Commutative Algebra – Lecture 3: Lattices and Categories (Sept. 13, 2013)

Navid Alaei

September 17, 2013

1 Lattice Basics

There are, in general, two equivalent approaches to defining a lattice; one is rather "algebraic" in nature, whereas the other is based on the notion of order. We present both approaches here and then show that they are indeed equivalent.

Definition 1.1 (**Lattice - an "algebraic" approach**)**.** A lattice is a non-empty set L together with two binary operations $\vee$ and $\wedge$ on L satisfying, for each $x, y, z \in L$, the following identities:

1. $x \vee y = y \vee x$ and $x \wedge y = y \wedge x$ (commutativity)
2. $x \vee (y \vee z) = (x \vee y) \vee z$ and $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ (associativity)
3. $x \vee x = x$ and $x \wedge x = x$ (idempotent)
4. $x \wedge (x \vee y) = x$ and $x \vee (x \wedge y) = x$ (absorption)

Example 1.2. *Power set and divisibility:*

- *Let S be a given set and consider $\mathcal{P}(S)$, the power set of S. Then $\mathcal{P}(S)$ forms a lattice under set inclusion, where $\vee$ and $\wedge$ are interpreted as union and intersection respectively.*
- *The set $\mathbb{N}$ of natural numbers forms a lattice under divisibility where $\vee$ and $\wedge$ correspond to the greatest common divisor and the least common divisor functions respectively.*
- *Given a group G, the set of all subgroups of G forms a lattice under set inclusion.*

Next, recall that a *partial oder* on a given set S is a binary relation, usually denoted $\leq$, such that $\leq$ is *reflexive*, *antisymmetric*, and *transitive*. If, in addition, one of $s \leq t$ or $t \leq s$ holds for all $s, t \in S$, then $\leq$ is said to be a *total order* on S.

Definition 1.3 (**Poset**)**.** A poset is any non-empty set P with a partial order defined on it.

Given a poset P and a subset A of P, we say that an element $p \in P$ is an *upper bound* (resp. *lower bound*) for A if $a \leq p$ (resp. $p \leq a$) for each $a \in A$. If, in addition, p has the property that whenever there exists $b \in P$ with $a \leq b$ (resp. $b \leq a$) for each $a \in A$ then $p \leq b$ (resp. $b \leq p$), we call p the *least upper bound/supremum* (resp. *greatest lower bound/infimum*) for A and write $\sup A = p$ (resp. $\inf A = p$). We are now ready to present the second approach to defining a lattice.

Definition 1.4 (**Lattice** - revisited)**.** A poset L is a lattice if and only if for every $a, b \in L$, both $\sup\{a, b\}$ and $\inf\{a, b\}$ exist in L.

We now state, and prove, the equivalence of the two definitions of a lattice mentioned earlier.

Proposition. *If L is a lattice according to (1.1), then define an order $\leq$ on L via the rule $a \leq b$ if and only if $a = a \wedge b$ for all $a, b \in L$. If, on the other hand, L is a lattice defined through (1.4), then define the operations $\vee$ and $\wedge$ via $a \vee b = \sup\{a, b\}$ and $a \wedge b = \inf\{a, b\}$ for each $a, b \in L$.*

Proof. We begin by verifying the first assertion. Suppose L is a lattice defined by (1.1) and let $\leq$ be as in the statement of the proposition. Then the reflexive and antisymmetric properties of $\leq$ follow from the idempotent and commutative laws of (1.1) respectively. Also, if $a \leq b$ and $b \leq c$, for some $a, b, c \in L$, then

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

where the first, second, and third equalities follow from $a \leq b$, $b \leq c$, and associativity law of (1.1) respectively. Hence, $a \leq c$ and $\leq$ is indeed a partial order on L. So it remains to show that $\sup\{a, b\}$ and $\inf\{a, b\}$ exist in L. Indeed, the absorption law of (1.1) applied to a and b tells us that $a \vee b$ is an upper bound for both a and b. Suppose there exists another element $p \in L$ such that $a \leq p$ and $b \leq p$. Then $a = a \wedge p$ and $b = b \wedge p$ so that

$$a \vee p = (a \wedge p) \vee p = p, \qquad \text{and} \qquad b \vee p = (b \wedge p) \vee p = p, \tag{1}$$

where the second equalities both follow from the absorption law of (1.1). Further, the commutativity and associativity of $\vee$ give

$$(a \vee p) \vee (b \vee p) = (a \vee p) \vee (p \vee b) = a \vee (p \vee p) \vee b = (a \vee b) \vee (p \vee p) = (a \vee b) \vee p. \tag{2}$$

