)\big) \\ &\iff \quad h(a) \neq h(b) \end{aligned}$$

So h is injective. We now check that it is a homomorphism from $\boldsymbol{L}$ into $\langle \boldsymbol{\mathcal{P}}(I), \cup, \cap, \emptyset, I\rangle$. For every $i \in I$ we have

$$\begin{aligned} i \in h(a \vee b) \quad &\iff \quad g(a \vee^{\boldsymbol{L}} b)(i) = 1 \\ &\iff \quad \big(g(a) \vee^{\boldsymbol{D}_2^I} g(b)\big)(i) = 1 \\ &\iff \quad \big(g(a)(i) \vee^{\boldsymbol{D}_2} g(b)(i) = 1 \\ &\iff \quad g(a)(i) = 1 \text{ or } g(b)(i) = 1 \\ &\iff \quad i \in h(a) \cup h(b). \end{aligned}$$

So $h(a \vee b) = h(a) \cup h(b)$. The equality $h(a \wedge b) = h(a) \cap h(b)$ is verified in a similar way. $g(0)$ and $g(1)$ are respectively the characteristic functions of $\emptyset$ and I. So h is a homomorphism. □

Exercise: Let $\boldsymbol{A}$ be a finitely generated Abelian group. Then $\boldsymbol{A}$ is SDI iff $\boldsymbol{A} \cong \boldsymbol{\mathbb{Z}}_{p^n}$ for some prime p and some $n \in \omega \setminus \{0\}$. Hint: Use the Fundamental Theorem of Abelian Groups.

Note that by the Fundamental Theorem of Abelian Groups the Birkhoff Subdirect Product Theorem holds in a much stronger form when restricted to finitely generated Abelian groups: every such algebra is isomorphic to a direct product (not just a subdirect product) of subdirectly irreducible algebras.

Every simple algebra is SDI but not conversely, and every SDI algebra is directly indecomposable (DI) but not conversely. The analog of the Birkhoff Subdirect Product Theorem does not hold for direct products. However we do have the following partial result.

Theorem 2.75. *If $\boldsymbol{A}$ is a finite Σ-algebra, then there exist* DI *Σ-algebras $\boldsymbol{B}_1, \ldots, \boldsymbol{B}_n$ such that $\boldsymbol{A} \cong \boldsymbol{B}_1 \times \cdots \times \boldsymbol{B}_n$.*

Proof. The proof is by induction on $|A|$. If $\boldsymbol{A}$ itself is DI then we are done. Otherwise $\boldsymbol{A} \cong \boldsymbol{A}' \times \boldsymbol{A}''$ with $1 < |A'|, |A''| < |A|$. By the induction hypothesis $\boldsymbol{A}' \cong \boldsymbol{B}'_1 \times \boldsymbol{B}'_{n'}$ and $\boldsymbol{A}'' \cong \boldsymbol{B}''_1 \times \boldsymbol{B}''_{n''}$ with $\boldsymbol{B}'_1, \ldots, \boldsymbol{B}'_{n'}, \boldsymbol{B}''_1, \ldots, \boldsymbol{B}''_{n''}$ DI. Then $\boldsymbol{A} \cong \boldsymbol{B}'_1 \times \cdots \times \boldsymbol{B}'_{n'} \times \boldsymbol{B}''_1 \times \cdots \times \boldsymbol{B}''_{n''}$. □

Every direct factor of a group $\boldsymbol{G}$ must also be a group because it is a homomorphic image of $\boldsymbol{G}$ and the group identities are clearly preserved under homomorphism. (In the next chapter we will systematically study the preservation of identities.) Every finite group has the *unique direct decomposition property*, i.e., if $\boldsymbol{G}$ is finite, and $\boldsymbol{G} \cong \boldsymbol{A}_1 \times \cdots \times \boldsymbol{A}_n$ and $\boldsymbol{G} \cong \boldsymbol{B}_1 \times \cdots \times \boldsymbol{B}_m$ with $\boldsymbol{A}_1, \ldots, \boldsymbol{A}_n, \boldsymbol{B}_1, \ldots, \boldsymbol{B}_m$ DI, then $n = m$ and, after reordering the $\boldsymbol{B}_i$ if necessary, we have $\boldsymbol{A}_1 \cong \boldsymbol{B}_1, \ldots, \boldsymbol{A}_n \cong \boldsymbol{B}_n$. This is the well know *Krull-Schmidt Theorem* of group theory.

In general however finite algebras do not have the unique direct decomposition property. For example, consider the following two mono-unary algebras $\boldsymbol{A}$ and $\boldsymbol{B}$ over the same universe $\{0, 1\}$ such that $f^{\boldsymbol{A}}(0) = 1, f^{\boldsymbol{A}}(1) = 0$ and $f^{\boldsymbol{B}}(0) = 0, f^{\boldsymbol{B}}(1) = 1$.

Exercise. Show that $\boldsymbol{A} \times \boldsymbol{B} \cong \boldsymbol{A}^2$ but $\boldsymbol{A} \ncong \boldsymbol{B}$.

We now show that there exist infinite algebras that are not isomorphic to any product, finite or infinite, of SD algebras.

Recall that a groupoid $\boldsymbol{A} = \langle A, \cdot \rangle$ is a *left-trivial semigroup* if it satisfies the identity $x \cdot y \approx x$. Any two left-trivial semigroups $\boldsymbol{A}$ and $\boldsymbol{B}$ of the same cardinality are isomorphic. Indeed any bijection $h\colon A \xrightarrow{\sim} B$ is a homomorphism and hence an isomorphism, for $h(a \cdot b) = h(a) = h(a) \cdot h(b)$.

We claim that a left-trivial semigroup $\boldsymbol{A}$ is DI iff it is finite and $|A|$ is a prime. The implication from left to right is obvious. For the implication in the opposite direction, suppose first of all that $\boldsymbol{A}$ is finite and composite, say $|A| = n \cdot m$ with $1 < n, m < |A|$. Let $\boldsymbol{B}$ and $\boldsymbol{C}$ be left-trivial semigroups of cardinality n and m respectively. Then $\boldsymbol{A} \cong \boldsymbol{B} \times \boldsymbol{C}$. If $|A|$ is infinite,then $|A| = |A \times A|$ by set theory. So $\boldsymbol{A} \cong \boldsymbol{A} \times \boldsymbol{A}$.

Take $\boldsymbol{A}$ to be the (unique) left-trivial semigroup with universe ω. Suppose $\boldsymbol{A} \cong \prod_{i \in I} \boldsymbol{B}_i$ with $1 < |B_i|$ for each $i \in I$. The claim is that the index set I must be finite. Otherwise, we get $|\omega| = |A| = \left|\prod_{i \in I} \boldsymbol{B}_i\right| \geq 2^{|I|} \geq |2^{\omega}| = |\mathbb{R}|$, contradicting the fact that the real numbers cannot be enumerated. Thus I must be finite and hence, for at least one $i \in I$, the cardinality of $\boldsymbol{B}_i$ is infinite and hence cannot be directly indecomposable.

The final thing to do in this section is show how the direct product of a system of multi-sorted algebras is defined.

Let Σ be a multi-sorted signature with sort set S. Let $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ be a a system of Σ-algebras, where the universe of each $\boldsymbol{A}_i$ is an S-sorted set $\langle\, A_{i,s} : s \in S \,\rangle$. The universe $\langle\, A_i : i \in I \,\rangle$ of the direct product $\prod_{i \in I} \boldsymbol{A}_i$ is the S-sorted system of direct products of sets $\left\langle \prod_{i \in I} A_{i,s} : s \in S \right\rangle$. Let $\sigma \in \Sigma$ be of type $s_1, \ldots, s_n \to s$, and let $\vec{a}_j \in \prod_{i \in I} A_{i,s_j}$ for $j = 1, \cdots, n$. Then

$$\sigma^{\prod \boldsymbol{A}_i}(\vec{a}_1, \ldots, \vec{a}_n) = \underbrace{\langle\, \sigma^{\boldsymbol{A}_i}\big(\underset{s_1}{\vec{a}_1(i)}, \ldots, \underset{s_n}{\vec{a}_n(i)}\big) : i \in I \,\rangle}_{s}.$$

3. Free Algebras, Polynomial Algebras, Varieties

Almost all the main classes of algebras studied in abstract algebra are either defined by identities or are derived in some natural way from classes that are defined by identites. Groups, rings, fields, vector spaces, modules are examples. In the general theory of algebra a *variety* is any class of algebras of fixed but arbitrary signature that is defined by identites. An algebra is free over a variety if it does not satisfy any identity that is not satisfied by all

members of the variety. Every variety contains algebras that is free over the variety; they play a key role in the theory of varieties.

We begin by discussing a property of algebras expressed in terms of homomorphisms that will eventually be shown to be equivalent to freedom.

Definition 3.1. Let K be a class of Σ-algebras, and let $\boldsymbol{A}$ be a Σ-algebra and X a subset of A. $\boldsymbol{A}$ has the *universal mapping property* (UMP) *over* K *with respect to* (wrt) X if

(i) $A = \mathrm{Sg}^{\boldsymbol{A}}(X)$, and
(ii) for every $\boldsymbol{B} \in \mathsf{K}$ and every mapping $h\colon X \to B$ there exists a homomorphism $h^*\colon \boldsymbol{A} \to \boldsymbol{B}$ such that $h^* \restriction X = h$.

Note that the condition (i) implies that h^* is unique by Thm. 2.13.

Lemma 3.2. *If $\boldsymbol{A}$ has the* UMP *over K wrt X, then $\boldsymbol{A}$ has the* UMP *over $\mathsf{HSP}(\mathsf{K})$ wrt to X.*

Proof. It suffices to show that $\boldsymbol{A}$ has the UMP over $\mathsf{S}(\mathsf{K})$, $\mathsf{H}(\mathsf{K})$, and $\mathsf{P}(\mathsf{K})$ wrt to X.

$\mathsf{S}(\mathsf{K})$: Assume $\boldsymbol{B} \subseteq \boldsymbol{C} \in \mathsf{K}$ and $h\colon X \to \boldsymbol{B}$. Then by assumption there is a $h^*\colon \boldsymbol{A} \to \boldsymbol{C}$ such that $h^* \restriction X = h$. We note first of all that $h^*(X) \subseteq B \in \mathrm{Sub}(\boldsymbol{C})$, and hence that $\mathrm{Sg}^{\boldsymbol{C}}\big(h^*(X)\big) \subseteq B$ because $\mathrm{Sg}^{\boldsymbol{C}}\big(h^*(X)\big)$ is the smallest subuniverse of $\boldsymbol{C}$ that includes X. Thus by Thm 2.14(iii) we have

$$h^*(A) = h^*\big(\mathrm{Sg}^{\boldsymbol{A}}(X)\big) = \mathrm{Sg}^{\boldsymbol{C}}\big(h^*(X)\big) \subseteq B,$$

i.e., $h^*\colon \boldsymbol{A} \to \boldsymbol{B}$. (Strictly speaking what we should say is that there exists a $h^{**} : \boldsymbol{A} \to \boldsymbol{B}$ such that h^{**} and h^* have the same graph, because we have adopted the categorical definition of a function that says a function is determined by three pieces of data, its graph, its domain, and its codomain; so if the codomains of two functions are different they must be different.)

$\mathsf{H}(\mathsf{K})$: Assume that $\boldsymbol{B} \preccurlyeq \boldsymbol{C} \in \mathsf{K}$ and let $h\colon X \to B$. Let $g\colon \boldsymbol{C} \twoheadrightarrow \boldsymbol{B}$ be an epimorphism, and choose $\bar{h}\colon X \to C$ such that $h = g \circ \bar{h}$; such a $\bar{h}$ exists by the axiom of choice because g is surjective; see Figure 21. By assumption there is a $\bar{h}^*\colon \boldsymbol{A} \to \boldsymbol{C}$ such that $\bar{h}^* \restriction X = \bar{h}$.

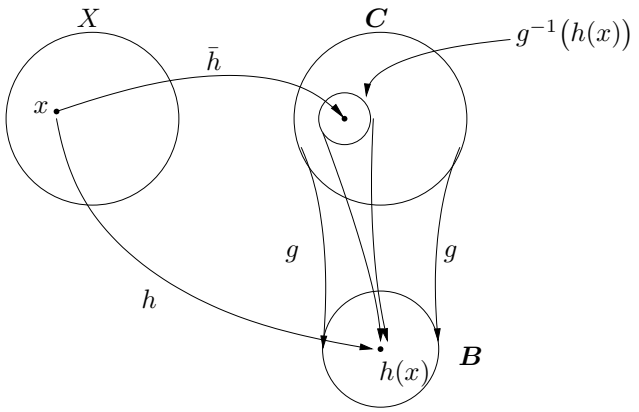


FIGURE 21

Thus $g \circ \bar{h}^*\colon \boldsymbol{A} \to \boldsymbol{B}$ and $(g \circ \bar{h}^*) \restriction X = g \circ (\bar{h}^* \restriction X) = g \circ \bar{h} = h$.

$\mathbf{P}(\mathsf{K})$: Let $h\colon X \to \boldsymbol{B} = \prod_{i\in I} \boldsymbol{C}_i$, where $\langle\, \boldsymbol{C}_i : i \in I \,\rangle \in \mathsf{K}^I$. For every $i \in I$ there is by assumption a $(\pi_i \circ h)^*\colon \boldsymbol{A} \to \boldsymbol{C}_i$ such that $(\pi_i \circ h)^* \restriction X = \pi_i \circ h$. By the Categorical Product Property there is an $h^*\colon \boldsymbol{A} \to \boldsymbol{B}$ such that, for every $i \in I$, $\pi_i \circ h^* = (\pi_i \circ h)^*$. Thus, for every $x \in X$ and every $i \in I$ we have $\pi_i\big(h^*(x)\big) = (\pi_i \circ h^*)(x) = (\pi_i \circ h)^*(x) = (\pi_i \circ h)(x) = \pi_i\big(h(x)\big)$. Thus, for every $x \in X$, $h^*(x) = h(x)$, i.e., $h^* \restriction X = h$. □

Theorem 3.3. *Assume $\boldsymbol{A}$ has the* UMP *over a class K of Σ-algebras wrt to X, and that $\boldsymbol{B}$ has the* UMP *over K wrt Y. If $\boldsymbol{A}, \boldsymbol{B} \in \mathbf{H}\,\mathbf{S}\,\mathbf{P}(\mathsf{K})$ and $|X| = |Y|$, then $\boldsymbol{A} \cong \boldsymbol{B}$. Moreover, for every bijection $f\colon X \cong Y$ there is an isomorphism $f^*\colon \boldsymbol{A} \cong \boldsymbol{B}$ such that $f^* \restriction X = f$.*

Proof. $f\colon X \to B$. So there is an $f^*\colon \boldsymbol{A} \to \boldsymbol{B}$ such that $f^* \restriction X = f$. Also, $f^{-1}\colon Y \to A$. So there is a $(f^{-1})^*\colon \boldsymbol{B} \to \boldsymbol{A}$ such that $(f^{-1})^* \restriction Y = f^{-1}$. Then $(f^{-1})^* \circ f^*\colon \boldsymbol{A} \to \boldsymbol{A}$, and, for every $x \in X$, $\big((f^{-1})^* \circ f^*\big)(x) = (f^{-1})^*\big(f^*(x)\big) = (f^{-1})^*\big(f(x)\big) = f^{-1}\big(f(x)\big) = (f^{-1} \circ f)(x) = x$. So $(f^{-1})^* \circ f^* = \Delta_A$ by the uniqueness property. Similarly, $f^* \circ (f^{-1})^* = \Delta_B$. So $(f^{-1})^* = (f^*)^{-1}$ and $f^*\colon \boldsymbol{A} \cong \boldsymbol{B}$. □

Here are two well known examples from abstract algebra of algebras with the UMP.

(1) If K is the class of all Abelian groups, then, for every $n \in \omega$, $\mathbb{Z}^n$ has the UMP over K wrt the set of "unit vectors", i.e., $\{\langle 1, 0, \ldots, 0\rangle, \langle 0, 1, 0, \ldots, 0\rangle, \ldots, \langle 0, \ldots, 0, 1\rangle\}$.

(2) If K is the class of all vector spaces over a field, then every $\boldsymbol{V} \in \mathsf{K}$ has the UMP wrt any basis of $\boldsymbol{V}$.

We now construct for each signature Σ and each set X such that $X \cap \Sigma = \emptyset$, a Σ-algebra that has the UMP over the class of all Σ-algebras wrt X.

Let $\mathrm{St}_\Sigma(X) = (\Sigma \cup X)^*$, the set of all finite sequences of elements of $\Sigma \cup X$. An element $\langle a_1, \ldots, a_n\rangle$ of $\mathrm{St}_\Sigma(X)$ is called a *string* and written simply as $a_1 \ldots a_n$. Define for each $n \in \omega$ and $\sigma \in \Sigma_n$,

$$\sigma^{\mathbf{St}_\Sigma(X)}(a_{1,1}a_{1,2}\ldots a_{1,m_1}, \cdots, a_{n,1}a_{n,2}\ldots a_{n,m_n}) = a_{1,1}a_{1,2}\ldots a_{1,m_1}, \cdots, a_{n,1}a_{n,2}\ldots a_{n,m_n}.$$

The Σ-algebra

$$\mathbf{St}_\Sigma(X) = \big\langle \mathrm{St}_\Sigma(X), \sigma^{\mathbf{St}_\Sigma(X)} \big\rangle_{\sigma\in\Sigma}$$

is called the *string Σ-algebra in X*.

Definition 3.4. $\mathrm{Te}_\Sigma(X) = \mathrm{Sg}^{\mathbf{St}_\Sigma(X)}(X)$. An element of $\mathrm{Te}_\Sigma(X)$ is called a Σ-term in X; the corresponding subalgebra of $\mathbf{St}_\Sigma(X)$ is

$$\mathbf{Te}_\Sigma(X) = \big\langle \mathrm{Te}_\Sigma(X), \sigma^{\mathbf{Te}_\Sigma(X)} \big\rangle_{\sigma\in\Sigma}$$

is called the *Σ-term algebra in X*. X is called the set of *variables* of $\mathbf{Te}_\Sigma(X)$.

By Lemma 2.6 $\mathrm{Te}_\Sigma(X)$ has the following recursive characterization. $X \subseteq \mathrm{Te}_\Sigma(X)$ (base step). If $t_1, \ldots, t_n \in \mathrm{Te}_\Sigma(X)$, then for every $\sigma \in \Sigma_n$,

$$\sigma^{\mathbf{Te}_\Sigma(X)}(t_1, \ldots, t_n) = \sigma \frown t_1 \frown \cdots \frown t_n \in \mathrm{Te}_\Sigma(X),$$

where "$\frown$" denotes the concatenation of strings. In the sequel we will normally omit the superscript on $\sigma^{\mathbf{Te}_\Sigma(X)}$ and write simply $\sigma(t_1, \ldots, t_n)$ for $\sigma^{\mathbf{Te}_\Sigma(X)}(t_1, \ldots, t_n)$; we leave it to context to indicate that we are applying the term-builder operation of the term algebra.

The set of new terms that are created at the the n-th step in this process is $E_n(X) \setminus E_{n-1}(X)$. n is called their *structural height*. Structural induction can be viewed as induction on the structural height.

Example. Let $\Sigma = \{\vee, \wedge, \neg, 0, 1\}$, the signature of Boolean algebras, and let

$$t = \wedge - x_1 0 \wedge x_2 1.$$

Here is the "parse tree" for t. (We use quotes in refereeing to the parse tree because we do not give a mathematically precise definition. But the intuition is clear and proves useful.)

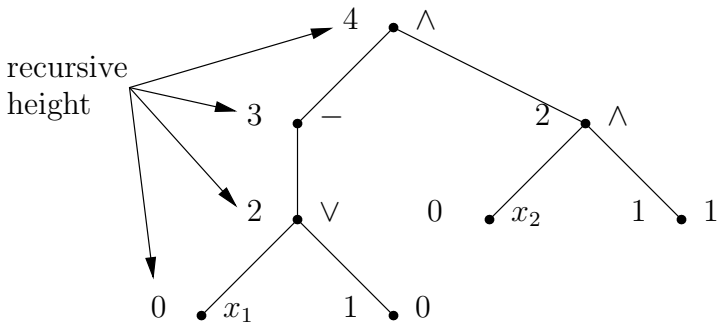


FIGURE 22

If a Σ-term contains no nullary operations its structural height is the same as the height of its parse tree.

Although technically not needed we will use parentheses to make terms easy to parse, We also write binary operations in between their arguments, as is ordinarily done, rather than to the left of them. If we do this for every binary operation, parentheses are necessary for unique parsing. For example, we will write the above term t in the form $-(x_1 \vee 0) \wedge (x_2 \wedge 1)$.

Theorem 3.5. $\mathbf{Te}_\Sigma(X)$ *has the* ***unique parsing property wrt*** X*, i.e.,*

(i) $x \neq \sigma(t_1, \ldots, t_n)$ *for every* $x \in X$*, every* $\sigma \in \Sigma_n$*, and all* $t_1, \ldots, t_n \in \mathrm{Te}_\Sigma(X)$.

(ii) *For all* $n, m \in \omega$*, every* $\sigma \in \Sigma_n$*, every* $\tau \in \Sigma_m$*, and all* $t_1, \ldots, t_n, s_1, \ldots, s_m \in \mathrm{Te}_\Sigma(X)$,

$$\sigma(t_1, \ldots, t_n) = \tau(s_1, \ldots, s_m) \text{ iff } n = m, \sigma = \tau, \text{ and } t_i = s_i \text{ for all } i \leq n.$$

The proof of this theorem is left as an exercise.

The theorem says that the parse tree for each Σ-term is unique.

