Introduction to Universal Algebra

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

Subsection 1

Definitions of Lattices

Definition of a Lattice

Definition (Lattice)

A nonempty set L together with two binary operations $\vee$ and $\wedge$ (read "**join**" and "**meet**" respectively) on L is called a **lattice** if it satisfies the following identities:

- L1 **(commutative laws)**
  - (a) $x \vee y \approx y \vee x$;
  - (b) $x \wedge y \approx y \wedge x$
- L2 **(associative laws)**
  - (a) $x \vee (y \vee z) \approx (x \vee y) \vee z$;
  - (b) $x \wedge (y \wedge z) \approx (x \wedge y) \wedge z$;
- L3 **(idempotent laws)**
  - (a) $x \vee x \approx x$;
  - (b) $x \wedge x \approx x$;
- L4 **(absorption laws)**
  - (a) $x \approx x \vee (x \wedge y)$;
  - (b) $x \approx x \wedge (x \vee y)$.

Example: Let L be the set of propositions, $\vee$ the connective "or" and $\wedge$ the connective "and". L1 to L4 are well-known properties from propositional logic.

Example: Let $L = \mathbb{N}$, $\vee$ the least common multiple and $\wedge$ the greatest common divisor. Then properties L1 to L4 are easily verifiable.

Ordered Sets

Definition (Orders)

A binary relation $\leq$ defined on a set A is a **partial order** on the set A if the following conditions hold identically in A:

(i) $a \leq a$ (**reflexivity**)

(ii) $a \leq b$ and $b \leq a$ imply $a = b$ (**antisymmetry**)

(iii) $a \leq b$ and $b \leq c$ imply $a \leq c$ (**transitivity**)

If, in addition, for every a, b in A,

(iv) $a \leq b$ or $b \leq a$,

then we say $\leq$ is a **total order** on A.

A nonempty set with a partial order on it is called a **partially ordered set**, or more briefly a **poset**. If the relation is a total order then we speak of a **totally ordered set**, or a **linearly ordered set**, or simply a **chain**.

In a poset A we use the expression $a < b$ to mean $a \leq b$ but $a \neq b$.

Examples of Partially Ordered Sets

(1) Let Su(A) denote the **power set** of A, i.e., the set of all subsets of A. Then $\subseteq$ is a partial order on Su(A).

(2) Let A be the set of natural numbers and let $\leq$ be the relation "divides". Then $\leq$ is a partial order on A.

(3) Let A be the set of real numbers and let $\leq$ be the usual ordering. Then $\leq$ is a total order on A.

Bounds

Definition (Bounds)

Let A be a subset of a poset P.
An element p in P is an **upper bound** for A if $a \leq p$, for every a in A.
An element p in P is the **least upper bound** of A (**l.u.b.** of A), or **supremum** of A ($\sup A$) if:

- p is an upper bound of A, and
- $a \leq b$, for every a in A implies $p \leq b$ (i.e., p is the smallest among the upper bounds of A).

An element p in P is a **lower bound** for A if $p \leq a$, for every a in A.
An element p in P is the **greatest lower bound** of A (**g.l.b.** of A), or **infimum** of A ($\inf A$) if:

- p is a lower bound of A, and
- $b \leq a$, for every a in A implies $b \leq p$ (i.e., p is the largest among the lower bounds of A).

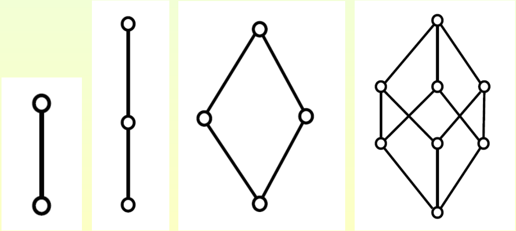
Covers and Intervals

Definition

Let A be a subset of a poset P and $a, b \in P$.
We say b **covers** a, or a **is covered by** b, if $a < b$, and whenever $a \leq c \leq b$, it follows that $a = c$ or $c = b$. We use the notation $a \prec b$ to denote a is covered by b.
The **closed interval** $[a, b]$ is defined to be the set of c in P, such that $a \leq c \leq b$.
The **open interval** (a, b) is the set of c in P, such that $a < c < b$.