Hence, combining (1) and (2) we obtain $(a \vee b) \vee p = p$. But then the absorption law gives

$$(a \vee b) \wedge p = (a \vee b) \wedge [(a \vee b) \vee p] = a \vee b.$$

In other words, $(a \vee b) \leq p$ and so $(a \vee b) = \sup\{a, b\} \in L$, as desired. The existence of infimum follows from a similar argument so we omit the details.
On the other hand, suppose L is defined via definition (1.4). We must verify that sup and inf satisfy the four properties of definition (1.1). Once again, it is sufficient to establish the result for sup. Indeed, $\sup\{x, y\} = \sup\{y, x\}$ and so sup is commutative. The idempotent law is also trivial. The absorption law is also clear since $z = \inf\{x, y\} \leq x$ and $\sup\{x, z\} = x$. Lastly, if $x, y, z \in L$ are any three elements, then note $y \vee z = \sup\{y, z\}$ and $x \vee y = \sup\{x, y\}$ both exist in L as L satisfies definition (1.4). Without loss of generality, suppose $\sup\{y, z\} = y$ and $\sup\{x, y\} = x$. Then

$$\sup\{x, \sup\{y, z\}\} = x = \sup\{\sup\{x, y\}, z\},$$

and so sup is associative. Hence, one can readily see that the two definition are indeed equivalent; i.e., given a lattice according to one of the two definitions, it is possible to construct a lattice according to the other definition (and vice versa) in such a way that the two constructions are inverses of one another. □

Our next task is to introduce the notion of *modularity* of lattices, which we will use to study the lattice of submodules of a given module.

Definition 1.5 (**Lattice Homomorphism**). Let L_1 and L_2 be any two lattices. We say that $\phi : L_1 \to L_2$ is a lattice homomorphism if ϕ preserves the two binary operations $\vee$ and $\wedge$; in other words, given $a, b \in L_1$ we have

$$\phi(a \vee b) = \phi(a) \vee \phi(b), \qquad \text{and} \qquad \phi(a \wedge b) = \phi(a) \wedge \phi(b).$$

Observe that a lattice isomorphism is simply a bijective lattice homomorphism.

Definition 1.6 (**Sublattice**). Given a lattice L and $L' \subseteq L$ non-empty, we say that L' is a sublattice of L, if $(a \vee b), (a \wedge b) \in L'$ whenever $a, b \in L'$.

We say that a lattice L_1 can be *embedded* into a lattice L_2 if there exists a sublattice of L_2 which is isomorphic to L_1.

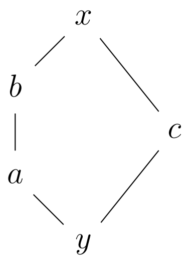
Definition 1.7 (**Modular Lattice**). A lattice L is said to be *modular* (or has the *modularity property*) if the following condition holds:

$$x \vee (y \wedge z) = y \wedge (x \vee z), \qquad \text{whenever} \qquad x \leq y,$$

for each $z \in L$.

We now present one of the most celebrated results in the theory of lattices which is due to Dedekind. The proof is not difficult but is rather tedious and can be found in [1] so we omit the details.

Theorem 1.8 (Dedekind). *A lattice L is non-modular if and only if N_5 can be embedded into L, where N_5 is the following lattice.*



Remark: *Observe that N_5 is in fact non-modular. One readily sees that $a \leq b$ but $a \vee (b \wedge c) = a \vee y = a$ whereas $b \wedge (a \vee c) = b \wedge x = b$.*

We now introduce the lattice of submodules of a module.

