Introduction to R-modules

Grant Talbert

October 26, 2026

Abstract

These are notes for a talk given to the Society of Mathematics in the Fall 2026 semester, as part of their semesterly Colloquium. This semester's topic is on symmetries and invariants. In section 1, we will motivate modules by discussing how the structure of an abelian group is precisely that of a $\mathbb{Z}$-module. In section 2, we will introduce rings, and modules over a ring. In section 3, we introduce standard linear algebra constructions, such as R-linear maps, kernels, images, and products. One of the main difficulties with doing linear algebra over arbitrary rings is the lack of a basis in general. To better understand this, we strict our attention to modules over integral domains, and introduce an invariant of modules known as *torsion*, which provides an obstruction to free-ness. If time permits, we conclude with an introduction to the tensor product because I think it's cool.

Contents

1 Motivation **1**

2 Modules **4**

3 R-linear algebra **7**

1 Motivation

So far in the Colloquium, we have seen the definition of a group, and in particular, an *abelian group*. We have focused on groups as symmetries of an object, but they are still interesting algebraic structure to study abstractly. We will begin by investigating abelian groups, sine they are generally easier to investigate.

Definition 1.1. A *group* is a set G and an operation $\cdot : G \times G \to G$ called *the group operation* or *group multiplication*, which satisfies the following properties, called the *group axioms* (here we often write $a \cdot b$ as ab and call this their *product*):

1. For all $a, b, c \in G$, we have $(ab)c = a(bc)$. This is called *associativity*.
2. There exists some element $e \in G$ called the *identity*, with the property that for all elements $a \in G$, we have $ea = ae = a$.
3. For all $a \in G$, there is an element a^{-1} called the *inverse* of a, with the property that $aa^{-1} = a^{-1}a = e$.

If G also has the property that for all $a, b \in G$, we have $ab = ba$, then G is called an *abelian group*. This property is called the *commutative property*.

Note that the requirement that $\cdot$ be a function $G \times G \to G$ is the same as the *closure* axiom that many books use. This simply means that if $g, h \in G$, then $gh \in G$.

The set G is called the *underlying set* of the group G. We may sometimes refer to a group as a pair $(G, \cdot)$, where G is the underlying set and $\cdot$ is the group operation. This is mainly for notational convenience.

Note that in the above definition, we call the group operation "*multiplication*", and use common notation for multiplication when writing it. However, there are groups where it would make more sense to refer to the

group operation as something else. For example, consider the group of integers numbers $\mathbb{Z}$ under addition. This is indeed a group, since addition is associative, $0 \in \mathbb{Z}$ is the identity, and if $n \in \mathbb{Z}$, there is an additive identity $-n \in \mathbb{Z}$. It would make no sense to use the notation in definition 1.1 here, since I would then be writing $n \cdot m$ to mean $n + m$. I should not have to explain why this is a terrible idea.

Thus, there are two main notational conventions for groups. There is *multiplicative notation*, where the group operation is denoted by multiplication, and there is *additive notation*, where the group operation is denoted by addition. It will be useful for us to adopt the following convention.

Convention 1.2. If G is a group, then unless otherwise stated, we will use multiplicative notation if it is *not* an abelian group. If G is abelian, we will use additive notation (unless otherwise stated). To simplify this, I will often write $(G, +)$ to denote that we are using additive notation, and $(G, \cdot)$ to denote that we are using multiplicative notation.

Notation 1.3 (Additive notation)**.** Let $(G, +)$ be a group using additive notation. Then for $a, b \in G$, the group operation is written as $a + b$. The inverse of a is written as $-a$ and is called *negative* a. Finally, the identity element of G is written as $0 \in G$, and is also called *zero*. We may occasionally write 0_G instead of 0 to specify that 0_G is an element of G. This is useful when dealing with multiple groups at once.

We want to study groups abstractly, and abelian groups are a much simpler type of group due to their commutative property. As such, we will begin by investigating some basic properties of abelian groups.

Let's start with a basic observation. Suppose that $(G, +)$ is a group, and $a \in G$ is some element. Then if $n \in \mathbb{Z}_{>0}$ is a *positive* integer, then I can define the following element:

$$n \cdot a \coloneqq \underbrace{a + a + \cdots + a + a}_{n \text{ times}}.$$

This is very sensible notation; multiplication of integers $n \cdot m$ is just repeated addition $m + m + \cdots + m$, so we simply use the same notation for repeated addition in groups. This allows us to "multiply" a positive integer n with an element $a \in G$ of an abelian group.

We can extend this notation to all integers. First, recall that if n is an integer, then $0 \cdot n$ is simply 0. This suggests that 0-fold repeated addition should be the identity element. Thus, if $a \in G$, we define

$$0 \cdot a \coloneqq 0_G.$$

The 0 appearing on the left is the integer 0, and the 0 appearing on the right is the identity of the group G. Note that calling our group's identity "0" plays very nicely with this "multiplication by $\mathbb{Z}$" notation.

Finally, we define multiplication by -1 to simply be

$$-1 \cdot a = -a.$$

We can then define

$$-n \cdot a \coloneqq (-1 \cdot n) \cdot a = -1 \cdot (n \cdot a) = -(n \cdot a).$$

This allows us to define a multiplication operation $\mathbb{Z} \times G \to G$. We call this a "$\mathbb{Z}$-action" on the group G. we will often drop the multiplication dot, and will simply write na instead of $n \cdot a$.

Remark 1.4. This works in non-abelian groups, is written as a^n, and is called exponentiation.

We can now observe some basic, but extremely important, properties of abelian groups.