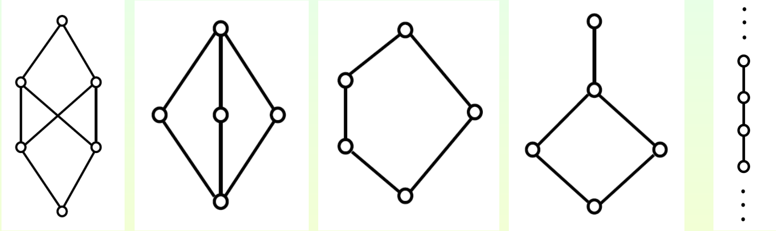
Hasse Diagrams

- We describe the method of associating a **Hasse diagram** with a finite poset P:
  - We represent each element of P by a small circle.
  - If $a \prec b$, then we draw the circle for b above the circle for a, joining the two circles with a line segment.
- From this diagram we can recapture the relation $\leq$ by noting that $a \leq b$ holds iff, for some finite sequence of elements $c_1, \ldots, c_n$ from P, we have $a = c_1 \prec c_2 \prec \cdots \prec c_{n-1} \prec c_n = b$.



Hasse Diagrams for Infinite Posets

- Some more examples



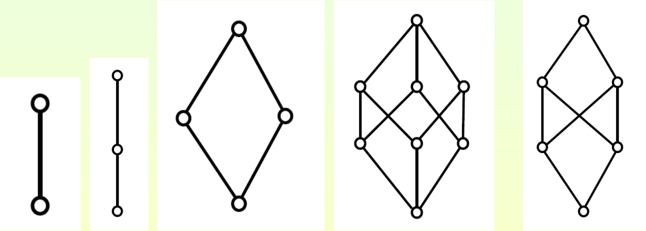
- It is not so clear how one would draw an infinite poset.
  - For example, the real line with the usual ordering has no covering relations, but it is quite common to visualize it as a vertical line. Unfortunately, the rational line would have the same picture.
  - The diagram on the very right depicts the integers under the usual ordering.

Lattices as Partially Ordered Sets

Definition (Lattice)

A poset L is a **lattice** iff for every a, b in L both $\sup\{a, b\}$ and $\inf\{a, b\}$ exist (in L).

- The poset in each of the first four following diagrams is a lattice:



- The poset corresponding to the last diagram has the interesting property that every pair of elements has an upper bound and a lower bound, but is not a lattice.

Algebraic Lattice to Partially Ordered Lattice

(A) If L is a lattice by the algebraic definition, then define $\leq$ on L by $a \leq b$ iff $a = a \wedge b$.

Suppose that L is a lattice by the first definition and $\leq$ is defined as in (A). Since $a \wedge a = a$, we get $a \leq a$. If $a \leq b$ and $b \leq a$, then $a = a \wedge b$ and $b = b \wedge a$. Hence $a = b$. If $a \leq b$ and $b \leq c$, then $a = a \wedge b$ and $b = b \wedge c$. So $a = a \wedge b = a \wedge (b \wedge c) = (a \wedge b) \wedge c = a \wedge c$, whence $a \leq c$. This shows $\leq$ is a partial order on L.

Since $a = a \wedge (a \vee b)$ and $b = b \wedge (a \vee b)$, we get $a \leq a \vee b$ and $b \leq a \vee b$, so $a \vee b$ is an upper bound of both a and b.

If $a \leq u$ and $b \leq u$, then $a \vee u = (a \wedge u) \vee u = u$, and likewise $b \vee u = u$. So $(a \vee u) \vee (b \vee u) = u \vee u = u$. Hence $(a \vee b) \vee u = u$, giving $(a \vee b) \wedge u = (a \vee b) \wedge [(a \vee b) \vee u] = a \vee b$ (by the absorption law). This says $a \vee b \leq u$. Thus $a \vee b = \sup\{a, b\}$.

Similarly, $a \wedge b = \inf\{a, b\}$.

Partially Ordered to Algebraic Lattice

(B) If L is a partially ordered lattice, then define the operations $\vee$ and $\wedge$ by $a \vee b = \sup\{a, b\}$ and $a \wedge b = \inf\{a, b\}$.

These operations satisfy the requirements L1 to L4. E.g., the absorption law L4(a) becomes

$$a = \sup\{a, \inf\{a, b\}\},$$

which is clearly true as $\inf\{a, b\} \leq a$.

- The two constructions (A) and (B) are inverses of each other.

Subsection 2

Isomorphic Lattices, and Sublattices

Lattice Isomorphisms and Order-Preserving Maps

Definition (Lattice Isomorphism)

Two lattices L_1 and L_2 are **isomorphic** if there is a bijection α from L_1 to L_2, such that for every a, b in L_1 the following two equations hold:

$$\alpha(a \vee b) = \alpha(a) \vee \alpha(b) \quad \text{and} \quad \alpha(a \wedge b) = \alpha(a) \wedge \alpha(b).$$

Such an α is called an **isomorphism**.

- If α is an isomorphism from L_1 to L_2, then α^{-1} is an isomorphism from L_2 to L_1;
- If, in addition, β is an isomorphism from L_2 to L_3, then $\beta \circ \alpha$ is an isomorphism from L_1 to L_3.

