

**MATH 115, SUMMER 2012**  
**LECTURE 8**

JAMES MCIVOR

Today we'll use the concepts we've learned so far to introduce the notion of a ring, which is a concept from abstract algebra of huge importance in number theory.

Abstract algebra relates different mathematical objects by comparing and contrasting "structural properties". These include: ability to add and multiply, various properties of these operations, such as whether there are inverses, commutativity, associativity, etc. The basic types of "structures" one studies in algebra are groups, rings, and fields, and later modules. In fact, every ring is a group "with some extra structure", and a field is a special type of ring. So it's a little unnatural to start with rings, but let's do so anyway.

1. WHAT ARE RINGS?

The model for all rings is the set of integers,  $\mathbb{Z}$ . Once you've isolated the key properties of  $\mathbb{Z}$ , you already understand, at least implicitly, the definition of a ring. So what is  $\mathbb{Z}$  like? It's a set (an infinite set), in which we can A) add, B) subtract, C) multiply, but we can't really divide (that's what the rational numbers  $\mathbb{Q}$  are good for). Subtraction is the same as adding a negative, so we can instead say that  $\mathbb{Z}$  is a set with two operations: addition and multiplication, and addition happens to have inverses for every element of the set, but multiplication doesn't. Also  $\mathbb{Z}$  comes with two special elements: 0 and 1. 0 is interesting because adding it does nothing. 1 is interesting because multiplying by it does nothing. Then there are of course some properties that addition and multiplication both satisfy: associativity, commutativity, etc. That's basically the definition of a ring!

**Definition 1.** A **ring** is a set  $R$  equipped with two operations  $+$  and  $\cdot$ , with the following properties

- (1) Existence of additive identity, 0
- (2) Commutativity of  $+$
- (3) Associativity of  $+$
- (4) Every element has an additive inverse
- (5) Existence of multiplicative identity, 1
- (6) Associativity of  $\cdot$
- (7) Commutativity of  $\cdot$ <sup>1</sup>
- (8) Distributive law

The first four say that if we ignore the second operation,  $\cdot$ ,  $R$  is just an "abelian group". If you don't know what that is, it doesn't matter. The distributive law is maybe the most interesting - it's the only one that connects the two operations!

---

<sup>1</sup>This means that what we're really defining is a **commutative ring** - there are also rings without this property.

You may have seen axioms like this for a vector space in some linear algebra class. There are some similarities, but be warned: a vector space is *not* a ring! In a vector space, our set consists of the vectors, and then we also have some scalars that we can multiply by. But the scalars and the vectors are different. In a ring, there's only one set, and the multiplication happens between two elements of the set, not an element and some "scalar".

**Examples 1.1.** (1) The mother of all rings is  $\mathbb{Z}$ .

- (2) The set consisting of just one element, let's call it 0, can be thought of as a ring. To define the addition, we just have to say what is  $0 + 0$ . It must be 0, since there's nothing left in the set. Similarly  $0 \cdot 0 = 0$ . This means that the multiplicative identity, which we usually would call 1, is in this case the same as 0! Not a very interesting ring...
- (3) We denote by  $\mathbb{Z}[x]$  the ring of all polynomials with integer coefficients. To add and multiply just do the normal operations on polynomials. Note that if we just look at the *degree zero* polynomials (the constant polynomials), we see that they're just a copy of  $\mathbb{Z}$ . We say that  $\mathbb{Z}$  is a **subring** of  $\mathbb{Z}[x]$ .
- (4) Similarly, if we consider polynomials whose coefficients are allowed to be rational numbers (or real numbers, or complex numbers), we get a ring  $\mathbb{Q}[x]$  (or  $\mathbb{R}[x]$  or  $\mathbb{C}[x]$ ).
- (5) The set of rational numbers is itself a ring. Again,  $\mathbb{Z}$  is a subring of  $\mathbb{Q}$ , because  $\mathbb{Q}$  consists of all the integers, with some more stuff (namely fractions whose denominator is *not* 1).  $\mathbb{Q}$  has the property that every element (except for 0!) has a multiplicative inverse. This isn't part of the definition of a ring, but it is allowed, and when we a ring has that property it's called a **field**. So  $\mathbb{Q}$  is a field, as are  $\mathbb{R}$  and  $\mathbb{C}$ .
- (6) (Important Example) For us the most interesting ring is the following. Fix a positive integer  $m > 1$ . Then consider the set of congruence classes of integers modulo  $m$ . We can represent them by choosing a complete residue system. Let's call the congruence class of 0  $[0]$ , that of 1  $[1]$ , and so on, so our set looks like  $\{[0], [1], \dots, [m-1]\}$ . This set is a ring, called the **ring of integers mod  $m$** , and denoted by  $\mathbb{Z}/m$ . Some people write it as  $\mathbb{Z}_m$  or  $\mathbb{Z}/m\mathbb{Z}$ . The theorem on "properties of congruences" basically says that this is a ring!

