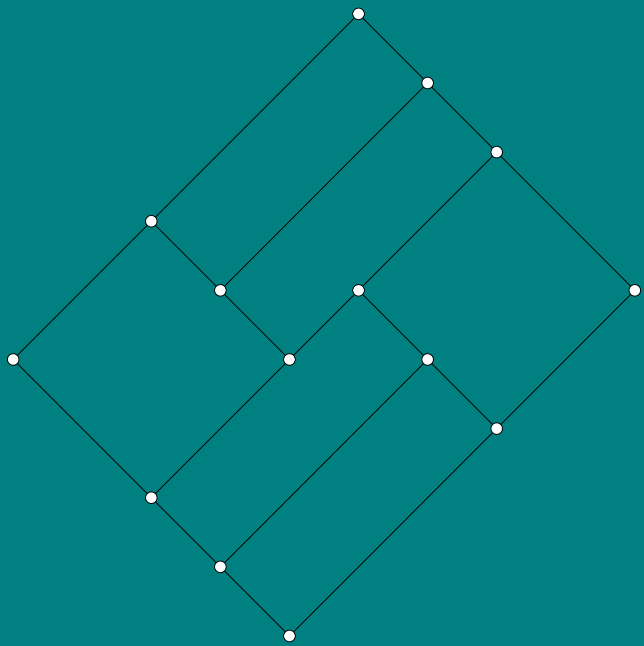
Notes on Lattice Theory



J. B. Nation
University of Hawaii

Introduction

In the early 1890's, Richard Dedekind was working on a revised and enlarged edition of Dirichlet's *Vorlesungen über Zahlentheorie*, and asked himself the following question: Given three subgroups $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ of an abelian group $\mathcal{G}$, how many different subgroups can you get by taking intersections and sums, e.g., $\mathcal{A}+\mathcal{B}$, $(\mathcal{A}+\mathcal{B})\cap\mathcal{C}$, etc. The answer, as we shall see, is 28 (Chapter 7). In looking at this and related questions, Dedekind was led to develop the basic theory of lattices, which he called *Dualgruppen*. His two papers on the subject, *Über Zerlegungen von Zahlen durch ihre größten gemeinsamen Teiler* (1897) and *Über die von drei Moduln erzeugte Dualgruppe* (1900), are classics, remarkably modern in spirit, which have inspired many later mathematicians.

"There is nothing new under the sun," and so Dedekind found. Lattices, especially distributive lattices and Boolean algebras, arise naturally in logic, and thus some of the elementary theory of lattices had been worked out earlier by Ernst Schröder in his book *Die Algebra der Logik*. Nonetheless, it is the connection between modern algebra and lattice theory, which Dedekind recognized, that provided the impetus for the development of lattice theory as a subject, and which remains our primary interest.

Unfortunately, Dedekind was ahead of his time in making this connection, and so nothing much happened in lattice theory for the next thirty years. Then, with the development of universal algebra in the 1930's by Garrett Birkhoff, Oystein Ore and others, Dedekind's work on lattices was rediscovered. From that time on, lattice theory has been an active and growing subject, in terms of both its application to algebra and its own intrinsic questions.

These notes are intended as the basis for a one-semester introduction to lattice theory. Only a basic knowledge of modern algebra is presumed, and I have made no attempt to be comprehensive on any aspect of lattice theory. Rather, the intention is to provide a textbook covering what we lattice theorists would like to think every mathematician should know about the subject, with some extra topics thrown in for flavor, all done thoroughly enough to provide a basis for a second course for the student who wants to go on in lattice theory or universal algebra.

It is a pleasure to acknowledge the contributions of students and colleagues to these notes. I am particularly indebted to Michael Tischendorf, Alex Pogel and the referee for their comments. *Mahalo* to you all.

Finally, I hope these notes will convey some of the beauty of lattice theory as I learned it from two wonderful teachers, Bjarni Jónsson and Bob Dilworth.

1. Ordered Sets

"And just how far would you like to go in?" he asked....
"Not too far but just far enough so's we can say that we've been there," said the first chief.
"All right," said Frank, "I'll see what I can do."
–Bob Dylan

In group theory, groups are defined algebraically as a model of permutations. The Cayley representation theorem then shows that this model is "correct": every group is isomorphic to a group of permutations. In the same way, we want to define a partial order to be an abstract model of set containment $\subseteq$, and then we should prove a representation theorem for partially ordered sets in terms of containment.

A *partially ordered set*, or more briefly just *ordered set*, is a system $\mathcal{P} = (P, \leq)$ where P is a nonempty set and $\leq$ is a binary relation on P satisfying, for all $x, y, z \in P$,

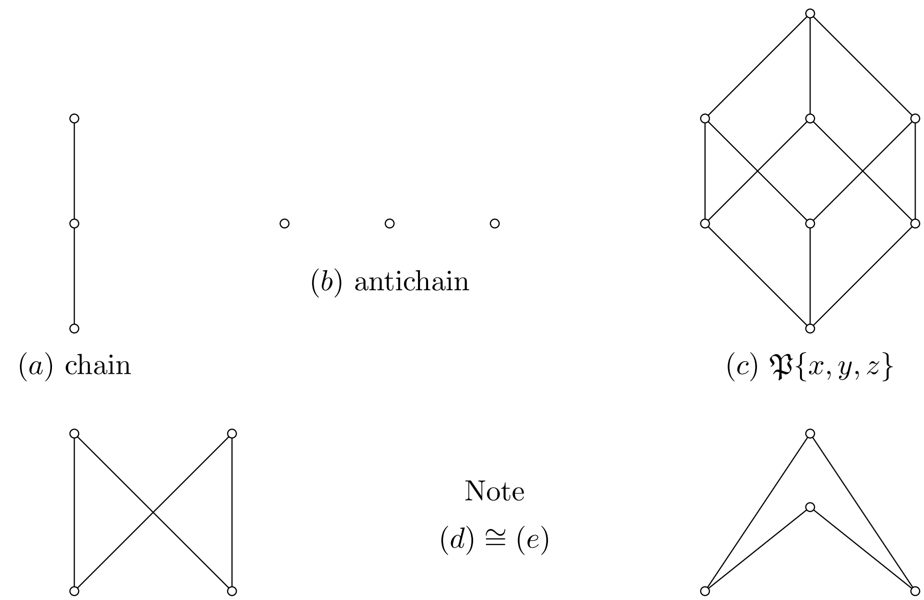
(1) $x \leq x$, (*reflexivity*)
(2) if $x \leq y$ and $y \leq x$, then $x = y$, (*antisymmetry*)
(3) if $x \leq y$ and $y \leq z$, then $x \leq z$. (*transitivity*)

The most natural example of an ordered set is $\mathfrak{P}(X)$, the collection of all subsets of a set X, ordered by $\subseteq$. Another familiar example is **Sub** $\mathcal{G}$, all subgroups of a group $\mathcal{G}$, again ordered by set containment. You can think of lots of examples of this type. Indeed, any nonempty collection Q of subsets of X, ordered by set containment, forms an ordered set.

More generally, if $\mathcal{P}$ is an ordered set and $Q \subseteq P$, then the restriction of $\leq$ to Q is a partial order, leading to a new ordered set $\mathcal{Q}$.

The set $\Re$ of real numbers with its natural order is an example of a rather special type of partially ordered set, namely a totally ordered set, or chain. $\mathcal{C}$ is a *chain* if for every $x, y \in C$, either $x \leq y$ or $y \leq x$. At the opposite extreme we have *antichains*, ordered sets in which $\leq$ coincides with the equality relation $=$.

We say that x *is covered by* y in $\mathcal{P}$, written $x \prec y$, if $x < y$ and there is no $z \in P$ with $x < z < y$. It is clear that the covering relation determines the partial order in a finite ordered set $\mathcal{P}$. In fact, the order $\leq$ is the smallest reflexive, transitive relation containing $\prec$. We can use this to define a *Hasse diagram* for a finite ordered set $\mathcal{P}$: the elements of P are represented by points in the plane, and a line is drawn from a up to b precisely when $a \prec b$. In fact this description is not precise, but it



(a) chain (b) antichain (c) $\mathfrak{P}\{x, y, z\}$

(d) Note $(d) \cong (e)$ (e)

FIGURE 1.1

is close enough for government purposes. In particular, we can now generate lots of examples of ordered sets using Hasse diagrams, as in Figure 1.1.

The natural maps associated with the category of ordered sets are the *order preserving* maps, those satisfying the condition $x \leq y$ implies $f(x) \leq f(y)$. We say that $\mathcal{P}$ is *isomorphic* to $\mathcal{Q}$, written $\mathcal{P} \cong \mathcal{Q}$, if there is a map $f : P \to Q$ which is one-to-one, onto, and both f and f^{-1} are order preserving, i.e., $x \leq y$ iff $f(x) \leq f(y)$.

With that we can state the desired representation of any ordered set as a system of sets ordered by containment.

Theorem 1.1. *Let $\mathcal{Q}$ be an ordered set, and let $\phi : Q \to \mathfrak{P}(Q)$ be defined by*

$$\phi(x) = \{y \in Q : y \leq x\}.$$

Then Q is isomorphic to the range of ϕ ordered by $\subseteq$.

Proof. If $x \leq y$, then $z \leq x$ implies $z \leq y$ by transitivity, and hence $\phi(x) \subseteq \phi(y)$. Since $x \in \phi(x)$ by reflexivity, $\phi(x) \subseteq \phi(y)$ implies $x \leq y$. Thus $x \leq y$ iff $\phi(x) \subseteq \phi(y)$. That ϕ is one-to-one then follows by antisymmetry. $\square$

A subset I of $\mathcal{P}$ is called an *order ideal* if $x \leq y \in I$ implies $x \in I$. The set of all order ideals of $\mathcal{P}$ forms an ordered set $\mathcal{O}(\mathcal{P})$ under set inclusion. The map

ϕ of Theorem 1.1 embeds $\mathcal{Q}$ in $\mathcal{O}(\mathcal{Q})$. Note that we have the additional property that the intersection of any collection of order ideals of $\mathcal{P}$ is again in an order ideal (which may be empty). Likewise, the union of a collection of order ideals is an order ideal.

Given an ordered set $\mathcal{P} = (P, \leq)$, we can form another ordered set $\mathcal{P}^d = (P, \leq^d)$, called the *dual* of $\mathcal{P}$, with the order relation defined by $x \leq^d y$ iff $y \leq x$. In the finite case, the Hasse diagram of $\mathcal{P}^d$ is obtained by simply turning the Hasse diagram of $\mathcal{P}$ upside down (see Figure 1.2). Many concepts concerning ordered sets come in dual pairs, where one version is obtained from the other by replacing "$\leq$" by "$\geq$" throughout.

$\mathcal{P}$ FIGURE 1.2 $\mathcal{P}^d$

For example, a subset F of $\mathcal{P}$ is called an *order filter* if $x \geq y \in F$ implies $x \in F$. An order ideal of $\mathcal{P}$ is an order filter of $\mathcal{P}^d$, and *vice versa*.

An ideal or filter determined by a single element is said to be *principal*. We denote principal ideals and principal filters by

$$\downarrow x = \{y \in P : y \leq x\},$$
$$\uparrow x = \{y \in P : y \geq x\},$$

respectively.

The ordered set $\mathcal{P}$ has a *maximum* (or *greatest*) element if there exists $x \in P$ such that $y \leq x$ for all $y \in P$. An element $x \in P$ is *maximal* if there is no element $y \in P$ with $y > x$. Clearly these concepts are different. *Minimum* and *minimal* elements are defined dually.

The next lemma is simple but particularly important.

Lemma 1.2. *The following are equivalent for an ordered set $\mathcal{P}$.*

(1) *Every nonempty subset $S \subseteq P$ contains an element minimal in S.*
(2) *$\mathcal{P}$ contains no infinite descending chain*

$$a_0 > a_1 > a_2 > \dots$$

(3) *If*

$$a_0 \geq a_1 \geq a_2 \geq \dots$$

in $\mathcal{P}$, then there exists k such that $a_n = a_k$ for all $n \geq k$.

Proof. The equivalence of (2) and (3) is clear, and likewise that (1) implies (2). There is, however, a subtlety in the proof of (2) implies (1). Suppose $\mathcal{P}$ fails (1) and that $S \subseteq P$ has no minimal element. In order to find an infinite descending chain in S, rather than just arbitrarily long finite chains, we must use the Axiom of Choice. One way to do this is as follows.

Let f be a choice function on the subsets of S, i.e., f assigns to each nonempty subset $T \subseteq S$ an element $f(T) \in T$. Let $a_0 = f(S)$, and for each $i \in \omega$ define $a_{i+1} = f(\{s \in S : s < a_i\})$; the argument of f in this expression is nonempty because S has no minimal element. The sequence so defined is an infinite descending chain, and hence $\mathcal{P}$ fails (2). $\square$

The conditions described by the preceding lemma are called the *descending chain condition* (DCC). The dual notion is called the *ascending chain condition* (ACC). These conditions should be familiar to you from ring theory (for ideals). The next lemma just states that ordered sets satisfying the DCC are those for which the principle of induction holds.

Lemma 1.3. *Let $\mathcal{P}$ be an ordered set satisfying the DCC. If $\varphi(x)$ is a statement such that*

(1) *$\varphi(x)$ holds for all minimal elements of P, and*
(2) *whenever $\varphi(y)$ holds for all $y < x$, then $\varphi(x)$ holds,*

then $\varphi(x)$ is true for every element of P.

Note that (1) is in fact a special case of (2). It is included in the statement of the lemma because in practice minimal elements usually require a separate argument (like the case $n = 0$ in ordinary induction).

The proof is immediate. The contrapositive of (2) states that the set $F = \{x \in P : \varphi(x) \text{ is false}\}$ has no minimal element. Since $\mathcal{P}$ satisfies the DCC, F must therefore be empty.

We now turn our attention more specifically to the structure of ordered sets. Define the *width* of an ordered set $\mathcal{P}$ by

$$w(\mathcal{P}) = sup\{|A| : A \text{ is an antichain in } \mathcal{P}\}$$

where $|A|$ denotes the cardinality of A.[1] A second invariant is the *chain covering number* $c(\mathcal{P})$, defined to be the least cardinal γ such that P is the union of γ chains in $\mathcal{P}$. Because no chain can contain more than one element of a given antichain, we must have $|A| \leq |I|$ whenever A is an antichain in $\mathcal{P}$ and $P = \bigcup_{i \in I} C_i$ is a chain covering. Therefore

$$w(\mathcal{P}) \leq c(\mathcal{P})$$

[1] Note that the width function $w(\mathcal{P})$ does not distinguish, for example, between ordered sets that contain arbitrarily large finite antichains and those that contain a countably infinite antichain. For this reason, in ordered sets of infinite width it is sometimes useful to consider the function $\mu(\mathcal{P})$, which is defined to be the least cardinal κ such that $\kappa + 1 > |A|$ for every antichain A of $\mathcal{P}$. We will restrict our attention to $w(\mathcal{P})$.

for any ordered set $\mathcal{P}$. The following result, due to R. P. Dilworth [2], says in particular that if $\mathcal{P}$ is finite, then $w(\mathcal{P}) = c(\mathcal{P})$.

Theorem 1.4. *If $w(\mathcal{P})$ is finite, then $w(\mathcal{P}) = c(\mathcal{P})$.*

Our discussion of the proof will take the scenic route. We begin with the case when $\mathcal{P}$ is finite, using H. Tverberg's nice proof [17].

Proof in the finite case. We need to show $c(\mathcal{P}) \leq w(\mathcal{P})$, which is done by induction on $|P|$. Let $w(\mathcal{P}) = k$, and let C be a maximal chain in $\mathcal{P}$. If $\mathcal{P}$ is a chain, $w(\mathcal{P}) = c(\mathcal{P}) = 1$, so assume $C \neq \mathcal{P}$. Because C can contain at most one element of any maximal antichain, the width $w(\mathcal{P} - C)$ is either k or $k-1$, and both possibilities can occur. If $w(\mathcal{P} - C) = k - 1$, then $\mathcal{P} - C$ is the union of $k - 1$ chains, whence $\mathcal{P}$ is a union of k chains.

So suppose $w(\mathcal{P} - C) = k$, and let $A = \{a_1, \ldots, a_k\}$ be a maximal antichain in $\mathcal{P} - C$. As $|A| = k$, it is also a maximal antichain in $\mathcal{P}$. Set

$$L = \{x \in P : x \leq a_i \text{ for some } i\},$$
$$U = \{x \in P : x \geq a_j \text{ for some } j\}.$$

Since every element of P is comparable with some element of A, we have $P = L \cup U$, while $A = L \cap U$. Moreover, the maximality of C insures that the largest element of C does not belong to L (remember $A \subseteq P - C$), so $|L| < |P|$. Dually, $|U| < |P|$ also. Hence L is a union of k chains, $L = D_1 \cup \cdots \cup D_k$, and similarly $U = E_1 \cup \cdots \cup E_k$ as a union of chains. By renumbering, if necessary, we may assume that $a_i \in D_i \cap E_i$ for $1 \leq i \leq k$, so that $C_i = D_i \cup E_i$ is a chain. Thus

$$P = L \cup U = C_1 \cup \cdots \cup C_k$$

is a union of k chains. $\square$

So now we want to consider an infinite ordered set $\mathcal{P}$ of finite width k. Not surprisingly, we will want to use one of the 210 equivalents of the Axiom of Choice! (See H. Rubin and J. Rubin [14].) This requires some standard terminology.

Let $\mathcal{P}$ be an ordered set, and let S be a subset of P. We say that an element $x \in P$ is an *upper bound* for S if $x \geq s$ for all $s \in S$. An upper bound x need not belong to S. We say that x is the *least upper bound* for S if x is an upper bound for S and $x \leq y$ for every upper bound y of S. If the least upper bound of S exists, then it is unique. *Lower bound* and *greatest lower bound* are defined dually.

Theorem 1.5. *The following set theoretic axioms are equivalent.*

1. (Axiom of Choice) *If X is a nonempty set, then there is a map $\phi : \mathfrak{P}(X) \to X$ such that $\phi(A) \in A$ for every nonempty $A \subseteq X$.*
2. (Zermelo well-ordering principle) *Every nonempty set admits a well-ordering (a total order satisfying the DCC).*

(3) (Hausdorff maximality principle) *Every chain in an ordered set $\mathcal{P}$ can be embedded in a maximal chain.*
(4) (Zorn's Lemma) *If every chain in an ordered set $\mathcal{P}$ has an upper bound in $\mathcal{P}$, then $\mathcal{P}$ contains a maximal element.*
(5) *If every chain in an ordered set $\mathcal{P}$ has a least upper bound in $\mathcal{P}$, then $\mathcal{P}$ contains a maximal element.*

The proof of Theorem 1.5 is given in Appendix 2.

Our plan is to use Zorn's Lemma to prove the compactness theorem (due to K. Gödel [6]); then, following a suggestion of Bjarni Jónsson, use the compactness theorem to prove the infinite case of Dilworth's theorem. We need to first recall some of the basics of sentential logic.

Let S be a set, whose members will be called sentence symbols. Initially the sentence symbols carry no intrinsic meaning; in applications they will correspond to various mathematical statements.

We define *well formed formulas* (wff) on S by the following rules.

(1) Every sentence symbol is a wff.
(2) If α and β are wffs, then so are $(\neg\alpha)$, $(\alpha \text{ AND } \beta)$ and $(\alpha \text{ OR } \beta)$.
(3) Only symbols generated by the first two rules are wffs.

The set of all wffs on S is denoted by $\overline{S}$.[2]

A *truth assignment* on S is a map $\nu : S \to \{T, F\}$. Each truth assignment has a natural extension $\overline{\nu} : \overline{S} \to \{T, F\}$. The map $\overline{\nu}$ is defined recursively by the rules

(1) $\overline{\nu}(\neg\varphi) = T$ if and only if $\overline{\nu}(\varphi) = F$,
(2) $\overline{\nu}(\varphi \text{ AND } \psi) = T$ if and only if $\overline{\nu}(\varphi) = T$ and $\overline{\nu}(\psi) = T$,
(3) $\overline{\nu}(\varphi \text{ OR } \psi) = T$ if and only if $\overline{\nu}(\varphi) = T$ or $\overline{\nu}(\psi) = T$ (including the case that both are equal to T).

A set $\Sigma \subseteq \overline{S}$ is *satisfiable* if there exists a truth assignment ν such that $\overline{\nu}(\varphi) = T$ for all $\varphi \in \Sigma$. Σ is *finitely satisfiable* if every finite subset $\Sigma_0 \subseteq \Sigma$ is satisfiable. Note that these concepts refer only to the internal consistency of Σ; there is so far no meaning attached to the sentence symbols themselves.

Theorem 1.6. (The compactness theorem) *A set of wffs is satisfiable if and only if it is finitely satisfiable.*

Proof. Let S be a set of sentence symbols and $\overline{S}$ the corresponding set of wffs. Assume that $\Sigma \subseteq \overline{S}$ is finitely satisfiable. Using Zorn's Lemma, let Δ be maximal in $\mathfrak{P}(\overline{S})$ such that

(1) $\Sigma \subseteq \Delta$,
(2) Δ is finitely satisfiable.

[2]Technically, $\overline{S}$ is just the absolutely free algebra generated by S with the operation symbols given in (2). We use AND and OR in place of the traditional symbols $\wedge$ and $\vee$ for conjunction and disjunction, respectively, in order to avoid confusion with the lattice operations in later chapters, while retaining the symbol $\neg$ for negation.

We claim that for all $\varphi \in \overline{S}$, either $\varphi \in \Delta$ or $(\neg\varphi) \in \Delta$ (but of course not both).

Otherwise, by the maximality of Δ, we could find a finite subset $\Delta_0 \subseteq \Delta$ such that $\Delta_0 \cup \{\varphi\}$ is not satisfiable, and a finite subset $\Delta_1 \subseteq \Delta$ such that $\Delta_1 \cup \{\neg\varphi\}$ is not satisfiable. But $\Delta_0 \cup \Delta_1$ is satisfiable, say by a truth assignment ν. If $\overline{\nu}(\varphi) = T$, this contradicts the choice of Δ_0, while $\overline{\nu}(\neg\varphi) = T$ contradicts the choice of Δ_1. So the claim holds.

Now define a truth assignment μ as follows. For each sentence symbol $p \in S$, define

$$\mu(p) = T \quad \text{iff} \quad p \in \Delta \ .$$

Now we claim that for all $\varphi \in \overline{S}$, $\overline{\mu}(\varphi) = T$ iff $\varphi \in \Delta$. This will yield $\overline{\mu}(\varphi) = T$ for all $\varphi \in \Sigma$, so that Σ is satisfiable.

To prove this last claim, let $G = \{\varphi \in \overline{S} : \overline{\mu}(\varphi) = T \text{ iff } \varphi \in \Delta\}$. We have $S \subseteq G$, and we need to show that G is closed under the operations $\neg$, AND and OR, so that $G = \overline{S}$.

(1) Suppose $\varphi = \neg\beta$ with $\beta \in G$. Then, using the first claim,

$$\begin{aligned} \overline{\mu}(\varphi) = T \quad & \text{iff} \quad \overline{\mu}(\beta) = F \\ & \text{iff} \quad \beta \notin \Delta \\ & \text{iff} \quad \neg\beta \in \Delta \\ & \text{iff} \quad \varphi \in \Delta \ . \end{aligned}$$

Hence $\varphi = \neg\beta \in G$.

(2) Suppose $\varphi = \alpha \text{ AND } \beta$ with $\alpha, \beta \in G$. Note that $\alpha \text{ AND } \beta \in \Delta$ iff $\alpha \in \Delta$ and $\beta \in \Delta$. For if $\alpha \text{ AND } \beta \in \Delta$, since $\{\alpha \text{ AND } \beta, \neg\alpha\}$ is not satisfiable we must have $\alpha \in \Delta$, and similarly $\beta \in \Delta$. Conversely, if $\alpha \in \Delta$ and $\beta \in \Delta$, then since $\{\alpha, \beta, \neg(\alpha \text{ AND } \beta)\}$ is not satisfiable, we have $\alpha \text{ AND } \beta \in \Delta$. Thus

$$\begin{aligned} \overline{\mu}(\varphi) = T \quad & \text{iff} \quad \overline{\mu}(\alpha) = T \text{ and } \overline{\mu}(\beta) = T \\ & \text{iff} \quad \alpha \in \Delta \text{ and } \beta \in \Delta \\ & \text{iff} \quad (\alpha \text{ AND } \beta) \in \Delta \\ & \text{iff} \quad \varphi \in \Delta. \end{aligned}$$

Hence $\varphi = (\alpha \text{ AND } \beta) \in G$.

(3) The case $\varphi = \alpha \text{ OR } \beta$ is similar to (2). $\square$

We return to considering an infinite ordered set $\mathcal{P}$ of width k. Let $S = \{c_{xi} : x \in P,\ 1 \leq i \leq k\}$. We think of c_{xi} as corresponding to the statement "x is in the i-th chain." Let Σ be all sentences of the form

(a) $$c_{x1} \text{ OR } \ldots \text{ OR } c_{xk}$$

for $x \in P$, and

(b) $$\neg(c_{xi} \text{ AND } c_{yi})$$

for all incomparable pairs $x, y \in P$ and $1 \leq i \leq k$. By the finite version of Dilworth's theorem, Σ is finitely satisfiable, so by the compactness theorem Σ is satisfiable, say by ν. We obtain the desired representation by putting $C_i = \{x \in P : \nu(c_{xi}) = T\}$. The sentences (a) insure that $C_1 \cup \cdots \cup C_k = P$, and the sentences (b) say that each C_i is a chain.

This completes the proof of Theorem 1.4.

A nice example due to M. Perles shows that Dilworth's theorem is no longer true when the width is allowed to be infinite [11]. Let κ be an infinite ordinal,[3] and let $\mathcal{P}$ be the direct product $\kappa \times \kappa$, ordered pointwise. Then $\mathcal{P}$ has no infinite antichains, so $w(\mathcal{P}) = \aleph_0$, but $c(\mathcal{P}) = |\kappa|$.

There is a nice discussion of the consequences and extensions of Dilworth's Theorem in Chapter 1 of [1]. Algorithmic aspects are discussed in Chapter 11 of [4], while a nice alternate proof appears in F. Galvin [5].

It is clear that the collection of all partial orders on a set X, ordered by set inclusion, is itself an ordered set $\mathcal{PO}(X)$. The least member of $\mathcal{PO}(X)$ is the equality relation, corresponding to the antichain order. The maximal members of $\mathcal{PO}(X)$ are the various total (chain) orders on X. Note that the intersection of a collection of partial orders on X is again a partial order. The next theorem, due to E. Szpilrajn, expresses an arbitrary partial ordering as an intersection of total orders [16].[4]

Theorem 1.7. *Every partial ordering on a set X is the intersection of the total orders on X containing it.*

Szpilrajn's theorem is a consequence of the next lemma.

Lemma 1.8. *Given an ordered set $(P, \leq)$ and $a \nleq b$, there exists an extension $\leq^*$ of $\leq$ such that $(P, \leq^*)$ is a chain and $b <^* a$.*

Proof. Let $a \nleq b$ in $\mathcal{P}$. Then the transitive closure of $\leq \cup (b, a)$ is a partial order extending $\leq$ in which $b <' a$. Explicitly, let

$$x \leq' y \quad \text{if} \quad \begin{cases} x \leq y \\ \text{or} \\ x \leq b \text{ and } a \leq y. \end{cases}$$

It is straightforward to check that this is a partial order.

[3] See Appendix 1.

[4] The Polish logician Edward Szpilrajn changed his last name to Marczewski in 1940 to avoid Nazi persecution, and survived the war.

If P is finite, repeated application of this construction yields a total order $\leq^*$ extending $\leq'$, so that $b <^* a$. For the infinite case, we can either use the compactness theorem, or perhaps easier Zorn's Lemma (the union of a chain of partial orders on X is again one) to obtain a total order $\leq^*$ extending $\leq'$. $\square$

Theorem 1.7 now follows, because the intersection of all such extensions contains only the pairs (c, d) with $c \leq d$.

Define the *dimension* $d(\mathcal{P})$ of an ordered set $\mathcal{P}$ to be the smallest cardinal κ such that the order $\leq$ on $\mathcal{P}$ is the intersection of κ total orders. The next result summarizes two basic facts about the dimension.

Theorem 1.9. *Let $\mathcal{P}$ be an ordered set. Then*

(1) *$d(\mathcal{P})$ is the smallest cardinal γ such that $\mathcal{P}$ can be embedded into the direct product of γ chains,*
(2) *$d(\mathcal{P}) \leq c(\mathcal{P})$.*

Proof. First suppose $\leq$ is the intersection of total orders $\leq_i$ $(i \in I)$ on P. If we let C_i be the chain $(P, \leq_i)$, then it is easy to see that the natural map $\varphi : P \to \prod_{i \in I} C_i$, with $(\varphi(x))_i = x$ for all $x \in P$, satisfies $x \leq y$ iff $\varphi(x) \leq \varphi(y)$. Hence φ is an embedding.

Conversely, assume $\varphi : P \to \prod_{i \in I} C_i$ is an embedding of P into a direct product of chains. We want to show that this leads to a representation of $\leq$ as the intersection of $|I|$ total orders. Define

$$x \; R_i \; y \quad \text{if} \quad \begin{cases} x \leq y \\ \text{or} \\ \varphi(x)_i < \varphi(y)_i \; . \end{cases}$$

You should check that R_i is a partial order extending $\leq$. By Lemma 1.8 each R_i can be extended to a total order $\leq_i$ extending $\leq$. To see that $\leq$ is the intersection of the $\leq_i$'s, suppose $x \nleq y$. Since φ is an embedding, then $\varphi(x)_i \nleq \varphi(y)_i$ for some i. Thus $\varphi(x)_i > \varphi(y)_i$, implying $y \; R_i \; x$ and hence $y \leq_i x$, or equivalently $x \nleq_i y$ (as $x \neq y$), as desired.

Thus the order on $\mathcal{P}$ is the intersection of κ total orders if and only if $\mathcal{P}$ can be embedded into the direct product of κ chains, yielding (1).

For (2), assume $P = \bigcup_{j \in J} C_j$ with each C_j a chain. Then, for each $j \in J$, the ordered set $\mathcal{O}(C_j)$ of order ideals of C_j is also a chain. Define a map $\varphi : P \to \prod_{j \in J} \mathcal{O}(C_j)$ by $(\varphi(x))_j = \{y \in C_j : y \leq x\}$. (Note $\emptyset \in \mathcal{O}(C_j)$, and $(\varphi(x))_j = \emptyset$ is certainly possible.) Then φ is clearly order-preserving. On the other hand, if $x \nleq y$ in P and $x \in C_j$, then $x \in (\varphi(x))_j$ and $x \notin (\varphi(y))_j$, so $(\varphi(x))_j \nsubseteq (\varphi(y))_j$ and $\varphi(x) \nleq \varphi(y)$. Thus P can be embedded into a direct product of $|J|$ chains. Using (1), this shows $d(P) \leq c(P)$. $\square$

Now we have three invariants defined on ordered sets: $w(P)$, $c(P)$ and $d(P)$. The exercises will provide you an opportunity to work with these in concrete cases. We have shown that $w(P) \leq c(P)$ and $d(P) \leq c(P)$, but width and dimension are independent. Indeed, if κ is an ordinal and κ^d its dual, then $\kappa \times \kappa^d$ has width $|\kappa|$ but dimension 2. It is a little harder to find examples of high dimension but low width (necessarily infinite by Dilworth's theorem), but it is possible (see [10] or [12]).

This concludes our brief introduction to ordered sets *per se*. We have covered only the most classical results of what is now an active field of research. A standard textbook is Schröder [15]; for something completely different, see Harzheim [7].

The journal **Order** is devoted to publishing results on ordered sets. The author's favorite papers in this field include Duffus and Rival [3], Jónsson and McKenzie [8], [9] and Roddy [13].

Exercises for Chapter 1

1. Draw the Hasse diagrams for all 4-element ordered sets (up to isomorphism).

2. Let N denote the positive integers. Show that the relation $a \mid b$ (a divides b) is a partial order on N. Draw the Hasse diagram for the ordered set of all divisors of 60.

3. A *partial map* on a set X is a map $\sigma : S \to X$ where $S = dom\ \sigma$ is a subset of X. Define $\sigma \leq \tau$ if $dom\ \sigma \subseteq dom\ \tau$ and $\tau(x) = \sigma(x)$ for all $x \in dom\ \sigma$. Show that the collection of all partial maps on X is an ordered set.

4. (a) Give an example of a map $f : \mathcal{P} \to \mathcal{Q}$ that is one-to-one, onto and order-preserving, but not an isomorphism.

(b) Show that the following are equivalent for ordered sets $\mathcal{P}$ and $\mathcal{Q}$.

(i) $\mathcal{P} \cong \mathcal{Q}$ (as defined before Theorem 1.1).
(ii) There exists $f : P \twoheadrightarrow Q$ such that $f(x) \leq f(y)$ iff $x \leq y$. ($\twoheadrightarrow$ means the map is onto.)
(iii) There exist $f : P \to Q$ and $g : Q \to P$, both order-preserving, with $gf = id_P$ and $fg = id_Q$.

5. Find all order ideals of the rational numbers $\mathbb{Q}$ with their usual order.

6. Prove that all chains in an ordered set $\mathcal{P}$ are finite if and only if $\mathcal{P}$ satisfies both the ACC and DCC.

7. Find $w(\mathcal{P})$, $c(\mathcal{P})$ and $d(\mathcal{P})$ for

(a) an antichain $\mathcal{A}$ with $|A| = \kappa$, where κ is a cardinal,
(b) $\mathcal{M}_\kappa$, where κ is a cardinal, the ordered set diagrammed in Figure 1.3(a).
(c) an n-crown, the ordered set diagrammed in Figure 1.3(b).
(d) $\mathfrak{P}(X)$ with X a finite set,
(e) $\mathfrak{P}(X)$ with X infinite.

8. Embed $\mathcal{M}_n$ ($2 \leq n < \infty$) into a direct product of two chains. Express the order on $\mathcal{M}_n$ as the intersection of two totally ordered extensions.

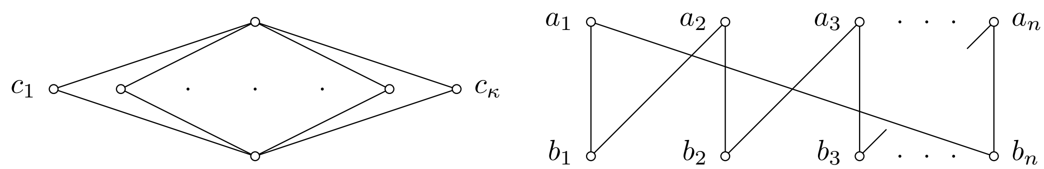


FIGURE 1.3

9. Let $\mathcal{P}$ be a finite ordered set with at least $ab + 1$ elements. Prove that $\mathcal{P}$ contains either an antichain with $a + 1$ elements, or a chain with $b + 1$ elements.

10. Phillip Hall proved that if X is a finite set and $S_1, \ldots, S_n$ are subsets of X, then there is a system of distinct representatives (SDR) $a_1, \ldots, a_n$ with $a_j \in S_j$ if and only if for all $1 \leq k \leq n$ and distinct indices $i_1, \ldots, i_k$ we have $|\bigcup_{1 \leq j \leq k} S_{i_j}| \geq k$.

(a) Derive this result from Dilworth's theorem.
(b) Prove Marshall Hall's extended version: If S_i $(i \in I)$ are finite subsets of a (possibly infinite) set X, then they have an SDR if and only if the condition of P. Hall's theorem holds for every n.

11. Let R be a binary relation on a set X that contains no cycle of the form $x_0 \, R \, x_1 \, R \, \ldots R \, x_n \, R \, x_0$ with $x_i \neq x_{i+1}$. Show that the reflexive transitive closure of R is a partial order.

12. A reflexive, transitive, binary relation is called a *quasiorder*.

(a) Let R be a quasiorder on a set X. Define $x \equiv y$ if $x \, R \, y$ and $y \, R \, x$. Prove that $\equiv$ is an equivalence relation, and that R induces a partial order on $X/\!\equiv$.
(b) Let $\mathcal{P}$ be an ordered set, and define a relation $\ll$ on the subsets of P by $X \ll Y$ if for each $x \in X$ there exists $y \in Y$ with $x \leq y$. Verify that $\ll$ is a quasiorder.

13. Let R be any relation on a nonempty set X. Describe the smallest quasiorder containing R.

14. Let ω_1 denote the first uncountable ordinal.

(a) Let $\mathcal{P}$ be the direct product $\omega_1 \times \omega_1$. Prove that every antichain of $\mathcal{P}$ is finite, but $c(\mathcal{P}) = \aleph_1$.
(b) Let $\mathcal{Q} = \omega_1 \times \omega_1^d$. Prove that $\mathcal{Q}$ has width $\aleph_1$ but dimension 2.

15. Generalize exercise 14(a) to the direct product of two ordinals, $\mathcal{P} = \kappa \times \lambda$. Describe the maximal antichains in $\kappa \times \lambda$.

REFERENCES

1. K. Bogart, R. Freese and J. Kung, Eds., *The Dilworth Theorems*, Birkhäuser, Boston, Basel, Berlin, 1990.

2. R. P. Dilworth, *A decomposition theorem for partially ordered sets*, Annals of Math. **51** (1950), 161–166.
3. D. Duffus and I. Rival, *A structure theorey for ordered sets*, Discrete Math. **35** (1981), 53–118.
4. R. Freese, J. Ježek and J. B. Nation, *Free Lattices*, Mathematical Surveys and Monographs, vol. 42, Amer. Math. Soc., Providence, R. I., 1995.
5. F. Galvin, *A proof of Dilworth's chain decomposition theorem*, Amer. Math. Monthly **101** (1994), 352–353.
6. K. Gödel, *Die Vollständigkeit der Axiome des logischen Funktionenkalküls*, Monatsh. Math. Phys. **37** (1930), 349–360.
7. E. Harzheim, *Ordered Sets*, vol. 7, Springer, Advances in Mathematics, New York, 2005.
8. B. Jónsson and R. McKenzie, *Powers of partially ordered sets: cancellation and refinement properties*, Math. Scand. **51** (1982), 87–120.
9. B. Jónsson and R. McKenzie, *Powers of partially ordered sets: the automorphism group*, Math. Scand. **51** (1982), 121–141.
10. J. B. Nation, D. Pickering and J. Schmerl, *Dimension may exceed width*, Order **5** (1988), 21–22.
11. M. A. Perles, *On Dilworth's theorem in the infinite case*, Israel J. Math. **1** (1963), 108–109.
12. M. Pouzet, *Généralisation d'une construction de Ben-Dushnik et E. W. Miller*, Comptes Rendus Acad. Sci. Paris **269** (1969), 877–879.
13. M. Roddy, *Fixed points and products*, Order **11** (1994), 11–14.
14. H. Rubin and J. Rubin, *Equivalents of the Axiom of Choice II*, Studies in Logic and the Foundations of Mathematics, vol. 116, North-Holland, Amsterdam, 1985.
15. B.S.W. Schröder, *Ordered Sets, An Introduction*, Birkhäuser, Boston, Basel, Berlin, 2003.
16. E. Szpilrajn, *Sur l'extension de l'ordre partiel*, Fund. Math. **16** (1930), 386–389.
17. H. Tverberg, *On Dilworth's decomposition theorem for partially ordered sets*, J. Combinatorial Theory **3** (1967), 305–306.

2. Semilattices, Lattices and Complete Lattices

There's nothing quite so fine
As an earful of Patsy Cline.
–Steve Goodman

The most important partially ordered sets come endowed with more structure than that. For example, the significant feature about $\mathcal{PO}(X)$ for Theorem 1.7 is not just its partial order, but that it is closed under arbitrary intersections. In this chapter we will meet several types of structures that arise naturally in algebra.

A *semilattice* is an algebra $\mathcal{S} = (S, *)$ satisfying, for all $x, y, z \in S$,

(1) $x * x = x$,
(2) $x * y = y * x$,
(3) $x * (y * z) = (x * y) * z$.

In other words, a semilattice is an idempotent commutative semigroup. The symbol $*$ can be replaced by any binary operation symbol, and in fact we will most often use one of $\vee$, $\wedge$, $+$ or $\cdot$, depending on the setting. The most natural example of a semilattice is $(\mathfrak{P}(X), \cap)$, or more generally any collection of subsets of X closed under intersection. For example, the semilattice $\mathcal{PO}(X)$ of partial orders on X is naturally contained in $(\mathfrak{P}(X^2), \cap)$.

Theorem 2.1. *In a semilattice $\mathcal{S}$, define $x \leq y$ if and only if $x * y = x$. Then $(S, \leq)$ is an ordered set in which every pair of elements has a greatest lower bound. Conversely, given an ordered set $\mathcal{P}$ with that property, define $x * y = g.l.b.\,(x, y)$. Then $(P, *)$ is a semilattice.*

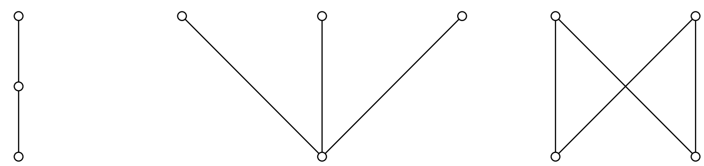
Proof. Let $(S, *)$ be a semilattice, and define $\leq$ as above. First we check that $\leq$ is a partial order.

(1) $x * x = x$ implies $x \leq x$.
(2) If $x \leq y$ and $y \leq x$, then $x = x * y = y * x = y$.
(3) If $x \leq y \leq z$, then $x * z = (x * y) * z = x * (y * z) = x * y = x$, so $x \leq z$.

Since $(x * y) * x = x * (x * y) = (x * x) * y = x * y)$ we have $x * y \leq x$; similarly $x * y \leq y$. Thus $x * y$ is a lower bound for $\{x, y\}$. To see that it is the greatest lower bound, suppose $z \leq x$ and $z \leq y$. Then $z * (x * y) = (z * x) * y = z * y = z$, so $z \leq x * y$, as desired.

The proof of the converse is likewise a direct application of the definitions, and is left to the reader. $\square$

A semilattice with the above ordering is usually called a *meet* semilattice, and as a matter of convention $\wedge$ or $\cdot$ is used for the operation symbol. In Figure 2.1, (a) and (b) are meet semilattices, while (c) fails on several counts.



(a) (b) (c)

FIGURE 2.1

Sometimes it is more natural to use the dual order, setting $x \geq y$ iff $x * y = x$. In that case, $\mathcal{S}$ is referred to as a *join* semilattice, and the operation is denoted by $\vee$ or $+$.

A *subsemilattice* of $\mathcal{S}$ is a subset $T \subseteq S$ which is closed under the operation $*$ of $\mathcal{S}$: if $x, y \in T$ then $x * y \in T$. Of course, that makes T a semilattice in its own right, since the equations defining a semilattice still hold in $(T, *)$.[1]

Similarly, a *homomorphism* between two semilattices is a map $h : \mathcal{S} \to \mathcal{T}$ with the property that $h(x * y) = h(x) * h(y)$. An *isomorphism* is a homomorphism that is one-to-one and onto. It is worth noting that, because the operation is determined by the order and *vice versa*, two semilattices are isomorphic if and only if they are isomorphic as ordered sets.

The collection of all order ideals of a meet semilattice $\mathcal{S}$ forms a semilattice $\mathcal{O}(S)$ under set intersection. The mapping from Theorem 1.1 gives us a set representation for meet semilattices.

Theorem 2.2. *Let $\mathcal{S}$ be a meet semilattice. Define $\phi : S \to \mathcal{O}(S)$ by*

$$\phi(x) = \{y \in S : y \leq x\}.$$

Then $\mathcal{S}$ is isomorphic to $(\phi(\mathcal{S}), \cap)$.

Proof. We already know that ϕ is an order embedding of $\mathcal{S}$ into $\mathcal{O}(\mathcal{S})$. Moreover, $\phi(x \wedge y) = \phi(x) \cap \phi(y)$ because $x \wedge y$ is the greatest lower bound of x and y, so that $z \leq x \wedge y$ if and only if $z \leq x$ and $z \leq y$. $\square$

A *lattice* is an algebra $\mathcal{L} = (L, \wedge, \vee)$ satisfying, for all $x, y, z \in S$,

(1) $x \wedge x = x$ and $x \vee x = x$,

---

[1]However, it is not enough that the elements of T form a semilattice under the ordering $\leq$. For example, the sets $\{1, 2\}$, $\{1, 3\}$ and $\emptyset$ do not form a subsemilattice of $(\mathfrak{P}(\{1, 2, 3\}), \cap)$.

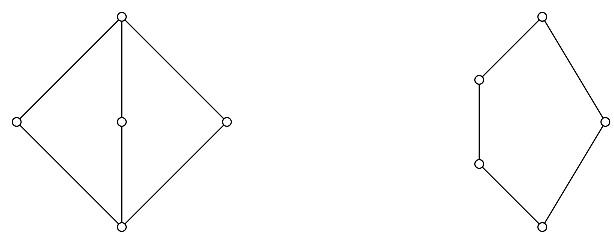
(2) $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$,
(3) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ and $x \vee (y \vee z) = (x \vee y) \vee z$,
(4) $x \wedge (x \vee y) = x$ and $x \vee (x \wedge y) = x$.

The first three pairs of axioms say that $\mathcal{L}$ is both a meet and join semilattice. The fourth pair (called the *absorption laws*) say that both operations induce the same order on L. The lattice operations are sometimes denoted by $\cdot$ and $+$; for the sake of consistency we will stick with the $\wedge$ and $\vee$ notation.

An example is the lattice $(\mathfrak{P}(X), \cap, \cup)$ of all subsets of a set X, with the usual set operations of intersection and union. This turns out not to be a very general example, because subset lattices satisfy the distributive law

$$(D) \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

The corresponding lattice equation does not hold in all lattices: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ fails, for example, in the two lattices in Figure 2.2. Hence we cannot expect to prove a representation theorem which embeds an arbitrary lattice in $(\mathfrak{P}(X), \cap, \cup)$ for some set X, although we will prove such a result for distributive lattices. A more general example would be the lattice $\mathbf{Sub}(\mathcal{G})$ of all subgroups of a group $\mathcal{G}$. Most of the remaining results in this section are designed to show how lattices arise naturally in mathematics, and to point out additional properties that some of these lattices have.



$\mathcal{M}_3$ $\qquad$ $\mathcal{N}_5$

FIGURE 2.2

Theorem 2.3. *In a lattice $\mathcal{L}$, define $x \leq y$ if and only if $x \wedge y = x$. Then $(L, \leq)$ is an ordered set in which every pair of elements has a greatest lower bound and a least upper bound. Conversely, given an ordered set $\mathcal{P}$ with that property, define $x \wedge y = g.l.b.\,(x, y)$ and $x \vee y = l.u.b.\,(x, y)$. Then $(P, \wedge, \vee)$ is a lattice.*

The crucial observation in the proof is that, in a lattice, $x \wedge y = x$ if and only if $x \vee y = y$ by the absorption laws. The rest is a straightforward extension of Theorem 2.1.

This time we leave it up to you to figure out the correct definitions of *sublattice, homomorphism* and *isomorphism* for lattices. If a lattice has a least element, it is denoted by 0; the greatest element, if it exists, is denoted by 1. Of special importance are the *interval* (or *quotient*) sublattices, for each of which there are various notations used in the literature:

$$\begin{aligned}[b,a] &= a/b = \{x \in L : b \le x \le a\} \\ \downarrow a &= a/0 = (a] = \{x \in L : x \le a\} \\ \uparrow a &= 1/a = [a) = \{x \in L : a \le x\}.\end{aligned}$$

To avoid confusion, we will mostly use $[b,a]$ and $\downarrow a$ and $\uparrow a$.[2]

One further bit of notation will prove useful. For a subset A of an ordered set $\mathcal{P}$, let A^u denote the set of all upper bounds of A, i.e.,

$$\begin{aligned}A^u &= \{x \in P : x \ge a \text{ for all } a \in A\} \\ &= \bigcap_{a \in A} \uparrow a.\end{aligned}$$

Dually, A^ℓ is the set of all lower bounds of A,

$$\begin{aligned}A^\ell &= \{x \in P : x \le a \text{ for all } a \in A\} \\ &= \bigcap_{a \in A} \downarrow a.\end{aligned}$$

Let us consider the question of when a subset A of an ordered set $\mathcal{P}$ has a least upper bound. Clearly A^u must be nonempty, and this will certainly be the case if $\mathcal{P}$ has a greatest element. If moreover it happens that A^u has a greatest lower bound z in $\mathcal{P}$, then in fact $z \in A^u$, i.e., $a \le z$ for all $a \in A$, because each $a \in A$ is a lower bound for A^u. Therefore by definition z is the least upper bound of A. In this case we say that the join of A exists, and write $z = \bigvee A$ (treating the join as a partially defined operation).

But if $\mathcal{S}$ is a finite meet semilattice with a greatest element, then $\bigwedge A^u$ exists for every $A \subseteq S$. Thus we have the following result.

Theorem 2.4. *Let $\mathcal{S}$ be a finite meet semilattice with greatest element* 1*. Then $\mathcal{S}$ is a lattice with the join operation defined by*

$$x \vee y = \bigwedge \{x, y\}^u = \bigwedge (\uparrow x \cap \uparrow y).$$

This result not only yields an immediate supply of lattice examples, but it provides us with an efficient algorithm for deciding when a finite ordered set is a lattice:

[2]The notations $a/0$ and $1/a$ were historically used irrespective of whether $\mathcal{L}$ actually has a least element 0 or a greatest element 1.

if a finite ordered set $\mathcal{P}$ has a greatest element and every pair of elements has a meet, then $\mathcal{P}$ is a lattice. The dual version is of course equally useful.

Every finite subset of a lattice has a greatest lower bound and a least upper bound, but these bounds need not exist for infinite subsets. Let us define a *complete lattice* to be an ordered set $\mathcal{L}$ in which every subset A has a greatest lower bound $\bigwedge A$ and a least upper bound $\bigvee A$.[3] Clearly every finite lattice is complete, and every complete lattice is a lattice with 0 and 1 (but not conversely). Again $\mathfrak{P}(X)$ is a natural (but not very general) example of a complete lattice, and $\mathbf{Sub}(\mathcal{G})$ is a better one. The rational numbers with their natural order form a lattice that is not complete.

Likewise, a *complete meet semilattice* is an ordered set $\mathcal{S}$ with a greatest element and the property that every nonempty subset A of S has a greatest lower bound $\bigwedge A$. By convention, we define $\bigwedge \emptyset = 1$, the greatest element of $\mathcal{S}$. The analogue of Theorem 2.4 is as follows.

Theorem 2.5. *If $\mathcal{L}$ is a complete meet semilattice, then $\mathcal{L}$ is a complete lattice with the join operation defined by*

$$\bigvee A = \bigwedge A^u = \bigwedge (\bigcap_{a \in A} \uparrow a).$$

Complete lattices abound in mathematics because of their connection with closure systems. We will introduce three different ways of looking at these things, each with certain advantages, and prove that they are equivalent.

A *closure system* on a set X is a collection $\mathcal{C}$ of subsets of X that is closed under arbitrary intersections (including the empty intersection, so $\bigcap \emptyset = X \in \mathcal{C}$). The sets in $\mathcal{C}$ are called *closed* sets. By Theorem 2.5, the closed sets of a closure system form a complete lattice. Various examples come to mind:

(i) closed subsets of a topological space,
(ii) subgroups of a group,
(iii) subspaces of a vector space,
(iv) convex subsets of euclidean space $\Re^n$.
(v) order ideals of an ordered set,

You can probably think of other types of closure systems, and more will arise as we go along.

A *closure operator* on a set X is a map $\Gamma : \mathfrak{P}(X) \to \mathfrak{P}(X)$ satisfying, for all subsets $A, B \subseteq X$,

(1) $A \subseteq \Gamma(A)$,
(2) $A \subseteq B$ implies $\Gamma(A) \subseteq \Gamma(B)$,
(3) $\Gamma(\Gamma(A)) = \Gamma(A)$.

[3]We could have defined complete lattices as a type of infinitary algebra satisfying some axioms, but since these kinds of structures are not very familiar the above approach seems more natural. Following standard usage, we only allow finitary operations in an algebra (see Appendix 1). Thus a complete lattice as such, with its arbitrary operations $\bigvee A$ and $\bigwedge A$, does not count as an algebra.

The closure operators associated with the closure systems above are as follows:

(i) X a topological space and $\Gamma(A)$ the closure of A,
(ii) $\mathcal{G}$ a group and $\mathrm{Sg}(A)$ the subgroup generated by A,
(iii) $\mathcal{V}$ a vector space and $\mathrm{Span}(A)$ the set of all linear combinations of elements of A,
(iv) $\Re^n$ and $H(A)$ the convex hull of A.
(v) $\mathcal{P}$ an ordered set and $\mathcal{O}(A)$ the order ideal generated by A,

For a closure operator, a set D is called *closed* if $\Gamma(D) = D$, or equivalently (by (3)), if $D = \Gamma(A)$ for some A.

A set of *closure rules* on a set X is a collection Σ of properties $\varphi(S)$ of subsets of X, where each $\varphi(S)$ has one of the forms

$$x \in S$$

or

$$Y \subseteq S \implies z \in S$$

with x, $z \in X$ and $Y \subseteq X$. (Note that the first type of rule is a degenerate case of the second, taking $Y = \emptyset$.) A subset D of X is said to be *closed* with respect to these rules if $\varphi(D)$ is true for each $\varphi \in \Sigma$. The closure rules corresponding to our previous examples are:

(i) all rules $Y \subseteq S \implies z \in S$ where z is an accumulation point of Y,
(ii) the rule $1 \in S$ and all rules

$$x \in S \implies x^{-1} \in S$$
$$\{x, y\} \subseteq S \implies xy \in S$$

with x, $y \in G$,
(iii) $0 \in S$ and all rules $\{x, y\} \subseteq S \implies ax + by \in S$ with a, b scalars,
(iv) for all $\overline{x}$, $\overline{y} \in \Re^n$ and $0 < t < 1$, the rules $\{\overline{x}, \overline{y}\} \subseteq S \implies t\overline{x} + (1-t)\overline{y} \in S$.
(v) for all pairs with $x < y$ in $\mathcal{P}$ the rules $y \in S \implies x \in S$,

So the closure rules just list the properties that we check to determine if a set S is closed or not.

The following theorem makes explicit the connection between these ideas.

