Math 350: Abstract Algebra II

Rings, Modules, and Algebras

Timothy Magee

Hollins University, Spring 2026

1 Introduction

In this class we will discuss three important algebraic structures – rings, modules, and algebras. These are concepts that we will have to define with care. You've seen examples of all three. Most of the number systems you've encountered (the integers, the rationals, the reals, and the complex numbers) are rings. Vector spaces are examples of modules. Algebras combine the previous two notions – they are both rings and modules. Various flavors of functions you've encountered (polynomials in n variables, continuous real-valued functions, smooth vector-valued functions, etc.) form algebras. We're going to explore all of these topics systematically. We'll consider the essential features of number systems, vector spaces, and functions, then use these features to define rings, modules, and algebras.

2 Rings

We're going to try to define algebraic structures that encompass "number systems". There isn't a single *right way* to do this; the algebraic structure we come up with will depend upon what we ask for. So let's consider some of our favorite number systems and see if we can come up with some of their common features, and some differences between them.

Examples of Number Systems.

- the natural numbers $\mathbb{N}$ (with or without 0) Let's call them $\mathbb{Z}_{\geq 0}$ and $\mathbb{Z}_{>0}$.
- the integers $\mathbb{Z}$
- the rational numbers $\mathbb{Q}$
- the real numbers $\mathbb{R}$

- the complex numbers $\mathbb{C}$
- modular numbers $\mathbb{Z}/n\mathbb{Z}$
- the quaternions $\mathbb{H}$ (You probably haven't encountered the quaternions yet. We'll discuss them now.)

Example 1 (The Quaternions)**.** The quaternions $\mathbb{H}$ are an extension of the complex numbers $\mathbb{C}$. Like the complex numbers, we can write quaternions as a linear combination of real numbers: $a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$. Their multiplication is defined by the rules:

- $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$
- $\mathbf{i} \cdot \mathbf{j} = \mathbf{k}$, $\mathbf{j} \cdot \mathbf{k} = \mathbf{i}$, $\mathbf{k} \cdot \mathbf{i} = \mathbf{j}$
- $\mathbf{j} \cdot \mathbf{i} = -\mathbf{k}$, $\mathbf{k} \cdot \mathbf{j} = -\mathbf{i}$, $\mathbf{i} \cdot \mathbf{k} = -\mathbf{j}$

Note that this is a number system where multiplication is *not* commutative.

In all of the number systems we mentioned above, we can add numbers and multiply numbers, and there is a compatibility between these two operations. Except for the natural numbers without 0, all of these number systems have an additive identity (0). They all have a multiplicative identity (1). In each case, both the addition and multiplication are associative: $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. And in each case we also have the distributive property relating these two operations: $a \cdot (b+c) = (a \cdot b)+(a \cdot c)$ and $(a+b) \cdot c = (a \cdot c)+(b \cdot c)$. The addition operation in each of these examples is commutative: $a+b = b+a$, and in each example except for the quaternions the multiplication is commutative as well: $a \cdot b = b \cdot a$. In each case except for the natural numbers (with or without 0), every number a has an additive inverse $-a$, meaning $a + (-a) = 0$.

Question 2. Can you make an analogous statement involving multiplicative inverses? (You may have to make some change to get an interesting answer.)

If we ask whether or not every number a in our number system has a multiplicative inverse, the answer will always be *"no"* – for instance, 0 has no multiplicative inverse. So, instead we can ask whether or not every *non-zero* a in our number system has a multiplicative inverse.

Let's summarize the properties of each of these number systems in a table. In line with the previous comment, existence of multiplicative inverses in this chart is for non-zero numbers.

	0	1	Associativity		Commutativity		Distributivity	Inverses	
			$+$	$\cdot$	$+$	$\cdot$		$+$	$\cdot$
$\mathbb{Z}_{\geq 0}$	✓	✓	✓	✓	✓	✓	✓		
$\mathbb{Z}_{>0}$		✓	✓	✓	✓	✓	✓		
$\mathbb{Z}$	✓	✓	✓	✓	✓	✓	✓	✓	
$\mathbb{Q}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathbb{R}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathbb{C}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathbb{Z}/n\mathbb{Z}$	✓	✓	✓	✓	✓	✓	✓	✓	If n prime
$\mathbb{H}$	✓	✓	✓	✓	✓		✓	✓	✓

If we now want to build an algebraic structure that captures our idea of a number system, we have some choices to make. We definitely want a pair of associative operations like addition and multiplication, and we want them to be compatible with each other. That is, we want the distributive property to hold. Beyond that, there are plenty of reasonable options that are genuinely used in modern mathematics. The different options have different names, and unfortunately each name may mean different things to different people – just like the *natural numbers* may mean $\mathbb{Z}_{\geq 0}$ or $\mathbb{Z}_{>0}$, depending on whom you ask. All of the options will be defined in a similar way:

Definition. A _____ is a set R together with a pair of associative binary operations

$$+ : R \times R \to R$$

and

$$\cdot : R \times R \to R$$

(called *addition* and *multiplication*) such that the following properties hold.

- *(Commutativity of Addition)* For all a and b in R, we have $a + b = b + a$.
- *(Distributivity)* For all a, b, and c in R, we have

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad \text{and} \qquad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

- ...

For instance,

Definition 3. A *semi-ring* is a set R together with a pair of associative binary operations

$$+ : R \times R \to R$$

and

$$\cdot : R \times R \to R$$

(called *addition* and *multiplication*) such that the following properties hold.

- *(Commutativity of Addition)* For all a and b in R, we have $a + b = b + a$.
- *(Distributivity)* For all a, b, and c in R, we have

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad \text{and} \qquad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

- *(Additive Identity)* There is an element $0 \in R$ such that $0 + a = a$ for all $a \in R$.
- *(Multiplicative Identity)* There is an element $1 \in R$ such that $1 \cdot a = a = a \cdot 1$ for all $a \in R$.

Question 4. Of the number systems we considered above, which are semi-rings?

Definition 5. A *ring* is a set R together with a pair of associative binary operations

$$+ : R \times R \to R$$

and

$$\cdot : R \times R \to R$$

(called *addition* and *multiplication*) such that the following properties hold.

- *(Commutativity of Addition)* For all a and b in R, we have $a + b = b + a$.
- *(Distributivity)* For all a, b, and c in R, we have

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad \text{and} \qquad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

- *(Additive Identity)* There is an element $0 \in R$ such that $0 + a = a$ for all $a \in R$.
- *(Multiplicative Identity)* There is an element $1 \in R$ such that $1 \cdot a = a = a \cdot 1$ for all $a \in R$.
- *(Additive Inverses)* For every $a \in R$ there is an element $-a \in R$ such that $a + (-a) = 0$.

Question 6. Of the number systems we considered above, which are rings?

Definition 7. A *commutative ring* is a set R together with a pair of associative binary operations

$$+ : R \times R \to R$$

and

$$\cdot : R \times R \to R$$

(called *addition* and *multiplication*) such that the following properties hold.

- *(Commutativity of Addition)* For all a and b in R, we have $a + b = b + a$.
- *(Commutativity of Multiplication)* For all a and b in R, we have $a \cdot b = b \cdot a$.
- *(Distributivity)* For all a, b, and c in R, we have

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

- *(Additive Identity)* There is an element $0 \in R$ such that $0 + a = a$ for all $a \in R$.
- *(Multiplicative Identity)* There is an element $1 \in R$ such that $1 \cdot a = a = a \cdot 1$ for all $a \in R$.
- *(Additive Inverses)* For every $a \in R$ there is an element $-a \in R$ such that $a + (-a) = 0$.

Notice that we could give Definitions 5 and 7 more succinctly by building on previous definitions.

Definition 8. A *ring* is a semi-ring R such that each $a \in R$ has an additive inverse in R. That is, for each $a \in R$ there is an element $-a \in R$ such that $a + (-a) = 0$.

Definition 9. A *commutative ring* is a ring R whose multiplication operation is commutative. That is, for all a and b in R, we have $a \cdot b = b \cdot a$.

Question 10. Notice that I wrote the distributive property more concisely in Definition 7 than in Definition 5. Was this a mistake? If not, why can I state this property more concisely in Definition 7?

Remark 11. As mentioned above, the terms *semi-ring*, *ring*, and *commutative ring* may mean slightly different things to different people. For instance, it is common not to require the existence of a multiplicative identity 1 in each of these cases. Authors that take this approach will generally refer to what we have called a *ring*, for instance, as either a *unital ring* or a *ring with 1*. It's also common to drop the requirement of existence of an additive identity 0 in the definition of a semi-ring. Doing so would make $\mathbb{Z}_{>0}$ a semi-ring. In this class, we'll focus on rings more than semi-rings, and our rings will be understood to have a multiplicative identity 1.

So far we have viewed these algebraic structures as ways to capture different notions of number systems – and that was indeed our motivation. But now that we have carefully defined *semi-rings*, *rings*, and *commutative rings*, we may find that these terms also encompass notions that we generally wouldn't associate with number systems.

Question 12. Consider the $n \times n$ matrices with real entries $\text{Mat}_{n\times n}(\mathbb{R})$, with the usual notions of matrix addition and multiplication. Is $\text{Mat}_{n\times n}(\mathbb{R})$ a *semi-ring*? A *ring*? A *commutative ring*?

Question 13. Do polynomials in one variable x with integer coefficients form a *semi-ring*? A *ring*? A *commutative ring*? What about polynomials in n variables $x_1, \ldots, x_n$?

Let's now summarize the definitions with a chart.

	0	**1**	**Associativity**		**Commutativity**		**Distributivity**	**Inverses**	
			$+$	$\cdot$	$+$	$\cdot$		$+$	$\cdot$
semi-ring	✓	✓	✓	✓	✓		✓		
ring	✓	✓	✓	✓	✓		✓	✓	
commutative ring	✓	✓	✓	✓	✓	✓	✓	✓	

Defining algebraic structures in terms of properties as we have just done allows us to study them systematically. Ideally, many different objects will have the algebraic structure we've defined. By studying the algebraic structure we can draw conclusions about all of these objects at once, and develop a real understanding of what's going on " beneath the hood".

