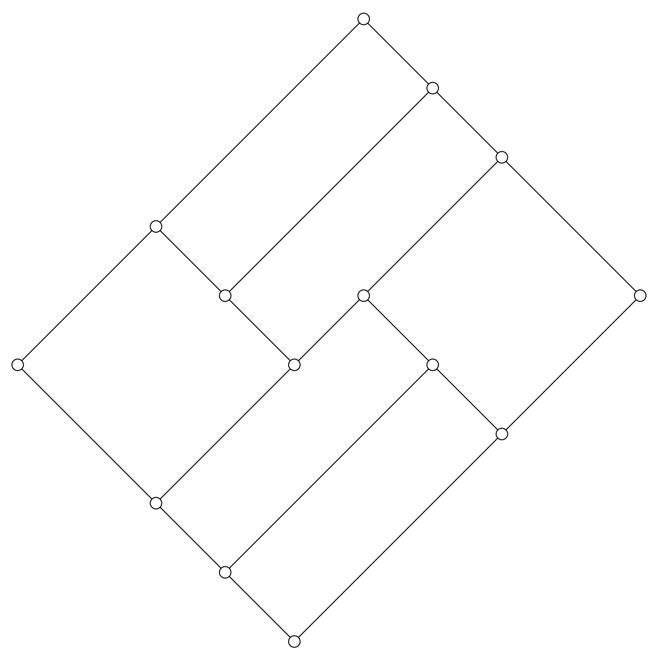
Notes on Lattice Theory



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 to show that this is what we have.

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

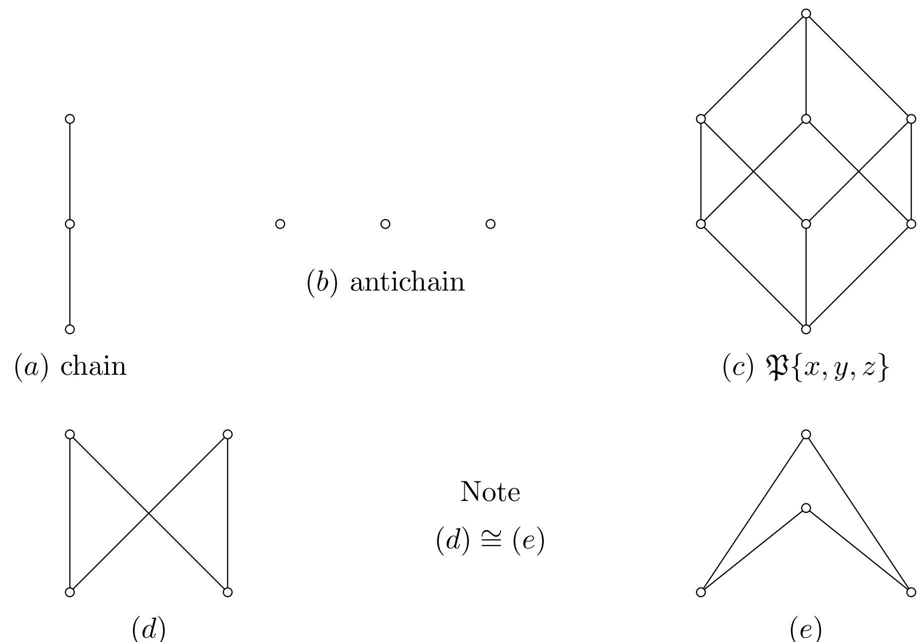


FIGURE 1.1

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).

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.

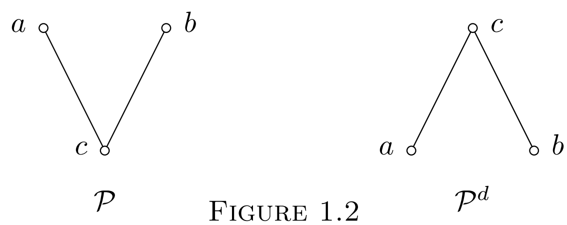


FIGURE 1.2

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*.

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 $|A| \le |I|$ whenever A is an antichain in $\mathcal{P}$ and $P = \bigcup_{i \in I} C_i$ is a chain covering. Therefore

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

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 $w(\mathcal{P}) = c(\mathcal{P})$.

[1]Note that the width function $w(\mathcal{P})$ does not distinguish, for example, between ordered sets which contain arbitrarily large finite antichains and those which 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 $w(\mathcal{P})$.

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 [11].

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

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

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. □

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 [9].) 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 [5]), and then 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 $(\neg\alpha)$, $(\alpha \wedge \beta)$ and $(\alpha \vee \beta)$.
(3) Only symbols generated by the first two rules are wffs.

The set of all wffs on S is denoted by $\overline{S}$.[2] Of course, we think of $\neg$, $\wedge$ and $\vee$ as corresponding to "not", "and" and "or", respectively.

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) $\overline{\nu}(\varphi \wedge \psi) = T$ if and only if $\overline{\nu}(\varphi) = T$ and $\overline{\nu}(\psi) = T$,
(3) $\overline{\nu}(\varphi \vee \psi) = T$ 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 $\overline{\nu}(\phi) = T$ for all $\phi \in \Sigma$. 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.

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

[2] Technically, $\overline{S}$ is just the absolutely free algebra generated by S with the operation symbols given in (2).

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 $\neg$, $\wedge$ and $\vee$, 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 $\varphi = \alpha \wedge \beta$ with α, $\beta \in G$. Note that $\alpha \wedge \beta \in \Delta$ iff $\alpha \in \Delta$ and $\beta \in \Delta$. For if $\alpha \wedge \beta \in \Delta$, since $\{\alpha \wedge \beta, \neg\alpha\}$ 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 $\{\alpha, \beta, \neg(\alpha \wedge \beta)\}$ is not satisfiable, we have $\alpha \wedge \beta \in \Delta$. Thus

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

Hence $\varphi = (\alpha \wedge \beta) \in G$.

(3) The case $\varphi = \alpha \vee \beta$ 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) $$c_{x1} \vee \cdots \vee c_{xk}$$

for $x \in P$, and

(b) $$\neg(c_{xi} \wedge c_{yi})$$

for all incomparable pairs $x, y \in P$ and $1 \le i \le k$. 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 [7]. 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 [3], while a nice alternate proof appears in F. Galvin [4].

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 [10].

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 an immediate consequence of the next lemma.