Proposition 1.5. *Let $(G, +)$ be an abelian group. Then there are operations $+ : G \times G \to G$ and $\cdot : \mathbb{Z} \times G \to G$, which satisfy the following eight properties.*

1. *For all $a, b, c \in G$, we have $(a + b) + c = a + (b + c)$.*
2. *There is some $0 \in G$ such that for all $a \in G$, we have $0 + a = a + 0 = a$.*
3. *For all $a \in G$, there is some $-a \in G$ such that $a + (-a) = -a + a = 0$.*
4. *For all $a, b \in G$, we have $a + b = b + a$.*

5. *For all $a \in G$, if $1 \in \mathbb{Z}$ is the number 1, then $1a = a$.*

6. *For all $n, m \in \mathbb{Z}$ and $a \in G$, we have $(nm)a = n(ma)$.*

7. *For all $n \in \mathbb{Z}$ and all $a, b \in G$, we have $n(a + b) = na + nb$.*

8. *For all $n, m \in \mathbb{Z}$ and all $a \in G$, we have $(n + m)a = na + ma$.*

Proof. Properties (1)-(4) are simply the axioms of an abelian group (definition 1.1), and thus are automatically true. To prove property (5), note that $1a$ denotes summing over 1 copy of a, and thus $1a = a$. The proofs for property (6)-(8) are longer (but not too tricky), and I only intend to cover the first in the talk. However, I will complete all three in these notes.

(6) Let $n, m \in \mathbb{Z}$ and $a \in G$. We want to show $(nm)a = n(ma)$. Note that

$$(nm)a = \underbrace{a + \cdots + a}_{nm \text{ times}} = \sum_{i=1}^{nm} a.$$

We also have

$$n(ma) = n\left(\sum_{i=1}^{m} a\right) = \sum_{j=1}^{n}\sum_{i=1}^{m} a = \sum_{k=1}^{nm} a.$$

Thus, $n(ma) = (nm)a$.

(7) Let $n \in \mathbb{Z}$ and $a, b \in G$. Then we have

$$n(a + b) = \sum_{i=1}^{n} a + b.$$

We also have

$$na + nb = \sum_{i=1}^{n} a + \sum_{i=1}^{n} b.$$

Since G is abelian, and thus addition is commutative, we can rearrange these sums to

$$\sum_{i=1}^{n} a + \sum_{i=1}^{n} b = \sum_{i=1}^{n} a + b.$$

Thus, $n(a + b) = na + nb$.

(8) Let $n \in \mathbb{Z}$ and $a, b \in G$. We have

$$(n + m)a = \sum_{i=1}^{n+m} a = \sum_{i=1}^{n} a + \sum_{j=n+1}^{n+m} a = \sum_{i=1}^{n} a + \sum_{j=1}^{m} a = na + ma.$$

Thus, we are done. ∎

I would like to compare the statements of proposition 1.5 to the definition of a vector space. In linear algebra, you likely learned how to define a vector space where the scalars were the real numbers $\mathbb{R}$. We can also define a *complex* vector space, where the scalars are the complex numbers $\mathbb{C}$. We will work with real vector spaces to keep this discussion simple, but the same discussion applies to any complex vector space. Observe the following.

Definition 1.6. A *vector space* is a set V, together with an operation $+ : V \times V \to V$ called *addition* and an operation $\cdot : \mathbb{R} \times V \to V$ called *scalar multiplication*, which satisfies the following eight properties.

1. For all $a, b, c \in V$, we have $(a + b) + c = a + (b + c)$.

2. There is some $0 \in V$ such that for all $a \in V$, we have $0 + a = a + 0 = a$.

3. For all $a \in V$, there is some $-a \in V$ such that $a + (-a) = -a + a = 0$.

4. For all $a, b \in V$, we have $a + b = b + a$.

5. For all $a \in V$, if $1 \in \mathbb{R}$ is the number 1, then $1a = a$.

6. For all $n, m \in \mathbb{R}$ and $a \in V$, we have $(nm)a = n(ma)$.

7. For all $n \in \mathbb{R}$ and all $a, b \in V$, we have $n(a + b) = na + nb$.

8. For all $n, m \in \mathbb{R}$ and all $a \in V$, we have $(n + m)a = na + ma$.

I have chosen my notation carefully to make the following observation immediate. Note that if we take definition 3.23, swap out V for G and swap out $\mathbb{R}$ for $\mathbb{Z}$, we get back *exactly* the eight properties of proposition 1.5!

And this leads me to the central topic of this paper. In linear algebra, we required that our scalars come from $\mathbb{R}$, or sometimes $\mathbb{C}$. But *why?* Why not let the scalars be $\mathbb{Z}$, or $\mathbb{Q}$, or polynomials, or smooth functions, or quaternions, or something even more exotic? Why restrict ourselves to $\mathbb{R}$ and $\mathbb{C}$?

The answer is we don't have to. In fact, it's better not to restrict ourselves to $\mathbb{R}$ and $\mathbb{C}$. As we will see, vector spaces (over $\mathbb{R}$ and $\mathbb{C}$) have very nice properties, and are easier to study, hence why they are covered in a linear algebra course. But there are many algebras in reality which are not vector spaces over these two sets of numbers, but over something else. These objects are important in their own right (as we will see many examples), but are not as "well-behaved" as a vector space is. Hence, we use a different name for them: a *module*.

2 Modules

In order to properly introduce modules, we need to be a little more precise about what the scalars actually are. Although we won't be restricting ourselves to $\mathbb{R}$ and $\mathbb{C}$, the scalars still can't be literally *anything*. For example, definition 3.23 property (5) requires the existence of some element 1 in our collection of scalars; property (6) requires that we can multiply scalars with scalars; and property (8) requires that we can add our scalars together. Thus, our collection of scalars has to be some sort of algebra with addition, multiplication, and 1. Such an algebraic structure is referred to mathematicians as a *ring*.

Definition 2.1. A *ring* is a set R together with *two* operations, addition $+ : R \times R \to R$ and *multiplication* $\cdot : R \times R \to R$, which satisfy the following properties.

1. The pair $(R, +)$ is an abelian group (definition 1.1).

2. For all $a, b, c \in R$, we have $a(bc) = (ab)c$. This is called *associativity*.

3. There exists some element $1 \in R$ with the property that for all $a \in R$, we have $1a = a1 = a$. This is called *one*, or the *multiplicative identity*, or the *unit*.