Specifying an algebraic structure can also clarify how we are thinking about the objects. We can associate many different algebraic structures to some objects. If I mention the *integers* in a number theory context, it probably makes sense to think of the integers as a commutative ring. On the other hand, if I use the integers as an indexing set, you're probably better off thinking of them as an ordered set. Specifying the algebraic structure in this case makes it clear what setting we are working in.

2.a Homomorphisms

So, now we know how to describe our landscape, and we can identify which objects are part of the landscape. How do we travel between these objects? That is, once we fix the algebraic structure we are considering, what sort of maps should we consider between objects having

this algebraic structure? For instance, if R and S are semi-rings, what should a semi-ring map $f : R \to S$ mean?

Once again, we have options. Thankfully, very often there's only one *good* option. Let's start with a bad option – a first attempt that will need some fixing.

Attempt 1. If R and S are semi-rings, then they are sets together with some additional structure. We know how to define set maps. So, we could try defining a semi-ring map $f : R \to S$ to be a map of the underlying sets. But this is philosophically disappointing. A semi-ring is a set together with additional structure, and this completely ignores the additional structure. We could call it a map of sets, but we've really got no right to call it a map of semi-rings.

This leads us to the idea of a *homomorphism* – *homo* meaning *same* and *morph* meaning *form*. A *homomorphism* f between two objects of some given algebraic structure is a function that respects the given algebraic structure. So:

Definition 14. Let R and S be semi-rings, and denote their additive identities by 0_R and 0_S and their multiplicative identities by 1_R and 1_S, respectively. A function $f : R \to S$ is a *semi-ring homomorphism* if for all $r_1, r_2 \in R$,

(1) $f(r_1 + r_2) = f(r_1) + f(r_2)$,

(2) $f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)$,

(3) $f(0_R) = 0_S$, and

(4) $f(1_R) = 1_S$.

This looks a lot better. It ensures that f respects all of the semi-ring structure. Before moving on to the definition of a ring homomorphism, let's make sure we understand Definition 14. Note that in Item (1) the symbol "+" means two different things. On the left hand side of the equation it means addition in R, while on the right hand side it means addition in S. In fact, if we wish to be explicit, we can rewrite Item (1) as

$$f(r_1 +_R r_2) = f(r_1) +_S f(r_2).$$

Similarly, on the left hand side of Item (2), the symbol "$\cdot$" means multiplication in R, while on the right hand side it means multiplication in S. We could rewrite Item (2) as

$$f(r_1 \cdot_R r_2) = f(r_1) \cdot_S f(r_2).$$

Now let's make an analogous definition for rings. The only difference between semi-rings and rings is that every element of a ring has an additive inverse, so maybe we can just add a condition that ensures additive inverses in R are sent to additive inverses in S?

Definition 15. Let R and S be rings, and denote their additive identities by 0_R and 0_S and their multiplicative identities by 1_R and 1_S, respectively. A function $f : R \to S$ is a *ring homomorphism* if for all $r_1, r_2 \in R$,

(1) $f(r_1 + r_2) = f(r_1) + f(r_2)$,

(2) $f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)$,

(3) $f(0_R) = 0_S$,

(4) $f(1_R) = 1_S$, and

(5) $f(-r_1) = -f(r_1)$.

Again, this looks like a very reasonable definition – we just directly asked our map to respect all of the properties of a ring. But it is *not* the most efficient definition. In fact, Items (3) and (5) are entirely unneeded. To be clear, we do need Items (3) and (5) to hold, we just don't need to write them explicitly. They follow from Item (1).

Proposition 16. *Let R and S be rings and let $f : R \to S$ be a function such that for all $r_1, r_2 \in R$,*

$$f(r_1 + r_2) = f(r_1) + f(r_2).$$

Then $f(0_R) = 0_S$.

Proof. Since S is a ring, every element of S has an additive inverse. In particular, $f(0_R)$ has an additive inverse $-f(0_R)$. Then

$$\begin{aligned} f(0_R) &= f(0_R) + 0_S \\ &= f(0_R) + f(0_R) + (-f(0_R)) \\ &= f(0_R + 0_R) + (-f(0_R)) \\ &= f(0_R) + (-f(0_R)) \\ &= 0_S. \end{aligned}$$

□

Proposition 17. *Let R and S be rings and let $f : R \to S$ be a function such that for all $r_1, r_2 \in R$,*

$$f(r_1 + r_2) = f(r_1) + f(r_2).$$

Then for every $r \in R$, we have $f(-r) = -f(r)$.

Proof. We want to show $f(r) + f(-r) = 0_S$, and by Proposition 16, we know $f(0_R) = 0_S$. So,

$$f(r) + f(-r) = f(r + (-r)) = f(0_R) = 0_S,$$

as desired. □

So, we can restate Definition 15 more compactly as follows:

Definition 18. Let R and S be rings, and denote their multiplicative identities by 1_R and 1_S, respectively. A function $f : R \to S$ is a *ring homomorphism* if for all $r_1, r_2 \in R$,

(1) $f(r_1 + r_2) = f(r_1) + f(r_2)$,

(2) $f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)$, and

(3) $f(1_R) = 1_S$.

Note: As Sydney observed in class, we can also simply reuse the definition of a semi-ring homomorphism. That is, if R and S are rings, they are *a fortiori* semi-rings. What we have just found is that the semi-ring homomorphisms and ring homomorphisms from R to S precisely coincide.

Question 19. Suppose we were to define special types of rings – meaning a ring with some additional required properties. Is there some property we could impose that would render Item (3) redundant as well?

This is an important type of ring and we will discuss it in more details in a couple weeks.

A word of caution – we have mentioned that many of the objects we study regularly have many different algebraic structures. As such, when we talk about homomorphisms, it's a good idea to be clear which sort of homomorphisms we are considering. See below:

Question 20.

(1) Describe all ring homomorphisms $f : \mathbb{Z} \to \mathbb{Z}$.

(2) Describe all *group* homomorphisms $f : \mathbb{Z} \to \mathbb{Z}$.

To view $\mathbb{Z}$ as a *group*, we only consider the addition operation and forget the multiplication operation. A group homomorphism $f : \mathbb{Z} \to \mathbb{Z}$ must satisfy $f(n+m) = f(n)+f(m)$ for all $n, m \in \mathbb{Z}$.

In fact, in Question 20, Item (1), we didn't need to specify that the codomain was also $\mathbb{Z}$ in order to find exactly one homomorphism.

Question 21. Let R be any ring. Show that there is exactly one ring homomorphism $f : \mathbb{Z} \to R$.

The fancy way of saying what you have just proved is that *"$\mathbb{Z}$ is an initial object in the category of rings and ring homomorphisms"*.

Question 22. Can you find all of the homomorphisms $f : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}$? What about $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ for some arbitrary integer n?

Question 23. Can you you describe every ring homomorphism $f : \mathbb{R}[x] \to \mathbb{R}$?

You have hopefully just described evaluation of a polynomial at a real number r.

Question 24. Give two different ring homomorphisms from the polynomial ring $\mathbb{Z}[x]$ to itself. Can you think of an elegant way to describe *any* ring homomorphism $f : \mathbb{Z}[x] \to \mathbb{Z}[x]$?

One homomorphism that you may have discovered while tackling Question 24 is the map defined by

$$\begin{aligned} f : \mathbb{Z}[x] &\to \mathbb{Z}[x] \\ x &\mapsto 0. \end{aligned}$$

This homomorphism sends every polynomial with constant term 0 to 0. That is, for every polynomial of the form $a_1x + a_2x^2 + \cdots + a_nx^n$, we have

$$f\left(a_1x + a_2x^2 + \cdots + a_nx^n\right) = 0.$$

This set of polynomials is called the *kernel* of f.

Definition 25. Let $f : R \to S$ be a ring homomorphism. The *kernel* of f is

$$\ker(f) := \{r \in R \mid f(r) = 0_S\}.$$

This notion will come up again when we discuss ideals in Section 2.c.

2.b Basic properties of rings

In this subsection we will explore some of the basic properties of rings through a series of questions. The results you are asked to prove here may all seem "*obviously true*". The goal is to show that they do in fact follow from the definitions we've given.

Question 26. Let R be a semi-ring. Show that the additive identity of R is unique. That is, if 0_R and $0_R{}'$ are additive identities of R, then $0_R = 0_R{}'$.

Since both 0_R and $0_R{}'$ are additive identities, we must have

$$0_R = 0_R + 0_R{}' = 0_R{}'.$$

While we're at it –

Question 27. Does a similar statement hold for the multiplicative identity of a semi-ring?

Yes.

Question 28. Let R be a ring and $r \in R$. Show that the additive inverse of r is unique. That is, if $r + s = 0_R$ and $r + t = 0_R$, then $s = t$.

Suppose $r + s = 0_R$ and $r + t = 0_R$. Then

$$\begin{aligned} s &= s + 0_R \\ &= s + (r + t) \\ &= (s + r) + t \\ &= 0_R + t \\ &= t. \end{aligned}$$

In fact, we can generalize Question 28:

Question 29. Let R be a ring and let r, s, and t be elements of R. Show that if $r+s = r+t$, then $s = t$.

Add $-r$ to both sides of the equation.

Question 30. Let R be a ring. Show $-0_R = 0_R$. That is, 0_R is its own additive inverse.

Since -0_R is the additive inverse of 0_R, we have $0_R + (-0_R) = 0_R$. Next, since 0_R is the identity of addition, $0_R + (-0_R) = -0_R$. So $0_R = -0_R$.

Alternatively, and more directly,

Since 0_R is the additive identity $0_R + 0_R = 0_R$. Then 0_R is the additive inverse of 0_R, *i.e.* $-0_R = 0_R$.

Question 31. Let R be a ring. Show that $0_R \cdot r = 0_R$ for all $r \in R$.

Hint: *Use Question 29.*

First, note that

$$\begin{aligned} 0_R \cdot r &= (0_R + 0_R) \cdot r \\ &= (0_R \cdot r) + (0_R \cdot r). \end{aligned}$$

Next, $0_R \cdot r = (0_R \cdot r) + 0_R$, so

$$(0_R \cdot r) + 0_R = (0_R \cdot r) + (0_R \cdot r).$$

But this implies $0_R \cdot r = 0_R$ by Question 29.

What would change above if we instead considered $r \cdot 0_R$?