Lemma 1.8. *Given an ordered set $(P, \le)$ and $a \not\le b$, there exists an extension $\le^*$ of $\le$ such that $(P, \le^*)$ is a chain and $b \le^* a$.*

Proof. Let $a \not\le b$ in $\mathcal{P}$. Define

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

It is straightforward to check that this is a partial order with $b \le' a$.

If P is finite, repeated application of this construction yields a total order $\le^*$ extending $\le'$, so that $b \le^* a$. 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 $\le^*$ extending $\le'$. □

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

[3] See Appendix 1.

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 [6] or [8]).

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, supporting its own journal, **Order**.

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 $f : \mathcal{P} \to \mathcal{Q}$ which 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.

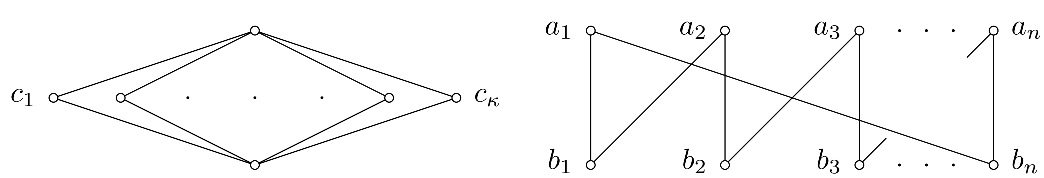


Figure 1.3

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.

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 $S_1, \dots, S_n$ are subsets of X, then there is a system of distinct representatives (SDR) $a_1, \dots, a_n$ with $a_j \in S_j$ if and only if for all $1 \le k \le n$ and distinct indices $i_1, \dots, i_k$ we have $|\bigcup_{1 \le j \le k} S_{i_j}| \ge k$.

(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 which contains no cycle of the form $x_0 \; R \; x_1 \; R \; \dots R \; x_n \; R \; x_0$ with $x_i \ne x_{i+1}$. 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 $x \le y$. Verify that $\ll$ is a quasiorder.

13. Let ω_1 denote the first uncountable ordinal, and let $\mathcal{P}$ be the direct product $\omega_1 \times \omega_1$. Prove that every antichain of $\mathcal{P}$ is finite, but $c(\mathcal{P}) = \aleph_1$.

References

1. K. Bogart, R. Freese and J. Kung, Eds., *The Dilworth Theorems*, Birkhäuser, Boston, 1990.
2. R. P. Dilworth, *A decomposition theorem for partially ordered sets*, Annals of Math. **51** (1950), 161–166.
3. R. Freese, J. Ježek and J. B. Nation, *Free Lattices*, Mathematical Surveys and Monographs, vol. 42, Amer. Math. Soc., Providence, R. I., 1995.
4. F. Galvin, *A proof of Dilworth's chain decomposition theorem*, Amer. Math. Monthly **101** (1994), 352–353.
5. K. Gödel, *Die Vollständigkeit der Axiome des logischen Funktionenkalküls*, Monatsh. Math. Phys. **37** (1930), 349–360.
6. J. B. Nation, D. Pickering and J. Schmerl, *Dimension may exceed width*, Order **5** (1988), 21–22.
7. M. A. Perles, *On Dilworth's theorem in the infinite case*, Israel J. Math. **1** (1963), 108–109.
8. M. Pouzet, *Généralisation d'une construction de Ben-Dushnik et E. W. Miller*, Comptes Rendus Acad. Sci. Paris **269** (1969), 877–879.
9. 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.
10. E. Szpilrajn, *Sur l'extension de l'ordre partiel*, Fund. Math. **16** (1930), 386–389.
11. 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 intersection. In this chapter we will meet several types of structures which 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. Thus 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 $x \le y$ if and only if $x * y = x$. Then $(S, \le)$ 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.*

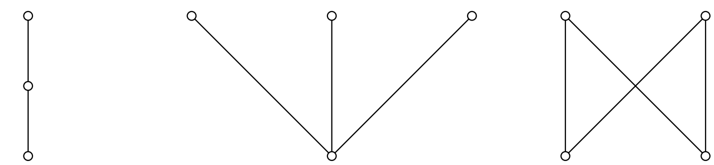
Proof. Let $(S, *)$ be a semilattice, and define $\le$ as above. First we check that $\le$ is a partial order.

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

Since $(x * y) * x = x * (x * y) = (x * x) * y = x * y)$ we have $x * y \le x$; similarly $x * y \le y$. Thus $x * y$ is a lower bound for $\{x, y\}$. To see that it is the greatest lower bound, suppose $z \le x$ and $z \le y$. Then $z * (x * y) = (z * x) * y = z * y = z$, so $z \le x * y$, 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, $\phi(x \wedge y) = \phi(x) \wedge \phi(y)$ 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 which some of these lattices have.

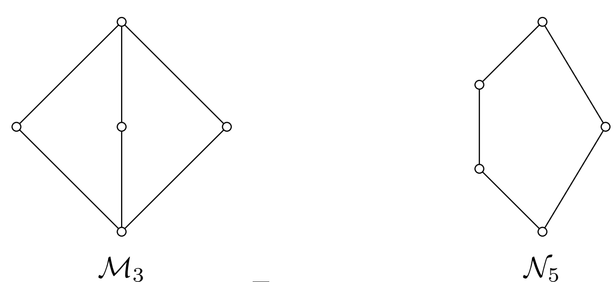


FIGURE 2.2

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 *quotient* (or *interval*) sublattices:

$$\begin{aligned} a/b &= \{x \in L : b \leq x \leq a\} \\ a/0 &= \{x \in L : x \leq a\} \\ 1/a &= \{x \in L : a \leq x\} \end{aligned}$$

The latter notations are used irrespective of whether $\mathcal{L}$ actually has a least element 0 or a greatest element 1.[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.,

$$\begin{aligned} A^u &= \{x \in P : x \geq a \text{ for all } a \in A\} \\ &= \bigcap_{a \in A} 1/a. \end{aligned}$$

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

$$\begin{aligned} A^\ell &= \{x \in P : x \leq a \text{ for all } a \in A\} \\ &= \bigcap_{a \in A} a/0. \end{aligned}$$

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., $a \leq z$ 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*

$$x \vee y = \bigwedge \{x, y\}^u = \bigwedge (1/x \cap 1/y).$$

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]There are several commonly used ways of denoting interval sublattices; the one we have adopted is as good as any, but hardly universal. The most common alternative has $a/b = [b, a]$, $a/0 = (a]$ and $1/a = [a)$. The notations $\downarrow a$ for $a/0$ and $\uparrow a$ for $1/a$ are also widely used.

if $\mathcal{P}$ 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 which 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*

$$\bigvee A = \bigwedge A^u = \bigwedge \Big(\bigcap_{a \in A} 1/a \Big).$$

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 which 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) order ideals of an ordered set,
(v) convex subsets of euclidean space $\Re^n$.

