INTRODUCTION TO ALGEBRA — HANDOUT 4

1. General algebraic structures

Definition 1. An n**-ary operation** on A is a function from A^n to A. 0-ary operations are called **constants**. 1-ary operations are called **unary operations**. 2-ary operations are called **binary operations**.

Example 1. $+$ and $\cdot$ are binary operations on $\mathbb{R}$. Multiplicative inverse is a unary operation on $\mathbb{R}^+$.

Definition 2. A $\langle A, f_1, \ldots, f_n, R_1, \ldots, R_m\rangle$ is a **structure** if A is a set and f_1, $\ldots$, f_n are operations and R_1, $\ldots$, R_m are relations.

Definition 3. An $\langle A, f_1, \ldots, f_n\rangle$ is an **algebraic structure** if A is a set and f_1, $\ldots$, f_n are operations.

Example 2. A partially ordered $\langle X \leq\rangle$ set and $\langle \mathbb{R}, \cdot, +, 0, 1, \leq\rangle$ are a structures, but not algebraic structures. $\langle \mathbb{R}, \cdot\rangle$, $\langle \mathbb{Z}, \cdot, +\rangle$, $\langle \mathbb{Q}, \cdot, +, 0, 1\rangle$, $\langle P(A), \cap, \cup\rangle$ are algebraic structures.

Definition 4. Structures $\langle A, f_1, \ldots, f_n, R_1, \ldots, R_m\rangle$ and $\langle B, g_1, \ldots, g_n, S_1, \ldots, S_m\rangle$ are **isomorphic** if there is a bijection $h : A \to B$ such that $h\big(f_i(x, y, \ldots)\big) = g_i\big(h(x), h(y), \ldots\big)$ for all $1 \leq i \leq n$ and $R_j(h(x), h(y), \ldots)$ holds iff $S_j(x, y, \ldots)$ holds for all $1 \leq j \leq m$.

Definition 5. Structure $\langle A, f_1, \ldots, f_n, R_1, \ldots, R_m\rangle$ is a **substructure** of structure $\langle B, g_1, \ldots, g_n, S_1, \ldots, S_m\rangle$ if $A \subseteq B$ and $f_i(x, y, \ldots) = g_i(x, y, \ldots)$ and $R_j(x, y, \ldots)$ holds iff $S_j(x, y, \ldots)$ holds for all $x, y, \ldots \in A$.

2. Latices

Definition 6. Algebraic structure $\langle L, \wedge, \vee\rangle$ is **lattice** if $\wedge$ and $\vee$ are binary operations satisfying the following identities:

$$
\begin{aligned}
a \vee a &= a && \text{(idempotence of } \vee\text{)}\\
a \wedge a &= a && \text{(idempotence of } \wedge\text{)}\\
a \vee b &= b \vee a && \text{(commutativity of } \vee\text{)}\\
a \wedge b &= b \wedge a && \text{(commutativity of } \wedge\text{)}\\
(a \vee b) \vee c &= a \vee (b \vee c) && \text{(associativity of } \vee\text{)}\\
(a \wedge b) \wedge c &= a \wedge (b \wedge c) && \text{(associativity of } \wedge\text{)}\\
a \vee (b \wedge a) &= a && \text{(absorption)}\\
a \wedge (b \vee a) &= a && \text{(absorption)}
\end{aligned}
$$

Theorem 1. The theory of lattices in the language $\{\wedge, \vee\}$ is definitionally equivalent to the theory of lattices in the language $\{\leq\}$.

TABLE 1.

Lattice as algebraic structures	Lattices as posets
$a \vee a = a$ and $a \wedge a = a$	$a \leq a$
$a \vee b = b \vee a$ and $a \wedge b = b \wedge a$	$a \leq b \leq c \to a \leq c$
$(a \vee b) \vee c = a \vee (b \vee c)$	$a \leq b \leq a \to a = b$
$(a \wedge b) \wedge c = a \wedge (b \wedge c)$	$\exists s\big(a, b \leq s \;\&\; \forall c[a, b \leq c \to s \leq c]\big)$
$a \vee (b \wedge a) = a$	$\exists i\big(i \leq a, b \;\&\; \forall c[c \leq a, b \to c \leq i]\big)$
$a \wedge (b \vee a) = a$	
$a \leq b \overset{def}{\Longleftrightarrow} a \wedge b = a$	$a \vee b := sup(a, b)$
	$a \wedge b := inf(a, b)$

Proof. We have to prove that the two theory of lattices have a common definitional extension. We will show that the two theories (together with the explicit definitions) in Table 1 have the same models.

Let $\langle L, \wedge, \vee\rangle$ be a lattice. Let $a \leq b \overset{def}{\Longleftrightarrow} a \wedge b = a$. We have to show that $\langle L, \wedge, \vee, \leq\rangle$ satisfies the axioms and the definitions in the right hand side of Table 1.
REFLEXIVITY: $a \leq a$ since $a \wedge a = a$.
TRANSITIVITY: Let $a \leq b$ and $b \leq c$, i.e., $a \wedge b = a$ and $b \wedge c = b$. Then $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$, i.e., $a \leq c$.
ANTI-SYMMETRY: Let $a \leq b$ and $b \leq a$, i.e., $a \wedge b = a$ and $b \wedge a = b$. Then $a = b$ since $a \wedge b = b \wedge a$.
$a \wedge b$ IS THE INFIMUM OF a AND b: $a \wedge b$ is a lower bound of a and b since $a \wedge (a \wedge b) = a$ by associativity and idempotence, i.e., $a \wedge b \leq a$. Similarly, $a \wedge b \leq b$. Let c be a lower bound of a and b, i.e., $c \wedge a = c$ and $c \wedge b = c$. Than $c \wedge (a \wedge b) = (c \wedge a) \wedge b = c \wedge b = c$, i.e., $c \leq a \wedge b$.
$a \vee b$ IS THE SUPREMUM OF a AND b: $a \vee b$ is an upper bound of a and b since $a \wedge (a \vee b) = a$ by absorption (and commutativity), i.e., $a \leq a \vee b$. Similarly, $b \leq a \vee b$. Let c be an upper bound of a and b, i.e., $a \wedge c = a$ and $b \wedge c = b$. We have to show that $(a \vee b) \wedge c = a \vee b$. To prove this, let us note that $a \wedge b = a$ iff $a \vee b = b$ since $a = (a \vee b) \wedge a$ and $b = (b \wedge a) \vee b$. Therefore, it is enough to show that $(a \vee b) \vee c = c$, which holds since $(a \vee b) \vee c = a \vee (b \vee c)) = a \vee c = c$.