Question 32. Let R be a ring and let $r, s \in R$. Show that $(-r) \cdot s = -(r \cdot s) = r \cdot (-s)$.

We want to show that $r \cdot s + (-r) \cdot s = 0_R$ and $r \cdot s + r \cdot (-s) = 0_R$.

$$\begin{aligned} r \cdot s + (-r) \cdot s &= (r + (-r)) \cdot s \\ &= 0_R \cdot s \\ &= 0_R \end{aligned}$$

by Question 31. The other equality is proved similarly.

Question 33. Let R be a ring and let $r \in R$. Show that $(-1_R) \cdot r = -r$.

We want to show that $r + (-1_R) \cdot r = 0_R$.

$$\begin{aligned} r + (-1_R) \cdot r &= 1_R \cdot r + (-1_R) \cdot r \\ &= (1_R + (-1_R)) \cdot r \\ &= (0_R) \cdot r \\ &= 0_R \end{aligned}$$

2.c Subrings and Ideals

We'll now look at two different types of subsets of a ring, each having their own algebraic structure – *subrings* and *ideals*. A *subring* is exactly what you would expect.

Definition 34. Let S be a subset of a ring R. We say S is a *subring* of R if S is itself a ring with:

- $+_S = +_R$
- $\cdot_S = \cdot_R$

- $0_S = 0_R$
- $1_S = 1_R$

Equivalently, S is a subset of R that contains 1_R and is closed under addition, negation, and multiplication.

To motivate the definition of an ideal, let's return to the concept of the *kernel* of a ring homomorphism.

Definition 35. Let $f : R \to S$ be a ring homomorphism. The *kernel* of f is

$$\ker(f) := \{r \in R \mid f(r) = 0_S\}.$$

In other algebraic landscapes, we form quotients by modding out by kernels of maps. The same will be true here. But –

Question 36. Is the kernel of f a subring of R?

No. The issue is that $\ker(f)$ almost never contains 1_R.

On the other hand, it is closed under multiplication by all of R rather than just $\ker(f)$ multiplication (which is all we would expect if $\ker(f)$ were a subring). If $r \in R$ and $k \in \ker(f)$, then

$$\begin{aligned} f(r \cdot k) &= f(r) \cdot f(k) \\ &= f(r) \cdot 0_S \\ &= 0_S. \end{aligned}$$

That is, $r \cdot k$ is also in $\ker(f)$. And we would clearly run into the same conclusion if we were to multiply in the opposite order: $k \cdot r \in \ker(f)$. We also have closure under addition. If $k_1, k_2 \in \ker(f)$, then

$$\begin{aligned} f(k_1 + k_2) &= f(k_1) + f(k_2) \\ &= 0_S + 0_S \\ &= 0_S. \end{aligned}$$

That is, $k_1 + k_2$ is also in $\ker(f)$. We encapsulate the algebraic properties of the kernel of a ring homomorphism in the following definition:

Definition 37. Let R be a ring and I a non-empty subset of R. We say I is a *left ideal* of R if

(1) I is closed under addition, and

(2) if $r \in R$ and $i \in I$, then $r \cdot i$ is also in I.

As the name *left ideal* suggests, when we consider multiplication of ring elements with ideal elements, the convention is to place the ideal elements on the right. Jokes aside, in this setting we view the ring R as scalars, and in a left ideal our scalar multiplication is on the left side of the ideal elements. We define a *right ideal* analogously, with scalar multiplication on the right side of ideal elements. And a *two-sided ideal* is an ideal that is both a left and right ideal. The kernel of a ring homomorphism is always a two-sided ideal.

Question 38. Let I be a left (or right) ideal of a ring R, and let i be an element of I. Is $-i$ also necessarily in I?

Yes. Take I to be a left ideal of R. Since $-1_R \in R$, and $-1_R \cdot i = -i$ by Question 33, $-i$ must be in I.

Question 39. Let I be a left (or right) ideal of a ring R. Is 0_R necessarily in I?

Yes. By definition, I is non-empty and closed under addition. Next, by Question 38 if $i \in I$, then so is $-i$. As a consequence, $0_R = i + (-i)$ must be in I.

Question 40. Let I be a left (or right) ideal of a ring R. If I contains 1_R, show that in fact $I = R$.

Let r be any element of R. If $1_R \in I$, then $r = r \cdot 1_R \in I$, so $I = R$.

With this in mind, there are two ideals that just aren't very interesting. For any ring R, the set $\{0_R\}$ forms an ideal (called the *zero ideal*), as does the ring R itself. This leads to the following definition:

Definition 41. An ideal I of a ring R is called a *proper ideal* if it is neither the zero ideal nor R itself.

Proposition 42. *Let R be a ring and I a left (or right) ideal of R. Define a relation $\sim_I$ on R as follows. For $r, s \in R$,*

$$r \sim_I s \quad \text{if} \quad r + (-s) \in I.$$

This relation $\sim_I$ is an equivalence relation on R.

Proof. We want to show that this relation is:

(1) Reflexive. For all $r \in R$, we have $r \sim_I r$.

(2) Symmetric. For all $r, s \in R$, if $r \sim_I s$ then $s \sim_I r$.

(3) Transitive. For all $r, s, t \in R$, if $r \sim_I s$ and $s \sim_I t$, then $r \sim_I t$.

(1) We have already shown in Question 39 that $0_R \in I$, so $r + (-r) = 0_R \in I$ and $r \sim_I r$.

(2) If $r \sim_I s$, then $r + (-s) \in I$. But by Question 38, $-(r + (-s))$ must be in I if $r + (-s)$ is. Observe:

$$\begin{aligned}(r + (-s)) + (s + (-r)) &= r + ((-s) + s) + (-r) \\ &= -(r + 0_R + (-r)) \\ &= r + (-r) \\ &= 0_R.\end{aligned}$$

That is, $s + (-r) = -(r + (-s))$, so $s + (-r)$ must be in I if $r + (-s)$ is. $r \sim_I s$ implies $s \sim_I r$.

(3) If $r \sim_I s$ and $s \sim_I t$, then $r + (-s) \in I$ and $s + (-t) \in I$. By definition, ideals are closed under addition, so

$$(r + (-s)) + (s + (-t)) \in I.$$

Let's simplify.

$$\begin{aligned}(r + (-s)) + (s + (-t)) &= r + ((-s) + s) + (-t) \\ &= r + 0_R + (-t) \\ &= r + (-t)\end{aligned}$$

So, if $r \sim_I s$ and $s \sim_I t$, then $r \sim_I t$ as well. □

As you will recall from Math 310, an equivalence relation on a set induces a partition of that set. The blocks of this partition are the equivalence classes. We denote the set of equivalence classes by R/I and call it the *quotient of R by I*. If $r \in R$, we'll denote its equivalence class by $\overline{r}$.

Question 43. Let R be a ring and I a left (or right) ideal of R. Is R/I necessarily a ring? Can you introduce some condition to I that will ensure R/I is a ring?

Not necessarily. Take I to be a left ideal. The problem is the multiplication. If R/I is going to be a ring, it must have well-defined multiplication. Suppose $r_1 \sim_I r_2$, *i.e.* $r_1 + (-r_2) = I$. Then for R/I to be a ring, we must have $\overline{r_1} \cdot \overline{s} = \overline{r_2} \cdot \overline{s}$ for all $s \in R$. In other words, we must have

$$(\overline{r_1} \cdot \overline{s}) + (-(\overline{r_2} \cdot \overline{s})) = \overline{0} = I.$$

This holds only if

$$(r_1 \cdot s) + ((-r_2) \cdot s) \in I.$$

That is, it holds only if

$$(r_1 + (-r_2)) \cdot s \in I.$$

We know that $r_1 + (-r_2) = I$, so we have something of the form $i \cdot s$, where $i \in I$ and $s \in R$. So, does that mean we have an element of I as we desired? Unfortunately not. We asked I to be a *left* ideal not a right ideal. The multiplication is in the wrong order. A similar issue would arise if we used a right ideal rather than a left ideal. We can fix the issue by asking I to be a two-sided ideal. In fact, if we take I to be a two-sided ideal, then the quotient map

$$\begin{aligned} \pi : R &\to R/I \\ r &\mapsto \overline{r} \end{aligned}$$

is a ring homomorphism. (You should verify this.)

Question 44. If I were a subring rather than a two-sided ideal, would it still induce an equivalence relation on R? If so, would R/I still be a ring?

It does still induce an equivalence relation – nothing about the proof changes if we take I to be a subring rather that an ideal. However, the quotient would not have a ring structure. The problem is that a proper subring S of a ring R is not closed under multiplication by elements R. So, if I were a subring rather than a two-sided ideal, we would not be able to conclude that $(r_1 + (-r_2)) \cdot s \in I$.

So, the kernel of a ring homomorphism $f : R \to S$ is a two-sided ideal, and we have a quotient map $\pi : R \to R/\ker(f)$ which is a ring homomorphism.

Question 45. What about the image of f? Does it have any special sort of algebraic structure?

It is not an ideal in general – $f(R)$ must contain 1_S but f doesn't need to be surjective. Instead, $f(R)$ is a subring of S. (You should verify this.) This will be relevant in the next section when we discuss the *isomorphism theorems*.

Question 46. Consider the following set of 2×2 real matrices.

$$C := \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$$

Is C a left ideal of $\mathrm{Mat}_{2\times 2}(\mathbb{R})$? Is it a right ideal? A two-sided ideal?

Question 47.

(1) Can you come up with a proper two-sided ideal I of $\mathrm{Mat}_{2\times 2}(\mathbb{R})$?

(2) Can you come up with a proper two-sided ideal J of $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$ that is *not* $I \cap \mathrm{Mat}_{2\times 2}(\mathbb{Z})$?

Ideals are often given in terms of a collection of generators.