Definition (Order-Preserving Map)

If P_1 and P_2 are two posets and α is a map from P_1 to P_2, then we say α is **order-preserving** if, for all $a, b \in P_1$, $a \leq b$ in P_1 implies $\alpha(a) \leq \alpha(b)$ in P_2.

Lattice Isomorphisms and Order-Preservation

Theorem

Two lattices L_1 and L_2 are isomorphic iff there is a bijection α from L_1 to L_2, such that both α and α^{-1} are order-preserving.

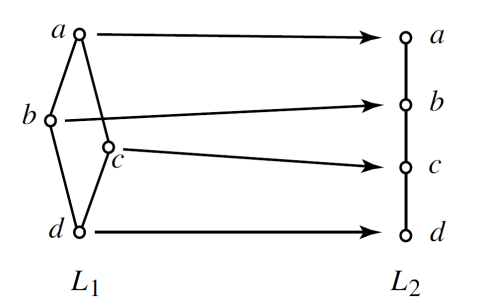
- Suppose α is an isomorphism from L_1 to L_2. If $a \leq b$ holds in L_1, then $a = a \wedge b$, so $\alpha(a) = \alpha(a \wedge b) = \alpha(a) \wedge \alpha(b)$. Hence $\alpha(a) \leq \alpha(b)$, and, thus, α is order-preserving. Since α^{-1} is an isomorphism, it is also order-preserving.

  Conversely, let α be a bijection from L_1 to L_2, such that both α and α^{-1} are order-preserving. For a, b in L_1, we have $a \leq a \vee b$ and $b \leq a \vee b$. So $\alpha(a) \leq \alpha(a \vee b)$ and $\alpha(b) \leq \alpha(a \vee b)$. Hence, $\alpha(a) \vee \alpha(b) \leq \alpha(a \vee b)$. Furthermore, if $\alpha(a) \vee \alpha(b) \leq u$, then $\alpha(a) \leq u$ and $\alpha(b) \leq u$. Hence $a \leq \alpha^{-1}(u)$ and $b \leq \alpha^{-1}(u)$. So $a \vee b \leq \alpha^{-1}(u)$, and, thus, $\alpha(a \vee b) \leq u$. This implies that $\alpha(a) \vee \alpha(b) = \alpha(a \vee b)$.

  Similarly, it can be argued that $\alpha(a) \wedge \alpha(b) = \alpha(a \wedge b)$.

A Non-Isomorphism Order-Preserving Bijection

- An example of a bijection α between lattices which is order-preserving but not an isomorphism is shown below:

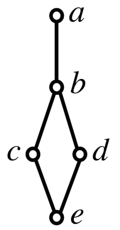


Sublattices

Definition (Sublattice)

If L is a lattice and $L' \neq \emptyset$ is a subset of L, such that, for every pair of elements a, b in L', both $a \vee b$ and $a \wedge b$ are in L', where $\vee$ and $\wedge$ are the lattice operations of L, then we say that L' with the same operations (restricted to L') is a **sublattice** of L.

- If L' is a sublattice of L, then for a, b in L', we have $a \leq b$ in L' iff $a \leq b$ in L.
- Given a lattice L, one can often find subsets which, as posets, are lattices, but which do not qualify as sublattices, as the operations $\vee$ and $\wedge$ do not agree with those of the original lattice L.
  Example: $P = \{a, c, d, e\}$ as a poset is indeed a lattice. But P is not a sublattice of the lattice $\{a, b, c, d, e\}$.

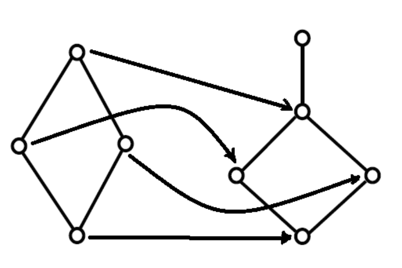


Lattice Embeddings

Definition (Lattice Embedding)

A lattice L_1 can be **embedded into** a lattice L_2 if there is a sublattice of L_2 isomorphic to L_1. In this case we also say L_2 **contains a copy of** L_1 **as a sublattice**.

Example:



Subsection 3

Distributive and Modular Lattices

Distributive Lattices

Definition (Distributive Lattice)

A **distributive lattice** is a lattice which satisfies either (and hence, as we shall see, both) of the distributive laws:

D1 $x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z)$;

D2 $x \vee (y \wedge z) \approx (x \vee y) \wedge (x \vee z)$.

Theorem

A lattice L satisfies D1 iff it satisfies D2.

