Exercises on Stone’s Representation Theorem

Paul VanKoughnett

October 23, 2011

1 Introduction

Stone’s representation theorem is one of the things people point to when they’ve had a few too many drinks and are talking about the ‘duality between topology and algebra.’ I’m not convinced that such a duality exists or that we get anything out of claiming that it does, but this theorem is still worth talking about for two reasons:

• First, it’s a nontrivial example of a mathematical ‘representation theorem,’ which expresses every example of some confusing structure in a uniform and ‘nice’ way. An example from linear algebra is Jordan normal form: every matrix can be written as a conjugation of a very simple matrix in which all information about the matrix’s eigenvalues is easily readable. An example from group theory is the classification theorem of finitely generated abelian groups.
• Second, it’s tremendously fun to prove.

What the theorem does is express a deep relationship between two disparate structures. The first is a type of topological space: namely, the compact, totally disconnected, Hausdorff spaces. You should know what ‘compact’ and ‘Hausdorff’ are; ‘totally disconnected’ means that every point is a connected component (there are no larger connected subsets). Because of this theorem, these are also called Stone spaces.

Exercise 1.1 (Easy). Prove that every totally disconnected space is Hausdorff, so that I’m being really redundant.

We’ve seen several examples of Stone spaces, though we’ve never really focused on them. \(\mathbb{Q} \cap [0, 1]\) is one example; any finite discrete space is another. More generally, any profinite set, or inverse limit of finite sets, is a Stone space, as we saw on the homework. The \(p\)-adic numbers are one example.

The second structure is something called a ‘Boolean algebra.’ You may have heard this phrase before, and with good reason: Boolean algebras formalize the sort of ‘Venn diagram thinking’ one uses in logic. Start with the power set, or set of subsets, of some set \(S\); this is written \(\mathcal{P}(S)\). It is partially ordered under inclusion. Given any two \(A, B \in \mathcal{P}(S)\), we can form their greatest lower bound or meet, and their least upper bound or join; these are just \(A \cap B\) and \(A \cup B\) respectively. There’s also a least element \(\emptyset\) and a greatest element \(S\); finally, there’s a complement operation \(\neg A = S - A\), such that \(A \cup \neg A = S\) and \(A \cap \neg A = \emptyset\).

Definition 1.2. So we define a Boolean algebra to be a partially ordered set \(P\) with the following extra properties:

• There is a least element 0 and a greatest element 1.
• Every \(a, b \in P\) have a meet \(a \wedge b\) such that \(c \leq a \wedge b\) if and only if \(c \leq a\) and \(c \leq b\).
• Likewise, every \(a, b \in P\) have a join \(a \vee b\) such that \(c \geq a \vee b\) if \(c \geq a\) and \(c \geq b\).
• Join distributes over meet and vice versa: we have \(a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)\), and likewise with \(\wedge\) and \(\vee\) switched.
• Every element \(a\) has a complement \(\neg a\) with \(a \wedge \neg a = 0\) and \(a \vee \neg a = 1\).
Instead of starting with the order, we could start with the meet/join structure and derive the order from that. Under this alternative definition, Boolean algebras look more algebraic. In this case, we define a **Boolean algebra** to be a set $P$ with two elements $0, 1$, two binary operations $\land, \lor$, and a unary operation $\neg$ such that

- $\land$ and $\lor$ are associative and commutative and distribute over each other.
- $\land$ and $\lor$ satisfy the **absorption laws** $a \land (a \lor b) = a \lor (a \land b) = a$.
- $a \land \neg a = 0$ and $a \lor \neg a = 1$.

**Exercise 1.3.** Prove that these two definitions are equivalent. Ideally, discover a bunch more useful properties of Boolean algebras, like De Morgan’s Laws, along the way. How can you define the partial order in terms of only $\land$ and $\lor$?

**Definition 1.4.** A **homomorphism of Boolean algebras** is a function $P \rightarrow Q$ between two Boolean algebras such that $f(0) = 0$, $f(1) = 1$, $f(a \land b) = f(a) \land f(b)$, $f(a \lor b) = f(a) \lor f(b)$, and $f(\neg a) = \neg f(a)$. No surprises here. We can use this to define **isomorphisms** and **sub-Boolean-algebras** (domains of injective homomorphisms).

**Exercise 1.5.** Define the only Boolean algebra with two elements (up to isomorphism), $2$. Does this remind you of anything? Is there a set $S$ such that $2 \cong \mathcal{P}(S)$? Prove that there is a unique homomorphism from $2$ to any Boolean algebra. Is there a Boolean algebra $1$ with the dual property (there is a unique homomorphism from any given Boolean algebra to $1$), and is it the power set of some set?