Corollary 3.6. $\mathbf{Te}_\Sigma(X)$ *has the unique mapping property over* $\mathsf{Alg}(\Sigma)$ *wrt* X.

Proof. Let $\boldsymbol{A}$ be any Σ-algebra and let $h\colon X \to A$ be any map. Define $h^*\colon \mathrm{Te}_\Sigma(X) \to A$ by structural induction, i.e., induction on the structural height of a Σ-term t. If $t = x$, $h^*(t) = h(x)$. If $t = \sigma(t_1, \dots, t_n)$, $h^*(t) = \sigma^{\boldsymbol{A}}\big(h^*(t_1), \dots, h^*(t_n)\big)$. h^* is well defined by the unique parsing property. It is clearly a homomorphism that agrees with h on X. □

A mapping $h\colon X \to A$ is called an *assignment* of elements of A to the variables in X, and its unique extension h^* to a homomorphism form $\mathbf{Te}_\Sigma(X)$ to $\boldsymbol{A}$ is called the *evaluation map* based on this assignment.

Let $n \in \omega$ be fixed but arbitrary and let $x_1, \dots, x_n$ be a sequence of distinct variable symbols. Let $X = \{x_1, \dots, x_n\}$. We often write a term t in the form $t(x_1, \dots, x_n)$ as an alternative way of specifying that the variables of t are in X, i.e., that $t \in \mathrm{Te}_\Sigma(X)$. In the same spirit we write $t^{\boldsymbol{A}}(a_1, \dots, a_n)$ for the image $h^*(t)$ of t in $\boldsymbol{A}$ under the evaluation map based on the assignment $h(x_i) = a_i$ for all $i \leq n$.

For example, let $t(x_1, x_2)$ be the term $-(x_1 \vee 0) \wedge (x_2 \wedge 1)$ considered above, and let $\boldsymbol{B}_2 = \langle \{0,1\}, \vee^{\boldsymbol{B}_2}, \wedge^{\boldsymbol{B}_2}, -^{\boldsymbol{B}_2}, 0, 1\rangle$ be the 2-element Boolean algebra. Then

$$\begin{aligned} t_2^{\boldsymbol{B}}(0,1) = h^*(t) &= h^*\big(-(x_1 \vee 0) \wedge (x_2 \wedge 1)\big) \\ &= -^{\boldsymbol{B}_2}(h(x_1) \vee^{\boldsymbol{B}_2} 0) \wedge^{\boldsymbol{B}_2} (h(x_2) \wedge^{\boldsymbol{B}_2} 1) \\ &\quad -^{\boldsymbol{B}_2} (0 \vee^{\boldsymbol{B}_2} 0) \wedge^{\boldsymbol{B}_2} (1 \wedge^{\boldsymbol{B}_2} 1) \\ &= 0. \end{aligned}$$

Terms in $\mathrm{Te}_\Sigma(\{x_1, \dots, x_n\})$ are said to be *n-ary*. An n-ary term t determines, for each Σ-algebra $\boldsymbol{A}$, an n-ary operation $t^{\boldsymbol{A}}\colon A^n \to A$ on A that maps $\langle a_1, \dots, a_n\rangle$ to $t^{\boldsymbol{A}}(a_1, \dots, a_n)$.

Definition 3.7. Let $\boldsymbol{A}$ be a Σ-algebra. An n-ary operation $f\colon A^n \to A$ on A is called a *term* or *derived operation* of $\boldsymbol{A}$ if there exists a Σ-term $t(x_1, \dots, x_n)$ such that $f = t^{\boldsymbol{A}}$.

The set of all term operations of $\boldsymbol{A}$ of rank n is denoted by $\mathrm{Clo}_n(\boldsymbol{A})$ and is called the *n-ary clone of $\boldsymbol{A}$*.

By the *clone* of $\boldsymbol{A}$, in symbols, $\mathrm{Clo}_\omega(\boldsymbol{A})$, we mean the union of the n-ary clones over all $n \in \omega$, i.e., $\bigcup_{n\in\omega} \mathrm{Clo}_n(\boldsymbol{A})$. Some authors define the clone of $\boldsymbol{A}$ to be the ω-sorted set $\langle\, \mathrm{Clo}_n(\boldsymbol{A}) : n \in \omega \,\rangle$.

Here are some basic facts about term operations; all have easy proofs by structural induction.

(1) Subuniverses are closed under term operations, i.e., if $B \in \mathrm{Sub}(\boldsymbol{A})$ and $t(x_1, \dots, x_n)$ is a Σ-term, then for all $b_1, \dots, b_n \in B$, $t^{\boldsymbol{A}}(b_1, \dots, b_n) \in B$. Moreover, if $\boldsymbol{B} \subseteq \boldsymbol{A}$, then, for all $b_1, \dots, b_n \in B$, $t^{\boldsymbol{B}}(b_1, \dots, b_n) = t^{\boldsymbol{A}}(a_1, \dots, a_n)$, i.e., $t^{\boldsymbol{B}} = t^{\boldsymbol{A}} \restriction B^n$.

(2) Homomorphisms preserve term operations, i.e., if $h\colon \boldsymbol{A} \to \boldsymbol{B}$, then for all $a_1, \dots, a_n \in A$, $h\big(t^{\boldsymbol{A}}(a_1, \dots, a_n)\big) = t^{\boldsymbol{B}}\big(h(a_1), \dots, h(a_n)\big)$.

(3)Every term operation has the substitution property wrt congruences, i.e., if $\alpha \in \mathrm{Co}(\boldsymbol{A})$ and $a_1 \,\alpha\, b_1, \dots, a_n \,\alpha\, b_n$, then $t^{\boldsymbol{A}}(a_1, \dots, a_n) \;\alpha\; t^{\boldsymbol{A}}(b_1, \dots, b_n)$.

Definition 3.8. Let Σ, Σ' be signatures, and let $\boldsymbol{A}$, $\boldsymbol{A}'$ be $\Sigma-$ and Σ'-algebras, respectively. $\boldsymbol{A}'$ is *termwise definable in* $\boldsymbol{A}$ if every fundamental operation of $\boldsymbol{A}'$ is a term operation of $\boldsymbol{A}$. $\boldsymbol{A}$ and $\boldsymbol{A}'$ are *termwise definitionally equivalent* if each is termwise definable in the other.

It follows immediately from the basic facts about term operations listed above that, if $\boldsymbol{A}'$ is termwise definable in $\boldsymbol{A}$ then $\mathrm{Sub}(\boldsymbol{A}) \subseteq \mathrm{Sub}(\boldsymbol{A}')$ and $\mathrm{Co}(\boldsymbol{A}) \subseteq \mathrm{Co}(\boldsymbol{A}')$ Thus termwise definitionally equivalent algebras have the same subuniverses and same congruence relations. Moreover if $\boldsymbol{B}$ and $\boldsymbol{B}'$ are other termwise definitionally equivalent Σ- and Σ'-algebras,respectively, then $\mathrm{Hom}(\boldsymbol{A}', \boldsymbol{B}') = \mathrm{Hom}(\boldsymbol{A}, \boldsymbol{B})$.

Lemma 3.9. *$\boldsymbol{A}$ and $\boldsymbol{A}'$ are termwise definitionally equivalent iff* $\mathrm{Clo}_\omega(\boldsymbol{A}) = \mathrm{Clo}_\omega(\boldsymbol{A}')$, *i.e.,* $\mathrm{Clo}_n(\boldsymbol{A}) = \mathrm{Clo}_n(\boldsymbol{A}')$ *for every* $n \in \omega$.

The proof is left as an exercise.

Termwise defintionally equivalent algebras have essentially the same algebraic properties and are often identified. From this point of view, what really defines an algebra is its clone, the set of all its term operations. Its fundamental operations in this view are useful mainly for conveniently specifying, i.e., generating, the clone, and there are usually many different choices of the fundamental operations that can serve this purpose. This is part of the motivation behind the categorical approach to universal algebra This is illustrated in the following example.

Example. Let $\boldsymbol{B} = \langle \boldsymbol{B}, \vee, \wedge, -, 0, 1\rangle$ be a Boolean algebra over the signature $\Sigma = \{\vee, \wedge, -, 0, 1\}$, and consider its two reducts $\boldsymbol{A} = \langle \boldsymbol{A}, \vee, -, 0, 1\rangle$ and $\boldsymbol{A}' = \langle \boldsymbol{A}, \wedge, -, 0, 1\rangle$ to the respective signatures $\Sigma = \{\vee, -, 0, 1\}$ and $\Sigma' = \{\wedge, -, 0, 1\}$. By DeMorgan's laws and the law of double negation we know that the identities $x_1 \wedge x_2 \approx -(-x_1 \vee -x_2)$ and $x_1 \vee x_2 \approx -(-x_1 \wedge -x_2)$ are satisfied in $\boldsymbol{B}$. Thus $\boldsymbol{A}$ and $\boldsymbol{A}'$ are termwise definitionally equivalent.

We note that the basic facts about term operations can often be used to show that and operation on an algebra is not a term operation. Consider for example the semigroup reduct $\langle \mathbb{Z}, +\rangle$ of the group $\mathbb{Z} = \langle \mathbb{Z}, +, -, 0\rangle$ of integers. $-$ is not a term operation of $\langle \mathbb{Z}, +\rangle$ because, for example, the subuniverse ω of $\langle \mathbb{Z}, +\rangle$ is not closed under $-$. Thus $\langle \mathbb{Z}, +\rangle$ and $\mathbb{Z}$ are not termwise definitionally equivalent. This is the reason that, from the point of view of universal algebras, groups of type I and type II (See the examples following Def. 2.2) are considered different.

The best known example of an n-ary clone over an algebra is the set of polynomial functions in n indeterminants over a ring (in particular the ring of real numbers) with integer coefficients. Let $\mathbb{R} = \langle \mathbb{R}, +, \cdot, -, 0, 1\rangle$ be the ring of real numbers (a field). Then

$$\mathrm{Clo}_1(\mathbb{R}) = \{\, (k_0 + k_1 x + \cdots + k_n x^n)^{\mathbb{R}} : k_0, \ldots, k_n \in \mathbb{Z} \,\}.$$

We make two observations:

(1) An element of this clone is a polynomial *function* over $\mathbb{R}$, as opposed to a formal polynomial; this distinct is usually made in a course in abstract algebra, but not in the calculus where polynomials are always thought of as functions. Of course formal polynomials correspond to our terms.

(2) The elements of the clone are the polynomials with integer coefficients. For example, a typical example would be the term operation determined by term $3 + (-2)x + 3x^2 = 1 + 1 + 1 + -x + -x + x \cdot x + x \cdot x + x \cdot x$. In the construction of the term we can use only the fundamental operation symbols of the signature $\{+, \cdot, -, 0, 1\}$. However, we can get all

the polynomial functions simply by expanding the signature to include a symbol for each element of $\mathbb{R}$. Here is how it is done in general.

Let Σ be an arbitrary signature and let $\boldsymbol{A}$ be a Σ-algebra. For each $a \in A$ let $\bar{a}$ be a new nullary operation symbol. Let $\Sigma_A = \Sigma \cup \{\, \bar{a} : a \in A \,\}$ and let $\boldsymbol{A}^+$ be the Σ_A-algebra

$$\boldsymbol{A}^+ = \big\langle A, \langle\, \sigma^{\boldsymbol{A}} : \sigma \in \Sigma \,\rangle \frown \langle\, \bar{a}^{\boldsymbol{A}} : a \in A \,\rangle \big\rangle,$$

where $\bar{a}^{\boldsymbol{A}} = a$ for every $a \in A$.

Definition 3.10. Let $n \in \omega$. A element of $\mathrm{Clo}_n(\boldsymbol{A}^+)$ is called an *n-ary polynomial operations over $\boldsymbol{A}$*.

Notice that the nullary fundamental operation $\bar{a}^{\mathbf{Clo}_n(\boldsymbol{A}^+)}$ of $\mathbf{Clo}_n(\boldsymbol{A}^+)$ denotes the constant n-ary operation on A with (unique) value a, i.e., $\bar{a}^{\mathbf{Clo}_n(\boldsymbol{A}^+)}(b_1, \dots, b_n) = a$ for all $\langle b_1, \dots, b_n \rangle \in A^n$.

For every natural number n, $\mathrm{Clo}_n(\mathbb{R}^+)$ is the set of all polynomial functions over the real numbers in n-indeterminants, and $\mathrm{Clo}_n(\mathbb{R})$ is subset consisting of polynomial functions with only integer coefficients.

An important and well known feature of both the term operations and the the polynomial operations over the reals is that they can both have a ring structure. We now show that a similar situation holds for the term and polynomial operations over any algebra and any signature. For this purpose we need the following lemma.

Lemma 3.11. *Let $t_1(x_1, \dots, x_n), \dots, t_k(x_1, \dots, x_n)$ be n-ary Σ-terms. Let $s(x_1, \dots, x_n) = \sigma(t_1, \dots, t_k)$ for some $\sigma \in \Sigma_k$. Then for every Σ-algebra $\boldsymbol{A}$ and all $a_1, \dots, a_k \in A$*

$$s^{\boldsymbol{A}}(a_1, \dots, a_n) = \sigma^{\boldsymbol{A}}\big(t^{\boldsymbol{A}}(a_1, \dots, a_k), \dots, t^{\boldsymbol{A}}(a_1, \dots, a_k)\big).$$

Proof. Let $X = \{x_1, \dots, x_n\}$ and let $h\colon X \to A$ such that $h(x_i) = a_i$ for every $i \leq n$. Let $h^*\colon \mathbf{Te}_\Sigma(X) \to \boldsymbol{A}$ such that $h^* \restriction X = h$. Then we have

$$\begin{aligned}
s^{\boldsymbol{A}}(a_1, \dots, a_n) &= h^*(s),, && \text{by definition of } s^{\boldsymbol{A}} \\
&= h^*\big(\sigma(t_1, \dots, t_m)\big) \\
&= \sigma^{\boldsymbol{A}}\big(h^*(t_1), \dots, h^*(t_k)\big),, && \text{since } h^* \text{ is a homomorphism} \\
&= \sigma^{\boldsymbol{A}}\big(t_1^{\boldsymbol{A}}(a_1, \dots, a_n), \dots, t_k^{\boldsymbol{A}}(a_1, \dots, a_n)\big).
\end{aligned}$$

□

Let Σ be a signature and $\boldsymbol{A}$ a Σ-algebra. For each $n \in \omega$ we can give the set $\mathrm{Clo}_n(\boldsymbol{A})$ of n-ary term operations of $\boldsymbol{A}$ the structure of a Σ-algebra $\mathbf{Clo}_n(\boldsymbol{A})$. Let $\sigma \in \Sigma_k$ and let $f_1, \dots, f_k \in \mathrm{Clo}_n(\boldsymbol{A})$. Choose n-ary terms $t_1(x_1, \dots, x_n), \dots, t_k(x_1, \dots, x_n)$ such that $t_i^{\boldsymbol{A}} = f_i$ for each $i \leq k$. Define $\sigma^{\mathbf{Clo}_n(\boldsymbol{A})}(f_1, \dots, f_k) = t^{\boldsymbol{A}}$, where $t = \sigma(t_1, \dots, t_n)$. Since the definition depends on a choice of representative terms for the term operations $f_1, \dots, f_k$ we have to show $\sigma^{\mathbf{Clo}_n(\boldsymbol{A})}$ is well defined, i.e., it does not depend on the particular choice of representative terms.

Suppose $f_1 = s_1^{\boldsymbol{A}}, \dots, f_k = s_k^{\boldsymbol{A}}$ and $s = \sigma(s_1, \dots, s_k)$. Then for all $a_1, \dots, a_n \in A$ we have

$$\begin{aligned} t^{\boldsymbol{A}}(a_1, \dots, a_n) &= \big(\sigma(t_1, \dots, t_k)\big)^{\boldsymbol{A}}(a_1, \dots, a_n) \\ &= \sigma^{\boldsymbol{A}}\big(t_1^{\boldsymbol{A}}(a_1, \dots, a_n), \dots, t_k^{\boldsymbol{A}}(a_1, \dots, a_n)\big), \quad \text{by Lemma 3.11} \\ &= \sigma^{\boldsymbol{A}}\big(f_1(a_1, \dots, a_n), \dots, f_k(a_1, \dots, a_n)\big) \\ &= \sigma^{\boldsymbol{A}}\big(s_1^{\boldsymbol{A}}(a_1, \dots, a_n), \dots, s_k^{\boldsymbol{A}}(a_1, \dots, a_n)\big) \\ &= \big(\sigma(s_1, \dots, s_k)\big)^{\boldsymbol{A}}(a_1, \dots, a_n), \quad \text{by Lemma 3.11} \\ &= s^{\boldsymbol{A}}(a_1, \dots, a_n). \end{aligned}$$

So $\sigma^{\mathbf{Clo}_n(\boldsymbol{A})}$ is well defined.

Definition 3.12. let Σ be a Σ-algebra and $n \in \omega$. Then

(i) $\mathbf{Clo}_n(\boldsymbol{A}) = \langle \mathrm{Clo}_n(\boldsymbol{A}),\ \sigma^{\mathbf{Clo}_n(\boldsymbol{A})}\rangle_{\sigma\in\Sigma}$. It is called the *$n$-ary clone algebra over $\boldsymbol{A}$*, or alternatively, the *algebra of n-ary term operations over $\boldsymbol{A}$*.

(ii) The $\Sigma_{\boldsymbol{A}}$-algebra $\mathbf{Clo}_n(\boldsymbol{A}^+)$ is called the *algebra of n-ary polynomial operations over $\boldsymbol{A}$*.

We make several observations.

(1) $\mathrm{Clo}_n(\boldsymbol{A})$ is generated by $\{x_1^{\boldsymbol{A}}, \dots, x_n^{\boldsymbol{A}}\}$ (exercise).

(2) If $\boldsymbol{A}$ is nontrivial (i.e., $|A| \geq 2$), then, for all $i, j \leq n$,

$$i \neq j \text{ implies } x_i^{\boldsymbol{A}} \neq x_j^{\boldsymbol{A}},$$

i.e., $|\{x_1^{\boldsymbol{A}}, \dots, x_n^{\boldsymbol{A}}\}| = n$. To see this consider any two distinct elements a and b of $\boldsymbol{A}$. Then

$$x_i^{\boldsymbol{A}}(a, \dots, a, \underset{j}{b}, a, \dots, a) = a \quad \text{and} \quad x_j^{\boldsymbol{A}}(a, \dots, a, \underset{j}{b}, a, \dots, a) = b.$$

(3) The mapping $a \mapsto \bar{a}^{\mathbf{Clo}_n(\boldsymbol{A}^+)}$ is a monomorphism from $\boldsymbol{A}^+$ into $\mathbf{Clo}_n(\boldsymbol{A}^+)$. This is an easy exercise. Thus if we identify a and $\bar{a}^{\mathbf{Clo}_n(\boldsymbol{A}^+)}$ we can assume the $\boldsymbol{A}^+$ is a subalgebra of $\mathbf{Clo}_n(\boldsymbol{A}^+)$.

We all know that the ring of integer-coefficient polynomials over $\mathbb{R}$ has the universal mapping property over the $\mathbb{R}$ wrt to the set of indeterminants. This holds in general as we now show.

Theorem 3.13. *let $\boldsymbol{A}$ be a Σ-algebra and $n \in \omega$. Then $\mathbf{Clo}_n(\boldsymbol{A})$ has the universal mapping property over $\boldsymbol{A}$ (i.e., over $\{\boldsymbol{A}\}$) wrt to $\{x_1^{\boldsymbol{A}}, \dots, x_n^{\boldsymbol{A}}\}$.*

Proof. If $\boldsymbol{A}$ is trivial, then the theorem is trivially true. Assume $\boldsymbol{A}$ is nontrivial. Let $h\colon \{x_1^{\boldsymbol{A}}, \dots, x_n^{\boldsymbol{A}}\} \to A$. Define $h^*\colon \mathrm{Clo}_n(\boldsymbol{A}) \to A$ by

$$h^*(t^{\boldsymbol{A}}) = t^{\boldsymbol{A}}\big(h(x_1^{\boldsymbol{A}}), \dots, h(x_n^{\boldsymbol{A}})\big), \quad \text{for every } n\text{-ary term } t(x_1, \dots, x_n).$$

h^* is obviously well defined. We check it is a homomorphism.

$$\begin{aligned}
&h^*\big(\sigma^{\mathbf{Clo}_n(\boldsymbol{A})}(t_1^{\boldsymbol{A}},\dots,t_k^{\boldsymbol{A}})\big)\\
&\qquad = h^*\big(\big(\sigma(t_1,\dots,t_n)\big)^{\boldsymbol{A}}\big), && \text{by defn. of } \sigma^{\mathrm{Clo}_n(\boldsymbol{A})}\\
&\qquad = \sigma(t_1,\dots,t_n)^{\boldsymbol{A}}\big(h(x_1^{\boldsymbol{A}}),\dots,h(x_n^{\boldsymbol{A}})\big), && \text{by defn. of } h^*\\
&\qquad = \sigma^{\boldsymbol{A}}\big(t_1^{\boldsymbol{A}}\big(h(x_1^{\boldsymbol{A}}),\dots,h(x_n^{\boldsymbol{A}})\big),\dots,t_k^{\boldsymbol{A}}\big(h(x_1),\dots,h(x_n)\big)\big), && \text{by Lemma 3.11}\\
&\qquad = \sigma^{\boldsymbol{A}}\big(h^*(t_1^{\boldsymbol{A}}),\dots,h^*(t_k^{\boldsymbol{A}})\big), && \text{by defn. of } h^*.
\end{aligned}$$

Finally, we note that, for each $i \leq n$, $h^*(x_i^{\boldsymbol{A}}) = x_i^{\boldsymbol{A}}\big(h(x_1^{\boldsymbol{A}}),\dots,h(x_n^{\boldsymbol{A}})\big) = h(x_i^{\boldsymbol{A}})$. □

Corollary 3.14. *For every $h\colon\{x_1^{\boldsymbol{A}^+},\dots,x_n^{\boldsymbol{A}^+}\} \to A$ there is a unique homomorphism $h^*\colon \mathbf{Clo}_n(\boldsymbol{A}^+) \to \boldsymbol{A}^+$ such that*

(i) $h^* \restriction \{x_1^{\boldsymbol{A}^+},\dots,x_n^{\boldsymbol{A}^+}\} = h$.
(ii) $h^* \restriction A = \Delta_A$.