4. For all $a, b, c \in R$, we have $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$. These are called the *left and right distributive properties*.

Remark 2.2. Many authors, especially for undergraduate texts, do not require that rings have a unit 1. They would refer to a ring with a unit as a *unital ring*. However, most rings in practice (and all rings I personally work with) have an element 1, so I include a unit in the definition of a ring. These are both fairly standard conventions, and you would be justified in either agreeing or disagreeing with my convention. A ring without a unit is then referred to (in my convention) as an *rng* (we remove the "i" since "i" stands for "identity").

Rings are one of the most general type of interesting algebra that has two operations $+, \cdot$. It's possible to make more general algebras with two operations, but they're much less interesting. For example, without the associativie property for multiplication, it would be incredibly hard to work with rings at all. Without the distributive property, there would be no relationship between addition and multiplication, meaning it would be weird to even think of a ring as an algebra with 2 operations; one could just consider each operation fully independently of the other.

Example 2.3. The integers $\mathbb{Z}$ are a ring, using normal addition and multiplication. So are the real numbers $\mathbb{R}$, the rational numbers $\mathbb{Q}$, and the complex numbers $\mathbb{C}$. All of these rings have the property that $ab = ba$. Such a ring is known as a *commutative ring*. The natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$ are *not* a ring, since they are not a group. Natural numbers only contain non-negative integers, meaning they don't contain additive inverses, since the inverse of a non-negative integer is negative. However, $\mathbb{N}$ satisfies every other axiom of a ring, yielding a structure known as a *semiring* or a *rig* (we remove the "n" since "n" stands for "negative"). I personally know of zero applications of rigs, so we will not discuss them further.

Example 2.4. Consider the set of $n \times n$ matrices with real entries, which we will denote by $M_n(\mathbb{R})$. This is a ring using normal matrix addition and multiplication. However, more general $n \times m$ matrices are *not* a ring if $n \neq m$, since we can't multiply two matrices if the dimensions don't line up properly.

Example 2.5. Let R be any *commutative* ring, such as $\mathbb{R}$ or $\mathbb{C}$. We can define a new ring called $R[x]$ called the *polynomial ring over* R. Elements of this ring are *formal polynomials* with coefficients in R, meaning if $p \in R[x]$, then we can write

$$p(x) = \sum_{i=0}^{n} r_i x^i$$

for some coefficients $r_i \in R$. Addition and multiplication are defined in the exact way you would expect (the formulas are quite messy, but addition is termwise and multiplication just distributes over addition). Polynomial rings are extremely important in *commutative algebra*, which can generally be described as the study of commutative rings (and similar algebras).

We can now define modules over a ring R.

Definition 2.6. Let R be a ring. Then an *R-module* is a set M and two operations $+ : M \times M \to M$ called *addition* and $\cdot : R \times M \to M$ called *scalar multiplication* such that the following properties hold:

1. The pair $(M, +)$ is an abelian group.
2. For all $m \in M$, if $1 \in R$ is the unit, then $1m = m$.
3. For all $r, s \in R$ and $m \in M$, we have $(rs)m = r(sm)$.
4. For all $r \in R$ and all $m, n \in M$, we have $r(m + n) = rm + rn$.
5. For all $r, s \in R$ and all $m \in M$, we have $(r + s)m = rm + sm$.

Warning 2.7. If R is not a commutative ring, then there is some extra book-keeping that must be done. In particular, definition 2.6 is the definition of a *left* R-module, where multiplication is done $R \times M \to M$ (i.e. $(r, m) \mapsto rm$). However, there is also the notion of a *right* R-module, where multiplication is done $M \times R \to M$ (i.e. $(m, r) \mapsto mr$). This might seem to not matter, since we could just define $rm = mr$, but if R is not commutative then this fails:

$$srm = (sr)m = m(sr), \qquad srm = s(rm) = s(mr) = (mr)s = mrs.$$

But this isn't necessarily true, since we might not have $sr = rs$. Regardless, much of the theory we develop in this talk can still be done in the setting of noncommutative rings by simply replacing every mention of the word "module" with "left module". Not all of linear algebra generalizes so neatly, but even the parts that don't perfectly generalize perfectly still generalize in a reasonable way. Regardless, I believe this extra level of bookkeeping is unnecessary for an introductory talk, so we will work only over commutative rings.

Convention 2.8. Unless specified otherwise, every ring R is assumed to be commutative, i.e. $ab = ba$ for all $a, b \in R$.

Remark 2.9. There is an alternative definition of a module, which is somewhat more complex but much cleaner. Given rings R, S, a *ring homomorphism* is a function $\varphi : R \to S$ such that for all $r_1, r_2 \in R$,

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) \quad \text{and} \quad \varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2) \quad \text{and} \quad \varphi(1) = 1.$$

Let $(M, +)$ be an abelian group, and write $\mathrm{End}_{\mathcal{A}\mathrm{b}}(M)$ for the set of all group homomorphisms $M \to M$ (we call such a map a *group endomorphism*). If $f, g \in \mathrm{End}_{\mathcal{A}\mathrm{b}}(M)$, then we define the functions $f + g$ and $f \circ g$ as follows: for all $m \in M$,

$$(f + g)(m) = f(m) + g(m), \qquad (f \circ g)(m) = f(g(m)).$$

I claim that by taking $+$ to be addition and $\circ$ to be multiplication, the set $\mathrm{End}_{\mathcal{A}\mathrm{b}}(M)$ is a ring. An R-module can then be defined as a ring homomorphism $\rho : R \to \mathrm{End}_{\mathcal{A}\mathrm{b}}(M)$. Definition 2.6 is then recovered as follows. Let $r \in R$ and $m \in M$; we want to define rm. Since ρ maps R to endomorphisms of M, we have that $\rho(r)$ is a function $M \to M$. Since $m \in M$, we can evaluate the function $\rho(r)$ at m, yielding an element $\rho(r)(m) \in M$. We define

$$rm \coloneqq \rho(r)(m).$$

All of the properties listed in definition 2.6 can be proven from this definition. In view of warning 2.7, this defines a *left* R-module when R is noncommutative.

