Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

November 28, 2006

TALK SLOWLY AND WRITE NEATLY!!

0.1 Partial Ordered Sets And Lattices

Today we begin the study of lattices and boolean algebra.

Definition of Partially Ordered Set

Definition 0.1.0.1. The most basic concept we will use for this week is that of a partially ordered set. A partially ordered set is a pair $(P, \leq)$ were

- P is a set, $\leq \subseteq P \times P$.

$$(\forall x \in P) x \leq x \qquad \text{(Reflexivity)}$$

$$(\forall x, y \in P) x \leq y \text{ and } y \leq x \rightarrow x = y \qquad \text{(Anti-Symmetry)}$$

$$(\forall x, y, z \in P) x \leq y \text{ and } y \leq z \rightarrow x \leq z. \qquad \text{(Transitivity)}$$

If $a \geq b$ and $a \neq b$ then we write $a > b$.

We say P is Totally Ordered if $(\forall a, b \in P) a \leq b \vee b \leq a$.

DRAW FINITE EXAMPLES WITH ARROW

Definition of Lattice

Definition 0.1.0.2. A lattice is a partially ordered set in which any two elements have a least upper bound and a greatest lower bound. We denote the least upper bound of a, b by $a \vee b$ and we denote the greatest lower bound by $a \wedge b$.

By induction it isn't hard to show that any finite collection of elements has a least upper bound and a greatest lower bound.

Definition of Complete Lattice

Definition 0.1.0.3. A lattice is Complete if given any set of element, there is a a least upper bound and a greatest lower bound. We denote the greatest lower bound of a st A by $\bigwedge A$ and the least upper bound of set A by

$\bigvee A$.

Examples Some examples of latices are

- For any set S, $P(S)$ is a complete lattice with $1 = S$ and $0 = \emptyset$.
- The set of subgroups of a group G ordered by inclusion.

Theorem 0.1.0.4. *A partially ordered set with a greatest element 1 such that every non-vacuous subset $\{a_\alpha\}$ has a greatest lower bound is a complete lattice. Dually a partially ordered set with a least element 0 such that every non-vacuous subset has a least upper bound is a complete lattice.*

Proof. Assuming the first set of hypothesis we have to show that any $A = \{a_\alpha : \alpha \in I\}$ has a sup. Since $1 \geq a_\alpha$ the set B of upper bounds of A is non-vacuous. Let $b = inf(B)$. The it is clear that $b = sup(A)$.

The second statement follows by symmetry. □

It will be useful to express the rules governing $\vee, \wedge$ explicitly.

Definition of Lattice in $\vee, \wedge$

Definition 0.1.0.5.

- $a \vee b = b \vee a, \;\; a \wedge b = b \wedge a$
- $(a \vee b) \vee c = a \vee (b \vee c), \;\; (a \wedge b) \wedge c = a \wedge (b \wedge c)$
- $a \vee a = a \;\; a \wedge a = a$
- $(a \vee b) \wedge a = a \;\; (a \wedge b) \vee a = a$

Notice that we each of these is symmetric with regards to $\vee, \wedge$. This leads to the following.

Principle of Duality

Theorem 0.1.0.6 (Principle of Duality)**.** *If S is a statement provable from the axioms for a lattice, and S' is the same statement with all $\vee$'s replaced by $\wedge$'s* *and vice versa then S' is provable form the axioms as well.*

Proof. Because all the axioms are symmetric. $\square$

Definition of $\leq$

Lemma 0.1.0.7. *In a lattice $a \vee b = a$ and $a \wedge b = b$ are equivalent. We say if either of these hold that $a \geq b$.*

Proof. If $a \vee b = a$ then $b = (a \vee b) \wedge b = a \wedge b$. The other direction is by the duality principle. $\square$

Lemma 0.1.0.8. *If $\langle L, \wedge, \vee \rangle$ is a lattice and $a \leq b \leftrightarrow a \wedge b = a$ then $a \wedge b$ is the greatest lower bound of a, b and $a \vee b$ is the least upper bound of a, b.*

Proof. Immediate. $\square$

Lattice isomorphism

Theorem 0.1.0.9. *A bijective map $f : L \to L'$ of latices is a lattice isomorphism if and only if both f and f^{-1} are order preserving.*

Proof. It is clear that if $a \to a'$ is the lattice isomorphism then this map is order preserving. It is also clear that the inverse map is also a lattice isomorphism and hence order preserving.

Conversely suppose $a \to a'$ is bijective and it and its inverse are order preserving. This means that $a \geq b$ in L if and only if $a' \geq b'$ in L'

Let $d = a \vee b$. Then $d \geq a, b$ so $d' \geq a', b'$. Let $e' \geq a', b'$ and let e be the inverse image of e. Then $e \geq a, b$. Hence $e \geq d$ and so $e' \geq d'$. Thus $d' = a' \vee b'$. In a similar way we show that $(a \wedge b)' = a' \wedge b'$. □

0.2 Distributivity and Modularity

Definition of Distributive

Definition 0.2.0.10. A lattice is distributive if it satisfies

$$(1) a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

Lemma 0.2.0.11. *If L is a distributive lattice then L satisfies*

$$(2) a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

Proof. We then have

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

□

Corollary 0.2.0.12. *For any lattice* (1) *and* (2) *are equivalent.*

Proof. This is by the duality property. □

Totally ordered sets

Lemma 0.2.0.13. *Every totally ordered set is a distributive lattice.*

Proof. We wish to establish (1) above for any three elements a, b, c. We will have two cases

(1) $a \geq b$, $a \geq c$

We have $a \wedge (b \vee c) = b \vee c$ and $(a \wedge b) \vee (a \wedge c) = b \vee c$.