Proof. By the theorem there is a unique $h^*\colon \mathbf{Clo}_n(\boldsymbol{A}^+) \to \boldsymbol{A}^+$ such that condition (i) holds. Since h^* is a homomorphism over the extended signature $\Sigma_{\boldsymbol{A}}$, h^* is identity on A since for each $a \in A$, $h^*(a) = h^*(\bar{a}^{\boldsymbol{A}}) = \bar{a}^{\mathbf{Clo}_n(\boldsymbol{A}^+)} = a$; the last equality holds because we have identified $\bar{a}^{\mathbf{Clo}_n(\boldsymbol{A}^+)}$ with a. □

The property of the n-ary clone algebra over $\boldsymbol{A}$ that sets it apart from the n-ary term algebra is that it is a subdirect power of $\boldsymbol{A}$, as we show in the next theorem.

Theorem 3.15. *Let $\boldsymbol{A}$ be a Σ-algebra and $n \in \omega$. Then $\mathbf{Clo}_n(\boldsymbol{A}) \in \mathsf{SP}(\boldsymbol{A})$. In fact, $\mathbf{Clo}_n(\boldsymbol{A})$ is the subalgebra of $\boldsymbol{A}^{A^n}$ generated by $\{\pi_1,\dots,\pi_n\}$, where $\pi_i\colon A^{A^n}$ is the i-projection function.*

Proof. Let $X = \{x_1,\dots,x_n\}$ and let $h^*\colon \mathbf{Te}_\Sigma(X) \to \boldsymbol{A}^{A^n}$ such that $h^*(x_i) = \pi_i$ for each $i \leq n$. By Thm. 2.14(iii), $h^*\big(\mathrm{Te}_\Sigma(X)\big) = \mathrm{Sg}^{\boldsymbol{A}^{A^n}}\big(\{\pi_1,\dots,\pi_n\}\big)$.

The claim is that, for every $t \in \mathrm{Te}_\Sigma(X)$, $h^*(t) = t^{\boldsymbol{A}}$, and hence

$$\mathbf{Clo}_n(\boldsymbol{A}) = h^*\big(\mathbf{Te}_\Sigma(X)\big) = \mathbf{Sg}^{\boldsymbol{A}^{A^n}}\big(\{\pi_1,\dots,\pi_n\}\big).$$

This is proved by induction on the structural height of t. For every $\langle a_1,\dots,a_n\rangle \in A^n$, $h^*(x_i)(a_1,\dots,a_n) = \pi_i(a_1,\dots,a_n) = a_i = x_i^{\boldsymbol{A}}(a_1,\dots,a_n)$. So $h^*(x_i) = x_i^{\boldsymbol{A}}$ for every $i \leq n$.

$$\begin{aligned}
&h^*\big(\sigma(t_1,\dots,t_k)\big)(a_1,\dots,a_n)\\
&\qquad = \sigma^{\boldsymbol{A}^{A^n}}\big(h^*(t_1),\dots,h^*(t_n)\big)(a_1,\dots,a_n), && \text{since } h^* \text{ is a homomorphism}\\
&\qquad = \sigma^{\boldsymbol{A}}\big(h^*(t_1)(a_1,\dots,a_n),\dots,h^*(t_k)(a_1,\dots,a_n)\big), && \text{by defn. of } \sigma^{\boldsymbol{A}^{A^n}}\\
&\qquad = \sigma^{\boldsymbol{A}}\big(t_1^{\boldsymbol{A}}(a_1,\dots,a_n),\dots,t_k^{\boldsymbol{A}}(a_1,\dots,a_n)\big), && \text{by ind. hyp.}\\
&\qquad = \big(\sigma(t_1,\dots,t_n)\big)^{\boldsymbol{A}}(a_1,\dots,a_n), && \text{by Lemma 3.11.}
\end{aligned}$$

Since this holds for every $\langle a_1,\dots,a_n\rangle \in A^n$, we get $h^*\big(\sigma(t_1,\dots,t_n)\big) = \big(\sigma(t_1,\dots,t_n)\big)^{\boldsymbol{A}}$. This proves the claim and hence the theorem. □

It is easy to see that, whenever $n \leq m$, each n-ary term $t(x_1, \ldots, x_n)$ is also an m-ary term $t(x_1, \ldots, x_m)$, even though the variables $x_{n+1}, \ldots, x_m$ don't actually occur in t. Functionally, if we write f for $t^{\boldsymbol{A}}$ as a function form A^n to A, and write g for $t^{\boldsymbol{A}}$ as a function from A^m to A, then, for every $\langle a_1, \ldots, a_m \rangle \in A^m$, $g(a_1, \ldots, a_m) = f(a_1, \ldots, a_n)$. It is easy to check that he mapping $f \mapsto g$ gives a embedding of $\mathbf{Clo}_n(\boldsymbol{A})$ in $\mathbf{Clo}_m(\boldsymbol{A})$. We identify $\mathbf{Clo}_n(\boldsymbol{A})$ with its image in $\mathbf{Clo}_m(\boldsymbol{A})$ so that $\mathbf{Clo}_n(\boldsymbol{A})$ can actually be viewed as a subalgebra of $\mathbf{Clo}_m(\boldsymbol{A})$. The whole clone $\mathrm{Clo}_\omega \boldsymbol{A}) = \bigcup_{n\in\omega} \mathrm{Clo}_n(\boldsymbol{A})$ can then be made into a Σ-algebra in the natural way: if $t(x_1, \ldots, x_{n_i})$ is an n_i-ary term for $i \leq k$ and $\sigma \in \Sigma_k$, then $\sigma(t_1, \ldots, t_k)$ is an m-ary term where $m = \mathrm{Max}\{n_1, \ldots, n_k\}$ and thus $\sigma^{\mathbf{Clo}_\omega(sbA)}(t_1^{\boldsymbol{A}}, \ldots, t_k^{\boldsymbol{A}}) = \sigma^{\mathbf{Clo}_m(\boldsymbol{A})}(t_1^{\boldsymbol{A}}, \ldots, t_k^{\boldsymbol{A}})$.

$\mathbf{Clo}_\omega(\boldsymbol{A})$ can be thought of as the set of term operations associated with terms over the infinite set of variables $X = \{x_1, x_2, x_3, \ldots\}$. Each such term contains only a finite number of variables, but of course the number of different variables that can occur in a term is unbounded. Thus $t^{\boldsymbol{A}} \colon A^\omega \to A$ is an operation with a nominally infinite number of arguments, but it is independent of all but an infinite number of them.

It is not difficult to check that $\mathbf{Clo}_\omega(\boldsymbol{A})$ has the UMP over $\boldsymbol{A}$ wrt to the infinite set $\{x_1^{\boldsymbol{A}}, x_2^{\boldsymbol{A}}, x_3^{\boldsymbol{A}}, \ldots\}$, and that $\mathbf{Clo}_\omega(\boldsymbol{A}) \cong \mathbf{;} \subseteq \boldsymbol{A}^{A^\omega}$. But we want to show how to construct algebras of term operations over sets of variables of arbitrary large cardinality which will give us algebras with the UMP wrt arbitrary large sets. This requires a little transfinite cardinal arithmetic.

In standard set theory a cardinal number is identified with the set of all ordinal numbers less than it, i.e., for each cardinal number α, $\alpha = \{\, \xi : \xi \text{ is an ordinal and } \xi < \alpha \,\}$. Consider for example the finite ordinals: $0 < 1 < 2 < 3 < \cdots$. Each of them is also a cardinal number (finite ordinals and cardinals are the same). $0 = \emptyset$, $1 = \{0\} = \{\emptyset\}$, $2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$, $\ldots$, $n = \{0, 1, 2, \ldots, n-1\}$. The first infinite cardinal is $\aleph_0 = \omega = \{0, 1, 2, 3, \ldots\}$. The next infinite cardinal is $\aleph_1 = \{0, 1, 2, \ldots, \omega, \omega+1, \omega+2, \ldots, \omega+\omega, \omega+\omega+1, \ldots\}$.[2] The "+" in "$\omega + 1$, "$\omega + 2$",...,"$\omega + \omega + 1$",... is ordinal addition, but don't worry about it, it doesn't play any role in our work. Notice that for any cardinal α and any ordinal ξ, $\xi \in \alpha$ iff $\xi < \alpha$; in particular, $n \in \omega$ iff $n < \omega$.

Let α be an infinite cardinal, and let $X_\alpha = \{\, x_\xi : \xi \in \alpha \,\}$ be a set of pairwise distinct variable symbols indexed by the ordinals less than α so that the cardinality of X is α. For every $t \in \mathrm{Te}_\Sigma(X)$ we define a term operation $t^{\boldsymbol{A}} \colon A^\alpha \to A$ just as before by replacing the finite cardinal "n" everywhere by "α". Note that an α-ary term $t(\langle x_\xi : \xi < \alpha \rangle)$ still contains occurrences only a finite number of the x_ξ, and the corresponding term operation $t^{\boldsymbol{A}}$ is independent of all but a finite number of its α arguments. The set of all α-ary term operations is called the *α-ary clone of $\boldsymbol{A}$* and is denoted by $\mathrm{Clo}_\alpha(\boldsymbol{A})$. $\mathrm{Clo}_\alpha(\boldsymbol{A})$ can be given the structure of a Σ-algebra $\mathbf{Clo}_\alpha(\boldsymbol{A})$, just like $\mathbf{Clo}_n(\boldsymbol{A})$ for finite n. The following two theorems are proved just like Theorems 3.13 and 3.15, the corresponding theorems for finitary clone algebras, essentially by replacing "n" everywhere by "α".

Theorem 3.16. *let $\boldsymbol{A}$ be a Σ-algebra and α any infinite cardinal Then $\mathbf{Clo}_\alpha(\boldsymbol{A})$ has the universal mapping property over $\boldsymbol{A}$ wrt to $\{\, x_\xi^{\boldsymbol{A}} : \xi < \alpha \,\}$.*

[2] By the Continuum Hypothesis $\aleph_1$ is the cardinality of the continuum, i.e., $\aleph_1 = |\mathbb{R}|$. But the Continuum Hypothesis is not provable form the axioms of set theory, so there are models of set theory in which $\aleph_1$ is much smaller than $|\mathbb{R}|$.

Theorem 3.17. *Let $\boldsymbol{A}$ be a Σ-algebra and α any infinite cardinal. Then* $\mathbf{Clo}_\alpha(\boldsymbol{A}) \in \mathbf{S}\,\mathbf{P}(\boldsymbol{A})$. *In fact,* $\mathbf{Clo}_\alpha(\boldsymbol{A})$ *is the subalgebra of* $\boldsymbol{A}^{A^\alpha}$ *generated by* $\{\,\pi_\xi : \xi \in \alpha\,\}$, *where* $\pi_\xi \colon A^{A^\alpha}$ *is the* ξ*-projection function.*

3.1. **Identities, models, and varieties.** We now change the focus of our investigations from individual algebras to classes of algebras, and in particular to the way these classes are defined. The axiomatic approach is a fundamental feature of modern algebra. For instance, while the number theorist focuses all his or her attention on the ring of integers, to the algebraist the integers are but one member, albeit the paradigm, of the class of principal ideal domains. More precisely, the algebraist is concerned less with the particular structure of the integers than with the abstract properties of the integers that give them their special nature. These abstract properties are formulated in a formal language, and the language itself, including the deductive apparatus by which the logical relationships between the propositions of the language are specified, then becomes the object of mathematical investigation. The mathematics of the language of mathematics is called *metamathematics*. In algebra many of the most important classes of algebras are defined by laws, or identities. Consequently we concentrate first on mathematics of the language of equations and the deductive apparatus associated with them. This is called *equational logic*.

From now on, unless specifically indicated otherwise, the symbol X will stand for $X_\omega = \{x_0, x_1, x_2, \dots\}$, a fixed countably infinite set of pairwise distinct variable symbols. Note that the numbering starts at zero. From now on all enumerated systems will be ordered by cardinals and hence the numbering will start with 0. In particular a finite sequence of length n will be written as $a_0, \dots, a_{n-1}$ rather than as $a_1, \dots, a_n$.

Note that $\mathrm{Te}_\Sigma(X) = \bigcup_{n\in\omega} \mathrm{Te}_\Sigma(x_0, \dots, x_{n-1})$.

An *Σ-equation*, or simply an *equation* when the specific signature is not relevant, is an ordered pair $\langle t, s\rangle$ with $t, s \in \mathrm{Te}_\Sigma(X)$. We will almost always write $\langle t, s\rangle$ in the form $t \approx s$ in order to exploit the intuitive meaning of equations. X represents a countably infinite "reservoir" of variable symbols to draw from, but in a particular term or equation, or more generally in any particular finite set of terms or equations, only a finite number of variables will actually occur. When we want to indicate explicitly the variables that may actually occur in an equation $t \approx s$ we often write $t(x_0, \dots, x_{n-1}) \approx s(x_0, \dots, x_{n-1})$. We emphasize that these two expressions represent exactly the same equation; the "$(x_0, \dots, x_{n-1})$" should be look on as simply annotation in the metalanguage that imparts some additional information about the equation.

Definition 3.18. Let $\boldsymbol{A}$ be a Σ-algebra.

(i) A Σ-equation $t(x_0, \dots, x_{n-1}) \approx s(x_0, \dots, x_{n-1})$ is an *identity of* $\boldsymbol{A}$, and $\boldsymbol{A}$ is a *model of* $t \approx s$, in symbols $\boldsymbol{A} \vDash t \approx s$, if, for all $a_0, \dots, a_{n-1} \in A$, $t^{\boldsymbol{A}}(a_0, \dots, a_{n-1}) = s^{\boldsymbol{A}}(a_0, \dots, a_{n-1})$, i.e., for every $h^* \in \mathrm{Hom}(\mathbf{Te}_\Sigma(X), \boldsymbol{A})$, $h^*(t) = h^*(s)$.

(ii) $\boldsymbol{A}$ is a *model* of a set E of equations if, for every $t \approx s \in E$, $\boldsymbol{A} \vDash t \approx s$. The class of all models of E is denoted by $\mathsf{Mod}(E)$.

(iii) $t \approx s$ is an *identity* of a class K of Σ-algebras if, for every $\boldsymbol{A} \in \mathsf{K}$, $\boldsymbol{A} \vDash t \approx s$. The set of all identities of K is denoted by $\mathrm{Id}(\mathsf{K})$.

Lemma 3.19. *Let $\boldsymbol{A}$ be a Σ-algebra and $t(x_0, \dots, x_{n-1}) \approx s(x_0, \dots, x_{n-1})$ a Σ-equation.*

(i) *If $\boldsymbol{A} \vDash t \approx s$, then, for every $\boldsymbol{B} \subseteq \boldsymbol{A}$, $\boldsymbol{B} \vDash t \approx s$.*

(ii) *If $\boldsymbol{A} \vDash t \approx s$, then, for every $\boldsymbol{B} \preccurlyeq \boldsymbol{A}$, $\boldsymbol{B} \vDash t \approx s$.*

Let $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ be a system of Σ-algebras.

(iii) *If, for all $i \in I$, $\boldsymbol{A}_i \vDash t \approx s$, then $\prod_{i\in I} \boldsymbol{A}_i \vDash t \approx s$.*

Proof. (i) For all $b_0, \dots, b_{n-1} \in B$, $t^{\boldsymbol{B}}(b_0, \dots, b_{n-1}) = t^{\boldsymbol{A}}(b_0, \dots, b_{n-1}) = s^{\boldsymbol{A}}(b_0, \dots, b_{n-1}) = s^{\boldsymbol{B}}(b_0, \dots, b_{n-1})$.

(ii) Let $h\colon \boldsymbol{A} \twoheadrightarrow \boldsymbol{B}$. Let $b_0, \dots, b_{n-1} \in B$ and choose $a_0, \dots, a_{n-1} \in A$ such that $h(a_i) = b_i$ for all $i \in I$. Then

$$\begin{aligned} t^{\boldsymbol{B}}(b_0, \dots, b_{n-1}) &= t^{\boldsymbol{B}}\big(h(a_0), \dots, h(a_{n-1})\big) \\ &= h\big(t^{\boldsymbol{A}}(a_0, \dots, a_{n-1})\big) \\ &= h\big(s^{\boldsymbol{A}}(a_0, \dots, a_{n-1})\big) \\ &= s^{\boldsymbol{B}}\big(h(a_0), \dots, h(a_{n-1})\big) \\ &= s^{\boldsymbol{B}}(b_0, \dots, b_{n-1}). \end{aligned}$$

(iii) Let $\vec{a}_0 = \langle\, a_{0,i} : i \in I \,\rangle, \dots, \vec{a}_{n-1} = \langle\, a_{n-1,i} : i \in I \,\rangle \in \prod_{i\in I} A_i$. By structural induction we have

$$\begin{aligned} t^{\prod_i A_i}(\vec{a}_0, \dots, \vec{a}_{n-1}) &= \big\langle\, t^{\boldsymbol{A}_i}(a_{0,i}, \dots, a_{n-1,i}) : i \in I \,\big\rangle, \quad \text{and,} \\ s^{\prod_i A_i}(\vec{a}_0, \dots, \vec{a}_{n-1}) &= \big\langle\, s^{\boldsymbol{A}_i}(a_{0,i}, \dots, a_{n-1,i}) : i \in I \,\big\rangle. \end{aligned}$$

Since $t^{\boldsymbol{A}_i}(a_{0,i}, \dots, a_{n-1,i}) = s^{\boldsymbol{A}_i}(a_{0,i}, \dots, a_{n-1,i})$, for all $i \in I$, we get $t^{\prod_i A_i}(\vec{a}_0, \dots, \vec{a}_{n-1}) = s^{\prod_i A_i}(\vec{a}_0, \dots, \vec{a}_{n-1})$. □

Theorem 3.20. *For any class* K *of* Σ*-algebras and any* Σ*-equation* $t \approx s$*, if* $\mathsf{K} \vDash t \approx s$*, then* $\mathbf{H}\,\mathbf{S}\,\mathbf{P}(\mathsf{K}) \vDash t \approx s$.

Proof. By the lemma, each of the successive entailments implies the following one. $\mathsf{K} \vDash t \approx s$ implies $\mathbf{P}(\mathsf{K}) \vDash t \approx s$ implies $\mathbf{S}\,\mathbf{P}(\mathsf{K}) \vDash t \approx s$ implies $\mathbf{H}\,\mathbf{S}\,\mathbf{P}(\mathsf{K}) \vDash t \approx s$. □

The original definition of a free group is metamathematical in nature. Specifically a group is *free* if its generators are *free* is the sense they satisfy no equation that is not satisfied by every choice of elements in every group. In its general form for and arbitrary class K of Σ-algebras this idea takes the following form.

Definition 3.21. Let K be a class of Σ-algebra, $\boldsymbol{F}$ a Σ-algebra, and $Y \subseteq F$. $\boldsymbol{F}$ is *free over* K *with free generators* Y if the following two conditions hold.

(i) $F = \mathrm{Sg}^{\boldsymbol{F}}(Y)$.

(ii) For every Σ-equation $t(x_0, \dots, x_{n-1}) \approx s(x_0, \dots, x_{n-1})$ and any choice of pairwise distinct $y_0, \dots, y_{n-1}$ elements of Y,

$$t^{\boldsymbol{F}}(y_0, \dots, y_{n-1}) = s^{\boldsymbol{F}}(y_0, \dots, y_{n-1}) \quad \text{iff} \quad \mathsf{K} \vDash t \approx s.$$

For example, the free group over the free generators $y_0, y_1, \dots, y_\xi, \dots$, $\xi < \lambda$, is usually defined to be the set of all *words*, that is finite sequences of variable symbols, $y_{\xi_0}^{k_0} \cdots y_{\xi_{n-1}}^{k_{n-1}}$, where each y_{ξ_i} is different from the symbol on either side of it (i.e., from $y_{\xi_{i-1}}$ and from $y_{\xi_{i+1}}$), k_i is an arbitary nonzero integer, and $y_{\xi_i}^{k_i}$ denotes the word $\underbrace{y_{\xi_i} y_{\xi_i} \cdots y_{\xi_i}}_{k_i}$ if $k_i > 0$ and the word $\underbrace{y_{\xi_i}^{-1} y_{\xi_i}^{-1} \cdots y_{\xi_i}^{-1}}_{-k_i}$ if $k_i < 0$. The product of the two words $y_{\xi_0}^{k_0} \cdots y_{\xi_{n-1}}^{k_{n-1}}$ and

$y_{\eta_0}^{l_0} \cdots y_{\eta_{n-1}}^{l_{m-1}}$ is defined as follows. Let q be the largest number such that, for all $j < q$, $y_{\xi_{n-j-1}} = y_{\eta_j}$ and $k_{n-j-1} = -l_j$. If $y_{\xi_{n-q-1}} \neq y_{\eta_q}$, then the product is

$$y_{\xi_0}^{k_0} \cdots y_{\xi_{n-q-1}}^{k_{n-q-1}} y_{\eta_q}^{l_q} \cdots y_{\eta_{n-1}}^{l_{m-1}};$$

otherwise, i.e., $y_{\xi_{n-q-1}} = y_{\eta_q}$ but $k_{n-q-1} \neq -l_q$. then the product is

$$y_{\xi_0}^{k_0} \cdots y_{\xi_{n-q-1}}^{k_{n-q-1}+l_q} \cdots y_{\eta_{n-1}}^{l_{m-1}}.$$

For example, the product of $y_0^2\, y_1^{-3}\, y_2^4$ and $y_2^{-4}\, y_1^3\, y_4^{-1}$ is $y_0^2\, y_4^{-1}$, and the product of $y_0^2\, y_1^{-3}\, y_2^4$ and $y_2^{-4}\, y_1^2\, y_4^{-1}$ is $y_0^2\, y_1^{-1}\, y_4^{-1}$. The inverse of $y_{\xi_0}^{k_0} \cdots y_{\xi_{n-1}}^{k_{n-1}}$ is $y_{\xi_{n-1}}^{-k_{n-1}} \cdots y_{\xi_0}^{-k_0}$. The identity if the empty word. It is not difficult to show that the $\{\cdot, {}^{-1}, e\}$-algebra constucted in this way is free over the class of groups with free generators $\{\, y_\xi : \xi < \lambda \,\}$.