Definition 1.9 (Lattice of Submodules). Given a ring R and an R-module M, let $\mathcal{L}_R(M)$ denote the set of R-submodules of M. Then $\mathcal{L}_R(M)$ is a lattice, where $\wedge$ and $\vee$ correspond to the intersection and sum of modules respectively.

This leads to the following important observation. But first, recall the correspondence theorem for modules:

Theorem 1.10 (Correspondence Theorem For Modules). *Let R be a ring and let M be an R-module with K a submodule of M. Then every submodule of M/K is of the form N/K for some submodule N of M containing K. In other words, there is a one-to-one correspondence between the submodules of M/K and the submodules of M that contain K. This correspondence is given via $N/K \mapsto N$.*

Observation: *Using the language of lattices, we see that Theorem (1.10) gives a one-to-one lattice homomorphism $\psi : \mathcal{L}_R(M/K) \to \mathcal{L}(M)$ whose image consists of the lattice of submodules containing K. Since such a homomorphism must respect sums and intersections, we see that*

$$\psi(N_1/K + N_2/K) = \psi(N_1/K) + \psi(N_2/K) = N_1 + N_2,$$

and

$$\psi(N_1/K \cap N_2/K) = \psi(N_1/K) \cap \psi(N_2/K) = N_1 \cap N_2,$$

For any submodules N_1, and N_2 containing K. On the other hand, $(N_1 + N_2)/K \mapsto N_1 + N_2$ and $(N_1 \cap N_2)/K \mapsto N_1 \cap N_2$ by the correspondence theorem; as ψ is injective, we obtain the following:

$$(N_1 + N_2)/K = N_1/K + N_2/K, \qquad \textit{and} \qquad (N_1 \cap N_2)/K = (N_1/K) \cap (N_2/K). \quad (3)$$

The following proposition is of particular importance.

Proposition (Modularity Property For $\mathcal{L}_R(M)$). *If $N_1 \subseteq N_2$ and K are submodules of an R-module M, then*

$$(N_1 + K) \cap N_2 = N_1 + (N_2 \cap K).$$

Proof. For the backward inclusion, note that $N_2 \supseteq N_1$ and $N_2 \supseteq N_2 \cap K$. Further, $(N_1 + K) \supseteq N_1$ and $(N_1 + K) \supseteq (N_2 \cap K)$ both follow from the definition of sum of modules. Hence, the right hand side is clearly contained in the left hand side.
Conversely, let $n_2 = n_1 + k \in N_2 \cap (N_1 + K)$ be given, where $n_1 \in N_1$, $n_2 \in N_2$, and $k \in K$. Then, we may write $k = n_2 - n_1$. But this means $k \in (N_2 \cap K)$ from which we immediately have $n_2 = n_1 + k \in N_1 + (N_2 \cap K)$. This establishes the forward inclusion, and thus, completes the proof. □

We end this section by describing a lattice isomorphism between $\mathcal{L}_R(M)$ and $\mathcal{L}_{R/I}(M)$, where I is an ideal of R. The construction is as follows:

- Given any R/I-module M, turn M into an R-module by defining rm, with $r \in R$ and $m \in M$, to be $(r+I)m$. Note we must have that I annihilates M by definition of R/I.

- Conversely, given an R-module M for which I annihilates M, define the new scalar multiplication $(r + I)m$ to be rm. Observe that this is well-defined. Indeed, if $r + I = r' + I$, for some $r, r' \in R$, then $r - r' \in I$ and so $(r - r')m = 0$ as I annihilates M. Hence, $rm = r'm$ as desired.

It is now straightforward that sending an R-submodule of M to itself by viewing it as an R/I-module (via the above construction) gives a lattice isomorphism between $\mathcal{L}_R(M)$ and $\mathcal{L}_{R/I}(M)$.

2 Categories

We begin with some basic definitions.