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 3). 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) $\mathcal{P}$ an ordered set and $\mathcal{O}(A)$ the order ideal generated by A,
(v) $\Re^n$ and $H(A)$ the convex hull of 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

$$\begin{aligned} x \in S &\implies x^{-1} \in S \\ \{x, y\} \subseteq S &\implies xy \in S \end{aligned}$$

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

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 which 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 which 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 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.

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 $\varphi(x) = x/0$.

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 $0 \notin J(\mathcal{L})$, as $0 = \bigvee \emptyset$.[5]

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, 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. $\square$

If $\mathcal{L}$ also satisfies the ACC, then join irreducible elements can be identified as those which cover a unique element, *viz.*,

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

The representation of lattices satisfying both chain conditions (in particular, finite lattices) as a closure system is quite straightforward.

[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.

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

$$f(x) = x/0 \cap J(\mathcal{L})$$
$$g(S) = \bigvee S.$$

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. □

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.

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 $x \in L$,

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

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

$$O(A) = \bigcup_{a \in A} a/0,$$

and the embedding ϕ is given by $\phi(p) = p/0$. 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* [2]. 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 $\phi(p) = p/0$ 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 10). 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 $\phi(c) = c/0 = M(A) = \bigvee \phi(A)$.

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 $\Phi(\{p\}) = p/0$ for all $p \in P$, then $(\mathcal{C}_\Phi, \phi)$ is a join dense completion of $\mathcal{P}$, where $\phi(p) = p/0$. 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, $\Phi(\{p\}) = p/0$ 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 $C \in \mathcal{C}_\Phi$,

$$\begin{aligned} C &= \bigvee\{\Phi(\{p\}) : p \in C\} \\ &= \bigvee\{p/0 : p/0 \subseteq C\} \\ &= \bigvee\{\phi(p) : \phi(p) \leq C\}. \end{aligned}$$

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 $g(x) = \{p \in P : \phi(p) \leq x\}$. 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. $\square$

Let $\mathcal{K}(\mathcal{P})$ be the collection of all closure operators on $\mathcal{P}$ such that $\Gamma(\{p\}) = p/0$ for all $p \in P$. There is a natural order on $\mathcal{K}(\mathcal{P})$: $\Gamma \le \Delta$ if $\Gamma(A) \subseteq \Delta(A)$ for all $A \subseteq P$. Moreover, $\mathcal{K}(\mathcal{P})$ is closed under arbitrary meets, where by definition

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

The least and greatest members of $\mathcal{K}(\mathcal{P})$ are the order ideal completion and the MacNeille completion, respectively.

Theorem 2.11. *$\mathcal{K}(\mathcal{P})$ is a complete lattice with least element O and greatest element M.*

Proof. The condition $\Gamma(\{p\}) = p/0$ 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 $b/0 = \Gamma(b/0) \supseteq \Gamma(A)$. Thus

$$\Gamma(A) \subseteq \bigcap_{b\in A^u} (b/0) = (A^u)^\ell = M(A),$$

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 [3].

We conclude this section with a classic theorem due to A. Tarski and Anne Davis (Morel) [1], [4].

Theorem 2.12. *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 $A = \{x \in L : f(x) \ge x\}$. Note A is nonempty as $0 \in A$. Let $a = \bigvee A$. Since $a \ge x$ for all $x \in A$, $f(a) \ge \bigvee_{x\in A} f(x) \ge \bigvee_{x\in A} x = a$. Thus $a \in A$. But then $a \le f(a)$ implies $f(a) \le f^2(a)$, so also $f(a) \in A$, whence $f(a) \le a$. Therefore $f(a) = a$.

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

Claim 1: *Either $\mathcal{L}$ has no 1 or there exists a chain $C \subseteq L$ which 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 $C_1 \le C_2$ 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 11 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. □

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

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

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

9. (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 $\mathcal{P}$.

10. 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 $\mathcal{L}$.

11. 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 $x \leq c$.)

12. Following Morgan Ward [5], 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 $f : L \to L$ which 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 $\mathcal{L}$.

13. 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. A. C. Davis, *A characterization of complete lattices*, Pacific J. Math. **5** (1955), 311–319.
2. H. M. MacNeille, *Partially ordered sets*, Trans. Amer. Math. Soc. **42** (1937), 90–96.
3. J. B. Nation and A. Pogel, *The lattice of completions of an ordered set*, Order **14** (1996), 1–7.
4. A. Tarski, *A lattice-theoretical fixpoint theorem and its applications*, Pacific J. Math. **5** (1955), 285–309.
5. 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 which 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 3.1(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 $a = t(b_1, \dots, b_n)$ for some finite subset $\{b_1, \dots, b_n\} \subseteq B$, in which case $a \in \mathrm{Sg}(\{b_1, \dots, b_n\})$. 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 with a least element 0. A subset J of S is called an *ideal* if

(1) $0 \in J$,
(2) $x, y \in J$ implies $x \vee y \in J$,
(3) $z \leq x \in J$ implies $z \in J$.

An ideal J is a *principal* ideal if $J = x/0$ for some $x \in S$. Since ideals are defined by closure rules, the intersection of a set of ideals of $\mathcal{S}$ is again one.[1] The closure operator I on S such that $I(B)$ is the ideal of $\mathcal{S}$ generated by B is given by

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

Hence I is algebraic. The ideal lattice of a join semilattice is denoted by $\mathcal{I}(\mathcal{S})$.

(5) An *ideal* of a lattice is defined in the same way, 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 partially 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 $M(\widehat{Y}) = \widehat{X} \supset \widehat{Y} = \bigcup\{M(F) : F \text{ is a finite subset of } \widehat{Y}\}$.

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., $x = \bigvee(x/0 \cap L^c)$ 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.

