1. LATTICES

1.1. Posets. A partially ordered set \( \langle A; \leq \rangle \) consists of a nonvoid set \( A \) and a binary relation \( \leq \) on \( A \) such that the relation \( \leq \) satisfies properties (P1)–(P3) for all \( a, b, c \in A \):

(P1) Reflexivity: \( a \leq a \).

(P2) Antisymmetry: \( a \leq b \) and \( b \leq a \) imply that \( a = b \).

(P3) Transitivity: \( a \leq b \) and \( b \leq c \) imply that \( a \leq c \).

A poset \( \langle A; \leq \rangle \) that also satisfies:

(P4) Linearity: \( a \leq b \) or \( b \leq a \).

is called a chain (also called fully ordered set, linearly ordered set, and so on). The length, \( l(C) \), of a finite chain \( C \) is \( |C| - 1 \). Let \( \mathfrak{C}_n \) denote the set \( \{0, \ldots, n-1\} \) ordered by \( 0 < 1 < 2 < \cdots < n-1 \); then \( \mathfrak{C}_n \) is an \( n \)-element chain and \( l(\mathfrak{C}_n) = n-1 \).

Let \( H \subseteq P \) and \( a \in P \). The element \( a \) is an upper bound of \( H \) iff \( h \leq a \) for all \( h \in H \). An upper bound \( a \) of \( H \) is the least upper bound (supremum) of \( H \) iff, for any upper bound \( b \) of \( H \), we have \( a \leq b \). We shall write \( a = \sup H \) or \( a = \bigvee H \).

The concepts of lower bound and greatest lower bound (infimum) are similarly defined; the latter is denoted by \( \inf H \) or \( \bigwedge H \).

1.2. Lattices. A poset \( \langle L; \leq \rangle \) is a lattice iff \( \inf \{a, b\} \) and \( \sup \{a, b\} \) exist for all \( a, b \in L \).

We will use the notation

\[
\begin{align*}
\wedge b &= \inf \{a, b\}, \\
\vee b &= \sup \{a, b\},
\end{align*}
\]

and call \( \wedge \) the meet and \( \vee \) the join. In lattices, they are both binary operations, which means that they can be applied to a pair of elements \( a, b \) of \( L \) to yield again an element of \( L \).
∧ and ∨ satisfy the following:

(L1) Idempotency: \[ a \land a = a, \quad a \lor a = a. \]

(L2) Commutativity: \[ a \land b = b \land a, \quad a \lor b = b \lor a. \]

(L3) Associativity: \[ (a \land b) \land c = a \land (b \land c), \quad (a \lor b) \lor c = a \lor (b \lor c). \]

There is another pair of rules that connect ∧ and ∨:

(L4) Absorption identities: \[ a \land (a \lor b) = a, \quad a \lor (a \land b) = a. \]

An algebra \( \langle L; \land, \lor \rangle \) is called a lattice iff \( L \) is a nonvoid set, ∧ and ∨ are binary operations on \( L \), both ∧ and ∨ are idempotent, commutative, and associative, and they jointly satisfy the two absorption identities. The following theorem states that a lattice as an algebra and a lattice as a poset are “equivalent” concepts.

**Theorem.**

(i) Let the poset \( \mathcal{L} = \langle L; \leq \rangle \) be a lattice. Set

\[
\begin{align*}
    a \land b &= \inf\{a, b\}, \\
    a \lor b &= \sup\{a, b\}.
\end{align*}
\]

Then the algebra \( \mathcal{L}^a = \langle L; \land, \lor \rangle \) is a lattice.

(ii) Let the algebra \( \mathcal{L} = \langle L; \land, \lor \rangle \) be a lattice. Set

\[ a \leq b \iff a \land b = a. \]

Then \( \mathcal{L}^p = \langle L; \leq \rangle \) is a poset, and the poset \( \mathcal{L}^p \) is a lattice.

(iii) Let the poset \( \mathcal{L} = \langle L; \leq \rangle \) be a lattice. Then \( (\mathcal{L}^a)^p = \mathcal{L} \).