Definition 2.1 (**Category**). A *category* $\mathcal{C}$ consists of a collection of *objects*, usually denoted obj $(\mathcal{C})$ (but we shall simply write $\mathcal{C}$ to refer to the objects), together with a set of *morphisms* (or *arrows*) between them. Given any two objects $A, B \in \mathcal{C}$, we write $\mathrm{Hom}_{\mathcal{C}}(A, B)$ to denote the set of morphisms between A and B. When the underlying category is understood, we shall omit the subscript $\mathcal{C}$ and simply write $\mathrm{Hom}(A, B)$. As one would expect, morphisms come equipped with a *composition* rule; given any three objects $A, B, C \in \mathcal{C}$, we have

$$\mathrm{Hom}(B, C) \times \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C),$$

usually denoted $(g, f) \mapsto g \circ f$, where $g : B \to C$ and $f : A \to B$. We further require that this composition rule satisfies the following two rules:

1. *Associativity*: if $f \in \mathrm{Hom}(A, B)$, $g \in \mathrm{Hom}(B, C)$ and $h \in \mathrm{Hom}(C, D)$, then $h \circ (g \circ f) = (h \circ g) \circ f$.

2. For each object $A \in \mathcal{C}$, the set $\mathrm{Hom}(A, A)$ is equipped with a unique *identity morphism*, denoted 1_A (or id_A) such that for any morphisms $f \in \mathrm{Hom}(A, B)$ and $g \in \mathrm{Hom}(B, C)$ we have $\mathrm{id}_B \circ f = f$ and $g \circ \mathrm{id}_B = g$.

Before we give some examples of categories, we have an important/technical remark.

REMARK (**Important Example**): *The most prototypical example of a category that we should keep in mind is the category of sets, denoted* ***Set****, whose objects are the sets and whose morphisms are functions between sets. Note that this definition does not interfere with Russell's paradox, since in our definition of a category we never required the existence of a set of all objects!*

Example 2.2. *The following are all examples of categories.*

- ***Grp*** *is the category whose objects are groups, and whose morphisms are group homomorphisms.*
- ***Vec***$_k$ *is the category whose objects are* k*-vector spaces (*k *is a field), and whose morphisms are linear transformations.*
- ***Ab*** *is the category of abelian groups along with group homomorphisms.*
- ***Ring*** *is the category of rings, where the objects are rings and the morphisms are maps of rings; i.e., maps that respect addition and multiplication, and send the multiplicative identity to itself.*
- ***Mod***$_R$ *is the category of (left)* R*-modules, (where* R *is any ring) whose objects are modules over* R*, and whose morphisms are maps between modules.*
- ***Top*** *is the category of topological spaces along with continuous maps as morphisms.*
- *Given a poset* P *with a relation* $\leq$*, one can think of the tuple* $(P, \leq)$ *as a category whose objects are elements of* P*, and with a single morphism from* x *to* y *if and only if* $y \leq x$ *and no morphism otherwise.*

Next, we have the notion of a *subcategory*.

Definition 2.3 ((Full) Subcategory). A category $\mathcal{D}$ is said to be a *subcategory* of another category $\mathcal{C}$ if all objects of $\mathcal{D}$ are objects of $\mathcal{C}$ and $\mathrm{Hom}_{\mathcal{D}}(A, B) \subseteq \mathrm{Hom}_{\mathcal{C}}(A, B)$ for all objects $A, B \in \mathcal{D}$. If, in addition, $\mathrm{Hom}_{\mathcal{D}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(A, B)$ for all $A, B \in \mathcal{D}$, we call $\mathcal{D}$ a *full subcategory* of $\mathcal{C}$.

NOTE: *Note that the categories that arise in universal algebra are all subcategories of* ***Set*** *whose objects are structures of a given signature with the morphisms being the homomorphisms in that signature.*

From the above examples we see that **Ring** is a subcategory of **Ab** and **Ab** is the full subcategory of **Grp**. Since categories are best understood through studying the morphisms between its objects, we now turn our attention to some properties of morphisms.

Definition 2.4 (Isomorphism). A morphism $f \in \mathrm{Hom}(A, B)$ is said to be an *isomorphism* if there exits a unique morphism $g \in \mathrm{Hom}(B, A)$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$.