Theorem 2.6. *(1) If $\mathcal{C}$ is a closure system on a set X, then the map $\Gamma_{\mathcal{C}} : \mathfrak{P}(X) \to \mathfrak{P}(X)$ defined by*

$$\Gamma_{\mathcal{C}}(A) = \bigcap \{D \in \mathcal{C} : A \subseteq D\}$$

is a closure operator. Moreover, $\Gamma_{\mathcal{C}}(A) = A$ if and only if $A \in \mathcal{C}$.

(2) If Γ is a closure operator on a set X, let Σ_Γ be the set of all rules

$$c \in S$$

where $c \in \Gamma(\emptyset)$, and all rules

$$Y \subseteq S \implies z \in S$$

with $z \in \Gamma(Y)$. Then a set $D \subseteq X$ satisfies all the rules of Σ_Γ if and only if $\Gamma(D) = D$.

(3) If Σ is a set of closure rules on a set X, let $\mathcal{C}_\Sigma$ be the collection of all subsets of X that satisfy all the rules of Σ. Then $\mathcal{C}_\Sigma$ is a closure system.

In other words, the collection of all closed sets of a closure operator forms a complete lattice, and the property of being a closed set can be expressed in terms of rules that are clearly preserved by set intersection. It is only a slight exaggeration to say that all important lattices arise in this way. As a matter of notation, we will also use $\mathcal{C}_\Gamma$ to denote the lattice of Γ-closed sets, even though this particular variant is skipped in the statement of the theorem.

Proof. Starting with a closure system $\mathcal{C}$, define $\Gamma_\mathcal{C}$ as above. Observe that $\Gamma_\mathcal{C}(A) \in \mathcal{C}$ for any $A \subseteq X$, and $\Gamma(D) = D$ for every $D \in \mathcal{C}$. Therefore $\Gamma_\mathcal{C}(\Gamma_\mathcal{C}(A)) = \Gamma_\mathcal{C}(A)$, and the other axioms for a closure operator hold by elementary set theory.

Given a closure operator Γ, it is clear that $\Gamma(D) \subseteq D$ iff D satisfies all the rules of Σ_Γ. Likewise, it is immediate because of the form of the rules that $\mathcal{C}_\Sigma$ is always a closure system. $\square$

Note that if Γ is a closure operator on a set X, then the operations on $\mathcal{C}_\Gamma$ are given by

$$\bigwedge_{i \in I} D_i = \bigcap_{i \in I} D_i$$
$$\bigvee_{i \in I} D_i = \Gamma(\bigcup_{i \in I} D_i).$$

For example, in the lattice of closed subsets of a topological space, the join is the closure of the union. In the lattice of subgroups of a group, the join of a collection of subgroups is the subgroup generated by their union. The lattice of order ideals of an ordered set is somewhat exceptional in this regard, because the union of a collection of order ideals is already an order ideal.

One type of closure operator is especially important. If $\mathcal{A} = \langle A, F, C \rangle$ is an algebra, then $S \subseteq A$ is a *subalgebra* of $\mathcal{A}$ if $c \in S$ for every constant $c \in C$, and $\{s_1, \ldots, s_n\} \subseteq S$ implies $f(s_1, \ldots, s_n) \in S$ for every basic operation $f \in F$. Of course these are closure rules, so the intersection of any collection of subalgebras of $\mathcal{A}$ is again one.[4] For a subset $B \subseteq A$, define

$$\mathrm{Sg}(B) = \bigcap \{\mathcal{S} : \mathcal{S} \text{ is a subalgebra of } \mathcal{A} \text{ and } B \subseteq S\}.$$

[4] If $\mathcal{A}$ has no constants, then we have to worry about the empty set. We want to allow $\emptyset$ in the subalgebra lattice in this case, but realize that it is an abuse of terminology to call it a subalgebra. The term *subuniverse* is sometimes used to avoid this problem.

By Theorem 2.6, Sg is a closure operator, and $\mathrm{Sg}(B)$ is of course the subalgebra generated by B. The corresponding lattice of closed sets is $\mathcal{C}_{\mathrm{Sg}} = \mathbf{Sub}\,\mathcal{A}$, the lattice of subalgebras of $\mathcal{A}$.

Galois connections provide another source of closure operators. These are relegated to the exercises not because they are unimportant, but rather to encourage you to grapple with how they work on your own.

For completeness, we include a representation theorem.

Theorem 2.7. *If $\mathcal{L}$ is a complete lattice, define a closure operator Δ on L by*

$$\Delta(A) = \{x \in L : x \leq \bigvee A\}.$$

Then $\mathcal{L}$ is isomorphic to $\mathcal{C}_\Delta$.

The isomorphism $\varphi : \mathcal{L} \to \mathcal{C}_\Delta$ is just given by $\varphi(x) = \downarrow x$.

The representation of $\mathcal{L}$ as a closure system given by Theorem 2.7 can be greatly improved upon in some circumstances. Here we will give a better representation for lattices satisfying the ACC and DCC. In Chapter 3 we will do the same for another class called algebraic lattices.

An element q of a lattice $\mathcal{L}$ is called *join irreducible* if $q = \bigvee F$ for a finite set F implies $q \in F$, i.e., q is not the join of other elements. The set of all join irreducible elements in $\mathcal{L}$ is denoted by $J(\mathcal{L})$. Note that according to the definition, if $\mathcal{L}$ has a least element 0, then $0 \notin J(\mathcal{L})$, as $0 = \bigvee \emptyset$.[5] To include zero, let $J_0(\mathcal{L}) = J(\mathcal{L}) \cup \{0\}$.

Lemma 2.8. *If a lattice $\mathcal{L}$ satisfies the DCC, then every element of $\mathcal{L}$ is a join of finitely many join irreducible elements.*

Proof. Suppose some element of $\mathcal{L}$ is not a join of join irreducible elements. Let x be a minimal such element. Then x is not itself join irreducible, nor is it zero. So $x = \bigvee F$ for some finite set F of elements strictly below x. By the minimality of x, each $f \in F$ is the join of a finite set $G_f \subseteq J(\mathcal{L})$. Then $x = \bigvee_{f \in F} \bigvee G_f$, a contradiction. $\square$

Analogously, an element q of a complete lattice $\mathcal{L}$ is said to be *completely join irreducible* if $q = \bigvee X$ implies $q \in X$ for arbitrary (possibly infinite) subsets $X \subseteq L$. If q is completely join irreducible, then q has a unique lower cover, *viz.*,

$$q_* = \bigvee \{x \in L : x < q\}.$$

Moreover, $x < q$ implies $x \leq q_*$. Let $J^*(\mathcal{L})$ denote the set of completely join irreducible elements. In general, $J^*(\mathcal{L}) \subseteq J(\mathcal{L})$, but for lattices satisfying the ACC, equality holds.

[5]This convention is not universal, as *join irreducible* is sometimes defined by $q = r \vee s$ implies $q = r$ or $q = s$, which is equivalent for nonzero elements.

Let us consider lattices that satisfy both the ACC and DCC. By Exercise 6 of Chapter 1, these are lattices in which every chain is finite, and thus just a slight generalization of finite lattices. The representation of lattices satisfying both chain conditions as a closure system is quite straightforward.

Theorem 2.9. *Let $\mathcal{L}$ be a lattice satisfying the ACC and DCC. Let Σ be the set of all closure rules on $J(\mathcal{L})$ of the form*

$$F \subseteq S \implies q \in S$$

where q is join irreducible, F is a finite subset of $J(\mathcal{L})$, and $q \leq \bigvee F$. (Include the degenerate cases $p \in S \implies q \in S$ for $q \leq p$ in $J(\mathcal{L})$.) Then $\mathcal{L}$ is isomorphic to the lattice $\mathcal{C}_\Sigma$ of Σ-closed sets.

Proof. Define order preserving maps $f : \mathcal{L} \to \mathcal{C}_\Sigma$ and $g : \mathcal{C}_\Sigma \to \mathcal{L}$ by

$$f(x) = {\downarrow} x \cap J(\mathcal{L})$$
$$g(S) = \bigvee S.$$

Now $gf(x) = x$ for all $x \in L$ by Lemma 2.8. On the other hand, $fg(S) = S$ for any Σ-closed set, because by the ACC we have $\bigvee S = \bigvee F$ for some finite $F \subseteq S$, which puts every join irreducible $q \leq \bigvee F$ in S by the closure rules. $\square$

A generalization of the preceding theorem is given in Exercises 15–17 of Chapter 3.

As an example of how we might apply these ideas, suppose we want to find the subalgebra lattice of a finite algebra $\mathcal{A}$. Now **Sub** $\mathcal{A}$ is finite, and every join irreducible subalgebra is of the form $\mathrm{Sg}(a)$ for some $a \in A$ (though not necessarily conversely). Thus we may determine **Sub** $\mathcal{A}$ by first finding all the 1-generated subalgebras $\mathrm{Sg}(a)$, and then computing the joins of sets of these.[6]

Let us look at another type of closure operator. Of course, an ordered set need not be complete. We say that a pair $(\mathcal{L}, \phi)$ is a *completion* of the ordered set $\mathcal{P}$ if $\mathcal{L}$ is a complete lattice and ϕ is an order embedding of $\mathcal{P}$ into $\mathcal{L}$. A subset Q of a complete lattice $\mathcal{L}$ is *join dense* if for every $x \in L$,

$$x = \bigvee \{q \in Q : q \leq x\}.$$

A completion $(\mathcal{L}, \phi)$ is *join dense* if $\phi(P)$ is join dense in $\mathcal{L}$, i.e., for every $x \in L$,

$$x = \bigvee \{\phi(p) : \phi(p) \leq x\}.$$

[6]The art of universal algebra computation lies in making the algorithms reasonably efficient. See Ralph Freese's Universal Algebra Calculator on the webpage *http://uacalc.org*. This builds on earlier versions by Freese, Emil Kiss and Matt Valeriote.

It is not hard to see that every completion of $\mathcal{P}$ contains a join dense completion. For, given a completion $(\mathcal{L}, \phi)$ of $\mathcal{P}$, let $\mathcal{L}'$ be the set of all elements of L of the form $\bigvee\{\phi(p) : p \in A\}$ for some subset $A \subseteq P$, including $\bigvee \emptyset = 0$. Then $\mathcal{L}'$ is a complete join subsemilattice of $\mathcal{L}$, and hence a complete lattice. Moreover, $\mathcal{L}'$ contains $\phi(p)$ for every $p \in P$, and $(\mathcal{L}', \phi)$ is a join dense completion of $\mathcal{P}$. Hence we may reasonably restrict our attention to join dense completions.

Our first example of a join dense completion is the lattice of order ideals $\mathcal{O}(\mathcal{P})$. Order ideals are the closed sets of the closure operator on P given by

$$O(A) = \bigcup_{a \in A} {\downarrow} a,$$

and the embedding ϕ is given by $\phi(p) = {\downarrow} p$. Note that the union of order ideals is again an order ideal, so $\mathcal{O}(\mathcal{P})$ obeys the distributive law (D).

Another example is the *MacNeille completion* $\mathcal{M}(\mathcal{P})$, a.k.a. *normal completion, completion by cuts* [9]. For subsets $S, T \subseteq P$ recall that

$$S^u = \{x \in P : x \geq s \text{ for all } s \in S\}$$

$$T^\ell = \{y \in P : y \leq t \text{ for all } t \in T\}.$$

The MacNeille completion is the lattice of closed sets of the closure operator on P given by

$$M(A) = (A^u)^\ell\ ,$$

i.e., $M(A)$ is the set of all lower bounds of all upper bounds of A. Note that $M(A)$ is an order ideal of $\mathcal{P}$. Again the map $\phi(p) = {\downarrow} p$ embeds $\mathcal{P}$ into $\mathcal{M}(\mathcal{P})$.

Now every join dense completion preserves all existing meets in $\mathcal{P}$: if $A \subseteq P$ and A has a greatest lower bound $b = \bigwedge A$ in $\mathcal{P}$, then $\phi(b) = \bigwedge \phi(A)$ (see Exercise 11). The MacNeille completion has the nice property that it also preserves all existing joins in $\mathcal{P}$: if A has a least upper bound $c = \bigvee A$ in $\mathcal{P}$, then $\phi(c) = {\downarrow} c = M(A) = \bigvee \phi(A)$.

In fact, every join dense completion corresponds to a closure operator on P.

Theorem 2.10. *Let $\mathcal{P}$ be an ordered set. If Φ is a closure operator on P such that $\Phi(\{p\}) = {\downarrow} p$ for all $p \in P$, then $(\mathcal{C}_\Phi, \phi)$ is a join dense completion of $\mathcal{P}$, where $\phi(p) = {\downarrow} p$. Conversely, if $(\mathcal{L}, \phi)$ is a join dense completion of $\mathcal{P}$, then the map Φ defined by*

$$\Phi(A) = \{q \in P : \phi(q) \leq \bigvee_{a \in A} \phi(a)\}$$

is a closure operator on P, $\Phi(\{p\}) = {\downarrow} p$ for all $p \in P$, and $\mathcal{C}_\Phi \cong \mathcal{L}$.

Proof. For the first part, it is clear that $(\mathcal{C}_\Phi, \phi)$ is a completion of $\mathcal{P}$. It is a join dense one because every closed set must be an order ideal, and thus for every $C \in \mathcal{C}_\Phi$,

$$\begin{aligned} C &= \bigvee\{\Phi(\{p\}) : p \in C\} \\ &= \bigvee\{{\downarrow} p : {\downarrow} p \subseteq C\} \\ &= \bigvee\{\phi(p) : \phi(p) \leq C\}. \end{aligned}$$

For the converse, it is clear that Φ defined thusly satisfies $A \subseteq \Phi(A)$, and $A \subseteq B$ implies $\Phi(A) \subseteq \Phi(B)$. But we also have $\bigvee_{q \in \Phi(A)} \phi(q) = \bigvee_{a \in A} \phi(a)$, so $\Phi(\Phi(A)) = \Phi(A)$.

To see that $\mathcal{C}_\Phi \cong \mathcal{L}$, let $f : \mathcal{C}_\Phi \to \mathcal{L}$ by $f(A) = \bigvee_{a \in A} \phi(a)$, and let $g : \mathcal{L} \to \mathcal{C}_\Phi$ by $g(x) = \{p \in P : \phi(p) \le x\}$. Then both maps are order preserving, $fg(x) = x$ for $x \in L$ by the definition of join density, and $gf(A) = \Phi(A) = A$ for $A \in \mathcal{C}_\Phi$. Hence both maps are isomorphisms. $\square$

There is a natural order on the closure operators on a set X.

Lemma 2.11. *Let Γ and Δ be closure operators on a set X. The following are equivalent.*

(1) *$\Gamma(A) \subseteq \Delta(A)$ for all $A \subseteq X$.*
(2) *$\Delta(C) = C$ implies $\Gamma(C) = C$ for all $C \subseteq X$.*

Proof. If (1) holds and $\Delta(C) = C$, then $C \subseteq \Gamma(C) \subseteq \Delta(C) = C$, whence $\Gamma(C) = C$. If (2) holds, then $\Gamma(A) \subseteq \Gamma(\Delta(A)) = \Delta(A)$. $\square$

Let $\mathrm{Cl}(X)$ be the set of all closure operators on the set X, ordered by $\Gamma \le \Delta$ if the conditions of Lemma 2.11 hold. For any collection Γ_i $(i \in I)$ contained in $\mathrm{Cl}(X)$, the operator $\bigwedge_{i \in I} \Gamma_i$ defined by

$$(\bigwedge_{i \in I} \Gamma_i)(A) = \bigcap_{i \in I} \Gamma_i(A)$$

is easily seen to be a closure operator, and of course the greatest lower bound of $\{\Gamma_i : i \in I\}$. Hence $\mathrm{Cl}(X)$ is a complete lattice. See Exercise 13 for a nice generalization.

Let $\mathcal{K}(\mathcal{P})$ be the collection of all closure operators on $\mathcal{P}$ such that $\Gamma(\{p\}) = {\downarrow} p$ for all $p \in P$. This is a complete sublattice – in fact, an interval – of $\mathrm{Cl}(P)$. The least and greatest members of $\mathcal{K}(\mathcal{P})$ are the order ideal completion and the MacNeille completion, respectively.

Theorem 2.12. *$\mathcal{K}(\mathcal{P})$ is a complete lattice with least element O and greatest element M.*

Proof. The condition $\Gamma(\{p\}) = {\downarrow} p$ implies that $O(A) \subseteq \Gamma(A)$ for all $A \subseteq P$, which makes O the least element of $\mathcal{K}(\mathcal{P})$. On the other hand, for any $\Gamma \in \mathcal{K}(\mathcal{P})$, if $b \ge a$ for all $a \in A$, then ${\downarrow} b = \Gamma({\downarrow} b) \supseteq \Gamma(A)$. Thus

$$\Gamma(A) \subseteq \bigcap_{b \in A^u} ({\downarrow} b) = (A^u)^\ell = M(A),$$

so M is its greatest element. $\square$

The lattices $\mathcal{K}(\mathcal{P})$ have an interesting structure, which was investigated by the author and Alex Pogel in [10].

We conclude this section with a classic theorem due to B. Knaster, A. Tarski and Anne Davis (Morel) [5], [8], [11].

Theorem 2.13. *A lattice $\mathcal{L}$ is complete if and only if every order preserving map $f : \mathcal{L} \to \mathcal{L}$ has a fixed point.*

Proof. One direction is easy. Given a complete lattice $\mathcal{L}$ and an order preserving map $f : \mathcal{L} \to \mathcal{L}$, put $A = \{x \in L : f(x) \geq x\}$. Note A is nonempty as $0 \in A$. Let $a = \bigvee A$. Since $a \geq x$ for all $x \in A$, $f(a) \geq \bigvee_{x \in A} f(x) \geq \bigvee_{x \in A} x = a$. Thus $a \in A$. But then $a \leq f(a)$ implies $f(a) \leq f^2(a)$, so also $f(a) \in A$, whence $f(a) \leq a$. Therefore $f(a) = a$.

Conversely, let $\mathcal{L}$ be a lattice that is not a complete lattice.

Claim 1: *Either $\mathcal{L}$ has no 1 or there exists a chain $C \subseteq L$ that satisfies the ACC and has no meet.* For suppose $\mathcal{L}$ has a 1 and that every chain C in $\mathcal{L}$ satisfying the ACC has a meet. We will show that every subset $S \subseteq L$ has a join, which makes $\mathcal{L}$ a complete lattice by the dual of Theorem 2.5.

Consider S^u, the set of all upper bounds of S. Note $S^u \neq \emptyset$ because $1 \in L$. Let $\mathcal{P}$ denote the collection of all chains $C \subseteq S^u$ satisfying the *ACC*, ordered by $C_1 \leq C_2$ if C_1 is a filter (dual ideal) of C_2.

The order on $\mathcal{P}$ insures that if C_i $(i \in I)$ is a chain of chains in $\mathcal{P}$, then $\bigcup_{i \in I} C_i \in \mathcal{P}$. Hence by Zorn's Lemma, $\mathcal{P}$ contains a maximal element C_m. By hypothesis $\bigwedge C_m$ exists in $\mathcal{L}$, say $\bigwedge C_m = a$. In fact, $a = \bigvee S$. For if $s \in S$, then $s \leq c$ for all $c \in C_m$, so $s \leq \bigwedge C_m = a$. Thus $a \in S^u$, i.e., a is an upper bound for S. If $a \nleq t$ for some $t \in S^u$, then we would have $a > a \wedge t \in S^u$, and the chain $C_m \cup \{a \wedge t\}$ would contradict the maximality of C_m. Therefore $a = \bigwedge S^u = \bigvee S$. This proves Claim 1; Exercise 12 indicates why the argument is necessarily a bit involved.

If $\mathcal{L}$ has a 1, let C be a chain satisfying the *ACC* but having no meet; otherwise take $C = \emptyset$. Dualizing the preceding argument, let $\mathcal{Q}$ be the set of all chains $D \subseteq C^\ell$ satisfying the *DCC*, ordered by $D_1 \leq D_2$ if D_1 is an ideal of D_2. Now $\mathcal{Q}$ could be empty, but only when C is not; if nonempty, $\mathcal{Q}$ has a maximal member D_m. Let $D = D_m$ if $\mathcal{Q} \neq \emptyset$, and $D = \emptyset$ otherwise.

Claim 2: *For all $x \in L$, either there exists $c \in C$ with $x \nleq c$, or there exists $d \in D$ with $x \ngeq d$.* Supposing otherwise, let $x \in L$ with $x \leq c$ for all $c \in C$ and $x \geq d$ for all $d \in D$. (The assumption $x \in C^\ell$ means we are in the case $\mathcal{Q} \neq \emptyset$.) Since $x \in C^\ell$ and $\bigwedge C$ does not exist, there is a $y \in C^\ell$ such that $y \nleq x$. So $x \vee y > x \geq d$ for all $d \in D$, and the chain $D \cup \{x \vee y\}$ contradicts the maximality of $D = D_m$ in $\mathcal{Q}$.

Now define a map $f : \mathcal{L} \to \mathcal{L}$ as follows. For each $x \in L$, put

$$C(x) = \{c \in C : x \nleq c\} \ ,$$
$$D(x) = \{d \in D : x \ngeq d\} \ .$$

We have shown that one of these two sets is nonempty for each $x \in L$. If $C(x) \neq \emptyset$, let $f(x)$ be its largest element (using the *ACC*); otherwise let $f(x)$ be the least element of $D(x)$ (using the *DCC*). Now for any $x \in L$, either $x \nleq f(x)$ or $x \ngeq f(x)$, so f has no fixed point.

It remains to check that f is order preserving. Suppose $x \leq y$. If $C(x) \neq \emptyset$ then $f(x) \in C$ and $f(x) \ngeq y$ (else $f(x) \geq y \geq x$); hence $C(y) \neq \emptyset$ and $f(y) \geq f(x)$. So assume $C(x) = \emptyset$, whence $f(x) \in D$. If perchance $C(y) \neq \emptyset$ then $f(y) \in C$, so $f(x) \leq f(y)$. On the other hand, if $C(y) = \emptyset$ and $f(y) \in D$, then $x \ngeq f(y)$ (else $y \geq x \geq f(y)$), so again $f(x) \leq f(y)$. Therefore f is order preserving. $\square$

Standard textbooks on lattice theory include Birkhoff [1], Blyth [2], Crawley and Dilworth [3], Davey and Priestley [4] and Grätzer ['Gratzer, Gratzer2011'], each with a slightly different perspective.

Exercises for Chapter 2

1. Draw the Hasse diagrams for
   (a) all 5 element (meet) semilattices,
   (b) all 6 element lattices,
   (c) the lattice of subspaces of the vector space $\Re^2$.

2. Prove that a lattice that has a 0 and satisfies the ACC is complete.

3. For the cyclic group $\mathbb{Z}_4$, give explicitly the subgroup lattice, the closure operator Sg, and the closure rules for subgroups.

4. Define a closure operator F on $\Re^n$ by the rules $\{\overline{x}, \overline{y}\} \subseteq S \implies t\overline{x} + (1-t)\overline{y} \in S$ for all $t \in \Re$. Describe $F(A)$ for an arbitrary subset $A \subseteq \Re^n$. What is the geometric interpretation of F?

5. Prove that the following are equivalent for a subset Q of a complete lattice $\mathcal{L}$.
   (1) Q is join dense in $\mathcal{L}$, i.e., $x = \bigvee\{q \in Q : q \leq x\}$ for every $x \in L$.
   (2) Every element of L is a join of elements in Q.
   (3) If $y < x$ in $\mathcal{L}$, then there exists $q \in Q$ with $q \leq x$ but $q \nleq y$.

6. Let $\mathcal{L}$ be a complete lattice, and let X be a join-dense subset of L. Define a closure operator Γ on X by $\Gamma(S) = ({\downarrow} \bigvee S) \cap X$. Prove that $\mathcal{C}_\Gamma \cong \mathcal{L}$. (This generalizes Theorems 2.7 and 2.9, and anticipates Theorem 3.3.)

7. Find the completions $\mathcal{O}(\mathcal{P})$ and $\mathcal{M}(\mathcal{P})$ for the ordered sets in Figures 2.1 and 2.2.

8. Find the lattice $\mathcal{K}(\mathcal{P})$ of all join dense completions of the ordered sets in Figures 2.1 and 2.2.

9. Show that the MacNeille operator satisfies $M(A) = A$ iff $A = B^\ell$ for some $B \subseteq P$.

10. (a) Prove that if $(\mathcal{L}, \phi)$ is a join dense completion of the ordered set $\mathcal{P}$, then ϕ preserves all existing greatest lower bounds in $\mathcal{P}$.
    (b) Prove that the MacNeille completion preserves all existing least upper bounds in $\mathcal{P}$.

11. Prove that if ϕ is an order embedding of $\mathcal{P}$ into a complete lattice $\mathcal{L}$, then ϕ extends to an order embedding of $\mathcal{M}(\mathcal{P})$ into $\mathcal{L}$.

12. Show that $\omega \times \omega_1$ has no cofinal chain. (A subset $C \subseteq P$ is *cofinal* if for every $x \in P$ there exists $c \in C$ with $x \leq c$.)

13. Following Morgan Ward [12], we can generalize the notion of a closure operator as follows. Let $\mathcal{L}$ be a complete lattice. (For the closure operators on a set X, $\mathcal{L}$ will be $\mathfrak{P}(X)$.) A *closure operator* on $\mathcal{L}$ is a function $f : L \to L$ that satisfies, for all x, $y \in L$,

(i) $x \leq f(x)$,
(ii) $x \leq y$ implies $f(x) \leq f(y)$,
(iii) $f(f(x)) = f(x)$.

(a) Prove that $\mathcal{C}_f = \{x \in L : f(x) = x\}$ is a complete meet subsemilattice of $\mathcal{L}$.

(b) For any complete meet subsemilattice $\mathcal{S}$ of $\mathcal{L}$, prove that the function $f_{\mathcal{S}}$ defined by $f_{\mathcal{S}}(x) = \bigwedge\{s \in S : s \geq x\}$ is a closure operator on $\mathcal{L}$.

14. Let A and B be sets, and $R \subseteq A \times B$ a relation. For $X \subseteq A$ and $Y \subseteq B$ let

$$\sigma(X) = \{b \in B : x\ R\ b \text{ for all } x \in X\}$$
$$\pi(Y) = \{a \in A : a\ R\ y \text{ for all } y \in Y\}.$$

Prove the following claims.

(a) $X \subseteq \pi\sigma(X)$ and $Y \subseteq \sigma\pi(Y)$ for all $X \subseteq A$, $Y \subseteq B$.
(b) $X \subseteq X'$ implies $\sigma(X) \supseteq \sigma(X')$, and $Y \subseteq Y'$ implies $\pi(Y) \supseteq \pi(Y')$.
(c) $\sigma(X) = \sigma\pi\sigma(X)$ and $\pi(Y) = \pi\sigma\pi(Y)$ for all $X \subseteq A$, $Y \subseteq B$.
(d) $\pi\sigma$ is a closure operator on A, and $\mathcal{C}_{\pi\sigma} = \{\pi(Y) : Y \subseteq B\}$. Likewise $\sigma\pi$ is a closure operator on B, and $\mathcal{C}_{\sigma\pi} = \{\sigma(X) : X \subseteq A\}$.
(e) $\mathcal{C}_{\pi\sigma}$ is dually isomorphic to $\mathcal{C}_{\sigma\pi}$.

The maps σ and π are said to establish a *Galois connection* between A and B. The most familiar example is when A is a set, B a group acting on A, and $a\ R\ b$ means b fixes a. As another example, the MacNeille completion is $\mathcal{C}_{\pi\sigma}$ for the relation $\leq$ as a subset of $\mathcal{P} \times \mathcal{P}$.

References

1. G. Birkhoff, *Lattice Theory*, Amer. Math. Soc. Colloquium Publications XXV, Providence, 1940, 1948, 1967.
2. T. Blyth, *Lattices and Ordered Algebraic Structures*, Springer-Verlag, London, 2005.
3. P. Crawley and R. P. Dilworth, *Algebraic Theory of Lattices*, Prentice-Hall, Englewood Cliffs, N. J., 1973.
4. B. Davey and H. Priestley, *Introduction to Lattices and Order*, Cambridge University Press, Cambridge, 1990, 2002.
5. A. C. Davis, *A characterization of complete lattices*, Pacific J. Math. **5** (1955), 311–319.
6. G. Grätzer, *General Lattice Theory*, Academic Press, New York, 1978, Birkhäuser, Boston, Basel, Berlin, 1998.
7. G. Grätzer, *Lattice Theory: Foundation*, Birkhäuser, Basel, 2011.
8. B. Knaster, *Une théorème sur les fonctions d'ensembles*, Annales Soc. Polonaise Math. **6** (1927), 133–134.
9. H. M. MacNeille, *Partially ordered sets*, Trans. Amer. Math. Soc. **42** (1937), 90–96.
10. J. B. Nation and A. Pogel, *The lattice of completions of an ordered set*, Order **14** (1996), 1–7.

11. A. Tarski, *A lattice-theoretical fixpoint theorem and its applications*, Pacific J. Math. **5** (1955), 285–309.
12. M. Ward, *The closure operators of a lattice*, Annals of Math. **43** (1942), 191–196.

3. Algebraic Lattices

The more I get, the more I want it seems ....
–King Oliver

In this section we want to focus our attention on the kind of closure operators and lattices that are associated with modern algebra. A closure operator Γ on a set X is said to be *algebraic* if for every $B \subseteq X$,

$$\Gamma(B) = \bigcup \{\Gamma(F) : F \text{ is a finite subset of } B\}.$$

Equivalently, Γ is algebraic if the right hand side RHS of the above expression is closed for every $B \subseteq X$, since $B \subseteq \text{RHS} \subseteq \Gamma(B)$ holds for any closure operator.

A closure rule is said to be *finitary* if it is a rule of the form $x \in S$ or the form $F \subseteq S \implies z \in S$ with F a finite set. Again the first form is a degenerate case of the second, taking $F = \emptyset$. It is not hard to see that a closure operator is algebraic if and only if it is determined by a set of finitary closure rules; see Theorem 3.2(1).

Let us catalogue some important examples of algebraic closure operators.

(1) Let $\mathcal{A}$ be any algebra with only finitary operations – for example, a group, ring, vector space, semilattice or lattice. The closure operator Sg on A such that $\mathrm{Sg}(B)$ is the subalgebra of $\mathcal{A}$ generated by B is algebraic, because we have $a \in \mathrm{Sg}(B)$ if and only if a can be expressed as a term $a = t(b_1, \ldots, b_n)$ for some finite subset $\{b_1, \ldots, b_n\} \subseteq B$, in which case $a \in \mathrm{Sg}(\{b_1, \ldots, b_n\})$. The corresponding complete lattice is of course the subalgebra lattice **Sub** $\mathcal{A}$.

(2) Looking ahead a bit (to Chapter 5), the closure operator Cg on $A \times A$ such that $\mathrm{Cg}(B)$ is the congruence on $\mathcal{A}$ generated by the set of pairs B is also algebraic. The corresponding complete lattice is the congruence lattice **Con** $\mathcal{A}$. For groups this is isomorphic to the normal subgroup lattice; for rings, it is isomorphic to the lattice of ideals.

(3) For ordered sets, the order ideal operator O is algebraic. In fact we have

$$O(B) = \bigcup \{O(\{b\}) : b \in B\}$$

for all $B \subseteq P$.

(4) Let $\mathcal{S} = (S; \vee)$ be a join semilattice. A subset J of S is called an *ideal* if

(i) $x, y \in J$ implies $x \vee y \in J$,
(ii) $z \leq x \in J$ implies $z \in J$.

Since ideals are defined by closure rules, the intersection of a set of ideals of $\mathcal{S}$ is again one. Since they are finitary closure rules, the lattice of ideals is algebraic. The closure operator I on S such that $I(B)$ is the ideal of $\mathcal{S}$ generated by B is given by

$$I(B) = \{x \in S : x \leq \bigvee F \text{ for some finite } F \subseteq B\}.$$

The ideal lattice of a join semilattice is denoted by $\mathcal{I}(\mathcal{S})$. Again, ideals of the form $\downarrow x$ are called *principal.* Note that the empty set is an ideal of $(S; \vee)$.

(5) If $\mathcal{S} = (S; \vee, 0)$ is a semilattice with a least element 0, *regarded as a constant of the algebra,* then an ideal J must also satisfy

(iii) $0 \in J$

so that $\{0\}$, rather than the empty set, is the least ideal. The crucial factor is not that there is a least element, but that it is considered to be a constant in the type of the algebra.

(6) An *ideal* of a lattice is defined in the same way as (4), since every lattice is in particular a join semilattice. The ideal lattice of a lattice $\mathcal{L}$ is likewise denoted by $\mathcal{I}(\mathcal{L})$. The dual of an ideal in a lattice is called a *filter.* (See Exercise 4.)

On the other hand, it is not hard to see that the closure operators associated with the closed sets of a topological space are usually *not* algebraic, since the closure depends on infinite sequences. The closure operator M associated with the MacNeille completion is not in general algebraic, as is seen by considering the ordered set $\mathcal{P}$ consisting of an infinite set X and all of its finite subsets, ordered by set containment. This ordered set is already a complete lattice, and hence its own MacNeille completion. For any subset $Y \subseteq X$, let $\widehat{Y} = \{S \in P : S \subseteq Y\}$. If Y is an infinite proper subset of X, then $M(\widehat{Y}) = \widehat{X}$. On the other hand, for any finite collection $F = \{Z_1, \ldots, Z_k\}$ of finite subsets, $M(F) = Z_1 \cup \cdots \cup Z_k$. Thus for an infinite proper subset $Y \subset X$ we have $M(\widehat{Y}) = \widehat{X} \supset \widehat{Y} = \bigcup\{M(F) : F \text{ is a finite subset of } \widehat{Y}\}$.

A subset S of an ordered set $\mathcal{P}$ is said to be *up-directed* if for every x, $y \in S$ there exists $z \in S$ with $x \leq z$ and $y \leq z$. Thus every chain, or more generally every join semilattice, forms an up-directed set.

The following observation can be useful.

Theorem 3.1. *Let Γ be a closure operator on a set X. The following are equivalent.*

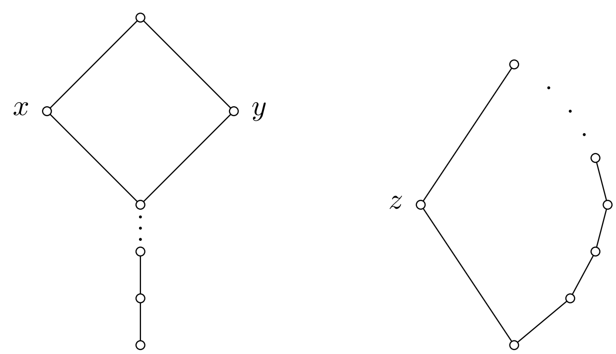
(1) *Γ is an algebraic closure operator.*
(2) *The union of any up-directed set of Γ-closed sets is Γ-closed.*
(3) *The union of any chain of Γ-closed sets is Γ-closed.*

The equivalence of (1) and (2), and the implication from (2) to (3), are straightforward. The implication from (3) to (1) can be done by induction, mimicking the proof of the corresponding step in Theorem 3.8. This is exercise 13.

We need to translate these ideas into the language of lattices. Let $\mathcal{L}$ be a complete lattice. An element $x \in L$ is *compact* if whenever $x \leq \bigvee A$, then there exists a finite subset $F \subseteq A$ such that $x \leq \bigvee F$. The set of all compact elements of $\mathcal{L}$ is denoted by $\mathcal{L}^c$. An elementary argument shows that $\mathcal{L}^c$ is closed under finite joins and contains 0, so it is a join semilattice with a least element. However, $\mathcal{L}^c$ is usually not closed under meets; see Figure 3.1(a), wherein x and y are compact but $x \wedge y$ is not.

A lattice $\mathcal{L}$ is said to be *algebraic*, or *compactly generated*, if it is complete and $\mathcal{L}^c$ is join dense in $\mathcal{L}$, i.e., $x = \bigvee(\downarrow x \cap L^c)$ for every $x \in L$. Clearly every finite lattice is algebraic. More generally, every element of a complete lattice $\mathcal{L}$ is compact, i.e., $\mathcal{L} = \mathcal{L}^c$ if and only if $\mathcal{L}$ satisfies the ACC.

For an example of a complete lattice that is not algebraic, let $\mathcal{K}$ denote the interval $[0, 1]$ in the real numbers with the usual order. Then $\mathcal{K}^c = \{0\}$, so $\mathcal{K}$ is not algebraic. The non-algebraic lattice in Figure 3.1(b) is another good example to keep in mind. The element z is not compact, and hence in this case not a join of compact elements.



(a) (b)

Figure 3.1

Historically, the role of algebraic closure operators arose in Birkhoff and Frink [3], with the modern definition of a compactly generated lattice following closely in Nachbin [12].

Theorem 3.2. *(1) A closure operator Γ is algebraic if and only if $\Gamma = \Gamma_\Sigma$ for some set Σ of finitary closure rules.*

(2) Let Γ be an algebraic closure operator on a set X. Then $\mathcal{C}_\Gamma$ is an algebraic lattice whose compact elements are $\{\Gamma(F) : F$ is a finite subset of $X\}$.

Proof. If Γ is an algebraic closure operator on a set X, then a set $S \subseteq X$ is closed if and only if $\Gamma(F) \subseteq S$ for every finite subset $F \subseteq S$. Thus the collection of all rules $F \subseteq S \implies z \in S$, with F a finite subset of X and $z \in \Gamma(F)$, determines closure for Γ.[1] Conversely, if Σ is a collection of finitary closure rules, then $z \in \Gamma_\Sigma(B)$ if and only if $z \in \Gamma_\Sigma(F)$ for some finite $F \subseteq B$, making Γ_Σ algebraic.

For (2), let us first observe that for any closure operator Γ on X, and for any collection of subsets A_i of X, we have $\Gamma(\bigcup A_i) = \bigvee \Gamma(A_i)$ where the join is computed in the lattice $\mathcal{C}_\Gamma$. The inclusion $\Gamma(\bigcup A_i) \supseteq \bigvee \Gamma(A_i)$ is immediate, while $\bigcup A_i \subseteq \bigcup \Gamma(A_i) \subseteq \bigvee \Gamma(A_i)$ implies $\Gamma(\bigcup A_i) \subseteq \Gamma(\bigvee \Gamma(A_i)) = \bigvee \Gamma(A_i)$.

In particular, for all $B \subseteq X$,

$$\Gamma(B) = \bigvee \{\Gamma(F) : F \text{ is a finite subset of } B\}.$$

Thus $\mathcal{C}_\Gamma$ will be an algebraic lattice, when Γ is an algebraic closure operator, if we can show that the closures of finite sets are compact.

So assume that Γ is algebraic, and let F be a finite subset of X. If $\Gamma(F) \leq \bigvee A_i$ in $\mathcal{C}_\Gamma$, then

$$F \subseteq \bigvee A_i = \Gamma(\bigcup A_i) = \bigcup \{\Gamma(G) : G \text{ finite } \subseteq \bigcup A_i\}.$$

Consequently each $x \in F$ is in some $\Gamma(G_x)$, where G_x is in turn contained in the union of finitely many A_i's. Therefore $\Gamma(F) \subseteq \Gamma(\bigcup_{x \in F} \Gamma(G_x)) \subseteq \bigvee_{j \in J} A_j$ for some finite subset $J \subseteq I$. We conclude that $\Gamma(F)$ is compact in $\mathcal{C}_\Gamma$.

Conversely, let C be compact in $\mathcal{C}_\Gamma$. Since C is closed and Γ is algebraic, $C = \bigvee \{\Gamma(F) : F \text{ finite } \subseteq C\}$. Since C is compact, there exist finitely many finite subsets of C, say $F_1, \ldots, F_n$, such that $C = \Gamma(F_1) \vee \ldots \vee \Gamma(F_n) = \Gamma(F_1 \cup \cdots \cup F_n)$. Thus C is the closure of a finite set. $\square$

Thus in a subalgebra lattice $\mathbf{Sub}\,\mathcal{A}$, the compact elements are the finitely generated subalgebras. In a congruence lattice $\mathbf{Con}\,\mathcal{A}$, the compact elements are the finitely generated congruences.

It is not true that $\mathcal{C}_\Gamma$ being algebraic implies that Γ is algebraic. For example, let X be the disjoint union of a one element set $\{b\}$ and an infinite set Y, and let Γ be the closure operator on X such that $\Gamma(A) = A$ if A is a proper subset of Y, $\Gamma(Y) = X$ and $\Gamma(B) = X$ if $b \in B$. The Γ-closed sets are all proper subsets of Y, and $X = Y \cup \{b\}$ itself. Thus $\mathcal{C}_\Gamma$ is isomorphic to the lattice of all subsets of Y. But $b \in \Gamma(Y)$, while b is not in the union of the closures of the finite subsets of Y, so Γ is not algebraic.

The following theorem includes a representation of any algebraic lattice as the lattice of closed sets of an algebraic closure operator.

Theorem 3.3. *If $\mathcal{S} = \langle S; \vee, 0\rangle$ is a join semilattice with 0, then the ideal lattice $\mathcal{I}(\mathcal{S})$ is algebraic. The compact elements of $\mathcal{I}(\mathcal{S})$ are the principal ideals $\downarrow x$ with*

[1] In general there are also valid infinitary closure rules for Γ, but for an algebraic closure operator these are redundant.

$x \in S$. Conversely, if $\mathcal{L}$ is an algebraic lattice, then $\mathcal{L}^c$ is a join semilattice with 0, and $\mathcal{L} \cong \mathcal{I}(\mathcal{L}^c)$.

Proof. Let $\mathcal{S}$ be a join semilattice with 0. I is an algebraic closure operator, so $\mathcal{I}(\mathcal{S})$ is an algebraic lattice. If $F \subseteq S$ is finite, then $I(F) = (\bigvee F)/0$, so compact ideals are principal.

Now let $\mathcal{L}$ be an algebraic lattice. There are two natural maps: $f : \mathcal{L} \to \mathcal{I}(\mathcal{L}^c)$ by $f(x) = \downarrow x \cap L^c$, and $g : \mathcal{I}(\mathcal{L}^c) \to \mathcal{L}$ by $g(J) = \bigvee J$. Both maps are clearly order preserving, and they are mutually inverse: $fg(J) = (\bigvee J)/0 \cap L^c = J$ by the definition of compactness, and $gf(x) = \bigvee(\downarrow x \cap L^c) = x$ by the definition of algebraic. Hence they are both isomorphisms, and $\mathcal{L} \cong \mathcal{I}(\mathcal{L}^c)$. □

Let us digress for a moment into universal algebra. A classic result of Birkhoff and Frink gives a concrete representation of algebraic closure operators [3].

Theorem 3.4. *Let Γ be an algebraic closure operator on a set X. Then there is an algebra $\mathcal{A}$ on the set X such that the subalgebras of $\mathcal{A}$ are precisely the closed sets of Γ.*

Corollary. *Every algebraic lattice is isomorphic to the lattice of all subalgebras of an algebra.*

Proof. An algebra in general is described by $\mathcal{A} = \langle A; F, C\rangle$ where A is a set, $F = \{f_i : i \in I\}$ a collection of operations on A (so $f_i : A^{n_i} \to A$), and C is a set of constants in A. The third section of Appendix 1 reviews the basic definitions of universal algebra.

The carrier set for our algebra must of course be X. For each nonempty finite set $G \subseteq X$ and element $x \in \Gamma(G)$, we have an operation $f_{G,x} : X^{|G|} \to X$ given by

$$f_{G,x}(a_1, \ldots, a_n) = \begin{cases} x & \text{if } \{a_1, \ldots, a_n\} = G \\ a_1 & \text{otherwise.} \end{cases}$$

Our constants are $C = \Gamma(\emptyset)$, the elements of the least closed set (which may be empty).

Note that since Γ is algebraic, a set $B \subseteq X$ is closed if and only if $\Gamma(G) \subseteq B$ for every finite $G \subseteq B$. Using this, it is very easy to check that the subalgebras of $\mathcal{A}$ are precisely the closed sets of $\mathcal{C}_\Gamma$. □

A direct proof of the Corollary is also of interest. Given an algebraic lattice $\mathcal{L}$, define an algebra $\mathcal{B}$ as follows. The carrier set of $\mathcal{B}$ is the set of compact elements $\mathcal{L}^c$, the join $\vee$ is one operation, and the least element 0 is a constant. For each $a \in \mathcal{L}^c$, define a unary operation f_a by

$$f_a(x) = \begin{cases} a & \text{if } a \leq x \\ x & \text{otherwise.} \end{cases}$$

The construction insures that the subalgebras of $\mathcal{B}$ are exactly the ideals of $\mathcal{L}^c$, whence $\mathbf{Sub}\,\mathcal{B} = \mathcal{I}(\mathcal{L}^c) \cong \mathcal{L}$.

However, the algebra constructed in the proof of Theorem 3.4 will have $|X|$ operations when X is infinite, and that in the second construction has $|\mathcal{L}^c| + 1$ operations. Having lots of operations is not necessarily a bad thing: vector spaces are respectable algebras, and a vector space over a field F has basic operations $f_r : \mathcal{V} \to \mathcal{V}$ where $f_r(v) = rv$ for every $r \in F$. Nonetheless, we like algebras to have few operations, like groups and lattices. A theorem due to Bill Hanf tells us when we can get by with a small number of operations.[2]

Theorem 3.5. *For any nontrivial algebraic lattice $\mathcal{L}$ the following conditions are equivalent.*

(1) *Each compact element of $\mathcal{L}$ contains only countably many compact elements.*
(2) *There exists an algebra $\mathcal{A}$ with only countably many operations and constants such that $\mathcal{L}$ is isomorphic to the subalgebra lattice of $\mathcal{A}$.*
(3) *There exists an algebra $\mathcal{B}$ with one binary operation (and no constants) such that $\mathcal{L}$ is isomorphic to the subalgebra lattice of $\mathcal{B}$.*

Proof. Of course (3) implies (2).

In general, if an algebra $\mathcal{A}$ has κ basic operations, λ constants and γ generators, then it is a homomorphic image of the absolutely free algebra $W(X)$ generated by a set X with $|X| = \gamma$ and the same κ operation symbols and λ constants. This free algebra can be constructed recursively: with F denoting the set of operation symbols and C the constant symbols, let $W_0 = X \cup C$ and $W_{k+1} = \{f(t_1, \ldots, t_n) : f \in F,\ t_1, \ldots, t_n \in W_k\}$. Then $W(X) = \bigcup_{k \geq 0} W_k$. Using this, it is easy to count that $|W(X)| \leq \max(\gamma, \kappa, \lambda, \aleph_0)$, with equality unless $\kappa = 0$. Moreover, $|\mathcal{A}| \leq |W(X)|$ since the former is a homomorphic image of the latter.

In particular then, if $\mathcal{C}$ is compact (i.e., finitely generated) in $\mathbf{Sub}\,\mathcal{A}$, and $\mathcal{A}$ has only countably many basic operations and constants, then $|\mathcal{C}| \leq \aleph_0$. Therefore $\mathcal{C}$ has only countably many finite subsets, and so there are only countably many finitely generated subalgebras $\mathcal{D}$ contained in $\mathcal{C}$. Thus (2) implies (1).

To show (1) implies (3), let $\mathcal{L}$ be a nontrivial algebraic lattice such that for each $x \in L^c$, $|\downarrow\! x \cap L^c| \leq \aleph_0$. We will construct an algebra $\mathcal{B}$ whose universe is $L^c - \{0\}$, with one binary operation $*$, whose subalgebras are precisely the ideals of $\mathcal{L}^c$ with 0 removed. This makes $\mathbf{Sub}\,\mathcal{B} \cong \mathcal{I}(\mathcal{L}^c) \cong \mathcal{L}$, as desired.

For each $c \in L^c - \{0\}$, we make a sequence $\langle c_i \rangle_{i \in \omega}$ as follows. If $2 \leq |\downarrow\! c \cap L^c| = n + 1 < \infty$, arrange $\downarrow\! c \cap L^c - \{0\}$ into a cyclically repeating sequence: $c_i = c_j$ iff $i \equiv j \bmod n$. If $\downarrow\! c \cap L^c$ is infinite (and hence countable), arrange $\downarrow\! c \cap L^c - \{0\}$ into a non-repeating sequence $\langle c_i \rangle$. In both cases start the sequence with $c_0 = c$.

[2] This result is unpublished but well known.

Define the binary operation $*$ for $c, d \in L^c - \{0\}$ by

$$c * d = c \vee d \text{ if } c \text{ and } d \text{ are incomparable,}$$
$$c * d = d * c = c_{i+1} \text{ if } d = c_i \leq c.$$

You can now check that $*$ is well defined, and that the algebra $\mathcal{B} = \langle L^c; * \rangle$ has exactly the sets of nonzero elements of ideals of $\mathcal{L}^c$ as subalgebras. $\square$

The situation with respect to congruence lattices is considerably more complicated. Nonetheless, the basic facts are the same: George Grätzer and E. T. Schmidt proved that every algebraic lattice is isomorphic to the congruence lattice of some algebra [10], and Bill Lampe showed that uncountably many operations may be required [9].

Ralph Freese and Walter Taylor modified Lampe's original example to obtain a very natural one. Let $\mathcal{V}$ be a vector space of countably infinite dimension over a field F with $|F| = \kappa > \aleph_0$. Let $\mathcal{L}$ be the congruence lattice $\mathbf{Con}\,\mathcal{V}$, which for vector spaces is isomorphic to the subspace lattice $\mathbf{Sub}\,\mathcal{V}$ (since homomorphisms on vector spaces are linear transformations, and any subspace of $\mathcal{V}$ is the kernel of a linear transformation). The representation we have just given for $\mathcal{L}$ involves κ operations f_r $(r \in F)$. In fact, one can show that *any* algebra $\mathcal{A}$ with $\mathbf{Con}\,\mathcal{A} \cong \mathcal{L}$ must have at least κ operations.

We now turn our attention to the structure of algebraic lattices. The lattice $\mathcal{L}$ is said to be *weakly atomic* if whenever $a > b$ in $\mathcal{L}$, there exist elements $u, v \in L$ such that $a \geq u \succ v \geq b$.

Theorem 3.6. *Every algebraic lattice is weakly atomic.*

Proof. Let $a > b$ in an algebraic lattice $\mathcal{L}$. Then there is a compact element $c \in L^c$ with $c \leq a$ and $c \not\leq b$. Let $\mathcal{P} = \{x \in a/b : c \not\leq x\}$. Note $b \in P$, and since c is compact the join of a chain in $\mathcal{P}$ is again in $\mathcal{P}$. Hence by Zorn's Lemma, $\mathcal{P}$ contains a maximal element v, and the element $u = c \vee v$ covers v. Thus $b \leq v \prec u \leq a$. $\square$

A lattice $\mathcal{L}$ is said to be *upper continuous* if whenever D is an up-directed set having a least upper bound $\bigvee D$, then for any element $a \in L$, the join $\bigvee_{d \in D}(a \wedge d)$ exists, and

$$a \wedge \bigvee D = \bigvee_{d \in D} (a \wedge d).$$

The property of being *lower continuous* is defined dually.

Upper continuity applies most naturally to complete lattices, but it also arises in non-complete lattices. See Section II.2 of Freese, Ježek and Nation [8] and for a more general setting Adaricheva, Gorbunov and Semenova [1].

Theorem 3.7. *Every algebraic lattice is upper continuous.*

Proof. Let $\mathcal{L}$ be algebraic and D an up-directed subset of $\mathcal{L}$. Of course $\bigvee_{d \in D}(a \wedge d) \leq a \wedge \bigvee D$. Let $r = a \wedge \bigvee D$. For each compact element $c \in {\downarrow} r \cap L^c$, we have $c \leq a$

and $c \leq \bigvee D$. The compactness of c implies $c \leq \bigvee F$ for some finite subset F of D. By the up-directed property, we can choose $e \in D$ with $\bigvee F \leq e$, so that $c \leq a \wedge e$. Consequently,

$$r = \bigvee(\downarrow r \cap L^c) \leq \bigvee_{d \in D} (a \wedge d),$$

and equality follows. $\square$

Two alternative forms of join continuity are often useful.

Theorem 3.8. *For a complete lattice $\mathcal{L}$, the following are equivalent.*

(1) *$\mathcal{L}$ is upper continuous.*
(2) *For every $a \in L$ and chain $C \subseteq L$, we have $a \wedge \bigvee C = \bigvee_{c \in C} a \wedge c$.*
(3) *For every $a \in L$ and $S \subseteq L$,*

$$a \wedge \bigvee S = \bigvee_{F \text{ finite } \subseteq S} (a \wedge \bigvee F).$$

Proof. It is straightforward that (3) implies (1) implies (2), so this is left to the reader. Following Crawley and Dilworth [7], we will show that (2) implies (3) by induction on $|S|$. Property (3) is trivial if $|S|$ is finite, so assume it is infinite, and let λ be the least ordinal with $|S| = |\lambda|$. Arrange the elements of S into a sequence $\langle x_\xi : \xi < \lambda \rangle$. Put $S_\xi = \{x_\nu : \nu < \xi\}$. Then $|S_\xi| < |S|$ for each $\xi < \lambda$, and the elements of the form $\bigvee S_\xi$ are a chain in $\mathcal{L}$. Thus, using (1), we can calculate

$$\begin{aligned} a \wedge \bigvee S &= a \wedge \bigvee_{\xi < \lambda} \bigvee S_\xi \\ &= \bigvee_{\xi < \lambda} (a \wedge \bigvee S_\xi) \\ &= \bigvee_{\xi < \lambda} (\bigvee_{F \text{ finite } \subseteq S_\xi} (a \wedge \bigvee F)) \\ &= \bigvee_{F \text{ finite } \subseteq S} (a \wedge \bigvee F), \end{aligned}$$

as desired. $\square$

An element $a \in L$ is called an *atom* if $a \succ 0$, and a *coatom* if $1 \succ a$. Theorem 3.8 shows that every atom in an upper continuous lattice is compact. More generally, if $\downarrow a$ satisfies the ACC in an upper continuous lattice, then a is compact.

We know that every element x in an algebraic lattice can be expressed as the join of $\downarrow x \cap L^c$ (by definition). It turns out to be at least as important to know how x can be expressed as a meet of other elements. We say that an element q in a complete lattice $\mathcal{L}$ is *completely meet irreducible* if, for every subset S of L, $q = \bigwedge S$ implies $q \in S$. These are of course the elements that cannot be expressed as the proper meet of other elements. Let $M^*(\mathcal{L})$ denote the set of all completely meet irreducible elements of $\mathcal{L}$. Note that $1 \notin M^*(\mathcal{L})$ (since $\bigwedge \emptyset = 1$ and $1 \notin \emptyset$).