There are a ton of great examples of R-modules. We will go through a few.

Example 2.10. We have shown previously in proposition 1.5 that any abelian group satisfies all the axioms of a $\mathbb{Z}$-module. Thus, all abelian groups are $\mathbb{Z}$-modules. Since all $\mathbb{Z}$-modules are also abelian groups (condition 1 of definition 2.6), we have a two-sided inclusion

$$\{\mathbb{Z}\text{-modules}\} \subseteq \{\text{abelian groups}\} \qquad \text{and} \qquad \{\mathbb{Z}\text{-modules}\} \supseteq \{\text{abelian groups}\}.$$

Therefore, $\mathbb{Z}$-modules are the same thing as abelian groups.

Example 2.11. Let's look at a more concrete example. First, any vector space over $\mathbb{R}$ is an $\mathbb{R}$-module. Similarly, any vector space over $\mathbb{C}$ is a $\mathbb{C}$-module. I will later define a *field* as a particular very nice type of ring, and we will define a vector space to be a module over a field. The reason vector spaces are given a special name is because they turn out to be much easier to work with than arbitrary modules, as we will see shortly.

Example 2.12. A module can be a module over multiple rings at once. For example, any ring R is an abelian group, and thus a $\mathbb{Z}$-module. However, R is also an R-module, where the scalar multiplication is just normal ring multiplication. Hence a ring R is both a $\mathbb{Z}$-module *and* an R-module. More generally, if R, S are commutative[1] rings and M is both an R-module and an S-module, and the scalar multiplications are compatible in the sense that for all $r \in R$, $s \in S$, and $m \in M$,

$$r(sm) = s(rm),$$

then we call M an (R, S)-bimodule.

Example 2.13. Here's a more complex, but more concrete and *very useful* example. A *vector field* on $\mathbb{R}^3$ is a function $X : \mathbb{R}^3 \to \mathbb{R}^3$. Recall that $\mathbb{R}^3$ is a vector space, meaning that for any point $(x, y, z) \in \mathbb{R}^3$, the vector field X produces a vector $X(x, y, z) \in \mathbb{R}^3$. Note that if I multiply this vector by a scalar $c \in \mathbb{R}$, I get a new vector $c \cdot X(x, y, z) \in \mathbb{R}^3$. We can use this fact to give the set of vector fields on $\mathbb{R}^3$ the structure of a $C^\infty(\mathbb{R}^3)$-module.

First, let $\mathfrak{X}(\mathbb{R}^3)$ be the set of all vector fields on $\mathbb{R}^3$. Define $C^\infty(\mathbb{R}^3)$ to be the set of all *smooth functions* $f : \mathbb{R}^3 \to \mathbb{R}$. Here, smooth simply means that any possible combination of partial derivatives of f exist. We can give $C^\infty(\mathbb{R}^3)$ the structure of a ring by using the ring structure of $\mathbb{R}$. If $f, g \in C^\infty(\mathbb{R}^3)$, then we define the new smooth functions $f + g$ and $f \cdot g$ as follows:

$$\forall (x, y, z) \in \mathbb{R}^3, \qquad (f + g)(x, y, z) = f(x, y, z) + g(x, y, z), \qquad (f \cdot g)(x, y, z) = f(x, y, z) \cdot g(x, y, z).$$

It's fairly easy to check that this forms a ring. Each ring axiom needs to be checked at a single arbitrary point (x, y, z) of $\mathbb{R}^3$, meaning that we can simply work with equations in $\mathbb{R}$, which is already a ring. Thus, we can consider a $C^\infty(\mathbb{R}^3)$-module.

[1] This is a technicality used to simplify the definition.

In order for $\mathfrak{X}(\mathbb{R}^3)$ to be a $C^\infty(\mathbb{R}^3)$-module, we need to define a multiplication operation which takes a smooth function $f : \mathbb{R}^3 \to \mathbb{R}$ and a vector field $X : \mathbb{R}^3 \to \mathbb{R}^3$, and outputs a new vector field $fX : \mathbb{R}^3 \to \mathbb{R}^3$. We define it as follows. Let $(x, y, z) \in \mathbb{R}^3$. then

$$(fX)(x, y, z) = f(x, y, z) \cdot X(x, y, z).$$

Since $f(x, y, z) \in \mathbb{R}$, we have that $f(x, y, z)$ is just a number, i.e. a *scalar*. Since $X(x, y, z)$ is a vector in $\mathbb{R}^3$, we know how to multiply it by a scalar. Thus, multiplying $f(x, y, z)$ and $X(x, y, z)$ can not only be done, but produces a new element of $\mathbb{R}^3$! Thus, $fX : \mathbb{R}^3 \to \mathbb{R}^3$ is indeed a vector field.

Example 2.13 is a more complex example of a module, and it can be difficult to understand at first. However, a *ton* of modules over rings of smooth functions (or other types of functions, eg. continuous, holomorphic, locally rational) show up in geometry. I won't use many more examples from geometry in these notes to keep them more understandable, but since one of the most interesting applications of module theory is with modules of this form in geometry, it's important (and very cool) to at least know about this.

3 R-linear algebra

A lot of linear algebra still works for R-modules, but not all of it. I will survey some of the main constructions and main results of the theory.

The most striking result in all of module theory is that if R is a random ring, then there is no requirement for an R-module M to have a basis! We can already see a simple example of this by looking at $\mathbb{Z}$-modules, which we recall (by example 2.10) are simply abelian groups. First, let's recall what a basis is.