Definition 2.5 (Monic/Epic Morphisms). A morphism $f \in \mathrm{Hom}(A, B)$ is called *monic* if for any two *distinct* morphisms $g, h \in \mathrm{Hom}(C, A)$, we have $f \circ g \neq f \circ h$. On the other hand, we say that f is an *epic* morphism if for any two *distinct* $g, h \in \mathrm{Hom}(B, C)$, we have $g \circ f \neq h \circ f$.

The following proposition tells us that in some special cases, our notions of one-to-one and onto coincide with notions of monic and epic.

Proposition. *If $\mathcal{C}$ is a subcategory of **Set**, then any one-to-one map is monic, and any onto map is epic.*

Proof. Suppose $f \in \mathrm{Hom}(A, B)$ is one-to-one and let $g, h \in \mathrm{Hom}(C, A)$ be any two distinct morphisms. Then there exists $c \in C$ such that $g(c) \neq h(c)$. As f is one-to-one, this implies that $f(g(c)) \neq f(h(c))$, and thus $f \circ g \neq f \circ h$; i.e., f is a monic morphism. Similarly, if $f \in \mathrm{Hom}(A, B)$ is onto and $g, h \in \mathrm{Hom}(B, C)$ are distinct, then there exists $b \in B$ such that $g(b) \neq h(b)$. As f is onto, there exists some $a \in A$ such that $f(a) = b$. But then $g(f(a)) \neq h(f(a))$, and so $g \circ f \neq h \circ f$; f is an epic morphism. □

Remark: *It is natural to ask if the converse to the above proposition is also valid. In fact, reversing the above argument gives the converse! But we should keep in mind that we are only working in **Set**; this is in general not true in other categories as the following example shows (see Exercise A2 in [2]).*

Example 2.6. *Consider $\mathbb{Z}, \mathbb{Q} \in$ **Ring**, and let $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$ be the natural inclusion map. Then f is epic, but not onto. Indeed, observe that if $R \in$ **Ring** and $g, h \in Hom(\mathbb{Q}, R)$ satisfy $g \circ f = h \circ f$, then $g(f(n)) = h(f(n))$ for all $n \in \mathbb{Z} \subset \mathbb{Q}$. Now if $r = a/b \in \mathbb{Q}$ is non-zero with $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$, then*

$$g(r) = g\left(ab^{-1}\right) = g(f(a))g(f(b))^{-1} = h(f(a))h(f(b))^{-1} = h(ab^{-1}) = h(r),$$

and thus, $g = h$; in other words, f is epic. However, it is trivial that f is not onto.

Note that the above argument boils down to the fact that any ring homomorphism $\mathbb{Q} \to R$ (R a ring) is determined by its action on $\mathbb{Z} \subset \mathbb{Q}$. Fortunately, the above result is always valid in $\mathbf{Mod}_R$ as we will show next.

Proposition. *In **Mod**$_R$, monic morphisms are one-to-one and epic morphisms are onto.*

Proof. First, suppose $f \in \mathrm{Hom}(M, N)$ is monic for some (left) R-modules M and N. Let $g, h \in \mathrm{Hom}(\ker f, M)$ be defined by $g := 0$ and h the canonical inclusion map. Then $f \circ g = 0$, and $f \circ h = 0$ by definition of $\ker f$. As f is monic, it follows that $g = h = 0$. But $h : \ker f \to M$ and h is injective, so we must have $\ker f = 0$; that is, f

is one-to-one.
On the other hand, if f is epic, let $g, h \in \mathrm{Hom}(N, N/f(M))$ be given by $g := 0$ and h the canonical surjection $N \to N/f(M)$. Again, $g \circ f = 0$ as $g = 0$, and $h \circ f = 0$ by definition of $N/f(M)$. As f is epic we must have $g = h = 0$; in other words, $N/f(M) = 0$ (since h is onto). Hence, $f(M) = N$ and so f is onto. □

References

[1] S. Burris, H.P. Sankappanavar *A course in Universal Algebra*. 2012 (`http://www.math.uwaterloo.ca/~snburris/htdocs/UALG/univ-algebra2012.pdf`).

[2] L.H. Rowen, *Graduate Algebra: Commutative View*, American Mathematical Society, 2006.