Definition 48. Let R be a ring and A a subset of R. The *left ideal generated by* A is the set

$$R \cdot A := \{r_1 \cdot a_1 + r_2 \cdot a_2 + \cdots + r_n \cdot a_n \mid r_i \in R,\, a_i \in A, \text{ and } n \in \mathbb{Z}_{>0}\}.$$

Similarly, the *right ideal generated by* A is the set

$$A \cdot R := \{a_1 \cdot r_1 + a_2 \cdot r_2 + \cdots + a_n \cdot r_n \mid r_i \in R,\, a_i \in A, \text{ and } n \in \mathbb{Z}_{>0}\}$$

and the *two-sided ideal generated by* A is the set

$$R \cdot A \cdot R := \{r_1 \cdot a_1 \cdot s_1 + r_2 \cdot a_2 \cdot s_2 + \cdots + r_n \cdot a_n \cdot s_n \mid r_i, s_i \in R,\, a_i \in A, \text{ and } n \in \mathbb{Z}_{>0}\}$$

Notation 49. If R is a commutative ring and A is the finite set $\{a_1, a_2, \ldots, a_n\}$, these ideals coincide and the standard notation for the ideal generated by A is

$$(a_1, a_2, \ldots, a_n) := R \cdot A = A \cdot R = R \cdot A \cdot R.$$

Question 50. Can you describe the ideal $(4, 6) \subseteq \mathbb{Z}$? Is there a simpler way to express this ideal?

Question 51. Let I and J be left (or right, or two-sided) ideals of a ring R. Which of the following are left (or right, or two-sided) ideals of R?

(1) $I + J := \{i + j \mid i \in I \text{ and } j \in J\}$

(2) $I \cap J$

(3) $I \cup J$

Now let I be a left and J a right ideal of R. Is

$$I \cdot J := \{i_1 \cdot j_1 + i_2 \cdot j_2 + \cdots + i_n \cdot j_n \mid i_k \in I,\, j_k \in J, \text{ and } n \in \mathbb{Z}_{>0}\}$$

a two-sided ideal of R?

Now let's look at each of these in a specific example.

Question 52. Let $I = 4\mathbb{Z}$ and $J = 6\mathbb{Z}$. Describe the following subsets of $\mathbb{Z}$ and say whether each is an ideal of $\mathbb{Z}$.

(1) $I + J$

(2) $I \cap J$

(3) $I \cup J$

(4) $I \cdot J$

Some types of ideals are of particular interest.

Definition 53. A left (or right, or two-sided) ideal I of a ring R is called a *left (or right, or two-sided) principal ideal* if it is generated by a single element. That is, if $I = R \cdot r$ (or $I = r \cdot R$, or $I = R \cdot r \cdot R$) for some $r \in R$.

A word of caution – this isn't a question about how our ideal *is* presented. It's a question of how our ideal *can be* presented.

Question 54. Is $(4, 6)$ a principal ideal of $\mathbb{Z}$?

The next type of ideal we will consider is *usually* described in the context of commutative rings. I've personally needed a non-commutative version of it in my own mathematical life though, so I'll give you that after the standard commutative version. Note that in a commutative ring every ideal is two-sided.

Definition 55. An ideal $P \neq R$ of a commutative ring R is called a *prime ideal* if $r \cdot s \in P$ implies either $r \in P$ or $s \in P$.

Question 56. Can you describe the prime ideals of $\mathbb{Z}$?

Now for the not-necessarily commutative version.[1]

Definition 57. A two-sided ideal $P \neq R$ of a ring R is called a *prime ideal* if whenever I and J are two-sided ideals of R with $I \cdot J \subseteq P$, either $I \subseteq P$ or $J \subseteq P$.

If R is a commutative ring, then Definitions 55 and 57 are actually equivalent.

Proposition 58. *Let R be a commutative ring and P an ideal of R. Then the following statements are equivalent.*

(1) If r and s are elements of R with $r \cdot s \in P$, then $r \in P$ or $s \in P$.

(2) If I and J are ideals of R with $I \cdot J \subseteq P$, then $I \subseteq P$ or $J \subseteq P$.

[1]There are other versions of this as well – such as a definition for one-sided ideals, and a definition that is more similar to Definition 55 – but Definition 57 is the most common definition of prime ideals in not-necessarily commutative rings.

Proof. First we'll show (1) implies (2). So, assume (1) holds, and let I and J be ideals of R with $I \cdot J \subseteq P$. If $I \not\subseteq P$, then there must be some $i \in I$ with $i \notin P$. Note that for every $j \in J$, we have $i \cdot j \in I \cdot J$. But $I \cdot J \subseteq P$, so $i \cdot j \in P$ for all $j \in J$. Since we have assumed $i \notin I$, (1) implies every $j \in J$ is in P, or $J \subseteq P$. So, either $I \subseteq P$ or $J \subseteq P$.

Now let's show (2) implies (1). Assume (2) holds, and let r and s be elements of R with $r \cdot s \in P$. Let I be the ideal generated by r and J the ideal generated by s. Then elements of I and J are of the form $a \cdot r$ and $b \cdot s$ for some a and b in R. So, elements of $I \cdot J$ are of the form

$$\begin{aligned}(a_1 \cdot r) \cdot (b_1 \cdot s) + \cdots + (a_n \cdot r) \cdot (b_n \cdot s) &= (a_1 \cdot b_1) \cdot (r \cdot s) + \cdots + (a_n \cdot b_n) \cdot (r \cdot s) \\ &= (a_1 \cdot b_1 + \cdots + a_n \cdot b_n) \cdot (r \cdot s),\end{aligned}$$

where each a_k, b_k is in R. But $r \cdot s \in P$, and P is an ideal, so $(a_1 \cdot b_1 + \cdots + a_n \cdot b_n) \cdot (r \cdot s)$ is in P. That is, $I \cdot J \subseteq P$. Since we are assuming (2) holds, this implies $I \subseteq P$ or $J \subseteq P$. In other words, the ideal generated by r is contained in P or the ideal generated by s is contained in P. In particular, $r \in P$ or $s \in P$. □

Question 59. Do you think Definitions 55 and 57 are also equivalent for non-commutative rings? Or maybe the conditions of one imply the conditions of the other? Where did we use commutativity in our proof?

We didn't use commutativity to show (1) implies (2), so this implication still holds in the non-commutative case. For the other implication, we used commutativity to combine the a_k and b_k coefficients. And in fact, (2) does *not* imply (1) in non-commutative rings. Ideals satisfying (1) are called *completely prime*. The 0 ideal in $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ is an example of a prime ideal that is not completely prime.

Definition 60. A left (or right, or two-sided) ideal $M \neq R$ of a ring R is called a *maximal left (or right, or two-sided) ideal* if M is not contained in any other proper left (or right, or two-sided) ideal of R.

Question 61. Proof or counter-example:

(1) Every principal ideal is prime.

(2) Every prime ideal is maximal.

(1) Counter-example – Consider the principal ideal $(6) \subseteq \mathbb{Z}$. Then $2 \cdot 3 \in (6)$, but $2 \notin (6)$ and $3 \notin (6)$. Alternatively, we can prove the claim in a less illuminating way by appealing to a technicality of our definition. $(1) = R$ is a principal ideal, but in our definition of a prime ideal P, we explicitly stated that $P \neq R$.

(2) Counter-example – The ideal $(0) \subset \mathbb{Z}$ is prime, but not maximal. For instance,

$$(0) \subsetneq (2) \subseteq \mathbb{Z}.$$

Proposition 62. *Let R be a (not necessarily commutative) ring and M a maximal two-sided ideal of R. Then M is a prime ideal of R.*

Proof. This proof is based on Arturo Magidin's great answer on *Math Stack Exchange*. Let I and J be two-sided ideals of R with $I \not\subseteq M$ and $J \not\subseteq M$. We will show that $I \cdot J \not\subseteq M$, implying M is prime.

Since $I \not\subseteq M$ and $J \not\subseteq M$, the ideals $M + I$ and $M + J$ must properly contain M. Since M is maximal, this implies $M + I = M + J = R$. Then

$$\begin{aligned} R &= R \cdot R \\ &= (M + I) \cdot (M + J) \\ &= M \cdot M + M \cdot J + I \cdot M + I \cdot J \\ &\subseteq M + I \cdot J. \end{aligned}$$

Since $M \neq R$, this implies $I \cdot J \not\subseteq M$. □

Question 63. Let $f : R \to S$ be a ring homomorphism, let I be an ideal of R, and let J be an ideal of S.

(1) Is $f(I) := \{s \in S \mid s = f(i) \text{ for some } i \in I\}$ an ideal of S?

(2) Is $f^{-1}(J) := \{r \in R \mid f(r) \in J\}$ an ideal of R?

(3) If J is principal, is $f^{-1}(J)$ principal as well?

(4) If J is prime, is $f^{-1}(J)$ prime as well?

You can assume R and S are commutative rings for this question. We'll want some tools from the next section to address this question in the non-commutative setting. But, if you want to take a crack at it without making this assumption, I'd be very curious to see what you come up with!

(5) If J is maximal, is $f^{-1}(J)$ maximal as well?

(1) No. It's not in general closed under multiplication by S. For instance, consider the inclusion map

$$\begin{aligned} \iota : \mathbb{Z} &\to \mathbb{Q} \\ n &\mapsto n. \end{aligned}$$

Then if I is any non-zero ideal of $\mathbb{Z}$, $\iota(I)$ is not closed under multiplication by $\mathbb{Q}$.

(2) Yes. First, note that since $0_S \in J$ and $f(0_R) = 0_S$, $f^{-1}(J)$ must be non-empty. Now let x and y be in $f^{-1}(J)$, and let r be in R. Then $f(x)$ and $f(y)$ are in J, and $f(r)$ is in S. Since J is closed under addition, $f(x)+f(y)$ is in J. But f is a ring homomorphism, so $f(x+y) \in J$,

and $x+y \in f^{-1}(J)$. Next, $f(r)\cdot f(x)$ is in J since J is closed under multiplication. Again, f is a ring homomorphism so, $f(r)\cdot f(x) = f(r\cdot x)$ is in J, and $r\cdot x \in f^{-1}(J)$. This shows $f^{-1}(J)$ is an ideal.

(3) No. Consider the map

$$\begin{aligned} f : \mathbb{Z}[x] &\to \mathbb{Z} \\ \sum_{i=0}^{n} a_i x^i &\mapsto a_0. \end{aligned}$$

Then

$$\begin{aligned} f^{-1}(2\mathbb{Z}) &= \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; a_0 \in 2\mathbb{Z} \right\} \\ &= (2, x) \in \mathbb{Z}[x]. \end{aligned}$$

This is a principal ideal whose preimage is not principal.