Definition 3.1. Let R be a ring, and let M be an R-module. A finite subset $\{m_1, \dots, m_n\} \subseteq M$ is *linearly independent* if the only collection of scalars $r_1, \dots, r_n \in R$ such that

$$r_1 m_1 + \cdots + r_n m_n = 0$$

are $r_1, \dots, r_n = 0$. The finite subset $\{m_1, \dots, m_n\} \subseteq M$ is a *spanning set* if for all $x \in M$, there are coefficients $r_1, \dots, r_n \in R$ such that

$$x = r_1 m_1 + \cdots + r_n m_n.$$

If S is a spanning set, we also call it a *generating set*, and say it *generates* M. A *basis* is a set $S \subseteq M$ that is both linearly independent and a spanning set.

Warning 3.2. We have only defined finite bases. Some modules have no finite basis, but *do* have infinite bases. To avoid overcomplicating this talk, we will restrict our attention to places where bases are finite, but almost all of our theory applies in the more general setting (the main part that doesn't is the fundamental theorem of finitely generated modules over a PID, but this is mostly an ending remark). I will, however, briefly define an infinite linearly independent set. The main issue with naively generalizing definition 3.1 to infinite sets is it requires a sum over all elements, but infinite sums need not converge. Thus if S is an infinite set, we say it is linearly independent if for all finite collections $s_1, \dots, s_n \in S$, if

$$r_1 s_1 + \cdots + r_n s_n = 0,$$

then $r_i = 0$ for all i. In other words, a set S is linearly independent if *all finite subsets* are linearly independent. We also say that an infinite set S is *spanning* if for all $m \in M$, there is a finite linear combination $r_1 s_1 + \cdots + r_n s_n = m$ with $s_i \in S$ for all i.

Consider the following very simple abelian group. Let $\mathbb{Z}/2$ be the set $\{0, 1\}$ with addition defined by

$$0 + 0 = 0 \qquad 0 + 1 = 1$$
$$1 + 0 = 1 \qquad 1 + 1 = 0$$

The only difference from normal addition is $1 + 1 = 0$. We call this the group of *integers modulo 2*. Other notations for this group are $\mathbb{Z}/(2)$, $\mathbb{Z}/2\mathbb{Z}$, and $\mathbb{Z}_2$. The addition operation is typically written as $n + m \pmod 2$, but we will drop the (mod 2).

Since all abelian groups are $\mathbb{Z}$-modules, we see that $\mathbb{Z}/2$ is a $\mathbb{Z}$-module. Does this $\mathbb{Z}$-module have a basis? There are only 4 subsets of $\mathbb{Z}/2$: the empty set, and the sets $\{0\}, \{1\}, \{0, 1\}$. Clearly the empty set is not spanning. Additionally, $\{0\}$ is not spanning, since there is no way to add 0 to itself in order to get 1. The set $\{1\}$ *is* spanning, since $2 \cdot 1 = 1 + 1 = 0$. However, it's *not linearly independent*. By the equation we just wrote, $2 \cdot 1 = 0$ for $2 \in \mathbb{Z}$. However, since $2 \neq 0$ in $\mathbb{Z}$, this immediately fails linear independence. The set $\{0, 1\}$ is also not linearly independent for the same reason: $0 \cdot 0 + 2 \cdot 1 = 0$, but $2 \neq 0$.

This immediately makes linear algebra with R-modules much harder. For example, without a basis, we can't define the *dimension* of an R-module. In order to talk about matrices, we need to have a basis; thus we cannot always do matrix algebra in arbitrary R-modules.

Definition 3.3. An R-module M with a basis $S \subseteq M$ is called a *free R-module*.

Although not all R-modules are free (unlike vector spaces), we can still do quite a lot of linear algebra with R-modules. Let's introduce some notions from linear algebra that extend to R-modules without much difficulty.

Definition 3.4. Let R be a ring, and let M, N be R-modules. An *R-linear map* from M to N is a function $\varphi : M \to N$ with the following properties:

1. For all $m_1, m_2 \in M$, we have $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$.
2. For all $m \in M$ and $r \in R$, we have $\varphi(rm) = r \cdot \varphi(m)$.

Note that definition 3.4 is the same definition as a normal linear map, except the scalars now come from a ring R, rather than $\mathbb{R}$ or $\mathbb{C}$.

Example 3.5. Let M, N be R-modules. The map $0 : M \to N$ which is defined by $0(m) = 0$ is an R-linear map. We call this the *zero morphism*, the *zero map*, or the *trivial map*. Another example is the map $1_M : M \to M$ defined by $1_M(m) = m$. This is called the *identity morphism* of M.

Example 3.6. Every linear map between vector spaces you have ever seen is an $\mathbb{R}$-linear (or $\mathbb{C}$-linear) map.

We can similarly extend a lot of definitions like vector subspaces, kernels and images to the setting of R-modules.

Definition 3.7. Let R be a ring, and let M, N be R-modules.

1. We say N is a *submodule* of M if $N \subseteq M$ as a set, N is nonempty, and if N is closed under addition and scalar multiplication.
2. Let $\varphi : M \to N$ be an R-linear map. The *kernel* of φ, denoted $\operatorname{Ker} \varphi$, is the submodule
$$\operatorname{Ker} \varphi = \{m \in M \mid \varphi(m) = 0\} \subseteq M.$$
3. Let $\varphi : M \to N$ be an R-linear map. The *image* of φ, denoted $\operatorname{Im} \varphi$, is the submodule
$$\operatorname{Im} \varphi = \{\varphi(m) \in N \mid m \in M\} \subseteq N.$$

We can also define Cartesian products (which we simply refer to as products), which will be extremely useful.

Definition 3.8. Let R be a ring, and let M and N be R-modules. We define the *product module* $M \times N$ to be the R-module defined as follows.