Theorem 3.9. *Let $q \in L$ where $\mathcal{L}$ is a complete lattice. The following are equivalent.*

(1) $q \in M^*(\mathcal{L})$.
(2) $\bigwedge\{x \in L : x > q\} > q$.
(3) *There exists $q^* \in L$ such that $q^* \succ q$ and for all $x \in L$, $x > q$ implies $x \geq q^*$.*

The connection between (2) and (3) is of course $q^* = \bigwedge\{x \in L : x > q\}$. In a finite lattice, $q \in M^*(\mathcal{L})$ iff there is a unique element q^* covering q, but in general we need the stronger property (3).

A *decomposition* of an element $a \in L$ is a representation $a = \bigwedge Q$ where Q is a set of completely meet irreducible elements of $\mathcal{L}$. An element in an arbitrary lattice may have any number of decompositions, including none. A theorem due to Garrett Birkhoff says that every element in an algebraic lattice has at least one decomposition [2].

Theorem 3.10. *If $\mathcal{L}$ is an algebraic lattice, then $M^*(\mathcal{L})$ is meet dense in $\mathcal{L}$. Thus for every $x \in L$, $x = \bigwedge(\uparrow x \cap M^*(\mathcal{L}))$.*

Proof. Let $m = \bigwedge(\uparrow x \cap M^*(\mathcal{L}))$, and suppose $x < m$. Then there exists a $c \in L^c$ with $c \leq m$ and $c \not\leq x$. Since c is compact, we can use Zorn's Lemma to find an element q that is maximal with respect to $q \geq x$, $q \not\geq c$. For any $y \in L$, $y > q$ implies $y \geq q \vee c$, so q is completely meet irreducible with $q^* = q \vee c$. Then $q \in \uparrow x \cap M^*(\mathcal{L})$ implies $q \geq m \geq c$, a contradiction. Hence $x = m$. $\square$

Note that the preceding argument is closely akin to that of Theorem 3.6.

It is rare for an element in an algebraic lattice to have a unique decomposition. A somewhat weaker property is for an element to have an *irredundant* decomposition, meaning $a = \bigwedge Q$ but $a < \bigwedge(Q - \{q\})$ for all $q \in Q$, where Q is a set of completely meet irreducible elements. An element in an algebraic lattice need not have an irredundant decomposition either. Let $\mathcal{L}$ be the lattice consisting of the empty set and all cofinite subsets of an infinite set X, ordered by set inclusion. This satisfies the ACC so it is algebraic. The completely meet irreducible elements of $\mathcal{L}$ are its coatoms, the complements of one element subsets of X. The meet of any infinite collection of coatoms is 0 (the empty set), but no such decomposition is irredundant. Clearly also these are the only decompositions of 0, so 0 has no irredundant decomposition.

A lattice is *strongly atomic* if $a > b$ in $\mathcal{L}$ implies there exists $u \in L$ such that $a \geq u \succ b$. A beautiful result of Peter Crawley guarantees the existence of irredundant decompositions in strongly atomic algebraic lattices [5].

Theorem 3.11. *If an algebraic lattice $\mathcal{L}$ is strongly atomic, then every element of $\mathcal{L}$ has an irredundant decomposition.*

If $\mathcal{L}$ is also distributive, we obtain the uniqueness of irredundant decompositions.

Theorem 3.12. *If $\mathcal{L}$ is a distributive, strongly atomic, algebraic lattice, then every element of $\mathcal{L}$ has a unique irredundant decomposition.*

The finite case of Theorem 3.12 is the dual of Theorem 8.6(c), which we will prove later.

The theory of decompositions was studied extensively by Dilworth and Crawley, and their book [7] contains most of the principal results. For refinements since then, see the section on decompositions in The Dilworth Theorems [4], Semenova [13], and the references in [13] to papers of Erné, Gorbunov, Richter, Semenova and Walendziak.

Exercises for Chapter 3

1. Prove that an upper continuous distributive lattice satisfies the infinite distributive law $a \wedge (\bigvee_{i \in I} b_i) = \bigvee_{i \in I}(a \wedge b_i)$.
2. Describe the complete sublattices of the real numbers $\Re$ that are algebraic.
3. Show that the natural map from a lattice to its ideal lattice, $\varphi : \mathcal{L} \to \mathcal{I}(\mathcal{L})$ by $\varphi(x) = \downarrow x$, is a lattice embedding. Show that $(\mathcal{I}(\mathcal{L}), \varphi)$ is a join dense completion of $\mathcal{L}$, and that it may differ from the MacNeille completion.
4. Recall that a *filter* is a dual ideal. The filter lattice $\mathcal{F}(\mathcal{L})$ of a lattice $\mathcal{L}$ is ordered by reverse set inclusion: $F \leq G$ iff $F \supseteq G$. Prove that $\mathcal{L}$ is naturally embedded in $\mathcal{F}(\mathcal{L})$, and that $\mathcal{F}(\mathcal{L})$ is dually compactly generated.
5. Prove that every element of a complete lattice $\mathcal{L}$ is compact if and only if $\mathcal{L}$ satisfies the ACC. (Cf. Exercise 2.2.)
6. A nonempty subset S of a complete lattice $\mathcal{L}$ is a *complete sublattice* if $\bigvee A \in S$ and $\bigwedge A \in S$ for every nonempty subset $A \subseteq S$. Prove that a complete sublattice of an algebraic lattice is algebraic.
7. (a) Represent the lattices $\mathcal{M}_3$ and $\mathcal{N}_5$ as **Sub** $\mathcal{A}$ for a finite algebra $\mathcal{A}$.

   (b) Show that $\mathcal{M}_3 \cong$ **Sub** $\mathcal{G}$ for a (finite) group $\mathcal{G}$, but that $\mathcal{N}_5$ cannot be so represented.

   (c) For which values of n is $\mathcal{M}_n$ the lattice of subgroups of an abelian group $\mathcal{G}$?
8. A closure rule is *nullary* if it has the form $x \in S$, and *unary* if it is of the form $y \in S \implies z \in S$. Prove that if Σ is a collection of nullary and unary closure rules, then nonempty unions of closed sets are closed, and hence the lattice of closed sets $\mathcal{C}_\Sigma$ is distributive. Conclude that the subalgebra lattice of an algebra with only constants and unary operations is distributive.
9. Let $\mathcal{L}$ be a complete lattice, J a join dense subset of L and M a meet dense subset of L. Define maps $\sigma : \mathfrak{P}(J) \to \mathfrak{P}(M)$ and $\pi : \mathfrak{P}(M) \to \mathfrak{P}(J)$ by

$$\sigma(X) = X^u \cap M$$

$$\pi(Y) = Y^\ell \cap J.$$

By Exercise 2.13, with R the restriction of $\leq$ to $J \times M$, $\pi\sigma$ is a closure operator on J and $\sigma\pi$ is a closure operator on M. Prove that $\mathcal{C}_{\pi\sigma} \cong \mathcal{L}$ and that $\mathcal{C}_{\sigma\pi}$ is dually isomorphic to $\mathcal{L}$.

10. A lattice is *semimodular* if $a \succ a \wedge b$ implies $a \vee b \succ b$. Prove that if every element of a finite lattice $\mathcal{L}$ has a unique irredundant decomposition, then $\mathcal{L}$ is semimodular. (Morgan Ward)

11. A decomposition $a = \bigwedge Q$ is *strongly irredundant* if $a < q^* \wedge \bigwedge(Q - \{q\})$ for all $q \in Q$. Prove that every irredundant decomposition in a strongly atomic semimodular lattice is strongly irredundant. (Keith Kearnes)

12. Let $\mathcal{L}$ be the lattice of ideals of the ring of integers Z. Find $M^*(\mathcal{L})$ and all decompositions of 0.

13. Complete the proof of Theorem 3.1. That is, let Γ be a closure operator on a set X, and assume that the union of any chain of Γ-closed sets is closed. Prove by induction on $|S|$ that, for any $S \subseteq X$,

$$\Gamma(S) = \bigcup\{\Gamma(F) : F \text{ is a finite subset of } S\}.$$

14. Let κ be an uncountable cardinal. Show that the following are equivalent.

(1) Each compact element of $\mathcal{L}$ contains at most κ compact elements.
(2) There exists an algebra $\mathcal{A}$ with at most κ operations and constants such that $\mathcal{L}$ is isomorphic to the subalgebra lattice of $\mathcal{A}$.

A complete lattice is said to be *spatial* if every element is a join of completely join irreducible elements, i.e., $x = \bigvee({\downarrow}x \cap J^*(\mathcal{L}))$. For applications and further references, see for example Santocanale and Wehrung [11]. The next exercises develop a generalization of Theorem 2.9.

15. Show that in a complete, upper continuous lattice, an element is completely join irreducible if and only if it is (finitely) join irreducible and compact.

16. Let $\mathcal{L}$ be a complete, upper continuous, spatial lattice. Show that $\mathcal{L}$ is algebraic, and moreover, $\mathcal{L}$ is isomorphic to the lattice of Σ-closed sets for the closure system Σ on $J^*(\mathcal{L})$ determined by the rules

$$F \subseteq S \implies q \in S$$

where q is completely join irreducible, F is a finite subset of $J^*(\mathcal{L})$, and $q \leq \bigvee F$.

17. Prove that if $\mathcal{L}$ is an algebraic lattice satisfying the DCC, then L is spatial.

References

1. K. Adaricheva, V. Gorbunov and M. Semenova, *On continuous noncomplete lattices*, Algebra Universalis **46** (2001), 215–230.
2. G. Birkhoff, *Subdirect unions in universal algebra*, Bull. Amer. Math. Soc. **50** (1944), 764–768.
3. G. Birkhoff and O. Frink, *Representations of sets by lattices*, Trans. Amer. Math. Soc. **64** (1948), 299–316.
4. K. Bogart, R. Freese and J. Kung, Eds., *The Dilworth Theorems*, Birkhäuser, Boston, Basel, Berlin, 1990.

5. P. Crawley, *Decomposition theory for nonsemimodular lattices*, Trans. Amer. Math. Soc. **99** (1961), 246–254.
6. P. Crawley and R. P. Dilworth, *Decomposition theory for lattices without chain conditions*, Trans. Amer. Math. Soc. **96** (1960), 1–22.
7. P. Crawley and R. P. Dilworth, *Algebraic Theory of Lattices*, Prentice-Hall, Englewood Cliffs, N. J., 1973.
8. R. Freese, J. Ježek, and J. B. Nation, *Free Lattices*, Mathematical Surveys and Monographs, vol. 42, Amer. Math. Soc., Providence, 1995.
9. R. Freese, W. A. Lampe and W. Taylor, *Congruence lattices of algebras of fixed similarity type,* I, Pacific J. Math. **82** (1979), 59–68.
10. G. Grätzer and E. T. Schmidt, *Characterizations of congruence lattices of abstract algebras*, Acta Sci. Math. (Szeged) **24** (1963), 34–59.
11. L. Santocanale and F. Wehrung, *Varieties of lattices with geometric descriptions*, preprint (2011).
12. L. Nachbin, *On characterization of the lattice of all ideals of a Boolean ring*, Fund. Math. **36** (1949), 137–142.
13. M. Semenova, *Decompositions in complete lattices*, Algebra and Logic **40** (2001), 384–390.

4. Representation by Equivalence Relations

No taxation without representation!

So far we have no analogue for lattices of the Cayley theorem for groups, that every group is isomorphic to a group of permutations. The corresponding representation theorem for lattices, that every lattice is isomorphic to a lattice of equivalence relations, turns out to be considerably deeper. Its proof uses a recursive construction technique that has become a standard tool of lattice theory and universal algebra.

An *equivalence relation* on a set X is a binary relation E satisfying, for all $x, y, z \in X$,

(1) $x \; E \; x$,
(2) $x \; E \; y$ implies $y \; E \; x$,
(3) if $x \; E \; y$ and $y \; E \; z$, then $x \; E \; z$.

We think of an equivalence relation as partitioning the set X into blocks of E-related elements, called equivalence classes. Conversely, any partition of X into a disjoint union of blocks induces an equivalence relation on X: $x \; E \; y$ iff x and y are in the same block. As usual with relations, we write $x \; E \; y$ and $(x, y) \in E$ interchangeably.

The most important equivalence relations are those induced by maps. If Y is another set, and $f : X \to Y$ is any function, then

$$\ker f = \{(x, y) \in X^2 : f(x) = f(y)\}$$

is an equivalence relation, called the *kernel* of f. If X and Y are algebras and $f : X \to Y$ is a homomorphism, then $\ker f$ is a *congruence relation*.

Thinking of binary relations as subsets of X^2, the axioms (1)–(3) for an equivalence relation are finitary closure rules. Thus the collection of all equivalence relations on X forms an algebraic lattice $\mathbf{Eq}\, X$. The order on $\mathbf{Eq}\, X$ is given by set containment, i.e.,

$$\begin{aligned} R \leq S \quad &\text{iff} \quad R \subseteq S \text{ in } \mathfrak{P}(X^2) \\ &\text{iff} \quad (x, y) \in R \implies (x, y) \in S. \end{aligned}$$

The greatest element of $\mathbf{Eq}\, X$ is the universal relation X^2, and its least element is the equality relation $=$. The meet operation in $\mathbf{Eq}\, X$ is of course set intersection, which means that $(x, y) \in \bigwedge_{i \in I} E_i$ if and only if $x \; E_i \; y$ for all $i \in I$. The join

$\bigvee_{i\in I} E_i$ is the transitive closure of the set union $\bigcup_{i\in I} E_i$. Thus $(x, y) \in \bigvee E_i$ if and only if there exists a finite sequence of elements x_j and indices i_j such that

$$x = x_0 \ E_{i_1} \ x_1 \ E_{i_2} \ x_2 \dots x_{k-1} \ E_{i_k} \ x_k = y.$$

The lattice $\mathbf{Eq}\, X$ has many nice properties: it is algebraic, strongly atomic, semimodular, relatively complemented and simple [8]; see Chapter 12 of Crawley and Dilworth [1].[1] The proofs of these facts are exercises in this chapter and Chapter 11.

If R and S are relations on X, define the *relative product* $R \circ S$ to be the set of all pairs $(x, y) \in X^2$ for which there exists a $z \in X$ with $x \ R \ z \ S \ y$. If R and S are equivalence relations, then because $x \ R \ x$ we have $S \subseteq R \circ S$; similarly $R \subseteq R \circ S$. Thus

$$R \circ S \ \subseteq \ R \circ S \circ R \ \subseteq \ R \circ S \circ R \circ S \ \subseteq \ \cdots$$

and it is not hard to see that $R \vee S$ is the union of this chain. It is possible, however, that $R \vee S$ is in fact equal to some term in the chain; for example, this is always the case when X is finite. Our proof will yield a representation in which this is always the case, for any two equivalence relations that represent elements of the given lattice.

To be precise, a *representation* (by equivalence relations) of a lattice $\mathcal{L}$ is an ordered pair (X, F) where X is a set and $F : \mathcal{L} \to \mathbf{Eq}\, X$ is a lattice embedding. We say that the representation is

(1) *of type* 1 if $F(x) \vee F(y) = F(x) \circ F(y)$ for all $x, y \in L$,
(2) *of type* 2 if $F(x) \vee F(y) = F(x) \circ F(y) \circ F(x)$ for all $x, y \in L$,
(3) *of type* 3 if $F(x) \vee F(y) = F(x) \circ F(y) \circ F(x) \circ F(y)$ for all $x, y \in L$.

P. M. Whitman [11] proved in 1946 that every lattice has a representation. In 1953 Bjarni Jónsson [7] found a simpler proof that gives a slightly stronger result.

Theorem 4.1. *Every lattice has a type 3 representation.*

Proof. Given a lattice $\mathcal{L}$, we will use transfinite recursion to construct a type 3 representation of $\mathcal{L}$.

A *weak representation* of $\mathcal{L}$ is a pair (U, F) where U is a set and $F : \mathcal{L} \to \mathbf{Eq}\, U$ is a one-to-one meet homomorphism. Let us order the weak representations of $\mathcal{L}$ by

$$(U, F) \sqsubseteq (V, G) \text{ if } U \subseteq V \text{ and } G(x) \cap U^2 = F(x) \text{ for all } x \in L.$$

We want to construct a (transfinite) sequence $(U_\xi, F_\xi)_{\xi<\lambda}$ of weak representations of $\mathcal{L}$, with $(U_\alpha, F_\alpha) \sqsubseteq (U_\beta, F_\beta)$ whenever $\alpha \le \beta$, whose limit (union) will be a lattice embedding of L into $\mathbf{Eq} \bigcup_{\xi<\lambda} U_\xi$. We can begin our construction by letting (U_0, F_0) be the weak representation with $U_0 = L$ and $(y, z) \in F_0(x)$ iff $y = z$ or $y \vee z \le x$. The crucial step is where we fix up the joins one at a time.

[1] The terms *relatively complemented* and *simple* are defined in Chapter 10; we include them here for the sake of completeness.

Sublemma 1. *If (U,F) is a weak representation of $\mathcal{L}$ and $(p,q) \in F(x \vee y)$, then there exists $(V,G) \sqsupseteq (U,F)$ with $(p,q) \in G(x) \circ G(y) \circ G(x) \circ G(y)$.*

Proof of Sublemma 1. Form V by adding three new points to U, say $V = U \,\dot{\cup}\, \{r,s,t\}$, as in Figure 4.1. We want to make

$$p \; G(x) \; r \; G(y) \; s \; G(x) \; t \; G(y) \; q.$$

Accordingly, for $z \in L$ we define $G(z)$ to be the reflexive, symmetric relation on U satisfying, for u, $v \in U$,

(1) $u \; G(z) \; v$ iff $u \; F(z) \; v$,
(2) $u \; G(z) \; r$ iff $z \geq x$ and $u \; F(z) \; p$,
(3) $u \; G(z) \; s$ iff $z \geq x \vee y$ and $u \; F(z) \; p$,
(4) $u \; G(z) \; t$ iff $z \geq y$ and $u \; F(z) \; q$,
(5) $r \; G(z) \; s$ iff $z \geq y$,
(6) $s \; G(z) \; t$ iff $z \geq x$,
(7) $r \; G(z) \; t$ iff $z \geq x \vee y$.

You must check that each $G(z)$ defined thusly really is an equivalence relation, i.e., that it is transitive. This is routine but a bit tedious to write down, so we leave it to the reader. There are four cases, depending on whether or not $z \geq x$ and on whether or not $z \geq y$. Straightforward though it is, this verification would not work if we had only added one or two new elements between p and q; see Theorems 4.5 and 4.6.

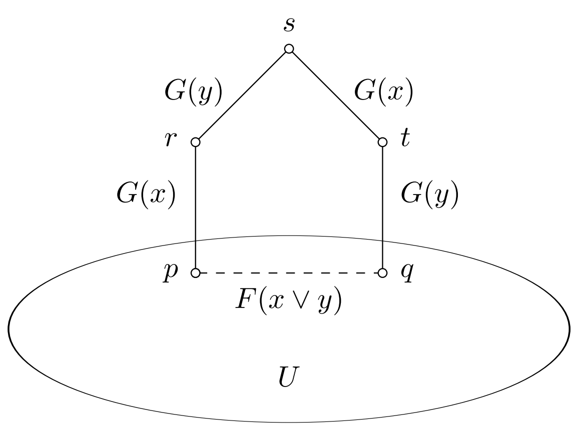


FIGURE 4.1

Now (1) says that $G(z) \cap U^2 = F(z)$. Since F is one-to-one, this implies G is also. Note that for z, $z' \in L$ we have $z \wedge z' \geq x$ iff $z \geq x$ and $z' \geq x$, and symmetrically for y. Using this with conditions (1)–(7), it is not hard to check that $G(z \wedge z') = G(z) \cap G(z')$. Hence, G is a weak representation of $\mathcal{L}$, and clearly $(U, F) \sqsubseteq (V, G)$. $\square$

Sublemma 2. *Let λ be a limit ordinal, and for $\xi < \lambda$ let (U_ξ, F_ξ) be weak representations of $\mathcal{L}$ such that $\alpha < \beta < \lambda$ implies $(U_\alpha, F_\alpha) \sqsubseteq (U_\beta, F_\beta)$. Let $V = \bigcup_{\xi<\lambda} U_\xi$ and $G(x) = \bigcup_{\xi<\lambda} F_\xi(x)$ for all $x \in L$. Then (V, G) is a weak representation of $\mathcal{L}$ with $(U_\xi, F_\xi) \sqsubseteq (V, G)$ for each $\xi < \lambda$.*

Proof. Let $\xi < \lambda$. Since $F_\alpha(x) = F_\xi(x) \cap U_\alpha^2 \subseteq F_\xi(x)$ whenever $\alpha < \xi$ and $F_\xi(x) = F_\beta(x) \cap U_\xi^2$ whenever $\beta \geq \xi$, for all $x \in L$ we have

$$\begin{aligned} G(x) \cap U_\xi^2 &= \big(\bigcup_{\gamma<\lambda} F_\gamma(x)\big) \cap U_\xi^2 \\ &= \bigcup_{\gamma<\lambda} (F_\gamma(x) \cap U_\xi^2) \\ &= F_\xi(x). \end{aligned}$$

Thus $(U_\xi, F_\xi) \sqsubseteq (V, G)$. Since F_0 is one-to-one, this implies that G is also.

It remains to show that G is a meet homomorphism. Clearly G preserves order, so for any x, $y \in L$ we have $G(x \wedge y) \subseteq G(x) \cap G(y)$. On the other hand, if $(u, v) \in G(x) \cap G(y)$, then there exists $\alpha < \lambda$ such that $(u, v) \in F_\alpha(x)$, and there exists $\beta < \lambda$ such that $(u, v) \in F_\beta(y)$. If γ is the larger of α and β, then $(u, v) \in F_\gamma(x) \cap F_\gamma(y) = F_\gamma(x \wedge y) \subseteq G(x \wedge y)$. Thus $G(x) \cap G(y) \subseteq G(x \wedge y)$. Combining the two inclusions gives equality. $\square$

Now we want to use these two sublemmas to construct a type 3 representation of $\mathcal{L}$, i.e., a weak representation that also satisfies $G(x \vee y) = G(x) \circ G(y) \circ G(x) \circ G(y)$.

Start with an arbitrary weak representation (U_0, F_0), and consider the set of all quadruples (p, q, x, y) such that $p, q \in U_0$ and $x, y \in L$ and $(p, q) \in F_0(x \vee y)$. Arrange these into a well ordered sequence $(p_\xi, q_\xi, x_\xi, y_\xi)$ for $\xi < \eta$. Applying the sublemmas repeatedly, we can obtain a sequence of weak representations (U_ξ, F_ξ) for $\xi \leq \eta$ such that

(1) if $\xi < \eta$, then $(U_\xi, F_\xi) \sqsubseteq (U_{\xi+1}, F_{\xi+1})$ and $(p_\xi, q_\xi) \in F_{\xi+1}(x_\xi) \circ F_{\xi+1}(y_\xi) \circ F_{\xi+1}(x_\xi) \circ F_{\xi+1}(y_\xi)$;

(2) if $\lambda \leq \eta$ is a limit ordinal, then $U_\lambda = \bigcup_{\xi<\lambda} U_\xi$ and $F_\lambda(x) = \bigcup_{\xi<\lambda} F_\xi(x)$ for all $x \in L$.

Let $V_1 = U_\eta$ and $G_1 = F_\eta$. If $p, q \in U_0$, and $x, y \in L$ and $p\ F_0(x \vee y)\ q$, then $(p, q, x, y) = (p_\xi, q_\xi, x_\xi, y_\xi)$ for some $\xi < \eta$, so that $(p, q) \in F_{\xi+1}(x) \circ F_{\xi+1}(y) \circ F_{\xi+1}(x) \circ F_{\xi+1}(y)$. Consequently,

$$F_0(x \vee y) \subseteq G_1(x) \circ G_1(y) \circ G_1(x) \circ G_1(y).$$

Note $(U_0, F_0) \sqsubseteq (V_1, G_1)$.

Of course, along the way we have probably introduced lots of new failures of the join property that need to be fixed up. So repeat this whole process ω times, obtaining a sequence

$$(U_0, F_0) = (V_0, G_0) \sqsubseteq (V_1, G_1) \sqsubseteq (V_2, G_2) \sqsubseteq \cdots$$

such that $G_n(x \vee y) \subseteq G_{n+1}(x) \circ G_{n+1}(y) \circ G_{n+1}(x) \circ G_{n+1}(y)$ for all $n \in w$, $x, y \in L$.

Finally, let $W = \bigcup_{n \in w} V_n$ and $H(x) = \bigcup_{n \in \omega} G_n(x)$ for all $x \in L$, and you get a type 3 representation of $\mathcal{L}$. $\square$

Since the proof involves transfinite recursion, it produces a representation (X, F) with X infinite, even when $\mathcal{L}$ is finite. For a long time one of the outstanding questions of lattice theory was whether every finite lattice can be embedded into the lattice of equivalence relations on a finite set. In 1980, Pavel Pudlák and Jíři Tůma showed that the answer is *yes* [10]. The proof is quite difficult.

Theorem 4.2. *Every finite lattice has a representation (Y, G) with Y finite.*

One of the motivations for Whitman's theorem was Garrett Birkhoff's observation, made in the 1930's, that a representation of a lattice $\mathcal{L}$ by equivalence relations induces an embedding of $\mathcal{L}$ into the lattice of subgroups of a group. Given a representation (X, F) of $\mathcal{L}$, let $\mathcal{G}$ be the group of all permutations on X that move only finitely many elements, and let **Sub** $\mathcal{G}$ denote the lattice of subgroups of $\mathcal{G}$. Let $h : \mathcal{L} \to \mathbf{Sub}\, \mathcal{G}$ by

$$h(a) = \{\pi \in G : x \; F(a) \; \pi(x) \text{ for all } x \in X\}.$$

Then it is not too hard to check that h is an embedding.

Theorem 4.3. *Every lattice can be embedded into the lattice of subgroups of a group.*

Not all lattices have representations of type 1 or 2, so it is natural to ask which ones do. First we consider sublattices of **Eq** X with type 2 joins.

Lemma 4.4. *Let $\mathcal{L}$ be a sublattice of* **Eq** X *with the property that $R \vee S = R \circ S \circ R$ for all R, $S \in L$. Then $\mathcal{L}$ satisfies*

$$(M) \qquad x \geq y \quad \textit{implies} \quad x \wedge (y \vee z) = y \vee (x \wedge z).$$

The implication (M) is known as the *modular law.*

Proof. Assume that $\mathcal{L}$ is a sublattice of **Eq** X with type 2 joins, and let $A, B, C \in L$ with $A \geq B$. If $p, q \in X$ and $(p, q) \in A \wedge (B \vee C)$, then

$$p \; A \; q$$
$$p \; B \; r \; C \; s \; B \; q$$

for some $r, s \in X$ (see Figure 4.2). Since

$$r \; B \; p \; A \; q \; B \; s$$

and $B \le A$, we have $(r, s) \in A \wedge C$. It follows that $(p, q) \in B \vee (A \wedge C)$. Thus $A \wedge (B \vee C) \le B \vee (A \wedge C)$. The reverse inclusion is trivial, so we have equality. □

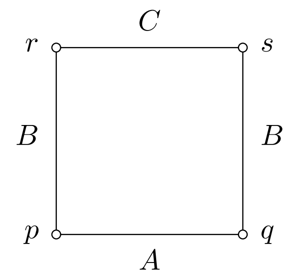


FIGURE 4.2

On the other hand, Jónsson gave a slight variation of the proof of Theorem 4.1 that shows that every modular lattice has a type 2 representation [7], [1]. Combining this with Lemma 4.4, we obtain the following.

Theorem 4.5. *A lattice has a type 2 representation if and only if it is modular.*

The modular law (M) plays an important role in lattice theory, and we will see it often. It was invented in the 1890's by Richard Dedekind, who showed that the lattice of normal subgroups of a group is modular [2], [3]. Note that (M) fails in the pentagon $\mathcal{N}_5$. In fact, Dedekind proved that a lattice is modular if and only if it does not contain the pentagon as a sublattice; see Theorem 9.1.

The modular law is equivalent to the equation,

$$(M') \qquad x \wedge ((x \wedge y) \vee z) = (x \wedge y) \vee (x \wedge z).$$

It is easily seen to be a special case of (and hence weaker than) the distributive law,

$$(D) \qquad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),$$

viz., (M) says that (D) should hold for $x \ge y$.

Note that the normal subgroup lattice of a group has a natural representation (X, F): take $X = G$ and $F(N) = \{(x, y) \in G^2 : xy^{-1} \in N\}$. This representation is in fact type 1 (Exercise 3), and Jónsson showed that lattices with a type 1 representation, or equivalently sublattices of $\mathbf{Eq}\ X$ in which $R \vee S = R \circ S$, satisfy an implication stronger than the modular law. A lattice is said to be *Arguesian* if it satisfies

$$(A) \qquad (a_0 \vee b_0) \wedge (a_1 \vee b_1) \leq a_2 \vee b_2 \text{ implies } c_2 \leq c_0 \vee c_1$$

where

$$c_i = (a_j \vee a_k) \wedge (b_j \vee b_k)$$

for $\{i, j, k\} = \{0, 1, 2\}$. The Arguesian law is (less obviously) equivalent to a lattice inclusion,

$$(A') \qquad (a_0 \vee b_0) \wedge (a_1 \vee b_1) \wedge (a_2 \vee b_2) \leq a_0 \vee (b_0 \wedge (c \vee b_1))$$

where

$$c = c_2 \wedge (c_0 \vee c_1).$$

These are two of several equivalent forms of this law, which is stronger than modularity and weaker than distributivity. The Arguesian law is modelled after Desargues' Law in projective geometry.

Theorem 4.6. *If $\mathcal{L}$ is a sublattice of* $\mathbf{Eq}\, X$ *with the property that $R \vee S = R \circ S$ for all R, $S \in L$, then $\mathcal{L}$ satisfies the Arguesian law.*

Corollary. *Every lattice that has a type 1 representation is Arguesian.*

Proof. Let $\mathcal{L}$ be a sublattice of $\mathbf{Eq}\, X$ with type 1 joins. Assume $(A_0 \vee B_0) \wedge (A_1 \vee B_1) \leq A_2 \vee B_2$, and suppose $(p, q) \in C_2 = (A_0 \vee A_1) \wedge (B_0 \vee B_1)$. Then there exist r, s such that

$$\begin{gathered} p\ A_0\ r\ A_1\ q \\ p\ B_0\ s\ B_1\ q. \end{gathered}$$

Since $(r, s) \in (A_0 \vee B_0) \wedge (A_1 \vee B_1) \leq A_2 \vee B_2$, there exists t such that $r\ A_2\ t\ B_2\ s$. Now you can check that

$$\begin{gathered} (p, t) \in (A_0 \vee A_2) \wedge (B_0 \vee B_2) = C_1 \\ (t, q) \in (A_1 \vee A_2) \wedge (B_1 \vee B_2) = C_0 \end{gathered}$$

and hence $(p, q) \in C_0 \vee C_1$. Thus $C_2 \leq C_0 \vee C_1$, as desired. (This argument is diagrammed in Figure 4.3.) □

It follows that the lattice of normal subgroups of a group is not only modular, but Arguesian; see exercise 3. All these types of lattices are Arguesian: the lattice of subgroups of an abelian group, the lattice of ideals of a ring, the lattice of subspaces of a vector space, the lattice of submodules of a module. More generally, Ralph

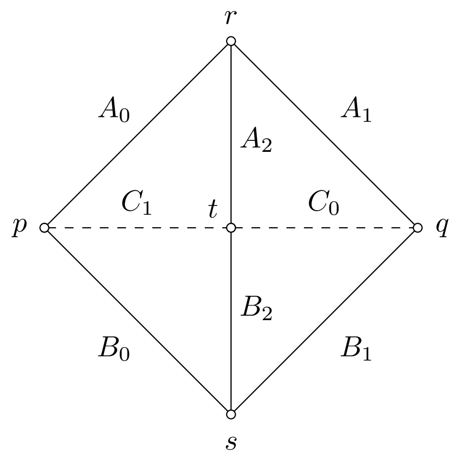


FIGURE 4.3

Freese and Bjarni Jónsson proved that $\mathcal{V}$ is a variety of algebras, all of whose congruence lattices are modular (such as groups or rings), then the congruence lattices of algebras in $\mathcal{V}$ are Arguesian [4].

Mark Haiman has shown that the converse of Theorem 4.6 is false: there are Arguesian lattices that do not have a type 1 representation [5], [6]. In fact, his proof shows that lattices with a type 1 representation must satisfy equations that are strictly stronger than the Arguesian law. It follows, in particular, that the lattice of normal subgroups of a group also satisfies these stronger equations, as do the other types of lattices mentioned in the preceding paragraph. Interestingly, P. P. Pálfy and Laszlo Szabó have shown that subgroup lattices of abelian groups satisfy an equation that does not hold in all normal subgroup lattices [9].

The question remains: *Does there exist a set of equations* Σ *such that a lattice has a type 1 representation if and only if it satisfies all the equations of* Σ*?* Haiman proved that if such a Σ exists, it must contain infinitely many equations. In Chapter 7 we will see that a class of lattices is characterized by a set of equations if and only if it is closed with respect to direct products, sublattices, and homomorphic images. The class of lattices having a type 1 representation is easily seen to be closed under sublattices and direct products, so the question is equivalent to: *Is the class of all lattices having a type 1 representation closed under homomorphic images?*

Exercises for Chapter 4

1. Draw $\mathbf{Eq}\, X$ for $|X| = 3, 4$.
2. Find representations in $\mathbf{Eq}\, X$ for
   (a) $\mathfrak{P}(Y)$, Y a set,
   (b) $\mathcal{N}_5$,

(c) $\mathcal{M}_n$, $n < \infty$.

3. Let $\mathcal{G}$ be a group. Let $F : \mathbf{Sub}\,\mathcal{G} \to \mathbf{Eq}\,G$ be the standard representation by cosets: $F(H) = \{(x, y) \in G^2 : xy^{-1} \in H\}$.

(a) Verify that $F(H)$ is indeed an equivalence relation.
(b) Verify that F is a lattice embedding.
(c) Show that $F(H) \vee F(K) = F(H) \circ F(K)$ iff $HK = KH$ $(= H \vee K)$.
(d) Conclude that the restriction of F to the normal subgroup lattice $\mathcal{N}(\mathcal{G})$ is a type 1 representation.

4. Show that for $R, S \in \mathbf{Eq}\,X$, $R \vee S = R \circ S$ iff $S \circ R \subseteq R \circ S$ iff $R \circ S = S \circ R$. (For this reason, such equivalence relations are said to *permute*.)

5. Recall from Exercise 6 of Chapter 3 that a complete sublattice of an algebraic lattice is algebraic.

(a) Let $\mathcal{S}$ be a join semilattice with 0. Assume that $\varphi : \mathcal{S} \to \mathbf{Eq}\ X$ is a join homomorphism with the properties

(i) for each pair a, $b \in X$ there exists $\sigma(a, b) \in S$ such that $(a, b) \in \varphi(s)$ iff $s \geq \sigma(a, b)$, and
(ii) for each $s \in S$, there exists a pair (x_s, y_s) such that $(x_s, y_s) \in \varphi(t)$ iff $s \leq t$.

Show that φ induces a complete representation $\overline{\varphi} : \mathcal{I}(\mathcal{S}) \to \mathbf{Eq}\,X$.

(b) Indicate how to modify the proof of Theorem 4.1 to obtain, for an arbitrary join semilattice $\mathcal{S}$ with 0, a set X and a join homomorphism $\varphi : \mathcal{S} \to \mathbf{Eq}\ X$ satisfying (i) and (ii).

(c) Conclude that a complete lattice $\mathcal{L}$ has a complete representation by equivalence relations if and only if $\mathcal{L}$ is algebraic.

6. Prove that $\mathbf{Eq}\,X$ is a strongly atomic, semimodular, algebraic lattice.

7. Prove that a lattice with a type 1 representation satisfies the Arguesian inclusion (A').

8. Mimicking the proof of Theorem 4.6, find an 8-variable implication, like the Arguesian law, that holds in every lattice of permuting equivalence relations. (The hard part of Haiman's work was to show that such laws are not a consequence of the Arguesian law, nor of each other as more variables are added.)

References

1. P. Crawley and R. P. Dilworth, *Algebraic Theory of Lattices*, Prentice-Hall, Englewood Cliffs, New Jersey, 1973.
2. R. Dedekind, Supplement XI to P.G.L. Dirichlet, *Vorlesungen über Zahlentheorie*, 1892 ed., F. Vieweg und Sohn, Braunschweig.
3. R. Dedekind, *Über Zerlegungen von Zahlen durch ihre grössten gemeinsamen Teiler*, Festschrift der Herzogl. technische Hochschule zur Naturforscher-Versammlung, Braunschweig (1897), Reprinted in "Gesammelte mathematische Werke", Vol. 2, pp. 103–148, Chelsea, New York, 1968.
4. R. Freese and B. Jónsson, *Congruence modularity implies the Arguesian identity*, Algebra Universalis **6** (1976), 225–228.

5. M. Haiman, *Arguesian lattices which are not linear*, Bull. Amer. Math. Soc. **16** (1987), 121–124.
6. M. Haiman, *Arguesian lattices which are not type*-1, Algebra Universalis **28** (1991), 128–137.
7. B. Jónsson, *On the representation of lattices*, Math. Scand. **1** (1953), 193–206.
8. O. Ore, *Theory of equivalence relations*, Duke Math. J. **9** (1942), 573–627.
9. P. P. Pálfy and Cs. Szabó, *An identity for subgroup lattices of abelian groups*, Algebra Universalis **33** (1995), 191–195.
10. P. Pudlák and J. Tůma, *Every finite lattice can be embedded in the lattice of all equivalences over a finite set*, Algebra Universalis **10** (1980), 74–95.
11. P. Whitman, *Lattices, equivalence relations and subgroups*, Bull. Amer. Math. Soc. **52** (1946), 507–522.

5. Congruence Relations

"You're young, Myrtle Mae. You've got a lot to learn, and I hope you never learn it."
– Vita in "Harvey"

You are doubtless familiar with the connection between homomorphisms and normal subgroups of groups. In this chapter we will establish the corresponding ideas for lattices (and other general algebras). Borrowing notation from group theory, if X is a set and θ an equivalence relation on X, for $x \in X$ let $x\theta$ denote the equivalence class $\{y \in X : x \; \theta \; y\}$, and let

$$X/\theta = \{x\theta : x \in X\}.$$

Thus the elements of X/θ are the equivalence classes of θ.

Recall that if $\mathcal{L}$ and $\mathcal{K}$ are lattices and $h : \mathcal{L} \to \mathcal{K}$ is a homomorphism, then the *kernel* of h is the induced equivalence relation,

$$\ker h = \{(x, y) \in L^2 : h(x) = h(y)\}.$$

We can define lattice operations naturally on the equivalence classes of $\ker h$, *viz.,* if $\theta = \ker h$, then

$$(\S) \qquad \begin{aligned} x\theta \, \vee \, y\theta &= (x \vee y)\theta \\ x\theta \, \wedge \, y\theta &= (x \wedge y)\theta. \end{aligned}$$

The homomorphism property shows that these operations are well defined, for if $(x, y) \in \ker h$ and $(r, s) \in \ker h$, then $h(x \vee r) = h(x) \vee h(r) = h(y) \vee h(s) = h(y \vee s)$, whence $(x \vee r, y \vee s) \in \ker h$. Moreover, $L/\ker h$ with these operations forms an algebra $\mathcal{L}/\ker h$ isomorphic to the image $h(\mathcal{L})$, which is a sublattice of $\mathcal{K}$. Thus $\mathcal{L}/\ker h$ is also a lattice.

Theorem 5.1. First Isomorphism Theorem. *Let $\mathcal{L}$ and $\mathcal{K}$ be lattices, and let $h : \mathcal{L} \to \mathcal{K}$ be a lattice homomorphism. Then $L/\ker h$ with the operations defined by (§) is a lattice $\mathcal{L}/\ker h$, which is isomorphic to the image $h(\mathcal{L})$ of $\mathcal{L}$ in $\mathcal{K}$.*

Let us define a *congruence relation* on a lattice $\mathcal{L}$ to be an equivalence relation θ such that $\theta = \ker h$ for some homomorphism h.[1] We have seen that, in addition to

[1] This is not the standard definition, but we are about to show it is equivalent to it.

being equivalence relations, congruence relations must preserve the operations of $\mathcal{L}$: if θ is a congruence relation, then

$$x\ \theta\ y \text{ and } r\ \theta\ s \text{ implies } x \vee r\ \theta\ y \vee s, \tag{$\dagger$}$$

and analogously for meets. Note that (†) is equivalent for an equivalence relation θ to the apparently weaker, and easier to check, condition

$$x\ \theta\ y \text{ implies } x \vee z\ \theta\ y \vee z. \tag{$\dagger'$}$$

For (†) implies (†′) because every equivalence relation is reflexive, while if θ has the property (†′) and the hypotheses of (†) hold, then applying (†) twice yields $x \vee r\ \theta\ y \vee r\ \theta\ y \vee s$.

We want to show that, conversely, any equivalence relation satisfying (†′) and the corresponding implication for meets is a congruence relation.

Theorem 5.2. *Let $\mathcal{L}$ be a lattice, and let θ be an equivalence relation on L satisfying*

$$\begin{aligned} &x\ \theta\ y \textit{ implies } x \vee z\ \theta\ y \vee z, \\ &x\ \theta\ y \textit{ implies } x \wedge z\ \theta\ y \wedge z. \end{aligned} \tag{$\ddagger$}$$

Define join and meet on L/θ by the formulas (§). Then $\mathcal{L}/\theta = (L/\theta, \wedge, \vee)$ is a lattice, and the map $h : \mathcal{L} \to \mathcal{L}/\theta$ defined by $h(x) = x\theta$ is a surjective homomorphism with $\ker h = \theta$.

Proof. The conditions (‡) ensure that the join and meet operations are well defined on L/θ. By definition, we have

$$h(x \vee y) = (x \vee y)\theta = x\theta \vee y\theta = h(x) \vee h(y)$$

and similarly for meets, so h is a homomorphism. The range of h is clearly L/θ.

It remains to show that $\mathcal{L}/\theta$ satisfies the equations defining lattices. This follows from the general principle that homomorphisms preserve the satisfaction of equations, i.e., if $h : \mathcal{L} \twoheadrightarrow \mathcal{K}$ is a surjective homomorphism and an equation $p = q$ holds in $\mathcal{L}$, then it holds in $\mathcal{K}$. (See Exercise 4.) For example, to check commutativity of meets, let $a, b \in K$. Then there exist $x, y \in L$ such that $h(x) = a$ and $h(y) = b$. Hence

$$\begin{aligned} a \wedge b = h(x) \wedge h(y) &= h(x \wedge y) \\ &= h(y \wedge x) = h(y) \wedge h(x) = b \wedge a. \end{aligned}$$

Similar arguments allow us to verify the commutativity of joins, the idempotence and associativity of both operations, and the absorption laws. Thus a homomorphic image of a lattice is a lattice.[2] As $h : \mathcal{L} \to \mathcal{L}/\theta$ is a surjective homomorphism, we conclude that $\mathcal{L}/\theta$ is a lattice, which completes the proof. $\square$

Thus congruence relations are precisely equivalence relations that satisfy (‡). But the conditions of (‡) and the axioms for an equivalence relation are all finitary closure rules on L^2. Hence, by Theorem 3.1, the set of congruence relations on a lattice $\mathcal{L}$ forms an algebraic lattice $\mathbf{Con}\,\mathcal{L}$. The closure operator on L^2 that gives the congruence generated by a set of pairs is denoted by "con" or sometimes "Cg." So, with the former notation, for a set Q of ordered pairs, con Q is the congruence relation generated by Q; for a single pair, $Q = \{(a, b)\}$, we write just $\mathrm{con}(a, b)$.

Moreover, the equivalence relation join (the transitive closure of the union) of a set of congruence relations again satisfies (‡). For if θ_i $(i \in I)$ are congruence relations and $x\,\theta_{i_1}\,r_1\,\theta_{i_2}\,r_2\,\ldots\,\theta_{i_n}\,y$, then $x \vee z\,\theta_{i_1}\,r_1 \vee z\,\theta_{i_2}\,r_2 \vee z\,\ldots\,\theta_{i_n}\,y \vee z$, and likewise for meets. Thus the transitive closure of $\bigcup_{i\in I} \theta_i$ is a congruence relation, and so it is the join $\bigvee_{i\in I} \theta_i$ in $\mathbf{Con}\,\mathcal{L}$. Since the meet is also the same (set intersection) in both lattices, $\mathbf{Con}\,\mathcal{L}$ is a complete sublattice of $\mathbf{Eq}\,L$.

Theorem 5.3. $\mathbf{Con}\,\mathcal{L}$ *is an algebraic lattice. A congruence relation* θ *is compact in* $\mathbf{Con}\,\mathcal{L}$ *if and only if it is finitely generated, i.e., there exist finitely many pairs* $(a_1, b_1), \ldots, (a_k, b_k)$ *of elements of* L *such that* $\theta = \bigvee_{1\le i\le k} \mathrm{con}(a_i, b_i)$.

Note that the universal relation and the equality relation on L^2 are both congruence relations; they are the greatest and least elements of $\mathbf{Con}\,\mathcal{L}$, respectively. Also, since $x\ \theta\ y$ if and only if $x \wedge y\ \theta\ x \vee y$, a congruence relation is determined by the ordered pairs (a, b) with $a < b$ which it contains.

A subset $S \subseteq \mathcal{L}$ is *convex* if $x \le y \le z$ and $x,\, z \in S$ implies $y \in S$. The reader should verify that *if* θ *is a congruence relation on a lattice* $\mathcal{L}$*, then every congruence class is a convex sublattice of* $\mathcal{L}$*.* This observation helps immensely in computing lattice congruences.

A congruence relation θ is *principal* if $\theta = \mathrm{con}(a, b)$ for some pair $a,\, b \in L$. The principal congruence relations are join dense in $\mathbf{Con}\,\mathcal{L}$: for any congruence relation θ, we have

$$\theta = \bigvee \{\mathrm{con}(a, b) : a\ \theta\ b\}.$$

It follows from the general theory of algebraic closure operators that principal congruence relations are compact, but this can be shown directly as follows: if $\mathrm{con}(a, b) \le \bigvee_{i\in I} \theta_i$, then there exist elements $c_1, \ldots, c_m$ and indices $i_0, \ldots, i_m$ such that

$$a\ \theta_{i_0}\ c_1\ \theta_{i_1}\ c_2 \ldots \theta_{i_m}\ b\ ,$$

whence $(a, b) \in \theta_{i_0} \vee \ldots \vee \theta_{i_m}$ and thus $\mathrm{con}(a, b) \le \bigvee_{0\le j\le m} \theta_{i_j}$.

One of the most basic facts about congruences says that congruences of $\mathcal{L}/\theta$ correspond to congruences on $\mathcal{L}$ containing θ.

[2]The corresponding statement is true for any equationally defined class of algebras, including modular, Arguesian and distributive lattices.

Theorem 5.4. Second Isomorphism Theorem. *If $\theta \in \mathbf{Con}\,\mathcal{L}$, then $\mathbf{Con}\,(\mathcal{L}/\theta)$ is isomorphic to the filter $\uparrow\theta$ in $\mathbf{Con}\,\mathcal{L}$, i.e., $\mathbf{Con}\,(\mathcal{L}/\theta) \cong \{\varphi \in \mathbf{Con}\,\mathcal{L} : \varphi \geq \theta\}$.*

Proof. A congruence relation on $\mathcal{L}/\theta$ is an equivalence relation R on the θ-classes of L such that

$$x\theta \; R \; y\theta \quad \text{implies} \quad x\theta \vee z\theta \; R \; y\theta \vee z\theta$$

and analogously for meets. Given $R \in \mathbf{Con}\,\mathcal{L}/\theta$, define the corresponding relation ρ on L by $x\,\rho\,y$ iff $x\theta \; R \; y\theta$. Clearly $\rho \in \mathbf{Eq}\;L$ and $\theta \leq \rho$. Moreover, if $x\,\rho\,y$ and $z \in L$, then

$$(x \vee z)\theta \;=\; x\theta \vee z\theta \; R \; y\theta \vee z\theta \;=\; (y \vee z)\theta,$$

whence $x \vee z \;\rho\; y \vee z$, and similarly for meets. Hence $\rho \in \mathbf{Con}\,\mathcal{L}$, and we have established an order preserving map $f : \mathbf{Con}\,\mathcal{L}/\theta \to \uparrow\theta$.

Conversely, let $\sigma \in \uparrow\theta$ in $\mathbf{Con}\,\mathcal{L}$, and define a relation S on L/θ by $x\theta \; S \; y\theta$ iff $x\,\sigma\,y$. Since $\theta \leq \sigma$ the relation S is well defined. If $x\theta \; S \; y\theta$ and $z \in L$, then $x\,\sigma\,y$ implies $x \vee z\,\sigma\,y \vee z$, whence

$$x\theta \vee z\theta \;=\; (x \vee z)\theta \; S \; (y \vee z)\theta \;=\; y\theta \vee z\theta,$$

and likewise for meets. Thus S is a congruence relation on $\mathcal{L}/\theta$. This gives us an order preserving map $g : \uparrow\theta \to \mathbf{Con}\,\mathcal{L}/\theta$.

The definitions make f and g inverse maps, so they are in fact isomorphisms. □

It is interesting to interpret Theorem 5.4 in terms of homomorphisms. Essentially it corresponds to the fact that *if $h : \mathcal{L} \twoheadrightarrow \mathcal{K}$ and $f : \mathcal{L} \to \mathcal{M}$ are homomorphisms with h surjective, then there is a homomorphism $g : \mathcal{K} \to \mathcal{M}$ with $f = gh$ if and only if* $\ker h \;\leq\; \ker f$. This version of the Second Isomorphism Theorem will be used repeatedly in Chapters 6 and 7.

A lattice $\mathcal{L}$ is called *simple* if $\mathbf{Con}\;\mathcal{L}$ is a two element chain, i.e., $|L| > 1$ and $\mathcal{L}$ has no congruences except equality and the universal relation. For example, the two-dimensional modular lattice $\mathcal{M}_n$ is simple whenever $n \geq 3$. A lattice is *subdirectly irreducible* if it has a unique minimum nonzero congruence relation, i.e., if 0 is completely meet irreducible in $\mathbf{Con}\,\mathcal{L}$. So every simple lattice is subdirectly irreducible, and $\mathcal{N}_5$ is an example of a subdirectly irreducible lattice that is not simple .

The following are immediate consequences of the Second Isomorphism Theorem.

Corollary. *$\mathcal{L}/\theta$ is simple if and only if $1 \succ \theta$ in $\mathbf{Con}\,\mathcal{L}$.*

Corollary. *$\mathcal{L}/\theta$ is subdirectly irreducible if and only if θ is completely meet irreducible in $\mathbf{Con}\,\mathcal{L}$.*

Now we turn our attention to a decomposition of lattices which goes back to R. Remak in 1930 (for groups) [10]. In what follows, it is important to remember that the zero element of a congruence lattice is the equality relation.

Theorem 5.5. *If* $0 = \bigwedge_{i \in I} \theta_i$ *in* $\mathbf{Con}\,\mathcal{L}$*, then* $\mathcal{L}$ *is isomorphic to a sublattice of the direct product* $\prod_{i \in I} \mathcal{L}/\theta_i$*, and each of the natural homomorphisms* $\pi_i : \mathcal{L} \to \mathcal{L}/\theta_i$ *is surjective.*

Conversely, if $\mathcal{L}$ *is isomorphic to a sublattice of a direct product* $\prod_{i \in I} \mathcal{K}_i$ *and each of the projection homomorphisms* $\pi_i : \mathcal{L} \to \mathcal{K}_i$ *is surjective, then* $\mathcal{K}_i \cong \mathcal{L}/\ker \pi_i$ *and* $\bigwedge_{i \in I} \ker \pi_i = 0$ *in* $\mathbf{Con}\,\mathcal{L}$*.*

Proof. For any collection θ_i $(i \in I)$ in $\mathbf{Con}\,\mathcal{L}$, there is a natural homomorphism $\pi : \mathcal{L} \to \prod \mathcal{L}/\theta_i$ with $(\pi(x))_i = x\theta_i$. Since two elements of a direct product are equal if and only if they agree in every component, $\ker \pi = \bigwedge \theta_i$. So if $\bigwedge \theta_i = 0$, then π is an embedding.

Conversely, if $\pi : \mathcal{L} \to \prod \mathcal{K}_i$ is an embedding, then $\ker \pi = 0$, while as above $\ker \pi = \bigwedge \ker \pi_i$. Clearly, if $\pi_i(\mathcal{L}) = \mathcal{K}_i$ then $\mathcal{K}_i \cong \mathcal{L}/\ker \pi_i$. $\square$

A representation of $\mathcal{L}$ satisfying either of the equivalent conditions of Theorem 5.5 is called a *subdirect decomposition*, and the corresponding external construction is called a *subdirect product*. For example, Figure 5.1 shows how a six element lattice $\mathcal{L}$ can be written as a subdirect product of two copies of $\mathcal{N}_5$.

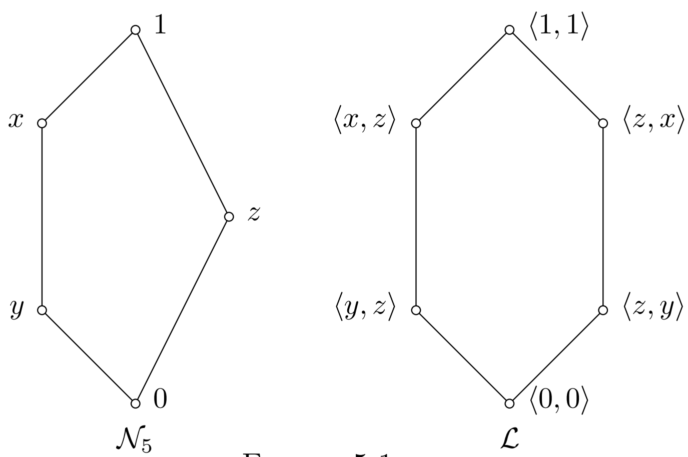


FIGURE 5.1

Next we should show that subdirectly irreducible lattices are indeed those that have no proper subdirect decomposition.