(4) Yes. Let J be prime and let r_1 and r_2 be elements of R with $r_1 \cdot r_2 \in f^{-1}(J)$. Then $f(r_1 \cdot r_2)$ is in J. Since f is a ring homomorphism, this means $f(r_1)\cdot f(r_2) \in J$. But J is a prime ideal, so this implies $f(r_1) \in J$ or $f(r_2) \in J$. In other words, $r_1 \in f^{-1}(J)$ or $r_2 \in f^{-1}(J)$. That is, $f^{-1}(J)$ is a prime ideal.

(5) No. Consider the inclusion map

$$\begin{aligned} \iota : \mathbb{Z} &\to \mathbb{Q} \\ n &\mapsto n. \end{aligned}$$

The only non-unit in $\mathbb{Q}$ is 0, so (0) is the unique maximal ideal in $\mathbb{Q}$. But $\iota^{-1}((0)) = (0) \subseteq \mathbb{Z}$ is not a maximal ideal – it is properly contained in $(2) \subseteq \mathbb{Z}$ for instance.

Question 63, Items (4) and (5) lie at the foundation of modern algebraic geometry. If we interpret rings as playing the role of the collection of functions on spaces, then points in these space (as you would typically envision points) correspond to maximal ideals in the rings. However, maximal ideals don't interact well with ring homomorphisms. The solution is childsplay – the game isn't going our way, so let's just change the rules. Prime ideals *do* interact well with ring homomorphisms. So, let's just *define* the points in our spaces to be prime ideals in the function rings rather than maximal ideals, and let's define our maps between these spaces to be homomorphisms between their function rings (in the opposite direction to account for the preimage). I'm being rather hand-wavey here because I would have to introduce a lot of background material before stating things carefully. If you're curious though, here is a marginally less hand-wavey description involving some mysterious words that you can look up at your leisure. The spaces we study in modern algebraic geometry are called *schemes*, and the basic building blocks of schemes are *affine schemes*. That is, we construct schemes by gluing together a bunch of affine schemes. And an affine scheme A is the collection of prime ideals in a commutative ring R – which we call the

spectrum of the ring, and denote by $A = \mathrm{Spec}(R)$. A morphism of affine schemes $\mathrm{Spec}(R) \to \mathrm{Spec}(S)$ is a ring homomorphism $S \to R$. In this way, we can build a geometry theory that is cleanly described in algebraic terms. It just took a bit of flexibility in what we were willing to call *geometry*.

2.d Noether's Isomorphism Theorems for Rings

In this subsection we are going to discuss some of the most import, foundational results in abstract algebra. We have discussed before how mathematicians have a habit of disagreeing about names of mathematical objects and concepts. Names associated with mathematical results fall into the same category – in a surprisingly nationalistic way. If an English and a French mathematician independently proved some result, it will probably be named after the English mathematician in England's cultural and linguistic sphere of influence while being named after the French mathematician in France's sphere of influence. Or, if there is no dispute over the provenance of a theorem, this theorem may be called "So-and-so's Theorem" in "So-and-so's" home country – where this is a point of pride – but perhaps not in other countries. The theorems we are about to discuss are due to the German mathematician Emmy Noether.[2] Emmy Noether is the most important female mathematician to date – and this isn't a remotely controversial statement. I was first introduced to these theorems in Germany, where they are naturally proud of Noether. So, I learned them as *Noether's Isomorphism Theorems*. Since then (and outside of Germany), I've generally heard them referred to simply as *The Isomorphism Theorems*.[3] I think Noether deserves to have her name attached to these important theorems, so we'll take up the pronunciation challenge.

I should also mention that analogous theorems hold for many other algebraic structures. The ones we will discuss here are *Noether's Isomorphism Theorems for Rings*. These theorems are generally referred to by number – the "first/ second/ third isomorphism theorem". You'll be shocked to learn however that there isn't actually general agreement about which theorem gets assigned which number. Our numbering and naming here will follow Dummit and Foote, simply out of familiarity for me. As a student I took Abstract Algebra courses using this book.

Theorem 64 (Noether's 1st Isomorphism Theorem)**.** *Let R and S be rings and $f : R \to S$ a ring homomorphism. Then*

(1) The kernel $\ker(f)$ *is a two-sided ideal of R.*

(2) The image $f(R)$ is a subring of S.

(3) The quotient $R/\ker(f)$ *is a ring.*

[2]Her original paper containing these results can be found here. I will post a link to Moodle as well.

[3]Beyond nationalistic explanations, this may be because non-German speakers tend to be at a loss as to how to pronounce her name. If you want to hear it pronounced properly, here is a German-language YouTube video about her.

(4) The quotient map

$$\begin{aligned} \pi : R &\to R/\ker(f) \\ r &\mapsto \overline{r} \end{aligned}$$

is a ring homomorphism.

(5) There is a unique ring homomorphism $\overline{f} : R/\ker(f) \to S$ such that $f = \overline{f} \circ \pi$.

(6) The quotient ring $R/\ker(f)$ is isomorphic to the image $f(R) \subseteq S$.

Proof. We have seen most elements of this claim already. For (1), the kernel of a ring homomorphism was our motivating example for the definition of a two-sided ideal, preceding Definition 37. Next, (2) is precisely the content of Question 45 (which you have certainly done, and would of course be prepared to reproduce on a test). We addressed (3) in Question 43. In answering Question 43, we also made mention of (4) and suggested it would be quite a nice question to put on a test. But, let's take a closer look now. Recall from Definition 18 that we have three properties to check. For all $r_1, r_2 \in R$:

- $\pi(r_1 + r_2) \stackrel{?}{=} \pi(r_1) + \pi(r_2)$
- $\pi(r_1 \cdot r_2) \stackrel{?}{=} \pi(r_1) \cdot \pi(r_2)$
- $\pi(1_R) \stackrel{?}{=} 1_{R/\ker(f)}$

First, we want to know whether $\pi(r_1 + r_2) = \pi(r_1) + \pi(r_2)$. In other words, does the following equality hold?

$$\pi(r_1 + r_2) + (-(\pi(r_1) + \pi(r_2))) \stackrel{?}{=} 0_{R/\ker(f)} = \ker(f)$$

Note that

$$\begin{aligned} \pi(r_1 + r_2) &= \overline{r_1 + r_2} \\ &= \{r \in R \mid (r_1 + r_2) + (-r) \in \ker(f)\}, \end{aligned}$$

and

$$\begin{aligned} \pi(r_1) + \pi(r_2) &= \overline{r_1} + \overline{r_2} \\ &= \{r' \in R \mid r_1 + (-r') \in \ker(f)\} + \{r'' \in R \mid r_2 + (-r'') \in \ker(f)\} \\ &= \{(r' + r'') \in R \mid r_1 + (-r') \in \ker(f) \text{ and } r_2 + (-r'') \in \ker(f)\}. \end{aligned}$$

Now, let $r \in \pi(r_1 + r_2)$, $r' \in \pi(r_1)$, and $r'' \in \pi(r_2)$. We want to know whether $r + (-(r' + r''))$ is in $\ker(f)$. Observe:

$$\begin{aligned} r - (r' + r'') &= (-r') + (-r'') + (-(-r)) \\ &= (r_1 + (-r')) + (r_2 + (-r'')) + (-((r_1 + r_2) + (-r))). \end{aligned}$$

But this is a sum of three elements of $\ker(f)$, so $r + (-(r' + r''))$ is indeed in $\ker(f)$.

Next, we want to know whether $\pi(r_1 \cdot r_2) = \pi(r_1) \cdot \pi(r_2)$. In other words, does the following equality hold?

$$\pi(r_1 \cdot r_2) + (-(\pi(r_1) \cdot \pi(r_2))) \stackrel{?}{=} 0_{R/\ker(f)} = \ker(f)$$

Note that

$$\begin{aligned} \pi(r_1 \cdot r_2) &= \overline{r_1 \cdot r_2} \\ &= \{r \in R \mid (r_1 \cdot r_2) + (-r) \in \ker(f)\}, \end{aligned}$$

$$\begin{aligned} \pi(r_1) &= \overline{r_1} \\ &= \{r' \in R \mid r_1 + (-r') \in \ker(f)\}, \end{aligned}$$

and

$$\begin{aligned} \pi(r_2) &= \overline{r_2} \\ &= \{r'' \in R \mid r_2 + (-r'') \in \ker(f)\}. \end{aligned}$$

Now, let $r \in \pi(r_1 \cdot r_2)$, $r' \in \pi(r_1)$, and $r'' \in \pi(r_2)$. Then $r = r_1 \cdot r_2 + k_{12}$ for some $k_{12} \in \ker(f)$, $r' = r_1 + k_1$ for some $k_1 \in \ker(f)$, and $r'' = r_2 + k_2$ for some $k_2 \in \ker(f)$. We want to know whether $r + (-(r' \cdot r''))$ is in $\ker(f)$.

$$\begin{aligned} r + (-(r' \cdot r'')) &= ((r_1 \cdot r_2) + k_{12}) + (-((r_1 + k_1) \cdot (r_2 + k_2))) \\ &= ((r_1 \cdot r_2) + k_{12}) + (-((r_1 \cdot r_2) + (r_1 \cdot k_2) + (k_1 \cdot r_2) + (k_1 \cdot k_2))) \\ &= k_{12} + (-(r_1 \cdot k_2)) + (-(k_1 \cdot r_2)) + (-(k_1 \cdot k_2)) \end{aligned}$$

Since $\ker(f)$ is a two-sided ideal, this must be in $\ker(f)$, as desired.

