

GENERAL THEORY OF ALGEBRAS

DON PIGOZZI

1. LATTICES

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

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

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

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

| a | b | $a \vee b$ | $a \wedge b$ |
|--------------|--------------|--------------|--------------|
| \mathbf{T} | \mathbf{T} | \mathbf{T} | \mathbf{T} |
| \mathbf{T} | \mathbf{F} | \mathbf{T} | \mathbf{F} |
| \mathbf{F} | \mathbf{T} | \mathbf{T} | \mathbf{F} |
| \mathbf{F} | \mathbf{F} | \mathbf{F} | \mathbf{F} |

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

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

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

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

Date: first week.

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

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

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

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

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

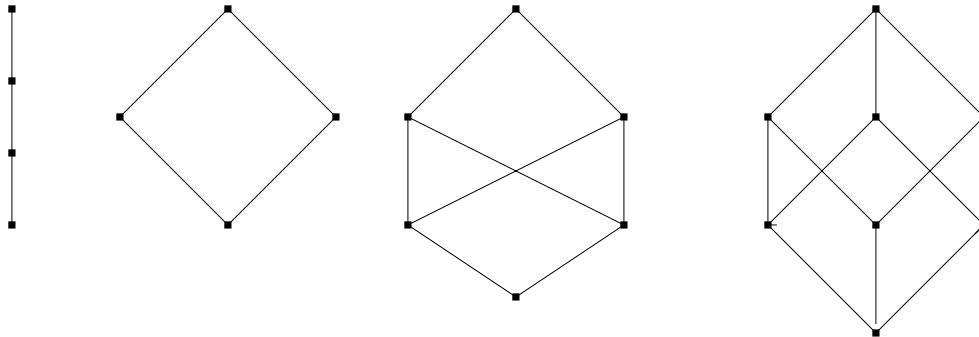
- (P1) $x \leq x$ (*reflexive law*)
 (P2) $x \leq y$ and $y \leq z$ implies $x \leq z$ (*transitive law*)
 (P3) $x \leq y$ and $y \leq x$ implies $x = y$. (*antisymmetric law*)

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

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

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

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



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

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

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

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

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

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

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

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

(L2). We must show that

$$(1) \quad \text{LUB}(a, \text{LUB}(b, c)) = \text{LUB}(\text{LUB}(a, b), c).$$

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

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

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

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

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

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

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

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

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

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

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

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

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

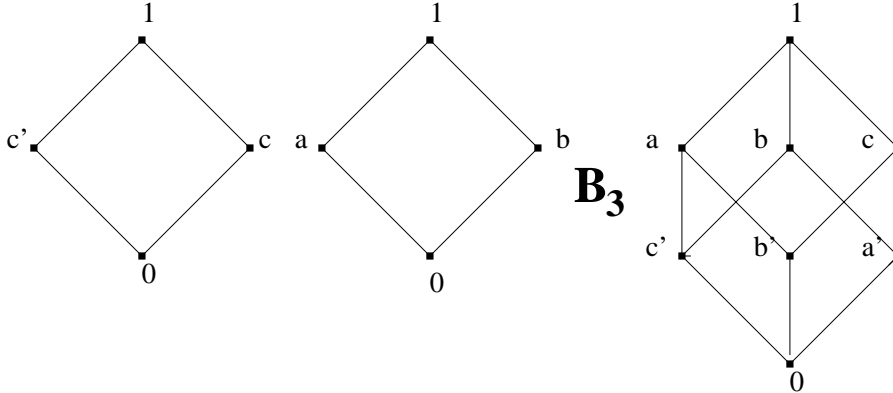
A mapping h is (*strictly*) *order-preserving map* between two lattices if it (strictly) preserves that lattice orderings.

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

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

\impliedby : Exercise. □

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



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

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

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

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

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

$$(D1) \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),$$

$$(D2) \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

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

Also, in every lattice \mathbf{A} , the following inidentities hold

$$(2) \quad x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z),$$

$$(3) \quad x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z).$$

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

Proof. (D1) \implies (D2).

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

The proof of (D1) \implies (D2) is obtained from the above by interchanging “ \vee ” and “ \wedge ”.

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

$$(4) \quad (x \wedge y) \vee (x \wedge z) \leq x.$$

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

$$(5) \quad (x \wedge y) \vee (x \wedge z) \leq y \vee z.$$

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

The proof of (3) is obtained by interchanging “ \vee ” and “ \wedge ” and “ \leq ” and “ \geq ”. \square

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

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

DEPARTMENT OF MATHEMATICS, IOWA STATE UNIVERSITY, AMES, IA 50011, USA
E-mail address: dpigozzi@iastate.edu