(ii) $a \leq b$ or $a \leq c$.

We then have $a \wedge (b \vee c) = a$ and $(a \wedge b) \vee (a \wedge c) = a$

We know these are the only two cases because we are in a totally ordered set. □

EXAMPLE Notice that the collection of integers ordered by $a \leq b$ if and only if $a|b$ is a distributive lattice.

Modular lattices

Definition 0.2.0.14. A lattice is called modular if it satisfies the following modularity condition

$$(M)\text{If } a \geq b \text{ then } a \wedge (b \vee c) = b \vee (a \wedge c)$$

Notice that the dual condition is

$$\text{If } a \geq b \text{ then } a \vee (b \wedge c) = b \wedge (a \vee c)$$

which is the same thing as (M) and so modular latices satisfy duality.

Lattice of normal subgroups

Theorem 0.2.0.15. *The lattice of normal subgroups of a group is modular.*

Proof. The normal subgroup generated by two normal subgroups H_1 and H_2 of a group G is $H_1H_2 = H_2H_1$.

Hence we have to prove that if H_1, H_2, H_3 are normal subgroups with $H_1 \supset H_2$ then

$$H_1 \cap (H_2 H_3) = H_2(H_1 \cap H_3)$$

But we know that

$$H_1 \cap (H_2 H_3) \supset H_2(H_1 \cap H_3)$$

and so it is enough to show that

$$H_1 \cap (H_2 H_3) \subset H_2(H_1 \cap H_3)$$

Suppose $a \in H_1 \cap (H_2 H_3)$. Then $a = h_1 = h_2 h_3$ where $h_i \in H_i$. And $h_3 = h_2^{-1} h_1 \in H_1$ (because $H_2 \subset H_1$. Thus $h_3 \in H_1 \cap H_3$ and so $a = h_2 h_3 \in h_2(H_1 \cap H_3)$. This proves the required inclusion. □

Modularity and Cancellation Laws

Theorem 0.2.0.16. *A lattice L is modular if and only if whenever $a \geq b$ and $a \wedge c = b \wedge c$ and $a \vee c = b \vee c$ for some $c \in L$ then $a = b$.*

Proof. Let L be a modular lattice and let $a, b, c \in L$ such that $a \geq b, a \vee c = b \vee c, a \wedge c = b \wedge c$. Then

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

Conversely suppose L is a lattice satisfying the conditions stated in the theorem. Let $a, b, c \in L$ and $a \geq b$. we know that

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

And that

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

and

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

hence

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

Since $b \leq a$ the dual of our first relation is

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

and the dual of the second one is

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

Thus we have

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

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

Hence the assumed property implies that $a \wedge (b \vee c) = b \vee (a \wedge c)$ which is the axiom. $\square$

Intervals

Definition 0.2.0.17. Let L be a lattice and let $a, b \in L$. Then the interval $I[a, b] = \{c \in L : a \leq c \wedge c \leq b\}$.

Equivalence of Intervals

Theorem 0.2.0.18. *If $a, b \in L$ and L is a modular lattice then the maps $x \to x \wedge b$ is an isomorphism of the interval $I[a, a \vee b]$ onto $I[a \wedge b, b]$. The inverse isomorphism is $y \to y \vee a$.*

Proof. We note first that in any lattice the maps $x \to x \vee a$ and $x \to x \wedge a$ are order preserving. for we have $x \geq y$ if and only if $x \vee y = x$ and if and only if $x \wedge y = y$. So $x \vee y = x$ implies $(x \vee a) \vee (y \vee a) = x \vee y) \vee (a \vee a) = (x \vee y) \vee a = x \vee a$. Hence $x \geq y$ implies $x \vee a \geq y \vee a$. Similarly we have $x \wedge a \geq y \wedge a$.

Now if $a \leq x \leq a \vee b$ then $a \wedge b \leq x \wedge b \leq b = (a \vee b) \wedge b$. Also if $a \wedge b \leq y \leq b$ then $a = a \vee (a \wedge b) \leq y \vee a \leq a \vee b$. Hence $x \to x \wedge b$ and $y \to y \vee a$ map $I[a, a \vee b]$ into $I[a \wedge b, b]$ and $I[a \wedge b, b]$ into $I[a, a \vee b]$ respectively.

Since both these maps are order preserving it suffices to show that they are inverses (by previous theorems).

Let $x \in I[a, a \vee b]$. Then since $x \geq a$ by modularity we have

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

and since $x \leq a \vee b$ this gives $(x \wedge b) \vee a = x$. Dually we have that if $y \in I[a \wedge b, b]$ then $(y \vee a) \wedge b = y$. And hence the maps are inverses. $\square$