- Suppose D1 holds. Then:

$$\begin{aligned} x \vee (y \wedge z) &\approx (x \vee (x \wedge z)) \vee (y \wedge z) \approx x \vee ((x \wedge z) \vee (y \wedge z)) \\ &\approx x \vee ((z \wedge x) \vee (z \wedge y)) \approx x \vee (z \wedge (x \vee y)) \\ &\approx x \vee ((x \vee y) \wedge z) \approx (x \wedge (x \vee y)) \vee ((x \vee y) \wedge z) \\ &\approx ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) \approx (x \vee y) \wedge (x \vee z). \end{aligned}$$

Thus D2 also holds. Similarly, if D2 holds, then so does D1.

Sufficient Conditions

- Note that every lattice satisfies both of the inequalities

$$\begin{array}{rcl} (x \wedge y) \vee (x \wedge z) & \leq & x \wedge (y \vee z); \\ x \vee (y \wedge z) & \leq & (x \vee y) \wedge (x \vee z). \end{array}$$

  To see this, note for example that $x \wedge y \leq x$ and $x \wedge y \leq y \vee z$. Hence $x \wedge y \leq x \wedge (y \vee z)$, etc.

- Thus to verify the distributive laws in a lattice it suffices to check either of the following inequalities:

$$\begin{array}{rcl} x \wedge (y \vee z) & \leq & (x \wedge y) \vee (x \wedge z); \\ (x \vee y) \wedge (x \vee z) & \leq & x \vee (y \wedge z). \end{array}$$

Modular Lattices

Definition (Modular Lattice)

A **modular lattice** is any lattice which satisfies the modular law:

M $x \leq y \rightarrow x \vee (y \wedge z) \approx y \wedge (x \vee z)$.

- The modular law is obviously equivalent (for lattices) to the identity

$$(x \wedge y) \vee (y \wedge z) \approx y \wedge ((x \wedge y) \vee z)$$

  since $a \leq b$ holds iff $a = a \wedge b$.
- Since every lattice satisfies $x \leq y \rightarrow x \vee (y \wedge z) \leq y \wedge (x \vee z)$, to verify the modular law it suffices to check the implication

$$x \leq y \rightarrow y \wedge (x \vee z) \leq x \vee (y \wedge z).$$

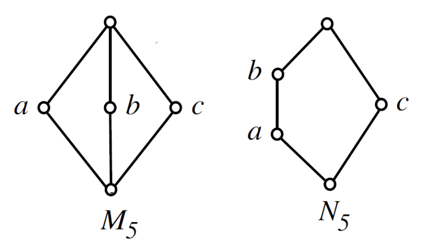
Theorem

Every distributive lattice is a modular lattice.

- Assume distributivity and let $x \leq y$. The $y \wedge x = x$. So $x \vee (y \wedge z) = (y \wedge x) \vee (y \wedge z) = y \wedge (x \vee z)$.

The Lattices M_5 and N_5

- Consider the two five-element lattices M_5 and N_5:



- We have:
  - In M_5: $a \vee (b \wedge c) = a \vee 0 = a \neq 1 = 1 \vee 1 = (a \vee b) \wedge (a \vee c)$
  - In N_5: $a \vee (b \wedge c) = a \vee 0 = a \neq b = b \wedge 1 = (a \vee b) \wedge (a \vee c)$

  So neither M_5 nor N_5 is a distributive lattice.
- In N_5, we also see that $a \leq b$, but
  $a \vee (b \wedge c) = a \vee 0 = a \neq b = b \wedge 1 = b \wedge (a \vee c)$ So N_5 is not modular.
  However, we can verify that M_5 satisfies the distributive law.

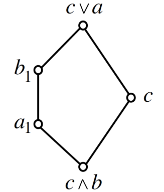
Characterization of Modular Lattices

Theorem (Dedekind)

L is a nonmodular lattice iff N_5 can be embedded into L.

- From the preceding remarks, if N_5 can be embedded into L, then L does not satisfy the modular law.

  For the converse, suppose that L does not satisfy the modular law. Then, for some a, b, c in L, we have $a \leq b$ but $a \vee (b \wedge c) < b \wedge (a \vee c)$. Let $a_1 = a \vee (b \wedge c)$ and $b_1 = b \wedge (a \vee c)$. Then $c \wedge b_1 = c \wedge [b \wedge (a \vee c)] = [c \wedge (c \vee a)] \wedge b = c \wedge b$ and $c \vee a_1 = c \vee [a \vee (b \wedge c)] = [c \vee (c \wedge b)] \vee a = c \vee a$. Now, as $c \wedge b \leq a_1 \leq b_1$, we have $c \wedge b \leq c \wedge a_1 \leq c \wedge b_1 = c \wedge b$, whence $c \wedge a_1 = c \wedge b_1 = c \wedge b$. Likewise $c \vee b_1 = c \vee a_1 = c \vee a$. Now it is straightforward to verify that the diagram in the figure gives the desired copy of N_5 in L.