- The underlying set $M \times N$ consists of all ordered pairs (m, n), where $m \in M$ and $n \in N$.
- The addition operation is defined *pointwise*, meaning for all $m_1, m_2 \in M$ and $n_1, n_2 \in N$, we have
$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2).$$

- The multiplication operation is also defined pointwise, meaning for all $m \in M$, $n \in N$, and $r \in R$, we define
$$r(m, n) = (rm, rn).$$

Notation 3.9. Due to some compliated but very nice properties of R-modules (remark 3.10), the notation $M \times N$ for the product is not used very often. Most of the times, we write $M \times N$ as $M \oplus N$, and call it either the *product* or the *direct sum*. The element (m, n) is often written as $m + n$. This notation makes sense since we can write
$$(m, n) = (m, 0) + (0, n),$$
and then we simply use the notation $m = (m, 0)$ and $n = (0, n)$. This notation turns out to be extremely convenient in particular cases, and is used fairly often. To avoid confusion, we will not be using this notation (we will be using ordered pairs and $\times$), because this is more aligned with undergraduate linear algebra notation. However, it's important to know that this notation exists.

Remark 3.10. The product of R-modules is both a product *and* a coproduct, in the sense of category theory.

We will now discuss something known as *torsion*, which can make a module fail to have a basis. Torsion isn't the only reason a module can not have a basis, but it's a fairly important one, and turns out to be an invariant. Let M be an R-module, and let $r \in R$ and $m \in M$ such that $rm = 0$. Suppose that $r \neq 0$. Does $m = 0$? If $R = \mathbb{R}$, then the answer is yes, since we can simply multiply by $1/r$ (since $r \neq 0$) to get
$$0 = \frac{1}{r}rm = \frac{r}{r}m = 1m = m.$$
However, if R is an arbitrary ring, we can't do this. For example, consider the ring of $n \times n$ matrices with real entries $M_n(\mathbb{R})$. Recall that *not all matrices are invertible*. Thus, if $r \in M_n(\mathbb{R})$ is some matrix, there might not be some element r^{-1} allowing us to cancel r in the equation $rm = 0$.

Definition 3.11. Let R be a ring, and M an R-module. An element $m \in M$ is called *torsion* if there is some nonzero $r \in R$ such that $rm = 0$. We denote the set of all torsion elements of M by $\mathrm{Tor}(M)$:
$$\mathrm{Tor}(M) = \{m \in M \mid m \text{ is torsion}\}.$$

The only torsion element of a vector space is 0, so if V is a vector space, then $\mathrm{Tor}(V) = \{0\}$. However, there can be R-modules with nonzero torsion elements.

For example, consider the $\mathbb{Z}$-module $\mathbb{Z}/2$ from before, which we know has no basis. The element 0 is obviously torsion, so let's consider the element 1. Recall that $2 \cdot 1 = 0$, but $2 \neq 0$. Thus, 1 is torsion. We thus have $\mathbb{Z}/2 = \mathrm{Tor}(\mathbb{Z}/2) = \{0, 1\}$.

Note that every subset of $\mathrm{Tor}(M)$ *cannot* be linearly independent: given any element $m \in \mathrm{Tor}(M)$, there is some nonzero $r \in R$ with $rm = 0$. Thus, any collection $m_1, \ldots, m_n$ of torsion elements admits nonzero scalars $r_1, \ldots, r_n \in R$ such that $r_i m_i = 0$ for all i, and thus
$$r_1 m_1 + \cdots + r_n m_n = 0.$$
Thus, no nonempty subset of $\mathrm{Tor}(M)$ is linearly independent.

Is torsion actually an issue though? Although no subset of $\mathrm{Tor}(M)$ can be linearly independent, one could imagine taking the basis to live in $M \setminus \mathrm{Tor}(M)$, and no linear independence issues would arise. To see if this is actually an issue, let's consider how a proof might go.

Proposition 3.12 (Incorrect!)**.** *Let R be a commutative ring, and M an R-module. If $\mathrm{Tor}(M) \neq \{0\}$, then M is not free.*

(Incorrect) Proof. Let $S = \{s_1, \ldots, s_n\} \subseteq M$ be a spanning set (remember we are working under the assumption that S is finite!). It suffices to show that S is not linearly indepedent, since this would imply *all* spanning sets are not linearly independent, and hence no basis can exist since a basis must be both spanning and linearly independent.

The way our proof works is as follows. Since S is spanning, for all $m \in M$, there are coefficients $r_1, \ldots, r_n \in R$ such that

$$m = r_1 s_1 + \cdots + r_n s_n.$$

In particular, consider what happens when $m \in \mathrm{Tor}(M)$ is a nonzero torsion element. Since m is nonzero, we see that at least one r_i is nonzero. Since m is torsion, there is some nonzero $a \in R$ such that $am = 0$. Since $m = r_1 s_1 + \cdots + r_n s_n$, we have

$$0 = am = a\left(r_1 s_1 + \cdots + r_n s_n\right) = ar_1 s_1 + \cdots + ar_n s_n.$$

The error in our proof is in this final step. If S were linearly independent, then this implies $ar_1, \ldots, ar_n = 0$. However, we know that a is nonzero, and at least one r_i is nonzero. Hence we want to say ar_i is nonzero, hence this set cannot be linearly independent. But we cannot say this!

Remember that matrices $M_n(\mathbb{R})$ form a ring. Consider the matrices

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

We have

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0.$$

Hence there are rings where we can have $A, B \neq 0$ but $AB = 0$ (we call such elements *zero divisors*). One might object that $M_n(\mathbb{R})$ is noncommutative, but our proof critically relies on R being commutative. However, there are examples of commutative rings with zero divisors as well. Consider $\mathbb{Z}/6$, the integers modulo 6. Notice that $2 \cdot 3 = 6 \equiv 0 \pmod 6$, but $2, 3 \neq 0$, meaning $\mathbb{Z}/6$ has zero divisors too. So we cannot finish this proof!