Let $\langle L, \leq\rangle$ be a lattice. Let $a \vee b := sup(a, b)$ and $a \wedge b := inf(a, b)$. We have to show that $\langle L, \wedge, \vee, \leq\rangle$ satisfies the axioms and the definitions in the left hand side of Table 1.
IDEMPOTENCE: $a \vee a = a$ and $a \wedge a = a$ since $sup(a, a) = a$ and $inf(a, a)$.
COMMUTATIVITY: $a \vee b = b \vee a$ and $a \wedge b = b \wedge a$ since $sup(a, b) = sup(b, a)$ and $inf(a, b) = inf(b, a)$.
ASSOCIATIVITY: To prove $(a \vee b) \vee c = a \vee (b \vee c)$, we have to show that

$$sup(sup(a, b), c) = sup(a, sup(b, c)).$$

By symmetry, it is enough to show that

$$sup(sup(a, b), c) \leq sup(a, sup(b, c)).$$

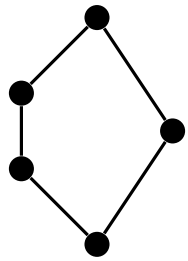

FIGURE 1. The smallest non-modular lattice: N5.

$b, c \leq sup(b, c)$, $sup(a, b) \leq sup(a, sup(b, c))$. Therefore,

$$sup(sup(a, b), c) \leq sup(a, sup(b, c))$$

since $sup(sup(a, b), c)$ is the least upper bound of $sup(a, b)$ and c.
Similarly, $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
ABSORPTION: $a \vee (b \wedge a) = a$ since $sup(a, inf(b, a)) \geq a$ and $a, inf(b, a) \leq a$ (hence $sup(a, inf(b, a)) \leq a$). Similarly, $a \wedge (b \vee a) = a$.
DEFINITION OF ORDER: We have to show that $a \leq b$ iff $inf(a, b) = a$. If $a \leq b$, then clearly $inf(a, b) = a$. If $inf(a, b) = a$, then $a \leq a, b$. □

Proposition 1. In every lattice,

$$a \leq b \Rightarrow a \vee (x \wedge b) \leq b \wedge (x \vee a)$$

Proof. $a \leq b$ and $a \leq x \vee a$. Hence $a \leq b \wedge (x \vee a)$. $x \wedge b \leq b$ and $x \wedge b \leq x \leq x \vee a$. Thus $x \wedge b \leq b \wedge (x \vee a)$. Consequently, $a \vee (x \wedge b) \leq b \wedge (x \vee a)$. □

Definition 7. A lattice is **modular** iff

$$a \leq b \Rightarrow a \vee (x \wedge b) = b \wedge (x \vee a)$$

holds in it.

Theorem 2. A lattice is modular iff contains no sublattice isomorphic to $N5$.

Definition 8. A lattice is **distributive** iff

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

holds in it.

Proposition 2. Identity $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ holds in every distributive lattice.

Proof. Duality. □

Proposition 3. Every distributive lattice is modular.

Proof. Let $a \leq b$. By distributivity, $a \vee (x \wedge b) = (a \vee x) \wedge (a \vee b) = (a \vee x) \wedge b$. □

Theorem 3. A lattice is distributive iff contains no sublattice isomorphic to $N5$ or $M3$.

Definition 9. A lattice is called **bounded** if there are elements 0 and 1 such that $0 \leq x \leq 1$.

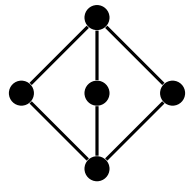

FIGURE 2. Another non-distributive lattice: M3.

Definition 10. A **complemented lattice** is a bounded lattice in which every element a has a complement a' such that $a \wedge a' = 0$ and $a \vee a' = 1$.

Example 3. In N5 and M3 are complemented lattices, but some elements have more than one complements.

Proposition 4. In a bounded distributive lattice, every element has at most one complement.

Exercise 1. Prove Proposition 4.

Definition 11. A complemented lattice is called **uniquely complemented** if every element has at most one complement.

Theorem 4 (Dilworht, 1945)**.** Every lattice can be embedded into an uniquely complemented lattice.

3. Boolean algebras

Definition 12. A **Boolean algebra** is a distributive complemented lattice.

Definition 13. By Proposition 4, Boolean algebras are uniquely complemented. Let $\overline{a}$ denote the unique **complement** of a.

Proposition 5. In any Boolean algebra, $\overline{0} = 1$, $\overline{1} = 0$, $\overline{\overline{x}} = x$, $\overline{x \wedge y} = \overline{x} \vee \overline{y}$ and $\overline{x \vee y} = \overline{x} \wedge \overline{y}$.

Definition 14. a is an **atom** if $a \neq 0$ and there is no element x such that $0 < x < a$. A Boolean algebra is called **atomless** if it contains no atoms.

Exercise 2. Prove that every two countably infinite atomless Boolean algebras are isomorphic.