Theorem 5.6. *The following are equivalent for a lattice* $\mathcal{L}$*.*

(1) $\mathcal{L}$ *is subdirectly irreducible, i.e.,* 0 *is completely meet irreducible in* $\mathbf{Con}\,\mathcal{L}$*.*
(2) *There is a unique minimal nonzero congruence* μ *on* $\mathcal{L}$ *with the property that* $\theta \geq \mu$ *for every nonzero* $\theta \in \mathbf{Con}\,\mathcal{L}$*.*
(3) *If* $\mathcal{L}$ *is isomorphic to a sublattice of* $\prod \mathcal{K}_i$*, then some projection homomorphism* π_i *is one-to-one.*
(4) *There exists a pair of elements* $a < b$ *in* $\mathcal{L}$ *such that* $a \mathrel{\theta} b$ *for every nonzero congruence* θ*.*

The congruence μ of condition (2) is called the *monolith* of the subdirectly irreducible lattice $\mathcal{L}$, and the pair (a, b) of condition (4), which need not be unique, is called a *critical pair.*

Proof. The equivalence of (1), (2) and (3) is a simple combination of Theorems 3.8 and 5.5. We get (2) implies (4) by taking $a = x \wedge y$ and $b = x \vee y$ for any pair of distinct elements with $x \, \mu \, y$. On the other hand, if (4) holds we obtain (2) with $\mu = \mathrm{con}(a, b)$. $\square$

Now we see the beauty of Birkhoff's Theorem 3.9, that every element in an algebraic lattice is a meet of completely meet irreducible elements. By applying this to the zero element of **Con** $\mathcal{L}$, we obtain the following fundamental result.

Theorem 5.7. *Every lattice is a subdirect product of subdirectly irreducible lattices.*

It should be clear that, with the appropriate modifications, Theorems 5.5 to 5.7 yield subdirect decompositions of groups, rings, semilattices, etc. into subdirectly irreducible algebras of the same type. Keith Kearnes [8] has shown that there are interesting varieties of algebras whose congruence lattices are strongly atomic. By Theorem 3.10, these algebras have irredundant subdirect decompositions.

Subdirectly irreducible lattices play a particularly important role in the study of varieties; see Chapter 7.

So far we have just done universal algebra with lattices: with the appropriate modifications, we can characterize congruence relations and show that **Con** $\mathcal{A}$ is an algebraic lattice for any algebra $\mathcal{A}$. (See Exercises 10 and 11.) However, the next property is special to lattices and related structures. It was first discovered by N. Funayama and T. Nakayama [5] in the early 1940's.

Theorem 5.8. *If* $\mathcal{L}$ *is a lattice, then* **Con** $\mathcal{L}$ *is a distributive algebraic lattice.*

Proof. In any lattice $\mathcal{L}$, let

$$m(x, y, z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z).$$

Then it is easy to see that $m(x, y, z)$ is a *majority polynomial*, in that if any two variables are equal then $m(x, y, z)$ takes on that value:

$$\begin{aligned} m(x, x, z) &= x \\ m(x, y, x) &= x \\ m(x, z, z) &= z. \end{aligned}$$

Now let $\alpha, \beta, \gamma \in \textbf{Con } \mathcal{L}$. Clearly $(\alpha \wedge \beta) \vee (\alpha \wedge \gamma) \leq \alpha \wedge (\beta \vee \gamma)$. To show the reverse inclusion, let $(x, z) \in \alpha \wedge (\beta \vee \gamma)$. Then $x \, \alpha \, z$ and there exist $y_1, \ldots, y_k$ such that

$$x = y_0 \; \beta \; y_1 \; \gamma \; y_2 \; \beta \ldots y_k = z \, .$$

Let $t_i = m(x, y_i, z)$ for $0 \le i \le k$. Then

$$t_0 = m(x, x, z) = x$$
$$t_k = m(x, z, z) = z$$

and for all i,

$$t_i = m(x, y_i, z) \; \alpha \; m(x, y_i, x) = x \; ,$$

so $t_i \, \alpha \, t_{i+1}$ by Exercise 4(b). If i is even, then

$$t_i = m(x, y_i, z) \; \beta \; m(x, y_{i+1}, z) = t_{i+1} \; ,$$

whence $t_i \; \alpha \wedge \beta \; t_{i+1}$. Similarly, if i is odd then $t_i \; \alpha \wedge \gamma \; t_{i+1}$. Thus

$$x = t_0 \; \alpha \wedge \beta \; t_1 \; \alpha \wedge \gamma \; t_2 \; \alpha \wedge \beta \ldots t_k = z$$

and we have shown that $\alpha \wedge (\beta \vee \gamma) \le (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$. As inclusion holds both ways, we have equality. Therefore **Con** $\mathcal{L}$ is distributive. $\square$

In the 1940's, R.P. Dilworth proved that every finite distributive lattice is isomorphic to the congruence lattice of a lattice. (This result appeared as a (starred) exercise in the 1948 edition of Birkhoff's *Lattice Theory* book.) For a long time thereafter, it was conjectured that every distributive algebraic lattice was the congruence lattice of a lattice, and evidence in favor of the conjecture was amassed. A distributive algebraic lattice $\mathcal{D}$ is isomorphic to the congruence lattice of a lattice if

(i) $\mathcal{D} \cong \mathcal{O}(\mathcal{P})$ for some ordered set $\mathcal{P}$ (R. P. Dilworth, see [6]), or
(ii) the compact elements are a sublattice of $\mathcal{D}$ (E. T. Schmidt [12]), or
(iii) $\mathcal{D}$ has at most $\aleph_1$ compact elements (A. Huhn [7]).

In Chapter 10 we will prove (i), which includes the fact that every finite distributive lattice is isomorphic to the congruence lattice of a (finite) lattice.

But in 2005, Fred Wehrung constructed distributive algebraic lattices that are not isomorphic to congruence lattices of lattices [15]. Wehrung's original counterexamples have $\aleph_{\omega+1}$ or more compact elements, but Pavel Růžička refined Wehrung's arguments to produce a counterexample with $\aleph_2$ compact elements [11].

This completely settles the problem for lattices, but it remains an open question whether every distributive algebraic lattice is isomorphic to the congruence lattice of an algebra with finitely many operations. Surveys on this problem, but pre-dating Wehrung's results, can be found in M. Tischendorf [13] and M. Ploščica, J. Tůma and F. Wehrung [9], [15].

We need to understand the congruence operator $\operatorname{con} Q$, where Q is a set of pairs, a little better. A *weaving polynomial* on a lattice $\mathcal{L}$ is a member of the set W of unary functions defined recursively by

(1) $w(x) = x \in W$,
(2) if $w(x) \in W$ and $a \in L$, then $u(x) = w(x) \wedge a$ and $v(x) = w(x) \vee a$ are in W,
(3) only these functions are in W.

Thus every weaving polynomial looks something like

$$w(x) = (\dots(((x \wedge s_1) \vee s_2) \wedge s_3) \dots) \vee s_k$$

where $s_i \in L$ for $1 \leq i \leq k$. The following characterization is a modified version of one found in Dilworth [2].

Theorem 5.9. *Suppose $a_i < b_i$ for $i \in I$. Then $(x, y) \in \bigvee_{i \in I} \mathrm{con}(a_i, b_i)$ if and only if there exist finitely many $r_j \in L$, $w_j \in W$, and $i_j \in I$ such that*

$$x \vee y = r_0 \geq r_1 \geq \cdots \geq r_k = x \wedge y$$

with $w_j(b_{i_j}) = r_j$ and $w_j(a_{i_j}) = r_{j+1}$ for $0 \leq j < k$.

Proof. Let R be the set of all pairs (x, y) satisfying the condition of the theorem. It is clear that

(1) $(a_i, b_i) \in R$ for all i,
(2) $R \subseteq \bigvee_{i \in I} \mathrm{con}(a_i, b_i)$.

Hence, if we can show that R is a congruence relation, it will follow that $R = \bigvee_{i \in I} \mathrm{con}(a_i, b_i)$.

Note that $(x, y) \in R$ if and only if $(x \wedge y, x \vee y) \in R$. It also helps to observe that if $x \, R \, y$ and $x \leq u \leq v \leq y$, then $u \, R \, v$. To see this, replace the weaving polynomials $w(t)$ witnessing $x \, R \, y$ by new polynomials $w'(t) = (w(t) \vee u) \wedge v$.

First we must show $R \in \mathbf{Eq}\ L$. Reflexivity and symmetry are obvious, so let $x \, R \, y \, R \, z$ with

$$x \vee y = r_0 \geq r_1 \geq \cdots \geq r_k = x \wedge y$$

using polynomials $w_j \in W$, and

$$y \vee z = s_0 \geq s_1 \geq \cdots \geq s_m = y \wedge z$$

via polynomials $v_j \in W$, as in the statement of the theorem. Replacing $w_j(t)$ by $w'_j(t) = w_j(t) \vee y \vee z$, we obtain

$$x \vee y \vee z = r_0 \vee y \vee z \geq r_1 \vee y \vee z \geq \cdots \geq (x \wedge y) \vee y \vee z = y \vee z.$$

Likewise, replacing $w_j(t)$ by $w''_j(t) = w_j(t) \wedge y \wedge z$, we have

$$y \wedge z = (x \vee y) \wedge y \wedge z \geq r_1 \wedge y \wedge z \geq \cdots \geq r_k \wedge y \wedge z = x \wedge y \wedge z.$$

Combining the two new sequences with the original one for $y \, R \, z$, we get a sequence from $x \vee y \vee z$ down to $x \wedge y \wedge z$. Hence $x \wedge y \wedge z \ R \ x \vee y \vee z$. By the observations above, $x \wedge z \ R \ x \vee z$ and $x \, R \, z$, so R is transitive.

Now we must check (‡). Let $x \, R \, y$ as before, and let $z \in L$. Replacing $w_j(t)$ by $u_j(t) = w_j(t) \vee z$, we obtain a sequence from $x \vee y \vee z$ down to $(x \wedge y) \vee z$. Thus $(x \wedge y) \vee z \ R \ x \vee y \vee z$, and since $(x \wedge y) \vee z \leq (x \vee z) \wedge (y \vee z) \leq x \vee y \vee z$, this implies $x \vee z \ R \ y \vee z$. The argument for meets is done similarly, and we conclude that R is a congruence relation, as desired. □

The condition of Theorem 5.9 is a bit unwieldy, but not as bad to use as you might think. Let us look at some consequences of the theorem.

Corollary. *If $\theta_i \in \mathbf{Con}\,\mathcal{L}$ for $i \in I$, then $(x, y) \in \bigvee_{i \in I} \theta_i$ if and only if there exist finitely many $r_j \in L$ and $i_j \in I$ such that*

$$x \vee y = r_0 \geq r_1 \geq \cdots \geq r_k = x \wedge y$$

and $r_j \; \theta_{i_j} \; r_{j+1}$ for $0 \leq j < k$.

At this point we need some basic facts about distributive algebraic lattices (like $\mathbf{Con}\,\mathcal{L}$). Recall that an element p of a complete lattice is *completely join irreducible* if $p = \bigvee Q$ implies $p = q$ for some $q \in Q$. An element p is *completely join prime* if $p \leq \bigvee Q$ implies $p \leq q$ for some $q \in Q$. Clearly every completely join prime element is completely join irreducible, but in general completely join irreducible elements need not be join prime.

Now every algebraic lattice has lots of completely meet irreducible elements (by Theorem 3.9), but they may have no completely join irreducible elements. This happens, for example, in the lattice consisting of the empty set and all cofinite subsets of an infinite set (which is distributive and algebraic). However, such completely join irreducible elements as there are in a distributive algebraic lattice are completely join prime!

Theorem 5.10. *The following are equivalent for an element p in an algebraic distributive lattice.*

(1) *p is completely join prime.*
(2) *p is completely join irreducible.*
(3) *p is compact and (finitely) join irreducible.*

Proof. Clearly (1) implies (2), and since every element in an algebraic lattice is a join of compact elements, (2) implies (3).

Let p be compact and finitely join irreducible, and assume $p \leq \bigvee Q$. As p is compact, $p \leq \bigvee F$ for some finite subset $F \subseteq Q$. By distributivity, this implies $p = p \wedge (\bigvee F) = \bigvee_{q \in F} p \wedge q$. Since p is join irreducible, $p = p \wedge q \leq q$ for some $q \in F$. Thus p is completely join prime. (Cf. Exercise 3.1) $\square$

We will return to the theory of distributive lattices in Chapter 8, but let us now apply what we know to $\mathbf{Con}\,\mathcal{L}$. As an immediate consequence of the Corollary to Theorem 5.9 we have the following.

Theorem 5.11. *If $a \prec b$, then $\mathrm{con}(a, b)$ is completely join prime in $\mathbf{Con}\,\mathcal{L}$.*

The converse is false, as there are infinite simple lattices with no covering relations (E. T. Schmidt). However, for finite lattices, or more generally principally chain finite lattices, the converse does hold. A lattice is *principally chain finite* if every principal ideal $\downarrow c$ satisfies the ACC and DCC. This is a fairly natural finiteness condition that includes many interesting infinite lattices, and many results for finite lattices can be extended to principally chain finite lattices with a minimum of effort. Recall that if x is a join irreducible element in such a lattice, then x_* denotes the unique element such that $x \succ x_*$.

Theorem 5.12. *Let $\mathcal{L}$ be a principally chain finite lattice. Then every congruence relation on $\mathcal{L}$ is the join of completely join irreducible congruences. Moreover, every completely join irreducible congruence is of the form* $\operatorname{con}(x, x_*)$ *for some join irreducible element x of $\mathcal{L}$.*

Proof. Every congruence relation is a join of compact congruences, and every compact congruence is a join of finitely many congruences $\operatorname{con}(a, b)$ with $a > b$. In a principally chain finite lattice, every chain in a/b is finite by Exercise 1.5, so there exists a covering chain $a = r_0 \succ r_1 \succ \cdots \succ r_k = b$. Clearly $\operatorname{con}(a, b) = \bigvee_{0 \leq j < k} \operatorname{con}(r_j, r_{j+1})$, and these latter are completely join prime by Theorem 5.11. Thus every congruence relation on $\mathcal{L}$ is the join of completely join irreducible congruences $\operatorname{con}(r, s)$ with $r \succ s$.

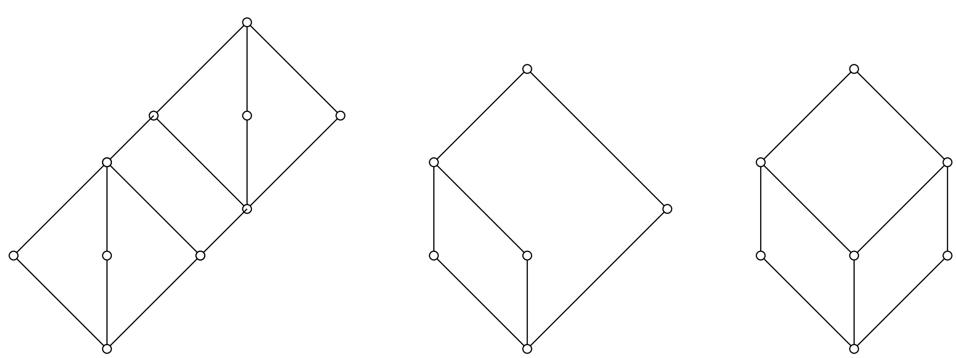
Now let $a \succ b$ be any covering pair in $\mathcal{L}$. By the DCC for $\downarrow a$, there is an element x that is minimal with respect to the properties $x \leq a$ and $x \not\leq b$. Since any element strictly below x is below b, the element x is join irreducible and $x_* = x \wedge b$. It is also true that $a = x \vee b$, since $b < x \vee b \leq a$, and it follows easily from these two facts that $\operatorname{con}(a, b) = \operatorname{con}(x, x_*)$. □

There is much more to be said about congruence lattices of finite lattices, or more generally, principally chain finite lattices. We will return to these matters in Chapter 10. See also the references there.

We have ignored congruence lattices of semilattices, interesting on their own and applicable in universal algebra. Unlike congruence lattices of lattices, which are distributive, congruence lattices of semilattices satisfy no lattice identities. For the basic results, see Freese and Nation [4], Fajtlowicz and Schmidt [3], and Adaricheva [1].

Exercises for Chapter 5

1. Find $\mathbf{Con}\,\mathcal{L}$ for the lattices (a) $\mathcal{M}_n$ where $n \geq 3$, (b) $\mathcal{N}_5$, (c) the lattice $\mathcal{L}$ of Figure 5.1, and the lattices in Figure 5.2.



(d) (e) (f)

Figure 5.2

2. An element p of a lattice $\mathcal{L}$ is *join prime* if for any finite subset F of L, $p \leq \bigvee F$ implies $p \leq f$ for some $f \in F$. Let $\mathrm{P}(\mathcal{L})$ denote the set of join prime elements of $\mathcal{L}$, and define

$$x \,\Delta\, y \qquad \text{iff} \qquad {\downarrow}x \cap \mathrm{P}(\mathcal{L}) = {\downarrow}y \cap \mathrm{P}(\mathcal{L}).$$

Prove that Δ is a congruence relation on $\mathcal{L}$.

3. Let X be any set. Define a binary relation on $\mathfrak{P}(X)$ by $A \approx B$ iff the symmetric difference $(A-B)\cup(B-A)$ is finite. Prove that $\approx$ is a congruence relation on $\mathfrak{P}(X)$.

4. Lattice *terms* are defined in the proof of Theorem 6.1.

(a) Show that if $p(x_1, \ldots, x_n)$ is a lattice term and $h : \mathcal{L} \to \mathcal{K}$ is a homomorphism, then $h(p(a_1, \ldots, a_n)) = p(h(a_1), \ldots, h(a_n))$ for all $a_1, \ldots, a_n \in L$.

(b) Show that if $p(x_1, \ldots, x_n)$ is a lattice term and $\theta \in \mathbf{Con}\,\mathcal{L}$ and $a_i \;\theta\; b_i$ for $1 \leq i \leq n$, then $p(a_1, \ldots, a_n) \;\theta\; p(b_1, \ldots, b_n)$.

(c) Let $p(x_1, \ldots, x_n)$ and $q(x_1, \ldots, x_n)$ be lattice terms, and let $h : \mathcal{L} \twoheadrightarrow \mathcal{K}$ be a surjective homomorphism. Prove that if $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$ for all $a_1, \ldots, a_n \in L$, then $p(c_1, \ldots, c_n) = q(c_1, \ldots, c_n)$ holds for all $c_1, \ldots, c_n \in K$.

5. Show that each element of a finite distributive lattice has a unique irredundant decomposition. What does this say about subdirect decompositions of finite lattices?

6. Let $\theta \in \mathbf{Con}\,\mathcal{L}$.

(a) Show that $x \succ y$ implies $x\theta \succ y\theta$ or $x\theta = y\theta$.

(b) Prove that if $\mathcal{L}$ is a finite semimodular lattice, then so is $\mathcal{L}/\theta$.

(c) Prove that a subdirect product of semimodular lattices is semimodular.

7. Let $\mathcal{L}$ be a finitely generated lattice, and let θ be a congruence on $\mathcal{L}$ such that $\mathcal{L}/\theta$ is finite. Prove that θ is compact.

8. Prove that $\mathbf{Con}\,\mathcal{L}_1 \times \mathcal{L}_2 \;\cong\; \mathbf{Con}\,\mathcal{L}_1 \times \mathbf{Con}\,\mathcal{L}_2$. (Note that this is not true for groups; see Exercise 9.)

9. Find the congruence lattice of the abelian group $Z_p \times Z_p$, where p is prime. Find all finite abelian groups whose congruence lattice is distributive. (Recall that the congruence lattice of an abelian group is isomorphic to its subgroup lattice.)

For Exercises 10 and 11 we refer to §3 (Universal Algebra) of Appendix 1.

10. Let $\mathcal{A} = \langle A; \mathcal{F}, \mathcal{C}\rangle$ be an algebra.

(a) Prove that if $h : \mathcal{A} \to \mathcal{B}$ is a homomorphism and $\theta = \ker h$, then for each $f \in \mathcal{F}$,

$$(\yen) \qquad x_i \,\theta\, y_i \text{ for } 1 \leq i \leq n \quad \text{implies} \quad f(x_1, \ldots, x_n) \,\theta\, f(y_1, \ldots, y_n).$$

(b) Prove that (¥) is equivalent to the apparently weaker condition that for all $f \in \mathcal{F}$ and every i,

$$(\$) \qquad x_i \,\theta\, y \quad \text{implies} \quad f(x_1, \ldots, x_i, \ldots x_n) \,\theta\, f(x_1, \ldots, y, \ldots x_n).$$

(c) Show that if $\theta \in \mathbf{Eq}\,A$ satisfies (¥), then the natural map $h : \mathcal{A} \to \mathcal{A}/\theta$ is a homomorphism with $\theta = \ker h$.

Thus congruence relations, defined as homomorphism kernels, are precisely equivalence relations satisfying (¥).

11. Accordingly, let $\mathbf{Con}\,\mathcal{A} = \{\theta \in \mathbf{Eq}\,A : \theta$ satisfies (¥)$\}$.

(a) Prove that $\mathbf{Con}\,\mathcal{A}$ is a complete sublattice of $\mathbf{Eq}\,A$. (In particular, you must show that $\bigvee$ and $\bigwedge$ are the same in both lattices.)

(b) Show that $\mathbf{Con}\,\mathcal{A}$ is an algebraic lattice.

12. Let $\mathcal{A} = \mathcal{B} \times \mathcal{C}$ be a direct product of two algebras. Let π_1 and π_2 denote the kernels of the projections onto $\mathcal{B}$ and $\mathcal{C}$. Prove that:

(i) $\mathcal{A}/\pi_1 \cong \mathcal{B}$ and $\mathcal{A}/\pi_2 \cong \mathcal{C}$.

(ii) In $\mathbf{Con}\,\mathcal{A}$, $\pi_1 \wedge \pi_2 = 0$ and $\pi_1 \vee \pi_2 = \pi_1 \circ \pi_2 = \pi_2 \circ \pi_1 = 1$.

Conversely, let $\mathcal{A}$ be an algebra with congruences φ_1 and φ_2 satisfying the analogues of the properties in (ii). Prove that $\mathcal{A} \cong \mathcal{A}/\varphi_1 \times \mathcal{A}/\varphi_2$.

References

1. K. V. Adaricheva, *A characterization of congruence lattices of finite semilattices*, Algebra i Logika **35** (1996), 3–30.
2. R. P. Dilworth, *The structure of relatively complemented lattices*, Ann. of Math. **51** (1950), 348–359.
3. S. Fajtlowicz and J. Schmidt, *Bézout families, join-congruences and meet-irreducible ideals*, Lattice Theory (Proc. Colloq., Szeged, 1974),Colloq. Math. Soc. Janos Bolyai, Vol. 14, North Holland, Amsterdam, 1976, pp. 51–76.
4. R. Freese and J. B. Nation, *Congruence lattices of semilattices*, Pacific J. Math. **49** (1973), 51–58.
5. N. Funayama and T. Nakayama, *On the distributivity of a lattice of lattice-congruences*, Proc. Imp. Acad. Tokyo **18** (1942), 553–554.
6. G. Grätzer and E. T. Schmidt, *On congruence lattices of lattices*, Acta Math. Acad. Sci. Hungar. **13** (1962), 179–185.
7. A. Huhn, *On the representation of distributive algebraic lattices I–III*, Acta Sci. Math. (Szeged), **45** (1983), 239–246; **53** (1989), 3–10 and 11–18.
8. K. A. Kearnes, *Atomicity and Nilpotence*, Canadian J. Math. **42** (1990), 1–18.
9. M. Ploščica, J. Tůma and F. Wehrung, *Congruence lattices of free lattices in nondistributive varieties*, Coll. Math. **76** (1998), 269–278.
10. R. Remak, *Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produckte*, Jour. für Math. **163** (1930), 1–44.
11. P. Růžička, *Free trees and the optimal bound in Wehrung's theorem*, Fund. Math. **198** (2008), 217–228.
12. E. T. Schmidt, *The ideal lattice of a distributive lattice with* 0 *is the congruence lattice of a lattice*, Acta Sci. Math. (Szeged). **43** (1981), 153–168.
13. M. Tischendorf, *On the representation of distributive semilattices*, Algebra Universalis **31** (1994), 446-455.
14. J. Tůma and F. Wehrung, *A survey on recent results on congruence lattices of lattices*, Algebra Universalis **45** (2002), 439-471.
15. F. Wehrung, *A solution to Dilworth's congruence lattice problem*, Adv. Math. **216** (2007), 610–625.

6. Free Lattices

Freedom's just another word for nothing left to lose ....
–Kris Kristofferson

If x, y and z are elements of a lattice, then $x \vee (y \vee (x \wedge z)) = x \vee y$ is always true, while $x \vee y = z$ is usually not true. *Is there an algorithm that, given two lattice expressions p and q, determines whether $p = q$ holds for every substitution of the variables in every lattice?* The answer is yes, and finding this algorithm (Corollary to Theorem 6.2) is our original motivation for studying free lattices.

We say that a lattice $\mathcal{L}$ is *generated* by a set $X \subseteq L$ if no proper sublattice of $\mathcal{L}$ contains X. In terms of the subalgebra closure operator Sg introduced in Chapter 3, this means $\mathrm{Sg}(X) = \mathcal{L}$.

A lattice $\mathcal{F}$ is *freely generated by X* if

(I) $\mathcal{F}$ is a lattice,
(II) X generates $\mathcal{F}$,
(III) for every lattice $\mathcal{L}$, every map $h_0 : X \to L$ can be extended to a homomorphism $h : \mathcal{F} \to \mathcal{L}$.

A *free lattice* is a lattice that is freely generated by one of its subsets.

Condition (I) is sort of redundant, but we include it because it is important when constructing a free lattice to be sure that the algebra constructed is indeed a lattice. In the presence of condition (II), there is only one way to define the homomorphism h in condition (III): for example, if $x, y, z \in X$ then we must have $h(x \vee (y \wedge z)) = h_0(x) \vee (h_0(y) \wedge h_0(z))$. Condition (III) really says that this natural extension is well defined. This in turn says that the only time two lattice terms in the variables X are equal in $\mathcal{F}$ is when they are equal in every lattice.

Now the class of lattices is an *equational class*, i.e., it is the class of all algebras with a fixed set of operation symbols ($\vee$ and $\wedge$) satisfying a given set of equations (the idempotent, commutative, associative and absorption laws). Equational classes are also known as *varieties*, and in Chapter 7 we will take a closer look at varieties of lattices. A fundamental theorem of universal algebra, due to Garrett Birkhoff [3], says that given any nontrivial[1] equational class $\mathbf{V}$ and any set X, there is an algebra in $\mathbf{V}$ freely generated by X. Thus the existence of free groups, free semilattices, and in particular free lattices is guaranteed.[2] Likewise, there are free distributive

[1]A variety $\mathbf{T}$ is *trivial* if it satisfies the equation $x \approx y$, which means that every algebra in $\mathbf{T}$ has exactly one element. This is of course the smallest variety of any type.

[2]However, there is no free lunch.

lattices, free modular lattices, and free Arguesian lattices, since each of these laws can be written as a lattice equation.

Theorem 6.1. *For any nonempty set X, there exists a free lattice generated by X.*

The proof uses three basic principles of universal algebra. The principles correspond for lattices to Theorems 5.1, 5.4, and 5.5 respectively. However, the proofs of these theorems involved nothing special to lattices except the operation symbols $\wedge$ and $\vee$, which can easily be changed to arbitrary operation symbols. Thus, with only minor modification, the proof of this theorem can be adapted to show the existence of free algebras in any nontrivial equational class of algebras.

Basic Principle 1. If $h : \mathcal{A} \twoheadrightarrow \mathcal{B}$ is a surjective homomorphism, then $\mathcal{B} \cong \mathcal{A}/\ker h$.

Basic Principle 2. If $f : \mathcal{A} \to \mathcal{B}$ and $g : \mathcal{A} \twoheadrightarrow \mathcal{C}$ are homomorphism with g surjective, and $\ker g \leq \ker f$, then there exists $h : C \to B$ such that $f = hg$.

$$\begin{tikzcd} \mathcal{A} \arrow[rr, "f"] \arrow[dr, two heads, "g"'] & & \mathcal{B} \\ & \mathcal{C} \arrow[ur, dashed, "h"'] & \end{tikzcd}$$

FIGURE 6.1

Basic Principle 3. If $\psi = \bigwedge_{i \in I} \theta_i$ in **Con** $\mathcal{A}$, then $\mathcal{A}/\psi$ is isomorphic to a subalgebra of the direct product $\Pi_{i \in I} \mathcal{A}/\theta_i$.

With these principles in hand, we proceed with the proof of Theorem 6.1.

Proof of Theorem 6.1. Given the set X, define the *word algebra* $W(X)$ to be the set of all formal expressions (strings of symbols) satisfying the following properties:

(1) $X \subseteq W(X)$,
(2) if $p, q \in W(X)$, then $(p \vee q)$ and $(p \wedge q)$ are in $W(X)$,
(3) only the expressions given by the first two rules are in $W(X)$.

Thus $W(X)$ is the absolutely free algebra with operation symbols $\vee$ and $\wedge$ generated by X. The elements of $W(X)$, which are called *terms*, are all well-formed expressions in the variables X and the operation symbols $\wedge$ and $\vee$. Clearly $W(X)$ is an algebra generated by X, which is property (II) from the definition of a free lattice. Because two terms are equal if and only if they are identical, $W(X)$ has the mapping property (III). On the other hand, it is definitely not a lattice. We need to identify those pairs $p, q \in W(X)$ that evaluate the same in every lattice, e.g., x and $(x \wedge (x \vee y))$. The point of the proof is that when this is done, properties (II) and (III) still hold.

Let $\Lambda = \{\theta \in \textbf{Con } W(X) : W(X)/\theta \text{ is a lattice}\}$, and let $\lambda = \bigwedge \Lambda$. We claim that $W(X)/\lambda$ is a lattice freely generated by $\{x\lambda : x \in X\}$.

By Basic Principle 3, $W(X)/\lambda$ is isomorphic to a subalgebra of a direct product of lattices, so it is a lattice.[3] Clearly $W(X)/\lambda$ is generated by $\{x\lambda : x \in X\}$, and because there exist nontrivial lattices (more than one element) for X to be mapped to in different ways, $x \neq y$ implies $x\lambda \neq y\lambda$ for $x, y \in X$.

Now let $\mathcal{L}$ be a lattice and let $f_0 : X \to L$ be any map. By the preceding observation, the corresponding map $h_0 : X/\lambda \to L$ defined by $h_0(x\lambda) = f_0(x)$ is well defined. Now f_0 can be extended to a homomorphism $f : W(X) \to \mathcal{L}$, whose range is some sublattice $\mathcal{S}$ of $\mathcal{L}$. By Basic Principle 1, $W(X)/\ker f \cong \mathcal{S}$ so $\ker f \in \Lambda$, and hence $\ker f \geq \lambda$. If we use ε to denote the standard homomorphism $W(X) \twoheadrightarrow W(X)/\lambda$ with $\varepsilon(u) = u\lambda$ for all $u \in W(X)$, then $\ker f \geq \ker \varepsilon = \lambda$. Thus by Basic Principle 2 there exists a homomorphism $h : W(X)/\lambda \to \mathcal{L}$ with $h\varepsilon = f$ (see Figure 6.2). This means $h(u\lambda) = f(u)$ for all $u \in W(X)$; in particular, h extends h_0 as required. $\square$

$$
\begin{tikzcd}
W(X) \arrow[rr, "f"] \arrow[dr, two heads, "\varepsilon"'] & & \mathcal{L} \\
& W(X)/\lambda \arrow[ur, dashed, "h"'] &
\end{tikzcd}
$$

Figure 6.2

It is easy to see, using the mapping property (III), that if $\mathcal{F}$ is a lattice freely generated by X, $\mathcal{G}$ is a lattice freely generated by Y, and $|X| = |Y|$, then $\mathcal{F} \cong \mathcal{G}$. Thus we can speak of *the* free lattice generated by X, which we will denote by $\mathrm{FL}(X)$. If $|X| = n$, then we also denote this lattice by $\mathrm{FL}(n)$. The lattice $\mathrm{FL}(2)$ has four elements, so there is not much to say about it. But $\mathrm{FL}(n)$ is infinite for $n \geq 3$, and we want to investigate its structure.

The advantage of the general construction we used is that it gives us the existence of free algebras in any variety; the disadvantage is that it does not, indeed cannot, tell us anything about the arithmetic of free lattices. For this we need a result due to Thoralf Skolem [22] (reprinted in [23]), and independently, P. M. Whitman [25].[4]

[3] This is where we use that lattices are equationally defined, since we need closure under subalgebras and direct products. For example, the class of integral domains is not equationally defined, and the direct product of two or more integral domains is not one.

[4] The history here is rather interesting. Skolem, as part of his 1920 paper which proves the Lowenheim-Skolem Theorem, solved the word problem not only for free lattices, but for finitely presented lattices as well. But by the time the great awakening of lattice theory occurred in the 1930's, his solution had been forgotten. Thus Whitman's 1941 construction of free lattices became the standard reference on the subject. It was not until 1992 that Stan Burris rediscovered Skolem's solution.

Theorem 6.2. *Every free lattice* $\mathrm{FL}(X)$ *satisfies the following conditions, where* $x, y \in X$ *and* $p, q, p_1, p_2, q_1, q_2 \in \mathrm{FL}(X)$*.*

(1) $x \leq y$ *iff* $x = y$.
(2) $x \leq q_1 \vee q_2$ *iff* $x \leq q_1$ *or* $x \leq q_2$.
(3) $p_1 \wedge p_2 \leq x$ *iff* $p_1 \leq x$ *or* $p_2 \leq x$.
(4) $p_1 \vee p_2 \leq q$ *iff* $p_1 \leq q$ *and* $p_2 \leq q$.
(5) $p \leq q_1 \wedge q_2$ *iff* $p \leq q_1$ *and* $p \leq q_2$.
(6) $p = p_1 \wedge p_2 \leq q_1 \vee q_2 = q$ *iff* $p_1 \leq q$ *or* $p_2 \leq q$ *or* $p \leq q_1$ *or* $p \leq q_2$.

Finally, $p = q$ *iff* $p \leq q$ *and* $q \leq p$.

Condition (6) in Theorem 6.2 is known as *Whitman's condition*, and it is usually denoted by (W).

Proof of Theorem 6.2. Properties (4) and (5) hold in every lattice, by the definition of least upper bound and greatest lower bound, respectively. Likewise, the "if" parts of the remaining conditions hold in every lattice.

We can take care of (1) and (2) simultaneously. Fixing $x \in X$, let

$$G_x = \{w \in \mathrm{FL}(X) : w \geq x \text{ or } w \leq \bigvee F \text{ for some finite } F \subseteq X - \{x\}\}.$$

Then $X \subseteq G_x$, and G_x is closed under joins and meets, so $G_x = \mathrm{FL}(X)$. Thus every $w \in \mathrm{FL}(X)$ is either above x or below $\bigvee F$ for some finite $F \subseteq X - \{x\}$. Properties (1) and (2) will follow if we can show that this "or" is exclusive: $x \nleq \bigvee F$ for all finite $F \subseteq X - \{x\}$. So let $h_0 : X \to \mathbf{2}$ (the two element chain) be defined by $h_0(x) = 1$, and $h_0(y) = 0$ for $y \in X - \{x\}$. This map extends to a homomorphism $h : \mathrm{FL}(X) \to \mathbf{2}$. For every finite $F \subseteq X - \{x\}$ we have $h(x) = 1 \nleq 0 = h(\bigvee F)$, whence $x \nleq \bigvee F$.

Condition (3) is the dual of (2). Note that the proof shows $x \ngeq \bigwedge H$ for all finite $H \subseteq X - \{x\}$.

Whitman's condition (6), or (W), can be proved using a slick construction due to Alan Day [5]. This construction can be motivated by a simple example. In the lattice of Figure 6.3(a), the elements a, b, c, d fail (W); in Figure 6.3(b) we have "fixed" this failure by making $a \wedge b \nleq c \vee d$. Day's method provides a formal way of doing this for any (W)-failure.

Let $I = u/v$ be an interval in a lattice $\mathcal{L}$. We define a new lattice $\mathcal{L}[I]$ as follows. The universe of $\mathcal{L}[I]$ is $(L - I) \cup (I \times \mathbf{2})$. Thus the elements of $\mathcal{L}[I]$ are of the form x with $x \notin I$, and (y, i) with $i \in \{0, 1\}$ and $y \in I$. The order on $\mathcal{L}[I]$ is defined by:

$$\begin{aligned} x \leq y &\text{ if } x \leq_{\mathcal{L}} y \\ (x, i) \leq y &\text{ if } x \leq_{\mathcal{L}} y \\ x \leq (y, j) &\text{ if } x \leq_{\mathcal{L}} y \\ (x, i) \leq (y, j) &\text{ if } x \leq_{\mathcal{L}} y \text{ and } i \leq j. \end{aligned}$$

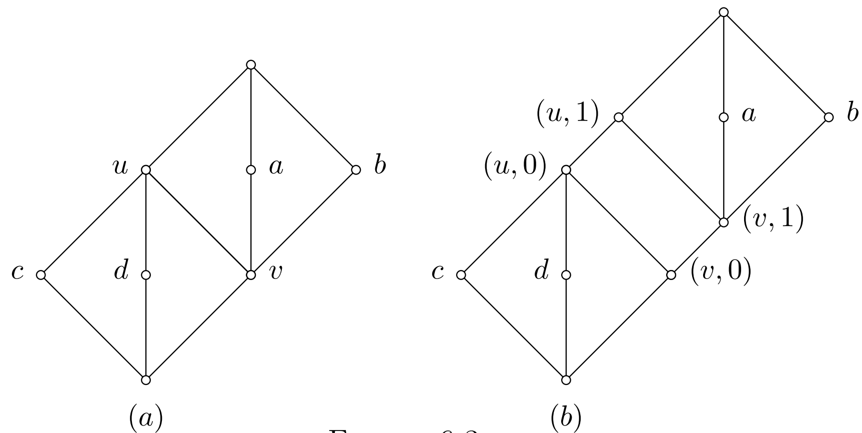


FIGURE 6.3

It is not hard to check the various cases to show that each pair of elements in $L[I]$ has a meet and join, so that $\mathcal{L}[I]$ is indeed a lattice.[5] Moreover, the natural map $\kappa : \mathcal{L}[I] \twoheadrightarrow \mathcal{L}$ with $\kappa(x) = x$ and $\kappa((y, i)) = y$ is a homomorphism. Figure 6.4 gives another example of the doubling construction, where the doubled interval consists of a single element $\{u\}$.

Now suppose a, b, c, d witness a failure of (W) in FL(X). Let $u = c \vee d$, $v = a \wedge b$ and $I = u/v$. Let $h_0 : X \to \text{FL}(X)[I]$ with $h_0(x) = x$ if $x \notin I$, $h_0(y) = (y, 0)$ if $y \in I$, and extend this map to a homomorphism h. Now $\kappa h : \text{FL}(X) \to \text{FL}(X)$ is also a homomorphism, and since $\kappa h(x) = x$ for all $x \in X$, it is in fact the identity. Therefore $h(w) \in \kappa^{-1}(w)$ for all $w \in \text{FL}(X)$, i.e., $h(w)$ is one of w, $(w, 0)$ or $(w, 1)$. Since $a, b, c, d \notin I$, this means $h(t) = t$ for $t \in \{a, b, c, d\}$. Now $v = a \wedge b \leq c \vee d = u$ in FL(X), so $h(v) \leq h(u)$. But we can calculate

$$h(v) = h(a) \wedge h(b) = a \wedge b = (v, 1) \nleq (u, 0) = c \vee d = h(c) \vee h(d) = h(u)$$

in FL$(X)[I]$, a contradiction. Thus (W) holds in FL(X). $\square$

Theorem 6.2 gives us a solution to the *word problem* for free lattices, i.e., an algorithm for deciding whether two lattice terms $p, q \in W(X)$ evaluate to the same element in FL(X) (and hence in all lattices). Strictly speaking, we have an evaluation map $\varepsilon : W(X) \to \text{FL}(X)$ with $\varepsilon(x) = x$ for all $x \in X$, and we want to decide whether $\varepsilon(p) = \varepsilon(q)$. Following tradition, however, we suppress the ε and ask whether $p = q$ in FL(X).

[5] This construction yields a lattice if, instead of requiring that I be an interval, we only ask that it be convex, i.e., if $x, z \in I$ and $x \leq y \leq z$, then $y \in I$. This generalized construction has also proved very useful; see Section II.3 of [12], which is based on Day [6], [7] and [8].

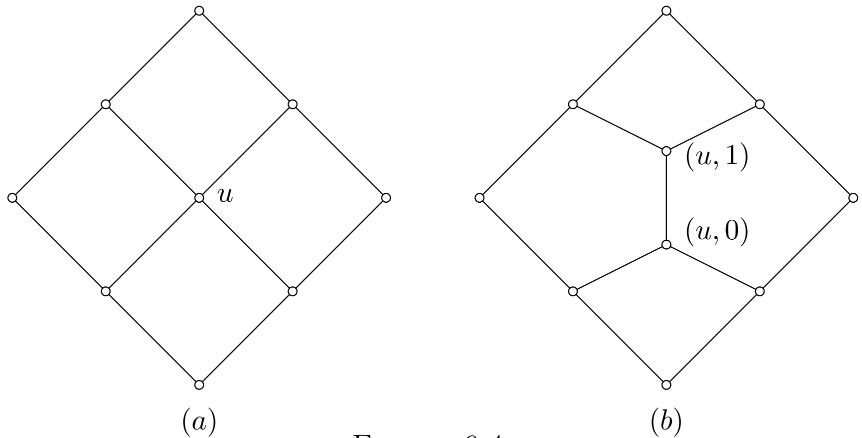


FIGURE 6.4

Corollary. *Let $p, q \in W(X)$. To decide whether $p \leq q$ in $\mathrm{FL}(X)$, apply the conditions of Theorem 6.2 recursively. To test whether $p = q$ in $\mathrm{FL}(X)$, check both $p \leq q$ and $q \leq p$.*

The algorithm works because it eventually reduces $p \leq q$ to a statement involving the conjunction and disjunction of a number of inclusions of the form $x \leq y$, each of which holds if and only if $x = y$. Using the algorithm requires a little practice; you should try showing that $x \wedge (y \vee z) \nleq (x \wedge y) \vee (x \wedge z)$ in $\mathrm{FL}(X)$, which is equivalent to the statement that not every lattice is distributive.[6] To appreciate its significance, you should know that it is not always possible to solve the word problem for free algebras. For example, the word problem for a free modular lattice $\mathcal{F}_{\mathbf{M}}(X)$ is not solvable if $|X| \geq 4$ (see Chapter 7).

By isolating the properties that do not hold in every lattice, we can rephrase Theorem 6.2 in the following useful form.

Theorem 6.3. *A lattice $\mathcal{F}$ is freely generated by its subset X if and only if $\mathcal{F}$ is generated by X, $\mathcal{F}$ satisfies (W), and the following two conditions hold for each $x \in X$:*

(1) *if $x \leq \bigvee G$ for some finite $G \subseteq X$, then $x \in G$;*
(2) *if $x \geq \bigwedge H$ for some finite $H \subseteq X$, then $x \in H$.*

It is worthwhile to compare the roles of $\mathbf{Eq}\, X$ and $\mathrm{FL}(X)$: every lattice can be embedded into a lattice of equivalence relations, while every lattice is a homomorphic image of a free lattice.

---

[6] The algorithm for the word problem, and other free lattice algorithms, can be efficiently programmed; see Chapter XI of [12]. These programs have proved to be a useful tool in the investigation of the structure of free lattices.

Note that it follows from (W) that no element of $\mathrm{FL}(X)$ is properly both a meet and a join, i.e., every element is either meet irreducible or join irreducible. Moreover, the generators are the only elements that are both meet and join irreducible. Thus *the generating set of* $\mathrm{FL}(X)$ *is unique.* This is very different from the situation say in free groups: the free group on $\{x, y\}$ is also generated (freely) by $\{x, xy\}$.

Each element $w \in \mathrm{FL}(X)$ corresponds to an equivalence class of terms in $W(X)$. Among the terms that evaluate to w, there may be several of minimal length (total number of symbols), e.g., $(x \vee (y \vee z))$, $((y \vee x) \vee z)$, etc. Note that if a term p can be obtained from a term q by applications of the associative and commutative laws only, then p and q have the same length. This allows us to speak of the length of a term $t = \bigvee t_i$ without specifying the order or parenthesization of the joinands, and likewise for meets. We want to show that a minimal length term for w is unique up to associativity and commutativity. This is true for generators, so by duality it suffices to consider the case when w is a join.

Lemma 6.4. *Let $t = \bigvee t_i$ in $W(X)$, where each t_i is either a generator or a meet. Assume that $\varepsilon(t) = w$ and $\varepsilon(t_i) = w_i$ under the evaluation map $\varepsilon : W(X) \to \mathrm{FL}(X)$. If t is a minimal length term representing w, then the following are true.*

(1) *Each t_i is of minimal length.*
(2) *The w_i's are pairwise incomparable.*
(3) *If t_i is not a generator, so $t_i = \bigwedge_j t_{ij}$, then $\varepsilon(t_{ij}) = w_{ij} \nleq w$ for all j.*

Proof. Only (3) requires explanation. Suppose $w_i = \bigwedge w_{ij}$ in $\mathrm{FL}(X)$, corresponding to $t_i = \bigwedge t_{ij}$ in $W(X)$. Note that $w_i \leq w_{ij}$ for all j. If for some j_0 we also had $w_{ij_0} \leq w$, then

$$w = \bigvee w_i \leq w_{ij_0} \vee \bigvee_{k \neq i} w_k \leq w,$$

whence $w = w_{ij_0} \vee \bigvee_{k \neq i} w_k$. But then replacing t_i by t_{ij_0} would yield a shorter term representing w, a contradiction. □

If A and B are finite subsets of a lattice, we say that A *refines* B, written $A \ll B$, if for each $a \in A$ there exists $b \in B$ with $a \leq b$. We define dual refinement by $C \gg D$ if for each $c \in C$ there exists $d \in D$ with $c \geq d$; note that because of the reversed order of the quantification in the two statements, $A \ll B$ is not the same as $B \gg A$. The elementary properties of refinement can be set out as follows, with the proofs left as an exercise.

Lemma 6.5. *The refinement relation on finite subsets of a lattice $\mathcal{L}$ has the following properties.*

(1) *$A \ll B$ implies $\bigvee A \leq \bigvee B$.*
(2) *The relation $\ll$ is a quasiorder on the finite subsets of L.*
(3) *If $A \subseteq B$ then $A \ll B$.*
(4) *If A is an antichain, $A \ll B$ and $B \ll A$, then $A \subseteq B$.*

(5) *If A and B are antichains with $A \ll B$ and $B \ll A$, then $A = B$.*
(6) *If $A \ll B$ and $B \ll A$, then A and B have the same set of maximal elements.*

The preceding two lemmas are connected as follows.

Lemma 6.6. *Let $w = \bigvee_{1 \le i \le m} w_i = \bigvee_{1 \le k \le n} u_k$ in $\mathrm{FL}(X)$. If each w_i is either a generator or a meet $w_i = \bigwedge_j w_{ij}$ with $w_{ij} \nleq w$ for all j, then*

$$\{w_1, \dots, w_m\} \ll \{u_1, \dots, u_n\}.$$

Proof. For each i we have $w_i \le \bigvee u_k$. If w_i is a generator, this implies $w_i \le u_s$ for some s by Theorem 6.2(2). If $w_i = \bigwedge w_{ij}$, we apply Whitman's condition (W) to the inclusion $w_i = \bigwedge w_{ij} \le \bigvee u_k = w$. Since we are given that $w_{ij} \nleq w$ for all j, it must be that $w_i \le u_t$ for some t. Hence $\{w_1, \dots, w_m\} \ll \{u_1, \dots, u_n\}$. □

Now let $t = \bigvee t_i$ and $s = \bigvee s_j$ be two minimal length terms that evaluate to w in $\mathrm{FL}(X)$. Let $\varepsilon(t_i) = w_i$ and $\varepsilon(s_j) = u_j$, so that $w = \bigvee w_i = \bigvee u_j$ in $\mathrm{FL}(X)$. By Lemma 6.4(1) each t_i is a minimal length term for w_i, and each s_j is a minimal length term for u_j. By induction, these are unique up to associativity and commutativity. Hence we may assume that $t_i = s_j$ whenever $w_i = u_j$. By Lemma 6.4(2), the sets $\{w_1, \dots, w_m\}$ and $\{u_1, \dots, u_n\}$ are antichains in $\mathrm{FL}(X)$. By Lemma 6.4(3), the elements w_i satisfy the hypothesis of Lemma 6.6, so $\{w_1, \dots, w_m\} \ll \{u_1, \dots, u_n\}$. Symmetrically, $\{u_1, \dots, u_n\} \ll \{w_1, \dots, w_m\}$. Applying Lemma 6.5(5) yields $\{w_1, \dots, w_m\} = \{u_1, \dots, u_n\}$, whence by our assumption above $\{t_1, \dots, t_m\} = \{s_1, \dots, s_n\}$. Thus we obtain the desired uniqueness result.

Theorem 6.7. *The minimal length term representing an element $w \in \mathrm{FL}(X)$ is unique up to associativity and commutativity.*

This minimal length term is called the *canonical form* of w. The canonical form of a generator is just x. The proof of the theorem has shown that if w is a proper join, then its canonical form is determined by the conditions of Lemma 6.4. If w is a proper meet, then of course its canonical form must satisfy the dual conditions.

The proof of Lemma 6.4 gives us an algorithm for finding the canonical form of a lattice term. Let $t = \bigvee t_i$ in $W(X)$, where each t_i is either a generator or a meet, and suppose that we have already put each t_i into canonical form, which we can do inductively. This will guarantee that condition (1) of Lemma 6.4 holds when we are done. For each t_i that is not a generator, say $t_i = \bigwedge t_{ij}$, check whether any $t_{ij} \le t$ in $\mathrm{FL}(X)$; if so, replace t_i by t_{ij}. Continue this process until you have an expression $u = \bigvee u_i$ which satisfies condition (3). Finally, check whether $u_i \le u_j$ in $\mathrm{FL}(X)$ for any pair $i \ne j$; if so, delete u_i. The resulting expression $v = \bigvee v_i$ evaluates to the same element as t in $\mathrm{FL}(X)$, and v satisfies (1), (2) and (3). Hence v is the canonical form of t.

If $w = \bigvee w_i$ canonically in $\mathrm{FL}(X)$, then the elements w_i are called the *canonical joinands* of w (dually, *canonical meetands*). It is important to note that these elements satisfy the refinement property of Lemma 6.6.

Corollary. *If w is a proper join in* $\mathrm{FL}(X)$ *and* $w = \bigvee U$, *then the set of canonical joinands of w refines U.*

This has an important structural consequence, observed by Bjarni Jónsson [16].

Theorem 6.8. *Free lattices satisfy the following implications, for all* $u, v, a, b, c \in \mathrm{FL}(X)$*:*

$$(SD_\vee) \quad \text{if } u = a \vee b = a \vee c \text{ then } u = a \vee (b \wedge c),$$

$$(SD_\wedge) \quad \text{if } v = a \wedge b = a \wedge c \text{ then } v = a \wedge (b \vee c).$$

The implications ($\mathrm{SD}_\vee$) and ($\mathrm{SD}_\wedge$) are known as the *semidistributive laws.* Exercises 5 and 6 concern properties of finite join semidistributive lattices.

Proof. We will prove that $\mathrm{FL}(X)$ satisfies ($\mathrm{SD}_\vee$); then ($\mathrm{SD}_\wedge$) follows by duality. We may assume that u is a proper join, for otherwise u is join irreducible and the implication is trivial. So let $u = u_1 \vee \ldots \vee u_n$ be the canonical join decomposition. By the Corollary above, $\{u_1, \ldots, u_n\}$ refines both $\{a, b\}$ and $\{a, c\}$. Any u_i that is not below a must be below both b and c, so in fact $\{u_1, \ldots, u_n\} \ll \{a, b \wedge c\}$. Hence

$$u = \bigvee u_i \leq a \vee (b \wedge c) \leq u \ ,$$

whence $u = a \vee (b \wedge c)$, as desired. $\square$

Now let us recall some basic facts about free groups, so we can ask about their analogs for free lattices. Every subgroup of a free group is free, and the countably generated free group $FG(\omega)$ is isomorphic to a subgroup of $FG(2)$. Every identity which does not hold in all groups fails in some finite group.

Whitman used Theorem 6.3 and a clever construction to show that $\mathrm{FL}(\omega)$ can be embedded in $\mathrm{FL}(3)$. It is not known exactly which lattices are isomorphic to a sublattice of a free lattice, but certainly they are not all free. The simplest result (to state, not to prove) along these lines is due to the author [18].

Theorem 6.9. *A finite lattice can be embedded in a free lattice if and only if it satisfies* (W), ($SD_\vee$) *and* ($SD_\wedge$).

We can weaken the question somewhat and ask which ordered sets can be embedded in free lattices. A characterization of sorts for these ordered sets was found by Freese and Nation ([13] and [19]), but unfortunately it is not particularly enlightening. We obtain a better picture of the structure of free lattices by considering the following collection of results due to P. Crawley and R. A. Dean [4], B. Jónsson [16], and J. B. Nation and J. Schmerl [20], respectively.

Theorem 6.10. *Every countable ordered set can be embedded in* $\mathrm{FL}(3)$. *On the other hand, every chain in a free lattice is countable, so no uncountable chain can be embedded in a free lattice. If $\mathcal{P}$ is an infinite ordered set that can be embedded in* *a free lattice, then the dimension* $d(\mathcal{P}) \leq \mathfrak{m}$, *where* $\mathfrak{m}$ *is the smallest cardinal such that* $|\mathcal{P}| \leq 2^{\mathfrak{m}}$.

R. A. Dean showed that every equation that does not hold in all lattices fails in some finite lattice [9] (see Exercise 7.5). It turns out (though this is not obvious) that this is related to a beautiful structural result of Alan Day ([6], using [17]).

Theorem 6.11. *If* X *is finite, then* $\mathrm{FL}(X)$ *is weakly atomic.*

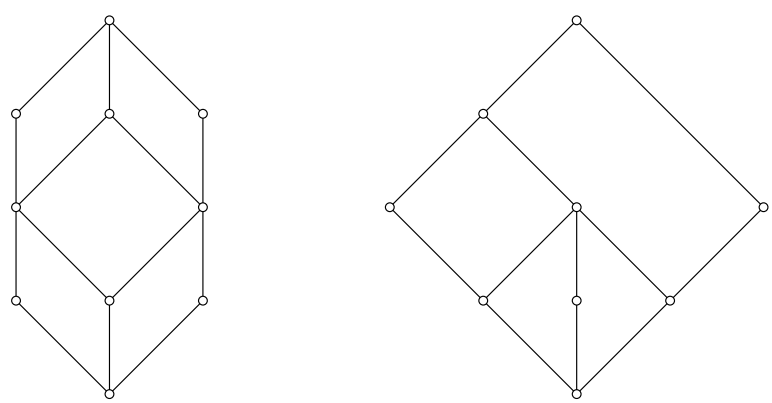
The book *Free Lattices* by Freese, Ježek and Nation [12] contains more information about the surprisingly rich structure of free lattices. Two papers of Ralph Freese contain analagous structure theory for finitely presented lattices [10], [11].