In fact, $\mathbb{Z}/6$ provides a direct counterexample to this proof. Consider $\mathbb{Z}/6$ as a module over itself. Then $2 \cdot 3$ implies that both 2 and 3 are torsion. However, $\mathbb{Z}/6$ is free as a $\mathbb{Z}/6$-module; its basis is simply the unit $1 \in \mathbb{Z}/6$. Hence we have a free module with nonzero torsion, which proves our proposition false by contrapositive. To correct this issue, we will restrict our attention to "nice" rings, where there are no zero divisors.

Definition 3.13 (Integral domain)**.** An *integral domain* is a commutative ring R such that $1 \neq 0$, and if $a, b \in R$ are nonzero, then ab is also nonzero. We say R *has no zero divisors.*

We can now state a corrected version of proposition 3.12.

Proposition 3.14. *Let R be an* integral domain*, and M an R-module. If $\mathrm{Tor}(M) \neq \{0\}$, then M is not free.*

Proof. Follow all the steps of the (incorrect) proof of proposition 3.12, until we get to the last step. We know that a is nonzero, and at least one r_i is nonzero. Since R is an integral domain, we see that ar_i is nonzero, hence we have a sum

$$ar_1 s_1 + \cdots + ar_n s_n = 0,$$

but not all the coefficients are 0. Therefore S cannot be linearly independent. ∎

We now have a class of rings called *integral domains* where torsion is indeed an obstruction to free-ness. But how useful really is torsion if it doesn't apply to all rings? It turns out that there are many integral domains in nature, and it is much easier to do algebra with integral domains. Torsion is useful because of how simple it is. Integral domains are well-behaved rings, and thus their modules have a simple construction allowing us to examine whether they have bases. For more complicated rings, the methods of determining if a module has a basis are more complex, and beyond the scope of this talk. It turns out that torsion and integral domains allow us to learn a lot more about a module than whether or not it has a basis, but we will explore this after giving some examples of integral domains.

Example 3.15. The integers $\mathbb{Z}$ are an integral domain. So are $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{C}$.

Example 3.16. Let R be an integral domain. Then the *polynomial ring* $R[x]$ (see example 2.5). This ring is also an integral domain.

Example 3.17. The ring of smooth functions $C^\infty(\mathbb{R})$ is *not* an integral domain. Given an interval $(a, b) \subseteq \mathbb{R}$ and a smaller interval $(c, d) \subseteq (a, b)$, I can define what is known as a *bump function*, which is a smooth function f that is zero everywhere outside of $[a, b]$, and $f(x) = 1$ for all $c < x < d$. We say f is a bump function for (c, d) supported on (a, b). Now simply choose two intervals (a, b) and (a', b') which do not intersect each other. Then any bump functions for any interval inside of (a, b) and (a', b') that are supported on these intervals must multiply to zero.

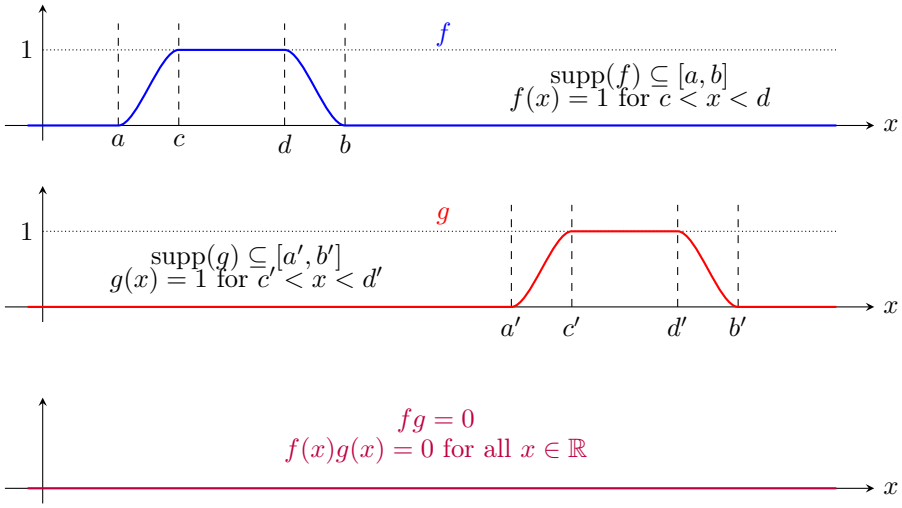


Figure 1: Two bump functions with disjoint supports. Since their supports do not intersect, their product is identically zero. Here, the "support" of a function f, denoted $\text{supp}(f)$, can be thought of as a closed set wherein f is zero everywhere *outside* of its support.

Example 3.18. If you know some complex analysis, it turns out that *holomorphic functions* $\mathcal{O}(U)$ *are* an integral domain for any open and connected subset $U \subseteq \mathbb{C}$. Indeed, recall the identity theorem, which says that if f, g are holomorphic functions on U which agree on an at least countable subset $D \subseteq U$ with an accumulation point, then $f = g$. Every (nonempy) open subset $V \subseteq \mathbb{C}$ is both uncountable, and has an accumulation point. Suppose that $fg = 0$; we must show either $f = 0$ or $g = 0$. If $f = 0$ we are done, so assume $f \neq 0$. Then there is at least one $z_0 \in U$ with $f(z_0) \neq 0$. By continuity, there is an open neigborhood $z_0 \in V \subseteq U$ where f is never 0 on V. But for all $z \in V$, we have $(fg)(z) = f(z)g(z) = 0$. Since $f(z) \neq 0$, we know that $g(z)$ must be zero (recall that $\mathbb{C}$ does not have zero divisors). Thus g is zero everywhere on the open subset V. By the identity theorem, $g = 0$ on all of U, so we are done. Thus $\mathcal{O}(U)$ is an integral domain.

Let's return our attention to torsion for modules over integral domains. There are a few very interesting things we can prove which rely critically on working over integral domains.