(iv) Let the algebra \( \mathcal{L} = \langle L; \land, \lor \rangle \) be a lattice. Then \( (\mathcal{L}^p)^a = \mathcal{L} \).

2. Diagrams

In the poset \( \langle P; \leq \rangle \), \( a \) covers \( b \), in notation, \( a \succ b \) (or \( b \) is covered by \( a \)), in notation, \( b \prec a \) iff \( b < a \) and \( b < x < a \) holds for no \( x \). The covering relation determines the partial ordering in a finite poset.

The **diagram** of a poset \( \langle P; \leq \rangle \) represents the elements with small circles; the circles representing two elements \( x, y \) are connected by a straight line iff one covers the other; if \( x \) covers \( y \), then the circle representing \( x \) is higher than the circle representing \( y \). Three small examples are shown in Figures 1 and 2.

Note that in a diagram the intersection of two lines does not indicate an element. A diagram is **planar** if no two lines intersect. Figures 1 and 2 show planar diagrams; Figure 3 is not a planar diagram.
The order dimension of a finite poset \((P, \leq)\) is the smallest integer \(n \geq 1\) such that \(\leq\) can be represented as the intersection of the partial ordering relations of \(n\) chains defined on the set \(P\). The order dimension of a finite lattice \(L\) is 1 iff \(L\) is a chain. The order dimension of \(L\) is 2 iff \(L\) has a planar diagram. The order dimension of the lattice of Figure 3 is 3.

A finite lattice \(L\) is of breadth \(n\), if \(n\) is the smallest natural number with the following property: for every \(X \subseteq L\), there is a subset \(X' \subseteq X\) such that \(\bigwedge X = \bigwedge X'\) and \(|X'| \leq n\). Interestingly, this concept is self-dual (that is, defining it for joins yields the same number).

The breadth of a planar lattice is 2. The lattice of Figure 3 is also of breadth 2. The breadth is always less than or equal to the order dimension. David Kelly proved that for every \(n \geq 3\), there is a (modular) lattice of breadth 3 and order dimension \(n\).

### 3. Some algebraic concepts

Let \(L\) be a lattice. \(K \subseteq L\) is a sublattice of \(L\) (or \(L\) is an extension of \(K\)) if \(K\) is closed under the operations of \(L\) and the operations of \(K\) are the restrictions of the operations of \(L\) to \(K\). If \(a, b \in L\), then

\[
[a, b] = \{ x \mid a \leq x \leq b \}
\]

is a sublattice of \(L\), called an interval. If \(a\) covered by \(b\), then \([a, b]\) is a prime interval; it has only two elements.
A related concept is an ideal. A sublattice $I$ of a lattice $L$ is an ideal, if $a \land i \in I$ for all $i \in I$ and $a \in L$. The ideals of a lattice form a lattice under set inclusion; $\text{Id } L$ is the notation for this lattice.

A homomorphism $\varphi$ of the lattice $L$ into the lattice $K$ is a map of $L$ into $K$ satisfying both

$$\begin{align*}
(a \land b)\varphi &= a\varphi \land b\varphi, \\
(a \lor b)\varphi &= a\varphi \lor b\varphi.
\end{align*}$$

If only the first (resp., second) holds, then $\varphi$ is a meet-homomorphism (resp., join-homomorphism).

Figures 4–6 show three maps of the four-element lattice $L$ of Figure 1 into the three-element chain $\mathcal{C}_3$. The map of Figure 4 is isotone (that is, if $x \leq y$ in $L$, then $x\varphi \leq y\varphi$ in $K$) but is neither a meet- nor a join-homomorphism. The map of Figure 5 is a join-homomorphism but is not a meet-homomorphism, thus not a homomorphism. The map of Figure 6 is a homomorphism.

A one-to-one and onto homomorphism is an isomorphism. An isomorphism of a lattice with itself is called an automorphism. The automorphisms of a lattice $L$ form a group under composition, called the automorphism group of $L$; it is denoted by $\text{Aut } L$.

