8 Rings

We'll now discuss the second main topic of this course: rings.

Guiding Question
Groups have only one operation, but lots of familiar sets $(\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Q})$ have two operations: addition and multiplication. How can we generalize the idea of sets with two operations, rather than one?

8.1 What is a Ring?

Informally, a ring is a set of elements which can be added and multiplied, so that the natural properties we would expect of addition and multiplication all hold.

Example 8.1
The familiar sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are rings.

Example 8.2
There are various rings between $\mathbb{Z}$ and $\mathbb{Q}$: for example,

$$\mathbb{Z}[1/2] \coloneqq \left\{a/2^k \mid a, k \in \mathbb{Z}\right\}$$

is a ring. Similarly, the **Gaussian integers**

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

and

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

are rings. So is

$$\mathbb{Z}[\zeta] = \left\{a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1} \mid a_i \in \mathbb{Z}\right\},$$

where ζ is some nth root of unity.

We can now state the formal definition of a ring:

Definition 8.3
A **ring** R is a set with two binary operations $R \times R \to R$, written as $+$ and $\cdot$ (and called addition and multiplication), which satisfy the following axioms:

1. $(R, +)$ is an abelian group: addition is associative and commutative, there is an additive identity 0_R such that $0_R + a = a$ for all $a \in R$, and every element has an additive inverse.
2. Multiplication is also associative and commutative, and there is a multiplicative identity 1_R. (In other words, under multiplication, R is a *semigroup* — a group without the condition that every element has an inverse.)
3. Addition and multiplication satisfy *distributivity*: for all $a, b, c \in R$, we have

$$a(b + c) = ab + ac.$$

In this class, we'll use "ring" in this sense; but usually a ring satisfying this definition is called a *commutative unital ring*. In defining a general ring, one can drop the requirement of commutativity of multiplication, or the existence of 1_R. If every condition holds except for $ab = ba$ — and we add distributivity in the other direction as well, meaning $(b + c)a = ba + ca$ — then R is called a **noncommutative ring**.

Example 8.4 (Matrices)
The ring of matrices $\mathrm{Mat}_{n\times n}(\mathbb{C})$ is a noncommutative ring, since matrix multiplication is noncommutative (and all the other axioms are satisfied). Similarly, $\mathrm{End}(V)$ for a vector space V is a noncommutative ring.

Example 8.5 (Group Ring)
If G is a group, then take the vector space with basis vectors v_g for $g \in G$ (note that this is the vector space acted on by the regular representation). Clearly, addition is already defined; and multiplication can be defined in the natural way, as

$$v_g v_h = v_{gh}.$$

Then this gives the **group ring**, which is noncommutative if G is nonabelian.

From now on, all rings will be commutative as in the definition, unless stated otherwise.

8.2 Zero and Inverses

The following proposition confirms a property that we would like rings to have.

Proposition 8.6
In any ring R, $0_R \cdot a = 0_R$ for all $a \in R$.

Proof. Pick some $x \in R$. Then, since $0_R + x = x$, we have

$$xa = (0_R + x)a = 0_R a + xa.$$

We can cancel out xa (since R is an abelian group under addition), so $0_R = 0_R a$. □

Corollary 8.7
The additive identity 0_R cannot have a multiplicative inverse unless $0_R = 1_R$. (In other words, division by 0 is only possible when $0 = 1$.)

The axioms do not require that $0_R \neq 1_R$. But if $0_R = 1_R$, then for any $x \in R$,

$$x = x \cdot 1_R = x \cdot 0_R = 0_R.$$

So R must be a one-element ring; there's only one binary operation on a set with one element, which does satisfy the axioms. This ring is called the **zero ring**; it is a legitimate but trivial example. In all other cases, $0_R \neq 1_R$, as we would expect.

Definition 8.8
A (nonzero) ring where every nonzero element has a multiplicative inverse is called a **field**.

Note that by definition, the zero ring is not a field.