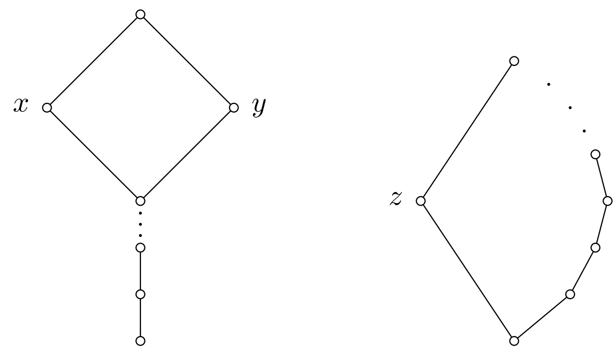
For an example of a complete lattice which is not algebraic, let $\mathcal{K}$ denote the interval $[0, 1]$ in the real numbers with the usual order. Then $\mathcal{K}^c = \{0\}$, so $\mathcal{K}$ is not algebraic. The non-algebraic lattice in Figure 3.1(b) is another good example to keep in mind. (The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

Theorem 3.1. (*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

[1] If $\mathcal{S}$ has no least element, then it is customary to allow the empty set as an ideal; however, this convention is not universal.



(a) (b)

FIGURE 3.1

$F \subseteq S \implies z \in S$, with F a finite subset of X and $z \in \Gamma(F)$, determines closure for Γ.[2] 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 $\Gamma(\bigcup A_i) \subseteq \Gamma(\bigvee \Gamma(A_i)) = \bigvee \Gamma(A_i)$.

Now assume that Γ is algebraic. Then, for all $B \subseteq X$,

$$\begin{aligned}\Gamma(B) &= \bigcup \{\Gamma(F) : F \text{ is a finite subset of } B\} \\ &\subseteq \bigvee \{\Gamma(F) : F \text{ is a finite subset of } B\} \\ &= \Gamma(B),\end{aligned}$$

from which equality follows. Thus $\mathcal{C}_\Gamma$ will be an algebraic lattice if we can show that the closures of finite sets are compact.

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

[2] In general there are also valid infinitary closure rules for Γ, but for algebraic closure operators these are redundant.

of C, say $F_1, \dots, F_n$, such that $C = \Gamma(F_1) \vee \ldots \vee \Gamma(F_n) = \Gamma(F_1 \cup \dots \cup F_n)$. Thus C is the closure of a finite set. $\square$

Thus in a subalgebra lattice **Sub** $\mathcal{A}$, the compact elements are the finitely generated subalgebras. In a congruence lattice **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 following theorem includes a representation of any algebraic lattice as the lattice of closed sets of an algebraic closure operator.

Theorem 3.2. *If $\mathcal{S}$ 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 $x/0$ with $x \in S$. 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 $f(x) = x/0 \cap L^c$, 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 $gf(x) = \bigvee(x/0 \cap L^c) = x$ by the definition of algebraic. Hence they are both isomorphisms, and $\mathcal{L} \cong \mathcal{I}(\mathcal{L}^c)$. $\square$

Let us digress for a moment into universal algebra. A classic result of Birkhoff and Frink gives a concrete representation of algebraic closure operators [2].

Theorem 3.3. *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. Appendix 3 reviews the basic definitions of universal algebra.

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

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

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 $\Gamma(F) \subseteq B$ for every finite $F \subseteq B$. Using this, it is very easy to check that the subalgebras of $\mathcal{A}$ are precisely the closed sets of $\mathcal{C}_\Gamma$. $\square$

However, the algebra constructed in the proof of Theorem 3.3 will have $|X|$ operations when X is infinite. 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.[3]

Theorem 3.4. *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. It is easy to count that $|W(X)| = \max(\gamma, \kappa, \lambda, \aleph_0)$, and $|\mathcal{A}| \leq |W(X)|$.

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 $x \in L^c$, $|x/0 \cap L^c| \leq \aleph_0$. 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 $2 \leq |c/0 \cap L^c| = n + 1 < \infty$, arrange $c/0 \cap L^c - \{0\}$ into a cyclically repeating sequence: $c_i = c_j$ iff $i \equiv j \bmod n$. If $c/0 \cap L^c$ is infinite (and hence countable), arrange $c/0 \cap L^c - \{0\}$ into a non-repeating sequence $\langle c_i \rangle$. In both cases start the sequence with $c_0 = c$.

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

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

[3] This result is unpublished but well known.

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 [6], and Bill Lampe showed that uncountably many operations may be required [5].

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 3.5. *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 $c \nleq b$. Let $\mathcal{P} = \{x \in a/b : c \nleq x\}$. 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 $\mathcal{L}$ is complete and, for every element $a \in L$ and every chain C in $\mathcal{L}$, $a \wedge \bigvee C = \bigvee_{c \in C} a \wedge c$.

Theorem 3.6. *Every algebraic lattice is upper continuous.*

Proof. Let $\mathcal{L}$ be algebraic and C a chain in $\mathcal{L}$. Of course $\bigvee_{c \in C}(a \wedge c) \leq a \wedge \bigvee C$. Let $r = a \wedge \bigvee C$. For each $d \in r/0 \cap L^c$, we have $d \leq a$ and $d \leq \bigvee C$. The compactness of d implies $d \leq c_d$ for some $c_d \in C$, and hence $d \leq a \wedge c_d$. But then $r = \bigvee(r/0 \cap L^c) \leq \bigvee_{c \in C} a \wedge c$, as desired. $\square$

Two alternative forms of join continuity are often useful. An ordered set $\mathcal{P}$ is said to be *up-directed* if for every $x, y \in P$ there exists $z \in P$ with $x \leq z$ and $y \leq z$. So, for example, any join semilattice is up-directed.

Theorem 3.7. *For a complete lattice $\mathcal{L}$, the following are equivalent.*

(1) *$\mathcal{L}$ is upper continuous.*
(2) *For every $a \in L$ and up-directed set $D \subseteq L$, $a \wedge \bigvee D = \bigvee_{d \in D} a \wedge d$.*
(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 (2) implies (1); we will show that (1) 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

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

as desired. □

An element $a \in L$ is called an *atom* if $a \succ 0$, and a *coatom* if $1 \succ a$. Theorem 3.7 shows that every atom in an upper continuous lattice is compact. More generally, if $a/0$ 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 $x/0 \cap L^c$ (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 which 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 3.8. *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 [1].