To finish off (4), we need to verify that $\pi(1_R) = 1_{R/\ker(f)}$. That is, we must show that for all $\overline{r} \in R/\ker(f)$, we have

$$\overline{r} \cdot \pi(1_R) = \overline{r} = \pi(1_R) \cdot \overline{r}.$$

Now,

$$\begin{aligned} \overline{r} &= \{r' \in R \mid r + (-r') \in \ker(f)\} \\ &= \{r' \in R \mid r' = r + k \text{ for some } k \in \ker(f)\}. \end{aligned}$$

and

$$\begin{aligned} \pi(1_R) = \overline{1_R} &= \{r \in R \mid 1_R + (-r) \in \ker(f)\} \\ &= \{r \in R \mid r = 1_R + k \text{ for some } k \in \ker(f)\}. \end{aligned}$$

So, consider a product of the form $(r + k) \cdot (1_R + k')$, where k and k' are in $\ker(f)$.

$$\begin{aligned} (r + k) \cdot (1_R + k') &= (r \cdot 1_R) + (r \cdot k') + (k \cdot 1_R) + (k \cdot k') \\ &= r + (r \cdot k') + (k \cdot 1_R) + (k \cdot k') \end{aligned}$$

The last three terms are in all in $\ker(f)$, so this is in $\overline{r}$ as desired. The product in the opposite order is similar.

Now for Item (5). Define a map

$$\begin{aligned} \overline{f} : R/\ker(f) &\to S \\ \overline{r} &\mapsto f(r). \end{aligned}$$

We need to make sure this is well-defined. That is, if $r' \in \overline{r}$, do we have $f(r') = f(r)$? Well, if $r' \in \overline{r}$, then $r' = r + k$ for some $k \in \ker(f)$. But then

$$f(r') = f(r + k) = f(r) + f(k) = f(r) + 0_S = f(r).$$

So, $\overline{f}$ is indeed well-defined.

Next, given this definition it is clear that $f(r) = \overline{f}(\pi(r))$ and that $\overline{f}$ is the unique map with this property. Furthermore, given Item 4 and the fact that f is itself a homomorphism, it is clear that $\overline{f}$ satisfies the properties of a homomorphism as well.

Finally, for (6), we just need $\overline{f}$ to be injective. It automatically surjects onto its image. But by construction, the kernel of $\overline{f}$ is $\ker(f) = 0_{R/\ker(f)}$, so $\overline{f}$ is injective and $R/\ker(f)$ is isomorphic to $f(R)$. □

Example 65. Consider the ring homomorphism ϕ defined by

$$\begin{aligned} \mathbb{Z}[x, y] &\to \mathbb{Z}[z] \\ x &\mapsto z^2 \\ y &\mapsto z^2. \end{aligned}$$

Can you describe $\ker(\phi)$, $\mathbb{Z}[x, y]/\ker(\phi)$, and $\phi(\mathbb{Z}[x, y])$?

The kernel $\ker(\phi)$ is the two-sided ideal of $\mathbb{Z}[x, y]$ generated by $(x - y)$. The quotient ring $\mathbb{Z}[x, y]/\ker(\phi)$ is then the polynomial ring in two variables x and y over the integers, where the variables are subject to the relation $x = y$. The result is naturally isomorphic to a polynomial ring in one variable, say x or y – no need to record two variables if we will just set them equal to each other anyway. The image $\phi(\mathbb{Z}[x, y])$ is the subring $\mathbb{Z}[z^2] \subseteq \mathbb{Z}[z]$. This is also clearly a polynomial ring in one variable – z^2.

Now let's make the previous example slightly more interesting.

Example 66. Consider the ring homomorphism ϕ defined by

$$\begin{aligned} \mathbb{Z}[x, y] &\to \mathbb{Z}[z] \\ x &\mapsto z^2 \\ y &\mapsto z^3. \end{aligned}$$

Can you describe $\ker(\phi)$, $\mathbb{Z}[x, y]/\ker(\phi)$, and $\phi(\mathbb{Z}[x, y])$?

The kernel $\ker(\phi)$ is the two-sided ideal of $\mathbb{Z}[x,y]$ generated by $(x^3 - y^2)$. The quotient ring $\mathbb{Z}[x,y]/\ker(\phi)$ is then the polynomial ring in two variables x and y over the integers, where the variables are subject to the relation $x^3 = y^2$. The image $\phi(\mathbb{Z}[x,y])$ is the subring $\mathbb{Z}[z^2, z^3] \subseteq \mathbb{Z}[z]$.

This example is related to an important example from algebraic geometry called the *cuspidal cubic*. This is a singular cubic curve, generally defined over the complex numbers rather than the integers. Now let's look at an example that explicitly deals with the complex numbers.

Example 67. Use Noether's 1st Isomorphism Theorem to show that $\mathbb{C}$ is isomorphic to $\mathbb{R}[x]/(x^2+1)$.

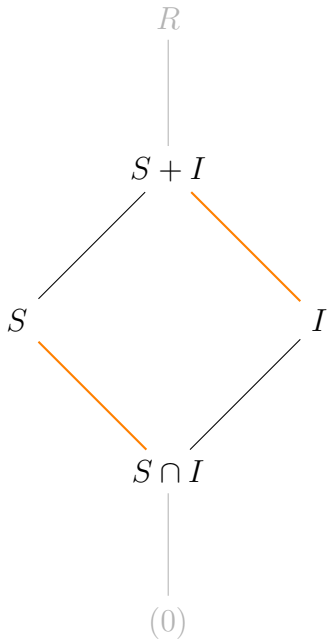
Theorem 68 (Noether's 2nd Isomorphism Theorem/ Diamond Isomorphism Theorem)**.** *Let R be a ring, S a subring of R, and I a two-sided ideal of R. Then:*

(1) $S + I$ *is a subring of* R.

(2) $S \cap I$ *is a two-sided ideal of* S.

(3) $(S+I)/I \cong S/(S \cap I)$.

Before we get into the proof, what's with the name *"Diamond Isomorphism Theorem"*? Well, let's consider the following poset of subsets of R, ordered by containment.



This theorem deals with the diamond in the middle. The pair of orange edges represent the pair of ideals in subrings of R yielding isomorphic quotients.

Proof. We begin with Item (1). First note that since 0_R is in I, $S \subseteq S + I$. In particular, $1_R \in S + I$. Next, an arbitrary element of $S + I$ is of the form $s + i$, where $s \in S$ and $i \in I$. Let $(s_1 + i_1)$ and $(s_2 + i_2)$ be a pair of arbitrary elements of $S + I$. Then

$$(s_1 + i_1) + (s_2 + i_2) = (s_1 + s_2) + (i_1 + i_2).$$

Since S and I are both closed under addition, this is also of the form $s + i$. That is, $S + I$ is closed under addition. Next, both S and I are closed under negation. So, if $s \in S$ and $i \in I$,

$$-(s + i) = (-s) + (-i)$$

must be in $S+I$. This means $S+I$ is closed under negation. For closure under multiplication, we consider the following product:

$$(s_1 + i_1) \cdot (s_2 + i_2) = (s_1 \cdot s_2) + (s_1 \cdot i_2) + (i_1 \cdot s_2) + (i_1 \cdot i_2).$$

The first term on the right hand side is in S since S is closed under multiplication. The remaining three terms are all in I since I is closed under left and right scalar multiplication. Then this product also lives in $S + I$. We conclude that $S + I$ is a subring of R.

Now onto Item (2). First, $0_R \in S \cap I$, so $S \cap I$ is non-empty. Next, since both S and I are closed under addition, a sum of elements in $S \cap I$ must also be in $S \cap I$. $S \cap I$ is closed under addition. Finally, since S is closed under multiplication and I is closed under left and right scalar multiplication. So, if $s \in S$ and $i \in S \cap I$, any product of the form $s \cdot i$ or $i \cdot s$ must lie in $S \cap I$. Then $S \cap I$ is a two-sided ideal of S.

Onto Item (3). For this, we will make use of Theorem 64. Let f be the following ring homomorphism:

$$\begin{aligned} f : S + I &\to S/(S \cap I) \\ s + i &\mapsto \overline{s}. \end{aligned}$$

Note that this *is* clearly a ring homomorphism:

$$f(1_{S+I}) = f(1_R) = \overline{1_R} = \overline{1_S} = 1_{S/(S \cap I)}$$

$$\begin{aligned} f\left((s_1 + i_1) + (s_2 + i_2)\right) &= f\left((s_1 + s_2) + (i_1 + i_2)\right) \\ &= \overline{s_1 + s_2} \\ &= \overline{s_1} + \overline{s_2} \\ &= f(s_1 + i_1) + f(s_2 + i_2) \end{aligned}$$

$$\begin{aligned} f\left((s_1 + i_1) \cdot (s_2 + i_2)\right) &= f\left((s_1 \cdot s_2) + ((s_1 \cdot i_2) + (i_1 \cdot s_2) + (i_1 \cdot i_2))\right) \\ &= \overline{s_1 \cdot s_2} \\ &= \overline{s_1} \cdot \overline{s_2} \\ &= f(s_1 + i_1) \cdot f(s_2 + i_2) \end{aligned}$$

Moreover, it is clearly surjective – for any element $\overline{s}$ in $S/(S \cap I)$, we have $\overline{s} = f(s+0)$ for instance. And it has kernel $\ker(f) = I = 0_S + I$. Then Theorem 64 implies

$$(S+I)/I \cong S/(S \cap I).$$

□

Theorem 69 (Noether's 3rd Isomorphism Theorem)**.** *Let R be a ring and I a two-sided ideal of R. Then:*

(1) If S is a subring of R with $I \subseteq S$, then S/I is a subring of R/I.

(2) Every subring of R/I is of the form S/I for some subring S of R with $I \subseteq S$.

(3) If J is a left (or right, or two-sided) ideal of R with $I \subseteq J$, then J/I is a left (or right, or two-sided) ideal of R/I.

(4) Every left (or right, or two-sided) ideal of R/I is of the form J/I for some left (or right, or two-sided) ideal J of R with $I \subseteq J$.

(5) If J is a two-sided ideal of R with $I \subseteq J$, then $(R/I)/(J/I) \cong R/J$.

Proof. (1) First we want to verify that S/I is indeed a ring. This is the case if I is a two-sided ideal of S. Since I is a two-sided ideal of R, it is closed under addition and left and right R-scalar multiplication. We just need it to also be closed under left and right S-scalar multiplication – which is true *a fortiori* since S is a subring of R. Next, we want S/I to be a subset of R/I. Let's recall that set theoretically, R/I is a partition of R. The elements of R/I are equivalence classes in R. Specifically,

$$\overline{r} = \{r + i \mid i \in I\}.$$

Since we have the inclusions $I \subseteq S \subseteq R$, if $s \in S \subseteq R$, then $(s+i) \in S \subseteq R$ for all $i \in I$. If $r \in R$ is *not* in S, then $(r+i) \notin S$ for all $i \in I$. That is, the elements of S/I are precisely the elements $\overline{s}$ of R/I which are equivalence classes of some $s \in S$. The addition and multiplication operations are defined identically for R/I and S/I. We also have

$$0_{S/I} = \overline{0_S} = \overline{0_R} = 0_{R/I},$$

and

$$1_{S/I} = \overline{1_S} = \overline{1_R} = 1_{R/I}.$$

So, S/I is a subring of R/I.