Proposition 3.19. *Let R be an integral domain, and M an R-module. Then $\text{Tor}(M)$ is a submodule of M.*

Proof. Since 0 is always torsion, it suffices to prove closure under addition and scalar multiplication (exercise: how does this imply that if $m \in \text{Tor}(M)$, then $-m \in \text{Tor}(M)$ too?). Let $a, b \in \text{Tor}(M)$ be torsion. Then there are scalars $r, s \in R$ with $ra = 0$ and $sb = 0$. Hence

$$rsa = sra = s(ra) = s0 = 0, \qquad rsb = r(sb) = r0 = 0.$$

Here we have used the fact that R is commutative to write $rs = sr$. Thus

$$0 = rsa + rsb = rs(a + b).$$

Thus there is a scalar $rs \in R$ such that $rs(a + b) = 0$. Since $r, s \neq 0$ and R is an integral domain, we see that rs is nonzero, hence $a + b$ is torsion.

Now let $m \in \mathrm{Tor}(M)$ be torsion, and $r \in R$. Then since m is torsion, there is some $s \in R$ such that $sm = 0$. Hence

$$s(rm) = (sr)m = (rs)m = r(sm) = r0 = 0.$$

Hence $s(rm) = 0$. Since $s \neq 0$, there is a nonzero scalar $s \in R$ which annihilates rm. Thus rm is torsion. ■

Proposition 3.20. *Let R be an integral domain, and let M, N be R-modules. Let $\varphi : M \to N$ be an R-linear isomorphism (meaning φ is bijective). Then there is an induced isomorphism $\mathrm{Tor}(M) \cong \mathrm{Tor}(N)$. In other words, torsion is an invariant of modules.*

Proof. We will define a map $\widetilde{\varphi} : \mathrm{Tor}(M) \to \mathrm{Tor}(N)$ by $\widetilde{\varphi}(m) = \varphi(m)$. In other words, if m is torsion, we must show $\varphi(m)$ is torsion. Indeed, since m is torsion, there is $r \in R$ with $rm = 0$. One can prove that $\varphi(0) = 0$ (the proof is the same as in linear algebra, can you do it?). Hence by R-linearity,

$$0 = \varphi(0) = \varphi(rm) = r\varphi(m).$$

Thus there is nonzero $r \in R$ with $r\varphi(m) = 0$, hence $\varphi(m)$ is torsion in N. Since φ is injective, clearly so is $\widetilde{\varphi}$, hence we must only prove surjectivity. Let $n \in \mathrm{Tor}(N)$ be torsion. Then since φ is surective, there is $m \in M$ with $\varphi(m) = n$. We must show m is torsion, Indeed, since n is torsion, there is $r \in R$ with $rn = 0$. Hence

$$0 = rn = r\varphi(m) = \varphi(rm).$$

Since $\varphi(0) = 0$, we now have $\varphi(rm) = \varphi(0)$. By injectivity, $rm = 0$. ■

Note that this proof did not require R to be an integral domain to prove. However, if R was not an integral domain, then $\mathrm{Tor}(M)$ and $\mathrm{Tor}(N)$ would just be sets, meaning this invariant wouldn't be as strong. But when working with integral domains, this invariant is an R-module, hence there is more information to extract.

Although torsion implies no basis can exist, we can still have modules (even over an integral domain) where there is no torsion, but still no basis. In order for no torsion to imply free-ness, we would have to restrict to an even smaller class of rings called *principal ideal domains* (PIDs), and we would have to restrict to *finitely generated* modules, meaning they have a finite spanning set. Discussing PIDs would take us too far afield for this talk, but when working over PIDs, not only does no torsion imply free-ness for finitely generated modules, but we can write every finitely generated module M as a product of a free component R^n with a torsion component

$$M \cong R^n \times \mathrm{Tor}(M).$$

Even better, we can explicitly calculate what $\mathrm{Tor}(M)$ is using *prime ideals*, which are a particular generalization of prime numbers. This particular decomposition is called the *fundamental theorem of finitely generated modules over a principal ideal domain.*

Finally, if we simply want to find an example of a ring where *all* modules are free, we can look at fields.

Definition 3.21. A *field* $\mathbb{K}$ is a ring $(\mathbb{K}, +, \cdot)$ such that the following additional properties hold.

1. $\mathbb{K}$ is a commutative ring, i.e. for all $a, b \in \mathbb{K}$, we have $ab = ba$.
2. For all nonzero $a \in \mathbb{K}$, there is some element $a^{-1} \in \mathbb{K}$ such that $aa^{-1} = a^{-1}a = 1$.
3. $1 \neq 0$.

The main three examples of fields are the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$. There are other interesting examples of fields (meromorphic functions, $\mathbb{Q}[\alpha]$ for algebraic α, etc.), but we will only consider these three for simplicity. It turns out that fields are always PIDs, so every module decomposes into a free component and a torsion component. However, every module over a field has no torsion.

Proposition 3.22. *Let $\mathbb{K}$ be a field, and M a $\mathbb{K}$-module. Then $\mathrm{Tor}(M) = \{0\}$.*

Proof. Let $m \in \mathrm{Tor}(M)$ be torsion. Then there is nonzero $k \in \mathbb{K}$ with $km = 0$. Since $\mathbb{K}$ is a field and $k \neq 0$, there is $k^{-1} \in \mathbb{K}$ with $k^{-1}k = 1$. Hence

$$k^{-1}km = (k^{-1}k)m = 1m = m.$$

But $km = 0$, so

$$k^{-1}km = k^{-1}(km) = k^{-1}0 = 0.$$

Thus $m = 0$. ■

Believe it or not, even $\mathbb{K}$-modules which *aren't* finitely generated have bases (using an appropriate definition of a basis of an infinite dimensional space). The fact that every module over a field is free is a profoundly important fact, as it allows us to start doing matrix calculus and all of normal linear algebra. Hence, we define:

Definition 3.23. A *vector space* is a module over a field. If $\mathbb{K}$ is a field, a module over $\mathbb{K}$ is called a $\mathbb{K}$-*vector space*.