Theorem 3.9. *If $\mathcal{L}$ is an algebraic lattice, then $M^*(\mathcal{L})$ is meet dense in $\mathcal{L}$. Thus for every $x \in L$, $x = \bigwedge(1/x \cap M^*(\mathcal{L}))$.*

Proof. Let $m = \bigwedge(1/x \cap M^*(\mathcal{L}))$, and suppose $x < m$. Then there exists a $c \in L^c$ with $c \leq m$ and $c \nleq x$. Since c is compact, we can use Zorn's Lemma to find an element q which is maximal with respect to $q \geq x$, $q \ngeq c$. 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 $q \in 1/x \cap M^*(\mathcal{L})$ implies $q \geq m \geq c$, a contradiction. Hence $x = m$. $\square$

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 [3].

Theorem 3.10. *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 3.11. *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 3.11 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 [4] contains most of the principal results.

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 $\Re$ which are algebraic.
3. Show that the natural map from a lattice to its ideal lattice, $\varphi : \mathcal{L} \to \mathcal{I}(\mathcal{L})$ by $\varphi(x) = x/0$, 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 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 $\mathbf{Sub}\,\mathcal{A}$ for a finite algebra $\mathcal{A}$.

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

8. A closure rule is *unary* if it is of the form $x \in C \implies y \in C$. Prove that if Σ is a collection of unary closure rules, then 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 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.

References

1. G. Birkhoff, *Subdirect unions in universal algebra*, Bull. Amer. Math. Soc. **50** (1944), 764–768.
2. G. Birkhoff and O. Frink, *Representations of sets by lattices*, Trans. Amer. Math. Soc. **64** (1948), 299–316.
3. P. Crawley, *Decomposition theory for nonsemimodular lattices*, Trans. Amer. Math. Soc. **99** (1961), 246–254.
4. P. Crawley and R. P. Dilworth, *Algebraic Theory of Lattices*, Prentice-Hall, Englewood Cliffs, N. J., 1973.
5. R. Freese, W. A. Lampe and W. Taylor, *Congruence lattices of algebras of fixed similarity type,* I, Pacific J. Math. **82** (1979), 59–68.
6. G. Grätzer and E. T. Schmidt, *Characterizations of congruence lattices of abstract algebras*, Acta Sci. Math. (Szeged) **24** (1963), 34–59.

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 which 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 $\mathbf{Eq}\, X$, with the order given by $R \leq S$ iff $(x, y) \in R \implies (x, y) \in S$ iff $R \subseteq S$ in $\mathfrak{P}(X^2)$. 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

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

The lattice $\mathbf{Eq}\,X$ has many nice properties: it is algebraic, strongly atomic, semimodular, relatively complemented and simple.[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 which represent elements of the given lattice.

To be precise, a *representation* 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 [7] proved in 1946 that every lattice has a representation. In 1953 Bjarni Jónsson [4] found a simpler proof which 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 $\alpha \leq \beta$, 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 $y \vee z \leq x$. The crucial step is where we fix up the joins one at a time.

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

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

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

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.

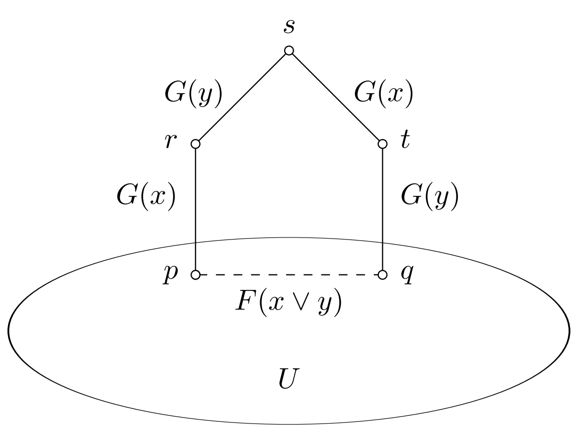


FIGURE 4.1

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 which 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 which 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* [6]. 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 which move only finitely many elements, and let $\mathbf{Sub}\,\mathcal{G}$ 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 $\mathbf{Eq}\,X$ with type 2 joins.

Lemma 4.4. *Let* $\mathcal{L}$ *be a sublattice of* $\mathbf{Eq}\,X$ *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 $\mathbf{Eq}\,X$ 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 $B \leq A$, we have $(r, s) \in A \wedge C$. It follows that $(p, q) \in B \vee (A \wedge C)$. Thus $A \wedge (B \vee C) \leq B \vee (A \wedge C)$. The reverse inclusion is trivial, so we have equality. $\square$

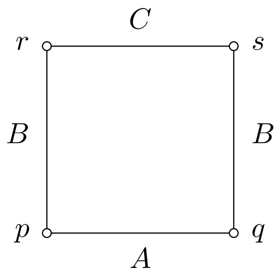


FIGURE 4.2

On the other hand, Jónsson gave a slight variation of the proof of Theorem 4.1 which shows that every modular lattice has a type 2 representation [4], [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. Note that (M) fails in the pentagon $\mathcal{N}_5$. It was invented in the 1890's by Richard Dedekind, who showed that the lattice of normal subgroups of a group is modular. 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 $x \geq y$.

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 **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. It 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 which 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

$$p\ A_0\ r\ A_1\ q$$
$$p\ B_0\ s\ B_1\ q.$$

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

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

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.) $\square$

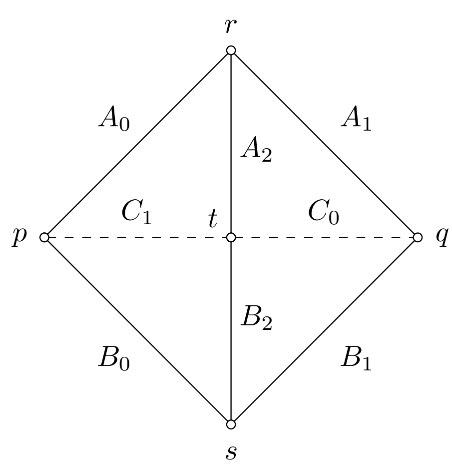


FIGURE 4.3

Mark Haiman has shown that the converse is false: there are Arguesian lattices which do not have a type 1 representation [2], [3]. In fact, his proof shows that lattices with a type 1 representation must satisfy equations which 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. Interestingly, P. P. Pálfy and Laszlo Szabó have shown that subgroup lattices of abelian groups satisfy an equation which does not hold in all normal subgroup lattices [5].