Characterization of Distributive Lattices

Theorem (Birkhoff)

L is a non-distributive lattice iff M_5 or N_5 can be embedded into L.

- If either M_5 or N_5 can be embedded into L, then it is clear from previous remarks that L cannot be distributive.

  For the converse, let us suppose that L is a non-distributive lattice and that L does not contain a copy of N_5 as a sublattice. Thus L is modular by the preceding theorem. Since the distributive laws do not hold in L, there must be elements a, b, c from L, such that $(a \wedge b) \vee (a \wedge c) < a \wedge (b \vee c)$. We define

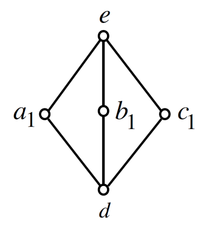
$$d = (a \wedge b) \vee (a \wedge c) \vee (b \wedge c), \quad e = (a \vee b) \wedge (a \vee c) \wedge (b \vee c),$$
$$a_1 = (a \wedge e) \vee d, \quad b_1 = (b \wedge e) \vee d, \quad c_1 = (c \wedge e) \vee d.$$

  It is easily seen that $d \leq a_1, b_1, c_1 \leq e$. Now from $a \wedge e = a \wedge (b \vee c)$,

$$\begin{aligned} a \wedge d &= a \wedge ((a \wedge b) \vee (a \wedge c) \vee (b \wedge c)) \\ &= ((a \wedge b) \vee (a \wedge c)) \vee (a \wedge (b \wedge c)) = (a \wedge b) \vee (a \wedge c), \end{aligned}$$

  it follows that $d < e$.

Characterization of Distributive Lattices (Cont'd)



- We now show that the diagram is a copy of M_5 in L. To do this it suffices to show that

$$a_1 \wedge b_1 = a_1 \wedge c_1 = b_1 \wedge c_1 = d$$

and

$$a_1 \vee b_1 = a_1 \vee c_1 = b_1 \vee c_1 = e.$$

We will verify one case only and the others require similar arguments:

$$\begin{aligned} a_1 \wedge b_1 &= ((a \wedge e) \vee d) \wedge ((b \wedge e) \vee d) \overset{(M)}{=} ((a \wedge e) \wedge ((b \wedge e) \vee d)) \vee d \\ &\overset{(M)}{=} ((a \wedge e) \wedge ((b \vee d) \wedge e)) \vee d = ((a \wedge e) \wedge e \wedge (b \vee d)) \vee d \\ &= ((a \wedge e) \wedge (b \vee d)) \vee d = (a \wedge (b \vee c) \wedge (b \vee (a \wedge c))) \vee d \\ &\overset{(M)}{=} (a \wedge (b \vee ((b \vee c) \wedge (a \wedge c)))) \vee d = (a \wedge (b \vee (a \wedge c))) \vee d \\ &\overset{(M)}{=} (a \wedge c) \vee (b \wedge a) \vee d = d. \end{aligned}$$

Subsection 4

Complete Lattices, Equivalences, and Algebraic Lattices

Complete Lattices

Definition (Complete Lattice)

A poset P is **complete** if, for every subset A of P, both $\sup A$ and $\inf A$ exist (in P). All complete posets are lattices, and a lattice L which is complete as a poset is a **complete lattice**.

Theorem

Let P be a poset such that $\bigwedge A$ exists for every subset A, or such that $\bigvee A$ exists for every subset A. Then P is a complete lattice.

- Suppose $\bigwedge A$ exists for every $A \subseteq P$. In particular, since $\bigwedge \varnothing = 1$, P has a largest element. We have, by definition of A^u, for all $a \in A$ and all $u \in A^u$, $a \leq u$. Thus, for all $a \in A$, $a \leq \bigwedge A^u$. Hence, $\bigvee A \leq \bigwedge A^u$. But, if u is an upper bound of A, then $u \in A^u$, whence $\bigwedge A^u \leq u$. Therefore, $\bigvee A = \bigwedge A^u$.

  The other half of the theorem is proved similarly.

An Alternative Formulation

- The existence of $\bigwedge\emptyset$ guarantees a largest element in P.
- The existence of $\bigvee\emptyset$ guarantees a smallest element in P.
- So an equivalent formulation of the theorem is:

Corollary

- P is complete if it has a largest element and the inf of every nonempty subset exists.
- P is complete if it has a smallest element and the sup of every nonempty subset exists.

Examples of Complete Lattices

(1) The set $\mathbb{R} \cup \{-\infty, +\infty\}$ of extended reals with the usual ordering is a complete lattice.