**Exercise 1.6.** Prove that the set of clopen sets of a topological space is a Boolean algebra.

If you feel like noting a mental tongue-twister, note that the set of clopen sets of a topological space is a sub-Boolean-algebra of the power set of its underlying set. Unlike $2$ and $1$, it’s not necessarily isomorphic to any power set, but it’s still ‘concrete’ in that all its elements are sets, meet and join are intersection and union, complement is complement, and so on. Such a Boolean algebra is sometimes called a **field of sets**. This raises a natural question:

**Question 1.7.** Is every Boolean algebra isomorphic to a field of sets?

What Stone proved was a ‘yes’ answer to this question; specifically:

**Theorem 1.8** (Stone’s representation theorem). *Every Boolean algebra is isomorphic to the set of clopen sets of a totally disconnected compact Hausdorff space.*

And now you are about to do the same.

The proof I outline below draws heavily on the exercises of the first chapter of Atiyah and Macdonald’s *Commutative Algebra*, where I first learned it. I recommend this book if you want to learn more about rings.

## 2 Some commutative algebra

The gap between topology and Boolean logic is bridged by commutative algebra. You may have studied this before, in 122, 123, or 55, in which case this will all be review. If you’re new to the subject, it’s more or less the abstract study of the multiplicative structures that crop up in number theory, algebraic geometry, Galois theory, and so on.

**Definition 2.1.** A (commutative, unital) **ring** is a set $A$ with the following structure:

- an associative and commutative addition operation;
- an element $0$ such that $a + 0 = 0 + a = a$ for all $a$;
- for every $a \in A$, an element $-a$ such that $a + (-a) = -a + a = 0$;
• an associative and commutative multiplication operation that distributes over addition (so \(a(b + c) = ab + ac\));

• an element 1 such that \(1a = a1 = a\) for all \(a\).

More succinctly, a ring is an abelian group under addition, and multiplication by any element is a group homomorphism, multiplication by 1 being the identity map. Intuitively, a ring is a structure where it makes sense to talk about addition, multiplication, and subtraction as one does in the integers.

**Example 2.2.** Any field. The integers. The set \({a + b\sqrt{2} : a, b \in \mathbb{Z}}\). The set of rational numbers with odd denominators. The set of polynomials in any number of variables with coefficients in any other ring. The set of power series in any number of variables with coefficients in any other ring. The set of continuous functions from any compact Hausdorff space to \(\mathbb{R}\), where addition and multiplication are done pointwise. Exercise: if any of the above confuses you, prove that it’s a ring.

**Definition 2.3.** A **subring** is a subset of a ring that contains 0 and 1 and is closed under addition and multiplication.

So far, so good. But we also want to take quotients, and the quotient \(A/B\) for \(B\) a subring of \(A\) would set all the elements of \(B\) to zero, including 1, which is bad. (Exercise: why is this bad?) So instead of taking quotients by subrings, we invent another substructure called an ‘ideal.’ In group theory, you can only take quotients by normal subgroups, which are a special kind of subgroup; in ring theory, ideals and subrings are totally different!

**Definition 2.4.** An ideal of a ring \(A\) is a subset \(a\) that is closed under addition and such that if \(x \in a\) and \(r \in A\), then \(rx \in a\). So it’s an additive subgroup and is closed under multiplication by arbitrary elements of \(A\). Given elements \(a, b, c, \ldots\) of \(A\), we can talk about the ideal generated by them, which is just the smallest ideal containing them. We write this \((a, b, c, \ldots)\). Note that \((0) = \{0\}\) and \((1) = A\).

**Exercise 2.5.** The quotient \(A/a\) exists as an abelian group. Prove that it inherits a ring structure from \(A\).

**Definition 2.6.** The **sum** of two ideals of \(A\) is \(a + b = \{x + y : x \in a, y \in b\}\). The **product** of two ideals is defined similarly. The **intersection** of two ideals is their intersection as sets.

**Exercise 2.7.** Prove that all of these are still ideals. Find a ring and two ideals in that ring whose product does not equal their intersection.

**Exercise 2.8.** Prove that a ring is a field iff its only ideals are \((0)\) and \((1)\).

The word ‘ideal’ is shorthand for Dedekind’s term ‘ideal number.’ The idea is that we could talk about number-theoretic ideas like factorization and primeness in more general rings than \(\mathbb{Z}\) by thinking in terms of their ideals rather than their elements.