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').

References

1. P. Crawley and R. P. Dilworth, *Algebraic Theory of Lattices*, Prentice-Hall, Englewood Cliffs, New Jersey, 1973.
2. M. Haiman, *Arguesian lattices which are not linear*, Bull. Amer. Math. Soc. **16** (1987), 121–124.
3. M. Haiman, *Arguesian lattices which are not type*-1, Algebra Universalis **28** (1991), 128–137.
4. B. Jónsson, *On the representation of lattices*, Math. Scand. **1** (1953), 193–206.
5. P. P. Pálfy and Cs. Szabó, *An identity for subgroup lattices of abelian groups*, Algebra Universalis **33** (1995), 191–195.
6. 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.
7. 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 see 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

$$(\dagger) \qquad x \;\theta\; y \text{ and } r \;\theta\; s \text{ implies } x \vee r \;\theta\; y \vee s,$$

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

$$(\dagger') \qquad x \;\theta\; y \text{ implies } x \vee z \;\theta\; y \vee z.$$

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

We want to show that, conversely, any equivalence relation satisfying $(\dagger')$ 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*

$$(\ddagger) \qquad \begin{aligned} &x \;\theta\; y \textit{ implies } x \vee z \;\theta\; y \vee z, \\ &x \;\theta\; y \textit{ implies } x \wedge z \;\theta\; y \wedge z. \end{aligned}$$

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 $(\ddagger)$ 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 which 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 corresponding closure operator on L^2 is denoted by "con". So 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 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.

Theorem 5.4. Second Isomorphism Theorem. *If $\theta \in$* $\mathbf{Con}\,\mathcal{L}$*, then* $\mathbf{Con}\,(\mathcal{L}/\theta)$ *is isomorphic to the interval $1/\theta$ in* $\mathbf{Con}\,\mathcal{L}$*.*

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

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 $f : \mathbf{Con}\,\mathcal{L}/\theta \to 1/\theta$.

Conversely, let $\sigma \in 1/\theta$ 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 $g : 1/\theta \to \mathbf{Con}\,\mathcal{L}/\theta$.

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

It is interesting to interpret the Second Isomorphism Theorem 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 $\ker h \;\leq\; \ker f$.

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 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 which 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) [7]. 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 **Con** $\mathcal{L}$.

Proof. For any collection θ_i $(i \in I)$ in **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 $\mathcal{K}_i \cong \mathcal{L}/\ker\pi_i$. □

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 $\mathcal{N}_5$.

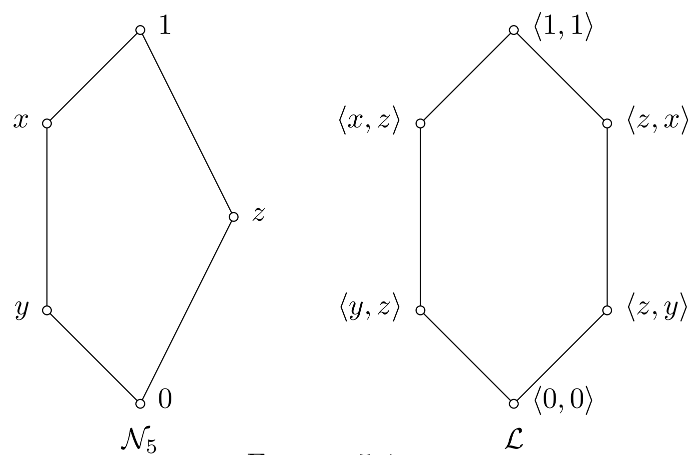


FIGURE 5.1

Next we should show that subdirectly irreducible lattices are indeed those which 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* **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 $\theta \in$* **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 $a \,\theta\, b$ 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 $\mu = \text{con}(a, b)$. $\square$

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 [5] 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 (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 [2] 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 $\alpha, \beta, \gamma \in$ **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

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

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. $\square$

What else can you say about congruence lattices of lattices? *Is every distributive algebraic lattice isomorphic to the congruence lattice of a lattice?* This is the $64,000 question. But while the general question remains open, it is known that 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 [3]), or
(ii) the compact elements are a sublattice of $\mathcal{D}$ (E. T. Schmidt [8]), or
(iii) $\mathcal{D}$ has at most $\aleph_1$ compact elements (A. Huhn [4]).

Thus a counterexample, if there is one, would have to be quite large and complicated.[3] 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.

We need to understand the congruence operator 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 $1 \le i \le k$. The following characterization is a modified version of one found in Dilworth [1].

[3] It is not even known whether every distributive algebraic lattice is isomorphic to the congruence lattice of an algebra with finitely many operations. For recent results on these problems, see M. Tischendorf [9] and M. Ploščica, J. Tůma and F. Wehrung [6], [10].

Theorem 5.9. *Suppose $a_i < b_i$ for $i \in I$. Then $(x, y) \in \bigvee_{i \in I} \operatorname{con}(a_i, b_i)$ 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) $R \subseteq \bigvee_{i \in I} \operatorname{con}(a_i, b_i)$.

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

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. $\square$

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. 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 $c/0$ satisfies the ACC and DCC. This is a fairly natural finiteness condition which 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 $\mathcal{L}$.*

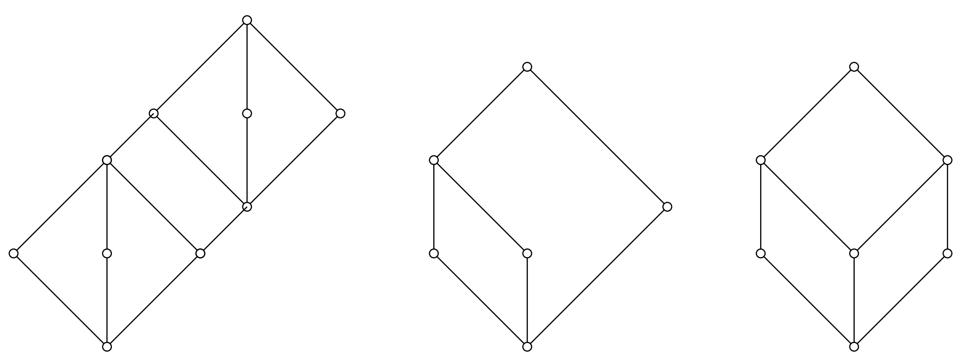
Proof. Every congruence relation is a join of compact congruences, and every compact congruence is a join of finitely many congruences $\operatorname{con}(a, b)$ with $a > b$. In a principally chain finite lattice, every chain in a/b is finite by Exercise 1.5, so there exists a covering chain $a = r_0 \succ r_1 \succ \cdots \succ r_k = b$. Clearly $\operatorname{con}(a, b) = \bigvee_{0 \le j < k} \operatorname{con}(r_j, r_{j+1})$, 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 $a/0$, there is an element x which is minimal with respect to the properties $x \le a$ and $x \not\le b$. 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 $b < x \vee b \le a$, and it follows easily from these two facts that $\operatorname{con}(a, b) = \operatorname{con}(x, x_*)$. $\square$

We will return to congruence lattices of principally chain finite lattices in Chapter 10.