The following lemma ties the universal mapping property to the notion of freedom.

Lemma 3.22. *Let* K *be a class of* Σ*-algebras, and assume that* $\boldsymbol{F}$ *is a* Σ*-algebra such that*

(i) $\boldsymbol{F} \in \mathbf{HSP}(\mathsf{K})$*, and*

(ii) $\boldsymbol{F}$ *has the universal mapping property over* K *wrt a set* Y *of generators of* $\boldsymbol{F}$*.*

Then $\boldsymbol{F}$ *if free over* K *with free generators* Y*.*

Proof. Assume (i) and (ii) hold. Then $F = \mathrm{Sg}^{\boldsymbol{F}}(Y)$ by (ii).

Suppose $t^{\boldsymbol{F}}(y_0, \ldots, y_{n-1}) = s^{\boldsymbol{F}}(y_0, \ldots, y_{n-1})$. Let $\boldsymbol{A} \in \mathsf{K}$ and $a_0, \ldots, a_{n-1} \in A$. Let $h^*\colon \boldsymbol{F} \to \boldsymbol{A}$ such that $h^*(y_i) = a_i$ for every $i < n$. Then

$$\begin{aligned} t^{\boldsymbol{A}}(a_0, \ldots, a_{n-1}) &= t^{\boldsymbol{A}}\big(h^*(y_0), \ldots, h^*(y_{n-1})\big) \\ &= h^*\big(t^{\boldsymbol{F}}(y_0, \ldots, y_{n-1})\big) \\ &= h^*\big(s^{\boldsymbol{F}}(y_0, \ldots, y_{n-1})\big) \\ &= s^{\boldsymbol{A}}\big(h^*(y_0), \ldots, h^*(y_{n-1})\big) \\ &= s^{\boldsymbol{A}}(a_0, \ldots, a_{n-1}). \end{aligned}$$

So $\mathsf{K} \vDash t \approx s$.

Now assume $\mathsf{K} \vDash t \approx s$. Then $\mathbf{HSP}(\mathsf{K}) \vDash t \approx s$ by Thm. 3.20. Thus $\boldsymbol{F} \vDash t \approx s$ and hence $t^{\boldsymbol{F}}(y_0, \ldots, y_{n-1}) = s^{\boldsymbol{F}}(y_0, \ldots, y_{n=1})$. □

The converse this lemma holds we cannot prove it now.

We want to prove that free algebras over every class exist with any given cardinality λ of free generators. It turns out that the λ-ary clone algebra $\mathrm{Clo}_\lambda(\boldsymbol{F})$ has this property for any algebra $\boldsymbol{F} \in \mathbf{HSP}(\mathsf{K})$ with the property that every algebra of K is a homomorphic image of $\boldsymbol{F}$. Clearly the product $\prod_{\boldsymbol{A} \in \mathsf{K}} \boldsymbol{A}$ has this property since every algebra in K is a homomorphic image of it by projection. The problem is that such a product does not exist because it is too big if K is a proper class. But for $\boldsymbol{F}$ to serve our purpose we do not need for every algebra of K to be a homomorphic image of $\boldsymbol{F}$, but only the subalgebras of members of K that can be generated my at most λ generators. Algebras $\boldsymbol{F}$ with this property do exist. One of them is the following algebra, as we shall see.

$$\prod\nolimits_\lambda^* \mathsf{K} := \prod \big\{\, \mathbf{Te}_\Sigma(X_\lambda)/\alpha : \alpha \in \mathrm{Co}(\mathbf{Te}_\Sigma(X_\lambda), \mathbf{Te}_\Sigma(X_\lambda)/\alpha \in \mathbf{IS}(\mathsf{K}) \,\big\}.$$

Lemma 3.23. *Let* K *be a class of* Σ*-algebras and* λ *a cardinal.*

(i) $\prod^*_\lambda \mathsf{K} \in \mathbf{P}\,\mathbf{S}(\mathsf{K})$.

(ii) *For every* $\boldsymbol{A} \in \mathsf{K}$ *and every* $\boldsymbol{B} \subseteq \boldsymbol{A}$ *such that* $\boldsymbol{B}$ *is generated by at most* λ *elements we have* $\boldsymbol{B} \preccurlyeq \prod^*_\lambda \mathsf{K}$.

Proof. (i) $\prod^*_\lambda \mathsf{K} \in \mathbf{P}\{\, \mathbf{Te}_\Sigma(X_\lambda)/\alpha : \alpha \in \mathrm{Co}\big(\mathbf{Te}_\Sigma(X_\lambda)\big), \mathbf{Te}_\Sigma(X_\lambda)/\alpha \in \mathbf{I}\,\mathbf{S}(\mathsf{K}) \,\} \subseteq \mathbf{P}\,\mathbf{I}\,\mathbf{S}(\mathsf{K}) = \mathbf{P}\,\mathbf{S}(\mathsf{K})$.

(ii) Let $\boldsymbol{B} \in \mathbf{S}(\mathsf{K})$ such that $\boldsymbol{B}$ is generated by at most λ elements. Then by Theorem thm:w6.1(iii) there exists a surjective mapping from the set of variables X_λ onto the generators of $\boldsymbol{B}$, which extends (uniquely) to an epimorphism h^* from $\mathbf{Te}_\Sigma(X_\lambda)$ onto $\boldsymbol{B}$. By the Isomorphism Theorem $h^*_\alpha\colon \mathbf{Te}_\Sigma(X_\lambda)/\alpha \cong \boldsymbol{B}$, where $\alpha = \mathrm{rker}(h^*)$. So $\mathbf{Te}_\Sigma(X_\lambda)/\alpha \in \mathbf{I}\,\mathbf{S}(\mathsf{K})$, and hence $\mathbf{Te}_\Sigma(X_\lambda)/\alpha$ is one of the factors in the direct product $\prod^*_\lambda \mathsf{K}$ and consequently is a homormorphic image of $\prod^*_\lambda \mathsf{K}$ under one of the projection mappings. Hence $\boldsymbol{B}$ is a homomorphic image of $\prod^*_\lambda \mathsf{K}$. □

Definition 3.24. Let K be a class of Σ-algebras, and let λ be a cardinal. Set

$$\mathbf{Fr}_\lambda(\mathsf{K}) := \mathbf{Clo}_\lambda\big(\prod^*_\lambda \mathsf{K}\big).$$

This is called the *free algebra of* K *of dimension* α.

Theorem 3.25. *Let* K *be a class of* Σ*-algebras and* λ *a cardinal.* $\mathbf{Fr}_\lambda(\mathsf{K})$ *is a free algebra over* K *with free generators* $X^{\mathsf{K}}_\lambda = \{\, x^{\mathsf{K}}_\xi : \xi < \lambda \,\}$.

Proof. By Lemma 3.22 it suffices to prove (1) $\mathbf{Fr}_\lambda(\mathsf{K}) \in \mathbf{H}\,\mathbf{S}\,\mathbf{P}(\mathsf{K})$, and (2) $\mathbf{Fr}_\lambda(\mathsf{K})$ has the universal mapping property over K wrt X^{K}_λ.

(1) By Theorem 3.17 and Lemma 3.23

$$\mathbf{Clo}_\lambda\big(\prod^*_\lambda \mathsf{K}\big) \in \mathbf{S}\,\mathbf{P}\big(\prod^*_\lambda \mathsf{K}\big) \subseteq \mathbf{S}\,\mathbf{P}\,\mathbf{P}\,\mathbf{S}(\mathsf{K}) \subseteq \mathbf{S}\,\mathbf{S}\,\mathbf{P}\,\mathbf{P}(\mathsf{K}) = \mathbf{S}\,\mathbf{P}(\mathsf{K}) \subseteq \mathbf{H}\,\mathbf{S}\,\mathbf{P}(\mathsf{K}).$$

(2) Let $\boldsymbol{A} \in \mathsf{K}$ and let $h\colon X^{\mathsf{K}}_\lambda \rightarrowtail A$. Let $\boldsymbol{A'}$ be the subalgebra of $\boldsymbol{A}$ generated by the image $h(X^{\mathsf{K}}_\lambda)$. Since $\boldsymbol{A'}$ is generated by at most λ elements, $\boldsymbol{A'} \preccurlyeq \prod^*_\lambda \mathsf{K}$ by Lemma 3.22(ii). So $\boldsymbol{A'} \in \mathbf{H}(\prod^*_\lambda \mathsf{K})$. Hence by Thm. 3.16 $\mathbf{Fr}_\lambda(\mathsf{K})$, which, as we recall, is $\mathrm{Clo}_\lambda\big(\prod^*_\lambda(\mathsf{K})\big)$, has the universal mapping property over $\boldsymbol{A'}$ wrt X^{K}_λ. Thus h can be extended to a epimorphism $h^*\colon \mathbf{Fr}_\lambda(\mathsf{K}) \twoheadrightarrow \boldsymbol{A'}$ (it is surjective since $\boldsymbol{A'}$ is generated by $h(X^{\mathsf{K}}_\lambda)$), and hence, again identifying h^* with its graph, $h^*\colon \mathbf{Fr}_\lambda(\mathsf{K}) \rightarrowtail \boldsymbol{A}$ and $h^* \restriction X^{\mathsf{K}}_\lambda$. So $\mathbf{Fr}_\lambda(\mathsf{K})$ has the UMP over K wrt X^{K}_λ. □

3.3. **Reduced Products and Ultraproducts.** Let I be a nonempty set. Let

$$\boldsymbol{\mathcal{P}}(I) = \langle \mathcal{P}(I), \cup, \cap, \overline{\ }, \emptyset, I \rangle,$$

where, for every $X \subseteq I$, $\overline{X} = I \setminus X$ is the *complement* of X relative to I. $\boldsymbol{\mathcal{P}}(I)$ is the Boolean algebra of all subsets of I. $\mathcal{F} \subseteq \mathcal{P}(I)$ is a *filter on* or *over* I if $\mathcal{F}$ is a dual ideal of the lattice $\langle \mathcal{P}(I), \cup, \cap, \emptyset, I \rangle$, i.e.,

(i) $\mathcal{F}$ is nonempty;
(ii) $\mathcal{F}$ is an upper segment, i.e., $X \in \mathcal{F}$ and $X \subseteq Y$ implies $Y \in \mathcal{F}$;
(iii) $\mathcal{F}$ is closed under intersection, i.e., $X, Y \in \mathcal{F}$ implies $X \cap Y \in \mathcal{F}$.

The set of filters of I is an algebraic closed-set system, since the set of ideals of any lattice forms one. Because of (ii), the condition (i) is equivalent to $I \in \mathcal{F}$. A filter $\mathcal{F}$ is *proper* if $\mathcal{F} \neq \mathcal{P}(I)$. Because of (ii), $\mathcal{F}$ is proper iff $\emptyset \notin \mathcal{F}$. Thus the union of any chain of proper filters is a proper filter, and consequently Zorn's lemma can be applied to show that every proper filter $\mathcal{F}$ is included in a maximal proper filter, that is, a proper filter $\mathcal{U}$ such that there is no filter $\mathcal{G}$ such that $\mathcal{U} \subset \mathcal{G} \subset \mathcal{P}(I)$. Maximal proper filters are called *ultrafilters*.

Examples:

(1) For $J \subseteq I$, $\mathcal{P}(I)[J) = \{ X : J \subseteq X \subseteq I \}$ is the *principal filter generated by* J; for simplicity we normally write $[J)$ for $\mathcal{P}(I)[J)$. A filter $\mathcal{F}$ is principal iff $\bigcap \mathcal{F} \,(= \bigcap \{ F : F \in \mathcal{F} \}) \in \mathcal{F}$, in which case $\mathcal{F} = [\bigcap \mathcal{F})$. Thus, if I is finite, every filter $\mathcal{F}$ on I is principal. The smallest filter is $[I) = \{I\}$ and the largest filter, the improper filter, is $[\emptyset) = \mathcal{P}(I)$.

(2) Every nonprincipal filter must be over an infinite set. A subset X of I is *cofinite* if $\overline{X}$ is finite. Let $\mathcal{C}f$ be the set of all cofinite subsets of I. Clearly I is cofinite, and any superset of a cofinite set is cofinite. If X and Y are cofinite, then $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$ is finite, and hence $\mathcal{C}f$ is closed under intersection. So $\mathcal{C}f$ is a filter. $\emptyset$ is cofinite iff I is finite. So $\mathcal{C}f$ is proper iff I is infinite. For each $i \in I$, $\overline{\{i\}}$ is obviously cofinite. Thus $\bigcap \mathcal{C}f \subseteq \bigcap_{i \in I} \overline{\{i\}} = \emptyset$. Hence $\mathcal{C}f$ is nonprincipal if I is infinite.

Lemma 3.31. *Let I be a set, and let $\mathcal{K}$ be an arbitrary set of subsets of I. Let $\mathcal{F}$ be the filter generated by $\mathcal{K}$, i.e., $\mathcal{F} := \bigcap \{ \mathcal{G} : \mathcal{G}$ a filter such that $\mathcal{K} \subseteq \mathcal{G} \}$. Then*

$$\mathcal{F} = \{ X : \exists\, n \in \omega \, \exists\, K_1, \ldots, K_n \in \mathcal{K} (K_1 \cap \cdots \cap K_n \subseteq X) \}.$$

Proof. Let $\mathcal{H} = \{ X : \exists\, n \in \omega \, \exists\, K_1, \ldots, K_n \in \mathcal{K} (K_1 \cap \cdots \cap K_n \subseteq X) \}$. If $\mathcal{K}$ is empty, then the only sequence $K_1, \ldots, K_n$ of members of $\mathcal{K}$ is the empty sequence (n=0). Then, by definition of the intersection of an empty sequence, $K_1 \cap \cdots \cap K_n = I$. Thus $I \in \mathcal{H}$, and in fact $\mathcal{H} = [I) = \{I\}$, the smallest filter. And $\mathcal{F} = \{I\}$, being in this case the intersection of all filters.

Now suppose $\mathcal{K}$ is nonempty. We first verify that $\mathcal{H}$ is a filter that includes $\mathcal{K}$. For each $K_1 \in \mathcal{K}$, $K_1 \subseteq K_1$, and hence $K_1 \in \mathcal{H}$. Thus $\mathcal{K} \subseteq \mathcal{F}$. If $\mathcal{K}$ is nonempty, so is $\mathcal{H}$. Suppose $X \in \mathcal{H}$; say $K_1 \cap \cdots \cap K_n \subseteq X$ with $K_1, \ldots, K_n \in \mathcal{K}$. Then $K_1 \cap \cdots \cap K_n \subseteq Y$, and hence $Y \in \mathcal{H}$, for every Y such that $X \subseteq Y$. So $\mathcal{H}$ is an upper segment. Suppose $X, Y \in \mathcal{H}$. Then $K_1 \cap \cdots \cap K_n \subseteq X$ and $L_1 \cap \cdots \cap L_m \subseteq Y$ with $K_1, \ldots, K_n, L_1, \ldots, L_m \in \mathcal{K}$. Then $K_1 \cap \cdots \cap K_n \cap L_1 \cap \cdots \cap L_m \subseteq X \cap Y$. So $X \cap Y \in \mathcal{H}$, and hence $\mathcal{H}$ is closed under intersection. Thus $\mathcal{H}$ is a filter.

We have seen that $\mathcal{K} \subseteq \mathcal{H}$. Let $\mathcal{G}$ be a filter such that $\mathcal{K} \subseteq \mathcal{G}$. Then $K_1 \cap \cdots \cap K_n \in \mathcal{G}$ for all $K_1, \ldots, K_n \in \mathcal{K}$, and hence $X \in \mathcal{G}$ for every X such that $K_1 \cap \cdots \cap K_n \subseteq X$, since $\mathcal{G}$ is an upper segment. So $\mathcal{H} \subseteq \mathcal{G}$. Thus $\mathcal{H} = \mathcal{F}$. □

Corollary 3.32. *Let $\mathcal{F}$ is a filter over I, and let $X \in \mathcal{P}(I)$. Let $\mathcal{G}$ be the smallest filter including $\mathcal{F}$ that contains X, i.e., the filter generated by $\mathcal{K} = \mathcal{F} \cup \{X\}$. Then*

$$\mathcal{G} = \{\, Y \subseteq I : \exists\, F \in \mathcal{F}\, (F \cap X \subseteq Y) \,\}.$$

Proof. Let $\mathcal{H} = \{\, Y \subseteq I : \exists\, F \in \mathcal{F}\, (F \cap X \subseteq Y) \,\}$. By the lemma, $\mathcal{G} = \{Y \subseteq I : \exists n \in \omega\, \exists\, K_1, \ldots, K_n \in \mathcal{F} \cup \{X\}\, (K_1 \cap \cdots \cap K_n \subseteq Y) \,\}$. Clearly $\mathcal{H} \subseteq \mathcal{G}$. Let $Y \in \mathcal{G}$. Then

$$K_1 \cap \cdots \cap K_n \subseteq Y, \tag{26}$$

for some $K_1, \ldots, K_n \in \mathcal{F} \cup \{X\}$. Suppose $X = K_i$ for some $i \leq n$; without loss of generality assume $X = K_n$. Then

$$K_1 \cap \cdots \cap K_n = \underbrace{K_1 \cap \cdots \cap K_{n-1}}_{F \in \mathcal{F}} \cap X \subseteq Y.$$

So $Y \in \mathcal{H}$. If $X \neq K_i$ for all $i \leq n$, then $K_1 \cap \cdots \cap K_n = F \in \mathcal{F}$, and hence (26) implies $F \cap X \subseteq Y$. So again $Y \in \mathcal{H}$. So $\mathcal{G} \subseteq \mathcal{H}$. □

Corollary 3.33. *Let $\mathcal{K} \subseteq \mathcal{P}(I)$. Then $\mathcal{K}$ is included in a proper filter and hence an ultrafilter iff, for all $n \in \omega$ and all $K_1, \ldots, K_n \in \mathcal{K}$, $K_1 \cap \cdots \cap K_n \neq \emptyset$.*

Proof. Exercise. □

A set $\mathcal{K}$ of subsets of a nonempty set I is said to have the *finite intersection property* if the intersection of every finite subset of $\mathcal{K}$ is nonempty. By the above corollary, every set of subsets of I with this property is included in a proper filter.

The following gives a convenient characterization of ultrafilters.

Theorem 3.34. *Let $\mathcal{F}$ be a filter over a set I. $\mathcal{F}$ is an ultrafilter iff*

$$\text{for every } X \subseteq I, \text{ either } X \in \mathcal{F} \text{ or } \overline{X} \in \mathcal{F}, \text{ but not both.} \tag{27}$$

Proof. $\Longleftarrow$ Assume (27) holds. Then $\emptyset \notin \mathcal{F}$ since $I \in \mathcal{F}$ and $\emptyset = \overline{I}$. So $\mathcal{F}$ is proper. Let $\mathcal{G}$ be a filter such that $\mathcal{F} \subset \mathcal{G}$. Let $X \in \mathcal{G} \setminus \mathcal{F}$. Then by (27) $\overline{X} \in \mathcal{F} \subseteq \mathcal{G}$. Thus $\emptyset = X \cap \overline{X} \in \mathcal{G}$, i.e., $\mathcal{G} = \mathcal{P}(I)$. Thus $\mathcal{F}$ is an ultrafilter.

$\Longrightarrow$ Suppose $\mathcal{F}$ is an ultrafilter and $X \notin \mathcal{F}$. Since $\mathcal{F}$ is maximal and proper, $\mathcal{P}(I)$ is smallest filter including $\mathcal{F}$ that contains X. By Cor. 3.32 $\mathcal{P}(I) = \{\, Y \subseteq I : \exists\, F \in \mathcal{F}\, (F \cap X \subseteq Y) \,\}$. Thus there is an $F \in \mathcal{F}$ such that $F \cap X = \emptyset$. So $F \subseteq \overline{X}$, and hence $\overline{X} \in \mathcal{F}$. □

Exercises:

(1) A principal filter $[X)$ is an ultrafilter iff $|X| = 1$.

The filter $\mathcal{C}f$ of cofinite sets is never an ultrafilter. If I is finite, $\mathcal{C}f$ is the improper filter. If I if infinite, then I includes a set X such that neither X nor $\overline{X}$ is finite, and hence neither X nor $\overline{X}$ is cofinite.

(2) Let I be infinite. Then $\mathcal{C}f$ is the smallest nonprincipal filter on I, i.e., for any filter $\mathcal{F}$ on I, $\mathcal{F}$ is nonprincipal iff $\mathcal{C}f \subseteq \mathcal{F}$.