(2) Now let A be a subring of R/I, and let π be the quotient map $\pi : R \to R/I$. Define $S := \pi^{-1}(A)$. We want to show that S is a subring of R containing I. To see that S contains I, we simply note that $0_A = 0_{R/I}$, and $\pi^{-1}\left(0_{R/I}\right) = I$. Next, to see that S is a subring of R,

we will check that S contains 1_R and is closed under addition, negation, and multiplication. Since $1_A = 1_{R/I} = \pi(1_R)$, we have that $1_R \in S$. Now let s_1 and s_2 be elements of S, say with $s_1 \in \pi^{-1}(a_1)$ and $s_2 \in \pi^{-1}(a_2)$. Then $\pi(s_1+s_2) = \pi(s_1)+\pi(s_2) = a_1+a_2$, which is in A since A is closed under addition. So $s_1 + s_2 \in \pi^{-1}(a_1 + a_2)$, and S is closed under addition. Next, $-s_1 \in \pi^{-1}(-a_1)$ and S is closed under negation. Finally, $\pi(s_1 \cdot s_2) = \pi(s_1) \cdot \pi(s_2) = a_1 \cdot a_2$, which is in A since A is closed under multiplication. That is, $s_1 \cdot s_2 \in \pi^{-1}(a_1 + a_2)$, and S is closed under multiplication. We conclude that S is a subring of R containing I.

(3) Let J be a left ideal of R. We want to show that J/I is a left ideal of R/I. The first step is to see that J/I is a non-empty subset of R/I. This is identical to our proof that S/I is a subset of R/I in (1). Since we have the inclusions $I \subseteq J \subseteq R$, if $j \in J \subseteq R$, then $(j+i) \in J \subseteq R$ for all $i \in I$. If $r \in R$ is *not* in J, then $(r+i) \notin J$ for all $i \in I$. That is, the elements of J/I are precisely the elements $\overline{j}$ of R/I which are equivalence classes of some $j \in J$. So it is indeed a subset, and it is non-empty – since $I \subseteq J$, $0_{R/I} \in J$. Next, we want to see that J/I is closed under addition. If $\overline{j_1}$ and $\overline{j_2}$ are in J/I, then as cosets we have

$$\begin{aligned}
\overline{j_1} + \overline{j_2} &= \{j_1 + i_1 \mid i_1 \in I\} + \{j_2 + i_2 \mid i_2 \in I\} \\
&= \{(j_1 + i_1) + (j_2 + i_2) \mid i_1, i_2 \in I\} \\
&= \{(j_1 + j_2) + (i_1 + i_2) \mid i_1, i_2 \in I\} \\
&= \{(j_1 + j_2) + i \mid i \in I\} \\
&= \overline{j_1 + j_2}.
\end{aligned}$$

So J/I is closed under addition. Finally, we want to see that J/I is closed under left R/I-scalar multiplication. If $\overline{r} \in R/I$ and $\overline{j} \in J/I$,

$$\begin{aligned}
\overline{r} \cdot \overline{j} &= \{r + i \mid i \in I\} \cdot \{j + i' \mid i' \in I\} \\
&= \{(r + i) \cdot (j + i') \mid i, i' \in I\} \\
&= \{(r \cdot j) + (r \cdot i') + (i \cdot j) + (i \cdot i') \mid i, i' \in I\} \\
&= \{(r \cdot j) + i'' \mid i'' \in I\} \\
&= \overline{r \cdot j}.
\end{aligned}$$

So J/I is closed under left R/I-scalar multiplication, and J/I is a left ideal of R/I. The right ideal and two-sided ideal cases are proved *mutatis mutandis*.

(4) Now let K be a left ideal of R/I, and let π be the quotient map $\pi : R \to R/I$. Define $J := \pi^{-1}(K)$. We want to show that J is a left ideal of R containing I. To see that J contains I, we simply note that $\left(0_{R/I}\right) \in K$ and $I = \pi^{-1}\left(0_{R/I}\right)$, so

$$I = \pi^{-1}\left(0_{R/I}\right) \subseteq \pi^{-1}(K) =: J.$$

Next, to see that J is a left ideal of R, we will check that J is closed under both addition and left R-scalar multiplication. (J is automatically non-empty since we have just seen it contains I.) Now let j_1 and j_2 be elements of S, say with $j_1 \in \pi^{-1}(k_1)$ and $j_2 \in \pi^{-1}(k_2)$. Then $\pi(j_1 + j_2) = \pi(j_1) + \pi(j_2) = k_1 + k_2$, which is in K since K is closed under addition. So $j_1 + j_2 \in \pi^{-1}(k_1 + k_2)$, and J is closed under addition. Finally, for r in R we have

$\pi(r \cdot j_1) = \pi(r) \cdot \pi(j_1) = \overline{r} \cdot k_1$, which is in K since K is closed under left R/I-scalar multiplication. That is, $r \cdot j_1 \in \pi^{-1}(\overline{r} \cdot k_1)$, and J is closed under left R-scalar multiplication. We conclude that J is a left ideal of R containing I. The right ideal and two-sided ideal cases are proved *mutatis mutandis*.

(5) Now let J be a two-sided ideal of R with $I \subseteq J$. As with the final point of Theorem 68, we will use Theorem 64 to prove the isomorphism $(R/I)/(J/I) \cong R/J$. There are several quotient rings here, so to avoid confusion we'll use different notation for the equivalence classes in each.

- $\overline{r}$ will denote an element of R/I.
- $\overline{\overline{r}}$ will denote an element of $(R/I)/(J/I)$.
- $[r]$ will denote an element of R/J.

Now consider the map

$$\begin{aligned} f : R/I &\to R/J \\ \overline{r} &\mapsto [r]. \end{aligned}$$

I claim that this is a surjective ring homomorphism. Let's first note that it is a well-defined map. If $\overline{r} = \overline{r'}$, then $(r - r') \in I$. But $I \subseteq J$, so $(r - r') \in J$ as well, and $[r] = [r']$. Next, we have

$$\begin{aligned} f(\overline{r_1} + \overline{r_2}) &= f(\overline{r_1 + r_2}) \\ &= [r_1 + r_2] = [r_1] + [r_2] \\ &= f(\overline{r_1}) + f(\overline{r_2}), \end{aligned}$$

$$\begin{aligned} f(\overline{r_1} \cdot \overline{r_2}) &= f(\overline{r_1 \cdot r_2}) \\ &= [r_1 \cdot r_2] \\ &= [r_1] \cdot [r_2] \\ &= f(\overline{r_1}) \cdot f(\overline{r_2}), \end{aligned}$$

and

$$f\left(1_{R/I}\right) = f\left(\overline{1_R}\right) = [1_R] = 1_{R/J}.$$

So, f is indeed a ring homomorphism. To see that f is surjective, let $[r]$ be any element of R/J. Since $I \subseteq J$, $r \sim_I r'$ implies $r \sim_J r'$. That is, the equivalence class $\overline{r}$ in R is contained in the equivalence class $[r]$. Then for any r' in the equivalence class $[r] \subseteq R$, we have $f(\overline{r'}) = [r]$. So, Theorem 64 implies $(R/I)/\ker(f) \cong R/J$. All that remains is to see that $\ker(f) = J/I$, in which case we could conclude that

$$\begin{aligned} \overline{f} : (R/I)/(J/I) &\mapsto R/J \\ \overline{\overline{r}} &\mapsto [r] \end{aligned}$$

is an isomorphism. But the kernel of f is the set of elements $\overline{r}$ of R/I that are sent to $0_{R/J} = [0_R]$ by f. The equivalence class $[0_R]$ is precisely $J \subset R$. So, $\overline{r} \in \ker(f)$ if and only if $\overline{r} \in J/I$. □

For an example of both Theorem 68 and Theorem 69, we will take look at an interesting number system called the *Gaussian integers*. It is due to Johann Carl Friedrich Gauss in 1832. The Gaussian integers are complex numbers $a + ib$ with both a and b in $\mathbb{Z}$. That is, the Gaussian integers are $\mathbb{Z}[i]$.

Example 70. Let R be the ring of Gaussian integers $\mathbb{Z}[i]$, S the subring $\mathbb{Z} \subseteq \mathbb{Z}[i]$, I the ideal $(5 - i) \subseteq \mathbb{Z}[i]$, and J the ideal $(1 + i) \subseteq \mathbb{Z}[i]$.

(1) Describe the subsets $S + I$ and $S \cap I$ of R as simply as possible.

(2) Is $S + I$ a subring of R? Is it an ideal of R? Prove each claim.

(3) Is $S \cap I$ a subring of R? Is it an ideal of R? Prove each claim.

(4) Explicitly describe the quotient rings $(S+I)/I$ and $S/(S\cap I)$, then give an isomorphism of these rings.

(5) Show that $I \subseteq J$.

(6) Explicitly describe the quotient ring R/I.

(7) Verify that J/I is an ideal of R/I, then explicitly describe the quotient ring $(R/I)/(J/I)$.

(8) Explicitly describe the quotient ring R/J.

(9) Give an isomorphism of $(R/I)/(J/I)$ and R/J.

2.e Some special types of rings

So far our focus has been on rings, broadly speaking. Sometimes our interest will be quite a bit narrower than *rings*. That is, we may have reason to look only at those rings that satisfy some additional properties – perhaps rings with commutative multiplication, or rings where every non-zero element has a multiplicative inverse, or rings in which $r \cdot s = 0$ implies either $r = 0$ or $s = 0$. When we have additional properties such as these, we can push our theory further. Simply speaking, more statements are true in the specialized setting than in the fully general setting. The point of this section is to introduce you to some special types of rings. We'll go over their definitions and highlight some of their key features. Unfortunately, we are just about out of time, so this section will be disappointingly brief. Plenty of important material will be omitted as will some proofs.