Exercises for Chapter 5

1. Find **Con** $\mathcal{L}$ for the lattices (a) $\mathcal{M}_n$ where $n \ge 3$, (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, $p \le \bigvee F$ implies $p \le f$ for some $f \in F$. Let $\mathrm{P}(\mathcal{L})$ denote the set of join prime elements of $\mathcal{L}$, and define

$$x \,\Delta\, y \qquad \text{iff} \qquad x/0 \cap \mathrm{P}(\mathcal{L}) = y/0 \cap \mathrm{P}(\mathcal{L}).$$

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

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

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

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. 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.)

8. 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.

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 $f \in \mathcal{F}$,

$$(\text{¥}) \qquad x_i \,\theta\, y_i \text{ for } 1 \le i \le n \quad \text{implies} \quad f(x_1,\dots,x_n) \;\theta\; f(y_1,\dots,y_n).$$

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

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

(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 $\mathbf{Con}\ \mathcal{A} = \{\theta \in \mathbf{Eq}\ A : \theta \text{ satisfies } (¥)\}$.

(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.

References

1. R. P. Dilworth, *The structure of relatively complemented lattices*, Ann. of Math. **51** (1950), 348–359.
2. N. Funayama and T. Nakayama, *On the distributivity of a lattice of lattice-congruences*, Proc. Imp. Acad. Tokyo **18** (1942), 553–554.
3. G. Grätzer and E. T. Schmidt, *On congruence lattices of lattices*, Acta Math. Acad. Sci. Hungar. **13** (1962), 179–185.
4. A. Huhn, *On the representation of distributive algebraic lattices II*, Acta Sci. Math. (Szeged). (1989).
5. K. A. Kearnes, *Atomicity and Nilpotence*, Canadian J. Math. **42** (1990), 1–18.
6. M. Ploščica, J. Tuma and F. Wehrung, *Congruence lattices of free lattices in nondistributive varieties*, Coll. Math. (to appear).
7. R. Remak, *Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produckte*, Jour. für Math. **163** (1930), 1–44.
8. 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.
9. M. Tischendorf, *On the representation of distributive semilattices*, Algebra Universalis **31** (1994), 446-455.
10. F. Wehrung, *A uniform refinement property of certain congruence lattices*, Proc. Amer. Math. Soc. (to appear).

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 which, 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 which 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 [1], 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. These 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 $\vee$; these 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 $p, q \in W(X)$ which 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 $\Lambda = \{\theta \in \mathbf{Con}\ W(X) : W(X)/\theta \text{ is a lattice}\}$, 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 [15] (reprinted in [16]), and independently, P. M. Whitman [18] in 1941.[4]

[3] This is where we use that lattices are equationally defined. 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 $x \ngeq \bigwedge G$ for all finite $G \subseteq X - \{x\}$.

Whitman's condition (6), or (W), can be proved using a slick construction due to Alan Day [3]. 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:

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

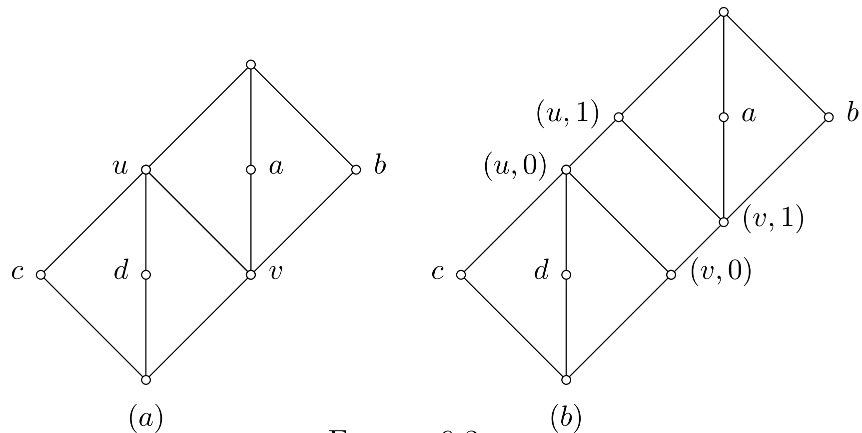


FIGURE 6.3

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 $\mathrm{FL}(X)$. Let $u = c \vee d$, $v = a \wedge b$ and $I = u/v$. Let $h_0 : X \to \mathrm{FL}(X)[I]$ 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 $\kappa h : \mathrm{FL}(X) \to \mathrm{FL}(X)$ 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 $w \in \mathrm{FL}(X)$. 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 $\mathrm{FL}(X)$, so $h(v) \leq h(u)$. But we can calculate

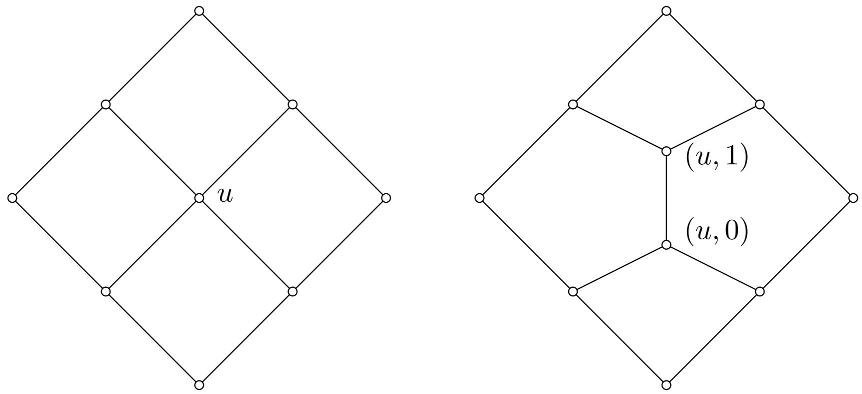
$$h(v) = h(a) \wedge h(b) = a \wedge b = (v, 1) \nleq (u, 0) = c \vee d = h(c) \vee h(d) = h(u)$$

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

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 $\mathrm{FL}(X)$ (and hence in all lattices). Strictly speaking, we have an evaluation map $\varepsilon : W(X) \to \mathrm{FL}(X)$ 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 $\mathrm{FL}(X)$.