(2) The open subsets of a topological space with the ordering $\subseteq$ form a complete lattice.

(3) $\mathrm{Su}(I)$ with the usual ordering $\subseteq$ is a complete lattice.

Complete Sublattices

- A complete lattice may have sublattices which are incomplete:

  Consider the reals as a sublattice of the extended reals.
- It is also possible for a sublattice of a complete lattice to be complete, but the sups and infs of the sublattice not to agree with those of the original lattice:

  Consider the sublattice of the extended reals consisting of those numbers whose absolute value is less than one together with the numbers $-2, +2$.

Definition (Complete Sublattice)

A sublattice L' of a complete lattice L is called a **complete sublattice** of L if for every subset A of L' the elements $\bigvee A$ and $\bigwedge A$, as defined in L, are actually in L'.

Relations and Equivalence Relations

Definition

Let A be a set. Recall that a **binary relation** r on A is a subset of A^2. If $\langle a, b\rangle \in r$, we also write $a\ r\ b$.

- If r_1 and r_2 are binary relations on A, then the **relational product** $r_1 \circ r_2$ is the binary relation on A defined by $\langle a, b\rangle \in r_1 \circ r_2$ iff there is a $c \in A$, such that $\langle a, c\rangle \in r_1$ and $\langle c, b\rangle \in r_2$. Inductively, one defines $r_1 \circ r_2 \circ \cdots \circ r_n = (r_1 \circ r_2 \circ \cdots \circ r_{n-1}) \circ r_n$.
- The **inverse** of r is given by $r^{\vee} = \{\langle a, b\rangle \in A^2 : \langle b, a\rangle \in r\}$.
- The **diagonal relation** Δ_A on A is the set $\{\langle a, a\rangle : a \in A\}$.
- The **all** or **nabla relation** A^2 is denoted by ∇_A.
- A relation r on A is an **equivalence relation** if, for any a, b, c from A:
  - E1 $a\ r\ a$ (**reflexivity**)
  - E2 $a\ r\ b$ implies $b\ r\ a$ (**symmetry**)
  - E3 $a\ r\ b$ and $b\ r\ c$ imply $a\ r\ c$ (**transitivity**)

  Eq(A) is the set of all equivalence relations on A.

Lattice Structure of Eq(A)

Theorem

The poset Eq(A), with $\subseteq$ as the partial ordering, is a complete lattice.

- Note that Eq(A) is closed under arbitrary intersections.
- For θ_1 and θ_2 in Eq(A) it is clear that $\theta_1 \wedge \theta_2 = \theta_1 \cap \theta_2$.

Theorem

If θ_1 and θ_2 are two equivalence relations on A, then

$$\theta_1 \vee \theta_2 = \theta_1 \cup (\theta_1 \circ \theta_2) \cup (\theta_1 \circ \theta_2 \circ \theta_1) \cup (\theta_1 \circ \theta_2 \circ \theta_1 \circ \theta_2) \cup \cdots,$$

or, equivalently, $\langle a, b \rangle \in \theta_1 \vee \theta_2$ iff, there is a sequence of elements $c_1, c_2, \ldots, c_n$ from A, such that

$$\langle c_i, c_{i+1} \rangle \in \theta_1 \quad \text{or} \quad \langle c_i, c_{i+1} \rangle \in \theta_2,$$

for $i = 1, \ldots, n-1$, and $a = c_1, b = c_n$.

- Verify that the condition of the right-hand side of the above equation defines an equivalence relation. Each of the relational products in parentheses is contained in $\theta_1 \vee \theta_2$.

Infinite Meets and Joins and Equivalence Classes

- If $\{\theta_i\}_{i\in I}$ is a subset of $\mathrm{Eq}(A)$, then $\bigwedge_{i\in I}\theta_i$ is just $\bigcap_{i\in I}\theta_i$.

Theorem

If $\theta_i \in \mathrm{Eq}(A)$, for $i \in I$, then

$$\bigvee_{i\in I}\theta_i = \bigcup\{\theta_{i_0}\circ\theta_{i_1}\circ\cdots\circ\theta_{i_k} : i_0,\ldots,i_k \in I, k<\infty\}.$$

Definition (Equivalence Class)

Let θ be a member of $\mathrm{Eq}(A)$. For $a \in A$, the **equivalence class** (or **coset**) **of** a **modulo** θ is the set $a/\theta = \{b \in A : \langle b,a\rangle \in \theta\}$. The set $\{a/\theta : a \in A\}$ is denoted by A/θ.

Theorem

For $\theta \in \mathrm{Eq}(A)$ and $a,b \in A$ we have:

(a) $A = \bigcup_{a\in A} a/\theta$.

(b) $a/\theta \neq b/\theta$ implies $a/\theta \cap b/\theta = \varnothing$.