Anyway, this set of congruence classes is a ring - we can add and multiply modulo  $m$ . Some interesting things happen here. Say  $m = 6$ . Then we have  $[3] \cdot [2] = [6] = [0]$ , since  $0 \equiv 6 \pmod{6}$ . So in this ring, two nonzero elements can multiply to make zero. We call such elements **zerodivisors**, for obvious reasons. Also, we have seen that if  $a$  is relatively prime to 6, then it has a multiplicative inverse. For example, 5 has an inverse, namely itself, since  $[5] \cdot [5] = [25] = [1]$ , since  $25 \equiv 1 \pmod{6}$ . An element which has a multiplicative inverse is called a **unit**.

If every nonzero element is a unit, then the ring is a field. Since  $a$  is a unit if and only if  $(a, m) = 1$ ,  $\mathbb{Z}/m$  will be a field if and only if all the integers from 1 to  $m-1$  are prime to  $m$ . This happens if and only if  $m$  is prime. So there are a bunch of **finite fields**  $\mathbb{Z}/p$ , for various primes  $p$ . If  $m$  is composite, then the ring  $m$  is not a field.

## 2. HOMOMORPHISMS

If rings weren't great enough already, things only get more interesting when we consider multiple different rings, and functions between them. But we shouldn't care about just any function. In calculus, one focuses on continuous or differentiable functions from  $\mathbb{R}$  to  $\mathbb{R}$  - these are special types of functions which are interesting in that context. In the study of rings, the functions that are interesting are the ones that are compatible with the addition and multiplication. This makes sense, because that's the only structure going on in a ring.

**Definition 2.** If  $R$  and  $S$  are two rings, a **homomorphism** from  $R$  to  $S$  is a function  $\phi: R \rightarrow S$  with the following properties:

- (1)  $\phi(a + b) = \phi(a) + \phi(b)$
- (2)  $\phi(ab) = \phi(a)\phi(b)$
- (3)  $\phi(1) = 1$

The first two are about order of operations: we can add first in  $R$ , and then send the answer over to  $S$  with  $\phi$ , or we can send both  $a$  and  $b$  over to  $S$  and add there; either way, we should get the same result. Similarly for multiplication. The third one says that "1 goes to 1". Notice that the two 1's are different! The 1 on the left lives in  $R$ , while the 1 on the right lives in  $S$ .

Often I'll call a homomorphism a "ring map" or even just a "map" if I'm feeling lazy.

Similar to the comment in the previous section, notice how this differs from the definition of a linear map. Also, if you've seen some abstract algebra, you may know that there is a notion of a homomorphism of groups, too, which is not the same, since in a group there is only one operation, whereas in a ring there are two, so there are more compatibility requirements for a function to be a homomorphism of rings than just of groups. Of course, every ring is an abelian group, too, if we just forget about the multiplication, and then a homomorphism of rings is also a homomorphism of groups. But not every group can be made into a ring.

- Examples 2.1.**
- (1) The identity map  $\mathbb{Z} \rightarrow \mathbb{Z}$  is a ring homomorphism.
  - (2) The map  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  given by  $f(n) = 2n$  is not.
  - (3) (Important Example) The function  $\mathbb{Z} \rightarrow \mathbb{Z}/m$  which sends an integer  $n$  to its residue class  $[n] \bmod m$  is a ring homomorphism.
  - (4) Sort of "opposite" to the previous example: Consider the function  $\mathbb{Z}/4 \rightarrow \mathbb{Z}$  sending  $[0]$  to 0,  $[1]$  to 1,  $[2]$  to 2,  $[3]$  to 3. This is *not* a ring map!
  - (5) When can we have a ring map  $\mathbb{Z}/n \rightarrow \mathbb{Z}/m$ ? Explore this in discussion section.