Chapter 2 of the *Free Lattice* book contains an introduction to upper and lower bounded lattices, a topic only hinted at in Exercise 11. These ideas grew from the work of Bjarni Jónsson and Ralph McKenzie; the paper [17] is a classic. For more recent results in this area, see Kira Adaricheva *et. al.* [1], [2] and the references therein.

Exercises for Chapter 6

1. Verify that if $\mathcal{L}$ is a lattice and I is an interval in $\mathcal{L}$, then $\mathcal{L}[I]$ is a lattice.

2. Use the doubling construction to repair the (W)-failures in the lattices in Figure 6.5. (Don't forget to double elements that are both join and meet reducible.) Then repeat the process until you either obtain a lattice satisfying (W), or else prove that you never will get one in finitely many steps.



(a) (b)

Figure 6.5

3. (a) Show that $x \wedge ((x \wedge y) \vee z) \not\leq y \vee (z \wedge (x \vee y))$ in $\mathrm{FL}(X)$.
(b) Find the canonical form of $x \wedge ((x \wedge y) \vee (x \wedge z))$.
(c) Find the canonical form of $(x \wedge ((x \wedge y) \vee (x \wedge z) \vee (y \wedge z))) \vee (y \wedge z)$.

4. There are five small lattices that fail $\mathrm{SD}_\vee$, but have no proper sublattice failing $\mathrm{SD}_\vee$. Find them.

5. Show that the following conditions are equivalent (to $\mathrm{SD}_\vee$) in a finite lattice.

(a) $u = a \vee b = a \vee c$ implies $u = a \vee (b \wedge c)$.
(b) For each $m \in M(\mathcal{L})$ there is a unique $j \in J(\mathcal{L})$ such that for all $x \in L$, $m^* \wedge x \not\leq m$ iff $x \geq j$.
(c) For each $a \in L$, there is a set $C \subseteq J(\mathcal{L})$ such that $a = \bigvee C$, and for every subset $B \subseteq L$, $a = \bigvee B$ implies $C \ll B$.
(d) $u = \bigvee_i u_i = \bigvee_j v_j$ implies $u = \bigvee_{i,j}(u_i \wedge v_j)$.

In a finite lattice satisfying these conditions, the elements of the set C given by part (c) are called the *canonical joinands* of a. See Jónsson and Kiefer [15].

6. An element $p \in L$ is *join prime* if $p \leq x \vee y$ implies $p \leq x$ or $p \leq y$; *meet prime* is defined dually. Let $\mathrm{JP}(\mathcal{L})$ denote the set of all join prime elements of $\mathcal{L}$, and let $\mathrm{MP}(\mathcal{L})$ denote the set of all meet prime elements of $\mathcal{L}$. Consider a finite lattice $\mathcal{L}$ satisfying $\mathrm{SD}_\vee$.

(a) Prove that the canonical joinands of 1 are join prime.
(b) Prove that the coatoms of $\mathcal{L}$ are meet prime.
(c) Show that for each $q \in \mathrm{MP}(\mathcal{L})$ there exists a unique element $\eta(q) \in \mathrm{JP}(\mathcal{L})$ such that L is the disjoint union of $\downarrow q$ and $\uparrow \eta(q)$.

7. Prove Lemma 6.5.

8. Let $\mathcal{A}$ and $\mathcal{B}$ be lattices, and let $X \subseteq A$ generate $\mathcal{A}$. Prove that a map $h_0 : X \to \mathcal{B}$ can be extended to a homomorphism $h : \mathcal{A} \to \mathcal{B}$ if and only if, for every pair of lattice terms p and q, and all $x_1, \ldots, x_n \in X$,

$$p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n) \text{ implies } p(h_0(x_1), \ldots, h_0(x_n)) = q(h_0(x_1), \ldots, h_0(x_n)).$$

9. A complete lattice $\mathcal{L}$ has *canonical decompositions* if for each $a \in L$ there exists a set C of completely meet irreducible elements such that $a = \bigwedge C$ irredundantly, and $a = \bigwedge B$ implies $C \gg B$. Prove that an upper continuous lattice has canonical decompositions if and only if it is strongly atomic and satisfies $\mathrm{SD}_\wedge$ (Viktor Gorbunov [14]).

For any ordered set $\mathcal{P}$, a lattice $\mathcal{F}$ is said to be *freely generated by* $\mathcal{P}$ if $\mathcal{F}$ contains a subset P such that

(1) P with the order it inherits from $\mathcal{F}$ is isomorphic to $\mathcal{P}$,
(2) P generates $\mathcal{F}$,
(3) for every lattice $\mathcal{L}$, every order preserving map $h_0 : P \to \mathcal{L}$ can be extended to a homomorphism $h : \mathcal{F} \to \mathcal{L}$.

In much the same way as with free lattices, we can show that there is a unique (up to isomorphism) lattice $\mathrm{FL}(\mathcal{P})$ generated by any ordered set $\mathcal{P}$. Indeed, free lattices $\mathrm{FL}(X)$ are just the case when $\mathcal{P}$ is an antichain.

10. (a) Find the lattice freely generated by $\{x, y, z\}$ with $x \geq y$.
(b) Find $\mathrm{FL}(\mathcal{P})$ for $\mathcal{P} = \{x_0, x_1, x_2, z\}$ with $x_0 \leq x_1 \leq x_2$.

The lattice freely generated by $\mathcal{Q} = \{x_0, x_1, x_2, x_3, z\}$ with $x_0 \leq x_1 \leq x_2 \leq x_3$ is infinite, as is that generated by $\mathcal{R} = \{x_0, x_1, y_0, y_1\}$ with $x_0 \leq x_1$ and $y_0 \leq y_1$ (Yu. I. Sorkin [24], see [21]).

11. A homomorphism $h : \mathcal{L} \to \mathcal{K}$ is *lower bounded* if for each $a \in K$, $\{x \in L : h(x) \geq a\}$ is either empty or has a least element $\beta(a)$. For example, if $\mathcal{L}$ satisfies the DCC, then h is lower bounded. We regard β as a partial map from $\mathcal{K}$ to $\mathcal{L}$. Let $h : \mathcal{L} \to \mathcal{K}$ be a lower bounded homomorphism.

(a) Show that the domain of β is an ideal of $\mathcal{K}$.
(b) Prove that β preserves finite joins.
(c) Show that if h is onto and $\mathcal{L}$ satisfies $\mathrm{SD}_\vee$, then so does $\mathcal{K}$.

References

1. K. V. Adaricheva and V. A. Gorbunov, *On lower bounded lattices*, Algebra Universalis **46** (2001), 203–213.
2. K. V. Adaricheva and J. B. Nation, *Reflections on lower bounded lattices*, Algebra Universalis **53** (2005), 307–330.
3. G. Birkhoff, *On the structure of abstract algebras*, Proc. Cambridge Phil. Soc. **31** (1935), 433–454.
4. P. Crawley and R. A. Dean, *Free lattices with infinite operations*, Trans. Amer. Math. Soc. **92** (1959), 35–47.
5. A. Day, *A simple solution of the word problem for lattices*, Canad. Math. Bull. **13** (1970), 253–254.
6. A. Day, *Splitting lattices generate all lattices*, Algebra Universalis **7** (1977), 163–170.
7. A. Day, *Characterizations of finite lattices that are bounded-homomorphic images or sublattices of free lattices*, Canad. J. Math. **31** (1979), 69–78.
8. A. Day, *Congruence normality: the characterization of the doubling class of convex sets*, Addendum by J. B. Nation, 407–410, Algebra Universalis **31** (1994), 397–406.
9. R. A. Dean, *Component subsets of the free lattice on n generators*, Proc. Amer. Math. Soc. **7** (1956), 220–226.
10. R. Freese, *Finitely presented lattices: canonical form and the covering relation*, Trans. Amer. Math. Soc. **312** (1989), 841–860.
11. R. Freese, *Finitely presented lattices: continuity and semidistributivity*, Lattices, Semigroups and Universal Algebra, (J. Almeida, G. Bordalo and Ph. Dwinger, eds.), Proceedings of the Lisbon Conference 1988, Plenum Press, New York, 1990, pp. 67–70.
12. R. Freese, J. Ježek, and J. B. Nation, *Free Lattices*, Mathematical Surveys and Monographs, vol. 42, Amer. Math. Soc., Providence, 1995.
13. R. Freese and J. B. Nation, *Projective lattices*, Pacific J. Math. **75** (1978), 93–106.
14. V. A. Gorbunov, *Canonical decompositions in complete lattices*, Algebra i Logika **17** (1978), 495–511,622. (Russian)
15. B. Jónsson and J. E. Kiefer, *Finite sublattices of a free lattice*, Canad. J. Math. **14** (1962), 487–497.
16. B. Jónsson, *Sublattices of a free lattice*, Canad. J. Math. **13** (1961), 256–264.
17. R. McKenzie, *Equational bases and non-modular lattice varieties*, Trans. Amer. Math. Soc. **174** (1972), 1–43.

18. J. B. Nation, *Finite sublattices of a free lattice*, Trans. Amer. Math. Soc. **269** (1982), 311–337.
19. J. B. Nation, *On partially ordered sets embeddable in a free lattice*, Algebra Universalis **18** (1984), 327–333.
20. J. B. Nation and J. H. Schmerl, *The order dimension of relatively free lattices*, Order **7** (1990), 97–99.
21. H. L. Rolf, *The free lattice generated by a set of chains*, Pacific J. Math. **8** (1958), 585–595.
22. T. Skolem, *Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit und Beweisbarkeit mathematischen Sätze nebst einem Theoreme über dichte Mengen*, Videnskapsselskapets skrifter I, Matematisk-naturvidenskabelig klasse, Videnskabsakademiet i Kristiania **4** (1920), 1–36.
23. T. Skolem, *Select Works in Logic*, Scandinavian University Books, Oslo, 1970.
24. Yu. I. Sorkin, *Free unions of lattices*, Mat. Sbornik **30** (1952), 677–694. (Russian)
25. Ph. M. Whitman, *Free lattices*, Ann. of Math. (2) **42** (1941), 325–330.

7. Varieties of Lattices

Variety is the spice of life.

A *lattice equation* is an expression $p \approx q$ where p and q are lattice terms. Our intuitive notion of what it means for a lattice $\mathcal{L}$ to satisfy $p \approx q$ is that $p(x_1, \dots, x_n) = q(x_1, \dots, x_n)$ whenever elements of $\mathcal{L}$ are substituted for the variables. This is captured by the formal definition: $\mathcal{L}$ *satisfies* $p \approx q$ if $h(p) = h(q)$ for every homomorphism $h : W(X) \to \mathcal{L}$. We say that $\mathcal{L}$ satisfies a set Σ of equations if $\mathcal{L}$ satisfies every equation in Σ. Likewise, a class $\mathcal{K}$ of lattices satisfies Σ if every lattice $\mathcal{L} \in \mathcal{K}$ does so.

As long as we are dealing entirely with lattices, there is no loss of generality in replacing p and q by the corresponding elements of $\mathrm{FL}(X)$, since if terms p and p' evaluate the same in $\mathrm{FL}(X)$, then they evaluate the same for every substitution in every lattice. In practice it is often more simple and natural to think of equations between elements in a free lattice, rather than the corresponding terms, as in Theorem 7.2 below.

A *variety* (or *equational class*) of lattices is the class of all lattices satisfying some set Σ of lattice equations. The class $\mathbf{L}$ of all lattices is defined by equations (the idempotent, commutative, associative and absorption laws), so it forms a variety. Contained within $\mathbf{L}$ are some familiar subvarieties:

(1) the variety $\mathbf{M}$ of modular lattices, satisfying $(x \vee y) \wedge (x \vee z) \approx x \vee (z \wedge (x \vee y))$;
(2) the variety $\mathbf{D}$ of distributive lattices, satisfying $x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z)$;
(3) the variety $\mathbf{T}$ of one-element lattices, satisfying $x \approx y$ (not very exciting).

If $\mathbf{K}$ is any class of lattices, we say that a lattice $\mathcal{F}$ is $\mathbf{K}$-*freely generated* by its subset X if

(1) $\mathcal{F} \in \mathbf{K}$,
(2) X generates $\mathcal{F}$,
(3) for every lattice $\mathcal{L} \in \mathbf{K}$, every map $h_0 : X \to L$ can be extended to a homomorphism $h : \mathcal{F} \to \mathcal{L}$.

A lattice is $\mathbf{K}$-*free* if it is $\mathbf{K}$-freely generated by one of its subsets, and *relatively free* if it is $\mathbf{K}$-free for some (unspecified) class $\mathbf{K}$.

While these ideas floated around for some time before, it was Garrett Birkhoff [5] who proved the basic theorem about varieties in the 1930's.

Theorem 7.1. *If* $\mathbf{K}$ *is a nonempty class of lattices, then the following are equivalent.*

(1) $\mathbf{K}$ *is a variety.*

(2) $\mathbf{K}$ *is closed under the formation of homomorphic images, sublattices and direct products.*
(3) *Either* $\mathbf{K} = \mathbf{T}$ *(the variety of one-element lattices), or for every nonempty set* X *there is a lattice* $\mathcal{F}_{\mathbf{K}}(X)$ *that is* $\mathbf{K}$*-freely generated by* X*, and* $\mathbf{K}$ *is closed under homomorphic images.*

Proof. It is easy to see that varieties are closed under homomorphic images, sublattices and direct products, so (1) implies (2).

The crucial step in the equivalence, the construction of relatively free lattices $\mathcal{F}_{\mathbf{K}}(X)$, is a straightforward adaptation of the construction of $\mathrm{FL}(X)$. Let $\mathbf{K}$ be a class that is closed under the formation of sublattices and direct products, and let $\kappa = \bigcap\{\theta \in \mathbf{Con}\, W(X) : W(X)/\theta \in \mathbf{K}\}$. Following the proof of Theorem 6.1, we can show that $W(X)/\kappa$ is a subdirect product of lattices in $\mathbf{K}$, and that it is $\mathbf{K}$-freely generated by $\{x\kappa : x \in X\}$. Unless $\mathbf{K} = \mathbf{T}$, the classes $x\kappa$ $(x \in X)$ will be distinct. Thus (2) implies (3).

Finally, suppose that $\mathbf{K}$ is a class of lattices that is closed under homomorphic images and contains a $\mathbf{K}$-freely generated lattice $\mathcal{F}_{\mathbf{K}}(X)$ for every nonempty set X. For each nonempty X there is a homomorphism $f_X : W(X) \twoheadrightarrow \mathcal{F}_{\mathbf{K}}(X)$ that is the identity on X. Fix the countably infinite set $X_0 = \{x_1, x_2, x_3, \dots\}$, and let Σ be the collection of all equations $p \approx q$ such that $(p, q) \in \ker f_{X_0}$. Thus $p \approx q$ is in Σ if and only if $p(x_1, \dots, x_n) = q(x_1, \dots, x_n)$ in the countably generated lattice $\mathcal{F}_{\mathbf{K}}(X_0) \cong \mathcal{F}_{\mathbf{K}}(\omega)$.

Let $\mathbf{V}_\Sigma$ be the variety of all lattices satisfying Σ; we want to show that $\mathbf{K} = \mathbf{V}_\Sigma$. We formulate the critical argument as a sublemma.

Sublemma. *Let* $\mathcal{F}_{\mathbf{K}}(Y)$ *be a relatively free lattice. Let* $p, q \in W(Y)$ *and let* $f_Y : W(Y) \twoheadrightarrow \mathcal{F}_{\mathbf{K}}(Y)$ *with* f_Y *the identity on* Y*. Then* $\mathbf{K}$ *satisfies* $p \approx q$ *if and only if* $f_Y(p) = f_Y(q)$*.*

Proof. If $\mathbf{K}$ satisfies $p \approx q$, then $f_Y(p) = f_Y(q)$ because $\mathcal{F}_{\mathbf{K}}(Y) \in \mathbf{K}$. Conversely, if $f_Y(p) = f_Y(q)$, then by the mapping property (III) every lattice in $\mathbf{K}$ satisfies $p \approx q$.[1] □

Applying the Sublemma with $Y = X_0$, we conclude that $\mathbf{K}$ satisfies every equation of Σ, so $\mathbf{K} \subseteq \mathbf{V}_\Sigma$.

Conversely, let $\mathcal{L} \in \mathbf{V}_\Sigma$, and let X be a generating set for $\mathcal{L}$. The identity map on X extends to a surjective homomorphism $h : W(X) \twoheadrightarrow \mathcal{L}$, and we also have the map $f_X : W(X) \to \mathcal{F}_{\mathbf{K}}(X)$. For any pair $(p, q) \in \ker f_X$, the Sublemma says that $\mathbf{K}$ satisfies $p \approx q$. Again by the Sublemma, there is a corresponding equation in Σ (perhaps involving different variables). Since $\mathcal{L} \in \mathbf{V}_\Sigma$ this implies $h(p) = h(q)$. So $\ker f_X \le \ker h$, and hence by the Second Isomorphism Theorem there is

[1] However, if Y is finite and $Y \subseteq Z$, then $\mathcal{F}_{\mathbf{K}}(Y)$ may satisfy equations not satisfied by $\mathcal{F}_{\mathbf{K}}(Z)$. For example, for any lattice variety, $\mathcal{F}_{\mathbf{K}}(2)$ is distributive. The Sublemma only applies to equations with at most $|Y|$ variables.

a homomorphism $g : \mathcal{F}_{\mathbf{K}}(X) \to \mathcal{L}$ such that $h = gf_X$. Thus $\mathcal{L}$ is a homomorphic image of $\mathcal{F}_{\mathbf{K}}(X)$. Since $\mathbf{K}$ is closed under homomorphic images, this implies $\mathcal{L} \in \mathbf{K}$. Hence $\mathbf{V}_\Sigma \subseteq \mathbf{K}$, and equality follows. Therefore (3) implies (1). $\square$

The three parts of Theorem 7.1 reflect three different ways of looking at varieties. The first is to start with a set Σ of equations, and to consider the variety $V(\Sigma)$ of all lattices satisfying those equations. The given equations will in general imply other equations, *viz.*, all the relations holding in the relatively free lattices $\mathcal{F}_{V(\Sigma)}(X)$. It is important to notice that while the proof of Birkhoff's theorem tells us abstractly how to construct relatively free lattices, it does not tell us how to solve the word problem for them. Consider the variety $\mathbf{M}$ of modular lattices. Richard Dedekind [6] showed in the 1890's that $\mathcal{F}_{\mathbf{M}}(3)$ has 28 elements; it is drawn in Figure 9.2. On the other hand, Ralph Freese [9] proved in 1980 that the word problem for $\mathcal{F}_{\mathbf{M}}(5)$ is unsolvable: *there is no algorithm for determining whether* $p = q$ *in* $\mathcal{F}_{\mathbf{M}}(5)$. Christian Herrmann [10] later showed that the word problem for $\mathcal{F}_{\mathbf{M}}(4)$ is also unsolvable. It follows, by the way, that the variety of modular lattices is not generated by its finite members:[2] *there is a lattice equation that holds in all finite modular lattices, but not in all modular lattices.*

Skipping to the third statement of Theorem 7.1, let $\mathbf{V}$ be a variety, and let κ be the kernel of the natural homomorphism $h : \mathrm{FL}(X) \to \mathcal{F}_{\mathbf{V}}(X)$ with $h(x) = x$ for all $x \in X$. Then, of course, $\mathcal{F}_{\mathbf{V}}(X) \cong \mathrm{FL}(X)/\kappa$. We want to ask which congruences on $\mathrm{FL}(X)$ arise in this way, i.e., *for which* $\theta \in \mathbf{Con}\ \mathrm{FL}(X)$ *is* $\mathrm{FL}(X)/\theta$ *relatively free?* To answer this, we need a couple of definitions.

An *endomorphism* of a lattice $\mathcal{L}$ is a homomorphism $f : \mathcal{L} \to \mathcal{L}$. The set of endomorphisms of $\mathcal{L}$ forms a semigroup $\mathbf{End}\ \mathcal{L}$ under composition. It is worth noting that an endomorphism of a lattice is determined by its action on a generating set, since $f(p(x_1, \ldots, x_n) = p(f(x_1), \ldots, f(x_n))$ for any lattice term p. In particular, an endomorphism f of $\mathrm{FL}(X)$ corresponds to a substitution $x_i \mapsto f(x_i)$ of elements for the generators.

A congruence relation θ is *fully invariant* if $(x, y) \in \theta$ implies $(f(x), f(y)) \in \theta$ for every endomorphism f of $\mathcal{L}$. The fully invariant congruences of $\mathcal{L}$ can be thought of as the congruence relations of the algebra $\mathcal{L}^* = (L, \wedge, \vee, \{f : f \in \mathrm{End}\ \mathcal{L}\})$. In particular, they form an algebraic lattice, in fact a complete sublattice of $\mathbf{Con}\,\mathcal{L}$.

The answer to our question, in these terms, is again due to Garrett Birkhoff [4].

Theorem 7.2. $\mathrm{FL}(X)/\theta$ *is relatively freely generated by* $\{x\theta : x \in X\}$ *if and only if* θ *is fully invariant.*

Proof. Let $\mathbf{V}$ be a lattice variety and let $h : \mathrm{FL}(X) \to \mathcal{F}_{\mathbf{V}}(X)$ with $h(x) = x$ for all $x \in X$. Then $h(p) = h(q)$ if and only if $\mathbf{V}$ satisfies $p \approx q$ (as in the Sublemma).

[2] If a variety $\mathbf{V}$ of algebras (1) has only finitely many operation symbols, (2) is finitely based, and (3) is generated by its finite members, then the word problem for $\mathcal{F}_{\mathbf{V}}(X)$ is solvable. This result is due to A. I. Malcev for groups; see T. Evans [7].

Hence, for any endomorphism f and elements p, $q \in \mathrm{FL}(X)$, if $h(p) = h(q)$ then

$$\begin{aligned} hf(p) = h(f(p(x_1, \ldots, x_n))) &= h(p(f(x_1), \ldots, f(x_n))) \\ &= h(q(f(x_1), \ldots, f(x_n))) \\ &= h(f(q(x_1, \ldots, x_n))) = hf(q) \end{aligned}$$

so that $(f(p), f(q)) \in \ker h$. Thus the congruence $\ker h$ is fully invariant.

Conversely, assume that θ is a fully invariant congruence on $\mathrm{FL}(X)$. If $\theta = 1_{\mathbf{Con}\ \mathrm{FL}(X)}$, then θ is fully invariant and $\mathrm{FL}(X)/\theta$ is relatively free for the trivial variety $\mathbf{T}$. So without loss of generality, θ is not the universal relation. Let $k : \mathrm{FL}(X) \to \mathrm{FL}(X)/\theta$ be the canonical homomorphism with $\ker k = \theta$. Let $\mathbf{V}$ be the variety determined by the set of equations $\Sigma = \{p \approx q : (p, q) \in \theta\}$. To show that $\mathrm{FL}(X)/\theta$ is $\mathbf{V}$-freely generated by $\{x\theta : x \in X\}$, we must verify that

(1) $\mathrm{FL}(X)/\theta \in \mathbf{V}$, and
(2) if $\mathcal{M} \in \mathbf{V}$ and $h_0 : X \to M$, then there is a homomorphism $h : \mathrm{FL}(X)/\theta \to \mathcal{M}$ such that $h(x\theta) = h_0(x)$, i.e., $hk(x) = h_0(x)$ for all $x \in X$.

For (1), we must show that the lattice $\mathrm{FL}(X)/\theta$ satisfies every equation of Σ, i.e., that if $p(x_1, \ldots, x_n)\ \theta\ q(x_1, \ldots, x_n)$ and $w_1, \ldots, w_n$ are elements of $\mathrm{FL}(X)$, then $p(w_1, \ldots, w_n)\ \theta\ q(w_1, \ldots, w_n)$. Since there is an endomorphism f of $\mathrm{FL}(X)$ with $f(x_i) = w_i$ for all i, this follows from the fact that θ is fully invariant.

To prove (2), let $g : \mathrm{FL}(X) \to \mathcal{M}$ be the homomorphism such that $g(x) = h_0(x)$ for all $x \in X$. Since $\mathcal{M}$ is in $\mathbf{V}$, $g(p) = g(q)$ whenever $p \approx q$ is in Σ, and thus $\theta = \ker k \leq \ker g$. By the Second Isomorphism Theorem, there is a homomorphism $h : \mathrm{FL}(X)/\theta \to \mathcal{M}$ such that $hk = g$, as desired. $\square$

It follows that varieties of lattices are in one-to-one correspondence with fully invariant congruences on $\mathrm{FL}(\omega)$. The consequences of this fact can be summarized as follows.

Theorem 7.3. *The set of all lattice varieties ordered by containment forms a lattice Λ that is dually isomorphic to the lattice of all fully invariant congruences of* $\mathrm{FL}(\omega)$. *Thus Λ is dually algebraic, and a variety $\mathbf{V}$ is dually compact in Λ if and only if $\mathbf{V} = V(\Sigma)$ for some finite set of equations Σ.*

Going back to statement (2) of Theorem 7.1, the third way of looking at varieties is model theoretic: a variety is a class of lattices closed under the operators H (homomorphic images), S (sublattices) and P (direct products). Now elementary arguments show that, for any class $\mathbf{K}$,

$$\begin{aligned} \mathrm{PS}(\mathbf{K}) &\subseteq \mathrm{SP}(\mathbf{K}) \\ \mathrm{PH}(\mathbf{K}) &\subseteq \mathrm{HP}(\mathbf{K}) \\ \mathrm{SH}(\mathbf{K}) &\subseteq \mathrm{HS}(\mathbf{K}). \end{aligned}$$

Thus the smallest variety containing a class $\mathbf{K}$ of lattices is $\mathrm{HSP}(\mathbf{K})$, the class of all homomorphic images of sublattices of direct products of lattices in $\mathbf{K}$. We refer to $\mathrm{HSP}(\mathbf{K})$ as the variety *generated by* $\mathbf{K}$. We can think of HSP as a closure operator, but not an algebraic one: Λ is not upper continuous, so it cannot be algebraic (see Exercise 6). The many advantages of this point of view will soon become apparent.

Lemma 7.4. *Two lattice varieties are equal if and only if they contain the same subdirectly irreducible lattices.*

Proof. Recall from Theorem 5.6 that every lattice $\mathcal{L}$ is a subdirect product of subdirectly irreducible lattices $\mathcal{L}/\varphi$ with φ completely meet irreducible in $\mathbf{Con}\ \mathcal{L}$. Suppose $\mathbf{V}$ and $\mathbf{K}$ are varieties, and that the subdirectly irreducible lattices of $\mathbf{V}$ are all in $\mathbf{K}$. Then for any X the relatively free lattice $\mathcal{F}_{\mathbf{V}}(X)$, being a subdirect product of subdirectly irreducible lattices $\mathcal{F}_{\mathbf{V}}(X)/\varphi$ in $\mathbf{V}$, is a subdirect product of lattices in $\mathbf{K}$. Hence $\mathcal{F}_{\mathbf{V}}(X) \in \mathbf{K}$ and $\mathbf{V} \subseteq \mathbf{K}$. The lemma follows by symmetry. $\square$

This leads us directly to a crucial question: *If* $\mathbf{K}$ *is a set of lattices, how can we find the subdirectly irreducible lattices in* $\mathrm{HSP}(\mathbf{K})$*?* The answer, due to Bjarni Jónsson, requires that we once again venture into the world of logic.

Let us recall that a *filter* (or *dual ideal*) of a lattice $\mathcal{L}$ with greatest element 1 is a subset F of L such that

(1) $1 \in F$,
(2) $x, y \in F$ implies $x \wedge y \in F$,
(3) $z \geq x \in F$ implies $z \in F$.

For any $x \in L$, the set $\uparrow x$ is called a *principal filter*. As an example of a nonprincipal filter, in the lattice $\mathfrak{P}(X)$ of all subsets of an infinite set X we have the filter F of all complements of finite subsets of X. A maximal proper filter is called an *ultrafilter*.

We want to describe an important type of congruence relation on direct products. Let $\mathcal{L}_i$ $(i \in I)$ be lattices, and let F be a filter on the lattice of subsets $\mathfrak{P}(I)$. We define an equivalence relation $\equiv_F$ on the direct product $\prod_{i \in I} \mathcal{L}_i$ by

$$x \equiv_F y \text{ if } \{i \in I : x_i = y_i\} \in F.$$

A routine check shows that $\equiv_F$ is a congruence relation.

Lemma 7.5. *(1) Let $\mathcal{L}$ be a lattice, F a filter on $\mathcal{L}$, and $a \notin F$. Then there exists a filter G on $\mathcal{L}$ maximal with respect to the properties $F \subseteq G$ and $a \notin G$.*

(2) A proper filter U on $\mathfrak{P}(I)$ is an ultrafilter if and only if for every $A \subseteq I$, either $A \in U$ or $I - A \in U$.

(3) If U is an ultrafilter on $\mathfrak{P}(I)$, then its complement $\mathfrak{P}(I) - U$ is a maximal proper ideal.

(4) If U is an ultrafilter and $A_1 \cup \cdots \cup A_n \in U$, then $A_i \in U$ for some i.

(5) An ultrafilter U is nonprincipal if and only if it contains the filter of all complements of finite subsets of I.

Proof. Part (1) is a straightforward Zorn's Lemma argument. Moreover, it is clear that a proper filter U is maximal if and only if for every $A \notin U$ there exists $B \in U$ such that $A \cap B = \emptyset$, i.e., $B \subseteq I - A$. For if F is a filter and A is a subset of I with the property that $A \notin F$ and $A \cap B \neq \emptyset$ for all $B \in F$, then the filter G generated by $F \cup \{A\}$ does not contain $\emptyset$, and $G \supset F$ properly. Thus U is an ultrafilter if and only if $A \notin U$ implies $I - A \in U$, which is (2). DeMorgan's Laws then yield (3), which in turn implies (4). It follows from (4) that if an ultrafilter U on I contains a finite set, then it contains a singleton $\{i_0\}$, and hence is principal with $U = \uparrow \{i_0\} = \{A \subseteq I : i_0 \in A\}$. Conversely, if U is a principal ultrafilter $\uparrow S$, then S must be a singleton. Thus an ultrafilter is nonprincipal if and only if it contains no finite set, which by (2) means that it contains the complement of every finite set. □

Corollary. *If I is an infinite set, then there is a nonprincipal ultrafilter on $\mathfrak{P}(I)$.*

Proof. Apply Lemma 7.5(1) with $\mathcal{L} = \mathfrak{P}(I)$, F the filter of all complements of finite subsets of I, and $a = \emptyset$. □

If F is a filter on $\mathfrak{P}(I)$, the quotient lattice $\prod_{i \in I} \mathcal{L}_i / \equiv_{\mathrm{F}}$ is called a *reduced product*. If U is an ultrafilter, then $\prod_{i \in I} \mathcal{L}_i / \equiv_{\mathrm{U}}$ is an *ultraproduct*. The interesting case is when U is a nonprincipal ultrafilter. Good references on reduced products and ultraproducts are [3] and [8].

Our next immediate goal is to investigate what properties are preserved by the ultraproduct construction. In order to be precise, we begin with a slough of definitions, reserving comment for later.

The elements of a *first order language* for lattices are

(1) a countable alphabet X with members denoted $x, y, z, \dots$,
(2) equations $p \approx q$ with $p, q \in W(X)$,
(3) logical connectives AND, OR, and $\neg$,
(4) quantifiers $\forall x$ and $\exists x$ for all $x \in X$.

These symbols can be combined appropriately to form *well formed formulas* (wffs) by the following rules.

(1) Every equation $p \approx q$ is a wff.
(2) If α and β are wffs, then so are $(\neg\alpha)$, $(\alpha \text{ AND } \beta)$ and $(\alpha \text{ OR } \beta)$.
(3) If γ is a wff and $x \in X$, then $(\forall x\gamma)$ and $(\exists x\gamma)$ are wffs.
(4) Only expressions generated by the first three rules are wffs.

Now let $\mathcal{L}$ be a lattice, let $h : W(X) \to \mathcal{L}$ be a homomorphism, and let φ be a well formed formula. We say that the pair $(\mathcal{L}, h)$ *models* φ, written symbolically as $(\mathcal{L}, h) \models \varphi$, according to the following recursive definition. By way of notation, for $g : W(X) \to \mathcal{L}$ and $Y \subseteq X$, $g|_Y$ denotes the restriction of g to Y.

(1) $(\mathcal{L}, h) \models p \approx q$ if $h(p) = h(q)$, i.e., if $p(h(x_1), \dots, h(x_n)) = q(h(x_1), \dots, h(x_n))$.
(2) $(\mathcal{L}, h) \models (\neg\alpha)$ if $(\mathcal{L}, h)$ does not model α (written $(\mathcal{L}, h) \not\models \alpha$).
(3) $(\mathcal{L}, h) \models (\alpha \text{ AND } \beta)$ if $(\mathcal{L}, h) \models \alpha$ and $(\mathcal{L}, h) \models \beta$.

(4) $(\mathcal{L}, h) \models (\alpha \text{ OR } \beta)$ if $(\mathcal{L}, h) \models \alpha$ or $(\mathcal{L}, h) \models \beta$ (or both).
(5) $(\mathcal{L}, h) \models (\forall x\gamma)$ if $(\mathcal{L}, g) \models \gamma$ for every g such that $g|_{X-\{x\}} = h|_{X-\{x\}}$.
(6) $(\mathcal{L}, h) \models (\exists x\gamma)$ if $(\mathcal{L}, g) \models \gamma$ for some g such that $g|_{X-\{x\}} = h|_{X-\{x\}}$.

Finally, $\mathcal{L}$ *satisfies* φ if $(\mathcal{L}, h)$ models φ for every homomorphism $h : W(X) \to \mathcal{L}$.

We are particularly interested in well formed formulas φ for which all the variables appearing in φ are quantified (by $\forall$ or $\exists$). The set F_φ of variables that *occur freely in* φ is defined recursively as follows.

(1) For an equation, $F_{p\approx q}$ is the set of all variables that actually appear in p or q.
(2) $F_{\neg\alpha} = F_\alpha$.
(3) $F_{\alpha \text{ AND } \beta} = F_\alpha \cup F_\beta$.
(4) $F_{\alpha \text{ OR } \beta} = F_\alpha \cup F_\beta$.
(5) $F_{\forall x\alpha} = F_\alpha - \{x\}$.
(6) $F_{\exists x\alpha} = F_\alpha - \{x\}$.

A *first order sentence* is a well formed formula φ such that F_φ is empty, i.e., no variable occurs freely in φ. It is not hard to show inductively that, for a given lattice $\mathcal{L}$ and any well formed formula φ, whether or not $(\mathcal{L}, h) \models \varphi$ is true depends only on the values of $h|_{F_\varphi}$, i.e., if $g|_{F_\varphi} = h|_{F_\varphi}$, then $(\mathcal{L}, g) \models \varphi$ iff $(\mathcal{L}, h) \models \varphi$. So if φ is a sentence, then either $\mathcal{L}$ satisfies φ or $\mathcal{L}$ satisfies $\neg\varphi$.

Now some comments are in order. First of all, we did not include the predicate $p \leq q$ because we can capture it with the equation $p \vee q \approx q$. Likewise, the logical connective $\Longrightarrow$ is omitted because $(\alpha \Longrightarrow \beta)$ is equivalent to $(\neg\alpha)$ OR β. On the other hand, our language is redundant because OR can be eliminated by the use of DeMorgan's law, and $\exists x\varphi$ is equivalent to $\neg\forall x(\neg\varphi)$.

Secondly, for any well formed formula φ, a lattice $\mathcal{L}$ satisfies φ if and only if it satisfies the sentence $\forall x_{i_1} \dots \forall x_{i_k}\varphi$ where the quantification runs over the variables in F_φ. Thus we can consistently speak of a lattice satisfying an equation or Whitman's condition, for example, when what we really have in mind is the corresponding universally quantified sentence.

Fortunately, our intuition about what sort of properties can be expressed as first order sentences, and what it means for a lattice to satisfy a sentence φ, tends to be pretty good, particularly after we have seen a lot of examples. With this in mind, let us list some first order properties.

(1) $\mathcal{L}$ satisfies $p \approx q$.
(2) $\mathcal{L}$ satisfies the semidistributive laws $(SD_\vee)$ and $(SD_\wedge)$.
(3) $\mathcal{L}$ satisfies Whitman's condition (W).
(4) $\mathcal{L}$ has width 7.
(5) $\mathcal{L}$ has at most 7 elements.
(6) $\mathcal{L}$ has exactly 7 elements.
(7) $\mathcal{L}$ is isomorphic to $\mathcal{M}_5$.

And, of course, we can do negations and finite conjunctions and disjunctions of these. The sort of things that *cannot* be expressed by first order sentences includes the following.

(1) $\mathcal{L}$ is finite.
(2) $\mathcal{L}$ satisfies the ACC.
(3) $\mathcal{L}$ has finite width.
(4) $\mathcal{L}$ is subdirectly irreducible.

Now we are in a position to state for lattices the fundamental theorem about ultraproducts, due to J. Łos in 1955 [14].

Theorem 7.6. *Let φ be a first order lattice sentence, $\mathcal{L}_i$ $(i \in I)$ lattices, and U an ultrafilter on $\mathfrak{P}(I)$. Then the ultraproduct $\prod_{i\in I} \mathcal{L}_i/\equiv_{\mathrm{U}}$ satisfies φ if and only if $\{i \in I : \mathcal{L}_i$ satisfies $\varphi\}$ is in U.*

Corollary. *If each $\mathcal{L}_i$ satisfies φ, then so does the ultraproduct $\prod_{i\in I} \mathcal{L}_i/\equiv_{\mathrm{U}}$.*

Proof. Suppose we have a collection of lattices $\mathcal{L}_i$ $(i \in I)$ and an ultrafilter U on $\mathfrak{P}(I)$. The elements of the ultraproduct $\prod_{i\in I} \mathcal{L}_i/\equiv_{\mathrm{U}}$ are equivalence classes of elements of the direct product. Let $\mu : \prod \mathcal{L}_i \to \prod \mathcal{L}_i/\equiv_{\mathrm{U}}$ be the canonical homomorphism, and let $\pi_j : \prod \mathcal{L}_i \to \mathcal{L}_j$ denote the projection map. We will prove the following claim, which includes Theorem 7.6.

Claim. *Let $h : W(X) \to \prod_{i\in I} \mathcal{L}_i$ be a homomorphism, and let φ be a well formed formula. Then $(\prod \mathcal{L}_i/\equiv_{\mathrm{U}}, \mu h) \models \varphi$ if and only if $\{i \in I : (\mathcal{L}_i, \pi_i h) \models \varphi\} \in U$.*

We proceed by induction on the complexity of φ. In view of the observations above (e.g., DeMorgan's Laws), it suffices to treat equations, AND, $\neg$ and $\forall$. The first three are quite straightforward.

Note that for $a, b \in \prod \mathcal{L}_i$ we have $\mu(a) = \mu(b)$ if and only if $\{i : \pi_i(a) = \pi_i(b)\} \in U$. Thus, for an equation $p \approx q$, we have

$$\begin{aligned}
(\prod \mathcal{L}_i/\equiv_{\mathrm{U}}, \mu h) \models p \approx q \quad &\text{iff} \quad \mu h(p) = \mu h(q) \\
&\text{iff} \quad \{i : \pi_i h(p) = \pi_i h(q)\} \in U \\
&\text{iff} \quad \{i : (\mathcal{L}_i, \pi_i h) \models p \approx q\} \in U.
\end{aligned}$$

.

For a conjunction α AND β, using $A \cap B \in U$ iff $A \in U$ and $B \in U$, we have

$$\begin{aligned}
(\prod \mathcal{L}_i/\equiv_{\mathrm{U}}, \mu h) \models \alpha \text{ AND } \beta \text{ iff } &(\prod \mathcal{L}_i/\equiv_{\mathrm{U}}, \mu h) \models \alpha \text{ and } (\prod \mathcal{L}_i/\equiv_{\mathrm{U}}, \mu h) \models \beta \\
\text{iff } &\{i : (\mathcal{L}_i, \pi_i h) \models \alpha\} \in U \text{ and } \{i : (\mathcal{L}_i, \pi_i h) \models \beta\} \in U \\
\text{iff } &\{i : (\mathcal{L}_i, \pi_i h) \models \alpha \text{ AND } \beta\} \in U.
\end{aligned}$$

.

For a negation $\neg\alpha$, using the fact that $A \in U$ iff $I - A \notin U$, we have

$$\begin{aligned}(\prod \mathcal{L}_i/\equiv_{\mathrm{U}}, \mu h) \models \neg\alpha \quad &\text{iff} \quad (\prod \mathcal{L}_i/\equiv_{\mathrm{U}}, \mu h) \not\models \alpha \\ &\text{iff} \quad \{i : (\mathcal{L}_i, \pi_i h) \models \alpha\} \notin U \\ &\text{iff} \quad \{j : (\mathcal{L}_j, \pi_j h) \not\models \alpha\} \in U \\ &\text{iff} \quad \{j : (\mathcal{L}_j, \pi_j h) \models \neg\alpha\} \in U.\end{aligned}$$

.

Finally, we consider the case when φ has the form $\forall x\gamma$. First, assume $A = \{i : (\mathcal{L}_i, \pi_i h) \models \forall x\gamma\} \in U$, and let $g : W(X) \to \prod \mathcal{L}_i$ be a homomorphism such that $\mu g|_{X-\{x\}} = \mu h|_{X-\{x\}}$. This means that for each $y \in X - \{x\}$, the set $B_y = \{j : \pi_j g(y) = \pi_j h(y)\} \in U$. Since F_γ is a finite set and U is closed under intersection, it follows that $B = \bigcap_{y \in F_\gamma - \{x\}} B_y = \{j : \pi_j g(y) = \pi_j h(y) \text{ for all } y \in F_\gamma - \{x\}\} \in U$. Therefore $A \cap B = \{i : (\mathcal{L}_i, \pi_i h) \models \forall x\gamma \text{ and } \pi_i g|_{F_\gamma - \{x\}} = \pi_i h|_{F_\gamma - \{x\}}\} \in U$. Hence $\{i : (\mathcal{L}_i, \pi_i g) \models \gamma\} \in U$, and so by induction $(\prod \mathcal{L}_i/\equiv_{\mathrm{U}}, \mu g) \models \gamma$. Thus $(\prod \mathcal{L}_i/\equiv_{\mathrm{U}}, \mu h) \models \forall x\gamma$, as desired.

Conversely, suppose $A = \{i : (\mathcal{L}_i, \pi_i h) \models \forall x\gamma\} \notin U$. Then the complement $I - A = \{j : (\mathcal{L}_j, \pi_j h) \not\models \forall x\gamma\} \in U$. For each $j \in I - A$, there is a homomorphism $g_j : W(X) \to \mathcal{L}_j$ such that $g_j|_{X-\{x\}} = \pi_j h|_{X-\{x\}}$ and $(L_j, g_j) \not\models \gamma$. Let $g : W(X) \to \prod \mathcal{L}_i$ be a homomorphism such that $\pi_j g = g_j$ for all $j \in I - A$. Then $\mu g|_{X-\{x\}} = \mu h|_{X-\{x\}}$ but $(\prod \mathcal{L}_i/\equiv_{\mathrm{U}}, \mu g) \not\models \gamma$. Thus $(\prod \mathcal{L}_i/\equiv_{\mathrm{U}}, \mu h) \not\models \forall x\gamma$.

This completes the proof of Lemma 7.6. $\square$

To our operators H, S and P let us add a fourth: $\mathrm{P_u}(\mathbf{K})$ is the class of all ultraproducts of lattices from $\mathbf{K}$. Finally we get to answer the question: *Where do subdirectly irreducibles come from?*

Theorem 7.7. Jónsson's Lemma. *Let* $\mathbf{K}$ *be a class of lattices. If* $\mathcal{L}$ *is subdirectly irreducible and* $\mathcal{L} \in \mathrm{HSP}(\mathbf{K})$, *then* $\mathcal{L} \in \mathrm{HSP_u}(\mathbf{K})$.

Proof. Now $\mathcal{L} \in \mathrm{HSP}(\mathbf{K})$ means that there are lattices $\mathcal{K}_i \in \mathbf{K}$ $(i \in I)$, a sublattice $\mathcal{S}$ of $\prod_{i \in I} \mathcal{K}_i$, and a surjective homomorphism $h : \mathcal{S} \twoheadrightarrow \mathcal{L}$. If we also assume that $\mathcal{L}$ is finitely subdirectly irreducible (this suffices), then $\ker h$ is meet irreducible in $\mathbf{Con}\,\mathcal{S}$. Since $\mathbf{Con}\,\mathcal{S}$ is distributive, this makes $\ker h$ meet prime, i.e., $\varphi \wedge \psi \leq \ker h$ implies $\varphi \leq \ker h$ or $\psi \leq \ker h$.

For any $J \subseteq I$, let π_J be the kernel of the projection of $\mathcal{S}$ onto $\prod_{j \in J} \mathcal{K}_j$. Thus for a, $b \in S$ we have $a \;\pi_J\; b$ iff $a_j = b_j$ for all $j \in J$. Note that $H \supseteq J$ implies $\pi_H \leq \pi_J$, and that $\pi_{J \cup K} = \pi_J \wedge \pi_K$.

Let $\mathfrak{H} = \{J \subseteq I : \pi_J \leq \ker h\}$. By the preceding observations,

(1) $I \in \mathfrak{H}$ and $\emptyset \notin \mathfrak{H}$,
(2) $\mathfrak{H}$ is an order filter in $\mathfrak{P}(I)$,
(3) $J \cup K \in \mathfrak{H}$ implies $J \in \mathfrak{H}$ or $K \in \mathfrak{H}$.

However, $\mathfrak{H}$ need not be a (lattice) filter. Let us therefore consider

$$\mathcal{Q} = \{F \subseteq \mathfrak{P}(I) : F \text{ is a filter on } \mathfrak{P}(I) \text{ and } F \subseteq \mathfrak{H}\}.$$

By Zorn's Lemma, $\mathcal{Q}$ contains a maximal member with respect to set inclusion, say U. Let us show that U is an ultrafilter.

If not, then by Lemma 7.5(2) there exists $A \subseteq I$ such that A and $I - A$ are both not in U. By the maximality of U, this means that there exists a subset $X \in U$ such that $A \cap X \notin \mathfrak{H}$. Similarly, there is a $Y \in U$ such that $(I - A) \cap Y \notin \mathfrak{H}$. Let $Z = X \cap Y$. Then $Z \in U$, and hence $Z \in \mathfrak{H}$. However, $A \cap Z \subseteq A \cap X$, whence $A \cap Z \notin \mathfrak{H}$ by (2) above. Likewise $(I - A) \cap Z \notin \mathfrak{H}$. But

$$(A \cap Z) \cup ((I - A) \cap Z) = Z \in \mathfrak{H},$$

contradicting (3). Thus U is an ultrafilter.

Now $\equiv_U \in$ **Con** $\prod \mathcal{K}_i$, and its restriction is a congruence on $\mathcal{S}$. Moreover, $\mathcal{S}/\equiv_{\mathrm{U}}$ is (isomorphic to) a sublattice of $\prod \mathcal{K}_i/\equiv_{\mathrm{U}}$. If a, b are any pair of elements of $\mathcal{S}$ such that $a \equiv_U b$, then $J = \{i : a_i = b_i\} \in U$. This implies $J \in \mathfrak{H}$ and so $\pi_J \leq \ker h$, whence $h(a) = h(b)$. Thus the restriction of $\equiv_U$ to $\mathcal{S}$ is below $\ker h$, wherefore $\mathcal{L} = h(\mathcal{S})$ is a homomorphic image of $\mathcal{S}/\equiv_{\mathrm{U}}$. We conclude that $\mathcal{L} \in \mathrm{HSP_u}(\mathbf{K})$. $\square$

The proof of Jónsson's Lemma [12] uses the distributivity of **Con** $\mathcal{L}$ in a crucial way, and its conclusion is not generally true for varieties of algebras that do not have distributive congruence lattices. This means that varieties of lattices are more well-behaved than varieties of other algebras, such as groups and rings. The applications below will indicate some aspects of this.

Lemma 7.8. *Let U be an ultrafilter on $\mathfrak{P}(I)$ and $J \in U$. Then $V = \{B \subseteq J : B \in U\}$ is an ultrafilter on $\mathfrak{P}(J)$, and $\prod_{j \in J} \mathcal{L}_j/\equiv_{\mathrm{V}}$ is isomorphic to $\prod_{i \in I} \mathcal{L}_i/\equiv_{\mathrm{U}}$.*

Proof. V is clearly a proper filter. Moreover, if $A \subseteq J$ and $A \notin V$, then $I - A \in U$ and hence $J - A = J \cap (I - A) \in U$. It follows by Lemma 7.5(2) that V is an ultrafilter.

The projection $\rho_J : \prod_{i \in I} \mathcal{L}_i \twoheadrightarrow \prod_{j \in J} \mathcal{L}_j$ is a surjective homomorphism. As $A \cap J \in U$ if and only if $A \in U$, it induces a (well defined) isomorphism of $\prod_{i \in I} \mathcal{L}_i/\equiv_{\mathrm{U}}$ onto $\prod_{j \in J} \mathcal{L}_j/\equiv_{\mathrm{V}}$. $\square$

Theorem 7.9. *Let $\mathbf{K} = \{\mathcal{K}_1, \ldots, \mathcal{K}_n\}$ be a finite collection of finite lattices. If $\mathcal{L}$ is a subdirectly irreducible lattice in the variety* $\mathrm{HSP}(\mathbf{K})$*, then $\mathcal{L} \in \mathrm{HS}(\mathcal{K}_j)$ for some j.*

Proof. By Jónsson's Lemma, $\mathcal{L}$ is a homomorphic image of a sublattice of an ultraproduct $\prod_{i \in I} \mathcal{L}_i/\equiv_{\mathrm{U}}$ with each $\mathcal{L}_i$ isomorphic to one of $\mathcal{K}_1, \ldots, \mathcal{K}_n$. Let $A_j = \{i \in I : \mathcal{L}_i \cong \mathcal{K}_j\}$. As $A_1 \cup \cdots \cup A_n = I \in U$, by Lemma 7.5(4) there is a j such that $A_j \in U$. But then Lemma 7.8 says that there is an ultrafilter V on $\mathfrak{P}(A_j)$ such that the original ultraproduct is isomorphic to $\prod_{k \in A_j} \mathcal{L}_k / \equiv_{\mathrm{V}}$, wherein each $\mathcal{L}_k \cong K_j$. However, for any finite lattice $\mathcal{K}$ there is a first order sentence $\varphi_{\mathcal{K}}$ such that a lattice $\mathcal{M}$ satisfies $\varphi_{\mathcal{K}}$ if and only if $\mathcal{M} \cong \mathcal{K}$. Therefore, by Łos' Theorem, $\prod_{k \in A_j} \mathcal{L}_k / \equiv_{\mathrm{V}}$ is isomorphic to $\mathcal{K}_j$. Hence $\mathcal{L} \in HS(\mathcal{K}_j)$, as claimed. $\square$

Since a variety is determined by its subdirectly irreducible members, we have the following consequence.

Corollary. *If* $\mathbf{V} = \mathrm{HSP}(\mathbf{K})$ *where* $\mathbf{K}$ *is a finite collection of finite lattices, then* $\mathbf{V}$ *contains only finitely many subvarieties.*

Note that $\mathrm{HSP}(\{\mathcal{K}_1, \ldots, \mathcal{K}_n\}) = \mathrm{HSP}(\mathcal{K}_1 \times \cdots \times \mathcal{K}_n)$, so w.l.o.g. we can talk about the variety generated by a single finite lattice. The author has shown that the converse of the Corollary is false [18]: *There is an infinite, subdirectly irreducible lattice* $\mathcal{L}$ *such that* $\mathrm{HSP}(\mathcal{L})$ *has only finitely many subvarieties, each of which is generated by a finite lattice.*

There are many other consequences of Jónsson's Lemma, especially for varieties of modular lattices. Many contributors combined to develop an elegant theory of lattice varieties, which we will not attempt to survey. The standard reference on the subject is the book of Peter Jipsen and Henry Rose [11].

Let us call a variety $\mathbf{V}$ *finitely based* if $\mathbf{V} = V(\Sigma)$ for some finite set of equations Σ. These are just the varieties that are dually compact in the lattice Λ of lattice varieties. Ralph McKenzie [15] proved the following nice result.

Theorem 7.10. *The variety generated by a finite lattice is finitely based.*

Kirby Baker [1] generalized this result by showing that if $\mathcal{A}$ is any finite algebra in a variety $\mathbf{V}$ such that (i) $\mathbf{V}$ has only finitely many operation symbols, and (ii) the congruence lattices of algebras in $\mathbf{V}$ are distributive, then $\mathrm{HSP}(\mathcal{A})$ is finitely based. It is also true that the variety generated by a finite group is finitely based (S. Oates and M. B. Powell [19]), and likewise the variety generated by a finite ring (R. Kruse [13]). See R. McKenzie [16] for a common generalization of these finite basis theorems. There are many natural examples of finite algebras that do not generate a finitely based variety; see, e.g., G. McNulty [17]. A good survey of finite basis results is R. Willard [20].

We will return to the varieties generated by some particular finite lattices in the next chapter.

If $\mathbf{V}$ is a lattice variety, let $\mathbf{V}_{si}$ be the class of subdirectly irreducible lattices in $\mathbf{V}$. The next result is proved by a straightforward modification of the first part of the proof of Theorem 7.9.

Theorem 7.11. *If* $\mathbf{V}$ *and* $\mathbf{W}$ *are lattice varieties, then* $(\mathbf{V} \vee \mathbf{W})_{si} = \mathbf{V}_{si} \cup \mathbf{W}_{si}$.

Corollary. Λ *is distributive.*

Theorem 7.11 does not extend to infinite joins. For example, finite lattices generate the variety of all lattices (see Exercise 6) but there are infinite subdirectly irreducible lattices. We already knew the Corollary by Theorem 7.3, because Λ is dually isomorphic to a sublattice of **Con** FL(ω), which is distributive, but this provides an interesting way of looking at it.