---

[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, but we will not need it here.



(a) (b)

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 which 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 [6]. 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 which are both meet and join irreducible. It follows that *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 which 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. $\square$

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 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 $w = \bigvee_{1 \le i \le k} w_i = \bigvee_{1 \le j \le m} u_j$ 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*

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

Proof. For each i we have $w_i \le \bigvee u_j$. If w_i is a generator, this implies $w_i \le u_k$ for some k 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 $w_i \le u_k$ for some k. Hence $\{w_1, \ldots, w_m\} \ll \{u_1, \ldots, u_n\}$. $\square$

Now let $t = \bigvee t_i$ and $s = \bigvee s_j$ be two minimal length terms which 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 $\{w_1, \ldots, w_m\}$ and $\{u_1, \ldots, u_n\}$ are antichains in $\mathrm{FL}(X)$. By Lemma 6.4(3), the elements w_i satisfy the hypothesis of Lemma 6.6, so $\{w_1, \ldots, w_m\} \ll \{u_1, \ldots, u_n\}$. Symmetrically, $\{u_1, \ldots, u_n\} \ll \{w_1, \ldots, w_m\}$. Applying Lemma 6.5(5) yields $\{w_1, \ldots, w_m\} = \{u_1, \ldots, u_n\}$, whence by our assumption above $\{t_1, \ldots, t_m\} = \{s_1, \ldots, s_n\}$. Thus we obtain the desired uniqueness result.

Theorem 6.7. *The minimal length term for $w \in \mathrm{FL}(X)$ 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 which 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 [9].

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

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

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

The implications ($\mathrm{SD}_\vee$) and ($\mathrm{SD}_\wedge$) are known as the *semidistributive laws*.

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 which 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. □

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 J. B. Nation [11].

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 ([7] and [12]), 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 [2], B.. Jónsson [9], and J. B. Nation and J. Schmerl [13], 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 which 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* $|\mathcal{P}| \leq 2^{\mathfrak{m}}$*.*

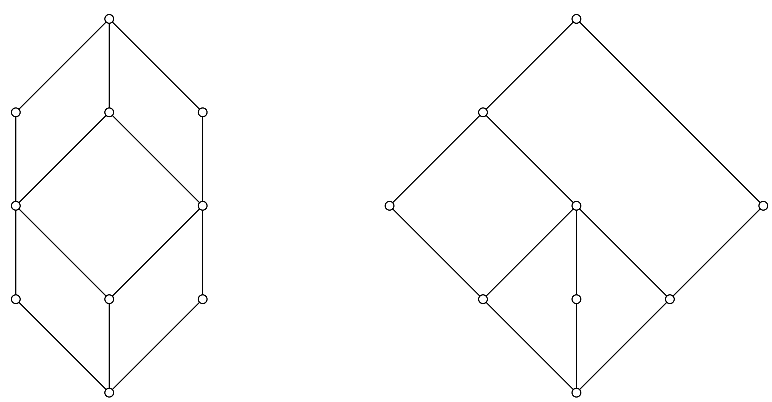
R. A. Dean showed that every equation which does not hold in all lattices fails in some finite lattice [5] (see Exercise 7.5). It turns out (though this is not obvious) that this is related to a beautiful structural result of Alan Day ([4], using [10]).

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

The book *Free Lattices* by Freese, Ježek and Nation [6] contains more information about the surprisingly rich structure of free lattices.

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 which 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 which 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.

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 $\mathcal{L}$. Let $\mathcal{L}$ be a finite lattice 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 $q/0$ and $1/\eta(q)$.

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 [8]).

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 [17], see [14]).

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. G. Birkhoff, *On the structure of abstract algebras*, Proc. Cambridge Phil. Soc. **31** (1935), 433–454.
2. P. Crawley and R. A. Dean, *Free lattices with infinite operations*, Trans. Amer. Math. Soc. **92** (1959), 35–47.
3. A. Day, *A simple solution of the word problem for lattices*, Canad. Math. Bull. **13** (1970), 253–254.
4. A. Day, *Splitting lattices generate all lattices*, Algebra Universalis **7** (1977), 163–170.
5. R. A. Dean, *Component subsets of the free lattice on n generators*, Proc. Amer. Math. Soc. **7** (1956), 220–226.
6. R. Freese, J. Ježek, and J. B. Nation, *Free Lattices*, Mathematical Surveys and Monographs, vol. 42, Amer. Math. Soc., Providence, 1995.
7. R. Freese and J. B. Nation, *Projective lattices*, Pacific J. Math. **75** (1978), 93–106.
8. V. A. Gorbunov, *Canonical decompositions in complete lattices*, Algebra i Logika **17** (1978), 495–511,622. (Russian)
9. B. Jónsson, *Sublattices of a free lattice*, Canad. J. Math. **13** (1961), 256–264.
10. R. McKenzie, *Equational bases and non-modular lattice varieties*, Trans. Amer. Math. Soc. **174** (1972), 1–43.
11. J. B. Nation, *Finite sublattices of a free lattice*, Trans. Amer. Math. Soc. **269** (1982), 311–337.
12. J. B. Nation, *On partially ordered sets embeddable in a free lattice*, Algebra Universalis **18** (1984), 327–333.
13. J. B. Nation and J. H. Schmerl, *The order dimension of relatively free lattices*, Order **7** (1990), 97–99.
14. H. L. Rolf, *The free lattice generated by a set of chains*, Pacific J. Math. **8** (1958), 585–595.
15. 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.
16. T. Skolem, *Select Works in Logic*, Scandinavian University Books, Oslo, 1970.
17. Yu. I. Sorkin, *Free unions of lattices*, Mat. Sbornik **30** (1952), 677–694. (Russian)
18. Ph. M. Whitman, *Free lattices*, Ann. of Math. (2) **42** (1941), 325–330.