The first example is one we have defined already.

Definition 71. A *commutative ring* is a R in which the multiplication operation is commutative. That is, for all $r, s \in R$, we have $r \cdot s = s \cdot r$.

These are the rings at the heart of modern algebraic geometry – an affine scheme is by definition the spectrum of a commutative ring.

Next,

Definition 72. A non-zero commutative ring R is called an *integral domain* if for all $r, s \in R$ we have:

$$r \cdot s = 0 \qquad \Longrightarrow \qquad r = 0 \text{ or } s = 0.$$

When we have an element r in a ring R such that $r \cdot s = 0_R$ for some nonzero s, we call r a (left) *zero divisor* (since r divides 0). (Right zero-divisors are defined analogously.) So, we can also say that an integral domain is a commutative ring without non-zero zero-divisors. Or, an integral domain is a commutative ring in which the zero ideal is prime.

Question 73. The rings that you interact with most frequently ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ...) are examples of integral domains. Can you give an example of a commutative ring that is *not* a integral domain?

One option is $\mathbb{Z}/4\mathbb{Z}$. Note that $\overline{2} \cdot \overline{2} = \overline{0}$.

Question 74. For which n is $\mathbb{Z}/n\mathbb{Z}$ an integral domain?

Proposition 75. *Let R be a commutative ring and I and ideal of R. Then the quotient ring R/I is an integral domain if and only if I is a prime ideal of R.*

Proof. Let π be the quotient ring homomorphism $\pi : R \to R/I$. This is surjective by construction, so we can write any element of R/I as $\pi(r)$ for some $r \in R$. Consider an arbitrary product $\pi(r_1) \cdot \pi(r_2)$. Note that this product is $0_{R/I}$ if and only if $r_1 \cdot r_2 \in I$:

- If $r_1 \cdot r_2 \in I = \ker(\pi)$, then $\pi(r_1) \cdot \pi(r_2) = \pi(r_1 \cdot r_2) = 0_{R/I}$.
- If $\pi(r_1) \cdot \pi(r_2) = 0_{R/I}$, then $\pi(r_1 \cdot r_2) = \pi(r_1) \cdot \pi(r_2) = 0_{R/I}$, and $r_1 \cdot r_2 \in \pi^{-1}(0_{R/I}) = I$.

Now suppose I is prime. Then for every pair of elements r_1 and r_2 in R, the inclusion $r_1 \cdot r_2 \in I$ implies either $r_1 \in I$ or $r_2 \in I$. It follows that for every pair of elements $\pi(r_1)$ and $\pi(r_2)$ in R/I, the equality $\pi(r_1) \cdot \pi(r_2) = 0_{R/I}$ implies either $\pi(r_1) = 0_{R/I}$ or $\pi(r_2) = 0_{R/I}$. That is, R/I is an integral domain.

Next, suppose R/I is an integral domain. Then for every pair of elements $\pi(r_1)$ and $\pi(r_2)$ in R/I, the equality $\pi(r_1) \cdot \pi(r_2) = 0_{R/I}$ implies either $\pi(r_1) = 0_{R/I}$ or $\pi(r_2) = 0_{R/I}$. It follows that for every pair of elements r_1 and r_2 in R, the inclusion $r_1 \cdot r_2 \in I$ implies either $r_1 \in I$ or $r_2 \in I$. That is, I is a prime ideal. □

There is also a not-necessarily-commutative version of an integral domain, which is sometimes just called a *domain*, but the commutative case gets a lot more attention. This is probably because the commutative case is important in algebraic geometry, where integral domains correspond to *"reduced"* and *"irreducible"* affine schemes. (Recall that affine schemes are the building blocks for the spaces we study in modern algebraic geometry – called schemes.)

Proposition 76. *Let R be an integral domain. Then so is $R[x_1, \ldots, x_n]$.*

Definition 77. A *division ring* is a non-zero ring R in which every non-zero element has a multiplicative inverse in R. That is, for all non-zero $r \in R$, there is an element $r^{-1} \in R$ with $r \cdot r^{-1} = 1_R = r^{-1} \cdot r$. In other words, every non-zero $r \in R$ is a unit in R.

The name is pretty self-explanatory – in a division ring, we can divide by non-zero elements.

Example 78. $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all examples of commutative division rings. $\mathbb{Z}$ is not a division ring since all non-zero elements other than 1 and -1 are non-units. The quaternions $\mathbb{H}$ are a non-commutative division ring.

Question 79. For which n is $\mathbb{Z}/n\mathbb{Z}$ a division ring?

The commutative case is of particular interest.

Definition 80. A commutative division ring is called a *field*.

Fields are the most studied type of ring, and for good reason. If you start with *rings* and then start adding on all of the nice properties you can imagine, you wind up with *fields*. In fact:

Proposition 81. *Every field is an integral domain.*

Proof. Let $\Bbbk$ be a field. Then $\Bbbk$ is a non-zero commutative ring and for every nonzero $r \in \Bbbk$ there is some element $r^{-1} \in \Bbbk$ with $r \cdot r^{-1} = 1_\Bbbk$. Suppose there is some $s \in \Bbbk$ with $s \cdot r = 0_\Bbbk$. Then we have

$$0_\Bbbk = 0_\Bbbk \cdot r^{-1} = (s \cdot r) \cdot r^{-1} = s \cdot \left(r \cdot r^{-1}\right) = s \cdot 1_\Bbbk = s.$$

That is, for any non-zero r in $\Bbbk$, the equality $s \cdot r = 0_\Bbbk$ implies $s = 0_\Bbbk$. So, $\Bbbk$ is an integral domain. □

Example 82. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}/p\mathbb{Z}$ for p a prime are all examples of fields. $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ for n non-prime are not fields since both have non-zero non-units. The quaternions $\mathbb{H}$ are not a field because this division ring is not commutative.

3 Modules and Algebras

Many different algebraic structures are built on top of rings. In fact, at the start of a math discussion or math paper, we will often specify which ring we are "working over". In this very brief section we will discuss two algebraic structures built on top of rings – *modules* and *algebras*.

To make the definition of a module more concise, I will first introduce a different term from Abstract Algebra I.

Definition 83. An Abelian group is a non-empty set G together with a commutative associative binary operation

$$+ : G \times G \to G$$

such that the following properties hold.

(1) *(Identity element)* There is some element 0_G in G with $0_G + g = g$ for all $g \in G$.

(2) *(Inverses)* For all g in G, there is some element $-g$ in G with $g + (-g) = 0_G$.

When (as suggested by the notation above) we view the binary operation as addition, we call G an *additive Abelian group*. Note that "*additive*" is only referring to our interpretation of the operation and has nothing at all to do with the algebraic structure. If we just replaced the "+" symbol with a "$\cdot$" symbol, we'd think of it as multiplication and call it a *multiplicative Abelian group*.

Definition 84. Let R be a ring. A *left R-module* is an additive Abelian group M together with an operation

$$\cdot : R \times M \to M$$

such that for all $r_1, r_2 \in R$ and $\mathbf{m}_1, \mathbf{m}_2 \in M$ we have:

(1) $r_1 \cdot (\mathbf{m}_1 + \mathbf{m}_2) = (r_1 \cdot \mathbf{m}_1) + (r_1 \cdot \mathbf{m}_2)$

(2) $(r_1 + r_2) \cdot \mathbf{m}_1 = (r_1 \cdot \mathbf{m}_1) + (r_2 \cdot \mathbf{m}_1)$

(3) $(r_1 \cdot r_2) \cdot \mathbf{m}_1 = r_1 \cdot (r_2 \cdot \mathbf{m}_1)$

(4) $1_R \cdot \mathbf{m}_1 = \mathbf{m}_1$

Right R-modules are defined analogously. Note that if R is commutative, we can easily identify left and right R-modules. The distinction amounts to an aesthetic choice rather than conveying anything mathematically meaningful. So, for commutative rings we will often drop the *left* and *right* qualifiers.

Question 85. You have all seen examples of left R-modules before. Can you think of any?

Definition 86. Let $\Bbbk$ be a field. Then a $\Bbbk$-module is called a $\Bbbk$-*vector space*.

Of course, not all rings of interest are fields.

Example 87. The following are examples of $\mathbb{Z}$-modules.

- A rank n lattice. (Think of the integral points $\mathbb{Z}^n$ in an n-dimensional real vector space $\mathbb{R}^n$.)
- A polynomial ring with coefficients in $\mathbb{Z}$, say $\mathbb{Z}[x_1, x_2, \cdots, x_n]$.
- More generally, *any* Abelian group.

Question 88. Let R be a ring, S a subring of R, and I a left ideal of R. Is S a left R-module? Is I a left R-module?

Sometime our R-modules come with some additional algebraic structure. For example, if R is any ring, then $R[x_1, \ldots, x_n]$ is a left R-module. But $R[x_1, \ldots, x_n]$ is also itself a ring. This leads us to our final topic.

Definition 89. Let R be a commutative ring. An R-*algebra* is an R-module A that is itself a ring[4] such that for all $r_1, r_2 \in R$ and $\mathbf{a}_1, \mathbf{a}_2 \in A$, we have

$$(r_1 \cdot \mathbf{a}_1) \cdot (r_2 \cdot \mathbf{a}_2) = (r_1 \cdot r_2) \cdot (\mathbf{a}_1 \cdot \mathbf{a}_2).$$

Alternatively, we can define R-algebras in terms of ring homomorphisms. We'll need one additional notion first:

Definition 90. Let A be a ring. The *center* of A, denoted $Z(A)$ is

$$Z(A) := \{a \in A \mid a \cdot b = b \cdot a \text{ for all } b \in A\}.$$

So $Z(A)$ is the set of elements that commute with every other element.

Definition 91. Let R be a commutative ring. An R-algebra is a ring A together with a ring homomorphism $\phi : R \to Z(A)$.

Question 92. Can you describe the quaternions $\mathbb{H}$ as an $\mathbb{R}$-algebra? What is $Z(\mathbb{H})$? Can you describe the ring homomorphism ϕ in this case?

[4]So, A comes with a multiplication operation as well as an addition operation. With these two operations, A satisfies the usual defining properties of a ring.