Let $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ be a system of Σ-algebras, and let $\mathcal{F}$ be a filter on I. Define $\Phi(\mathcal{F}) \subseteq \left(\prod_{i\in I} A_i\right)^2$ by the condition that

$$\Big\langle \underbrace{\langle\, a_i : i \in I \,\rangle}_{\vec{a}}, \underbrace{\langle\, b_i : i \in I \,\rangle}_{\vec{b}} \Big\rangle \in \Phi(\mathcal{F}) \quad \text{iff} \quad \underbrace{\{\, i \in I : a_i = b_i \,\}}_{\mathrm{EQ}(\vec{a},\vec{b})} \in \mathcal{F},$$

where $\mathrm{EQ}(\vec{a},\vec{b}) := \{\, i \in I : a_i = b_i \,\}$ is called the *equality set* of $\vec{a}$ and $\vec{b}$. Note that $\langle \vec{a}, \vec{b} \rangle \in \Phi(\mathcal{C}f)$ iff $\mathrm{EQ}(\vec{a},\vec{b})$ is cofinite, i.e., iff $\{\, i \in I : a_i \neq b_i \,\}$ is finite. It is traditional to say that $\vec{a}$ and $\vec{b}$ are equal "almost everywhere" in this case.

Lemma 3.35. *$\Phi(\mathcal{F}) \in \mathrm{Co}(\prod_{i\in I} \boldsymbol{A}_i)$ for every filter $\mathcal{F}$ on I.*

Proof. $\mathrm{EQ}(\vec{a},\vec{a}) = I \in \mathcal{F}$. So $\Phi(\mathcal{F})$ is reflexive, and it is symmetric because $\mathrm{EQ}(\vec{a},\vec{b}) = \mathrm{EQ}(\vec{b},\vec{a})$.

$$\underbrace{i \in \mathrm{EQ}(\vec{a},\vec{b})}_{a_i=b_i} \quad \text{and} \quad \underbrace{i \in \mathrm{EQ}(\vec{b},\vec{c})}_{b_i=c_i} \quad \text{implies} \quad \underbrace{i \in \mathrm{EQ}(\vec{a},\vec{c})}_{a_i=c_i}.$$

I.e., $\mathrm{EQ}(\vec{a},\vec{b}) \cap \mathrm{EQ}(\vec{b},\vec{c}) \subseteq \mathrm{EQ}(\vec{a},\vec{c})$. So if $\mathrm{EQ}(\vec{a},\vec{b})$ and $\mathrm{EQ}(\vec{b},\vec{c})$ are both in $\mathcal{F}$, then so is $\mathrm{EQ}(\vec{a},\vec{c})$. This means that $\Phi(\mathcal{F})$ is transitive.

Let $\sigma \in \Sigma_n$ and $\vec{a}_1, \ldots, \vec{a}_n, \vec{b}_1, \ldots, \vec{b}_n \in \prod_{i\in I} A_i$ such that $\mathrm{EQ}(\vec{a}_1,\vec{b}_1), \ldots, \mathrm{EQ}(\vec{a}_n,\vec{b}_n) \in \mathcal{F}$. Then as in the proof of transitivity it can be shown that $\mathrm{EQ}(\vec{a}_1,\vec{b}_1) \cap \cdots \cap \mathrm{EQ}(\vec{a}_n,\vec{b}_n) \subseteq \mathrm{EQ}\big(\sigma^{\prod \boldsymbol{A}_i}(\vec{a}_1,\ldots,\vec{a}_n), \sigma^{\prod \boldsymbol{A}_i}(\vec{b}_1,\ldots,\vec{b}_n)\big) \in \mathcal{F}$. So $\Phi(\mathcal{F})$ has the substitution property. □

$\Phi(\mathcal{F})$ is called the *filter congruence defined by $\mathcal{F}$*.

Definition 3.36. Let $\vec{\boldsymbol{A}} = \langle\, \boldsymbol{A}_i : i \in I \,\rangle$ be a system of Σ-algebras. A Σ-algebra $\boldsymbol{B}$ is a *reduced product of $\vec{\boldsymbol{A}}$* if $\boldsymbol{B} = \big(\prod_{i\in I} \boldsymbol{A}_i\big)/\Phi(\mathcal{F})$ for some filter $\mathcal{F}$ on I. $\boldsymbol{B}$ is called an *ultraproduct of $\vec{\boldsymbol{A}}$* if $\mathcal{F}$ is an ultrafilter.

Note that $\boldsymbol{B} \preccurlyeq \prod_{i\in I} \boldsymbol{A}_i$, i.e., $\boldsymbol{B}$ is a homomorphic image of $\prod_{i\in I} \boldsymbol{A}_i$, but it is a very special kind of homomorphic image as we shall see. For any Σ-algebra $\boldsymbol{C}$, we write $\boldsymbol{C} \preccurlyeq_{\mathrm{R}} \prod_{i\in I} \boldsymbol{A}_i$ if $\boldsymbol{C}$ is isomorphic to a reduced product of $\vec{\boldsymbol{A}}$; by the First Isomorphism Theorem, $\boldsymbol{C} \preccurlyeq_{\mathrm{R}} \prod_{i\in I} \boldsymbol{A}_i$ iff $\boldsymbol{C}$ is a homomorphic image of $\prod_{i\in I} \boldsymbol{A}_i$ by a homomorphism whose relation kernel is a filter congruence. We write $\boldsymbol{C} \preccurlyeq_{\mathrm{U}} \prod_{i\in I} \boldsymbol{A}_i$ if $\boldsymbol{C}$ is isomorphic to a ultraproduct of $\vec{\boldsymbol{A}}$.

For any class K of Σ-algebras,

$$\mathbf{P}_{\mathrm{R}}(\mathsf{K}) := \Big\{\, \boldsymbol{B} : \exists\, I\, \exists\, \vec{\boldsymbol{A}} \in \mathsf{K}^I \,(\boldsymbol{B} \preccurlyeq_{\mathrm{R}} \prod_{i\in I} \boldsymbol{A}_i) \,\Big\}.$$

$\mathbf{P}_{\mathrm{U}}(\mathsf{K})$ is similarly defined with "$\preccurlyeq_{\mathrm{U}}$" in place of "$\preccurlyeq_{\mathrm{R}}$".

Let I be a set and $\mathcal{F}$ a filter on I. Let $J \subseteq I$ and define

$$\mathcal{F}{\restriction}J := \{\, F \cap J : F \in \mathcal{F} \,\}.$$

$\mathcal{F}{\restriction}J$ is a filter on J: we verify the three defining properties of a filter.

$J = I \cap J \in \mathcal{F}{\restriction}J$. Suppose $X \in \mathcal{F}{\restriction}J$ and $X \subseteq Y \subseteq J$. Let $F \in \mathcal{F}$ such that $X = F \cap J$. Then $F \cup Y \in \mathcal{F}$ and $Y = X \cup Y = (F \cap J) \cup (Y \cap J) = (F \cup Y) \cap J \in \mathcal{F}{\restriction}J$. Finally, suppose $X, Y \in \mathcal{F}{\restriction}J$, and let $F, G \in \mathcal{F}$ such that $X = F \cap J$ and $Y = G \cap J$. Then $X \cap Y = (F \cap G) \cap J \in \mathcal{F}{\restriction}J$.

It is easy to see that, if $J \in \mathcal{F}$, then

$$\mathcal{F}\restriction J = \mathcal{P}(J) \cap \mathcal{F} (= \{\, X \subseteq J : X \in \mathcal{F} \,\}).$$

The inclusion from right to left holds for all $J \subseteq I$, without the assumption that $J \in \mathcal{F}$. Assume, $X \in \mathcal{F}\restriction J$, i.e., $X = F \cap J$ for some $F \in \mathcal{F}$. Then $X \in \mathcal{F}$ since $J \in \mathcal{F}$.

The following will prove useful in the sequel.

(28) If $J \in \mathcal{F}$, then $\forall\, X \subseteq I (X \in \mathcal{F} \quad \text{iff} \quad X \cap J \in \mathcal{F}\restriction J)$.

$X \in \mathcal{F}$ implies $X \cap J \in \mathcal{F}\restriction J$ by the definition of $\mathcal{F}\restriction J$. For the implication in the other direction, assume $X \cap J \in \mathcal{F}\restriction J$. Then, since $J \in \mathcal{F}$, $X \cap J \in \mathcal{F}$ by the above characterization of $\mathcal{F}\restriction J$ when $J \in \mathcal{F}$. Hence $X \in \mathcal{F}$ since $\mathcal{F}$ is an upper segment.

Lemma 3.37. *Let $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ be a system of Σ-algebras and $\mathcal{F}$ a filter on I. Then, for each $J \in \mathcal{F}$,*

$$\Big(\prod_{i\in I} \boldsymbol{A}_i\Big)/\Phi(\mathcal{F}) \cong \Big(\prod_{j\in J} \boldsymbol{A}_j\Big)/\Phi(\mathcal{F}\restriction J).$$

Proof. Consider the epimorphisms

$$\prod_{i\in I} \boldsymbol{A}_i \overset{\pi_J}{\twoheadrightarrow} \prod_{j\in J} \boldsymbol{A}_j \overset{\Delta_{\Phi(\mathcal{F}\restriction J)}}{\twoheadrightarrow} \Big(\prod_{j\in J} \boldsymbol{A}_j\Big)/\Phi(\mathcal{F}\restriction J),$$

where $\pi_J(\underbrace{\langle\, a_i : i \in I \,\rangle}_{\vec{a}}) = \underbrace{\langle\, a_j : j \in J \,\rangle}_{\vec{a}\restriction J}$. π_J is the *J-projection function*, and it is easily checked that it is an epimorphism; it generalizes the ordinary projection function π_i, which can be identified with $\pi_{\{i\}}$. $\Delta_{\Phi(\mathcal{F}\restriction J)}$ is of course the natural map.

Let $h = \Delta_{\Phi(\mathcal{F}\restriction J)} \circ \pi_J \colon \prod_{i\in I} \boldsymbol{A}_i \twoheadrightarrow \big(\prod_{j\in J} \boldsymbol{A}_j\big)/\Phi(\mathcal{F}\restriction J)$. Let $\vec{a} = \langle\, a_i : i \in I \,\rangle$ and $\vec{b} = \langle\, b_i : i \in I \,\rangle$.

$$\begin{aligned}
\langle \vec{a}, \vec{b} \rangle \in \operatorname{rker}(h) \quad &\text{iff} \quad \Delta_{\Phi(\mathcal{F}\restriction J)}(\vec{a}\restriction J) = \Delta_{\Phi(\mathcal{F}\restriction J)}(\vec{b}\restriction J) \\
&\text{iff} \quad \langle \vec{a}\restriction J, \vec{b}\restriction J \rangle \in \Phi(\mathcal{F}\restriction J) \\
&\text{iff} \quad \operatorname{EQ}(\vec{a}\restriction J, \vec{b}\restriction J)\, (= \{\, j \in J : a_j = b_j \,\}) \in \mathcal{F}\restriction J \\
&\text{iff} \quad \operatorname{EQ}(\vec{a}, \vec{b})\, (= \{\, i \in I : a_i = b_i \,\}) \in \mathcal{F};
\end{aligned}$$

this last equivalence holds by (28) since $\operatorname{EQ}(\vec{a}\restriction J, \vec{b}\restriction J) = \operatorname{EQ}(\vec{a}, \vec{b}) \cap J$

$$\text{iff} \quad \langle \vec{a}, \vec{b} \rangle \in \Phi(\mathcal{F}).$$

So $\operatorname{rker}(h) = \Phi(\mathcal{F})$. Now apply the First Isomorphism Theorem. □

By the next lemma, a product $\prod_{i\in I} \boldsymbol{A}_i$ that is reduced by the filter congruence defined by the filter of cofinite sets is a model of a given identity iff the factor $\boldsymbol{A}_i$ is a model of the identity for "almost all" i.

Lemma 3.38. *Let $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ be a system of Σ-algebras, and let $\mathcal{F}$ be a filter on I. Let ε be an arbitrary Σ-equation. Then*

$$\Big(\prod_{i\in I} \boldsymbol{A}_i\Big)/\Phi(\mathcal{F}) \vDash \varepsilon \quad \textit{iff} \quad \{\, i \in I : \boldsymbol{A}_i \vDash \varepsilon \,\} \in \mathcal{F}.$$

Proof. Let $J = \{\, i \in I : \boldsymbol{A}_i \vDash \varepsilon \,\}$.

$\Longleftarrow$ Assume $J \in \mathcal{F}$. Then by Lem. 3.37, $\big(\prod_{i\in I} \boldsymbol{A}_i\big)/\Phi(\mathcal{F}) \cong \big(\prod_{j\in J} \boldsymbol{A}_j\big)/\Phi(\mathcal{F}{\restriction}J) \in \mathbf{H}\,\mathbf{P}(\{\, \boldsymbol{A}_j : j \in J \,\}) \subseteq \mathbf{H}\,\mathbf{P}(\mathsf{Mod}(\varepsilon)) = \mathsf{Mod}(\varepsilon)$; the last equality holds by Thm. 3.20. Thus $\big(\prod_{i\in I} \boldsymbol{A}_i\big)/\Phi(\mathcal{F}) \vDash \varepsilon$.

$\Longrightarrow$ Suppose $J \notin \mathcal{F}$. Let $\varepsilon = t(x_0, \dots, x_{n-1}) \approx s(x_0, \dots, x_{n-1})$. For each $i \in I \setminus J$, choose $a_0(i), \dots, a_{n-1}(i) \in A_i$ such that $t^{\boldsymbol{A}_i}\big(a_0(i), \dots, a_{n-1}(i)\big) \neq s^{\boldsymbol{A}_i}\big(a_0(i), \dots, a_{n-1}(i)\big)$. This is possible since $\boldsymbol{A}_i \nvDash \varepsilon$. For each $i \in J$, let $a_0(i), \dots, a_{n-1}(i)$ be arbitrary elements of $\boldsymbol{A}_i$. Let $\vec{a}_0 = \langle\, \vec{a}_0(i) : i \in I \,\rangle, \dots, \vec{a}_{n-1} = \langle\, \vec{a}_{n-1}(i) : i \in I \,\rangle$. Recall, that

$$t^{\prod \boldsymbol{A}_i}(\vec{a}_0, \dots, \vec{a}_{n-1}) = \big\langle\, t^{\boldsymbol{A}_i}\big(\vec{a}_0(i), \cdots, \vec{a}_{n-1}(i)\big) : i \in I \,\big\rangle \text{ and}$$
$$s^{\prod \boldsymbol{A}_i}(\vec{a}_0, \dots, \vec{a}_{n-1}) = \big\langle\, s^{\boldsymbol{A}_i}\big(\vec{a}_0(i), \cdots, \vec{a}_{n-1}(i)\big) : i \in I \,\big\rangle.$$

Thus

$$\begin{aligned}
&\mathrm{EQ}\big(t^{\prod \boldsymbol{A}_i}(\vec{a}_0, \dots, \vec{a}_{n-1}),\, s^{\prod \boldsymbol{A}_i}(\vec{a}_0, \dots, \vec{a}_{n-1})\big) \\
&\quad = \{\, i \in I : t^{\boldsymbol{A}_i}\big(\vec{a}_0(i), \cdots, \vec{a}_{n-1}(i)\big) = s^{\boldsymbol{A}_i}\big(\vec{a}_0(i), \cdots, \vec{a}_{n-1}(i)\big) \,\} \\
&\quad \subseteq J.
\end{aligned}$$

So $\mathrm{EQ}\big(t^{\prod \boldsymbol{A}_i}(\vec{a}_0, \dots, \vec{a}_{n-1}),\, s^{\prod \boldsymbol{A}_i}(\vec{a}_0, \dots, \vec{a}_{n-1})\big) \notin \mathcal{F}$ since $J \notin \mathcal{F}$. Hence

$$t^{\left(\prod A_i\right)/\Phi(\mathcal{F})}\big(\vec{a}_0/\Phi(\mathcal{F}), \dots, \vec{a}_{n-1}/\Phi(\mathcal{F})\big) \neq s^{\left(\prod A_i\right)/\Phi(\mathcal{F})}\big(\vec{a}_0/\Phi(\mathcal{F}), \dots, \vec{a}_{n-1}/\Phi(\mathcal{F})\big),$$

and hence $\big(\prod_{i\in I} \boldsymbol{A}_i\big)/\Phi(\mathcal{F}) \nvDash \varepsilon$. □

A set E of Σ-equations is *consistent* if $\mathsf{Mod}(E)$ contains a nontrivial algebra.

Let $X \subseteq \omega\backslash\{0\}$. Let E consist of the five laws of groups (of type II) (i.e. $x{\cdot}(y{\cdot}z) \approx (x{\cdot}y){\cdot}z$, $x \cdot e \approx x$, $e \cdot x \approx x$, $x \cdot x^{-1} \approx e$, $x^{-1} \cdot x \approx e$), together with the law $x^n \approx e$ for each $n \in X$. E is consistent iff $\mathrm{GCD}(X) > 1$. Indeed, let $n = \mathrm{GCD}(X)$. Then $\boldsymbol{A}$ is a model of E iff $\boldsymbol{A}$ is a group and every element of $\boldsymbol{A}$ is of finite order dividing n. Thus $\mathbb{Z}_n$ is a nontrivial model of E if $n > 1$, and the trivial group is the only model of E if $n = 1$. Clearly $\mathrm{GCD}(X) = 1$ iff $\mathrm{GCD}(X') = 1$ for some finite $X' \subseteq X$. Thus

$$E \text{ is inconsistent iff some finite subset of } E \text{ is inconsistent.}$$

This result might appear to depend on special properties of the groups and of the ring of integers, but in fact it is but special case of a much more general result.

Theorem 3.39 (Compactness Theorem of Equational Logic)**.** *A set of Σ-equations is consistent iff every finite subset is consistent.*

Proof. The implication from left to right is trivial. For the opposite implication, assume E is a set of equations such that every finite subset of E is consistent. We also assume E is infinite, since otherwise it is trivially consistent. Let $\mathcal{P}_\omega(E)$ be the set of all finite subsets of E. Then by assumption each $E' \in \mathcal{P}_\omega(E)$ has a nontrivial model, say $\boldsymbol{A}_{E'}$. Consider the $\mathcal{P}_\omega(E)$-indexed system of Σ-algebras $\langle\, \boldsymbol{A}_{E'} : E' \in \mathcal{P}_\omega(E) \,\rangle$ and their direct product $\prod_{E' \in \mathcal{P}_\omega(E)} \boldsymbol{A}_{E'}$. Notice that, for each $\varepsilon \in E$, $\boldsymbol{A}_{E'}$ is a model of ε for every $E' \in \mathcal{P}_\omega(E)$ such that $\varepsilon \in E'$. We will see that there is a proper filter $\mathcal{F}$ on $\mathcal{P}_\omega(E)$ (and hence a subset of $\mathcal{P}\big(\mathcal{P}_\omega(E)\big)$) such that the set of all such E' is a member of $\mathcal{F}$. Thus by Lem. 3.38 the reduced product $\big(\prod_{E' \in \mathcal{P}_\omega(E)} \boldsymbol{A}_{E'}\big)/\Phi(\mathcal{F})$ is a model of every ε in E. The construction of $\mathcal{F}$ is straightforward, but is complicated by the fact that the index set is a set of sets (in fact a set of finite sets) rather than a simple set.

For each $E' \in \mathcal{P}_\omega(E)$, let $[E')$ be the set of all finite subsets of E that include E', i.e.,

$$[E') = \{\, F : E' \subseteq F \in \mathcal{P}_\omega(E) \,\} \in \mathcal{P}\big(\mathcal{P}_\omega(E)\big).$$

$[E')$ is the principal filter generated by E' in the lattice $\langle \mathcal{P}_\omega(E), \cup, \cap \rangle$ of finite subsets of E. (Although it plays no role in our proof, we note that this lattice is not complete because it has no upper bound. We also note that although $[E')$ consists of finite sets it is itself infinite.) Let $\mathcal{K} = \{\, [E') : E' \in \mathcal{P}_\omega(E) \,\}$. Consider any finite set $[E'_1), \ldots, [E'_n)$ of elements of $\mathcal{K}$. $E'_i \subseteq E'_1 \cup \cdots \cup E'_n$ for each $i \leq n$. Thus $E'_1 \cup \cdots \cup E'_n \in [E'_1) \cap \cdots \cap [E'_n)$ since $E'_1 \cup \cdots \cup E'_n$ is finite. So $[E'_1) \cap \cdots \cap [E'_n)$ is nonempty, and hence $\mathcal{K}$ has the finite intersection property. Consequently, by Cor. 3.33, $\mathcal{K}$ is included in a proper filter $\mathcal{F}$. Note that both K and $\mathcal{F}$ are subsets of $\mathcal{P}\big(\mathcal{P}_\omega(A)\big)$. Let $\boldsymbol{B} = \big(\prod_{E' \in \mathcal{P}_\omega(E)} \boldsymbol{A}_{E'}\big)/\Phi(\mathcal{F})$. For each $\varepsilon \in E$, we have

$$\{\, E' \in \mathcal{P}_\omega(E) : \boldsymbol{A}_{E'} \vDash \varepsilon \,\} \supseteq \{\, E' \in \mathcal{P}_\omega(E) : \varepsilon \in E' \,\} = [\{\varepsilon\}) \in \mathcal{F}.$$

So $\boldsymbol{B} \vDash \varepsilon$ by Lem. 3.37. Thus $\boldsymbol{B} \in \mathsf{Mod}(E)$.