**Definition 2.9.** An ideal \(p\) is **prime** if whenever a product \(xy\) is in \(p\), then either \(x\) or \(y\) are in \(p\). An ideal \(m\) is **maximal** if the only ideal strictly containing it is \((1)\). ((1) is never allowed to be maximal or prime.)

**Exercise 2.10.** What are the prime ideals of \(\mathbb{Z}\)? Of \(\mathbb{C}\)? Of \(\mathbb{C}[x]\)? Of \(\mathbb{R}[x]\)? What about the maximal ideals?

**Exercise 2.11.** Prove that the ideals (resp. prime ideals, maximal ideals) of the quotient ring \(A/a\) are in bijection with the ideals (resp. prime ideals, maximal ideals) of \(A\) that contain \(a\).

**Exercise 2.12.** What property does \(A/p\) have, for \(p\) prime? What about \(A/m\), for \(m\) maximal? Use this to conclude that all maximal ideals are prime.

**Exercise 2.13.** Prove that every ideal not equal to \((1)\) is contained in some maximal ideal. Thus, a set of elements \(\{x_i\}\) is contained in some prime ideal iff no linear combination of the \(x_i\) is equal to 1.

---

1I don’t know who started the practice of using letters in the Fraktur font to write ideals with, but I have very mixed feelings about it. They’re almost illegible to those who aren’t late-nineteenth-century Germans, and they look really stupid when you write them on a blackboard. On the other hand, they do give you twenty-six new symbols that can only be used for ideals and will never get confused for rings or something.
Definition 2.14. A ring homomorphism \( \phi : A \to B \) is a map such that \( \phi(x + y) = \phi(x) + \phi(y) \), \( \phi(xy) = \phi(x)\phi(y) \), and in particular \( \phi(0) = 0 \) and \( \phi(1) = 1 \). Examples: the inclusion of a subring, the projection to a quotient ring.

Exercise 2.15. Let \( \phi : A \to B \) be a ring homomorphism and let \( p \) be prime in \( B \). Prove that \( \phi^{-1}(p) \) is prime in \( A \). This is called the contraction of \( p \). Give examples to show that (a) the contraction of a maximal ideal need not be maximal, and (b) for \( p \) prime in \( A \), \( B \cdot \phi(p) \) (its expansion) need not be prime in \( B \).

3 The spectrum of a ring

Since prime ideals are preserved by contraction, for every ring homomorphism \( A \to B \) we get a function from the set of primes of \( B \) to the set of primes of \( A \). In fact, there’s a nice way to make these sets into topological spaces such that the contraction function is continuous.

Exercise 3.1. For \( E \) a subset of a ring \( A \), let \( V(E) \) be the set of primes of \( A \) containing \( E \). Show that
1. Every prime is in \( V(0) \) and none is in \( V(1) \).
2. \( V(E) = V((E)) \), where \( (E) \) is the ideal \( E \) generates.
3. \( V(\bigcup_{i \in I} E_i) = \bigcap_{i \in I} V(E_i) \) for any family of subsets \( E_i \) of \( A \).
4. \( V(ab) = V(a) \cup V(b) \).

Definition 3.2. The spectrum of \( A \), or Spec \( A \), is the set of primes of \( A \) with the topology in which the sets \( V(E) \) are the closed sets. The above shows that this is actually a topology.\(^2\)

Exercise 3.3. For \( \phi \) a ring homomorphism \( A \to B \), let \( \phi^* : \text{Spec } B \to \text{Spec } A \) be the map sending every prime to its contraction. Prove that \( \phi^* \) is continuous.

Exercise 3.4. For \( f \in A \), let \( D(f) \) be the set of primes not containing \( f \). Show that the sets \( D(f) \) are a basis for the topology on Spec \( A \). Show that \( D(f) \cap D(g) = D(fg) \).

Exercise 3.5. Describe Spec \( \mathbb{Z} \), Spec \( \mathbb{C} \), Spec \( \mathbb{C}[x] \), Spec \( \mathbb{R}[x] \).

Modern algebraic geometry is built around spectra of rings. Manifolds, the subjects of many important branches of topology, can be thought of as copies of Euclidean space glued together; algebraic geometry studies ‘schemes,’ which are glued together spectra.\(^3\)

Topologically, spectra are very different from a lot of the spaces we’ve seen in class, most of which are in some sense built out of Euclidean space. As we’ll see below, they’re only rarely Hausdorff or even \( T_1 \). The important connectedness condition is no longer connectedness or path-connectedness, but instead irreducibility, the property that every two open sets intersect. The spectra of a large class of rings – the noetherian rings – split up into irreducible components the way spaces split up into connected components or path components. Fortunately, a lot of our old techniques still work, and we can still build some sort of intuition.