An equivalence relation $\Theta$ (that is, a reflexive, symmetric, and transitive binary relation) on a lattice $L$ is called a congruence relation of $L$ iff

$$\begin{align*}
a_0 &\equiv b_0 \pmod{\Theta}, \\
a_1 &\equiv b_1 \pmod{\Theta}
\end{align*}$$

imply that

$$\begin{align*}
a_0 \land a_1 &\equiv b_0 \land b_1 \pmod{\Theta}, \\
a_0 \lor a_1 &\equiv b_0 \lor b_1 \pmod{\Theta}
\end{align*}$$

(Substitution Property). Trivial examples are $\omega$, $i$, defined by $x \equiv y$ ($\omega$) iff $x = y$; $x \equiv y$ ($i$) for all $x$ and $y$. ($\omega$ is the Greek $\omega$ and stands for 0; $i$ is the Greek $i$ and stands for identity and 1.) For $a \in L$, we write $[a]_{\Theta}$ for the congruence class containing $a$, that is,

$$[a]_{\Theta} = \{ x \mid x \equiv a \ (\Theta) \}.$$

Homomorphisms and congruence relations express two sides of the same phenomenon. Let $L$ be a lattice and let $\Theta$ be a congruence relation on $L$. Let $L/\Theta$ denote the set of blocks of the partition of $L$ induced by $\Theta$, that is,

$$L/\Theta = \{ [a]_{\Theta} \mid a \in L \}.$$
Set
\[ [a] \Theta \wedge [b] \Theta = [a \wedge b] \Theta, \]
\[ [a] \Theta \vee [b] \Theta = [a \vee b] \Theta. \]
This defines $\wedge$ and $\vee$ on $L/\Theta$. The lattice axioms are easily verified. The lattice $L/\Theta$ is the quotient lattice of $L$ modulo $\Theta$, and the map
\[ \varphi_\Theta : x \rightarrow [x] \Theta \quad (x \in L) \]
is a homomorphism of $L$ onto $L/\Theta$.

Next, we introduce direct products. Let $L$ and $K$ be lattices and form the set $L \times K$ of all ordered pairs $(a, b)$ with $a \in L$, $b \in K$. Define $\wedge$ and $\vee$ in $L \times K$ “componentwise”:
\[ (a_0, b_0) \wedge (a_1, b_1) = (a_0 \wedge a_1, b_0 \wedge b_1), \]
\[ (a_0, b_0) \vee (a_1, b_1) = (a_0 \vee a_1, b_0 \vee b_1). \]
This makes $L \times K$ into a lattice, called the direct product of $L$ and $K$ (for an example, see Figure 7).

Finally, we define identities and inequalities.

From variables $x_0, x_1, \ldots, x_n, \ldots$, we can form polynomials (terms) in the usual manner using $\wedge, \vee$, and, of course, parentheses. Examples of polynomials are:
\[ x_0, x_3, \quad x_0 \vee x_0, \quad (x_0 \wedge x_2) \vee (x_3 \wedge x_0), \quad (x_0 \wedge x_1) \vee (x_0 \wedge x_2) \vee (x_1 \wedge x_2). \]

A polynomial is just a sequence of symbols. It is defined because in terms of such a sequence of symbols we can define a function on any lattice. For instance, if $p = (x_0 \wedge x_1) \vee (x_2 \vee x_1)$, then $p(a, b, c) = (a \wedge b) \vee (c \vee b) = b \vee c = i$ in $\mathfrak{N}_5$.

A lattice identity is an expression of the form $p = q$, where $p$ and $q$ are polynomials. An identity $p = q$ holds in the lattice $L$ if $p(a_0, \ldots, a_{n-1}) = q(a_0, \ldots, a_{n-1})$ holds for any $a_0, \ldots, a_{n-1} \in L$. Similarly, we define a lattice inequality $p \leq q$.