It remains only to show that $\boldsymbol{B}$ is nontrivial. For every $E' \in \mathcal{P}_\omega(E)$ choose $a_{E'}$ and $b_{E'}$ to be distinct elements of $A_{E'}$; this is possible since all the $\boldsymbol{A}_{E'}$ are nontrivial. Let $\vec{a} = \langle\, a'_{E'} : E' \in \mathcal{P}_\omega(E) \,\rangle$ and $\vec{b} = \langle\, b'_{E'} : E' \in \mathcal{P}_\omega(E) \,\rangle$. Then $\mathrm{EQ}(\vec{a}, \vec{b}) = \emptyset \notin \mathcal{F}$. So $\vec{a}/\Phi(\mathcal{F}) \neq \vec{b}/\Phi(\mathcal{F})$. Hence $\boldsymbol{B}$ if nontrivial. □

We now give another application of the reduced product by showing that every algebra is isomorphic to a subalgebra of a reduced product of its finitely generated subalgebras.

Theorem 3.40. *Let $\boldsymbol{A}$ be a Σ-algebra. Then $\boldsymbol{A} \in \mathbf{S}\mathbf{P}_{\mathrm{U}}\{\, \boldsymbol{B} : \boldsymbol{B} \subseteq \boldsymbol{A},\ \boldsymbol{B}$ is finitely generated$\}$.*

Proof. Let $I = \mathcal{P}_\omega(A)$. As in the proof of the Compactness Theorem there exists a proper filter $\mathcal{F}$ on $\mathcal{P}_\omega(A)$ such that, for every $X \in \mathcal{P}_\omega(A)$, $[X) = \{\, Y \in \mathcal{P}_\omega(A) : X \subseteq Y \,\} \in \mathcal{F}$.

For each $X \in \mathcal{P}_\omega(A)$, let $\boldsymbol{B}_X$ be the subalgebra of $\boldsymbol{A}$ generated by X, i.e., the subalgebra with universe $\mathrm{Sg}^{\boldsymbol{A}}(X)$, provided this subuniverse is nonempty. (Of course, $\mathrm{Sg}^{\boldsymbol{A}}(X)$ can be empty only if X is empty.) If it is, take $\boldsymbol{B}_\emptyset$ to be any fixed but arbitrary (nonempty) finitely generated subalgebra of $\boldsymbol{A}$. For each $X \in \mathcal{P}_\omega(A)$ choose a fixed but arbitrary element b_X of $\boldsymbol{B}_X$. Let $\boldsymbol{B} = \prod_{X \in \mathcal{P}_\omega(A)} \boldsymbol{B}_X$ and consider the mappings

$$A \overset{h}{\rightarrowtail} B \overset{\Delta_{\Phi(\mathcal{F})}}{\rightarrowtail} B/\Phi(\mathcal{F}),$$

where, for each $a \in A$,

$$h(a) = \langle\, \hat{a}_X : X \in \mathcal{P}_\omega(A) \,\rangle \quad \text{with} \begin{cases} \hat{a}_X = a & \text{if } a \in B_X, \\ \hat{a}_X = b_X & \text{if } a \notin B_X. \end{cases}$$

Let $g = \Delta_{\Phi(\mathcal{F})} \circ h$. h is not a homomorphism from $\boldsymbol{A}$ into $\boldsymbol{B}$ (exercise), but we claim that

$$g \text{ is a homomorphism from } \boldsymbol{A} \text{ into } \boldsymbol{B}/\Phi(\mathcal{F}).$$

To see this assume $\sigma \in \Sigma_n$ and let $a_1, \dots, a_n \in A$. By the definition of h

$$h\big(\sigma^{\boldsymbol{A}}(a_1, \dots, a_n)\big) = \langle\, \widehat{\sigma^{\boldsymbol{A}}}(a_1, \dots, a_n)_X : X \in \mathcal{P}_\omega(A) \,\rangle,$$

and by the definition of the direct product,

$$\begin{aligned} \sigma^{\boldsymbol{B}}\big(h(a_1), \dots, h(a_n)\big) &= \sigma^{\boldsymbol{B}}\big(\langle\, \widehat{a_1}_X : X \in \mathcal{P}_\omega(A) \,\rangle, \dots, \langle\, \widehat{a_n}_X : X \in \mathcal{P}_\omega(A) \,\rangle\big) \\ &= \langle\, \sigma^{\boldsymbol{B}_X}(\widehat{a_1}_X, \dots, \widehat{a_n}_X) : X \in \mathcal{P}_\omega(A) \,\rangle. \end{aligned}$$

We now observe that, for every $X \in \mathcal{P}_\omega(A)$ such that $a_1, \dots, a_n \in X$ we have $\sigma^{\boldsymbol{A}}(a_1, \dots, a_n) \in B_X$ (since $\boldsymbol{B}_X$ is a subalgebra of $\boldsymbol{A}$), and hence

$$\widehat{\sigma^{\boldsymbol{A}}}(a_1, \dots, a_n)_X = \sigma^{\boldsymbol{A}}(a_1, \dots, a_n) = \sigma^{\boldsymbol{B}_X}(a_1, \dots, a_n) = \sigma^{\boldsymbol{B}_X}(\widehat{a_1}_X, \dots, \widehat{a_n}_X).$$

Thus, for each X such that $a_1, \dots, a_n \in X$, $X \in \mathrm{EQ}\big(h\big(\sigma^{\boldsymbol{A}}(a_1, \dots, a_n)\big),\ \sigma^{\boldsymbol{B}}\big(h(a_1), \dots, h(a_n)\big)\big)$. Hence

$$\mathrm{EQ}\big(h\big(\sigma^{\boldsymbol{A}}(a_1, \dots, a_n)\big),\ \sigma^{\boldsymbol{B}}\big(h(a_1), \dots, h(a_n)\big)\big) \supseteq \big[\{a_1, \dots, a_n\}\big) \in \mathcal{F}.$$

So

$$\begin{aligned} g\big(\sigma^{\boldsymbol{A}}(a_1, \dots, a_n)\big) &= h\big(\sigma^{\boldsymbol{A}}(a_1, \dots, a_n)\big)/\Phi(\mathcal{F}) \\ &= \sigma^{\boldsymbol{B}}\big(h(a_1), \dots, h(a_n)\big)/\Phi(\mathcal{F}) \\ &= \sigma^{\boldsymbol{B}/\Phi(\mathcal{F})}\big(h(a_1)/\Phi(\mathcal{F}), \dots, h(a_n)/\Phi(\mathcal{F})\big) \\ &= \sigma^{\boldsymbol{B}/\Phi(\mathcal{F})}\big(g(a_1), \dots, g(a_n)\big). \end{aligned}$$

Thus $g \in \mathrm{Hom}\big(\boldsymbol{A}, \boldsymbol{B}/\Phi(\mathcal{F})\big)$

We further claim that g is injective. To see this let a and a' be distinct elements of A. For every $X \in \mathcal{P}_\omega(A)$ such that $a, a' \in X$ we have $\widehat{a}_X = a \neq a' = \widehat{a'}_X$, and hence $X \notin \mathrm{EQ}\big(h(a), h(a')\big)$. Thus $\mathrm{EQ}\big(h(a), h(a')\big) \subseteq \overline{[\{a, a'\})}$. But $\overline{[\{a, a'\})} \notin \mathcal{F}$ since $[\{a, a'\}) \in \mathcal{F}$ and $\mathcal{F}$ is proper. So $\mathrm{EQ}\big(h(a), h(a')\big) \notin \mathcal{F}$ and thus $\langle h(a), h(a') \rangle \notin \Phi(\mathcal{F})$ by definition of $\Phi(\mathcal{F})$. Hence $g(a) \neq g(a')$. Thus g is injective as claimed.

We have shown that $g\colon \boldsymbol{A} \rightarrowtail \big(\prod_{X\in\mathcal{P}_\omega(A)} \boldsymbol{B}_X\big)/\Phi(\mathcal{F})$. So

$$\boldsymbol{A} \in \mathbf{S}\,\mathbf{P}_{\mathrm{U}}\{\, \boldsymbol{B} : \boldsymbol{B} \subseteq \boldsymbol{A},\ \boldsymbol{B} \text{ is finitely generated} \,\}.$$

□

Example: Let $\boldsymbol{A} = \langle \mathbb{Z}, S\rangle$, where S is the successor function. $\boldsymbol{A}$ is not finitely generated. Every finitely generated subalgebra of $\boldsymbol{A}$ is of the form $\boldsymbol{A}_n = \langle [n) : S\restriction[n)\rangle$, where $[n) = \{\, k \in \mathbb{Z} : n \leq k \,\}$, for each $n \in \mathbb{Z}$. The general construction of the reduced product in the proof of the above theorem can be simplified in this special case because every finitely generated subalgebra is in fact generated by a single element. Because of this the index set can be taken to be the set $\big\{\, \{n\} : n \in \mathbb{Z} \,\big\}$ of singleton subsets of $\mathbb{Z}$ rather than the set of all finite subsets. And then the natural bijection between a set and its corresponding set of singleton subsets allows the further simplification of taking the index set to be $\mathbb{Z}$ itself.

Thus we take I to be $\mathbb{Z}$, and let $\mathcal{K} = \big\{\, (n] : n \in \mathbb{Z} \,\big\}$, where $(n] = \{\, k \in \mathbb{Z} : k \leq n \,\}$. $\mathrm{Min}(n_1, \ldots, n_k) \in (n_1] \cap \cdots \cap (n_k]$ for every finite set $n_1, \ldots, n_k$ of elements of $\mathbb{Z}$. So $\mathcal{K}$ has the finite intersection property, i.e., the intersection of every finite subset of members of $\mathcal{K}$ is nonempty. Thus by Cor. 3.33 $\mathcal{K}$ is included in a proper filter $\mathcal{F}$. We can take $\mathcal{F}$ to be the smallest such filter, i.e., the filter generated by $\mathcal{K}$, which by Lem. 3.31 takes the form $\mathcal{F} = \big\{\, X : \exists\, n \in \omega \,\big((n] \subseteq X\,\big\}$.

Define $h\colon A \to \prod_{n\in\mathbb{Z}} A_n$ such that, for each $a \in \mathbb{Z}$, $h(a) = \big\langle\, \hat{a}_n : n \in \mathbb{Z} \,\big\rangle$, where

$$\hat{a}_n = \begin{cases} a & \text{if } a \in [n) \\ n & \text{otherwise.} \end{cases}$$

Finally, define $g\colon A \to \big(\prod_{n\in\mathbb{Z}} A_n\big)/\Phi(\mathcal{F})$ by $g(a) = h(a)/\Phi(\mathcal{F})$ for each $a \in \mathbb{Z}$. See Figure 21.

$h(0)$ and $h(1)$ are illustrated in Figure 21 by bold dashed and dot-dashed lines, respectively Note that $h(0)$ and $h(1)$ agree on $[1)$ and disagree on $(0]$. Both sets are infinite but only $(0]$ is in $\mathcal{F}$, so $h(0)/\Phi(\mathcal{F}) \neq h(1)/\Phi(\mathcal{F})$. But notice that these elements are distinct because $[1)$ fails to be in the filter, not because $(0]$ is in the filter.

Exercises:

(1) Show that h is not a homomorphism from $\boldsymbol{A}$ to $\prod_{n\in\mathbb{Z}} \boldsymbol{A}_n$.

(2) Show that g is an injective homomorphism from $\boldsymbol{A}$ to $\big(\prod_{n\in\mathbb{Z}} \boldsymbol{A}_n\big)/\Phi(\mathcal{F})$.

(3) Note that each $\boldsymbol{A}_n$ is isomorphic to $\langle \omega, S\rangle$; thus $\langle \mathbb{Z}, S\rangle$ is isomorphic to a subalgebra of a reduced power of $\langle \omega, S\rangle$. Show that a reduced product is really necessary here by proving that $\langle \mathbb{Z}, S\rangle$ is not isomorphic to a subalgebra of any power of $\langle \omega, S\rangle$, i.e. $\langle \mathbb{Z}, S\rangle \notin \mathbf{S}\,\mathbf{P}\big(\{\langle \omega, S\rangle\}\big)$.

It sufficed in the proof of the Compactness Theorem to use a proper filter rather than an ultrafilter because we were only interested in preserving identities. If we want to preserve nonidentities we have to use ultrafilters. This fact is reflected in the following lemma.

Lemma 3.41. *Let $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ be a system of Σ-algebras and let $\mathcal{F}$ be filter on I. Let ε be a Σ-equation. If $\mathcal{F}$ is an ultrafilter, then*

$$\Big(\prod_{i\in I} \boldsymbol{A}_i\Big)/\Phi(\mathcal{F}) \models \varepsilon \quad \textit{iff} \quad \{\, i \in I : \boldsymbol{A}_i \models \varepsilon \,\} \in \mathcal{F}.$$

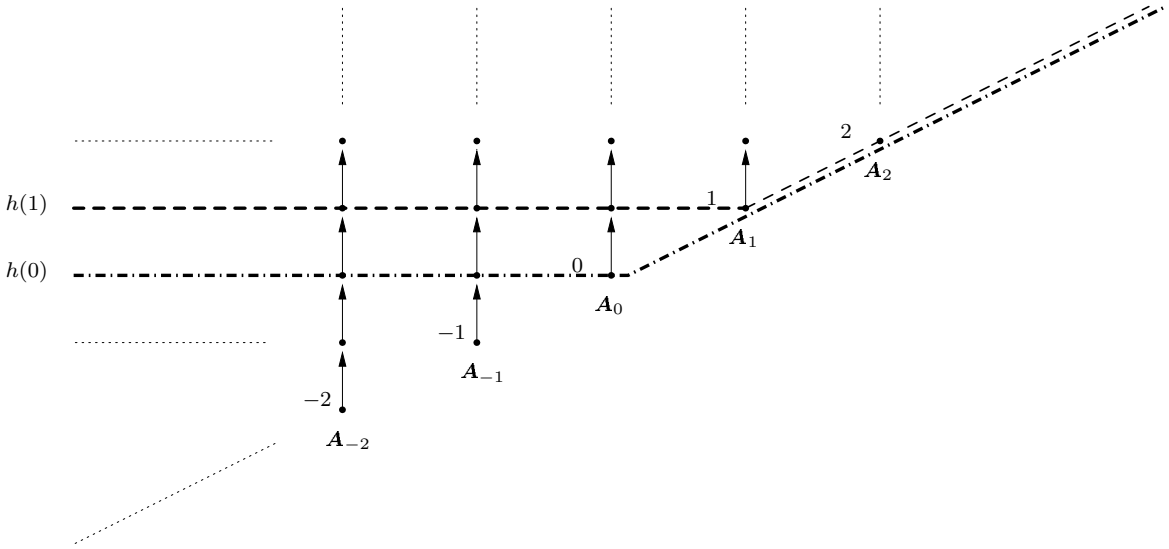


FIGURE 21

Proof.

$$\begin{aligned}
\Big(\prod_{i\in I}\boldsymbol{A}_i\Big)/\Phi(\mathcal{F}) \models \varepsilon \quad &\text{iff} \quad \{\, i\in I : \boldsymbol{A}_i \models \varepsilon \,\} \notin \mathcal{F}, \quad \text{by Lem. 3.38}\\
&\text{iff} \quad \overline{\{\, i\in I : \boldsymbol{A}_i \models \varepsilon \,\}} \in \mathcal{F}, \quad \text{by Thm. 3.34}\\
&\text{iff} \quad \{\, i\in I : \boldsymbol{A}_i \not\models \varepsilon \,\} \in \mathcal{F}.
\end{aligned}$$

□

That $\mathcal{F}$ is an ultrafilter is necessary here. Let ε be any Σ-equation, and let $\boldsymbol{B}$ and $\boldsymbol{C}$ be Σ-algebras such that $\boldsymbol{B} \not\models \varepsilon$ and $\boldsymbol{C} \models \varepsilon$. For each $n \in \omega$ let $\boldsymbol{A}_n = \boldsymbol{B}$ if n is even and $\boldsymbol{A}_n = \boldsymbol{C}$ if n is odd. Let $\mathcal{F} = \mathcal{C}f$, the filter of cofinite subsets of ω. $\{\, n \in \omega : \boldsymbol{A}_n \models \varepsilon \,\} = \{\, 2n+1 : n \in \omega \,\} \notin \mathcal{F}$, so $\big(\prod_{n\in\omega}\boldsymbol{A}_n\big)/\Phi(\mathcal{C}f) \not\models \varepsilon$ by Lem. 3.38. On the other hand, $\{\, n \in \omega : \boldsymbol{A}_n \not\models \varepsilon \,\} = \{\, 2n : n \in \omega \,\} \notin \mathcal{F}$.

Ultraproducts also preserve more logically complex conditions. We give an example which depends on the following result about ultrafilters.

Lemma 3.42. *Let $\mathcal{U}$ be an ultrafilter on a set I.*

(i) *Let $X_1, \dots, X_n$ be any finite set of subsets of I. Then $X_1 \cup \cdots \cup X_n \in \mathcal{U}$ iff $X_i \in \mathcal{U}$ for at least one $i \leq n$.*

(i) *Let $X_1, \dots, X_n$ and $Y_1, \dots, Y_m$ by two finite sets of subsets of I. Then $X_1 \cup \cdots \cup X_n \cup \overline{Y_1} \cup \cdots \cup \overline{Y_m} \in \mathcal{U}$ iff either some $X_i \in \mathcal{U}$ or some $Y_j \notin \mathcal{U}$.*

The proof is left as an exercise. Hint: prove the first part by induction on n.

Definition 3.43. Let

$$\varepsilon_1 = t_1(x_0, \dots, x_{k-1}) \approx s_1(x_0, \dots, x_{k-1}), \dots, \varepsilon_n = t_n(x_0, \dots, x_{k-1}) \approx s_n(x_0, \dots, x_{k-1})$$

and

$$\delta_1 = u_1(x_0, \dots, x_{k-1}) \approx v_1(x_0, \dots, x_{k-1}), \dots, \delta_m = u_m(x_0, \dots, x_{k-1}) \approx v_m(x_0, \dots, x_{k-1})$$

be two finite sets of Σ-equations. A Σ-algebra $\boldsymbol{A}$ is said to be a model of the formula

$$\varepsilon_1 \textbf{ or } \cdots \textbf{ or } \varepsilon_n \textbf{ or } (\textbf{not } \delta_1) \textbf{ or } \cdots \textbf{ or } (\textbf{not } \delta_m),$$

which in turn is said to be *universally valid in* $\boldsymbol{A}$, if, for all $a_0, \dots, a_{k-1} \in A$, either $t_i^{\boldsymbol{A}}(a_0, \dots, a_{k-1}) = s_i^{\boldsymbol{A}}(a_0, \dots, a_{k-1})$ for some $i \leq n$ or $u_j^{\boldsymbol{A}}(a_0, \dots, a_{k-1}) \neq v_j^{\boldsymbol{A}}(a_0, \dots, a_{k-1})$ for some $j \leq m$. In this case we write

$$\boldsymbol{A} \vDash \varepsilon_1 \textbf{ or } \cdots \textbf{ or } \varepsilon_n \textbf{ or } (\textbf{not } \delta_1) \textbf{ or } \cdots \textbf{ or } (\textbf{not } \delta_m).$$

By a (Σ)-*equational literal* we mean either a Σ-equation or a formula of the form $\textbf{not } \varepsilon$ where ε is a Σ-equation. A finite disjunction of equational literals, such as $\varepsilon_1 \textbf{ or } \cdots \textbf{ or } \varepsilon_n \textbf{ or } (\textbf{not } \delta_1) \textbf{ or } \cdots \textbf{ or } (\textbf{not } \delta_m)$, is called a (Σ)-*equational clause*. Strictly speaking this formula should be written in the form

$$\forall x_0 \dots \forall x_{k-1} \big(\varepsilon_1 \textbf{ or } \cdots \textbf{ or } \varepsilon_n \textbf{ or } (\textbf{not } \delta_1) \textbf{ or } \cdots \textbf{ or } (\textbf{not } \delta_m) \big),$$

with universal quantifiers at the front, but they are normally omitted for simplicity. The classes of all models of an equational clause ψ, and of a set Ψ of equational clauses, are written respectively as $\mathsf{Mod}(\psi)$ and $\mathsf{Mod}(\Psi)$.

Many important properties of algebras can be expressed as equational clauses. For example the property of a commutative ring with identity that it be an integral domain can be expressed as

$$(x \approx 0) \textbf{ or } (y \approx 0) \textbf{ or } ((\textbf{not}(x \cdot y \approx 0)).$$

We have the following generalization of Lemma 3.38 when applied to ultrafilters.

Lemma 3.44. *Let* $\langle\, \boldsymbol{A}_i : i \in I \,\rangle$ *be a system of* Σ*-algebras, and let* $\mathcal{U}$ *be an ultrafilter on* I*. Let* ψ *be an equational clause. Then*

$$\Big(\prod_{i \in I} \boldsymbol{A}_i \Big) / \Phi(\mathcal{U}) \vDash \psi \quad \textit{iff} \quad \{\, i \in I : \boldsymbol{A}_i \vDash \psi \,\} \in \mathcal{U}.$$

The proof is also left as an exercise. It is similar to that of Lemma 3.38, but of course it uses Lemma 3.42.

The following theorem is an immediate consequence of the last lemma.

Theorem 3.45. *Let* Ψ *be a set of equational clauses. Then* $\mathbf{P}_{\mathrm{U}}(\mathsf{Mod}(\Psi)) = \mathsf{Mod}(\Psi)$.

So the class of all integral domains is closed under taking ultraproducts. This is not true of course of arbitrary reduced products. The ring of integers $\mathbb{Z}$ is an integral domain but its square $\mathbb{Z} \times \mathbb{Z}$ is not ($\langle 0, 1 \rangle$ is a zero divisor). Note that every direct product is a reduced product; more precisely, $\prod_{i \in I} \boldsymbol{A}_i \cong \big(\prod_{i \in I} \boldsymbol{A}_i \big) / \Phi([I])$.