Partitions and Equivalence Relations

Definition (Partition)

A **partition** π of a set A is a family of nonempty pairwise disjoint subsets of A, such that $A = \bigcup \pi$. The sets in π are called the **blocks** of π. The set of all partitions of A is denoted by $\Pi(A)$.

- For π in $\Pi(A)$, let us define an equivalence relation $\theta(\pi)$ by

$$\theta(\pi) = \{\langle a, b\rangle \in A^2 : \{a, b\} \subseteq B, \text{ for some } B \text{ in } \pi\}.$$

- The mapping $\pi \mapsto \theta(\pi)$ is a bijection between $\Pi(A)$ and $\mathrm{Eq}(A)$.
- Define a relation $\leq$ on $\Pi(A)$ by $\pi_1 \leq \pi_2$ iff each block of π_1 is contained in some block of π_2.

Theorem

With the above ordering $\Pi(A)$ is a complete lattice, and it is isomorphic to the lattice $\mathrm{Eq}(A)$ under the mapping $\pi \mapsto \theta(\pi)$.

- The lattice $\Pi(A)$ is called the **lattice of partitions** of A.

Algebraic Lattices

Definition (Algebraic Lattice)

Let L be a lattice. An element a in L is **compact** iff whenever $\bigvee A$ exists and $a \leq \bigvee A$, for $A \subseteq L$, then $a \leq \bigvee B$, for some finite $B \subseteq A$. L is **compactly generated** iff every element in L is a sup of compact elements. A lattice L is **algebraic** if it is complete and compactly generated.

Examples:

(1) The lattice of subsets of a set is an algebraic lattice (where the compact elements are finite sets).
(2) The lattice of subgroups of a group is an algebraic lattice (in which "compact" = "finitely generated").
(3) Finite lattices are algebraic lattices.
(4) The subset $[0,1]$ of the real line is a complete lattice, but it is not algebraic.
(5) We will also see that *lattices of subuniverses of algebras* and *lattices of congruences on algebras* are algebraic.

Subsection 5

Closure Operators

Closure Operators

Definition (Closure Operator)

If we are given a set A, a mapping $C : \mathrm{Su}(A) \to \mathrm{Su}(A)$ is called a **closure operator** on A if, for $X, Y \subseteq A$, it satisfies:

- C1 $X \subseteq C(X)$ (**extensive**)
- C2 $C^2(X) = C(X)$ (**idempotent**)
- C3 $X \subseteq Y$ implies $C(X) \subseteq C(Y)$ (**isotone**)

A subset X of A is called a **closed subset** if $C(X) = X$. The poset of closed subsets of A, with set inclusion as the partial ordering, is denoted by L_C.

Complete Lattice Structure of L_C

Theorem

Let C be a closure operator on a set A. Then L_C is a complete lattice with

$$\bigwedge_{i\in I} C(A_i) = \bigcap_{i\in I} C(A_i) \quad \text{and} \quad \bigvee_{i\in I} C(A_i) = C(\bigcup_{i\in I} A_i).$$

- Let $(A_i)_{i\in I}$ be an indexed family of closed subsets of A. We have $\bigcap_{i\in I} A_i \subseteq A_i$, for each i. Hence, $C(\bigcap_{i\in I} A_i) \subseteq C(A_i) = A_i$. So $C(\bigcap_{i\in I} A_i) \subseteq \bigcap_{i\in I} A_i$. Since C is extensive, $C(\bigcap_{i\in I} A_i) = \bigcap_{i\in I} A_i$. We conclude $\bigcap_{i\in I} A_i$ is in L_C.
  Since $A = C(A)$ is itself in L_C, L_C is a complete lattice.
  - $\bigcap_{i\in I} C(A_i) \subseteq C(A_i)$, for all i. So $\bigcap_{i\in I} C(A_i) \subseteq \bigwedge_{i\in I} C(A_i)$. If $B \in L_C$ is such that $B \subseteq C(A_i)$, for all i, then $B \subseteq \bigcap_{i\in I} C(A_i)$. Hence $\bigwedge_{i\in I} C(A_i) = \bigcap_{i\in I} C(A_i)$.
  - $C(A_i) \subseteq C(\bigcup_{i\in I} A_I)$, for all i. Hence, $\bigvee_{i\in I} C(A_i) \subseteq C(\bigcup_{i\in I} A_i)$. If $C(A_i) \subseteq B \in L_C$, for all i, then $A_i \subseteq B$, for all i, whence $\bigcup_{i\in I} A_i \subseteq B$. Thus, $C(\bigcup_{i\in I} A_i) \subseteq C(B) = B$. So $\bigvee_{i\in I} C(A_i) = C(\bigcup_{i\in I} A_i)$.