The two identities:
\[ x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z), \]
\[ x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \]
are equivalent; a lattice satisfying one (or both) is called **distributive**.

A distributive lattice $B$ is called **Boolean** if it has a smallest element 0 and a largest element 1, and every element $x$ has a complement $x'$, that is, 

$$x \land x' = 0,$$

$$x \lor x' = 1.$$ 

Every finite Boolean lattice is isomorphic to some $\mathfrak{B}_n = (\mathfrak{C}_2)^n (= \mathfrak{C}_2 \times \cdots \times \mathfrak{C}_2)$. The identity

$$(x \land y) \lor (x \land z) = x \land (y \lor (x \land z))$$

is equivalent to the condition:

$x \geq z$ implies that $(x \land y) \lor z = x \land (y \lor z)$.

A lattice satisfying either condition is called **modular**.

A more complicated identity is the **arguesian** identity:

$$p \leq ((c \lor x_2) \land x_0) \lor ((c \lor x_5) \land x_3),$$

where

$$p = (x_0 \lor x_3) \land (x_1 \lor x_4) \land (x_2 \lor x_5)$$

$$c_{ij} = (x_i \lor x_j) \land (x_{3+i} \lor x_{3+j}), \quad 0 \leq i < j \leq 2,$$

$$c = c_{01} \land (c_{02} \lor c_{12}).$$

An arguesian lattice is modular. The subspace lattice of a projective space is arguesian iff Desargues’ Theorem holds for the projective space. The lattice of all subspaces of a vector space is arguesian.

### 4. DISTRIBUTIVE LATTICES

The two typical examples of nondistributive lattices are $\mathfrak{M}_3$ and $\mathfrak{N}_5$, whose diagrams are given in Figure 2. 

**Theorem.** A lattice $L$ is distributive iff $L$ does not contain $\mathfrak{M}_3$ or $\mathfrak{N}_5$ as a sublattice.

For a distributive lattice $D$, let $J(D)$ denote the set of all nonzero join-irreducible elements, that is, all elements $a \in D$ for which $a = x \lor y$ implies that $a = x$ or $a = y$. We regard $J(D)$ as a poset under the partial ordering of $D$. For $a \in D$, set

$$r(a) = \{ x \mid x \leq a, \ x \in J(D) \} = (a] \cap J(D).$$

For a poset $P$, call $A \subseteq P$ **hereditary** iff $x \in A$ and $y \leq x$ imply that $y \in A$. Let $H(P)$ denote the set of all hereditary subsets partially ordered by set inclusion. Note that $H(P)$ is a lattice in which meet and join are intersection and union, respectively, and thus $H(P)$ is distributive.

The structure of finite distributive lattices is revealed by the following result:

**Theorem.** Let $D$ be a finite distributive lattice. Then the map

$$\varphi: a \rightarrow r(a)$$

is an isomorphism between $D$ and $H(J(D))$.

**Corollary.** The correspondence $D \rightarrow J(D)$ makes the class of all finite distributive lattices with more than one element correspond to the class of all finite posets. Isomorphic lattices correspond to isomorphic posets, and vice versa.
Let $\text{Con} L$ denote the set of all congruence relations on $L$ partially ordered by set inclusion.

**Theorem (R. P. Dilworth).** $\text{Con} L$ is a lattice. For $\Theta, \Phi \in \text{Con} L$, $\Theta \land \Phi = \Theta \cap \Phi$. The join, $\Theta \lor \Phi$, can be described as follows:

\[ x \equiv y (\Theta \lor \Phi) \text{ iff there is a sequence } z_0 = x \land y, z_1, \ldots, z_{n-1} = x \lor y \text{ of elements of } L \text{ such that } z_0 \leq z_1 \leq \cdots \leq z_{n-1} \text{ and for each } i, 0 \leq i < n-1, \]
\[ z_i \equiv z_{i+1} (\Theta) \text{ or } z_i \equiv z_{i+1} (\Phi). \]

**Theorem (N. Funayama and T. Nakayama).** Let $L$ be an arbitrary lattice. Then $\text{Con} L$, the lattice of all congruence relations of $L$, is distributive.