4. Equational Logic

Recall that a Σ-equation ε is defined to be a logical consequence of a set E of Σ-equations if every model of E is a model of ε. Thus, taking Σ to be the signature of groups (of type II), ε is a law of groups if it is an identity in every group. To establish this fact one obviously cannot consider each group individually and check if ε is an identity. A proof is required and it must be a finite process. In the following we define the formal notion of a proof of ε from E; it is not immediately obviously what is its relation to logical consequence.

Definition 4.1. Let E be a set of Σ-equations. A Σ-equation ε is a (*logical*) *consequence* of E, in symbols $E \models \varepsilon$, if every model of E is a model of ε, i.e., $\mathsf{Mod}(E) \models \varepsilon$, that is $\mathsf{Mod}(E) \subseteq \mathsf{Mod}(\varepsilon)$.

Example: Let E be the axioms of groups (of type II). Then $E \models (x \cdot y)^{-1} \approx y^{-1} \cdot x^{-1}$.

Let be a Σ-term. By a *substitution instance* of a Σ-equation ε we mean any Σ-equation that is obtained by simultaneously substituting arbitrary Σ-terms for the variables of ε. Thus if $\varepsilon = \big(t(x_0, \ldots, x_{n-1}) \approx s(x_0, \ldots, x_{n-1})\big)$, then every equation of the form $t(u_0, \ldots, u_{n-1}) \approx s(u_0, \ldots, u_{n-1})$, where $u_0, \ldots, u_{n-1}$ are arbitrary Σ-terms, is a substitution instance of ε. A substitution instance of $x \approx x$ is called a (*logical*) *tautology*. Thus $u \approx u$ is a tautology for every term u.

Definition 4.2. Let E be a set of Σ-equations. By an (*equational*) *proof from* E we mean any finite sequence $\delta_1, \ldots, \delta_m$ of Σ-terms such that, for each $k \leq m$, at least one of the following conditions holds.

(*taut*) δ_k is substitution instance of $x \approx x$, i.e., a tautology.

(*E-axiom*) δ_k is a substitution instance of an equation in E.

(*sym*) ε is $t \approx s$ and there is an $i < k$ such that δ_i is $s \approx t$.

(*trans*) ε_k is $t \approx s$ and there exist $i, j < k$ such that δ_i is $t \approx r$ and δ_j is $r \approx s$.

(*repl*) ε_k is of the form $\sigma(t_0, \ldots, t_{n-1}) \approx \sigma(s_0, \ldots, s_{n-1})$, where $\sigma \in \Sigma_n$ and there are $i_0, \ldots, i_{n-1} < k$ such that $\delta_{i_0}, \ldots, \delta_{i_{n-1}}$ are respectively $t_0 \approx s_0, \cdots, t_{n-1} \approx s_{n-1}$.

The five conditions that define an equational proof are called *rules*. Each of the first two, (taut) and (E-axiom), is called an *axiom* because it allows one to introduce an equation in the proof independently of any particular equation or equations occurring earlier in the proof. The last three, (symm), (trans), and (repl) are called *inference rules*. The equation that each of them introduces into the proof is called the *conclusion* of the rule; the equation(s) occurring earlier in the proof that justify the conclusion are called *premisses*.

Traditionally axioms and inference rules are represented by drawing a horizontal line between the premisses and the conclusion. We summarize the axioms and rules of inference symbolically in this form below.

In the following $r, s, s_0, s_1, \ldots, t, t_0, t_1, \ldots, u_0, \ldots, u_{n-1}$ represent arbitrary Σ-terms and E an arbitrary set of Σ-equations.

(*taut*) $t \approx t$.

(E-*axiom*) $t(u_0, \cdots, u_{n-1}) \approx s(u_0, \ldots, u_{n-1})$,
for each $t(x_0, \ldots, x_{n-1}) \approx s(x_0, \ldots, x_{n-1})$ in E.

$$(sym) \quad \frac{t \approx s}{s \approx t}.$$

$$(trans) \quad \frac{t \approx r,\ r \approx s}{t \approx s}.$$

$$(repl) \quad \frac{t_0 \approx s_0, \cdots, t_{n-1} \approx s_{n-1}}{\sigma(t_0, \ldots, t_{n-1}) \approx \sigma(s_0, \ldots, s_{n-1})}, \quad \text{for each } \sigma \in \Sigma_n.$$

Definition 4.3. Let E be a set of Σ-equations. A Σ-equation ε is (*equationally*) *provable from* E, in symbols $E \vdash \varepsilon$, if there is a proof $\delta_1, \ldots, \delta_m$ from E such that the last equation δ_m is ε.

Example: As an example we construct an equational proof of $(x \cdot y)^{-1} \approx y^{-1} \cdot x^{-1}$ from the axioms of group theory. We first prove it informally, the way it would be done in an algebra course, and then show how to convert this into a formal equational proof.

The most natural way to prove it is to use the fact that in a group the inverse of each element is unique. Assume $x\,y = e$; as usual we omit the multiplication symbol "$\cdot$" when write products informally.

$$(29) \qquad (x\,y)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x\,e\,x^{-1} = x\,x^{-1} = e.$$

So by the uniqueness of the inverse, we have $(x\,y)^{-1} = y^{-1}x^{-1}$. The formal equational proof must incorporate the proof of the fact that the inverse is unique. Here is its informal proof: Assume $x\,y = e$. Then

$$(30) \qquad y = e\,y = (x^{-1}x)y = x^{-1}(x\,y) = x^{-1}e = x^{-1}.$$

Note that all the steps in this proof follow from the axioms of group theory except for the next-to-last equality; this uses the assumption that $x\,y = e$. We now transform (30) into an informal proof of $(x \cdot y)^{-1} \approx y^{-1} \cdot x^{-1}$ by substituting "$(x\,y)$" for all occurrences of "x" and "$(y^{-1}x^{-1})$" for all occurrences of "y". Note that under these substitutions the next-to-last equality of the transformed proof becomes "$(x\,y)^{-1}\big((x\,y)(y^{-1}x^{-1})\big) = (x\,y)^{-1}e$", which is obtained from a substitution instance of the assumption "$x\,y = e$" by replacement. This next-to-last equality in the transformed proof (30) is then expanded into a series of steps by incorporating the proof of $(x\,y)(y^{-1}x^{-1}) = e$ given in (29). This gives an informal of $(x \cdot y)^{-1} \approx y^{-1} \cdot x^{-1}$ directly from the axioms of group theory. Here it is.

$$(31) \quad \begin{aligned} y^{-1}x^{-1} &= e(y^{-1}x^{-1}) = \big(x\,y^{-1}(x\,y)\big)(y^{-1}x^{-1}) = (x\,y)^{-1}\big((x\,y)(y^{-1}x^{-1})\big) \\ &= (x\,y)^{-1}\big((x\,(y\,y^{-1}))x^{-1}\big) = (x\,y)^{-1}\big((x\,e)x^{-1}\big) = (x\,y)^{-1}(x\,x^{-1}) = (x\,y)^{-1}e = (x\,y)^{-1}. \end{aligned}$$

This informal proof appears to use only the axioms of groups, but it also implicitly uses properties of equality. For example, that we can write it as a long sequence of terms separated by equality symbols, rather than a sequence of indvidual equations, implicitly uses the transistivity of equality. In a formal equational proof each use of a property of equality must be justified by an axiom or rule of equality, i.e., by (*taut*) or by one of the inference rules (*sym*), (*trans*), or (*repl*). In Figure 22 we give a fragment of the formal equational proof of $(x \cdot y)^{-1} \approx y^{-1} \cdot x^{-1}$ from the axioms E of groups—the part that terminates in a proof $y^{-1} \cdot x^{-1} \approx \big((x \cdot y)^{-1} \cdot (x \cdot y)\big) \cdot (y^{-1} \cdot x^{-1})$.

We now clarify the relation between the semantical relation of logical consequence $\models$ and that of equational proof $\vdash$; we see that these conceptionally very different notions give the same abstract relation.

1.	$e \cdot (y^{-1} \cdot x^{-1}) \approx y^{-1} \cdot x^{-1}$	(*E-axiom*), subst. inst. of $e \cdot x \approx x$
2.	$y^{-1} \cdot x^{-1} \approx e \cdot (y^{-1} \cdot x^{-1})$	1, (*sym*)
3.	$(x \cdot y)^{-1} \cdot (x \cdot y) \approx e$	(*E-axiom*), subst. inst. of $x \cdot x^{-1} \approx e$
4.	$e \approx (x \cdot y)^{-1} \cdot (x \cdot y)$	3, (*sym*)
5.	$y^{-1} \cdot x^{-1} \approx y^{-1} \cdot x^{-1}$	(*taut*)
6.	$e \cdot (y^{-1} \cdot x^{-1}) \approx \big((x \cdot y)^{-1} \cdot (x \cdot y)\big) \cdot (y^{-1} \cdot x^{-1})$	4,5, (*repl*)
7.	$y^{-1} \cdot x^{-1} \approx \big((x \cdot y)^{-1} \cdot (x \cdot y)\big) \cdot (y^{-1} \cdot x^{-1})$	2,6, (*trans*)

FIGURE 22

Theorem 4.4 (Soundness Theorem for Equational Logic)**.** *For any set $E \cup \{\varepsilon\}$ of Σ-equations, if ε is equtionally provable from E then it is a logical consequence of E, i.e., $E \vdash \varepsilon$ implies $E \vDash \varepsilon$.*

Proof. Assume $E \vdash \varepsilon$. Let $\delta_1, \dots, \delta_m$ with $\delta_m = \varepsilon$ be an equational proof of ε from E. We prove that $E \vDash \delta_k$ for all $k \leq m$ by induction on k.

Let $\hat{v} = \langle x_0, \dots, x_{n-1} \rangle$ include every variable occurring in at least one of the δ_k. Assume δ_k is of the form $t_k(\hat{x}) \approx s_k(\hat{x})$ for every $k \leq m$. Recall that $E \vDash \delta_k$ means that, for every $\boldsymbol{A} \in \mathsf{Mod}(E)$ and every $\hat{a} = \langle a_0, \dots, a_{n-1} \rangle \in A^n$, $t_k^{\boldsymbol{A}}(\hat{a}) = s_k^{\boldsymbol{A}}(\hat{a})$. Let $\boldsymbol{A} \in \mathsf{Mod}(E)$ and $\hat{a} \in A^n$ be fixed but arbitrary.

For $k = 1$, δ_1 must be either a tautology or a substitution instance of an equation in E, i.e., δ_1 is in one of the two following forms: $u(\hat{x}) \approx u(\hat{x})$ or

$$u\big(w_0(\hat{x}), \dots, w_{l-1}(\hat{x})\big) \approx v\big(w_0(\hat{x}), \dots, w_{l-1}(\hat{x})\big) \quad \text{where } u(y_0, \dots, y_{l-1}) \approx v(y_0, \dots, y_{l-1}) \text{ is in } E.$$

In the first case $t_1^{\boldsymbol{A}}(\hat{a}) = u^{\boldsymbol{A}}(\hat{a}) = u^{\boldsymbol{A}}(\hat{a}) = s_1^{\boldsymbol{A}}(\hat{a})$. In the second case, by assumption we have that $u^{\boldsymbol{A}}(\hat{b}) = v^{\boldsymbol{A}}(\hat{b})$ for all $\hat{b} \in A^l$. Thus

$$t_1^{\boldsymbol{A}}(\hat{a}) = u^{\boldsymbol{A}}\big(\underbrace{w_0^{\boldsymbol{A}}(\hat{a})}_{b_0}, \cdots, \underbrace{w_{l-1}^{\boldsymbol{A}}(\hat{a})}_{b_{l-1}}\big) = v^{\boldsymbol{A}}\big(\underbrace{w_0^{\boldsymbol{A}}(\hat{a})}_{b_0}, \cdots, \underbrace{w_{l-1}^{\boldsymbol{A}}(\hat{a})}_{b_{l-1}}\big) = s_1^{\boldsymbol{A}}(\hat{a}).$$

Suppose $k > 1$. If ε_k is a tautology or substitution instance of an equation of E we proceed as above. So we can assume that ε_k is obtained from earlier equations in the proof by one of the inference rules.

Consider (*repl*). Suppose

$$\varepsilon_k = \Big(\underbrace{\sigma\big(t_{i_1}(\hat{x}), \dots, t_{i_m}(\hat{x})\big)}_{t_k(\hat{x})} \approx \underbrace{\sigma\big(s_{i_1}(\hat{x}), \dots, s_{i_m}(\hat{x})\big)}_{s_k(\hat{x})}\Big),$$

where $i_1, \dots, i_m < k$. By the induction hypothesis $E \vDash \underbrace{t_{i_j}(\hat{x}) \approx s_{i_j}(\hat{x})}_{\delta_{i_j}}$ for all $j \leq m$. Thus

$t_{i_j}^{\boldsymbol{A}}(\hat{a}) = s_{i_j}^{\boldsymbol{A}}(\hat{a})$ for $j \leq m$, and hence

$$t_k^{\boldsymbol{A}}(\hat{a}) = \sigma^{\boldsymbol{A}}\big(t_{i_1}^{\boldsymbol{A}}(\hat{a}), \dots, t_{i_m}^{\boldsymbol{A}}(\hat{a})\big) = \sigma^{\boldsymbol{A}}\big(s_{i_1}^{\boldsymbol{A}}(\hat{a}), \dots, s_{i_m}^{\boldsymbol{A}}(\hat{a})\big) = s_k^{\boldsymbol{A}}(\hat{a}).$$

Hence $E \vDash \delta_k$.

The rules (*sym*) and (*trans*) are left as exercises. □

Sometimes the following rule of substitution is included among the rules of equational logic.

$$(sub)\ \frac{t(x_0,\dots,x_{n-1}) \approx s(x_0,\dots,x_{n-1})}{t(u_0,\dots,u_{n-1}) \approx s(u_0,\dots,u_{n-1})},\quad \text{for all } u_0,\dots,u_{n-1} \in \mathrm{Te}_\Sigma(X).$$

The next lemma shows that the rule would be redundant—every equation that is provable with it is provable without it.

Lemma 4.5. *For any set of Σ-equations $E \cup \{t(x_0,\dots,x_{n-1} \approx s(x_0,\dots,x_{n-1})\}$ and any sequence $u_0,\dots,u_{n-1}$ of Σ-terms we have that $E \vdash t(x_0,\dots,x_{n-1}) \approx s(x_0,\dots,x_{n-1})$ implies $E \vdash t(u_0,\dots,u_{n-1} \approx s(u_0,\dots,u_{n-1})$, i.e., every substitution instance of an equation provable from E is itself provable from E.*

The proof is left as an exercise. It goes by induction on the length of proofs. Note that the base step is guaranteed by the fact that by (*E-axiom*) every substitution instance of an equation of E is automatically provable from E.

Problem: Suppose you are asked by your algebra instructor either to prove that every Boolean group is Abelian or to find a counterexample (a *Boolean group* is a group in which every nonidentity is of order 2). What does this mean? Let E be be the axioms of groups. Then you are asked to verify either

$$E \cup \{x \cdot x \approx e\} \vdash x \cdot y \approx y \cdot x \quad \text{or} \quad E \cup \{x \cdot x \approx e\} \nvdash x \cdot y \approx y \cdot x.$$

But why do you know that at least one of these two alternatives must be true? That is, how can you be sure that if $x \cdot y \approx y \cdot x$ is not provable from the axioms of groups together with $x \cdot x \approx e$, then a counterexample must exist? Formally, does

$$E \cup \{x \cdot x \approx e\} \nvdash x \cdot y \approx y \cdot x \quad \text{imply} \quad E \cup \{x \cdot x \approx e\} \nvDash x \cdot y \approx y \cdot x?$$

This implication, in its contrapositive form, is the completeness theorem of equational logic. The completeness theorem can be paraphrased as "If an equation is not provable there must be a counterexample."

Theorem 4.6 (Completeness Theorem of Equational Logic)**.** *For any set $E \cup \{\varepsilon\}$ of Σ-equations, if ε is a logical consequence of E, then ε is equationally provable from E, i.e.,*

$$E \vDash \varepsilon \quad \textit{implies} \quad E \vdash \varepsilon.$$

Proof. We prove the contrapositive, i.e., from the assumption that ε is not provable from E we construct a Σ-algebra $\boldsymbol{A}$ such that $\boldsymbol{A} \in \mathsf{Mod}(E)$ but $\boldsymbol{A} \notin \mathsf{Mod}(\varepsilon)$.

Let $\alpha = \{\, \langle t, s\rangle \in \mathrm{Te}_\Sigma(X)^2 : E \vdash t \approx s \,\}$.

Claim. $\alpha \in \mathrm{Co}(\mathbf{Te}_\Sigma(X))$.

Proof of claim. By (*taut*), $E \vdash t \approx t$ and hence $\langle t, t\rangle \in \alpha$ for every $t \in \mathrm{Te}_\Sigma(X)$, i.e., α is reflexive.

$$\langle t, s\rangle \in \alpha \implies E \vdash t \approx s \underset{(sym)}{\implies} E \vdash s \approx t \implies \langle t, s\rangle \in \alpha.$$

So α is symmetric.

$$\langle t, r\rangle, \langle r, s\rangle \in \alpha \implies E \vdash t \approx r, r \approx s \underset{(trans)}{\implies} E \vdash t \approx s \implies \langle t, s\rangle \in \alpha.$$

So α is transitive. For any $\sigma \in \Sigma_n$,

$$\begin{aligned}\langle t_1, s_1\rangle, \ldots, \langle t_n, s_n\rangle \in \alpha &\implies E \vdash t_1 \approx s_1, \ldots, t_n \approx s_n \\ &\underset{(repl)}{\implies} \vdash \sigma(t_1, \ldots, t_n) \approx \sigma(s_1, \ldots, s_n) \\ &\implies \langle \sigma(t_1, \ldots, t_n),\, \sigma(s_1, \ldots, s_n)\rangle \in \alpha.\end{aligned}$$

So α has the substitution property. □ claim.

Let $\boldsymbol{A} = \mathbf{Te}_\Sigma(X)/\alpha$.

Claim. $\boldsymbol{A} \in \mathsf{Mod}(E)$.

Proof of claim. Let $t(\hat{x}) \approx s(\hat{x})$ be in E, with $\hat{x} = \langle x_0, \ldots, x_{n-1}\rangle$. Let $\hat{a} = \langle a_0, \ldots, a_{n-1}\rangle \in A^n$. We must show that $t^{\boldsymbol{A}}(\hat{a}) = s^{\boldsymbol{A}}(\hat{a})$. Let $\hat{u} = u_0, \ldots, u_{n-1} \in \mathrm{Te}_\Sigma(X)^n$ such that $a_i = u_i/\alpha$ for all $i < n$, Then

$$t^{\boldsymbol{A}}(\hat{a}) = t^{\mathbf{Te}_\Sigma(X)/\alpha}(u_0/\alpha, \ldots, u_{n-1}/\alpha) = t(\hat{u})/\alpha, \quad \textit{and}$$
$$s^{\boldsymbol{A}}(\hat{a}) = t^{\mathbf{Te}_\Sigma(X)/\alpha}(u_0/\alpha, \ldots, u_{n-1}/\alpha) = s(\hat{u})/\alpha.$$

But $E \vdash t(\hat{u}) \approx s(\hat{u})$ by (*E-axiom*). So $\langle t(\hat{u}),\, s(\hat{u})\rangle \in \alpha$, i.e., $t(\hat{u})/\alpha = s(\hat{u})/\alpha$. □ claim.

Claim. $\boldsymbol{A} \notin \mathsf{Mod}(\varepsilon)$.

Proof of claim. Let ε be $t(\hat{x}) \approx s(\hat{x})$ with $\hat{x} = \langle x_0, \ldots, x_{n-1}\rangle$. Must show there exist $\hat{a} = \langle a_0, \ldots, a_{n-1}\rangle \in A^n$ such that $t^{\boldsymbol{A}}(\hat{a}) \neq s^{\boldsymbol{A}}(\hat{a})$.

Let $a_i = x_i/\alpha$ for each $i < n$. Then $t^{\boldsymbol{A}}(\hat{a}) = t(\hat{x})/\alpha$ and $s^{\boldsymbol{A}}(\hat{a}) = s(\hat{x})/\alpha$. But $\langle t(\hat{x}),\, s(\hat{x})\rangle \notin \alpha$ since $E \nvdash \varepsilon$ by assumption. So $t^{\boldsymbol{A}}(\hat{a}) \neq s^{\boldsymbol{A}}(\hat{a})$. □ claim.

Thus by the two claims $E \nvDash \varepsilon$. □

Recall that a set E of equations is *inconsistent* if it has only trivial models. The proof of the following corollary is left as an exercise.

Corollary 4.7. *A set E of Σ-equations is inconsistent iff $E \vdash x \approx y$, where x and y are distinct variables.*

This corollary can be used to obtain a new proof of the Compactness Theorem of Equational Logic that does not use reduced products. This is also left as an exercise.

4.1. **Logical consequence as a closure operator.** Recall that formally an equation is defined to be an ordered pair $\langle t, s\rangle$ with $t, s \in \mathrm{Te}_\Sigma(X)$. Thus the set of Σ-equations can be identified with the set $\mathrm{Te}_\Sigma(X)^2$. Define $\mathrm{Cn}_\Sigma : \mathcal{P}\big(\mathrm{Te}_\Sigma(X)^2\big) \to \mathcal{P}\big(\mathrm{Te}^2_\Sigma(X)\big)$ by

$$\mathrm{Cn}_\Sigma\big(E\big) = \{\, \varepsilon \in \mathrm{Te}^2_\Sigma(X) : E \vDash \varepsilon \,\}.$$

$\mathrm{Cn}_\Sigma\big(E\big)$ is the set of all logical consequences of E, that is, the set of all equations that are identities of every Σ-algebra in which each equation of E is an identity. By the soundness and completeness theorems, $\mathrm{Cn}_\Sigma(E)$ is the set of all equations that are provable from E:

$$\mathrm{Cn}_\Sigma\big(E\big) = \{\, \varepsilon \in \mathrm{Te}^2_\Sigma(X) : E \vdash \varepsilon \,\}.$$

Recall, that, for any class K of Σ-algebras, $\mathrm{Id}(\mathsf{K})$ is the set of all identities of K, i.e., $\mathrm{Id}(\mathsf{K}) = \{\, \varepsilon \in \mathrm{Te}_\Sigma(X) : \mathsf{K} \vDash \varepsilon \,\}$. Cn_Σ can be expressed in terms of the operators Mod and Id as follows.

$$\mathrm{Cn}_\Sigma(E) = \mathrm{Id}\big(\mathsf{Mod}(E)\big).$$

Cn_Σ is a closure operation on the set of Σ-equations, in fact an algebraic closure relation. This can be proved directly, but it turns out to be a consequence of a general method we now discuss for constructing closure operations in a wide variety of difference situations.