Exercise 3.6. For \( \mathfrak{a} \) an ideal of \( A \), show that Spec \( (A/\mathfrak{a}) \approx V(\mathfrak{a}) \) (where \( \approx \) means ‘is homeomorphic to’).

Exercise 3.7. A direct product of two rings, \( A_1 \times A_2 \), is the set of ordered pairs \((a_1, a_2) \) with \( a_1 \in A_1 \) and \( a_2 \in A_2 \), and with ring structure given by \((a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \) and \((a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2) \). Show that Spec \( (A_1 \times A_2) \approx \text{Spec } (A_1) \sqcup \text{Spec } (A_2) \). In fact, show that \( A \) is disconnected iff it is a direct product of two nonzero rings.

\(^2\)Side note: the word ‘spectrum’ has a ton of different and unrelated uses in mathematics. It’s used in analysis to describe a generalized set of eigenvalues, in stable homotopy theory for a certain infinite sequence of spaces, and ‘spectral sequences’ are generalized, three-dimensional exact sequences used in algebraic topology to make calculations. To make matters worse, the phrase ‘ring spectrum’ is also used to mean a spectrum of the stable-homotopy-theory type with a multiplicative structure.

\(^3\)Of course, it’s not quite so simple: something of the ring structure must be added back in, to distinguish rings like \( \mathbb{C} \) and \( \mathbb{R} \) whose spectra are homeomorphic.
Exercise 3.8. Prove that spectra are always $T_0$ (for every two points, one has a neighborhood that doesn’t contain the other), but often not $T_1$ (points are closed). What do the closed points correspond to?

Exercise 3.9. Prove that spectra are always compact, and more generally that the subspace $D(f)$ is always compact for $f \in A$.

Exercise 3.10 (Difficult). Is $D(f)$ homeomorphic to the spectrum of a ring? What ring? (This is something I don’t expect you to be able to figure out on your own. Here’s a hint: we want a ring where no prime ideal contains $f$, meaning that $(f) = (1)$.)

4 Bridging the gap

We are now going to use spectra to connect Boolean algebras and Stone spaces. We could go in either direction, but in some sense it’s easier to start with topology: what rings have spectra equal to Stone spaces? As we saw above, separations of spectra correspond to direct products of rings, so to get total disconnectedness, we would hope for our rings to be direct products ‘as many ways as possible.’ One thing about direct products (that you might have noticed in the course of the previous exercise) is that they have nontrivial idempotents: elements $e$ such that $e^2 = e$ (in this case, the ordered pairs $(0, 1)$ and $(1, 0)$).

Definition 4.1. A Boolean ring is a ring in which every element is idempotent.

Exercise 4.2. Prove that, in a Boolean ring,

1. 2 and 0 are equal;\(^4\)
2. every prime ideal is maximal;
3. every finitely generated ideal can be generated by a single element.

Hence the spectrum of a Boolean ring is $T_1$. What field are the quotients $A/p$ equal to?

Exercise 4.3. Show that in Spec $A$ for $A$ Boolean, the sets $D(f)$ are clopen. Show also that a finite union of $D(f_i)$’s is equal to some $D(g)$, and thus that the sets $D(f)$ are the only clopen sets. (Use compactness!) Conclude by showing that Spec $A$ is a Stone space.

Exercise 4.4. Let $P$ be a Boolean algebra. Show that by defining $a + b = (a \land \neg b) \lor (\neg a \land b)$ and $ab = a \land b$, we get a Boolean ring with the same elements as $P$. Show that this mapping is inverse to the one given in the previous paragraph.

Exercise 4.5. Given a Boolean algebra, embed it as the set of clopen sets of a Stone space, and show this gives a bijection between Stone spaces and Boolean algebras (up to homeomorphism/isomorphism).

Exercise 4.6 (Bonus exercise if you care about or plan to care about category theory). Let $P$ and $Q$ be Boolean algebras and $S(P)$ and $S(Q)$ their associated Stone spaces. Show that Boolean algebra homomorphisms $P \to Q$ are in bijection with continuous maps $S(Q) \to S(P)$. This shows that ‘the category of Boolean algebras and the opposite category of Stone spaces are equivalent’.

Congratulations!

\(^4\)‘But what if it doesn’t have a 2!’ No, shut up, we define 2 as $1 + 1$. 5