Let $L$ be a lattice and let $H \subseteq L^2$. We denote by $\Theta(H)$ the smallest congruence relation such that $a \equiv b$ for all $(a, b) \in H$, and call it the congruence relation generated by $H$. For any $H \subseteq L^2$, $\Theta(H)$ exists.

We shall use the notation $\Theta(a, b)$ for $\Theta(H)$ if $H = \{(a, b)\}$. Note that $\Theta(a, b)$ is the smallest congruence relation under which $a \equiv b$. The congruence relation $\Theta(a, b)$ is called principal.

![Figure 8](image_url)

If $L$ is finite, knowing $J(\text{Con} L)$, one knows $\text{Con} L$. In a finite lattice $L$, $\Theta$ is a join-irreducible congruence relation iff it is of the form $\Theta(a, b)$, where $a$ is covered by $b$. Such $\Theta(a, b)$ are usually easy to compute: for $c$ covered by $d$,

\[ c \equiv d \ (\Theta(a, b)) \]

iff we can get from $a$, $b$ to $c$, $d$ with a finite number of up- and down-steps, as illustrated by Figure 8. (In general, $c \equiv d \ (\Theta(a, b))$ iff $x \equiv y \ (\Theta(a, b))$ for any $c \leq x \prec y \leq d$.) An up-step joins the pair of elements with an element; a down-step meets the pair of elements with an element. Note that we start with—and end up with—a covering pair of elements, but the intermediate steps are not necessarily covering pairs. However, if $L$ is also modular, then all the intermediate steps are covering pairs, which implies the following result: $\text{Con} L$ is Boolean for a finite modular lattice $L$.

Another property of congruence lattices is given in the following definition.
Definition.

(i) Let $L$ be a complete lattice and let $a$ be an element of $L$. Then $a$ is called **compact** iff $a \leq \bigvee X$ for some $X \subseteq L$ implies that $a \leq \bigvee X_1$ for some finite $X_1 \subseteq X$.

(ii) A complete lattice is called **algebraic** iff every element is the join of compact elements.

It is easy to see that every principal congruence relation is compact, which implies that for an arbitrary lattice $L$, $\text{Con} L$ is an algebraic lattice.

**Lemma.** Let $L$ be an arbitrary lattice. Then $\text{Con} L$ is a distributive algebraic lattice.

The converse is a long-standing conjecture of lattice theory. We shall outline the proof for the finite case (R. P. Dilworth, G. Grätzer and E. T. Schmidt).

**Theorem.** Let $D$ be a finite distributive lattice. Then there exists a finite lattice $L$ such that $D$ is isomorphic to $\text{Con} L$.

Let $M$ be a finite poset such that $\inf\{a, b\}$ exists in $M$ for any $a, b \in M$. We define in $M$: $a \land b = \inf\{a, b\}$ for all $a, b \in M$; and $a \lor b = \sup\{a, b\}$ whenever $\sup\{a, b\}$ exists. This makes $M$ into a **chopped lattice**. (From a finite lattice $L$ with unit element $1$, we can obtain a chopped lattice $M = L - \{1\}$, and conversely.) An equivalence relation $\Theta$ on $M$ is a congruence relation iff $a_0 \equiv b_0 \ (\Theta)$ and $a_1 \equiv b_1 \ (\Theta)$ imply that $a_0 \land a_1 \equiv b_0 \land b_1 \ (\Theta)$ and that $a_0 \lor a_1 \equiv b_0 \lor b_1 \ (\Theta)$ whenever $a_0 \lor a_1$ and $b_0 \lor b_1$ both exist. Then the set $\text{Con} M$ of all congruence relations is again a lattice.

**Lemma 1.** Let $D$ be a finite distributive lattice. Then there exists a chopped lattice $M$ such that $\text{Con} M$ is isomorphic to $D$.