4.1.1. *Galois Connections.*

Definition 4.8. Let $\boldsymbol{A} = \langle A, \leq\rangle$ and $\boldsymbol{B} = \langle B, \leq\rangle$ be posets. Let $h\colon A \to B$ and $g\colon B \to A$ be mappings such that for all $a, a' \in A$ and $b, b' \in B$,

(i) $a \leq a'$ implies $h(a) \geq h(a')$.
(ii) $b \leq b'$ implies $g(b) \geq h(b')$.
(iii) $a \leq g\big(h(a)\big)$ and $b \leq g\big(h(b)\big)$.

The mappings h and g are said to define a *Galois connection* between $\boldsymbol{A}$ and $\boldsymbol{B}$.

Example. For sets E and F of Σ-equations and any classes K and L of Σ-algebras we have

- $E \subseteq F$ implies $\mathsf{Mod}(E) \supseteq \mathsf{Mod}(F)$.
- $\mathsf{K} \subseteq \mathsf{L}$ implies $\mathrm{Id}(\mathsf{K}) \supseteq \mathrm{Id}(\mathsf{L})$.
- $\mathsf{K} \subseteq \mathsf{Mod}\big(\mathrm{Id}(\mathsf{K})\big)$ and $E \subseteq \mathrm{Id}\big(\mathsf{Mod}(\mathsf{K})\big)$.

Thus Mod and Id are a Galois connection between the posets, in fact complete lattices, $\big\langle \mathcal{P}\big(Te_\Sigma(X)^2\big), \subseteq\big\rangle$ and $\big\langle \mathcal{P}\big(\mathsf{Alg}(\Sigma)\big), \subseteq\big\rangle$.

Galois connections give rise to closure operators in a natural way; before showing this however we first describe the more general notion of a closure operator on a poset.

Definition 4.9. Let $\boldsymbol{A} = \langle A, \leq\rangle$ be a poset. A map $c\colon A \to A$ is a *closure operator on* $\boldsymbol{A}$ if, for all $a, a' \in A$,

(i) $a \leq c(a)$;
(ii) $c(c(a)) = c(a)$;
(iii) $a \leq a'$ implies $c(a) \leq c(a')$.

Note that a closure operator C on a set A in the sense of Theorem 1.21 is a closure closure operator on the poset $\langle \mathcal{P}(A), \subseteq \rangle$.

Theorem 4.10. *Let h, g be a Galois connection between the posets $\boldsymbol{A} = \langle A, \leq \rangle$ and $\boldsymbol{B} = \langle B, \leq \rangle$. Then $g \circ h \colon A \to A$ and $h \circ g \colon B \to B$ are closure operators on $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively.*

Proof. We verify the three conditions of Defn. 4.9. Let a, a' be arbitrary elements of A and b, b' arbitrary elements of B.

(i) $a \leq (g \circ h)(a)$ and $b \leq (h \circ g)(b)$ by definition of a Galois connection.

(iii) $a \leq a'$ implies $h(a) \geq h(a')$ which in turn implies $(g \circ h)(a) \leq (g \circ h)(a')$. $b \leq b'$ implies $g(b) \geq g(b')$ which in turn implies $(h \circ g)(b) \leq (h \circ g)(b')$.

(ii) By (i), $(g \circ h)(a) \leq (g \circ h)\big((g \circ h)(a)\big)$. Also by (ii), $h(a) \leq (h \circ g)\big(h(a)\big)$. Then $g(h(a)) \geq g\big((h \circ g)(h(a))\big)$, i.e., $(g \circ h)(a) \geq (g \circ h)\big((g \circ h)(a)\big)$. So $(g \circ h)(a) = (g \circ h)(g \circ h)(a)$. Similarly, $(h \circ g)(b) = (h \circ g)(h \circ g)(b)$. □

We now show how every binary relation between two sets induces a Galois connection. Let A and B be sets and $R \subseteq A \times B$. Define $\bar{h} \colon A \to B$ and $\bar{g} \colon B \to A$ by

$$\bar{h}(a) = \{\, b \in B : a \mathrel{R} b \,\} \quad \text{and} \quad \bar{g}(b) = \{\, a \in A : \underbrace{a \mathrel{R} b}_{b \mathrel{\breve{R}} a} \,\}.$$

Define $H \colon \mathcal{P}(A) \to \mathcal{P}(B)$ and $G \colon \mathcal{P}(B) \to \mathcal{P}(A)$ by

$$H(X) = \bigcap \{\, \bar{h}(x) : x \in X \,\} = \{\, b \in B : \forall\, x \in X \,(x \mathrel{R} b) \,\} \quad \text{and}$$

$$G(Y) = \bigcap \{\, \bar{g}(y) : y \in Y \,\} = \{\, a \in A : \forall\, y \in Y \,(a \mathrel{R} y) \,\},$$

See Figure 23.

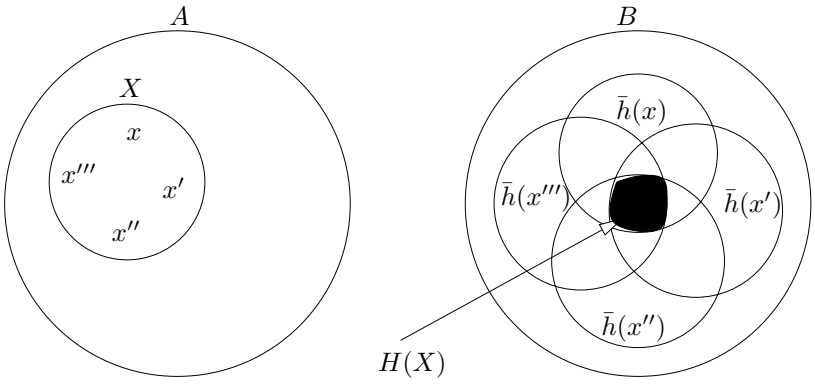


FIGURE 23

Theorem 4.11. *Let A, B be sets and $R \subseteq A \times B$. Then the H and G defined above give a Galois connection between $\langle \mathcal{P}(A), \subseteq \rangle$ and $\langle \mathcal{P}(B), \subseteq \rangle$.*

Proof. Consider any $X, X' \subseteq A$ such that $X \subseteq X'$. Clearly $\{\, \bar{h}(x) : x \in X \,\} \subseteq \{\, \bar{h}(x) : x \in X \,\}$, and hence $\bigcap \{\, \bar{h}(x) : x \in X \,\} \supseteq \bigcap \{\, \bar{h}(x) : x \in X$. So $X \subseteq X'$ implies $H(X) \supseteq H(X')$, and similarly, for all $Y, Y' \subseteq B$, $Y \subseteq Y'$ implies $G(Y) \supseteq G(Y')$.

Note that, for all $x \in A$ and $y \in B$,

$$y \in \bar{h}(x) \quad \text{iff} \quad x\,R\,y \quad \text{iff} \quad x \in \bar{g}(y).$$

Thus, for all $x \in A$, $x \in \bigcap\{\, \bar{g}(y) : y \in \bar{h}(x) \,\} = G(\bar{h}(x))$. If $x \in X$, then $H(X) \subseteq \bar{h}(x)$ by definition. So $G(H(X)) \supseteq G(\bar{h}(x))$, and hence for all $x \in X$, $x \in G(H(X))$, i.e., $X \subseteq G(H(X))$. Similarly, for every $Y \subseteq B$, $Y \subseteq H(G(Y))$. □

As a consequence of this theorem and Theorem 4.10, we have that $H \circ G\colon \mathcal{P}(A) \to \mathcal{P}(B)$ and $G \circ H\colon \mathcal{P}(B) \to \mathcal{P}(A)$ are closure operators on A and B respectively in the sense of Theorem 1.21.

Theorem 4.12. *Let A and B be sets and $R \subseteq A \times B$. Let $H\colon \mathcal{P}(A) \to \mathcal{P}(B)$ and $G\colon \mathcal{P}(B) \to \mathcal{P}(A)$ be the Galois connection defined by R. Let $\mathcal{C}_A = \{\, C \subseteq A : (G \circ H)(C) = C \,\}$, the closed subsets of A under $G \circ H$. Let $\mathcal{C}_B = \{\, C \subseteq B : (H \circ G)(C) = C \,\}$, the closed subsets of B under $H \circ G$. The complete lattices $\langle \mathcal{C}_A, \subseteq \rangle$ and $\langle \mathcal{C}_B, \subseteq \rangle$ are dually isomorphic under H.*

The proof is left as an exercise

If we take $A = \mathsf{Alg}(\Sigma)$ (the class of Σ-algebras) and $B = \mathrm{Te}_\Sigma(X)^2$ (the set of Σ-equations), and take

$$R = \vDash\; = \{\, \langle \boldsymbol{A}, \varepsilon \rangle : \boldsymbol{A} \vDash \varepsilon \,\} \subseteq \mathsf{Alg}(\Sigma) \times \mathrm{Te}_\Sigma(X)^2,$$

Then $H(\mathsf{K}) = \mathrm{Id}(K)$, the set of identities of K, and $G(E) = \mathsf{Mod}(E)$, the variety axiomatized by E. Thus, the consequence operator $\mathrm{Cn}_\Sigma = \mathrm{Id} \circ \mathsf{Mod}$ is a closure operator on the set of Σ-equations. In fact we have

Theorem 4.13. *The Cn_Σ is a finitary closure operation on the set of Σ-equations.*

Proof. As observed above, that Cn_Σ is a closure operator follows from Thms. 4.10 and 4.11. Consider any set E of Σ-equations. By the monotonicity of Cn we have $\bigcup\{\, \mathrm{Cn}(E') : E' \subseteq_\omega E \,\} \subseteq \mathrm{Cn}(E)$. Let $\varepsilon \in \mathrm{Cn}(E)$; $E \vdash \varepsilon$. Let $\delta_1, \ldots, \delta_m$ be a proof of ε from E. Obviously there can be only a finite number of applications of the (*E-axiom*) in the proof. Let E' be the finite set of equations in E used in these applications. Then $\delta_1, \ldots, \delta_m$ is also a proof of ε from E'. So $E' \vdash \varepsilon$. Hence $E' \vDash \varepsilon$ and $\varepsilon \in \mathrm{Cn}_\Sigma(E')$. So $\mathrm{Cn}_\Sigma(E) \subseteq \bigcup\{\, \mathrm{Cn}(E') : E' \subseteq_\omega E \,\}$. □

The closed-sets, i.e., the sets T of equations such that $\mathrm{Cn}_\Sigma(T) = T$ are called (*equational*) *theories*. T is a theory iff it is closed under consequence, i.e., $T \vDash \varepsilon$ (equivalently $T \vdash \varepsilon$) implies $\varepsilon \in T$. The theories form an algebraic closed-set system, and a complete lattice under set-theoretical inclusion. We will obtain a useful theories below.

Consider the dual closure operator $\mathsf{Mod} \circ \mathrm{Id}$ on $\mathsf{Alg}(\Sigma)$: by the Birkhoff HSP Theorem we have $\mathsf{Mod} \circ \mathrm{Id}(\mathsf{K}) = \mathbf{SHP}(\mathsf{K})$. The closed sets are the varieties. They form an closed-set system and hence are closed intersection (this is easy to verify directly); it is not however algebraic. They form a complete lattice under set-theoretical inclusion that is dually isomorphic to the lattice of theories by Thm. 4.12.

The informal method of proving an equation from a given set of equations can be formalized in a more direct way than we did Defn. 4.3. This is done in the following definition.

Definition 4.14. Let E be a set of Σ-equations. Let $\breve{I} = \{\, t \approx s : (s \approx t) \in E \,\}$. Define a relation $\equiv_E \subseteq \mathrm{Te}_\Sigma(X)^2$ as follows. $t \equiv_E s$ if there exists an equation $u(x_0, \ldots, x_{n-1}) \approx$

$v(x_0, \ldots, x_{n-1})$ in $E \cup \breve{E}$ and $w_0, \ldots, w_{n-1} \in \mathrm{Te}_\Sigma(X)$ such that t has a subterm $u(w_0, \ldots, w_{n-1})$ and s is obtained from t be replacing this subterm by $v(w_0, \ldots, w_{n-1})$.

Example. Let Σ consist of a single binary operation; as usual, we omit the operation symbol and simply concatenate terms. Suppose E contains the associtive law $(xy)z \approx x(yz)$. Let $t = \Big(\big(xy\big)\big((uw)z\big)\Big)(xy)$. Let $u(x, y, z) \approx v(x, y, z)$ be $x(yz) \approx (xy)z$ in $\breve{E}$ and let $w_0 = xy$, $w_1 = xw$, $w_2 = z$. Then $u(w_0, w_1, w_2)$ is the subterm $\big(xy\big)\big((uw)z\big)$ of t and when this is replaced by $v(w_0, w_1, w_2) = \big((xy)(uw)\big)z$ we get $s = \Big(\big((xy)(uw)\big)z\Big)(xy)$. Thus $\Big(\big(xy\big)\big((uw)z\big)\Big)(xy) \equiv_E \Big(\big((xy)(uw)\big)z\Big)(xy)$. The process of forming $\equiv_E$ can best be visualized of in terms of manipulating parse trees. See for Figure 24

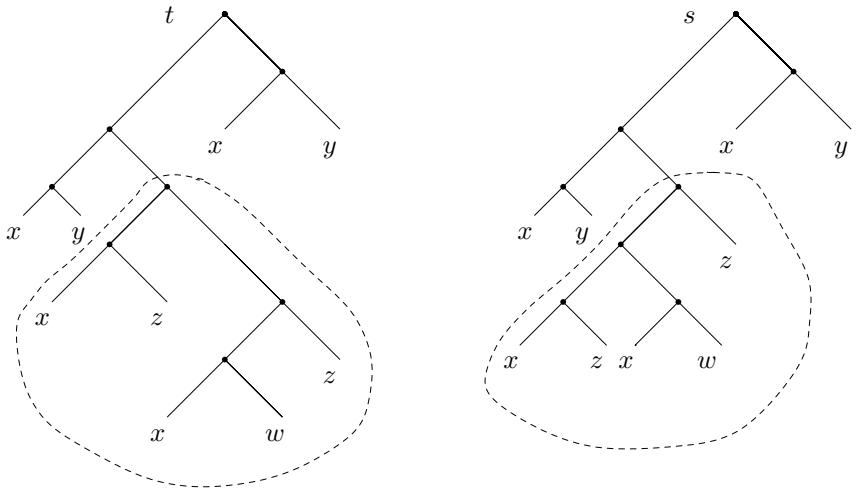


FIGURE 24

Let $\equiv_E^*$ be the the reflexive, transitive closure of $\equiv_E$. $\equiv_E$, i.e., $t \equiv_E s$ if $t = s$ or there exist $r_0, \ldots, r_m$ such that $t = r_0 \equiv_E r_1 \equiv_E \cdots \equiv_E r_m = s$.

Theorem 4.15. *For any set of Σ-equations, $E \vdash t \approx s$ iff $t \equiv_E^* s$.*

Proof. We first prove that, for each E, $\equiv_E^*$ is a congruence relation on the term algebra $\mathbf{Te}_\Sigma(X)$. It is obiously reflexive and transitive. To see it is symmetric, assume $t \equiv_E^* s$. Then s is obtained from t by replacing a subterm of the form $u(\hat{w})$ by $v(\hat{w})$ where $(u(\hat{x}) \approx v(\hat{x})) \in E \cup \breve{E}$ and $\hat{w}$ is an arbitrary choice of Σ-terms to substitute for the variables of $\hat{x}$. But clearly $v(\hat{x}) \approx u(\hat{x})$ is also in $E \cup \breve{E}$ and t is obtained from s by replacing $v(\hat{w})$ by $u(\hat{w})$. So $s \equiv_E^*$.

We now verify that $\equiv_E^*$ has that substitution property. For this purpose we introduce some useful notation. If $u(\hat{w})$ is a subterm of t, we will denote by $t[v(\hat{w})/u(v(\hat{w})]$ the term that is obtained by replacing $u(\hat{w})$ by $v(\hat{w})$. Suppose $\sigma \in \Sigma_n$ and $t_i \equiv_E^* s_i$ for each $i \leq n$. We must show that $\sigma(t_1, \ldots, t_n) \equiv_E^* \sigma(s_1, \ldots, s_n)$. For each $i \leq n$, we have $t_i = r_{i0} \equiv_E r_{i1} \equiv_E \cdots \equiv_E r_{im} = s_i$; we can assume that this sequence is the same length

m for all i by adding repetitions of the last term if needed (this uses that fact that $\equiv^*_E$ is reflexive). By the transitivity of $\equiv^*_E$ it suffices to show for all $i < n$ and all $j < m$ that

$$\sigma(r_{1(j+1)}, \ldots, r_{(i-1)(j+1)}, r_{ij}, r_{(i+1)j}, \ldots, r_{nj}) \\ \equiv_E \sigma(r_{1(j+1)}, \ldots, r_{(i-1)(j+1)}, r_{i(j+1)}, r_{(i+1)j} \ldots, r_{nj}).$$

Consequently, without loss of generality we can assume that, for some $i \leq n$, $t_i \equiv_E s_i$ and $t_j = s_j$ for all $j \neq i$. We want to show that

$$\sigma(t_1, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n) \equiv_E \sigma(t_1, \ldots, t_{i-1}, s_i, t_{i+1}, \ldots, t_n). \tag{32}$$

By assumption we have $s_i = t_i[v(\hat{w})/u(\hat{w})]$ with $(u \approx v) \in E \cup \breve{E}$. Then it is easy to see that $\sigma(t_1, \ldots, t_{i-1}, s_i, t_{i+1}, \ldots, t_n)$ is obtained from $\sigma(t_1, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n)$ by replacing the subterm $u(\hat{w})$ that occurs in t_i by $v(\hat{w})$. This gives (32). Hence $\equiv^*_E$ has the substitution property.

So $\equiv^*_E$ is a congruence relation on the formula algebra. It is *substitution-invariant* in the sense that if $t(\hat{x}) \equiv^*_E s(\hat{x})$ then $t(\hat{w}) \equiv^*_E s(\hat{w})$ for any choice of terms $\hat{w}$ to subsitute for the $\hat{x}$. This is easy to see and is left as an exercise.

$E \vdash t \approx s \Longrightarrow t \equiv^*_E s$. Let $u_1 \approx v_1, \ldots, u_n \approx v_n$ be a proof of $t \approx s$ from E. We prove that $u_i \equiv^*_E v_i$ for all $i \leq n$ by induction on i. If $u_i \approx v_i$ is a tautology then $u_i \equiv^*_E v_i$ because $\equiv^*_E$ is reflexive. If $u_i \approx v_i$ is a substitution instance of an equation in E, say $u_i \approx v_i$ is $q(\hat{w}) \approx r(\hat{w})$ with $q \approx r$ in E. Then $u_i \equiv_E v_i$ because v_i is obtained from u_i by replacing the subterm $q(\hat{w})$ by $r(\hat{w})$. If $u_i \approx v_i$ is obtained by an application of (*symm*), (*tran*), or (*repl*), then $u_i \equiv^*_E v_i$ because $\equiv^*_E$ is respectively symmetric, transitive, and has the substitution property.

$t \equiv^*_E s \Longrightarrow E \vdash t \approx s$. Because of the rules (*taut*), (*symm*), and (*tran*) it suffices to prove that $t \equiv_E s \Longrightarrow E \vdash t \approx s$. Suppose $t \equiv_E s$, say $s = t[v(\hat{w})/u(\hat{w})]$ where $v(\hat{x}) \approx u(\hat{x})$ is in $E \cup \breve{E}$. We prove $E \vdash t \approx s$ by the recursive depth of the principal operation symbol of $u(\hat{x})$ in the parse tree of t. If $t = u(\hat{w})$ then $s = v(\hat{w})$ and thus $t \equiv^*_E s$ by (*E-axiom*) or by (*E-axiom*) together with (*symm*). Assume $t = \sigma(q_1, \ldots, q_n)$ and $u(\hat{w})$ is a subterm of q_i so that $s = \sigma(q_1, \ldots, q_i[v(\hat{w})/u(\hat{w})], \ldots, q_n)$. Then $q_i \equiv^*_E q_i[v(\hat{w})/u(\hat{w})]$ and hence $E \vdash q_i \approx q_i[v(\hat{w})/u(\hat{w})]$ by the induction hypothesis. Hence $E \vdash t \approx s$ by (*repl*). □

Recalling again that equations are elements of $Te_\Sigma(X)^2$ we see that $\mathrm{Cn}_\Sigma(E) = \{\, \langle t, s\rangle : E \vdash t \approx s \,\} = \equiv^*_E$. So equational theories are exactly the subtitution-invariant congruence relations on $\mathbf{Te}_\Sigma(X)$. Then the Galois connection between consequence between Id and Mod induces a dual isomorphism between the lattice of Σ-varieties and the lattice of substution-invariant congruences on $\mathbf{Te}_\Sigma(X)$.