In closing let us consider the lattice $\mathcal{I}(\mathcal{L})$ of ideals of $\mathcal{L}$. An elementary argument shows that the map $x \to \downarrow x$ embeds $\mathcal{L}$ into $\mathcal{I}(\mathcal{L})$. A classic theorem of Garrett Birkhoff [4] says that $\mathcal{I}(\mathcal{L})$ satisfies every identity satisfied by $\mathcal{L}$, i.e., $\mathcal{I}(\mathcal{L}) \in \mathrm{HSP}(\mathcal{L})$. The following result of Kirby Baker and Alfred Hales [2] goes one better.

Theorem 7.12. *For any lattice $\mathcal{L}$, we have $\mathcal{I}(\mathcal{L}) \in \mathrm{HSP_u}(\mathcal{L})$.*

This is an ideal place to stop.

Exercises for Chapter 7

1. Show that fully invariant congruences form a complete sublattice of **Con** $\mathcal{L}$.

2. Let $\mathcal{L}$ be a lattice and **V** a lattice variety. Show that there is a unique minimum congruence $\rho_{\mathbf{V}}$ on $\mathcal{L}$ such that $\mathcal{L}/\rho_{\mathbf{V}} \in \mathbf{V}$.

3. (a) Prove that if $\mathcal{L}$ is a subdirectly irreducible lattice, then HSP($\mathcal{L}$) is (finitely) join irreducible in the lattice Λ of lattice varieties.

(b) Prove that if a variety **V** is completely join irreducible in Λ, then $\mathbf{V} = \mathrm{HSP}(\mathcal{K})$ for some finitely generated, subdirectly irreducible lattice $\mathcal{K}$.

4. Show that if F is a filter on $\mathfrak{P}(I)$, then $\equiv_F$ is a congruence relation on $\prod_{i\in I} \mathcal{L}_i$.

5. (a) Show that if F is a filter on $\mathfrak{P}(I)$, then F is the intersection of the ultrafilters U such that $U \supseteq F$.

(b) Then prove that the congruence $\equiv_F$ on $\prod_{i\in I} \mathcal{L}_i$ is the intersection of congruences $\equiv_U$ with U an ultrafilter.

(c) Conclude that the reduced product $\prod_{i\in I} \mathcal{L}_i/\equiv_F$ is a subdirect product of ultraproducts $\prod_{i\in I} \mathcal{L}_i/\equiv_U$.

6. Prove that every lattice equation that does not hold in all lattices fails in some finite lattice. (Let $p \neq q$ in FL(X). Then there exist a finite join subsemilattice $\mathcal{S}$ of FL(X) containing p, q and $0 = \bigwedge X$, and a lattice homomorphism $h : \mathrm{FL}(X) \to \mathcal{S}$, such that $h(p) = p$ and $h(q) = q$.)

The standard solution to Exercise 6 involves lattices which turn out to be lower bounded (see Exercise 11 of Chapter 6). Hence they satisfy $\mathrm{SD}_\vee$, and any finite collection of them generates a variety not containing $\mathcal{M}_3$, while all together they generate the variety of all lattices. On the other hand, the variety generated by $\mathcal{M}_3$ contains only the variety **D** of distributive lattices (generated by **2**) and the trivial variety **T**. It follows that the lattice Λ of lattice varieties is not join continuous.

7. Give a first order sentence characterizing each of the following properties of a lattice $\mathcal{L}$ (i.e., $\mathcal{L}$ has the property iff $\mathcal{L} \models \varphi$).

(a) $\mathcal{L}$ has a least element.
(b) $\mathcal{L}$ is atomic.
(c) $\mathcal{L}$ is strongly atomic.

(d) $\mathcal{L}$ is weakly atomic.
(e) $\mathcal{L}$ has no covering relations.

8. A lattice $\mathcal{L}$ has *breadth* n if L contains n elements whose join is irredundant, but every join of $n+1$ elements of L is redundant.

(a) Give a first order sentence characterizing lattices of breadth n (for a fixed finite integer $n \geq 1$).
(b) Show that the class of lattices of breadth $\leq n$ is not a variety.
(c) Show that a lattice $\mathcal{L}$ and its dual $\mathcal{L}^d$ have the same breadth.

9. Give a first order sentence φ such that a lattice $\mathcal{L}$ satisfies φ if and only if $\mathcal{L}$ is isomorphic to the four element lattice $\mathbf{2} \times \mathbf{2}$.

10. Prove Theorem 7.11.

11. Prove that $\mathcal{I}(\mathcal{L})$ is distributive if and only if $\mathcal{L}$ is distributive. Similarly, show that $\mathcal{I}(\mathcal{L})$ is modular if and only if $\mathcal{L}$ is modular.

References

1. K. Baker, *Finite equational bases for finite algebras in a congruence-distributive equational class*, Advances in Math. **24** (1977), 207–243.
2. K. Baker and A. W. Hales, *From a lattice to its ideal lattice*, Algebra Universalis **4** (1974), 250–258.
3. J. L. Bell and A. B. Slomson, *Models and Ultraproducts: an Introduction*, North-Holland, Amsterdam, 1971.
4. G. Birkhoff, *On the lattice theory of ideals*, Bull. Amer. Math. Soc. **40** (1934), 613–619.
5. G. Birkhoff, *On the structure of abstract algebras*, Proc. Cambridge Phil. Soc. **31** (1935), 433–454.
6. R. Dedekind, *Über die drei Moduln erzeugte Dualgruppe*, Math. Annalen **53** (1900), 371–403.
7. T. Evans, *Some connections between residual finiteness, finite embeddability and the word problem*, J. London. Math. Soc. (2) **2** (1969), 399–403.
8. T. Frayne, A. Morel and D. Scott, *Reduced direct products*, Fund. Math. **51** (1962), 195–228.
9. R. Freese, *Free modular lattices*, Trans. Amer. Math. Soc. **261** (1980), 81–91.
10. C. Herrmann, *Uber die von vier Moduln erzeugte Dualgruppe*, Abh. Braunschweig. Wiss. Ges. **33** (1982), 157–159.
11. P. Jipsen and H. Rose, *Varieties of Lattices*, Lecture Notes in Math., vol. 1533, Springer, Berlin-New York, 1991.
12. B. Jónsson, *Algebras whose congruence lattices are distributive*, Math. Scand. **21** (1967), 110–121.
13. R. Kruse, *Identities satisfied by a finite ring*, J. Algebra **26** (1973), 298–318.
14. J. Łos, *Quelques remarques, théorèmes et problèmes sur le classes définissables d'algèbras*, Mathematical interpretations of formal systems, North-Holland, Amsterdam, 1955.
15. R. McKenzie, *Equational bases for lattice theories*, Math. Scand. **27** (1970), 24–38.
16. R. McKenzie, *Finite equational bases for congruence modular varieties*, Algebra Universalis **24** (1987), 224-250.
17. G. McNulty, *How to construct finite algebras which are not finitely based*, Universal Algebra and Lattice Theory (Charleston, S.C., 1984), Lecture Notes in Math., vol. 1149, Springer, Berlin-New York, 1985, pp. 167–174.
18. J. B. Nation, *A counterexample to the finite height conjecture*, Order **13** (1996), 1–9.
19. S. Oates and M. B. Powell, *Identical relations in finite groups*, J. Algebra **1** (1964), 11–39.

20. R. Willard, *The finite basis problem*, Contributions to General Algebra, vol. 15, Heyn, Klagenfurt, 2004, pp. 199–206.

8. Distributive Lattices

Every dog must have his day.

In this chapter and the next we will look at the two most important lattice varieties: distributive and modular lattices. Let us set the context for our study of distributive lattices by considering varieties generated by a single finite lattice. A variety $\mathbf{V}$ is said to be *locally finite* if every finitely generated lattice in $\mathbf{V}$ is finite. Equivalently, $\mathbf{V}$ is locally finite if the relatively free lattice $\mathcal{F}_{\mathbf{V}}(n)$ is finite for every integer $n > 0$.

Theorem 8.1. *If $\mathcal{L}$ is a finite lattice and $\mathbf{V} = \mathrm{HSP}(\mathcal{L})$, then*

$$|\mathcal{F}_{\mathbf{V}}(n)| \leq |L|^{|L|^n}.$$

Hence $\mathrm{HSP}(\mathcal{L})$ *is locally finite.*

Proof. If $\mathbf{K}$ is any collection of lattices and $\mathbf{V} = \mathrm{HSP}(\mathbf{K})$, then $\mathcal{F}_{\mathbf{V}}(X) \cong \mathrm{FL}(X)/\theta$ where θ is the intersection of all homomorphism kernels $\ker f$ such that $f : \mathrm{FL}(X) \to \mathcal{L}$ for some $\mathcal{L} \in \mathbf{K}$. (This is the technical way of saying that $\mathrm{FL}(X)/\theta$ satisfies exactly the equations that hold in every member of $\mathbf{K}$.) When $\mathbf{K}$ consists of a single finite lattice $\{\mathcal{L}\}$ and $|X| = n$, then there are $|L|^n$ distinct mappings of X into L, and hence $|L|^n$ distinct homomorphisms $f_i : \mathrm{FL}(X) \to \mathcal{L}$ $(1 \leq i \leq |L|^n)$.[1] The range of each f_i is a sublattice of $\mathcal{L}$. Hence $\mathcal{F}_{\mathbf{V}}(X) \cong \mathrm{FL}(X)/\theta$ with $\theta = \bigcap \ker f_i$ means that $\mathcal{F}_{\mathbf{V}}(X)$ is a subdirect product of $|L|^n$ sublattices of $\mathcal{L}$, and so a sublattice of the direct product $\prod_{1 \leq i \leq |L|^n} \mathcal{L} = \mathcal{L}^{|L|^n}$, making its cardinality at most $|L|^{|L|^n}$.[2] $\square$

We should note that not every locally finite lattice variety is generated by a finite lattice.

Now it is clear that there is a unique minimum nontrivial lattice variety, *viz.*, the one generated by the two element lattice $\mathbf{2}$, which is isomorphic to a sublattice of any nontrivial lattice. We want to show that $\mathrm{HSP}(\mathbf{2})$ is the variety of all distributive lattices.

Lemma 8.2. *The following lattice equations are equivalent.*

(1) $x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z)$
(2) $x \vee (y \wedge z) \approx (x \vee y) \wedge (x \vee z)$
(3) $(x \vee y) \wedge (x \vee z) \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$

[1] The kernels of distinct homomorphisms need not be distinct, of course, but that is okay.

[2] It is sometimes useful to view this argument constructively: $\mathcal{F}_{\mathbf{V}}(X)$ is the sublattice of $\mathcal{L}^{|L|^n}$ generated by the vectors $\overline{x}$ $(x \in X)$ with $\overline{x}_i = f_i(x)$ for $1 \leq i \leq |L|^n$.

Thus each of these equations determines the variety $\mathbf{D}$ *of all distributive lattices.*

Proof. If (1) holds in a lattice $\mathcal{L}$, then for any x, y, $z \in L$ we have

$$\begin{aligned}(x \vee y) \wedge (x \vee z) &= [(x \vee y) \wedge x] \vee [(x \vee y) \wedge z] \\ &= x \vee (x \wedge z) \vee (y \wedge z) \\ &= x \vee (y \wedge z)\end{aligned}$$

whence (2) holds. Thus (1) implies (2), and dually (2) implies (1).

Similarly, applying (1) to the left hand side of (3) yields the right hand side, so (1) implies (3). Conversely, assume that (3) holds in a lattice $\mathcal{L}$. For $x \geq y$, equation (3) reduces to $x \wedge (y \vee z) = y \vee (x \wedge z)$, which is the modular law, so $\mathcal{L}$ must be modular. Now for arbitrary x, y, z in $\mathcal{L}$, meet x with both sides of (3) and then use modularity to obtain

$$\begin{aligned}x \wedge (y \vee z) &= x \wedge [(x \wedge y) \vee (x \wedge z) \vee (y \wedge z)] \\ &= (x \wedge y) \vee (x \wedge z) \vee (x \wedge y \wedge z) \\ &= (x \wedge y) \vee (x \wedge z)\end{aligned}$$

since $x \geq (x \wedge y) \vee (x \wedge z)$. Thus (3) implies (1). (Note that since (3) is self-dual, the second argument actually makes the first one redundant.) $\square$

In the first Corollary of the next chapter, we will see that a lattice is distributive if and only if it contains neither $\mathcal{N}_5$ nor $\mathcal{M}_3$ as a sublattice. But before that, let us look at the wonderful representation theory of distributive lattices. A few moments reflection on the kernel of a homomorphism $h : \mathcal{L} \twoheadrightarrow \mathbf{2}$ should yield the following conclusions. By a *proper* ideal or filter, we mean one that is neither empty nor the whole lattice.

Lemma 8.3. *Let* $\mathcal{L}$ *be a lattice and* $h : \mathcal{L} \twoheadrightarrow \mathbf{2} = \{0, 1\}$ *a surjective homomorphism. Then* $h^{-1}(0)$ *is a proper ideal of* $\mathcal{L}$*, and* $h^{-1}(1)$ *is a proper filter, and* L *is the disjoint union of* $h^{-1}(0)$ *and* $h^{-1}(1)$.

Conversely, if I *is a proper ideal of* $\mathcal{L}$ *and* F *a proper filter such that* $L = I \dot{\cup} F$ *(disjoint union), then the map* $h : \mathcal{L} \to \mathbf{2}$ *given by*

$$h(x) = \begin{cases} 0 & \text{if } x \in I, \\ 1 & \text{if } x \in F. \end{cases}$$

is a surjective homomorphism.

This raises the question: *When is the complement* $L - I$ *of an ideal a filter?* The answer is easy. A proper ideal I of a lattice $\mathcal{L}$ is said to be *prime* if $x \wedge y \in I$ implies $x \in I$ or $y \in I$. Dually, a proper filter F is *prime* if $x \vee y \in F$ implies $x \in F$ or $y \in F$. It is straightforward that the complement of an ideal I is a filter iff I is a prime ideal iff $L - I$ is a prime filter.

This simple observation allows us to work with prime ideals or prime filters (interchangeably), rather than ideal/filter pairs, and we shall do so.

Theorem 8.4. *Let $\mathcal{D}$ be a distributive lattice, and let $a \not\leq b$ in $\mathcal{D}$. Then there exists a prime filter F with $a \in F$ and $b \notin F$.*

Proof. Now $\uparrow a$ is a filter of $\mathcal{D}$ containing a and not b, so by Zorn's Lemma there is a maximal such filter (with respect to set containment), say M. For any $x \notin M$, the filter generated by x and M must contain b, whence $b \geq x \wedge m$ for some $m \in M$. Suppose x, $y \notin M$, with say $b \geq x \wedge m$ and $b \geq y \wedge n$ where m, $n \in M$. Then by distributivity

$$b \geq (x \wedge m) \vee (y \wedge n) = (x \vee y) \wedge (x \vee n) \wedge (m \vee y) \wedge (m \vee n).$$

The last three terms are in M, so we must have $x \vee y \notin M$. Thus M is a prime filter. $\square$

Now let $\mathcal{D}$ be any distributive lattice, and let $T_{\mathcal{D}} = \{\varphi \in \mathbf{Con}\ \mathcal{D} : \mathcal{D}/\varphi \cong \mathbf{2}\}$. Theorem 8.4 says that if $a \neq b$ in $\mathcal{D}$, then there exists $\varphi \in T_{\mathcal{D}}$ with $(a, b) \notin \varphi$, whence $\bigcap T_{\mathcal{D}} = 0$ in $\mathbf{Con}\ \mathcal{D}$, i.e., $\mathcal{D}$ is a subdirect product of two element lattices.

Corollary. *The two element lattice* $\mathbf{2}$ *is the only subdirectly irreducible distributive lattice. Hence* $\mathbf{D} = \mathrm{HSP}(\mathbf{2})$.

Corollary. $\mathbf{D}$ *is locally finite.*

Another consequence of Theorem 8.4 is that every distributive lattice can be embedded into a lattice of subsets, with set union and intersection as the lattice operations.

Theorem 8.5. *Let $\mathcal{D}$ be a distributive lattice, and let S be the set of all prime filters of $\mathcal{D}$. Then the map $\phi : \mathcal{D} \to \mathfrak{P}(S)$ by*

$$\phi(x) = \{F \in S : x \in F\}$$

is a lattice embedding.

For finite distributive lattices, this representation takes on a particularly nice form. Recall that an element $p \in L$ is said to be *join prime* if it is nonzero and $p \leq x \vee y$ implies $p \leq x$ or $p \leq y$. In a finite lattice, prime filters are necessarily of the form $\uparrow p$ where p is a join prime element.

Theorem 8.6. *Let $\mathcal{D}$ be a finite distributive lattice, and let $J(\mathcal{D})$ denote the ordered set of all nonzero join irreducible elements of $\mathcal{D}$. Then the following are true.*

(1) *Every element of $J(\mathcal{D})$ is join prime.*
(2) *$\mathcal{D}$ is isomorphic to the lattice of order ideals $\mathcal{O}(J(\mathcal{D}))$.*
(3) *Every element $a \in D$ has a unique irredundant join decomposition $a = \bigvee A$ with $A \subseteq J(\mathcal{D})$.*

Proof. In a distributive lattice, every join irreducible element is join prime, because $p \leq x \vee y$ is the same as $p = p \wedge (x \vee y) = (p \wedge x) \vee (p \wedge y)$.

For any finite lattice, the map $\phi : \mathcal{L} \to \mathcal{O}(J(\mathcal{L}))$ given by $\phi(x) = \downarrow x \cap J(\mathcal{L})$ is order preserving (in fact, meet preserving) and one-to-one. To establish the isomorphism of (2), we need to know that for a distributive lattice it is onto. If $\mathcal{D}$ is distributive and I is an order ideal of $J(\mathcal{D})$, then for $p \in J(\mathcal{D})$ we have by (1) that $p \leq \bigvee I$ iff $p \in I$, and hence $I = \phi(\bigvee I)$.

The join decomposition of (3) is then obtained by taking A to be the set of maximal elements of $\downarrow a \cap J(\mathcal{D})$. $\square$

It is clear that the same proof works if $\mathcal{D}$ is an algebraic distributive lattice whose compact elements satisfy the DCC, so that there are enough join irreducibles to separate elements. In Lemma 10.6 we will characterize those distributive lattices isomorphic to $\mathcal{O}(\mathcal{P})$ for some ordered set $\mathcal{P}$.

As an application, we can give a neat description of the free distributive lattice $\mathcal{F}_{\mathbf{D}}(n)$ for any finite n, which we already know to be a finite distributive lattice. Let $X = \{x_1, \ldots, x_n\}$. Now it is not hard to see that any element in a free distributive lattice can be written as a join of meets of generators, $w = \bigvee w_i$ with $w_i = x_{i_1} \wedge \ldots \wedge x_{i_k}$. Another easy argument shows that the meet of a nonempty proper subset of the generators is join prime in $\mathcal{F}_{\mathbf{D}}(X)$; note that $\bigwedge \emptyset = 1$ and $\bigwedge X = 0$ do not count. (See Exercise 3). Thus the set of join irreducible elements of $\mathcal{F}_{\mathbf{D}}(X)$ is isomorphic to the ordered set of nonempty, proper subsets of X, ordered by reverse set inclusion, and the free distributive lattice is isomorphic to the lattice of order ideals of that. As an example, $\mathcal{F}_{\mathbf{D}}(3)$ and its ordered set of join irreducibles are shown in Figure 8.1.

Dedekind [7] showed that $|\mathcal{F}_{\mathbf{D}}(3)| = 18$ and $|\mathcal{F}_{\mathbf{D}}(4)| = 166$. Several other small values are known exactly, and the rest can be obtained in principle, but they grow quickly (see Quackenbush [12]). While there exist more accurate expressions, the simplest estimate is an asymptotic formula due to D. J. Kleitman:

$$\log_2 \, |\mathcal{F}_{\mathbf{D}}(n)| \sim \binom{n}{\lfloor n/2 \rfloor}.$$

The representation by sets of Theorem 8.5 does not preserve infinite joins and meets. The corresponding characterization of complete distributive lattices that have a complete representation as a lattice of subsets is derived from work of Alfred Tarski and S. Papert [11], and was surely known to both of them. An element p of a complete lattice $\mathcal{L}$ is said to be *completely join prime* if $p \leq \bigvee X$ implies $p \leq x$ for some $x \in X$. It is not necessary to assume that $\mathcal{D}$ is distributive in the next theorem, though of course it will turn out to be so.

Theorem 8.7. *Let $\mathcal{D}$ be a complete lattice. There exists a complete lattice embedding $\phi : \mathcal{D} \to \mathcal{P}(X)$ for some set X if and only if $x \not\leq y$ in $\mathcal{D}$ implies there exists a completely join prime element p with $p \leq x$ and $p \not\leq y$.*

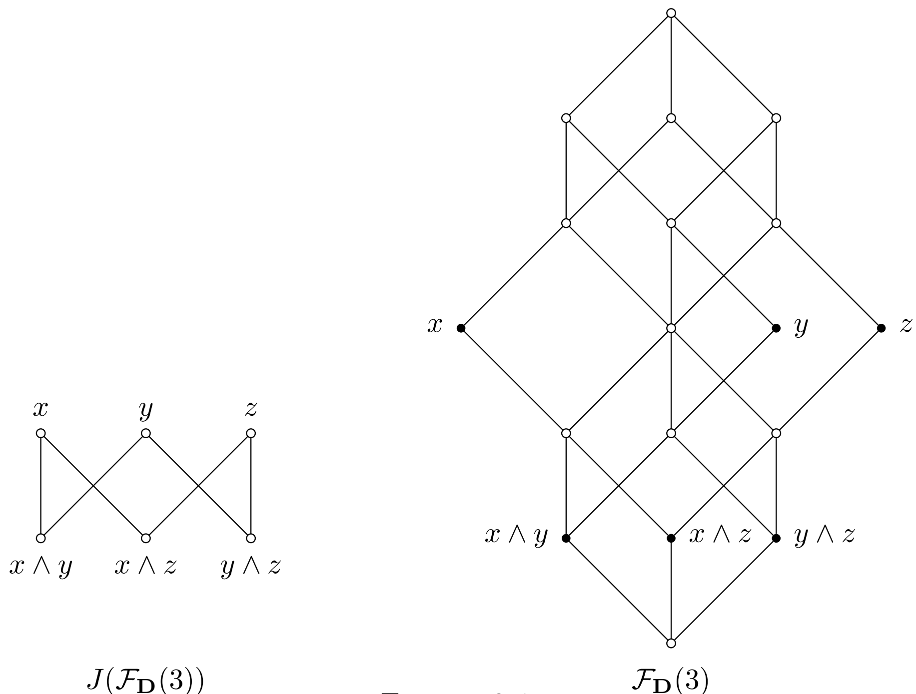


FIGURE 8.1

Thus, for example, the interval $[0, 1]$ in the real numbers is a complete distributive lattice that cannot be represented as a complete lattice of subsets of some set.

In a lattice with 0 and 1, the pair of elements a and b are said to be *complements* if $a \wedge b = 0$ and $a \vee b = 1$. A lattice is *complemented* if every element has at least one complement. For example, the lattice of subspaces of a vector space is a complemented modular lattice. In general, an element can have many complements, but it is not hard to see that each element in a distributive lattice can have at most one complement.

A *Boolean algebra* is a complemented distributive lattice. Of course, the lattice $\mathfrak{P}(X)$ of subsets of a set is a Boolean algebra. On the other hand, it is easy to see that $\mathcal{O}(\mathcal{P})$ is complemented if and only if $\mathcal{P}$ is an antichain, in which case $\mathcal{O}(\mathcal{P}) = \mathfrak{P}(\mathcal{P})$. Thus *every finite Boolean algebra is isomorphic to the lattice* $\mathfrak{P}(A)$ *of subsets of its atoms.*

For a very different example, the finite and cofinite subsets of an infinite set form a Boolean algebra.

If we regard Boolean algebras as algebras $\mathcal{B} = \langle B, \wedge, \vee, 0, 1, ^c \rangle$, then they form a variety, and hence there is a *free Boolean algebra* $\mathrm{FBA}(X)$ generated by a set X. If X is finite, say $X = \{x_1, \ldots, x_n\}$, then $\mathrm{FBA}(X)$ has 2^n atoms, *viz.,* all meets $z_1 \wedge \ldots \wedge z_n$ where each z_i is either x_i or x_i^c. Thus in this case $\mathrm{FBA}(X) \cong \mathfrak{P}(A)$ where $|A| = 2^n$. On the other hand, if X is infinite then $\mathrm{FBA}(X)$ has no atoms;

if $|X| = \aleph_0$, then $\mathrm{FBA}(X)$ is the unique (up to isomorphism) countable atomless Boolean algebra!

Another natural example is the Boolean algebra of all clopen (closed and open) subsets of a topological space. In fact, by adding a topology to the representation of Theorem 8.5, we obtain the celebrated Stone representation theorem for Boolean algebras [15]. Recall that a topological space is *totally disconnected* if for every pair of distinct points x, y there is a clopen set V with $x \in V$ and $y \notin V$.

Theorem 8.8. *Every Boolean algebra is isomorphic to the Boolean algebra of clopen subsets of a compact totally disconnected (Hausdorff) space.*

Proof. Let $\mathcal{B}$ be a distributive lattice. (We will add the other properties to make $\mathcal{B}$ a Boolean algebra as we go along.) Let $\mathfrak{F}_p$ be the set of all prime filters of $\mathcal{B}$, and for $x \in B$ let

$$V_x = \{F \in \mathfrak{F}_p : x \in F\}.$$

The sets V_x will form a basis for the Stone topology on $\mathfrak{F}_p$.

With only trivial changes, the argument for Theorem 8.4 yields the following stronger version.

Sublemma A. *Let $\mathcal{B}$ be a distributive lattice, G a filter on $\mathcal{B}$ and $x \notin G$. Then there exists a prime filter $F \in \mathfrak{F}_p$ such that $G \subseteq F$ and $x \notin F$.*

Next we establish the basic properties of the sets V_x, all of which are easy to prove.

(1) $V_x \subseteq V_y$ iff $x \leq y$.
(2) $V_x \cap V_y = V_{x \wedge y}$.
(3) $V_x \cup V_y = V_{x \vee y}$.
(4) If $\mathcal{B}$ has a least element 0, then $V_0 = \emptyset$. Thus $V_x \cap V_y = \emptyset$ iff $x \wedge y = 0$.
(5) If $\mathcal{B}$ has a greatest element 1, then $V_1 = \mathfrak{F}_p$. Thus $V_x \cup V_y = \mathfrak{F}_p$ iff $x \vee y = 1$.

Property (3) is where we use the primality of the filters in the sets V_x. In particular, the family of sets V_x is closed under finite intersections, and of course $\bigcup_{x \in B} V_x = \mathfrak{F}_p$, so we can legitimately take $\{V_x : x \in B\}$ as a basis for a topology on $\mathfrak{F}_p$.

Now we would like to show that if $\mathcal{B}$ has a largest element 1, then $\mathfrak{F}_p$ is a compact space. It suffices to consider covers by basic open sets, so this follows from the next Sublemma.

Sublemma B. *If $\mathcal{B}$ has a greatest element 1 and $\bigcup_{x \in S} V_x = \mathfrak{F}_p$, then there exists a finite subset $T \subseteq S$ such that $\bigvee T = 1$, and hence $\bigcup_{x \in T} V_x = \mathfrak{F}_p$.*

Proof. Set $I_0 = \{\bigvee T : T \subseteq S,\ T \text{ finite}\}$. If $1 \notin I_0$, then I_0 generates an ideal I of $\mathcal{B}$ with $1 \notin I$. By the dual of Sublemma A, there exists a prime ideal H containing I and not 1. Its complement $B - H$ is a prime filter K. Then $K \notin \bigcup_{x \in S} V_x$, else $z \in K$ for some $z \in S$, whilst $z \in I_0 \subseteq B - K$. This contradicts our hypothesis, so we must have $1 \in I_0$, as claimed. $\square$

The argument thus far has only required that $\mathcal{B}$ be a distributive lattice with 1. For the last two steps, we need $\mathcal{B}$ to be Boolean. Let x^c denote the complement of x in $\mathcal{B}$.

First, note that by properties (4) and (5) above, $V_x \cap V_{x^c} = \emptyset$ and $V_x \cup V_{x^c} = \mathfrak{F}_p$. Thus each set V_x $(x \in B)$ is clopen. On the other hand, let W be a clopen set. As it is open, $W = \bigcup_{x \in S} V_x$ for some set $S \subseteq B$. But W is also a closed subset of the compact space $\mathfrak{F}_p$, and hence compact. Thus $W = \bigcup_{x \in T} V_x = V_{\bigvee T}$ for some finite $T \subseteq S$. Therefore W *is a clopen subset of* $\mathfrak{F}_p$ *if and only if* $W = V_x$ *for some* $x \in B$.

It remains to show that $\mathfrak{F}_p$ is totally disconnected (which makes it Hausdorff). Let F and G be distinct prime filters on $\mathcal{B}$, with say $F \not\subseteq G$. Let $x \in F - G$. Then $F \in V_x$ and $G \notin V_x$, so that V_x is a clopen set containing F and not G. $\square$

There are similar topological representation theorems for arbitrary distributive lattices, the most useful being that due to Hilary Priestley in terms of ordered topological spaces. A good introduction is in Davey and Priestley [6].

In 1880, C. S. Peirce proved that every lattice with the property that each element b has a unique complement b^*, with the additional property that $a \wedge b = 0$ implies $a \leq b^*$, must be distributive, and hence a Boolean algebra. After a good deal of confusion over the axioms of Boolean algebra, the proof was given in a 1904 paper of E. V. Huntington [10]. Huntington then asked whether *every* uniquely complemented lattice must be distributive. It turns out that if we assume almost any additional finiteness condition on a uniquely complemented lattice, then it must indeed be distributive. As an example, there is the following theorem of Garrett Birkhoff and Morgan Ward [5].

Theorem 8.9. *Every complete, atomic, uniquely complemented lattice is isomorphic to the Boolean algebra of all subsets of its atoms.*

Other finiteness restrictions which insure that a uniquely complemented lattice will be distributive include weak atomicity, due to Bandelt and Padmanabhan [4], and upper continuity, due independently to Bandelt [3] and Saliĭ [13], [14]. A monograph written by Saliĭ [16] gives an excellent survey of results of this type.

Nonetheless, Huntington's conjecture is very far from true. In 1945, R. P. Dilworth [8] proved that *every lattice can be embedded in a uniquely complemented lattice.* This result has likewise been strengthened in various ways. See the surveys of Mick Adams [1] and George Grätzer [9].

The standard book for distributive lattices is by R. Balbes and Ph. Dwinger [2]. Though somewhat dated, it contains much of interest.

Exercises for Chapter 8

1. Show that a lattice $\mathcal{L}$ is distributive if and only if $x \wedge (y \vee z) \leq y \vee (x \wedge z)$ for all x, y, $z \in L$. (J. Bowden)
2. (a) Prove that every maximal ideal of a distributive lattice is prime.

(b) Show that a distributive lattice $\mathcal{D}$ with 0 and 1 is complemented if and only if every prime ideal of $\mathcal{D}$ is maximal.

3. These are the details of the construction of the free distributive lattice given in the text. Let X be a finite set.

(a) Let δ denote the kernel of the natural homomorphism from $\mathrm{FL}(X) \twoheadrightarrow \mathcal{F}_{\mathbf{D}}(X)$ with $x \mapsto x$. Thus $u \; \delta \; v$ iff $u(x_1, \ldots, x_n) = v(x_1, \ldots, x_n)$ in all distributive lattices. Prove that for every $w \in \mathrm{FL}(X)$ there exists w' which is a join of meets of generators such that $w \; \delta \; w'$. (Show that the set of all such elements w is a sublattice of $\mathrm{FL}(X)$ containing the generators.)
(b) Let $\mathcal{L}$ be any lattice generated by a set X, and let $\emptyset \subset Y \subset X$. Show that for all $w \in L$, either $w \geq \bigwedge Y$ or $w \leq \bigvee(X - Y)$.
(c) Show that $\bigwedge Y \nleq \bigvee(X - Y)$ in $\mathcal{F}_{\mathbf{D}}(X)$ by exhibiting a homomorphism $h : \mathcal{F}_{\mathbf{D}}(X) \to \mathbf{2}$ with $h(\bigwedge Y) \nleq h(\bigvee(X - Y))$.
(d) Generalize these results to the case when X is a finite ordered set (as in the next exercise).

4. Find the free distributive lattice generated by

(a) $\{x_0, x_1, y_0, y_1\}$ with $x_0 < x_1$ and $y_0 < y_1$,
(b) $\{x_0, x_1, x_2, y\}$ with $x_0 < x_1 < x_2$.

5. Let $\mathcal{P} = \mathcal{Q} \dot{\cup} \mathcal{R}$ be the disjoint union of two ordered sets, so that q and r are incomparable whenever $q \in Q$, $r \in R$. Show that $\mathcal{O}(\mathcal{P}) \cong \mathcal{O}(\mathcal{Q}) \times \mathcal{O}(\mathcal{R})$.

6. Let $\mathcal{D}$ be a distributive lattice with 0 and 1, and let x and y be complements in $\mathcal{D}$. Prove that $\mathcal{D} \cong \uparrow x \times \uparrow y$. (Dually, $\mathcal{D} \cong \downarrow x \times \downarrow y$; in fact, $\uparrow x \cong \downarrow y$ and $\uparrow y \cong \downarrow x$. This explains why $\mathbf{Con}\, \mathcal{L}_1 \times \mathcal{L}_2 \cong \mathbf{Con}\, \mathcal{L}_1 \times \mathbf{Con}\, \mathcal{L}_2$ (Exercise 5.6).)

7. Show that the following are true in a finite distributive lattice $\mathcal{D}$.

(a) For each join irreducible element x of $\mathcal{D}$, let $\kappa(x) = \bigvee\{y \in D : y \ngeq x\}$. Then $\kappa(x)$ is meet irreducible and $\kappa(x) \ngeq x$.
(b) For each $x \in J(\mathcal{D})$, $D = \uparrow x \,\dot{\cup}\, \downarrow \kappa(x)$.
(c) The map $\kappa : J(\mathcal{D}) \to M(\mathcal{D})$ is an order isomorphism.

8. A join semilattice with 0 is *distributive* if $x \leq y \vee z$ implies there exist $y' \leq y$ and $z' \leq z$ such that $x = y' \vee z'$. Prove that an algebraic lattice is distributive if and only if its compact elements form a distributive semilattice.

9. Find an infinite distributive law that holds in every algebraic distributive lattice. Show that this may fail in a complete distributive lattice.

10. Prove Theorem 8.7.

11. Prove Peirce's theorem: If a lattice $\mathcal{L}$ with 0 and 1 has a complementation operation $*$ such that

(1) $b \wedge b^* = 0$ and $b \vee b^* = 1$,
(2) $a \wedge b = 0$ implies $a \leq b^*$,
(3) $b^{**} = b$,

then $\mathcal{L}$ is a Boolean algebra.

12. Prove Papert's characterization of lattices of closed sets of a topological space [11]: *Let $\mathcal{D}$ be a complete distributive lattice. There is a topological space $\mathcal{T}$ and an isomorphism ϕ mapping $\mathcal{D}$ onto the lattice of closed subsets of $\mathcal{T}$, preserving finite joins and infinite meets, if and only if $x \not\leq y$ in $\mathcal{D}$ implies there exists a (finitely) join prime element p with $p \leq x$ and $p \not\leq y$.*

References

1. M. E. Adams, *Uniquely complemented lattices*, The Dilworth Theorems, K. Bogart, R. Freese and J. Kung, Eds., Birkhäuser, Boston, 1990, pp. 79–84.
2. R. Balbes and Ph. Dwinger, *Distributive Lattices*, University Missouri Press, Columbia, 1974.
3. H. J. Bandelt, *Complemented continuous lattices*, Arch. Math. (Basel) **36** (1981), 474–475.
4. H. J. Bandelt and R. Padmanabhan, *A note on lattices with unique comparable complements*, Abh. Math. Sem. Univ. Hamburg **48** (1979), 112–113.
5. G. Birkhoff and M. Ward, *A characterization of Boolean algebras*, Ann. of Math. **40** (1939), 609–610.
6. B. Davey and H. Priestley, *Introduction to Lattices and Order*, Cambridge University Press, Cambridge, 1990.
7. R. Dedekind, *Über die drei Moduln erzeugte Dualgruppe*, Math. Annalen **53** (1900), 371–403.
8. R. P. Dilworth, *Lattices with unique complements*, Trans. Amer. Math. Soc. **57** (1945), 123–154.
9. G. Grätzer, *Two problems that shaped a century of lattice theory*, Notices Amer. Math. Soc. **54** (2007), 696–707.
10. E. V. Huntington, *Sets of independent postulates for the algebra of logic*, Trans. Amer. Math. Soc. **5** (1904), 288–309.
11. S. Papert, *Which distributive lattices are lattices of closed sets?*, Proc. Cambridge Phil. Soc. **55** (1959), 172–176.
12. R. Quackenbush, *Dedekind's problem*, Order **2** (1986), 415–417.
13. V. N. Saliĭ, *A compactly generated lattice with unique complements is distributive*, Mat. Zametki **12** (1972), 617–620. (Russian)
14. V. N. Saliĭ, *A continuous uniquely complemented lattice is distributive*, Fifth All-Union Conf. Math. Logic, Abstracts of Reports, Inst. Mat. Sibirsk. Otdel. Akad. Nauk SSSR, Novosibirsk, 1979, p. 134. (Russian)
15. M. H. Stone, *The theory of representations of Boolean Algebras*, Trans. Amer. Math. Soc. **40** (1936), 37–111.
16. V. N. Saliĭ, *Lattices with unique complements*, Translations of the Amer. Math. Soc., vol. 69, Amer. Math. Soc., Providence, R. I., 1988.

9. Modular and Semimodular Lattices

To dance beneath the diamond sky with one hand waving free ...
–Bob Dylan

The modular law was invented by Dedekind to reflect a crucial property of the lattice of subgroups of an abelian group, or more generally the lattice of normal subgroups of a group. In this chapter on modular lattices you will see the lattice theoretic versions of some familiar theorems from group theory. This will lead us naturally to consider semimodular lattices.

Likewise, the lattice of submodules of a module over a ring is modular. Thus our results on modular lattices apply to the lattice of ideals of a ring, or the lattice of subspaces of a vector space. These applications make modular lattices particularly important.

The smallest nonmodular lattice is $\mathcal{N}_5$, which is called the *pentagon*. Dedekind's characterization of modular lattices is simple [5].

Theorem 9.1. *A lattice is modular if and only if it does not contain the pentagon as a sublattice.*

Proof. Clearly, a modular lattice cannot contain $\mathcal{N}_5$ as a sublattice. Conversely, suppose $\mathcal{L}$ is a nonmodular lattice. Then there exist $x > y$ and z in $\mathcal{L}$ such that $x \wedge (y \vee z) > y \vee (x \wedge z)$. Now the lattice freely generated by x, y, z with $x \geq y$ is shown in Figure 9.1; you should verify that it is correct. The elements $x \wedge (y \vee z)$, $y \vee (x \wedge z)$, z, $x \wedge z$ and $y \vee z$ form a pentagon there, and likewise in $\mathcal{L}$. Since the pentagon is subdirectly irreducible and $x \wedge (y \vee z)/y \vee (x \wedge z)$ is the critical quotient, these five elements are distinct. $\square$

Birkhoff [1] showed that there is a similar characterization of distributive lattices within the class of modular lattices. The *diamond* is $\mathcal{M}_3$, which is the smallest nondistributive modular lattice.

Theorem 9.2. *A modular lattice is distributive if and only if it does not contain the diamond as a sublattice.*

Proof. Again clearly, a distributive lattice cannot have a sublattice isomorphic to $\mathcal{M}_3$. Conversely, let $\mathcal{L}$ be a nondistributive modular lattice. Then, by Lemma 8.2, there exist x, y, z in $\mathcal{L}$ such that $(x \vee y) \wedge (x \vee z) \wedge (y \vee z) > (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$. Now the free modular lattice $\mathcal{F}_{\mathbf{M}}(3)$ is diagrammed in Figure 9.2; again you should

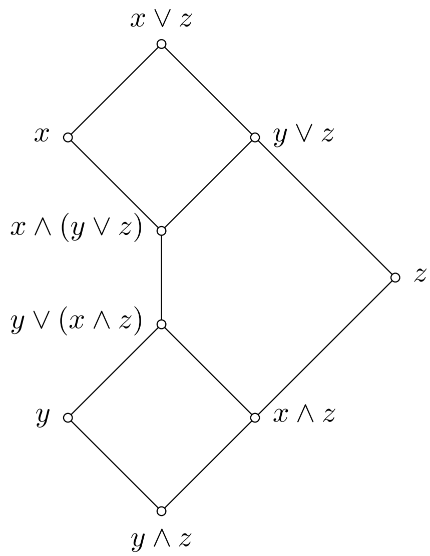


FIGURE 9.1: FL($\mathbf{2} + \mathbf{1}$)

verify that it is correct.[1] The interval between the two elements above is a diamond in $\mathcal{F}_{\mathbf{M}}(3)$, and the corresponding elements will form a diamond in $\mathcal{L}$.

The details go as follows. The middle elements of our diamond should be

$$[x \wedge (y \vee z)] \vee (y \wedge z) = [x \vee (y \wedge z)] \wedge (y \vee z)$$
$$[y \wedge (x \vee z)] \vee (x \wedge z) = [y \vee (x \wedge z)] \wedge (x \vee z)$$
$$[z \wedge (x \vee y)] \vee (x \wedge y) = [z \vee (x \wedge y)] \wedge (x \vee y)$$

where in each case the equality follows from modularity. The join of the first pair of elements is (using the first expressions)

$$\begin{aligned}[x \wedge (y \vee z)] \vee (y \wedge z) \vee [y \wedge (x \vee z)] \vee (x \vee z) &= [x \wedge (y \vee z)] \vee [y \wedge (x \vee z)] \\ &= [(x \wedge (y \vee z)) \vee y] \wedge (x \vee z) \\ &= (x \vee y) \wedge (x \vee z) \wedge (y \vee z).\end{aligned}$$

Symmetrically, the other pairs of elements also join to $(x \vee y) \wedge (x \vee z) \wedge (y \vee z)$. Since the second expression for each element is dual to the first, each pair of these three elements meets to $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$. Because the diamond is simple, the five elements will be distinct, and hence form a sublattice isomorphic to $\mathcal{M}_3$. □

[1]Recall from Chapter 7, though, that $\mathcal{F}_{\mathbf{M}}(n)$ is infinite and has an unsolvable word problem for $n \geq 4$.

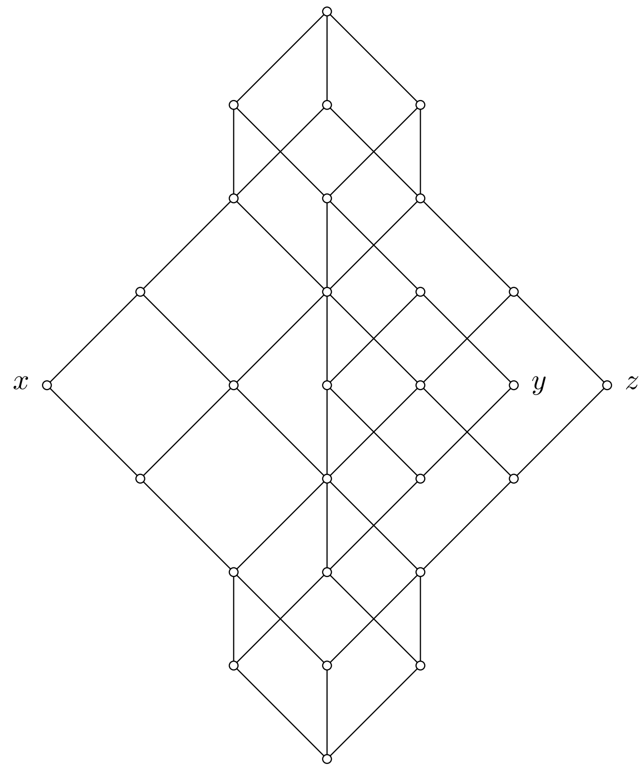


FIGURE 9.2: $\mathcal{F}_{\mathbf{M}}(3)$

Corollary. *A lattice is distributive if and only if it has neither* $\mathcal{N}_5$ *nor* $\mathcal{M}_3$ *as a sublattice.*

The preceding two results tell us something more about the bottom of the lattice Λ of lattice varieties. We already know that the trivial variety $\mathbf{T}$ is uniquely covered by $\mathbf{D} = \mathrm{HSP}(\mathbf{2})$, which is in turn covered by $\mathrm{HSP}(\mathcal{N}_5)$ and $\mathrm{HSP}(\mathcal{M}_3)$. By the Corollary, these are the only two varieties covering $\mathbf{D}$.

Much more is known about the bottom of Λ. Both $\mathrm{HSP}(\mathcal{N}_5)$ and $\mathrm{HSP}(\mathcal{M}_3)$ are covered by their join $\mathrm{HSP}\{\mathcal{N}_5, \mathcal{M}_3\} = \mathrm{HSP}(\mathcal{N}_5 \times \mathcal{M}_3)$. George Grätzer and Bjarni Jónsson ([8], [11]) showed that $\mathrm{HSP}(\mathcal{M}_3)$ has two additional covers, and Jónsson and Ivan Rival [12] proved that $\mathrm{HSP}(\mathcal{N}_5)$ has exactly fifteen other covers, each generated by a finite subdirectly irreducible lattice. You are encouraged to try and find these covers. Because of Jónsson's Lemma, it is never hard to tell if $\mathrm{HSP}(\mathcal{K})$ covers $\mathrm{HSP}(\mathcal{L})$ when $\mathcal{K}$ and $\mathcal{L}$ are finite lattices; the hard part is determining whether your list of covers is complete. Since a variety generated by a finite lattice can have infinitely many covering varieties, or a covering variety generated by an infinite subdirectly irreducible lattice, this can only be done near the bottom of Λ; see [16].

Now we return to modular lattices. For any two elements a, b in a lattice $\mathcal{L}$ there are natural maps $\mu_a : (a \vee b)/b \to a/(a \wedge b)$ and $\nu_b : a/(a \wedge b) \to (a \vee b)/b$ given by

$$\mu_a(x) = x \wedge a$$
$$\nu_b(x) = x \vee b.$$

Dedekind showed that these maps play a special role in the structure of modular lattices.

Theorem 9.3. *If a and b are elements of a modular lattice $\mathcal{L}$, then μ_a and ν_b are mutually inverse isomorphisms, whence $(a \vee b)/b \cong a/(a \wedge b)$.*

Proof. Clearly, μ_a and ν_b are order preserving. They are mutually inverse maps by modularity: for if $x \in (a \vee b)/b$, then

$$\nu_b\mu_a(x) = b \vee (a \wedge x) = (b \vee a) \wedge x = x$$

and, dually, $\mu_a\nu_b(y) = y$ for all $y \in a/(a \wedge b)$. $\square$

Corollary. *In a modular lattice, $a \succ a \wedge b$ if and only if $a \vee b \succ b$.*

For groups we actually have somewhat more. The First Isomorphism Theorem says that if $\mathcal{A}$ and $\mathcal{B}$ are subgroups of a group $\mathcal{G}$, and $\mathcal{B}$ is normal in $\mathcal{A} \vee \mathcal{B}$, then the quotient groups $\mathcal{A}/\mathcal{A} \wedge \mathcal{B}$ and $\mathcal{A} \vee \mathcal{B}/\mathcal{B}$ are isomorphic.

A lattice $\mathcal{L}$ is said to be *semimodular* (or *upper semimodular*) if $a \succ a \wedge b$ implies $a \vee b \succ b$ in $\mathcal{L}$. Equivalently, $\mathcal{L}$ is semimodular if $u \succ v$ implies $u \vee x \succeq v \vee x$, where $a \succeq b$ means a covers or equals b. The dual property is called *lower semimodular*. Traditionally, *semimodular* by itself always refers to upper semimodularity. Clearly the Corollary shows that modular lattices are both upper and lower semimodular. A strongly atomic, algebraic lattice that is both upper and lower semimodular is modular. (See Theorem 3.7 of [3]; you are asked to prove the finite dimensional version of this in Exercise 3.)

Dedekind proved in his seminal paper of 1900 that every maximal chain in a finite dimensional modular lattice has the same length. The proof extends naturally to semimodular lattices.

Theorem 9.4. *Let $\mathcal{L}$ be a semimodular lattice and let $a < b$ in $\mathcal{L}$. If there is a finite maximal chain from a to b, then every chain from a to b is finite, and all the maximal ones have the same length.*

Proof. We are given that there is a finite maximal chain in b/a, say

$$a = a_0 \prec a_1 \prec \cdots \prec a_n = b.$$

If $n = 1$, i.e., $a \prec b$, then the theorem is trivially true. So we may assume inductively that it holds for any interval containing a maximal chain of length less than n.

Let C be another maximal chain in b/a. If, perchance, $c \geq a_1$ for all $c \in C - \{a\}$, then $C - \{a\}$ is a maximal chain in b/a_1. In that case, $C - \{a\}$ has length $n-1$ by induction, and so C has length n.

Thus we may assume that there is an element $d \in C - \{a\}$ such that $d \ngeq a_1$. Moreover, since b/a_1 has finite length, we can choose d such that $d \vee a_1$ is minimal, i.e., $e \vee a_1 \geq d \vee a_1$ for all $e \in C - \{a\}$. We can show that $d \succ a$ as follows. Suppose not. Then $d > e > a$ for some $e \in L$; since C is a maximal chain containing a and d, we can choose $e \in C$. Now $a_1 \succ a = d \wedge a_1 = e \wedge a_1$. Hence by semimodularity $d \vee a_1 \succ d$ and $e \vee a_1 \succ e$. But the choice of d implies $e \vee a_1 \geq d \vee a_1 \succ d > e$, contradicting the second covering relation. Therefore $d \succ a$.

Now we are quickly done. As a_1 and d both cover a, their join $a_1 \vee d$ covers both of them. Since $a_1 \vee d \succ a_1$, every maximal chain in $b/(a_1 \vee d)$ has length $n-2$. Then every chain in b/d has length $n-1$, and C has length n, as desired. $\square$

Now let $\mathcal{L}$ be a semimodular lattice in which every principal ideal $\downarrow x$ has a finite maximal chain. Then we can define a *dimension function* δ on $\mathcal{L}$ by letting $\delta(x)$ be the length of a maximal chain from 0 to x:

$$\delta(x) = n \quad \text{if} \quad 0 = c_0 \prec c_1 \prec \cdots \prec c_n = x.$$

By Theorem 9.4, δ is well defined. For semimodular lattices the properties of the dimension function can be summarized as follows.

Theorem 9.5. *If $\mathcal{L}$ is a semimodular lattice and every principal ideal has only finite maximal chains, then the dimension function on $\mathcal{L}$ has the following properties.*

(1) $\delta(0) = 0$,
(2) $x > y$ *implies* $\delta(x) > \delta(y)$,
(3) $x \succ y$ *implies* $\delta(x) = \delta(y) + 1$,
(4) $\delta(x \vee y) + \delta(x \wedge y) \leq \delta(x) + \delta(y)$.

Conversely, if $\mathcal{L}$ is a lattice that admits an integer valued function δ satisfying (1)–(4), then $\mathcal{L}$ is semimodular and principal ideals have only finite maximal chains.

Proof. Given a semimodular lattice $\mathcal{L}$ in which principal ideals have only finite maximal chains, properties (1) and (2) are obvious, while (3) is a consequence of Theorem 9.4. The only (not very) hard part is to establish the inequality (4). Let x and y be elements of $\mathcal{L}$, and consider the join map $\nu_x : y/(x \wedge y) \to (x \vee y)/x$ defined by $\nu_x(z) = z \vee x$. Recall that, by semimodularity, $u \succ v$ implies $u \vee x \succeq v \vee x$. Hence ν_x takes maximal chains in $y/(x \wedge y)$ to maximal chains in $(x \vee y)/x$. So the length of $(x \vee y)/x$ is at most that of $y/(x \wedge y)$, i.e.,

$$\delta(x \vee y) - \delta(x) \leq \delta(y) - \delta(x \wedge y)$$

which establishes the desired inequality.

Conversely, suppose $\mathcal{L}$ is a lattice that admits a function δ satisfying (1)–(4). Note that, by (2), $\delta(x) \geq \delta(z)+2$ whenever $x > y > z$; hence if $x \geq z$ and $\delta(x) = \delta(z)+1$, then $x \succ z$.

To establish semimodularity, assume $a \succ a \wedge b$ in $\mathcal{L}$. By (3) we have $\delta(a) = \delta(a \wedge b) + 1$, and so by (4)

$$\begin{aligned} \delta(a \vee b) + \delta(a \wedge b) &\leq \delta(a) + \delta(b) \\ &= \delta(a \wedge b) + 1 + \delta(b) \end{aligned}$$

whence $\delta(a \vee b) \leq \delta(b) + 1$. As $a \vee b > b$, in fact $\delta(a \vee b) = \delta(b) + 1$ and $a \vee b \succ b$, as desired.

For any $a \in L$, if $a = a_k > a_{k-1} > \cdots > a_0$ is any chain in $\downarrow a$, then $\delta(a_j) > \delta(a_{j-1})$ so $k \leq \delta(a)$. Thus every chain in $\downarrow a$ has length at most $\delta(a)$. □

For modular lattices, the map μ_x is an isomorphism, so we obtain instead equality. It also turns out that we can dispense with the third condition, though this is not very important.

Theorem 9.6. *If $\mathcal{L}$ is a modular lattice and every principal ideal has only finite maximal chains, then*

(1) $\delta(0) = 0$,
(2) $x > y$ *implies* $\delta(x) > \delta(y)$,
(3) $\delta(x \vee y) + \delta(x \wedge y) = \delta(x) + \delta(y)$.

Conversely, if $\mathcal{L}$ is a lattice that admits an integer-valued function δ satisfying (1)–(3), then $\mathcal{L}$ is modular and principal ideals have only finite maximal chains.

At this point, it is perhaps useful to have some examples of semimodular lattices. The lattice of equivalence relations $\mathbf{Eq}\ X$ is semimodular, but nonmodular for $|X| \geq 4$. The lattice in Figure 9.3 is semimodular, but not modular.[2] We will see more semimodular lattices as we go along, arising from group theory (subnormal subgroups) in this chapter and from geometry in Chapter 11.