Example 8.9
The familiar sets $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.

Example 8.10
The integers $\mathbb{Z}$ do not form a field, since most numbers do not have inverses. For the same reason, the Gaussian integers $\mathbb{Z}[i]$ are not a field either. For example, 2 is not invertible in either ring.

Example 8.11
The integers modulo n, denoted $\mathbb{Z}/n\mathbb{Z}$, form a field if and only if n is prime (since in general, a is invertible mod n if and only if a and n are coprime).

More examples of rings (which are not fields) come from functions:

Example 8.12
The set $\mathbb{C}[x]$, consisting of polynomials in one variable with complex coefficients, is a ring. The set $C^\infty(\mathbb{R})$, consisting of real-valued functions which are continuous and infinitely differentiable, is also a ring.

In some sense, you can think of fields as a generalization of numbers, and more general rings as generalizations of functions.

8.3 Homomorphisms

When studying groups, one of the most powerful tools comes from thinking about mappings between groups. In particular, homomorphisms, which are functions that respect the group operation, and their kernels/images provide lots and lots of information about groups.

Guiding Question
How can we formalize the idea of "functions between rings that behave nicely with respect to addition and multiplication"?

Similarly to the path we took when studying groups, we can now define a ring homomorphism.

Definition 8.13
A ring **homomorphism** from R to S is a map $\varphi : R \to S$ such that:

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$;
2. $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$;
3. $\varphi(1_R) = 1_S$.

Example 8.14
The mapping $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $a \mapsto \overline{a}$ (where $\overline{a}$ denotes a mod n) is a ring homomorphism.

Why is it not necessary to require that $\varphi(0_R) = 0_S$? In fact, it is implied by the other axioms, because additive inverses exist!

Proposition 8.15
For a ring homomorphism $\varphi : R \to S$, it must be the case that $\varphi(0_R) = 0_S$.

Proof. Using the first property, $\varphi(a) = \varphi(a + 0_R) = \varphi(a) + \varphi(0_R)$, and so adding $-\varphi(a)$ to both sides gives $0_S = \varphi(0_R)$. □

On the other hand, because there are not necessarily multiplicative inverses, the property $\varphi(1_R) = 1_S$ must be explicitly written. In fact, there are examples of maps compatible with $+$ and $\cdot$ (meaning they satisfy the first two properties) that have $\varphi(1_R) \neq 1_S$.

Example 8.16
Let R be the zero ring, and S be any nonzero ring (for example, $\mathbb{Z}$). Then take the map $0_R \mapsto 0_S$. This is compatible with the additive and multiplicative structure of the two rings; but since $1_S \neq 0_S$, it is not a ring homomorphism. (There exist less trivial examples as well.)

If $\varphi : R \to S$ is one-to-one and onto (that is, φ is a bijection), then it is possible to check (as in the case of group homomorphisms) that the inverse bijection is also a homomorphism.

Definition 8.17
A bijective homomorphism is called an **isomorphism**.

If φ is one-to-one but *not* onto, then φ is an isomorphism from R to its image, so it identifies R with a **subring** of S:

Definition 8.18
A **subring** S of R is a subset which is closed under addition, taking additive inverses, and multiplication, and contains 1_R.

Meanwhile, if φ is *not* one-to-one, then we can think about its kernel

$$\ker(\varphi) = \{a \in R : \varphi(a) = 0\}.$$

(This is the same definition as we saw with groups.) If φ is not one-to-one, then $\ker(\varphi)$ is nontrivial.

Guiding Question
What information can be gained from ring homomorphisms with nontrivial kernel?

The kernel must be an additive subgroup of S. But it turns out that it must also be compatible with multiplication in some ways; this brings us to the concept of *ideals*.

8.4 Ideals

Definition 8.19 (Ideal)
An **ideal** of R is a subset $I \subset R$ such that I is an additive subgroup of R, and for any $x \in I$ and $a \in R$, we have $ax \in I$.