We outline the construction of $M$. Take the set $M_0 = J(D) \cup \{0\}$, and make it a chopped lattice by defining $\inf\{a, b\} = 0$ if $a \neq b$, as illustrated in Figure 9. Note that $a \equiv b \ (\Theta)$ and $a \neq b$ imply in $M_0$ that $a \equiv 0 \ (\Theta)$ and $b \equiv 0 \ (\Theta)$; therefore, the congruence relations of $M_0$ are in one-to-one correspondence with subsets of $J(D)$. Thus $\text{Con} M_0$ is a Boolean lattice whose atoms are associated with elements of $J(D)$; the congruence $\Phi_a$ associated with $a \in J(D)$ can be described as follows:

- $a \equiv 0 \ (\Phi_a)$ and if $\{x, y\} \neq \{a, 0\}$, then $x \equiv y \ (\Phi_a)$ implies that $x = y$. 

Figure 9
CONGRUENCE LATTICES

If \( J(D) \) is unordered, then we are ready. However, if, say, \( a, b \in J(D) \) and \( a > b \) in \( D \), then we must have \( \Phi_a > \Phi_b \). We make this happen by using the lattice \( M(a, b) \) of Figure 10. Note that \( M(a, b) \) has three congruence relations, namely, \( \omega \), \( \iota \), and \( \Theta \), where \( \Theta \) is the congruence relation with congruence classes \( \{0, b_1, b_2, b\} \) and \( \{a_1, a(b)\} \). Thus \( \Theta(a_1, 0) = \iota \). In other words, \( a_1 \equiv 0 \) “implies” that \( b_1 \equiv 0 \), but \( b_1 \equiv 0 \) “does not imply” that \( a_1 \equiv 0 \).

We construct \( M \) by “inserting” \( M(a, b) \) in \( M_0 \) whenever \( a > b \) in \( J(D) \). Figure 11 gives \( M \) if \( J(D) \) is the three-element chain.

For \( x, y \in M \), let us define \( x \leq y \) to mean that for some \( a, b \in J(D) \) with \( a > b \), we have \( x, y \in M(a, b) \) and \( x \leq y \) in the lattice \( M(a, b) \) as illustrated in Figure 11. It is easily seen that \( x \leq y \) does not depend on the choice of \( a \) and \( b \), and that \( \leq \) is a partial ordering relation under which \( M \) is a chopped lattice.

It is routine to check that \( \text{Con} \ M \cong D \).

The next lemma “completes” \( M \) to a lattice, while preserving the congruence lattice.

An ideal \( I \) of a chopped lattice \( M \) is a subset \( I \subseteq M \) with the property that for \( i \in I \) and \( a \in M \), \( i \wedge a \in I \) and for \( x, y \in I \), \( x \vee y \in I \) provided that \( x \vee y \) exists in \( M \). The ideals of \( M \) form a lattice \( \text{Id} \ M \).

**Lemma 2 (G. Grätzer and H. Lakser).** Let \( M \) be a chopped lattice. Then for every congruence relation \( \Theta \) of \( M \), there exists exactly one congruence relation \( \overline{\Theta} \) of \( \text{Id} \ M \) such that for \( a, b \in M \),

\[(a) \equiv (b) \quad (\overline{\Theta}) \quad \text{iff} \quad a \equiv b \quad (\Theta).\]
The proof of the theorem is immediate from these two lemmas. For the finite distributive lattice $D$, take the chopped lattice $M$ of Lemma 1; then $M$ satisfies $\text{Con} M \cong D$. Define the lattice $L$ as $\text{Id} M$. By Lemma 2, $\text{Con} L \cong \text{Con} M$. Hence $\text{Con} L \cong D$. Since $M$ is finite, so is $L$.

Department of Mathematics, University of Manitoba, Winnipeg, Man. R3T 2N2, Canada

E-mail address: George.Gratzer@umanitoba.ca

URL: http://www.maths.umanitoba.ca/homepages/gratzer.html/