For our applications to group theory, we need a supplement to Theorem 9.4. This in turn requires a definition. We say that a quotient a/b *transposes up* to c/d if $a \vee d = c$ and $a \wedge d = b$. We then say that c/d *transposes down* to a/b. We then define *projectivity* to be the smallest equivalence relation on the set of all quotients of a lattice $\mathcal{L}$ that contains all transposed pairs $\langle x/(x \wedge y), (x \vee y)/y \rangle$. Thus a/b is projective to c/d if and only if there exists a sequence of quotients

[2] One standard trick to construct semimodular lattices is to take a finite dimensional modular lattice $\mathcal{L}$, of dimension n say, so that $\delta(1) = n$. Choose an integer $k < n$, and remove all elements $x \in L$ with $k \leq \delta(x) < n$. (Alternatively, take the join semilattice congruence collapsing all these elements to 1.) The result is a semimodular lattice $\widehat{\mathcal{L}}$ of dimension k. The lattice in Figure 9.3 was obtained by applying this method to the lattice of subsets of a four element set. See Exercise 1 of Chapter 11.

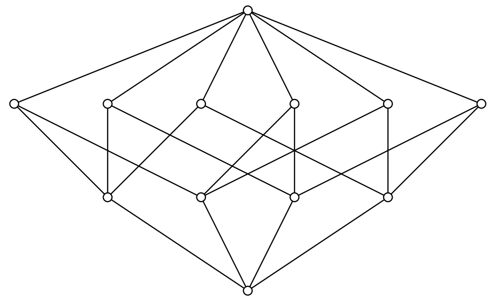


FIGURE 9.3

$a/b = a_0/b_0, a_1/b_1, \ldots, a_n/b_n = c/d$ such that a_i/b_i and a_{i+1}/b_{i+1} are transposes (up or down).

The strengthened version of Theorem 9.4 goes thusly. This can be (and was originally) obtained by a slight extension of Dedekind's arguments. The proof given here is due to George Grätzer and the author [9].

Theorem 9.7. *Let C and D be two maximal chains in a finite length semimodular lattice, say*

$$0 = c_0 \prec c_1 \prec \cdots \prec c_n = 1$$
$$0 = d_0 \prec d_1 \prec \cdots \prec d_n = 1.$$

Then there is a permutation π of the set $\{1, \ldots, n\}$ such that c_i/c_{i-1} is projective in two steps (up-down) to $d_{\pi(i)}/d_{\pi(i)-1}$ for all i.

Proof. Again, the proof is by induction on the length n. The statement is obvious for $n \leq 2$, so assume $n > 2$. The argument is illustrated in Figure 9.4.

Let k be the largest integer with $c_1 \nleq d_k$, noting $k < n$. If $k = 0$, then $c_1 = d_1$ and the statement follows by the induction hypothesis. So we can assume that $k > 0$.

For $0 \leq j \leq n$, let $e_j = c_1 \vee d_j$. Note that $e_0 = c_1$ and $e_k = e_{k+1} = d_{k+1}$, and indeed $e_j = d_j$ for $j \geq k + 1$. Now

$$c_1 = e_0 \prec e_1 \prec \cdots \prec e_k = e_{k+1} \prec e_{k+2} \prec \cdots \prec e_n = 1$$

is a maximal chain in the interval $1/c_1$. By induction, there is an bijective map $\sigma : \{2, \ldots, n\} \to \{1, \ldots, k, k + 2, \ldots, n\}$ such that, for $i > 1$, each interval c_i/c_{i-1} is projective up to some prime interval u_i/v_i in $\mathcal{L}$, which in turn projects down to $e_{\sigma(i)}/e_{\sigma(i)-1}$. For $j \leq k$, e_j/e_{j-1} projects down to d_j/d_{j-1}, while for $j > k + 1$ we have $e_j/e_{j-1} = d_j/d_{j-1}$. Meanwhile, $c_1/0$ projects up to d_{k+1}/d_k. So we may take π to be the permutation with $\pi(i) = \sigma(i)$ for $i \neq 1$, and $\pi(1) = k + 1$. $\square$

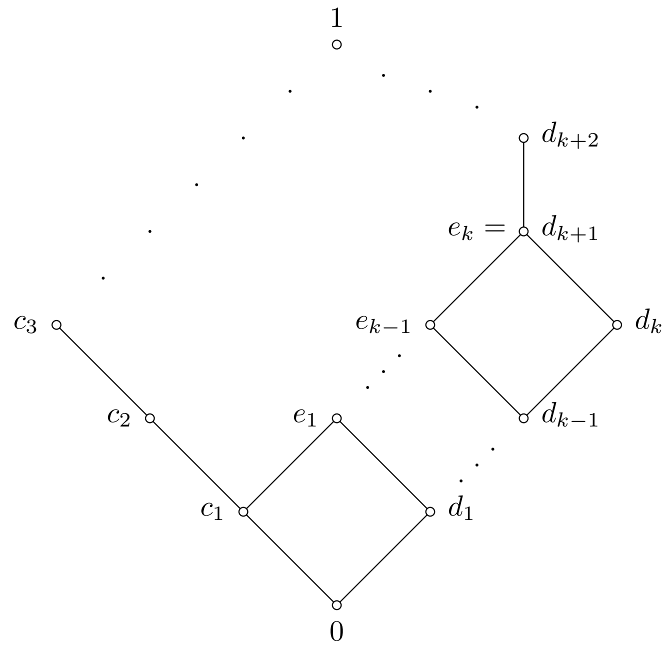


FIGURE 9.4

Theorems 9.4 and 9.7 are important in group theory. A *chief series* of a group $\mathcal{G}$ is a maximal chain in the lattice of normal subgroups $\mathcal{N}(\mathcal{G})$. Since $\mathcal{N}(\mathcal{G})$ is modular, our theorems apply.

Corollary. *If a group $\mathcal{G}$ has a finite chief series of length k,*

$$\{1\} = N_0 < N_1 < \cdots < N_k = \mathcal{G}$$

then every chief series of $\mathcal{G}$ has length k. Moreover, if

$$\{1\} = H_0 < H_1 < \cdots < H_k = \mathcal{G}$$

is another chief series of $\mathcal{G}$, then there is a permutation π of $\{1, \ldots, k\}$ such that $H_i/H_{i-1} \cong N_{\pi(i)}/N_{\pi(i)-1}$ for all i.

A subgroup H is *subnormal* in a group $\mathcal{G}$, written $H \lhd\lhd \mathcal{G}$, if there is a chain in **Sub** $\mathcal{G}$,

$$H = H_0 \lhd H_1 \lhd \ldots \lhd H_k = \mathcal{G}$$

with each H_{i-1} normal in H_i (but H_j need not be normal in $\mathcal{G}$ for $j < k$). Herman Wielandt proved that the subnormal subgroups of a finite group form a lattice [20].

Theorem 9.8. *If $\mathcal{G}$ is a finite group, then the subnormal subgroups of $\mathcal{G}$ form a lower semimodular sublattice $\mathcal{SN}(\mathcal{G})$ of* **Sub** $\mathcal{G}$.

Proof. Let H and K be subnormal in $\mathcal{G}$, with say

$$H = H_0 \lhd H_1 \lhd \ldots \lhd H_m = \mathcal{G}$$
$$K = K_0 \lhd K_1 \lhd \ldots \lhd K_n = \mathcal{G}.$$

Then $H \cap K_i \lhd H \cap K_{i+1}$, and so we have the series

$$H \cap K \lhd H \cap K_1 \lhd H \cap K_2 \lhd \ldots H \cap \mathcal{G} = H \lhd H_1 \lhd \ldots \lhd \mathcal{G}.$$

Thus $H \cap K \lhd\lhd \mathcal{G}$. Note that this argument shows that *if H, $K \lhd\lhd \mathcal{G}$ and $K \leq H$, then $K \lhd\lhd H$.*

The proof that $\mathcal{SN}(\mathcal{G})$ is closed under joins is a bit trickier. Let H, $K \lhd\lhd \mathcal{G}$ as before. Without loss of generality, H and K are incomparable. By induction, we may assume that $|\mathcal{G}|$ is minimal and that the result holds for larger subnormal subgroups of $\mathcal{G}$, i.e.,

(1) the join of subnormal subgroups is again subnormal in any group $\mathcal{G}'$ with $|\mathcal{G}'| < |\mathcal{G}|$,

(2) if $H < L \lhd\lhd \mathcal{G}$, then $L \vee K \lhd\lhd \mathcal{G}$; likewise, if $K < M \lhd\lhd \mathcal{G}$, then $H \vee M \lhd\lhd \mathcal{G}$.

If there is a subnormal proper subgroup S of $\mathcal{G}$ that contains both H and K, then H and K are subnormal subgroups of S (by the observation above). In that case, $H \vee K \lhd\lhd S$ by the first assumption, whence $H \vee K \lhd\lhd \mathcal{G}$. Thus we may assume that

(3) no subnormal proper subgroup of $\mathcal{G}$ contains both H and K.

Combining this with assumption (2) yields

(4) $H_1 \vee K = \mathcal{G} = H \vee K_1$.

Finally, if both H and K are normal in $\mathcal{G}$, then so is $H \vee K$. Thus we may assume (by symmetry) that

(5) H is not normal in $\mathcal{G}$, and hence $H < H_1 \leq H_{m-1} < \mathcal{G}$.

Now $\mathcal{G}$ is generated by the set union $H_1 \cup K$ by assumption (4), so we must have $x^{-1}Hx \neq H$ for some $x \in H_1 \cup K$. But $H \lhd H_1$, so $k^{-1}Hk \neq H$ for some $k \in K$.

However, $k^{-1}Hk$ is a subnormal subgroup of H_{m-1}, because

$$k^{-1}Hk \lhd k^{-1}H_1k \lhd \ldots \lhd k^{-1}H_{m-1}k = H_{m-1}$$

as $H_{m-1} \lhd \mathcal{G}$. Applying assumption (1) with $\mathcal{G}' = H_{m-1}$, we find that $H \vee k^{-1}Hk$ is a subnormal subgroup of H_{m-1}, and hence of $\mathcal{G}$. Moreover, $H < H \vee k^{-1}Hk \leq H \vee K$, whence $(H \vee k^{-1}Hk) \vee K = H \vee K$. Using assumption (2) with $L = H \vee k^{-1}Hk$, it follows that $H \vee K = L \vee K$ is subnormal in $\mathcal{G}$, as desired.

Finally, if $H \vee K \succ H$ in $\mathcal{SN}(\mathcal{G})$, then $H \lhd H \vee K$: by the observation after the first argument, H and $H \vee K$ both subnormal and $H \leq H \vee K$ makes $H \lhd\lhd H \vee K$, and since it is a covering relation in $\mathcal{SN}(\mathcal{G})$ then $H \lhd H \vee K$. Moreover, $(H \vee K)/H$ is simple. By one of the group isomorphism theorems, $K/(H \wedge K)$ is likewise simple, so $K \succ H \wedge K$. Thus $\mathcal{SN}(\mathcal{G})$ is lower semimodular. $\square$

A maximal chain in $\mathcal{SN}(\mathcal{G})$ is called a *composition series* for $\mathcal{G}$. As $\mathcal{SN}(\mathcal{G})$ is lower semimodular, the duals of Theorems 9.4 and 9.7 yield the Jordan-Hölder structure theorem for groups.

Corollary. *If a finite group $\mathcal{G}$ has a composition series of length n,*

$$\{1\} = H_0 \triangleleft H_1 \triangleleft \ldots \triangleleft H_n = \mathcal{G}$$

then every composition series of $\mathcal{G}$ has length n. Moreover, if

$$\{1\} = K_0 \triangleleft K_1 \triangleleft \ldots \triangleleft K_n = \mathcal{G}$$

is another composition series for $\mathcal{G}$, then there is a permutation π of $\{1, \ldots, n\}$ such that $K_i/K_{i-1} \cong H_{\pi(i)}/H_{\pi(i)-1}$ for all i.

Historical note. The Jordan-Hölder theorem provides a good example of the interaction between groups and lattice theory, with a long history. For the interestd reader, the primary references are, in order, Jordan [13], Hölder [10], Dedekind [5], Schreier [18], Zassenhaus [21], and Wielandt [20]. Secondary sources are Burnside Chap. V [2], Zassenhaus Chap. II.5 [22], and Birkhoff (1963 ed.) Chap. III.7 [1]. Slick modern proofs are in Grätzer and Nation [9] and Czedli and Schmidt [4].

A *finite decomposition* of an element $a \in L$ is an expression $a = \bigwedge Q$ where Q is a finite set of meet irreducible elements. If $\mathcal{L}$ satisfies the ACC, then every element has a finite decomposition. We have seen that every element of a finite distributive lattice has a unique irredundant decomposition. In a finite dimensional modular lattice, an element can have many different finite decompositions, but the number of elements in any irredundant decomposition is always the same. This is a consequence of the following replacement property (known as the Kurosh-Ore Theorem).

Theorem 9.9. *If a is an element of a modular lattice and*

$$a = q_1 \wedge \ldots \wedge q_m = r_1 \wedge \ldots \wedge r_n$$

are two irredundant decompositions of a, then $m = n$ and for each q_i there is an r_j such that

$$a = r_j \wedge \bigwedge_{k \neq i} q_k$$

is an irredundant decomposition.

Proof. Let $a = \bigwedge Q = \bigwedge R$ be two irredundant finite decompositions (dropping the subscripts temporarily). Fix $q \in Q$, and let $\overline{q} = \bigwedge(Q - \{q\})$. By modularity, $q \vee \overline{q}/q \cong \overline{q}/q \wedge \overline{q} = \overline{q}/a$. Since q is meet irreducible in $\mathbf{L}$, this implies that a is meet irreducible in $\overline{q}/a$. However, $a = \overline{q} \wedge \bigwedge R = \bigwedge_{r \in R}(\overline{q} \wedge r)$ takes place in $\overline{q}/a$, so we must have $a = \overline{q} \wedge r$ for some $r \in R$.

Next we observe that $a = r \wedge \bigwedge(Q - \{q\})$ is irredundant. For if not, we would have $a = r \wedge \bigwedge S$ irredundantly for some proper subset $S \subset Q - \{q\}$. Reapplying the first argument to the two decompositions $a = r \wedge \bigwedge S = \bigwedge Q$ with the element r, we obtain $a = q' \wedge \bigwedge S$ for some $q' \in Q$, contrary to the irredundance of Q.

It remains to show that $|Q| = |R|$. Let $Q = \{q_1, \ldots, q_m\}$ say. By the first part, there is an element $r_1 \in R$ such that $a = r_1 \wedge \bigwedge(Q - \{q_1\}) = \bigwedge R$ irredundantly. Applying the argument to these two decompositions and q_2, there is an element $r_2 \in R$ such that $a = r_1 \wedge r_2 \wedge \bigwedge(Q - \{q_1, q_2\}) = \bigwedge R$. Moreover, r_1 and r_2 are distinct, for otherwise we would have $a = r_1 \wedge \bigwedge(Q - \{q_1, q_2\})$, contradicting the irredundance of $a = r_1 \wedge \bigwedge(Q - \{q_1\})$. Continuing, we can replace q_3 by an element r_3 of R, distinct from r_1 and r_2, and so forth. After m steps, we obtain $a = r_1 \wedge \cdots \wedge r_m$, whence $R = \{r_1, \ldots, r_m\}$. Thus $|Q| = |R|$. $\square$

With a bit of effort, this can be improved to a *simultaneous* exchange theorem.

Theorem 9.10. *If a is an element of a modular lattice and $a = \bigwedge Q = \bigwedge R$ are two irredundant finite decompositions of a, then for each $q \in Q$ there is an $r \in R$ such that*

$$a = r \wedge \bigwedge(Q - \{q\}) = q \wedge \bigwedge(R - \{r\}).$$

The proof of this, and much more on the general theory of decompositions in lattices, can be found in Crawley and Dilworth [3]; see also Dilworth [7].

Now Theorems 9.9 and 9.10 are exactly what we want in a finite dimensional modular lattice. However, in algebraic modular lattices, finite decompositions into meet irreducible elements need not coincide with the (possibly infinite) decomposition into completely meet irreducible elements given by Birkhoff's Theorem. Consider, for example, the chain $\mathcal{C} = (\omega + 1)^d$, the dual of $\omega + 1$. This satisfies the ACC, and hence is algebraic. The least element of $\mathcal{C}$ is meet irreducible, but not completely meet irreducible. In the direct product $\mathcal{C}^n$, the least element has a finite decomposition into n meet irreducible elements, but every decomposition into completely meet irreducibles is necessarily infinite.

Fortunately, the proof of Theorem 9.9 adapts nicely to give us a version suitable for algebraic modular lattices.

Theorem 9.11. *Let a be an element of a modular lattice. If $a = \bigwedge Q$ is a finite, irredundant decomposition into completely meet irreducible elements, and $a = \bigwedge R$ is another decomposition into meet irreducible elements, then there exists a finite subset $R' \subseteq R$ with $|R'| = |Q|$ such that $a = \bigwedge R'$ irredundantly.*

The application of Theorem 9.11 to subdirect products is immediate.

Corollary. *Let $\mathcal{A}$ be an algebra such that* **Con** $\mathcal{A}$ *is a modular lattice. If $\mathcal{A}$ has a finite subdirect decomposition into subdirectly irreducible algebras, then every irredundant subdirect decomposition of $\mathcal{A}$ into subdirectly irreducible algebras has the same number of factors.*

A more important application is to the theory of direct decompositions of congruence modular algebras. The corresponding congruences form a complemented sublattice of **Con** $\mathcal{A}$. This subject is treated thoroughly in Chapter 5 of McKenzie, McNulty and Taylor [15].

Let us close this section by mentioning a nice combinatorial result about finite modular lattices, due to R. P. Dilworth [6].

Theorem 9.12. *In a finite modular lattice $\mathcal{L}$, let $J_k(\mathcal{L})$ be the set of elements that cover exactly k elements, and let $M_k(\mathcal{L})$ be the set of elements that are covered by exactly k elements. Then $|J_k(\mathcal{L})| = |M_k(\mathcal{L})|$ for any integer $k \geq 0$.*

In particular, the number of join irreducible elements in a finite modular lattice is equal to the number of meet irreducible elements. In fact, Joseph Kung proved that in a finite modular lattice, there is a bijection $m : J(\mathcal{L}) \cup \{0\} \to M(\mathcal{L}) \cup \{1\}$ such that $x \leq m(x)$; see Kung [14] and Reuter [17].

We will return to modular lattices in Chapter 12. The standard reference for semimodular lattices is the book by Manfred Stern [19].

Exercises for Chapter 9

1. (a) Prove that a lattice $\mathcal{L}$ is distributive if and only if it has the property that $a \vee c = b \vee c$ and $a \wedge c = b \wedge c$ imply $a = b$.

(b) Show that $\mathcal{L}$ is modular if and only if, whenever $a \geq b$ and $c \in L$, $a \vee c = b \vee c$ and $a \wedge c = b \wedge c$ imply $a = b$.

2. Show that every finite dimensional distributive lattice is finite.

3. Prove that if a finite dimensional lattice is both upper and lower semimodular, then it is modular.

4. Prove that the following conditions are equivalent for a strongly atomic, algebraic lattice.

(i) $\mathcal{L}$ is semimodular: $a \succ a \wedge b$ implies $a \vee b \succ b$.
(ii) If a and b both cover $a \wedge b$, then $a \vee b$ covers both a and b.
(iii) If b and c are incomparable and $b \wedge c < a < c$, then there exists x such that $b \wedge c < x \leq b$ and $a = c \wedge (a \vee x)$.

5. Let $\mathcal{L}$ be a finite length semimodular lattice, and let C be any maximal chain in $\mathcal{L}$. Prove that any congruence relation on $\mathcal{L}$ is uniquely determined by its restriction to C. (Use Theorem 9.7) (George Grätzer)

6. Let a and b be elements of a finite dimensional semimodular lattice, and let $\nu_b : a/(a \wedge b) \to (a \vee b)/b$ by $\nu_b(x) = x \vee b$. Show that ν_b is a join embedding, i.e., one-to-one and join-preserving.

7. (a) Find infinitely many simple modular lattices of width 4.

(b) Prove that the variety generated by all lattices of width ≤ 4 contains subdirectly irreducible lattices of width ≤ 4 only.

8. Prove that every arguesian lattice is modular.

9. Let $\mathcal{L}$ be a lattice, and suppose there exist an ideal I and a filter F of $\mathcal{L}$ such that $L = I \cup F$ and $I \cap F \neq \emptyset$.

(a) Show that $\mathcal{L}$ is distributive if and only if both I and F are distributive.

(b) Show that $\mathcal{L}$ is modular if and only if both I and F are modular.

(R. P. Dilworth)

10. Show that modular lattices satisfy the equation

$$x \wedge (y \vee (z \wedge (x \vee t))) = x \wedge (z \vee (y \wedge (x \vee t))).$$

11. Let C and D be two chains in a modular lattice $\mathcal{L}$. Prove that $C \cup D$ generates a distributive sublattice of $\mathcal{L}$. (Bjarni Jónsson)

12. Let a and b be two elements in a modular lattice $\mathcal{L}$ such that $a \wedge b = 0$. Prove that the sublattice generated by $\downarrow a \cup \downarrow b$ is isomorphic to the direct product $\downarrow a \times \downarrow b$.

13. Prove Theorem 9.11. (Mimic the proof of Theorem 9.9.)

14. Let $\mathcal{A} = \prod_{i \in \omega} \mathbb{Z}_2$ be the direct product of countably many copies of the two element group. Describe two decompositions of 0 in **Sub** $\mathcal{A}$, say $0 = \bigwedge Q = \bigwedge R$, such that $|Q| = \aleph_0$ and $|R| = 2^{\aleph_0}$.

References

1. G. Birkhoff, *Lattice Theory*, First edition, Colloquium Publications, vol. 25, Amer. Math. Soc., Providence, R. I., 1940.
2. W. Burnside, *Theory of Groups of Finite Order*, Reprinted by Dover Publications, New York, 1955, Cambridge University Press, Cambridge, 1911.
3. P. Crawley and R. P. Dilworth, *Algebraic Theory of Lattices*, Prentice-Hall, Englewood Cliffs, N. J., 1973.
4. G. Czedli and E.T. Schmidt, *The Jordan-Hölder theorem with uniqueness for groups and semimodular lattices*, Algebra Universalis (2011).
5. R. Dedekind, *Über die von drei Moduln erzeugte Dualgruppe gemeinsamen Teiler*, Math. Annalen **53** (1900), 371–403, reprinted in Gesammelte mathematische Werke, Vol. 2, pp. 236–271, Chelsea, New York, 1968.
6. R. P. Dilworth, *Proof of a conjecture on finite modular lattices*, Ann. of Math. **60** (1954), 359–364.
7. R. P. Dilworth, *Structure and Decomposition Theory*, Proceedings of Symposia on Pure Mathematics: Lattice Theory, vol. II, Amer. Math. Soc., Providence, R. I., 1961.
8. G. Grätzer, *Equational classes of lattices*, Duke Jour. Math. **33** (1966), 613–622.
9. G. Grätzer and J.B. Nation, *A new look at the Jordan-Hölder theorem for semimodular lattices*, Algebra Universalis **64** (2011), 309–311.
10. O. Hölder, *Zurčkfḧrung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen*, Math. Ann. **34** (1889), 33 ff..
11. B. Jónsson, *Equational classes of lattices*, Math. Scand. **22** (1968), 187–196.
12. B. Jónsson and I. Rival, *Lattice varieties covering the smallest non-modular variety*, Pacific J. Math. **82** (1979), 463–478.
13. C. Jordan, *Traité des substitutions et des équations algébiques*, Gauthier-Villars, Paris, 1870.
14. J.P.S. Kung, *Matchings and Radon transforms in lattices, I: Consisent lattices*, Order **2** (1985), 105–112.
15. R. McKenzie, G. McNulty and W. Taylor, *Algebras, Lattices, Varieties*, vol. I, Wadsworth and Brooks-Cole, Belmont, CA, 1987.
16. J. B. Nation, *A counterexample to the finite height conjecture*, Order **13** (1996), 1–9.

17. K. Reuter, *Matchings for linearly indecomposable modular lattices*, Discrete Math. **63** (1987), 245–249.
18. O. Schreier, *Über den J-H'schen Satz*, Abh. Math. Sem. Univ. Hamburg **6** (1928), 300–302.
19. M. Stern, *Semimodular Lattices: Theory and Applications*, Cambridge University Press, Cambridge, 1999.
20. H. Wielandt, *Eine Verallgemeinerung der invarianten Untergruppen*, Math. Zeit. **45** (1939), 209–244.
21. H. Zassenhaus, *Zum Satz von Jordan-Hölder-Schreier*, Abh. Math. Sem. Univ. Hamburg **10** (1934), 106–108.
22. H. Zassenhaus, *Theory of Groups*, 2nd. ed. 1958, Chelsea, 1949.

10. Finite Lattices and their Congruence Lattices

If memories are all I sing
I'd rather drive a truck.
–Ricky Nelson

In this chapter we want to study the structure of finite lattices, and how it is reflected in their congruence lattices. There are different ways of looking at lattices, each with its own advantages. For the purpose of studying congruences, it is useful to represent a finite lattice as the lattice of closed sets of a closure operator on its set of join irreducible elements. This is an efficient way to encode the structure, and will serve us well.[1]

The approach to congruences taken in this chapter is not the traditional one. It evolved from techniques developed over a period of time by Ralph McKenzie, Bjarni Jónsson, Alan Day, Ralph Freese and J. B. Nation for dealing with various specific questions (see [1], [4], [6], [7], [8], [9]). Gradually, the general usefulness of these methods dawned on us.

In the simplest case, recall that a finite distributive lattice $\mathcal{L}$ is isomorphic to the lattice of order ideals $\mathcal{O}(J(\mathcal{L}))$, where $J(\mathcal{L})$ is the ordered set of nonzero join irreducible elements of $\mathcal{L}$. This reflects the fact that join irreducible elements in a distributive lattice are join prime. In a nondistributive lattice, we seek a modification that will keep track of the ways in which one join irreducible is below the join of others. In order to do this, we must first develop some terminology.

Rather than just considering finite lattices, we can include with modest additional effort a larger class of lattices satisfying a strong finiteness condition. Recall that a lattice $\mathcal{L}$ is *principally chain finite* if no principal ideal of $\mathcal{L}$ contains an infinite chain (equivalently, every principal ideal $\downarrow x$ satisfies the ACC and DCC). In Theorem 11.1, we will see where this class arises naturally in an important setting.[2]

Recall that if $X, Y \subseteq L$, we say that X *refines* Y (written $X \ll Y$) if for each $x \in X$ there exists $y \in Y$ with $x \leq y$. It is easy to see that the relation $\ll$ is a quasiorder (reflexive and transitive), but not in general antisymmetric. Note $X \subseteq Y$ implies $X \ll Y$.

If $q \in J(\mathcal{L})$ is completely join irreducible, let q_* denote the unique element of L with $q \succ q_*$. Note that if $\mathcal{L}$ is principally chain finite, then q_* exists for each $q \in J(\mathcal{L})$.

[1] For an alternate approach, see Appendix. 3

[2] Many of the results in this chapter can be generalized to arbitrary lattices. However, these generalizations have not yet proved to be very useful unless one assumes at least the DCC.

A *join expression* of $a \in L$ is a finite set B such that $a = \bigvee B$. A join expression $a = \bigvee B$ is *minimal* if it is irredundant and B cannot be properly refined, i.e., $B \subseteq J(\mathcal{L})$ and $c \vee \bigvee(B - \{b\}) < a$ whenever $c < b \in B$. An equivalent way to write this technically is that $a = \bigvee B$ minimally if $a = \bigvee C$ and $C \ll B$ implies $B \subseteq C$.

A *join cover* of $p \in L$ is a finite set A such that $p \leq \bigvee A$. A join cover A of p is *minimal* if $\bigvee A$ is irredundant and A cannot be properly refined to another join cover of p, i.e., $p \leq \bigvee B$ and $B \ll A$ implies $A \subseteq B$.

We define a binary relation $\underline{D}$ on $J(\mathcal{L})$ as follows: $p \ \underline{D}\ q$ if there exists $x \in L$ such that $p \leq q \vee x$ but $p \not\leq q_* \vee x$. This relation will play an important role in our analysis of the congruences of a principally chain finite lattice.[3]

The following lemma summarizes some properties of principally chain finite lattices and the relation $\underline{D}$.

Lemma 10.1. *Let $\mathcal{L}$ be a principally chain finite lattice.*

(1) *If $b \not\leq a$ in $\mathcal{L}$, then there exists $p \in J(\mathcal{L})$ with $p \leq b$ and $p \not\leq a$.*
(2) *Every join expression in $\mathcal{L}$ refines to a minimal join expression, and every join cover refines to a minimal join cover.*
(3) *For $p, q \in J(\mathcal{L})$ we have $p \ \underline{D}\ q$ if and only if $q \in A$ for some minimal join cover A of p.*

Proof. (1) Since $b \not\leq a$ and $\downarrow b$ satisfies the DCC, the set $\{x \in \downarrow b : x \not\leq a\}$ has at least one minimal element p. Because $y < p$ implies $y \leq a$ for any $y \in L$, we have $\bigvee\{y \in L : y < p\} \leq p \wedge a < p$, and hence $p \in J(\mathcal{L})$ with $p_* = p \wedge a$.

(2) Suppose $\mathcal{L}$ contains an element s with a join representation $s = \bigvee F$ that does not refine to a minimal one. Since the DCC holds in $\downarrow s$, there is an element $t \leq s$ minimal with respect to having a join representation $t = \bigvee A$ which fails to refine to a minimal one. Clearly t is join reducible, and there is a proper, irredundant join expression $t = \bigvee B$ with $B \ll A$.

Let $B = \{b_1, \ldots, b_k\}$. Using the DCC on $\downarrow b_1$, we can find $c_1 \leq b_1$ such that $t = c_1 \vee b_2 \vee \ldots \vee b_k$, but c_1 cannot be replaced by any lower element: $t > u \vee b_2 \vee \ldots b_k$ whenever $u < c_1$. Now apply the same argument to b_2 and $\{c_1, b_2, \ldots, b_k\}$. After k such steps we obtain a join cover C that refines B and is minimal *pointwise*: no element can be replaced by a (single) lower element.

The elements of C may not be join irreducible, but each element of C is strictly below t, and hence has a minimal join expression. Choose a minimal join expression E_c for each $c \in C$. It is not hard to check that $E = \bigcup_{c \in C} E_c$ is a minimal join expression for t, and $E \ll C \ll B \ll A$, which contradicts the choice of t and B.

Now let $u \in L$ and let A be a join cover of u, i.e., $u \leq \bigvee A$. We can find $B \subseteq A$ such that $u \leq \bigvee B$ irredundantly. As above, refine B to a pointwise minimal

[3]Note that $\underline{D}$ is reflexive, i.e., $p \ \underline{D}\ p$ for all $p \in J(\mathbf{L})$. The relation D, defined similarly except that it requires $p \neq q$, is also important, and $\underline{D}$ stands for "D or equal to." For describing congruences, it makes more sense to use $\underline{D}$ rather than D.

join cover C. Now we know that minimal join expressions exist, so we may define $E = \bigcup_{c \in C} E_c$ exactly as before. Then E will be a minimal join cover of u, and again $E \ll C \ll B \ll A$.

(3) Assume $p \, \underline{D} \, q$, and let $x \in L$ be such that $p \leq q \vee x$ but $p \nleq q_* \vee x$. By (2), we can find a minimal join cover A of p with $A \ll \{q, x\}$. Since $p \nleq q_* \vee x$, we must have $q \in A$.

Conversely, if A is a minimal join cover of p, and $q \in A$, then we fulfill the definition of $p \, \underline{D} \, q$ by setting $x = \bigvee(A - \{q\})$. □

Now we want to define a closure operator on the join irreducible elements of a principally chain finite lattice. This closure operator should encode the structure of $\mathcal{L}$ in the same way the order ideal operator $\mathcal{O}$ does for a finite distributive lattice. For $S \subseteq J(\mathcal{L})$, let

$$\Gamma(S) = \{p \in J(\mathcal{L}) : p \leq \bigvee F \text{ for some finite } F \subseteq S\}.$$

It is easy to check that Γ is an algebraic closure operator. The compact (i.e., finitely generated) Γ-closed sets are of the form $\Gamma(F) = \{p \in J(\mathcal{L}) : p \leq \bigvee F\}$ for some finite subset F of $J(\mathcal{L})$. In general, we would expect these to be only a join subsemilattice of the lattice $\mathcal{C}_\Gamma$ of closed sets; however, for a principally chain finite lattice $\mathcal{L}$ the compact closed sets actually form an ideal (and hence a sublattice) of $\mathcal{C}_\Gamma$. For if $S \subseteq \Gamma(F)$ with F finite, then $S \subseteq \downarrow(\bigvee F)$, which satisfies the ACC. Hence $\{\bigvee G : G \subseteq S \text{ and } G \text{ is finite}\}$ has a largest element. So $\bigvee S = \bigvee G$ for some finite $G \subseteq S$, from which it follows that $\Gamma(S) = \Gamma(G)$, and $\Gamma(S)$ is compact. In particular, if $\mathcal{L}$ has a largest element 1, then every closed set will be compact.

With that preliminary observation out of the way, we proceed with our generalization of the order ideal representation for finite distributive lattices.

Theorem 10.2. *If $\mathcal{L}$ is a principally chain finite lattice, then the map ϕ with $\phi(x) = \{p \in J(\mathcal{L}) : p \leq x\}$ is an isomorphism of $\mathcal{L}$ onto the lattice of compact Γ-closed subsets of $J(\mathcal{L})$.*

Proof. Note that if $x = \bigvee A$ is a minimal join expression, then $\phi(x) = \Gamma(A)$, so $\phi(x)$ is indeed a compact Γ-closed set. The map ϕ is clearly order preserving, and it is one-to-one by part (1) of Lemma 10.1. Finally, ϕ is onto because $\Gamma(F) = \phi(\bigvee F)$ for each finite $F \subseteq J(\mathcal{L})$. □

To use this result, we need a structural characterization of Γ-closed sets.

Theorem 10.3. *Let $\mathcal{L}$ be a principally chain finite lattice. A subset C of $J(\mathcal{L})$ is Γ-closed if and only if*

(1) *C is an order ideal of $J(\mathcal{L})$, and*
(2) *if A is a minimal join cover of $p \in J(\mathcal{L})$ and $A \subseteq C$, then $p \in C$.*

Proof. It is easy to see that Γ-closed sets have these properties. Conversely, let $C \subseteq J(\mathcal{L})$ satisfy (1) and (2). We want to show $\Gamma(C) \subseteq C$. If $p \in \Gamma(C)$, then $p \leq \bigvee F$ for some finite subset $F \subseteq C$. By Lemma 10.1(2), there is a minimal join cover A of p refining F; since C is an order ideal, $A \subseteq C$. But then the second closure property gives that $p \in C$, as desired. $\square$

In words, Theorem 10.3 says that for principally chain finite lattices, Γ is determined by the order on $J(\mathcal{L})$ and the minimal join covers of elements of $J(\mathcal{L})$. Hence, by Theorem 10.2, $\mathcal{L}$ is determined by the same factors. Now we would like to see how much of this information we can extract from **Con** $\mathcal{L}$. The answer is, "not much." We will see that from **Con** $\mathcal{L}$ we can find $J(\mathcal{L})$ modulo a certain equivalence relation. We can determine nothing of the order on $J(\mathcal{L})$, nor can we recover the minimal join covers, but we can recover the $\underline{D}$ relation (up to the equivalence). This turns out to be enough to characterize the congruence lattices of principally chain finite lattices.

Now for a group $\mathcal{G}$, the map $\tau : \mathbf{Con}\, \mathcal{G} \to \mathcal{N}(\mathcal{G})$ given by $\tau(\theta) = \{x \in G : x \,\theta\, 1\}$ is a lattice isomorphism. The next two theorems and corollary establish a similar correspondence for principally chain finite lattices.

Theorem 10.4. *Let $\mathcal{L}$ be a principally chain finite lattice. Let σ map* **Con** $\mathcal{L}$ *to the lattice of subsets $\mathcal{P}(J(\mathcal{L}))$ by*

$$\sigma(\theta) = \{p \in J(\mathcal{L}) : p \;\theta\; p_*\}.$$

Then σ is a one-to-one complete lattice homomorphism.

Proof. Clearly σ is order preserving: $\theta \leq \psi$ implies $\sigma(\theta) \subseteq \sigma(\psi)$.

To see that σ is one-to-one, assume $\theta \nleq \psi$. Then there exists a pair of elements $a, b \in L$ with $a < b$ and $(a, b) \in \theta - \psi$. Since $(a, b) \notin \psi$, we also have $(x, b) \notin \psi$ for any element x with $x \leq a$. Let $p \leq b$ be minimal with respect to the property $p \,\psi\, x$ implies $x \nleq a$. We claim that p is join irreducible. If $y_1, \dots, y_n < p$, then for each i there exists an x_i such that $y_i \,\psi\, x_i \leq a$. Hence $\bigvee y_i \,\psi\, \bigvee x_i \leq a$, so $\bigvee y_i < p$. Now $p = p \wedge b \,\theta\, p \wedge a \leq p_*$, implying $p \,\theta\, p_*$, i.e., $p \in \sigma(\theta)$. But $(p, p_*) \notin \psi$ because $p_* \,\psi\, x \leq a$ for some x; thus $p \notin \sigma(\psi)$. Therefore $\sigma(\theta) \nsubseteq \sigma(\psi)$.

It is easy to see that $\sigma(\bigwedge \theta_i) = \bigcap \sigma(\theta_i)$ for any collection of congruences θ_i $(i \in I)$. Since σ is order preserving, we have $\bigcup \sigma(\theta_i) \subseteq \sigma(\bigvee \theta_i)$, and it remains to show that $\sigma(\bigvee \theta_i) \subseteq \bigcup \sigma(\theta_i)$.

If $(p, p_*) \in \bigvee \theta_i$, then there exists a connecting sequence

$$p = x_0 \,\theta_{i_1}\, x_1 \,\theta_{i_2}\, x_2 \dots x_{k-1} \,\theta_{i_k}\, x_k = p_*.$$

Let $y_j = (x_j \vee p_*) \wedge p$. Then $y_0 = p$, $y_k = p_*$, and $p_* \leq y_j \leq p$ implies $y_j \in \{p_*, p\}$ for each j. Moreover, we have $y_{j-1} \theta_{i_j} y_j$ for $j \geq 1$. There must exist a j with $y_{j-1} = p$ and $y_j = p_*$, whence $p \,\theta_{i_j}\, p_*$ and $p \in \sigma(\theta_{i_j}) \subseteq \bigcup \sigma(\theta_i)$. We conclude that σ also preserves arbitrary joins. $\square$

Next we need to identify the range of σ.

Theorem 10.5. *Let $\mathcal{L}$ be a principally chain finite lattice, and let $S \subseteq J(\mathcal{L})$. Then $S = \sigma(\theta)$ for some $\theta \in \mathbf{Con}\,\mathcal{L}$ if and only if $p \,\underline{D}\, q \in S$ implies $p \in S$.*

Proof. Let $S = \sigma(\theta)$. If $q \in S$ and $p \,\underline{D}\, q$, then $q \;\theta\; q_*$, and for some $x \in L$ we have $p \leq q \vee x$ but $p \nleq q_* \vee x$. Thus

$$p = p \wedge (q \vee x) \;\theta\; p \wedge (q_* \vee x) < p.$$

Hence $p \;\theta\; p_*$ and $p \in \sigma(\theta) = S$.

Conversely, assume we are given $S \subseteq J(\mathcal{L})$ satisfying the condition of the theorem. Then we must produce a congruence relation θ such that $\sigma(\theta) = S$. Let $T = J(\mathcal{L}) - S$, and note that T has the property that $q \in T$ whenever $p \,\underline{D}\, q$ and $p \in T$. Define

$$x \;\theta\; y \text{ if } \downarrow x \cap T = \downarrow y \cap T.$$

The motivation for this definition is outlined in the exercises: θ is the kernel of the *standard homomorphism* from $\mathcal{L}$ onto the join subsemilattice of $\mathcal{L}$ generated by $T \cup \{0\}$.

Three things should be clear: θ is an equivalence relation; $x \;\theta\; y$ implies $x \wedge z \;\theta\; y \wedge z$; and for $p \in J(\mathcal{L})$, $p \;\theta\; p_*$ if and only if $p \notin T$, i.e., $p \in S$. (The last statement will imply that $\sigma(\theta) = S$.) It remains to show that θ respects joins.

Assume $x \;\theta\; y$, and let $z \in L$. We want to show $\downarrow(x \vee z) \cap T \subseteq \downarrow(y \vee z) \cap T$, so let $p \in T$ and $p \leq x \vee z$. Then there exists a minimal join cover Q of p with $Q \ll \{x, z\}$. If $q \in Q$ and $q \leq z$, then of course $q \leq y \vee z$. Otherwise $q \leq x$, and since $p \in T$ and $p \,\underline{D}\, q$ (by Lemma 10.1(3)), we have $q \in T$. Thus $q \in \downarrow x \cap T = \downarrow y \cap T$, so $q \leq y \leq y \vee z$. It follows that $p \leq \bigvee Q \leq y \vee z$. This shows $\downarrow(x \vee z) \cap T \subseteq \downarrow(y \vee z) \cap T$; by symmetry, they are equal. Hence $x \vee z \;\theta\; y \vee z$. $\square$

In order to interpret the consequences of these two theorems, let $\trianglelefteq$ denote the transitive closure of $\underline{D}$ on $J(\mathcal{L})$. Then $\trianglelefteq$ is a quasiorder (reflexive and transitive), and so it induces an equivalence relation $\equiv$ on $J(\mathcal{L})$, modulo which $\trianglelefteq$ is a partial order, *viz.*, $p \equiv q$ if and only if $p \trianglelefteq q$ and $q \trianglelefteq p$. If we let $Q_{\mathcal{L}}$ denote the partially ordered set $(J(\mathcal{L})/\equiv, \trianglelefteq)$, then Theorem 10.5 translates as follows.

Corollary. *If $\mathcal{L}$ is a principally chain finite lattice, then $\mathbf{Con}\,\mathcal{L} \cong \mathcal{O}(Q_{\mathcal{L}})$.*

Because the $\underline{D}$ relation is easy to determine, it is not hard to find $Q_{\mathcal{L}}$ for a finite lattice $\mathcal{L}$. Hence this result provides a reasonably efficient algorithm for determining the congruence lattice of a finite lattice. Hopefully, the exercises will convince you of this. As an application, we have the following characterization.

Corollary. *A principally chain finite lattice $\mathcal{L}$ is subdirectly irreducible if and only if $Q_{\mathcal{L}}$ has a least element.*

Now let us turn our attention to the problem of representing a given distributive algebraic lattice $\mathcal{D}$ as the congruence lattice of a lattice. Recall from Chapter 5 that

Fred Wehrung has shown that there are distributive algebraic lattices that are not isomorphic to the congruence lattice of any lattice. However, we can represent a large class that includes all finite lattices.

Not every distributive algebraic lattice is isomorphic to $\mathcal{O}(\mathcal{P})$ for an ordered set $\mathcal{P}$. Indeed, those that are so have a nice characterization.

Lemma 10.6. *The following are equivalent for a distributive algebraic lattice $\mathcal{D}$.*

(1) *$\mathcal{D}$ is isomorphic to the lattice of order ideals of an ordered set.*
(2) *Every element of $\mathcal{D}$ is a join of completely join prime elements.*
(3) *Every compact element of $\mathcal{D}$ is a join of (finitely many) join irreducible compact elements.*

Proof. An order ideal I is compact in $\mathcal{O}(\mathcal{P})$ if and only if it is finitely generated, i.e., $I = \downarrow p_1 \cup \cdots \cup \downarrow p_k$ for some $p_1, \dots, p_k \in P$. Moreover, each $\downarrow p_i$ is join irreducible in $\mathcal{O}(\mathcal{P})$. Thus $\mathcal{O}(\mathcal{P})$ has the property (3).

Note that if $\mathcal{D}$ is a distributive algebraic lattice and p is a join irreducible compact element, then p is completely join prime. For if $p \leq \bigvee U$, then $p \leq \bigvee U'$ for some finite subset $U' \subseteq U$; as join irreducible elements are join prime in a distributive lattice, this implies $p \leq u$ for some $u \in U'$. On the other hand, a completely join prime element is clearly compact and join irreducible, so these elements coincide. If every compact element is a join of join irreducible compact elements, then so is every element of $\mathcal{D}$, whence (3) implies (2).

Now assume that the completely join prime elements of $\mathcal{D}$ are join dense, and let $\mathcal{P}$ denote the set of completely join prime elements with the order they inherit from $\mathcal{D}$. Then it is straightforward to show that the map $\phi : \mathcal{D} \to \mathcal{O}(\mathcal{P})$ given by $\phi(x) = \downarrow x \cap P$ is an isomorphism. $\square$

Now it is not hard to find lattices where these conditions fail. Nonetheless, distributive algebraic lattices with the properties of Lemma 10.6 are a nice class (including all finite distributive lattices), and it behooves us to try to represent each of them as **Con** $\mathcal{L}$ for some principally chain finite lattice $\mathcal{L}$. We need to begin by seeing how $Q_{\mathcal{L}}$ can be recovered from **Con** $\mathcal{L}$.

Theorem 10.7. *Let $\mathcal{L}$ be a principally chain finite lattice. A congruence relation θ is join irreducible and compact in* **Con** $\mathcal{L}$ *if and only if $\theta = \mathrm{con}(p, p_*)$ for some $p \in J$. Moreover, for $p, q \in J$, we have $\mathrm{con}(q, q_*) \leq \mathrm{con}(p, p_*)$ iff $q \trianglelefteq p$.*

Proof. We want to use the representation **Con** $\mathcal{L} \cong \mathcal{O}(Q_{\mathcal{L}})$. Note that if Q is a partially ordered set and I is an order ideal of Q, then $I = \bigcup_{x \in I} \downarrow x$, and, of course, set union is the join operation in $\mathcal{O}(Q)$. Hence join irreducible compact ideals are exactly those of the form $\downarrow x$ for some $x \in Q$.

Applying these remarks to our situation, using the isomorphism, join irreducible compact congruences are precisely those with $\sigma(\theta) = \{q \in J(\mathcal{L}) : q \trianglelefteq p\}$ for some $p \in J(\mathcal{L})$. Recalling that $p \in \sigma(\theta)$ if and only if $p \,\theta\, p_*$, and $\mathrm{con}(p, p_*)$ is the least congruence with $p \,\theta\, p_*$, the conclusions of the theorem follow. $\square$

Theorem 10.8. *Let $\mathcal{D}$ be a distributive algebraic lattice that is isomorphic to $\mathcal{O}(\mathcal{P})$ for some ordered set $\mathcal{P}$. Then there is a principally chain finite lattice $\mathcal{L}$ such that $\mathcal{D} \cong$ **Con** $\mathcal{L}$.*

Proof. We must construct $\mathcal{L}$ with $Q_{\mathcal{L}} \cong \mathcal{P}$. In view of Theorem 10.3 we should try to describe $\mathcal{L}$ as the lattice of finitely generated closed sets of a closure operator on an ordered set J. Let P^0 and P^1 be two unordered copies of the base set P of $\mathcal{P}$, disjoint except on the maximal elements of $\mathcal{P}$. Thus $J = P^0 \cup P^1$ is an antichain, and $p^0 = p^1$ if and only if p is maximal in $\mathcal{P}$. Define a subset C of J to be *closed* if $\{p^j, q^k\} \subseteq C$ implies $p^i \in C$ whenever $p < q$ in $\mathcal{P}$ and $\{i, j\} = \{0, 1\}$. Our lattice $\mathcal{L}$ will consist of all finite closed subsets of J, ordered by set inclusion.

It should be clear that we have made the elements of J atoms of $\mathcal{L}$ and

$$p^i \leq p^j \vee q^k$$

whenever $p < q$ in $\mathcal{P}$. Thus $p^i \, \underline{D} \, q^k$ iff $p \leq q$. (This is where you want only one copy of each maximal element). It remains to check that $\mathcal{L}$ is indeed a principally chain finite lattice with $Q_{\mathcal{L}} \cong \mathcal{P}$, as desired. The crucial observation is that the closure of a finite set is finite. We will leave this verification to the reader. □

Theorem 10.8 is due to R. P. Dilworth in the 1940's, but his proof was never published. The construction given is from George Grätzer and E. T. Schmidt [5].

We close this section with a new look at a pair of classic results. A lattice is said to be *relatively complemented* if $a < x < b$ implies there exists y such that $x \wedge y = a$ and $x \vee y = b$.[4]

Theorem 10.9. *If $\mathcal{L}$ is a principally chain finite lattice which is either modular or relatively complemented, then the relation $\underline{D}$ is symmetric on $J(\mathcal{L})$, and hence* **Con** $\mathcal{L}$ *is a Boolean algebra.*

Proof. First assume $\mathcal{L}$ is modular, and let $p \, \underline{D} \, q$ with $p \leq q \vee x$ but $p \not\leq q_* \vee x$. Using modularity, we have

$$(q \wedge (p \vee x)) \vee x = (q \vee x) \wedge (p \vee x) \geq p,$$

so $q \leq p \vee x$. On the other hand, if $q \leq p_* \vee x$, we would have

$$p = p \wedge (q \vee x) \leq p \wedge (p_* \vee x) = p_* \vee (x \wedge p) = p_*,$$

a contradiction. Hence $q \not\leq p_* \vee x$, and $q \, \underline{D} \, p$.

Now assume $\mathcal{L}$ is relatively complemented and $p \, \underline{D} \, q$ as above. Observe that a join irreducible element in a relatively complemented lattice must be an atom.

[4] Thus a relatively complemented lattice with 0 and 1 is complemented, but otherwise it need not be.

Hence $p_* = q_* = 0$, and given x such that $p \le q \vee x$, $p \not\le x$, we want to find y such that $q \le p \vee y$ and $q \not\le y$. Since $x < p \vee x \le q \vee x$, we can choose y to be a relative complement of $p \vee x$ in the interval $(q \vee x)/x$. Then $p \vee y = p \vee x \vee y \ge q$, and $q \not\le y$ for otherwise would imply $p \le y \wedge (p \vee x) = x$, a contradiction. Thus $q \, \underline{D} \, p$.

Finally, if $\underline{D}$ is symmetric, then $Q_{\mathcal{L}}$ is an antichain, and thus $\mathcal{O}(Q_{\mathcal{L}})$ is isomorphic to the Boolean algebra $\mathcal{P}(Q_{\mathcal{L}})$. □

A lattice is *simple* if $|L| > 1$ and $\mathcal{L}$ has no proper nontrivial congruence relations, i.e., **Con** $\mathcal{L} \cong \mathbf{2}$. Theorem 10.9 says that a subdirectly irreducible, modular or relatively complemented, principally chain finite lattice must be simple.

In the relatively complemented case we get even more. Let $\mathcal{L}_i$ $(i \in I)$ be a collection of lattices with 0. The *direct sum* $\sum \mathcal{L}_i$ is the sublattice of the direct product consisting of all elements that are only finitely non-zero. Combining Theorems 10.2 and 10.9, we obtain relatively easily a fine result of Dilworth [2].

Theorem 10.10. *A relatively complemented principally chain finite lattice is a direct sum of simple (relatively complemented principally chain finite) lattices.*

Proof. Let $\mathcal{L}$ be a relatively complemented principally chain finite lattice. Then every element of L is a finite join of join irreducible elements, every join irreducible element is an atom, and the $\underline{D}$ relation is symmetric, i.e., $p \, \underline{D} \, q$ implies $p \equiv q$. We can write $J(\mathcal{L})$ as a disjoint union of $\equiv$-classes, $J(\mathcal{L}) = \dot{\bigcup}_{i \in I} A_i$. Let

$$L_i = \{x \in L : x = \bigvee F \text{ for some finite } F \subseteq A_i\}.$$

We want to show that the L_i's are ideals (and hence sublattices) of $\mathcal{L}$, and that $\mathcal{L} \cong \sum_{i \in I} \mathcal{L}_i$.

The crucial technical detail is this: *if $p \in J(\mathcal{L})$, $F \subseteq J(\mathcal{L})$ is finite, and $p \le \bigvee F$, then $p \equiv f$ for some $f \in F$.* For F can be refined to a minimal join cover G of p, and since join irreducible elements are atoms, we must have $G \subseteq F$. But $p \, \underline{D} \, g$ (and hence $p \equiv g$) for every $g \in G$.

Now we can show that each $\mathcal{L}_i$ is an ideal of $\mathcal{L}$. Suppose $y \le x \in L_i$. Then $x = \bigvee F$ for some $F \subseteq A_i$, and $y = \bigvee H$ for some minimal join expression $H \subseteq J(\mathcal{L})$. By the preceding observation, $H \subseteq A_i$, and thus $y \in L_i$.

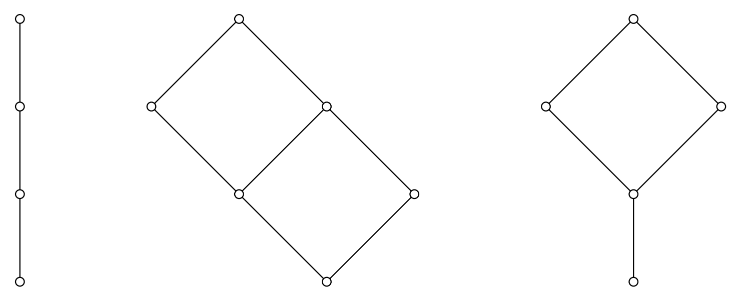
Define a map $\phi : \mathcal{L} \to \sum_{i \in I} \mathcal{L}_i$ by $\phi(x) = (x_i)_{i \in I}$, where $x_i = \bigvee {\downarrow} x \cap A_i)$. There are several things to check: that $\phi(x)$ is only finitely nonzero, that ϕ is one-to-one and onto, and that it preserves meets and joins. None is very hard, so we will only do the last one, and leave the rest to the reader.

We want to show that ϕ preserves joins, i.e., that $(x \vee y)_i = x_i \vee y_i$. It suffices to show that if $p \in J(\mathcal{L})$ and $p \le (x \vee y)_i$, then $p \le x_i \vee y_i$. Since $\mathcal{L}_i$ is an ideal, we have $p \in A_i$. Furthermore, since $p \le x \vee y$, there is a minimal join cover F of p refining $\{x, y\}$. For each $f \in F$, we have $f \le x$ or $f \le y$, and $p \, \underline{D} \, f$ implies $f \in A_i$; hence $f \le x_i$ or $f \le y_i$. Thus $p \le \bigvee F \le x_i \vee y_i$. □

Exercises for Chapter 10

1. Do Exercise 1 of Chapter 5 using the methods of this chapter.

2. Use the construction from the proof of Theorem 10.8 to represent the distributive lattices in Figure 10.1 as congruence lattices of lattices.