Complete Lattices and Lattices of Closed Sets

Theorem

Every complete lattice is isomorphic to the lattice of closed subsets of some set A with a closure operator C.

- Let L be a complete lattice. For $X \subseteq L$ define

$$C(X) = \{a \in L : a \leq \sup X\}.$$

Then C is a closure operator on L:

  - $X \subseteq \{a \in L : a \leq \sup X\} = C(X)$;
  - If $X \subseteq Y$, $C(X) = \{a \in L : a \leq \sup X\} \subseteq \{a \in L : a \leq \sup Y\} = C(Y)$.
  - If $a \in C(C(X))$, then $a \leq \sup C(X) = \sup \{a \in L : a \leq \sup X\} \leq \sup X$. Hence, $a \in C(X)$.

The mapping

$$a \mapsto \{b \in L : b \leq a\}$$

gives the desired isomorphism between L and L_C.

Algebraic Closure Operators

Definition (Algebraic Closure Operator)

A closure operator C on the set A is an **algebraic closure operator** if, for every $X \subseteq A$,

C4 $C(X) = \bigcup\{C(Y) : Y \subseteq X \text{ and } Y \text{ is finite}\}$.

- Note that C1, C2, C4 imply C3.

Theorem

If C is an algebraic closure operator on a set A then L_C is an algebraic lattice. The compact elements of L_C are precisely the closed sets $C(X)$, where X is a finite subset of A.

- First we show that $C(X)$ is compact iff X is finite.
  Then by (C4), we have $C(X) = \bigcup\{C(Y) : Y \subseteq X,\ Y \text{ finite}\} = C(\bigcup\{C(Y) : Y \subseteq X,\ Y \text{ finite}\}) = \bigvee\{C(Y) : Y \subseteq X,\ Y \text{ finite}\}$.
  Thus, L_C is algebraic.

Algebraic Closure Operators (Cont'd)

- Suppose $X = \{a_1, \ldots, a_k\}$ and $C(X) \subseteq \bigvee_{i \in I} C(A_i) = C(\bigcup_{i \in I} A_i)$. For each $a_j \in X$, we have a finite $X_j \subseteq \bigcup_{i \in I} A_i$, with $a_j \in C(X_j)$. There are finitely many A_i's, say $A_{j1}, \ldots, A_{jn_j}$, such that $X_j \subseteq A_{j1} \cup \cdots \cup A_{jn_j}$, Hence, $a_j \in C(A_{j1} \cup \cdots \cup A_{jn_j})$. But then $X \subseteq \bigcup_{1 \le j \le k} C(A_{j1} \cup \cdots \cup A_{jn_j})$, so $X \subseteq C(\bigcup_{\substack{1 \le j \le k \\ 1 \le i \le n_j}} A_{ji})$. Hence,

$$C(X) \subseteq C(\bigcup_{\substack{1 \le j \le k \\ 1 \le i \le n_j}} A_{ji}) = \bigvee_{\substack{1 \le j \le k \\ 1 \le i \le n_j}} C(A_{ji}).$$

  So $C(X)$ is compact.

  Now suppose $C(Y)$ is not equal to $C(X)$ for any finite X. From $C(Y) \subseteq \bigcup\{C(X) : X \subseteq Y \text{ and } X \text{ finite}\}$, it is easy to see that $C(Y)$ cannot be contained in any finite union of the $C(X)$'s. Hence $C(Y)$ is not compact.

Generating Sets

Definition (Generating Set)

If C is a closure operator on A and Y is a closed subset of A, then we say a set X is a **generating set** for Y if $C(X) = Y$.
The set Y is **finitely generated** if there is a finite generating set for Y.
The set X is a **minimal generating set** for Y if X generates Y and no proper subset of X generates Y.

Corollary

Let C be an algebraic closure operator on A. Then the finitely generated subsets of A are precisely the compact elements of L_C.

Algebraic Lattices and Algebraic Closure Operators

Theorem

Every algebraic lattice is isomorphic to the lattice of closed subsets of some set A with an algebraic closure operator C.

- Let L be an algebraic lattice, and let A be the subset of compact elements. For $X \subseteq A$, define

$$C(X) = \{a \in A : a \leq \bigvee X\}.$$

C is a closure operator. Moreover, for all $X \subseteq L$, $C(X) = \{a \in A : a \leq \bigvee X\} = \{a \in A : a \leq \bigvee Y : Y \subseteq X,\ Y \text{ finite}\} = \bigcup\{C(Y) : Y \subseteq X,\ Y \text{ finite}\}$. So C is algebraic. The map

$$a \mapsto \{b \in A : b \leq a\}$$

gives the desired isomorphism as L is compactly generated.