So an ideal isn't just closed under multiplication, it's in fact closed under multiplication by *any* element in R.

The kernel of a ring homomorphism is necessarily an ideal — if $\varphi(x) = 0$, then for any $a \in R$, we have

$$\varphi(ax) = \varphi(a)\varphi(x) = 0.$$

Example 8.20
For any $n \in \mathbb{Z}$, the subset $n\mathbb{Z}$ (consisting of multiples of n) is an ideal. More generally, if R is any ring and a an element of R, then $aR = \{ax \mid x \in R\}$ is an ideal.

In fact, this is an important example of an ideal, as we'll see later, so it has a name:

Definition 8.21 (Principal Ideal)
For an element $a \in R$, the ideal aR is called a **principal ideal**, and denoted (a).

Any additive subgroup of $\mathbb{Z}$ is cyclic, i.e., of the form $n\mathbb{Z}$. This means every ideal of $\mathbb{Z}$ is principal (since every ideal is an additive subgroup). However, in a general ring, not every ideal will be principal.

More generally, we can consider picking *several* elements:

Definition 8.22
For elements $a_1, \ldots, a_n \in R$, the set of linear combinations

$$\left\{\sum a_i x_i \mid x_i \in R\right\}$$

is an ideal of R, denoted as $(a_1, \ldots, a_n)$; this is called the ideal **generated** by $a_1, \ldots, a_n$.

Note that $(a_1, \ldots, a_n)$ is the smallest ideal containing all of $a_1, \ldots, a_n$ (as it is an ideal, while all elements $\sum a_i x_i$ must be in the ideal by the axioms).

Ideals in rings are in some sense analogous to normal subgroups in groups (in particular, both arise as the kernel of a homomorphism), and we can take quotients in a similar way as well:

Proposition 8.23 (Quotient Ring)
Let R be a ring and $I \subset R$ an ideal. Since I is a normal subgroup of R under addition (as both are abelian groups), we can construct the quotient R/I of additive groups. Then R/I is in fact a ring (with multiplication defined in the natural way — the product of the cosets corresponding to x and y is the coset corresponding to xy), called the **quotient ring**.

Proof. For each $x \in R$, we use $\overline{x}$ to denote the coset $x + I$.

We first need to check that multiplication is well-defined, meaning that if $\overline{x}$ is represented by two elements x_1 and x_2, then using either representative to calculate $\overline{x} \cdot \overline{y}$ will give us the same result. But we have $x_1 - x_2 = a$ for some $a \in I$, which means

$$x_1 y - x_2 y = ay \in I$$

as well (since I is closed under multiplication by any element $y \in R$), so $x_1 y$ and $x_2 y$ are also in the same coset. So the product of two cosets doesn't depend on our choice of representatives, which means multiplication really is well-defined.

As in the case of groups, once we know that multiplication is well-defined, it is easy to check that all the ring axioms are satisfied by R/I. □

Without going into detail, replacing "group" by "ring" and "normal subgroup" by "ideal," the story for rings is extremely similar to that for groups. For example, if φ is a homomorphism, then there is an isomorphism

$$R/\ker(\varphi) \cong \operatorname{im}(\varphi).$$

Additionally, for an ideal $I \subset R$, there is a bijection between ideals in R/I and ideals in R containing I (this is essentially the Correspondence Theorem for rings).

Example 8.24
For $R = \mathbb{Z}$ and $I = n\mathbb{Z}$, we have $R/I = \mathbb{Z}/n\mathbb{Z}$ (where $\mathbb{Z}/n\mathbb{Z}$ denotes the integers mod n) as rings, not just groups. This is essentially the fact that multiplication of residues mod n is well-defined, not just addition. (This is where the notation $\mathbb{Z}/n\mathbb{Z}$ comes from — to obtain the integers mod n, we're quotienting out the ring of integers by the ideal $n\mathbb{Z}$.)

Resource: Algebra II Student Notes

Spring 2022

Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng