Lecture 2

Axiomatic thinking and rings

2.1 Goals

1. Review what it means to think axiomatically, and how this shapes modern mathematical practice.
2. See the definition of "ring."
3. See examples of rings.
4. Get used to proofs utilizing the defining properties of a ring.

2.2 Axioms and proofs

You've already taken a class on proof, so you're probably familiar with axiomatic thinking. But let me remind you what axiomatic thinking is all about.

If you think of mathematics as nothing but a sea of facts and theorems, it becomes impossible to navigate. We would rather identify safe harbors, or at least locations to anchor, so that we may begin our voyages from a concrete, known location.

Such beginning points for any logical system are called axioms. Let me try to give a slightly more precise definition.

Definition 2.2.1 (Informal, but the best we'll do)**.** An *axiom* for a logical system is a statement declared to be true without proof.

Beginning with axioms, we use logical deduction to prove more substantial statements. The most substantial of the statements we prove are often called theorems.

To remember the axioms of a system is to remember home base. We'd like to begin at the simplest places possible, and to understand how we can travel from home base to more exotic places (i.e., how we can from the axioms prove substantial theorems).

Example 2.2.2. Fix three real numbers a, b, c. Here is a sea of facts you probably know about real numbers:

(a) $a + b = b + a$.

(b) $1 \cdot a = a$.

(c) $(-1) \cdot a = -a$.

(d) $a + (-a) = 0$.

(e) $c(a + b) = ca + cb$.

(f) $(a + b)^2 = a^2 + 2ab + b^2$.

(g) $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.

(h) $a - (-b) = a + b$.

(i) If $c \neq 0$ and if $ac = b$, then $a = b/c$.

(j) $-(-a) = a$.

(k) If $a + b = a + c$, then $b = c$.

Which of these should be considered starting points, and which should be considered as facts that we can arrive at from our starting points?

Remark 2.2.3. Because we will not be constructing number systems from scratch, you can think of "axioms" as "basic properties" of certain operations. Indeed, even modern mathematicians use the word axiom in this way.

To rephrase the question above, we can ask: Which properties of real numbers and their operations should be considered axioms? And which operations, and properties, can be deduced from these?

2.3 "Axioms" for number systems. Rings.

It turns out that mathematicians have come to agree on what properties and operations should form the "axiomatic" beginnings of the operations we can do on numbers. And any object equipped with operations satisfying these axiomatic properties is called a *ring*. So, in the following definition, you should have the usual set of numbers, and the usual operations of addition and multiplication, in mind.

Definition 2.3.1 (Ring)**.** A *ring* is the data of:

- a set R, and
- two binary operations on R that we will call addition and multiplication,

satisfying the following properties:

1. (Properties of addition)
   (a) R contains an element called 0 so that, for every $a \in R$, we have $a + 0 = a$ and $0 + a = a$. 0 is called the "additive identity" or "zero" or the "additive unit."
   (b) Addition is associative, so that for every $a, b, c \in R$, we have $a + (b + c) = (a + b) + c$.
   (c) Addition is commutative, so that for every $a, b \in R$, we have $a + b = b + a$.
   (d) For every $a \in R$, R contains an element called $-a$ so that $a + (-a) = 0$. This $-a$ is called the "additive inverse" or "negative" of a.
2. (Properties of multiplication)
   (a) R contains an element called 1 so that, for every $a \in R$, we have $1 \cdot a = a = a \cdot 1$. 1 is called the "multiplicative identity" or "1."
   (b) Multiplication is associative, so that for every $a, b, c \in R$, we have $a(bc) = (ab)c$.
3. (Compatibility between addition and multiplication)

(a) Finally, we demand that multiplication distributes over addition. This means that for all $a, b, c \in R$, we have that $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$.

Definition 2.3.2. We will say a ring R is a *commutative* ring if, for every $a, b \in R$, $ab = ba$. (In other words, R is called a commutative ring if multiplication is commutative.)

Remark 2.3.3. Let me assure that *you could* begin with slightly different axioms and arrive at the exact same properties of rings; I can further assure you that while such an exercise is fun, and can deepen your understanding of what's happening, I'm going to move forward with the standard, agreed-upon axiomatics above so that you know what mathematicians usually think of when we say the word "ring."

Remark 2.3.4. There are seven properties above (count them). It probably seems like a lot to have thrown at you. But compare this to the sea of random facts from before. It turns out all those facts in that sea can be proven to be true starting only with the knowledge that the real numbers $\mathbb{R}$ form a commutative ring. In other words, the sea of facts you knew for real numbers is a sea of facts true for *any* commutative ring!

This is one power of axiomatic thinking. By knowing the short list of axioms that your facts depend on, you may deduce all these facts in other settings quickly quickly, just by verifying that the short list of axioms are true in these other settings.

Warning 2.3.5 (What are these equalities of?)**.** When you see an equality like $(b+c)a = ba+ca$, you should always keep in mind what kinds of objects we are declaring equal. Here, a, b, c are all elements of R, as are $(b+c)a$ and $ba+ca$. So this equality is stating that $(b+c)a$ and $ba+ca$ are the *same element of* R.

In particular, these need not be equalities of numbers. R could be a set of bananas for all we care (perhaps with a very interesting addition and multiplication!).

Warning 2.3.6. Most people have a very intuitive meaning they attach to the symbols 0 and 1. You should keep thinking of these as the symbols you are used to.

However, as mentioned in the previous warning, remember that R may not be a set of numbers. So while the symbols 0 and 1 denote elements of R

that behave more or less like you expect, they may not literally be numbers. For example, we will later see that the collection of all 2-by-2 matrices is a ring. In this case, the additive identity 0 will actually be represented by a matrix whose entries are all the number zero. And the multiplicative identity will be a matrix with the number 1 along the diagonal, and the number zero in the off-diagonal entries.

Remark 2.3.7. When most people think of the negative of a number, they think of "flipping the sign." Visually, if a is a number to the right of 0 on the number line, $-a$ becomes a number to the left of 0. Let me give both a warning and a hope: In many rings, there is no such thing as a "negative number." More precisely, there is sometimes no notion of being "larger than 0" or "smaller than 0." This is a hope, because it is very interesting, and it gives us hope of discovering cool phenomena.

It is a warning, because you should no longer think of the minus symbol as only applying to real numbers and "flipping signs." Instead, one should literally think of $-a$ as referring only to the additive inverse of an element a.

As an example, when we later use the ring $\mathbb{Z}/2\mathbb{Z}$, we will see that $1 = -1$.

2.4 Examples of proofs using the ring properties

Let's see some examples of how to access the sea of properties using only the ring axioms. The following propositions state some facts you are very familiar with for real numbers; we are discovering that they are in fact true for *any* ring. We will see examples of rings soon.

Each of the proofs below are written using slightly different styles of writing. So read over each proof carefully—both to get used to different ways of justifying steps, and also to see how you might want to write proofs yourself.

Proposition 2.4.1 (Uniqueness of additive identity)**.** Let R be a ring and let 0 and $0'$ be two elements of R which are both the additive identity. Then $0 = 0'$.

(Note that axiom 1a did not demand that there exists only *one* additive identity; but Proposition 2.4.1 tells us that this uniqueness is a consequence

of the axioms.) Informally, the above proposition states that there is at most one element that deserves to be called zero.

Proof. Since 0 is the additive identity, we know that $0 + 0' = 0'$. On the other hand, because $0'$ is also an additive identity, we know that $0 + 0' = 0$. Hence we have that $0 + 0'$ equals both 0 and $0'$. In particular, $0 = 0'$. □

(In the proof, we only used axiom 1a.)

Fix an element a. The next proposition shows that the notation "$-a$" refers to the *unique* element of R for which $a + (-a) = 0$; in other words, $-a$ is unambiguously defined.

Proposition 2.4.2 (Uniqueness of additive inverse)**.** Let R be a ring and fix an element $a \in R$. Let b and b' both be an additive inverse to a (Axiom 1b). Then $b = b'$.

Proof. We know that $a + b = 0$ by definition of additive inverse. By adding b', we see

$$b' + (a + b) = b' + 0 = b'$$

where the second equality follows from the definition of additive identity. On the other hand, by associativity, we have

$$b' + (a + b) = (b' + a) + b = 0 + b = b.$$

Combining the above two lines, we conclude that $b' = b$. □

Note that we use both associativity of addition (Axiom 1d) and the defining property of zero (Axiom 1a) in the above proof.

Proposition 2.4.3 (Additive cancellation law)**.** Let R be a ring. For three elements $a, b, c \in R$, suppose that $a + b = a + c$. Then $b = c$.

Proof. We know that $a + b = a + c$. Adding the additive inverse of a to both sides, we have that

$$-a + (a + b) = -a + (a + c).$$

By applying the associative property to both sides, we have

$$(-a + a) + b = (-a + a) + c.$$

By using the definition of additive inverse, we then see

$$0 + b = 0 + c.$$

By definition of additive identity, we conclude

$$b = c.$$

□

Here are some propositions that mix additive ideas with multiplicative ideas. Because the only axiom that mixes additive and multiplicative structures is the distributivity axiom, you should anticipate that we need to use the distributivity property in the proofs.

Proposition 2.4.4. Let R be a ring. Then for any $a \in R$, we have $0 \cdot a = 0$ and $a \cdot 0 = 0$.

Proof. We have the following string of equalities:

$$\begin{aligned} a + 0 \cdot a &= 1 \cdot a + 0 \cdot a \\ &= (1 + 0) \cdot a \\ &= 1 \cdot a \\ &= a \\ &= a + 0. \end{aligned}$$

The first line is by definition of the multiplicative identity (Axiom 2a). The next line is by distributivity (Axiom 3a). The next line is by definition of additive identity (Axiom 1a). The next is by definition of multiplicative identity again, then we conclude by definition of additive identity again.

All told, we see that $a + 0 \cdot a = a + 0$. By the cancellation law (Proposition 2.4.3), we conclude that $0 = 0 \cdot a$.

The proof that $a \cdot 0 = 0$ is similar. □

Proposition 2.4.5. Let R be a ring, and fix $a \in R$. Then $(-1) \cdot a = -a$. Likewise, $a \cdot (-1) = -a$.

Make sure you understand the notation here. -1 is the additive inverse to the multiplicative unit, and we are multiplying a by -1 on the lefthand side. On the righthand side, we claim that the result is the additive inverse of a.

Proof. By the definition of $-a$ (Axiom 1b) and the uniqueness of additive inverse (Proposition 2.4.2), it suffices to prove that $a + (-1) \cdot a = 0$. We have:

$$\begin{aligned} a + (-1) \cdot a &= 1 \cdot a + (-1) \cdot a && \text{Definition of 1} \\ &= (1 + -1) \cdot a && \text{Distributivity} \\ &= 0 \cdot a. && \text{Definition of -1} \\ &= 0 && \text{Proposition 2.4.4.} \end{aligned}$$

A similar proof shows $a \cdot (-1) = -a$. □

2.5 Examples of rings

Equip each of the following sets with their usual notions of addition and multiplication. Then each of the following is a ring:

- $\mathbb{Z}$, the set of all integers.
- $\mathbb{Q}$, the set of all rational numbers.
- $\mathbb{R}$, the set of all real numbers.
- $\mathbb{C}$, the set of all complex numbers.

In fact, the above are all *commutative* rings.

The above rings are all quite special, as we will see in a week or so. The next ring we'll study next week is the ring of all 2-by-2 matrices with real entries.

2.6 Exercises

Exercise 2.6.1 (Uniqueness of multiplicative identity)**.** Show that there is exactly one multiplicative identity in a ring. Which axiom(s) of a ring did you use?

Exercise 2.6.2. Let R be a ring and let 0 be its additive identity. Prove that $0 = -0$.

Exercise 2.6.3 (Uniqueness of multiplicative inverse)**.** Let R be a ring and fix an element $a \in R$. We say that an element b is a *multiplicative inverse* to a if $ab = 1$ and $ba = 1$.

Prove that if b and b' are both multiplicative inverses to a, then $b = b'$.

Exercise 2.6.4. Let R be a ring and fix an element $a \in R$. Prove that $-(-a) = a$.

Exercise 2.6.5. Let R be a ring. Prove that $(-1)\cdot(-1) = 1$. More generally, prove that for any $a \in R$, we have $(-a) \cdot (-a) = a \cdot a$.

Exercise 2.6.6. Let R be a ring, and suppose that R has the funny property that $1 + 1 = 0$. Show that for every $a \in R$, we have $a + a = 0$.

Exercise 2.6.7. Let R be a ring. Prove that the following statements are equivalent.

(a) For every element $a \in R$, there exists a multiplicative inverse to a.

(b) $0 = 1$.

(c) R contains exactly one element.

2.7 Extra Credit

Let A be the set of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$. For example, elements of A include:

1. The function $f(x) = 3$,
2. The function $f(x) = x$,
3. The function $f(x) = \sin(x) + x^2$.

A does not include functions such as $\ln(x)$ or $\tan(x)$, as these functions are not defined on all of $\mathbb{R}$.

For the purposes of this problem, let us define the following two operations:

- $\oplus$, the addition of two functions. Namely, given two functions f and g, we define $f \oplus g$ to be a new function where $(f \oplus g)(x) := f(x) + g(x)$. [1]
- $\circ$, the composition of two functions. Namely, $f \circ g$ is the function given by $(f \circ g)(x) := f(g(x))$. We will call $\circ$ "multiplication" for the purposes of this problem.

As it turns out, the set A with the operations $\oplus$ (as addition) and $\circ$ (as multiplication) satisfies every single property of being a ring *except one*.

Prompt: (i) Find this one failed property, and show why this property does not hold. (ii) Prove that $(A, \oplus, \circ)$ satisfies all other properties of being a ring.

[1] We'd usually write this as $f + g$, not $f \oplus g$, but I'm writing $\oplus$ to make clear that addition of numbers is not the same thing as addition of functions.