(a) (b) (c)

Figure 10.1

3. Let $a = \bigvee B$ be a join expression in a lattice $\mathcal{L}$. Prove that the following two properties (used to define minimality) really are equivalent.

(a) $B \subseteq J(\mathcal{L})$ and $c \vee \bigvee(B - \{b\}) < a$ whenever $c < b \in B$.

(b) $a = \bigvee C$ and $C \ll B$ implies $B \subseteq C$.

4. Let $\mathcal{P}$ be an ordered set satisfying the DCC, and let $\mathcal{Q}$ be the set of finite antichains of $\mathcal{P}$, ordered by $\ll$. Show that $\mathcal{Q}$ satisfies the DCC. (This argument is rather tricky, but it is the proper explanation of Lemma 10.1(2).)

5. Let p be a join irreducible element in a principally chain finite lattice. Show that p is join prime if and only if $p \underline{D} q$ implies $p = q$.

6. Let $\mathcal{L}$ be a principally chain finite lattice, and $p \in J(\mathcal{L})$. Prove that there is a congruence ψ_p on $\mathcal{L}$ such that, for all $\theta \in \mathbf{Con}\,\mathcal{L}$, $(p, p_*) \notin \theta$ if and only if $\theta \leq \psi_p$.

(More generally, the following is true: Given a lattice $\mathcal{L}$ and a filter F of $\mathcal{L}$, there is a unique congruence ψ_F maximal with respect to the property that $(x, f) \in \theta$ implies $x \in F$ for all $x \in L$ and $f \in F$.)

7. Prove that a distributive lattice is isomorphic to $\mathcal{O}(\mathcal{P})$ for some ordered set $\mathcal{P}$ if and only if it is algebraic and dually algebraic. (This extends Lemma 10.6.)

8. A complete lattice is *completely distributive* if it satisfies the identity

$$\bigwedge_{i \in I} \bigvee_{j \in J} x_{ij} = \bigvee_{f \in J^I} \bigwedge_{i \in I} x_{if(i)}$$

where J^I denotes the set of all $f : I \to J$.

(1) Show that this identity is equivalent to its dual.

(2) Prove that $\mathcal{O}(\mathcal{P}))$ is completely distributive for any ordered set $\mathcal{P}$.

(Indeed, a complete lattice $\mathcal{L}$ is completely distributive if and only if there is a complete surjective homomorphism $h : \mathcal{O}(\mathcal{P}) \to \mathcal{L}$, for some ordered set $\mathcal{P}$; see Raney [10].)

9. Let $\mathcal{L}$ be a principally chain finite lattice, and let $T \subseteq J(\mathcal{L})$ have the property that $p \, \underline{D} \, q$ and $p \in T$ implies $q \in T$.

(a) Show that the join subsemilattice $\mathcal{S}$ of $\mathcal{L}$ generated by $T \cup \{0\}$, i.e., the set of all $\bigvee F$ where F is a finite subset of $T \cup \{0\}$, is a lattice. ($\mathcal{S}$ need not a be sublattice of $\mathcal{L}$, because the meet operation is different.)

(b) Prove that the map $f : \mathcal{L} \twoheadrightarrow \mathcal{S}$ given by $f(x) = \bigvee \downarrow x \cap T)$ is a lattice homomorphism.

(c) Show that the kernel of f is the congruence relation θ in the proof of Theorem 10.5.

10. Prove that if $\mathcal{L}$ is a finite lattice, then $\mathcal{L}$ can be embedded into a finite lattice $\mathcal{K}$ such that $\mathbf{Con}\,\mathcal{L} \cong \mathbf{Con}\,\mathcal{K}$ and every element of $\mathcal{K}$ is a join of atoms. (Michael Tischendorf)

11. Express the lattice of all finite subsets of a set X as a direct sum of two-element lattices.

12. Show that if $\mathcal{A}$ is a torsion abelian group, then the compact subgroups of $\mathcal{A}$ form a principally chain finite lattice (Khalib Benabdallah).

The main arguments in this chapter originated in a slightly different setting, geared towards application to lattice varieties [7], the structure of finitely generated free lattices [4], or finitely presented lattices [3]. The last three exercises give the version of these results which has proved most useful for these types of applications, with an example.

A lattice homomorphism $f : \mathcal{L} \to \mathcal{K}$ is *lower bounded* if for every $a \in K$, the set $\{x \in L : f(x) \geq a\}$ is either empty or has a least element, which is denoted $\beta(a)$. If f is onto, this is equivalent to saying that each congruence class of $\ker f$ has a least element. For example, if $\mathcal{L}$ satisfies the DCC, then every homomorphism $f : \mathcal{L} \to \mathcal{K}$ will be lower bounded. The dual condition is called *upper bounded*. These notions were introduced by Ralph McKenzie in [7].

13. Let $\mathcal{L}$ be a lattice with 0, $\mathcal{K}$ a finite lattice, and $f : \mathcal{L} \twoheadrightarrow \mathcal{K}$ a lower bounded, surjective homomorphism. Let $T = \{\beta(p) : p \in J(\mathcal{K})\}$. Show that:

(a) $T \subseteq J(\mathcal{L})$;

(b) $\mathcal{K}$ is isomorphic to the join subsemilattice $\mathcal{S}$ of $\mathcal{L}$ generated by $T \cup \{0\}$;

(c) for each $t \in T$, every join cover of t in $\mathcal{L}$ refines to a join cover of t contained in T.

14. Conversely, let $\mathcal{L}$ be a lattice with 0, and let T be a finite subset of $J(\mathcal{L})$ satisfying condition (c) of Exercise 13. Let $\mathcal{S}$ denote the join subsemilattice of $\mathcal{L}$ generated by $T \cup \{0\}$. Prove that the map $f : \mathcal{L} \twoheadrightarrow \mathcal{S}$ given by $f(x) = \bigvee \downarrow x \cap T)$ is a lower bounded lattice homomorphism with $\beta f(t) = t$ for all $t \in T$.

15. Let f be the (essentially unique) homomorphism from $FL(3)$ onto $\mathcal{N}_5$. Show that f is lower bounded. (By duality, f is also upper bounded.)

References

1. A. Day, *Characterizations of finite lattices that are bounded-homomorphic images or sublattices of free lattices*, Canad. J. Math **31** (1979), 69–78.
2. R. P. Dilworth, *The structure of relatively complemented lattices*, Ann. of Math. **51** (1950), 348–359.
3. R. Freese, *Finitely presented lattices: canonical forms and the covering relation*, Trans. Amer. Math. Soc. **312** (1989), 841–860.
4. R. Freese and J. B. Nation, *Covers in free lattices*, Trans. Amer. Math. Soc. **288** (1985), 1–42.
5. G. Grätzer and E. T. Schmidt, *On congruence lattices of lattices*, Acta Math. Acad. Sci. Hungar. **13** (1962), 179–185.
6. B. Jónsson and J. B. Nation, *A report on sublattices of a free lattice*, Coll. Math. Soc. János Bolyai **17** (1977), 233–257.
7. R. McKenzie, *Equational bases and non-modular lattice varieties*, Trans. Amer. Math. Soc. **174** (1972), 1–43.
8. J. B. Nation, *Lattice varieties covering $V(L_1)$*, Algebra Universalis **23** (1986), 132–166.
9. J. B. Nation, *An approach to lattice varieties of finite height*, Algebra Universalis **27** (1990), 521–543.
10. G. N. Raney, *Completely distributive complete lattices*, Proc. Amer. Math. Soc. **3** (1952), 677–680.

11. Geometric Lattices

Many's the time I've been mistaken
And many times confused . . . .
–Paul Simon

Now let us consider how we might use lattices to describe elementary geometry. There are two basic aspects of geometry: *incidence*, involving such statements as "the point p lies on the line l," and *measurement*, involving such concepts as angles and length. We will restrict our attention to incidence, which is most naturally stated in terms of lattices.

What properties should a *geometry* have? Without being too formal, surely we would want to include the following.

(1) The elements of a geometry (points, lines, planes, etc.) are subsets of a given set P of points.
(2) Each point $p \in P$ is an element of the geometry.
(3) The set P of all points is an element of the geometry, and the intersection of any collection of elements is again one.
(4) There is a dimension function on the elements of the geometry, satisfying some sort of reasonable conditions.

If we order the elements of a geometry by set inclusion, then we obtain a lattice in which the atoms correspond to points of the geometry, every element is a join of atoms, and there is a well-behaved dimension function defined. With a little more care we can show that "well-behaved" means "semimodular" (recall Theorem 9.6). On the other hand, there is no harm if we allow some elements to have infinite dimension.

Accordingly, we define a *geometric lattice* to be an algebraic semimodular lattice in which every element is a join of atoms. As we have already described, the points, lines, planes, etc. (and the empty set) of a finite dimensional Euclidean geometry ($\Re^n$) form a geometric lattice. Other examples are the lattice of all subspaces of a vector space, and the lattice **Eq** X of equivalence relations on a set X. More examples are included in the exercises.[1]

[1] The basic properties of geometric lattices were developed by Garrett Birkhoff in the 1930's [3]. Similar ideas were pursued by K. Menger, F. Alt and O. Schreiber at about the same time [12]. Traditionally, geometric lattices were required to be finite dimensional, meaning $\delta(1) = n < \infty$. The last two examples show that this restriction is artificial.

We should note here that the geometric dimension of an element is generally one less than the lattice dimension δ: points are elements with $\delta(p) = 1$, lines are elements with $\delta(l) = 2$, and so forth.

A lattice is said to be *atomistic* if every element is a join of atoms.

Theorem 11.1. *The following are equivalent.*

1. $\mathcal{L}$ *is a geometric lattice.*
2. $\mathcal{L}$ *is an upper continuous, atomistic, semimodular lattice.*
3. $\mathcal{L}$ *is isomorphic to the lattice of ideals of an atomistic, semimodular, principally chain finite lattice.*

In fact, we will show that if $\mathcal{L}$ is a geometric lattice and $\mathcal{K}$ its set of finite dimensional elements, then $\mathcal{L} \cong \mathcal{I}(\mathcal{K})$ and $\mathcal{K}$ is the set of compact elements of $\mathcal{L}$.

Proof. Every algebraic lattice is upper continuous, so (1) implies (2).

For (2) implies (3), we first note that the atoms of an upper continuous lattice are compact. For if $a \succ 0$ and $a \nleq \bigvee F$ for every finite $F \subseteq U$, then by Theorem 3.7 we have $a \wedge \bigvee U = \bigvee (a \wedge \bigvee F) = 0$, whence $a \nleq \bigvee U$. Thus in a lattice $\mathcal{L}$ satisfying condition (2), the compact elements are precisely the elements that are the join of finitely many atoms, in other words (using semimodularity) the finite dimensional elements. Let $\mathcal{K}$ denote the ideal of all finite dimensional elements of $\mathcal{L}$. Then $\mathcal{K}$ is a semimodular principally chain finite sublattice of $\mathcal{L}$, and it is not hard to see that the map $\phi : \mathcal{L} \to \mathcal{I}(\mathcal{K})$ by $\phi(x) = \downarrow x \,\cap\, \mathcal{K}$ is an isomorphism.

Finally, we need to show that if $\mathcal{K}$ is a semimodular principally chain finite lattice with every element the join of atoms, then $\mathcal{I}(\mathcal{K})$ is a geometric lattice. Clearly $\mathcal{I}(\mathcal{K})$ is algebraic, and every ideal is the join of the elements, and hence the atoms, it contains. It remains to show that $\mathcal{I}(\mathcal{K})$ is semimodular.

Suppose $I \succ I \cap J$ in $\mathcal{I}(\mathcal{K})$. Fix an atom $a \in I - J$. Then $I = (I \cap J) \vee \downarrow a$, and hence $I \vee J = \downarrow a \,\vee\, J$. Let x be any element in $(I \vee J) - J$. Since $x \in I \vee J$, there exists $j \in J$ such that $x \leq a \vee j$. Because $\mathcal{K}$ is semimodular, $a \vee j \succ j$. On the other hand, every element of $\mathcal{K}$ is a join of finitely many atoms, so $x \notin J$ implies there exists an atom $b \leq x$ with $b \notin J$. Now $b \leq a \vee j$ and $b \nleq j$, so $b \vee j = a \vee j$, whence $a \leq b \vee j$. Thus $\downarrow b \,\vee\, J = I \vee J$; *a fortiori* it follows that $\downarrow x \,\vee\, J = I \vee J$. As this holds for every $x \in (I \vee J) - J$, we have $I \vee J \succ J$, as desired. $\square$

At the heart of the preceding proof is the following little argument: *if $\mathcal{L}$ is semimodular, a and b are atoms of $\mathcal{L}$, $t \in L$, and $b \leq a \vee t$ but $b \nleq t$, then $a \leq b \vee t$.* It is useful to interpret this property in terms of closure operators.

A closure operator Γ has the *exchange property* if $y \in \Gamma(B \cup \{x\})$ and $y \notin \Gamma(B)$ implies $x \in \Gamma(B \cup \{y\})$. Examples of algebraic closure operators with the exchange property include the span of a set of vectors in a vector space, and the geometric closure of a set of points in Euclidean space. More generally, we have the following representation theorem for geometric lattices, due to Saunders Mac Lane [11].

Theorem 11.2. *A lattice $\mathcal{L}$ is geometric if and only if $\mathcal{L}$ is isomorphic to the lattice of closed sets of an algebraic closure operator with the exchange property.*

Proof. Given a geometric lattice $\mathcal{L}$, we can define a closure operator Γ on the set A of atoms of $\mathcal{L}$ by

$$\Gamma(X) = \{a \in A : a \leq \bigvee X\}.$$

Since the atoms are compact, this is an algebraic closure operator. By the little argument above, Γ has the exchange property. Because every element is a join of atoms, the map $\phi : \mathcal{L} \to \mathcal{C}_\Gamma$ given by $\phi(x) = \{a \in A : a \leq x\}$ is an isomorphism.

Now assume we have an algebraic closure operator Γ with the exchange property. Then $\mathcal{C}_\Gamma$ is an algebraic lattice. The exchange property insures that the closure of a singleton, $\Gamma(x)$, is either the least element $\Gamma(\emptyset)$ or an atom of $\mathcal{C}_\Gamma$: if $y \in \Gamma(x)$, then $x \in \Gamma(y)$, so $\Gamma(x) = \Gamma(y)$. Clearly, for every closed set we have $B = \bigvee_{b \in B} \Gamma(B)$. It remains to show that $\mathcal{C}_\Gamma$ is semimodular.

Let B and C be closed sets with $B \succ B \cap C$. Then $B = \Gamma(\{x\} \cup (B \cap C))$ for any $x \in B - (B \cap C)$. Suppose $C < D \leq B \vee C = \Gamma(B \cup C)$, and let y be any element in $D - C$. Fix any element $x \in B - (B \cap C)$. Then $y \in \Gamma(C \cup \{x\}) = B \vee C$, and $y \notin \Gamma(C) = C$. Hence $x \in \Gamma(C \cup \{y\})$, and $B \leq \Gamma(C \cup \{y\}) \leq D$. Thus $D = B \vee C$, and we conclude that $\mathcal{C}_\Gamma$ is semimodular. $\square$

Now we turn our attention to the structure of geometric lattices.

Theorem 11.3. *Every geometric lattice is relatively complemented.*

Proof. Let $a < x < b$ in a geometric lattice. By upper continuity and Zorn's Lemma, there exists an element y maximal with respect to the properties $a \leq y \leq b$ and $x \wedge y = a$. Suppose $x \vee y < b$. Then there is an atom p with $p \leq b$ and $p \not\leq x \vee y$. By the maximality of y we have $x \wedge (y \vee p) > a$; hence there is an atom q with $q \leq x \wedge (y \vee p)$ and $q \not\leq a$. Now $q \leq y \vee p$ but $q \not\leq y$, so by our usual argument $p \leq q \vee y \leq x \vee y$, a contradiction. Thus $x \vee y = b$, and y is a relative complement of x in $[a, b]$. $\square$

Let $\mathcal{L}$ be a geometric lattice, and let $\mathcal{K}$ be the ideal of compact elements of $\mathcal{L}$. By Theorem 10.10, $\mathbf{K}$ is a direct sum of simple lattices, and by Theorem 11.1, $\mathcal{L} \cong \mathcal{I}(\mathbf{K})$. So what we need now is a relation between the ideal lattice of a direct sum and the direct product of the corresponding ideal lattices.

Lemma 11.4. *For any collection of lattices $\mathbf{K}_i$ $(i \in I)$, we have $\mathcal{I}(\sum \mathbf{K}_i) \cong \prod \mathcal{I}(\mathbf{K}_i)$.*

Proof. If we identify $\mathbf{K}_i$ with the set of all vectors in $\sum \mathbf{K}_i$ that are zero except in the i-th place, then there is a natural map $\phi : \mathcal{I}(\sum \mathbf{K}_i) \to \prod \mathcal{I}(\mathbf{K}_i)$ given by $\phi(J) = \langle J_i \rangle_{i \in I}$, where $J_i = \{x \in L_i : x \in J\}$. It will be a relatively straightforward argument to show that this is an isomorphism. Clearly $J_i \in \mathcal{I}(\mathbf{K}_i)$, and the map ϕ is order preserving.

Assume $J, H \in \mathcal{I}(\sum \mathbf{K}_i)$ with $J \nleq H$, and let $x \in J - H$. There exists an i_0 such that $x_{i_0} \notin H$, and hence $J_{i_0} \nleq H_{i_0}$, whence $\phi(J) \nleq \phi(H)$. Thus $\phi(J) \leq \phi(H)$ if and only if $J \leq H$, so that ϕ is one-to-one.

It remains to show that ϕ is onto. Given $\langle T_i \rangle_{i \in I} \in \prod \mathcal{I}(\mathbf{K}_i)$, let $J = \{x \in \sum L_i : x_i \in T_i \text{ for all } i\}$. Then $J \in \mathcal{I}(\sum \mathbf{K}_i)$, and it is not hard to see that $J_i = T_i$ for all i, and hence $\phi(J) = \langle T_i \rangle_{i \in I}$, as desired. □

Thus if $\mathcal{L}$ is a geometric lattice and $\mathbf{K} = \sum \mathbf{K}_i$, with each $\mathbf{K}_i$ simple, its ideal of compact elements, then $\mathcal{L} \cong \prod \mathcal{I}(\mathbf{K}_i)$. Now each $\mathbf{K}_i$ is a simple semimodular lattice in which every element is a finite join of atoms. The direct factors of $\mathcal{L}$ are ideal lattices of those types of lattices.

So consider an ideal lattice $\mathcal{H} = \mathcal{I}(\mathbf{K})$ where $\mathbf{K}$ is a simple semimodular lattice wherein every element is a join of finitely many atoms. We claim that $\mathcal{H}$ is subdirectly irreducible: the unique minimal congruence μ is generated by collapsing all the finite dimensional intervals of $\mathcal{H}$. This is because any two prime quotients in $\mathbf{K}$ are projective, which property is inherited by $\mathcal{H}$. So if $\mathbf{K}$ is finite dimensional, whence $\mathcal{H} \cong \mathbf{K}$, then $\mathcal{H}$ is simple, and it may be simple even though $\mathbf{K}$ is not finite dimensional, as is the case with $\mathbf{Eq}\ X$. On the other hand, if $\mathbf{K}$ is modular and infinite dimensional, then μ will identify only those pairs (a, b) such that $[a \wedge b, a \vee b]$ is finite dimensional, and so $\mathcal{L}$ will not be simple. Summarizing, we have the following result.

Theorem 11.5. *Every geometric lattice is a direct product of subdirectly irreducible geometric lattices. Every finite dimensional geometric lattice is a direct product of simple geometric lattices.*

The finite dimensional case of Theorem 11.5 should be credited to Dilworth [4], and the extension is due to J. Hashimoto [8]. The best version of Hashimoto's theorem states that *a complete, weakly atomic, relatively complemented lattice is a direct product of subdirectly irreducible lattices.* A nice variation, due to L. Libkin [10], is that *every atomistic algebraic lattice is a direct product of directly indecomposable (atomistic algebraic) lattices.*

Before going on to modular geometric lattices, we should mention one of the most intriguing problems in combinatorial lattice theory. Let $\mathcal{L}$ be a finite geometric lattice, and let

$$w_k = |\{x \in L : \delta(x) = k\}|.$$

The *unimodal conjecture* states that there is always an integer m such that

$$1 = w_0 \leq w_1 \leq \dots w_{m-1} \leq w_m \geq w_{m+1} \geq \dots w_{n-1} \geq w_n = 1.$$

This is true if $\mathcal{L}$ is modular, and also for $\mathcal{L} = \mathbf{Eq}\ X$ with X finite ([7] and [9]). It is known that $w_1 \leq w_k$ always holds for for $1 \leq k < n$ ([2] and [6]). But a general resolution of the conjecture still seems to be a long way off. For related results, see Dowling and Wilson [5].

We note in closing that a very different kind of geometry is obtained if one considers instead closure operators with the *anti-exchange property*: $y \in \Gamma(B \cup \{x\})$ and $y \notin \Gamma(B)$ implies $x \notin \Gamma(B \cup \{y\})$. For a comprehensive account of these convex geometries, as well as the appropriate history and original sources, see Adaricheva, Gorbunov and Tumanov [1].

Exercises for Chapter 11

1. This exercise gives a method for constructing new geometric lattices from known ones.

(a) Let $\mathcal{L}$ be a lattice, and let F be a nonempty order filter on $\mathcal{L}$, i.e., $x \geq f \in F$ implies $x \in F$. Show that the ordered set $\widehat{L}$ obtained by identifying all the elements of F (a join semilattice congruence) is a lattice.

(b) Let $\mathcal{L}$ be a finite dimensional semimodular lattice, with dimension n say, so that $\delta(1) = n$. Let $k < n$, and let the order filter F consist of all elements $x \in L$ with dimension $\delta(x) \geq k$. Show that $\widehat{L}$ is again semimodular, with dimension k. Note that if $\mathcal{L}$ is atomistic, then so is $\widehat{L}$.

(c) Give an example of a geometric lattice $\mathcal{L}$ and a filter F such that the lattice $\widehat{L}$ obtained by this construction is not semimodular.

2. Draw the following geometric lattices and their corresponding geometries:

(a) **Eq 4**,

(b) **Sub** $(Z_2)^3$, the lattice of subspaces of a 3-dimensional vector space over Z_2.

3. Show that each of the following is an algebraic closure operator on $\Re^n$, and interpret them geometrically. Which ones have the exchange property, and which the anti-exchange property?

(a) $\text{Span}(A) = \{\sum_{i=1}^{k} \lambda_i a_i : k \geq 1,\ a_i \in A \cup \{0\}\}$

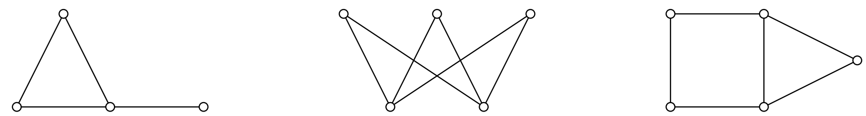
(b) $\Gamma(A) = \{\sum_{i=1}^{k} \lambda_i a_i : k \geq 1,\ a_i \in A,\ \sum_{i=1}^{k} \lambda_i = 1\}$

(c) $\Delta(A) = \{\sum_{i=1}^{k} \lambda_i a_i : k \geq 1,\ a_i \in A,\ \sum_{i=1}^{k} \lambda_i = 1,\ \lambda_i \geq 0\}$

4. Let G be a simple graph (no loops or multiple edges), and let X be the set of all edges of G. Define $S \subseteq X$ to be *closed* if whenever S contains all but one edge of a cycle, then it contains the entire cycle. Verify that the corresponding closure operator E is an algebraic closure operator with the exchange property. The lattice of E-closed subsets is called the *edge lattice* of G. Find the edge lattices of the graphs in Figure 11.1.

5. Show that the lattice for plane Euclidean geometry ($\Re^2$) is not modular. (Hint: Use two parallel lines and a point on one of them.)

6. (a) Let P and L be nonempty sets, which we will think of as "points" and "lines" respectively. Suppose we are given an arbitrary incidence relation $\in$ on $P \times L$. Then we can make $P \cup L \cup \{0, 1\}$ into a partially ordered set $\mathcal{K}$ in the obvious way, interpreting $p \in l$ as $p \leq l$. When is $\mathcal{K}$ a lattice? atomistic? semimodular? modular? subdirectly irreducible?



(a) (b) (c)

FIGURE 11.1

(b) Compare these results with Hilbert's axioms for a plane geometry.

(i) There exists at least one line.
(ii) On each line there exist at least two points.
(iii) Not all points are on the same line.
(iv) There is one and only one line passing through two given distinct points.

7. Let $\mathcal{L}$ be a geometric lattice, and let A denote the set of atoms of $\mathcal{L}$. A subset $S \subseteq A$ is *independent* if $p \not\leq \bigvee(S - \{p\})$ for all $p \in S$. A subset $B \subseteq A$ is a *basis* for $\mathcal{L}$ if B is independent and $\bigvee B = 1$.

(a) Prove that $\mathcal{L}$ has a basis.
(b) Prove that if B and C are bases for $\mathcal{L}$, then $|B| = |C|$.
(c) Show that the sublattice generated by an independent set S is isomorphic to the lattice of all finite subsets of S.

8. A lattice is *atomic* if for every $x > 0$ there exists $a \in L$ with $x \geq a \succ 0$. Prove that every element of a complete, relatively complemented, atomic lattice is a join of atoms.

9. Let I be an infinite set, and let $X = \{p_i : i \in I\} \dot\cup \{q_i : i \in I\}$. Define a subset S of X to be closed if $S = X$ or, for all i, at most one of p_i, q_i is in S. Let $\mathcal{L}$ be the lattice of all closed subsets of X.

(a) Prove that $\mathcal{L}$ is a relatively complemented algebraic lattice with every element the join of atoms.
(b) Show that the compact elements of $\mathcal{L}$ do not form an ideal.

(This example shows that the semimodularity hypothesis of Theorem 11.1 cannot be omitted.)

10. Prove that **Eq** X is relatively complemented and simple (Ore [13]).

11. Let $\mathcal{L}$ be a modular geometric lattice. Prove that $\mathcal{L}$ is subdirectly irreducible (in the finite dimensional case, simple) if and only if the following condition holds: *for any two distinct atoms a, b of $\mathcal{L}$, there exists a third atom c such that* $a \vee b = a \vee c = b \vee c$, i.e., the three atoms generate a diamond. Give an example to show that this condition is not necessary in the nonmodular (but still semimodular) case.

12. On a modular lattice $\mathcal{M}$, define a relation $a \,\mu\, b$ iff $[a \wedge b, a \vee b]$ has finite length. Show that μ is a congruence relation.

References

1. K.V. Adaricheva, V.A. Gorbunov and V.I. Tumanov, *Join-semidistributive lattices and convex geometries*, Advances in Math. **173** (2003), 1–49.
2. J. G. Basterfield and L. M. Kelly, *A characterization of sets of n points which determine n hyperplanes*, Proc. Camb. Phil. Soc. **64** (1968), 585–588.
3. G. Birkhoff, *Abstract linear dependence and lattices*, Amer. J. Math. **57** (1935), 800–804.
4. R. P. Dilworth, *A decomposition theorem for partially ordered sets*, Ann. of Math. **51** (1950), 161–166.
5. T.A. Dowling and R.M. Wilson, *Whitney number inequalities for geometric lattices*, Proc. Amer. Math. Soc. **47** (1975), 504–512.
6. C. Greene, *A rank inequality for finite geometric lattices*, J. Comb. Theory **9** (1970), 357–364.
7. L. H. Harper, *The morphology of partially ordered sets*, J. Combin. Theory Ser. A **17** (1974), 44–58.
8. J. Hashimoto, *Direct, subdirect decompositions and congruence relations*, Osaka J. Math. **9** (1957), 87–112.
9. W. N. Hsieh and D. J. Kleitman, *Normalized matching in direct products of partial orders*, Stud. Appl. Math. **52** (1973), 258–289.
10. L. Libkin, *Direct decompositions of atomistic algebraic lattices*, Algebra Universalis **33** (1995), 127–135.
11. S. Mac Lane, *A lattice formulation for transcendence degrees and p-bases*, Duke Math. J. **4** (1938), 455–468.
12. K. Menger, F. Alt, and O. Schreiber, *New foundations of projective and affine geometry*, Ann. of Math. **37** (1936), 456–482.
13. O. Ore, *Theory of equivalence relations*, Duke Math. J. **9** (1942), 573–627.

Appendix 1: Cardinals, Ordinals and Universal Algebra

In these notes we are assuming you have a working knowledge of cardinals and ordinals. Just in case, this appendix will give an informal summary of the most basic part of this theory. We also include an introduction to the terminology of universal algebra.

1. Ordinals

Let C be a well ordered set, i.e., a chain satisfying the descending chain condition (DCC). A *segment* of C is a proper ideal of C, which (because of the DCC) is necessarily of the form $\{c \in C : c < d\}$ for some $d \in C$.

Lemma. *Let C and D be well ordered sets. Then*

(1) *C is not isomorphic to any segment of itself.*
(2) *Either $C \cong D$, or C is isomorphic to a segment of D, or D is isomorphic to a segment of C.*

We say that two well ordered sets have the same *type* if $C \cong D$. An *ordinal* is an order type of well ordered sets. These are usually denoted by lower case Greek letters: α, β, γ, etc. For example, ω denotes the order type of the natural numbers, which is the smallest infinite ordinal. We can order ordinals by setting $\alpha \leq \beta$ if $\alpha \cong \beta$ or α is isomorphic to a segment of β. There are too many ordinals in the class of all ordinals to call this an ordered set without getting into set theoretic paradoxes, but we can say that locally it behaves like one big well ordered set.

Theorem. *Let β be an ordinal, and let B be the set of all ordinals α with $\alpha < \beta$, ordered by $\leq$. Then $B \cong \beta$.*

For example, ω is isomorphic to the collection of all finite ordinals.

Recall that the Zermelo well ordering principle (which is equivalent to the Axiom of Choice) says that every set can be well ordered. Another way of putting this is that every set can be indexed by ordinals,

$$X = \{x_\alpha : \alpha < \beta\}$$

for some β. Transfinite induction is a method of proof that involves indexing a set by ordinals, and then applying induction on the indices. This makes sense because the indices satisfy the DCC.

In doing transfinite induction, it is important to distinguish two types of ordinals. β is a *successor* ordinal if $\{\alpha : \alpha < \beta\}$ has a largest element. Otherwise, β is called a *limit* ordinal. For example, every finite ordinal is a successor ordinal, and ω is a limit ordinal.

2. Cardinals

We say that two sets X and Y have the same *cardinality*, written $|X| = |Y|$, if there exists a one-to-one onto map $f : X \to Y$. It is easy to see that "having the same cardinality" is an equivalence relation on the class of all sets, and the equivalence classes of this relation are called *cardinal numbers*. We will use lower case german letters such as $\mathfrak{m}$, $\mathfrak{n}$ and $\mathfrak{p}$ to denote unidentified cardinal numbers.

We order cardinal numbers as follows. Let X and Y be sets with $|X| = \mathfrak{m}$ and $|Y| = \mathfrak{n}$. Put $\mathfrak{m} \leq \mathfrak{n}$ if there exists a one-to-one map $f : X \rightarrowtail Y$ (equivalently, if there exists an onto map $g : Y \twoheadrightarrow X$). The Cantor-Bernstein theorem says that this relation is anti-symmetric: if $\mathfrak{m} \leq \mathfrak{n} \leq \mathfrak{m}$, then $\mathfrak{m} = \mathfrak{n}$, which is the hard part of showing that it is a partial order.

Theorem. *Let $\mathfrak{m}$ be any cardinal. Then there is a least ordinal α with $|\alpha| = \mathfrak{m}$.*

Theorem. *Any set of cardinal numbers is well ordered.*[1]

Now let $|X| = \mathfrak{m}$ and $|Y| = \mathfrak{n}$ with X and Y disjoint. We introduce operations on cardinals (which agree with the standard operations in the finite case) as follows.

$$\begin{aligned}
\mathfrak{m} + \mathfrak{n} &= |X \cup Y| \\
\mathfrak{m} \cdot \mathfrak{n} &= |X \times Y| \\
\mathfrak{m}^{\mathfrak{n}} &= |\{f : Y \to X\}|
\end{aligned}$$

It should be clear how to extend $+$ and $\cdot$ to arbitrary sums and products.

The basic arithmetic of infinite cardinals is fairly simple.

Theorem. *Let $\mathfrak{m}$ and $\mathfrak{n}$ be infinite cardinals. Then*

(1) $\mathfrak{m} + \mathfrak{n} = \mathfrak{m} \cdot \mathfrak{n} = \max\{\mathfrak{m}, \mathfrak{n}\}$,
(2) $2^{\mathfrak{m}} > \mathfrak{m}$.

The finer points of the arithmetic can get complicated, but that will not bother us here. The following facts are used frequently.

Theorem. *Let X be an infinite set, $\mathcal{P}(X)$ the lattice of subsets of X, and $\mathcal{P}_f(X)$ the lattice of finite subsets of X. Then $|\mathcal{P}(X)| = 2^{|X|}$ and $|\mathcal{P}_f(X)| = |X|$.*

A fine little book [2] by Irving Kaplansky, *Set Theory and Metric Spaces*, is easy reading and contains the proofs of these theorems and more. The book *Introduction to Modern Set Theory* by Judith Roitman [4] is recommended for a slightly more advanced introduction.

[1] Again, there are too many cardinals to talk about the "set of all cardinals."

3. Universal Algebra

Once you have seen enough different kinds of algebras: vector spaces, groups, rings, semigroups, lattices, even semilattices, you should be driven to abstraction. The proper abstraction in this case is the general notion of an "algebra." Thus *universal algebra* is the study of the properties that different types of algebras have in common. Historically, lattice theory and universal algebra developed together, more like Siamese twins than cousins. In these notes we do not assume you know much universal algebra, but where appropriate we do use its terminology.

An *operation* on a set A is just a function $f : A^n \to A$ for some $n \in \omega$. An *algebra* is a system $\mathcal{A} = \langle A; \mathcal{F} \rangle$ where A is a nonempty set and $\mathcal{F}$ is a set of operations on A. Note that we allow infinitely many operations, but each has only finitely many arguments. For example, lattices have two binary operations, $\wedge$ and $\vee$. We use different fonts to distinguish between an algebra and the set of its elements, e.g., $\mathcal{A}$ and A.

Many algebras have distinguished elements, or constants. For example, groups have a unit element e, rings have both 0 and 1. Technically, these constants are nullary operations (with no arguments), and are included in the set $\mathcal{F}$ of operations. However, in these notes we commonly revert to a more old-fashioned notation and write them separately, as $\mathcal{A} = \langle A; \mathcal{F}, \mathcal{C} \rangle$, where $\mathcal{F}$ is the set of operations with at least one argument and $\mathcal{C}$ is the set of constants. There is no requirement that constants with different names, e.g., 0 and 1, be distinct.

A *subalgebra* of $\mathcal{A}$ is a subset S of A that is closed under the operations, i.e., if $s_1, \ldots, s_n \in S$ and $f \in \mathcal{F}$, then $f(s_1, \ldots, s_n) \in S$. This means in particular that all the constants of $\mathcal{A}$ are contained in S. If $\mathcal{A}$ has no constants, then we allow the empty set as a subalgebra (even though it is not properly an algebra). Thus the empty set is a sublattice of a lattice, but not a subgroup of a group. A nonempty subalgebra S of $\mathcal{A}$ can of course be regarded as an algebra $\mathcal{S}$ of the same type as $\mathcal{A}$.

If $\mathcal{A}$ and $\mathcal{B}$ are algebras with the same operation symbols (including constants), then a *homomorphism* from $\mathcal{A}$ to $\mathcal{B}$ is a mapping $h : A \to B$ that preserves the operations, i.e., $h(f(a_1, \ldots, a_n)) = f(h(a_1), \ldots, h(a_n))$ for all $a_1, \ldots, a_n \in A$ and $f \in \mathcal{F}$. This includes that $h(c) = c$ for all $c \in \mathcal{C}$.

A homomorphism that is one-to-one is called an *embedding*, and sometimes written $h : \mathcal{A} \rightarrowtail \mathcal{B}$ or $h : \mathcal{A} \leq \mathcal{B}$. A homomorphism that is both one-to-one and onto is called an *isomorphism*, denoted $h : \mathcal{A} \cong \mathcal{B}$.

These notions directly generalize notions that should be perfectly familiar to you for say groups or rings. Note that we have given only terminology, but no results. The basic theorems of universal algebra are included in the text, either in full generality, or for lattices in a form that is easy to generalize. For deeper results in universal algebra, there are several nice textbooks available, including *A Course in Universal Algebra* by S. Burris and H. P. Sankappanavar [1], and *Algebras, Lattices, Varieties* by R. McKenzie, G. McNulty and W. Taylor [3]. The former text [1] is out of print, but available for free downloading at Ralph Freese's website:

$$/www.math.hawaii.edu/\%7Eralph/Classes/619/.$$

Also on that website are other references, and universal algebra class notes by both Jarda Ježek and Kirby Baker.

References

1. S. Burris and H. P. Sankappanavar, *A Course in Universal Algebra*, Springer-Verlag, New York, 1980.
2. I. Kaplansky, *Set Theory and Metric Spaces*, Allyn and Bacon, Boston, 1972.
3. R. McKenzie, G. McNulty and W. Taylor, *Algebras, Lattices, Varieties*, vol. I, Wadsworth and Brooks-Cole, Belmont, CA, 1987.
4. J. Roitman, *Introduction to Modern Set Theory*, Wiley, New York, 1990.

Appendix 2: The Axiom of Choice

In this appendix we want to prove Theorem 1.5.

Theorem 1.5. *The following set theoretic axioms are equivalent.*

(1) (Axiom of Choice) *If X is a nonempty set, then there is a map $\phi : \mathfrak{P}(X) \to X$ such that $\phi(A) \in A$ for every nonempty $A \subseteq X$.*
(2) (Zermelo well-ordering principle) *Every nonempty set admits a well-ordering (a total order satisfying the DCC).*
(3) (Hausdorff maximality principle) *Every chain in an ordered set $\mathcal{P}$ can be embedded in a maximal chain.*
(4) (Zorn's Lemma) *If every chain in an ordered set $\mathcal{P}$ has an upper bound in $\mathcal{P}$, then $\mathcal{P}$ contains a maximal element.*
(5) *If every chain in an ordered set $\mathcal{P}$ has a least upper bound in $\mathcal{P}$, then $\mathcal{P}$ contains a maximal element.*

Let us start by proving the equivalence of (1), (2) and (4).

(4) $\implies$ (2): Given a nonempty set X, let $\mathcal{Q}$ be the collection of all pairs (Y, R) such that $Y \subseteq X$ and R is a well ordering of Y, i.e., $R \subseteq Y \times Y$ is a total order satisfying the DCC. Order $\mathcal{Q}$ by $(Y, R) \sqsubseteq (Z, S)$ if Y is an initial segment of Z and R is the restriction of S to Y. In order to apply Zorn's Lemma, check that if $\{(Y_\alpha, R_\alpha) : \alpha \in A\}$ is a chain in $\mathcal{Q}$, then $(\overline{Y}, \overline{R}) = (\bigcup Y_\alpha, \bigcup R_\alpha) \in \mathcal{Q}$ and $(Y_\alpha, R_\alpha) \sqsubseteq (\overline{Y}, \overline{R})$ for every $\alpha \in A$, and so $(\overline{Y}, \overline{R})$ is an upper bound for $\{(Y_\alpha, R_\alpha) : \alpha \in A\}$. Thus $\mathcal{Q}$ contains a maximal element (U, T). Moreover, we must have $U = X$. For otherwise we could choose an element $z \in X - U$, and then the pair (U', T') with $U' = U \cup \{z\}$ and $T' = T \cup \{(u, z) : u \in U\}$ would satisfy $(U, T) \sqsubset (U', T')$, a contradiction. Therefore T is a well ordering of $U = X$, as desired.

(2) $\implies$ (1): Given a well ordering $\leq$ of X, we can define a choice function ϕ on the nonempty subsets of X by letting $\phi(A)$ be the least element of A under the ordering $\leq$.

(1) $\implies$ (4): For a subset S of an ordered set $\mathcal{P}$, let S^u denote the set of all upper bounds of S, i.e., $S^u = \{x \in P : x \geq s \text{ for all } s \in S\}$.

Let $\mathcal{P}$ be an ordered set in which every chain has an upper bound. By the Axiom of Choice there is a function ϕ on the subsets of P such that $\phi(S) \in S$ for every nonempty $S \subseteq P$. We use the choice function ϕ to construct a function that assigns a strict upper bound to every subset of P that has one as follows: if $S \subseteq P$ and $S^u - S = \{x \in P : x > s \text{ for all } s \in S\}$ is nonempty, define $\gamma(S) = \phi(S^u - S)$.

Fix an element $x_0 \in P$. Let $\mathfrak{B}$ be the collection of all subsets $B \subseteq P$ satisfying the following properties.

(1) B is a chain.
(2) $x_0 \in B$.
(3) $x_0 \leq y$ for all $y \in B$.
(4) If A is a nonempty order ideal of B and $z \in B \cap (A^u - A)$, then $\gamma(A) \in B \cap z/0$.

The last condition says that if A is a proper ideal of B, then $\gamma(A)$ is in B, and moreover it is the least element of B strictly above every member of A.

Note that $\mathfrak{B}$ is nonempty, since $\{x_0\} \in \mathfrak{B}$.

Next, we claim that *if B and C are both in $\mathfrak{B}$, then either B is an order ideal of C or C is an order ideal of B.* Suppose not, and let $A = \{t \in B \cap C : t/0 \cap B = t/0 \cap C\}$. Thus A is the largest common ideal of B and C; it contains x_0, and by assumption is a proper ideal of both B and C. Let $b \in B - A$ and $c \in C - A$. Now B is a chain and A is an ideal of B, so $b \notin A$ implies $b > a$ for all $a \in A$, whence $b \in B \cap (A^u - A)$. Likewise $c \in C \cap (A^u - A)$. Hence by (4), $\gamma(A) \in B \cap C$. Moreover, since b was arbitrary in $B - A$, again by (4) we have $\gamma(A) \leq b$ for all $b \in B - A$, and similarly $\gamma(A) \leq c$ for all $c \in C - A$. Therefore

$$\gamma(A)/0 \cap B = A \cup \{\gamma(A)\} = \gamma(A)/0 \cap C$$

whence $\gamma(A) \in A$, contrary to the definition of γ.

It follows, that if B and C are in $\mathfrak{B}$, $b \in B$ and $c \in C$, and $b \leq c$, then $b \in C$.

Also, you can easily check that if $B \in \mathfrak{B}$ and $B^u - B$ is nonempty, then $B \cup \{\gamma(B)\} \in \mathfrak{B}$.

Now let $U = \bigcup_{B \in \mathfrak{B}} B$. We claim that $U \in \mathfrak{B}$. It is a chain because for any two elements $b, c \in U$ there exist $B, C \in \mathfrak{B}$ with $b \in B$ and $c \in C$; one of B and C is an ideal of the other, so both are contained in the larger set and hence comparable. Conditions (2) and (3) are immediate. If a nonempty ideal A of U has a strict upper bound $z \in U$, then $z \in C$ for some $C \in \mathfrak{B}$. By the observation above, A is an ideal of C, and hence the conclusion of (4) holds.

Now U is a chain in $\mathcal{P}$, and hence by hypothesis U has an upper bound x. On the other hand, $U^u - U$ must be empty, for otherwise $U \cup \{\gamma(U)\} \in \mathfrak{B}$, whence $\gamma(U) \in U$, a contradiction. Therefore $x \in U$ and x is maximal in $\mathcal{P}$. In particular, $\mathcal{P}$ has a maximal element, as desired.

Now we prove the equivalence of (3), (4) and (5).

(4) $\implies$ (5): This is obvious, since the hypothesis of (5) is stronger.

(5) $\implies$ (3): Given an ordered set $\mathcal{P}$, let $\mathcal{Q}$ be the set of all chains in $\mathcal{P}$, ordered by set containment. If $\{C_\alpha : \alpha \in A\}$ is a chain in $\mathcal{Q}$, then $\bigcup C_\alpha$ is a chain in $\mathcal{P}$ that is the least upper bound of $\{C_\alpha : \alpha \in A\}$. Thus $\mathcal{Q}$ satisfies the hypothesis of (5), and hence it contains a maximal element C, which is a maximal chain in $\mathcal{P}$.

(3) $\implies$ (4): Let $\mathcal{P}$ be an ordered set such that every chain in $\mathcal{P}$ has an upper bound in P. By (3), there is a maximal chain C in $\mathcal{P}$. If b is an upper bound for C, then in fact $b \in C$ (by maximality), and b is a maximal element of $\mathcal{P}$.

There are many variations of the proof of Theorem 1.5, but it can always be arranged so that there is only one hard step, and the rest easy. The above version seems fairly natural.

Appendix 3: Formal Concept Analysis

Exercise 13 of Chapter 2 is to show that a binary relation $R \subseteq A \times B$ induces a pair of closure operators, described as follows. For $X \subseteq A$, let

$$\sigma(X) = \{b \in B : x \; R \; b \text{ for all } x \in X\}.$$

Similarly, for $Y \subseteq B$, let

$$\pi(Y) = \{a \in A : a \; R \; y \text{ for all } y \in Y\}.$$

Then the composition $\pi\sigma : \mathfrak{P}(A) \to \mathfrak{P}(A)$ is a closure operator on A, given by

$$\pi\sigma(X) = \{a \in A : a \; R \; b \text{ whenever } x \; R \; b \text{ for all } x \in X\}.$$

Likewise, $\sigma\pi$ is a closure operator on B, and for $Y \subseteq B$,

$$\sigma\pi(Y) = \{b \in B : a \; R \; b \text{ whenever } a \; R \; y \text{ for all } y \in Y\}.$$

In this situation, the lattice of closed sets $\mathcal{C}_{\pi\sigma} \subseteq \mathfrak{P}(A)$ is dually isomorphic to $\mathcal{C}_{\sigma\pi} \subseteq \mathfrak{P}(B)$, and we say that R establishes a *Galois connection* between the $\pi\sigma$-closed subsets of A and the $\sigma\pi$-closed subsets of B.

Of course, $\mathcal{C}_{\pi\sigma}$ is a complete lattice. Moreover, every complete lattice can be represented *via* a Galois connection.

Theorem. *Let $\mathcal{L}$ be a complete lattice, A a join dense subset of L and B a meet dense subset of L. Define $R \subseteq A \times B$ by $a \; R \; b$ if and only if $a \leq b$. Then, with σ and π defined as above, $\mathcal{L} \cong \mathcal{C}_{\pi\sigma}$ (and $\mathcal{L}$ is dually isomorphic to $\mathcal{C}_{\sigma\pi}$).*

In particular, for an arbitrary complete lattice, we can always take $A = B = L$. If $\mathcal{L}$ is algebraic, a more natural choice is $A = L^c$ and $B = M^*(\mathcal{L})$ (compact elements and completely meet irreducibles). If $\mathcal{L}$ is finite, the most natural choice is $A = J(\mathcal{L})$ and $B = M(\mathcal{L})$. Again the proof of this theorem is elementary.

Formal Concept Analysis is a method developed by Rudolf Wille and his colleagues in Darmstadt (Germany), whereby the philosophical Galois connection between objects and their properties is used to provide a systematic analysis of certain very general situations. Abstractly, it goes like this. Let G be a set of "objects" (*Gegenstände*) and M a set of relevant "attributes" (*Merkmale*). The relation $I \subseteq G \times M$ consists of all those pairs $\langle g, m \rangle$ such that g has the property m. A *concept* is a pair $\langle X, Y \rangle$ with $X \subseteq G$, $Y \subseteq M$, $X = \pi(Y)$ and $Y = \sigma(X)$. Thus

$\langle X, Y \rangle$ is a concept if X is the set of all elements with the properties of Y, and Y is exactly the set of properties shared by the elements of X. It follows (as in exercise 12, Chapter 2) that $X \in \mathcal{C}_{\pi\sigma}$ and $Y \in \mathcal{C}_{\sigma\pi}$. Thus if we order concepts by $\langle X, Y \rangle \leq \langle U, V \rangle$ iff $X \subseteq U$ (which is equivalent to $Y \supseteq V$), then we obtain a lattice $\mathfrak{B}(G, M, I)$ isomorphic to $\mathcal{C}_{\pi\sigma}$.

A small example will illustrate how this works. The rows of Table A1 correspond to seven fine musicians, and the columns to eight possible attributes (chosen by a musically trained sociologist). An $\times$ in the table indicates that the musician has that attribute.[1] The corresponding concept lattice is given in Figure A2, where the musicians are abbreviated by lower case letters and their attributes by capitals.

	Instrument	Classical	Jazz	Country	Black	White	Male	Female
J. S. Bach	$\times$	$\times$				$\times$	$\times$	
Rachmaninoff	$\times$	$\times$				$\times$	$\times$	
King Oliver	$\times$		$\times$		$\times$		$\times$	
W. Marsalis	$\times$	$\times$	$\times$		$\times$		$\times$	
B. Holiday			$\times$		$\times$			$\times$
Emmylou H.				$\times$		$\times$		$\times$
Chet Atkins	$\times$		$\times$	$\times$		$\times$	$\times$	

Table A1.

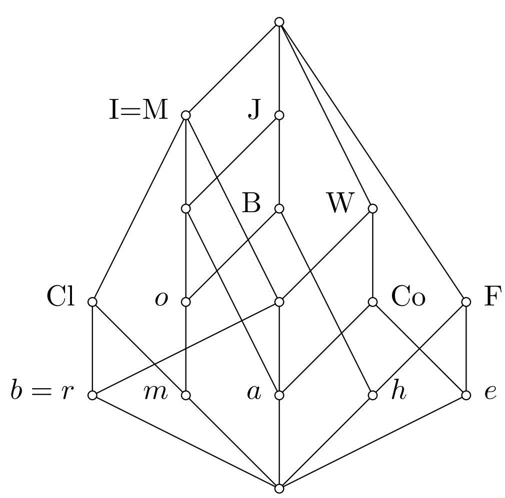


Figure A2

[1]To avoid confusion, androgynous rock stars were not included.

Formal concept analysis has been applied to hundreds of real situations outside of mathematics (e.g., law, medicine, psychology), and has proved to be a useful tool for understanding the relation between the concepts involved. Typically, these applications involve large numbers of objects and attributes, and computer programs have been developed to navigate through the concept lattice. A good brief introduction to concept analysis may be found in Wille [2] or [3], and the whole business is explained thoroughly in Ganter and Wille [1]. For online introductions, see the website of Uta Priss,

$$/www.upriss.org/fca/fca.html$$

Likewise, the representation of a finite lattice as the concept lattice induced by the order relation between join and meet irreducible elements (i.e., $\leq$ restricted to $J(\mathcal{L}) \times M(\mathcal{L})$) provides and effective and tractable encoding of its structure. As an example of the method, let us show how one can extract the ordered set $\mathcal{Q}_{\mathcal{L}}$ such that $\mathbf{Con}\,\mathcal{L} \cong \mathcal{O}(\mathcal{Q}(\mathcal{L}))$ from the table.

Given a finite lattice $\mathcal{L}$, for $g \in J(\mathcal{L})$ and $m \in M(\mathcal{L})$, define

$$\begin{aligned} g \nearrow m & \quad \text{if } g \nleq m \text{ but } g \leq m^*, \text{ i.e., } g \leq n \text{ for all } n > m, \\ m \searrow g & \quad \text{if } m \ngeq g \text{ but } m \geq g_*, \text{ i.e., } m \geq h \text{ for all } h < g, \\ g \updownarrow m & \quad \text{if } g \nearrow m \text{ and } m \searrow g. \end{aligned}$$

Note that these relations can easily be added to the table of $J(\mathcal{L}) \times M(\mathcal{L})$.

These relations connect with the relation $\underline{D}$ of Chapter 10 as follows.

Lemma. *Let $\mathcal{L}$ be a finite lattice and $g, h \in J(\mathcal{L})$. Then $g \,\underline{D}\, h$ if and only if there exists $m \in M(\mathcal{L})$ such that $g \nearrow m \searrow h$.*

Proof. If $g \,\underline{D}\, h$, then there exists $x \in L$ such that $g \leq h \vee x$ but $g \nleq h_* \vee x$. Let m be maximal such that $m \geq h_* \vee x$ but $m \ngeq g$. Then $m \in M(\mathcal{L})$, $g \leq m^*$, $m \geq h_*$ but $m \ngeq h$. Thus $g \nearrow m \searrow h$.

Conversely, suppose $g \nearrow m \searrow h$. Then $g \leq m^* \leq h \vee m$ while $g \nleq m = h_* \vee m$. Therefore $g \,\underline{D}\, h$. $\square$

As an example, the table for the lattice in Figure A2 is given in Table A3. This is a reduction of the original Table A1: $J(\mathcal{L})$ is a subset of the original set of objects, and likewise $M(\mathcal{L})$ is contained in the original attributes. Arrows indicating the relations $\nearrow$, $\searrow$ and $\updownarrow$ have been added. The Lemma allows us to calculate $\underline{D}$ quickly, and we find that $|\mathcal{Q}_{\mathcal{L}}| = 1$, whence $\mathcal{L}$ is simple.

	I=M	Cl	J	Co	B	W	F
b=r	$\times$	$\times$	$\updownarrow$	$\updownarrow$	$\searrow$	$\times$	$\updownarrow$
o	$\times$	$\updownarrow$	$\times$		$\times$	$\nearrow$	$\nearrow$
m	$\times$	$\times$	$\times$	$\searrow$	$\times$	$\updownarrow$	$\updownarrow$
h	$\updownarrow$	$\searrow$	$\times$	$\searrow$	$\times$	$\updownarrow$	$\times$
e	$\updownarrow$	$\searrow$	$\updownarrow$	$\times$	$\updownarrow$	$\times$	$\times$
a	$\times$	$\updownarrow$	$\times$	$\times$	$\updownarrow$	$\times$	$\updownarrow$

Table A3.

References

1. B. Ganter and R. Wille, *Formale Begriffsanalyse: Mathematische Grundlagen*, Springer-Verlag, Berlin-Heidelberg, 1996. Translated by C. Franzke as Formal Concept Analysis: Mathematical Foundations, Springer, 1998.
2. R. Wille, *Restructuring lattice theory: an approach based on hierarchies of concepts*, Ordered Sets, I. Rival, ed., Reidel, Dordrecht-Boston, 1982, pp. 445–470.
3. R. Wille, *Concept lattices and conceptual knowledge systems*, Computers and Mathematics with Applications **23** (1992), 493–515.