Modules

David McKinnon
Department of Pure Mathematics
University of Waterloo

Spring 2020

1 Modules

Let R be a commutative ring. An R-module is a bunch of things that you can add and subtract, and that you can multiply by elements of R.

OK, that's obviously a terrible definition. But it captures very well what a module is. We're pure math types, though, so we want a definition.

Definition 1.1. *Let R be a commutative ring. An R module is an abelian group M and a function $\cdot : R \times M \to M$ satisfying*

- $r(m_1 + m_2) = rm_1 + rm_2$
- $(r_1 + r_2)m = r_1m + r_2m$
- $r_1(r_2m) = (r_1r_2)m$
- $1m = m$

for all r, r_1, r_2 in R and all m, m_1, m_2 in M.

So for a module to make sense, you need to have a ring and a group. The actual module is the group, but you need to have the ring around to do the multiplying for you.

For example. If R is a field, then an R-module is a vector space.

If $R = \mathbb{Z}$, notice that a $\mathbb{Z}$-module is the same thing as an abelian group. One direction is obvious – any R-module is an abelian group regardless of what R is – and to go the other way, notice that an abelian group is an abelian group (yeah), and you can multiply it by elements of $\mathbb{Z}$ (heck yeah!). I mean, to multiply m by 5, just compute $m + m + m + m + m$.

If R is any ring, then any ideal I of R is an R-module. In fact, you could *define* an ideal to be an R-submodule of R. (An R-submodule of M is exactly what you think it is: it's an R-module whose elements are contained in M, and whose operations are the restrictions of the operations of M.)

Better yet, R/I is an R-module, for any commutative ring R and ideal I. Morally speaking: you can add and subtract the elements of R/I, and you can multiply them by elements of R (by reducing them mod I first). Technically speaking ... it's really boring and silly. Check it yourself, if you like. But bring a pillow.

An example that's a little more directly related to this course: the Gaussian integers $\mathbb{Z}[i]$ are a $\mathbb{Z}$-module. You can add and subtract them, and multiply them by elements of $\mathbb{Z}$. (Again, I leave it to you to check that all the axioms of the technical definition are satisfied.)

More generally, if T is any ring containing R, then T is an R-module. So, for example, $\mathbb{Q}$ is a $\mathbb{Z}$-module. So is $\mathbb{R}$.

More more generally, if $\phi\colon R \to T$ is a homomorphism, then T is an R-module. This explains the R/I example too.

As in any part of mathematics, once you define the objects, you have to define the morphisms.

Definition 1.2. *Let M and N be R-modules. An R-module homomorphism from M to N is a homomorphism $f\colon M \to N$ of abelian groups such that $f(rm) = rf(m)$ for all r in R and m in M. An R-module isomorphism is an R-module homomorphism that admits a two-sided inverse that is also an R-module homomorphism.*

In other words, an R-module homomorphism is a function that plays nice (commutes) with the addition, subtraction, and R-multiplication.

Notice that because R-module homomorphisms are always homomorphisms of abelian groups, it follows that an R-module homomorphism is an R-module isomorphism if and only if it's bijective:

$$f^{-1}(rn) = f^{-1}(rf(f^{-1}(n))) = f^{-1}(f(rf^{-1}(n))) = rf^{-1}(n)$$

For example, if R is a field, then an R-module homomorphism is the same thing as a linear transformation of vector spaces. (Check it out – the proof is really easy!)

Complex conjugation defines a $\mathbb{Z}$-module homomorphism from $\mathbb{Z}[i]$ to $\mathbb{Z}[i]$. This is also a homomorphism of rings.

The function $x \to 2x$ is a $\mathbb{Z}$-module homomorphism from $\mathbb{Z}[i]$

to $\mathbb{Z}[i]$, but it's not a ring homomorphism, because 1 doesn't map to 1.

And complex conjugation defines a ring homomorphism $\mathbb{Q}(i) \to \mathbb{Q}(i)$, but this homomorphism of rings is *not* a homomorphism of $\mathbb{Q}(i)$-modules.

Notice – and the proof here is very easy – that the image and preimage of a submodule under a module homomorphism are again submodules.

But there is more work to do before we leave the warm embrace of the modules section.

Definition 1.3. *Let M be an R-module, S a subset of M. The submodule generated by S is the intersection of all submodules containing S.*

It's easy to check that any intersection of R-modules is again an R-module, so this definition makes sense. And this definition leads to a few more, but most especially, we say that an R-module M is finitely generated if there is a finite set S that generates M.

I guess we should actually prove some stuff.

Theorem 1.4. *Let M be an R-module, $N \subset M$ a submodule. If M is finitely generated, then so is M/N.*

Proof: If you can write $m \in M$ as a linear combination of generators $\{x_i\}$, then that linear combination still works after you reduce modulo N. ♣

For the next theorem, we will recall a definition.

Definition 1.5. *A ring R is noetherian if and only if every ideal of R is finitely generated.*

Theorem 1.6. *Let M be a finitely generated module over a noetherian ring R. Then every submodule of M is also finitely generated.*

Proof: We're going to start by proving the theorem in the case that $M = R^n = R \times R \times \ldots \times R$. We will then use a cunning trick to prove it for a general M. Let N be a submodule of $M = R^n$.

If $n = 1$, then an R-submodule of M is better known as an ideal of R, and is therefore finitely generated by assumption.

We will now induce on n. (The verb "to induct" is what you use to admit people to a Hall of Fame. "Deduce" gives "deduction", so "induce" gives "induction". I know, I know. I'm telling the tide not to come in.)

If $n \geq 2$, then we can write $R^n = R^{n-1} \times R$. Let $N_1 = \{(r_1, \ldots, r_n) \in N \mid r_n = 0\}$. Then N_1 is isomorphic to an R-submodule of R^{n-1}, and so it is finitely generated.

Let $N_2 = \pi_n(N) \subset R$, where $\pi_n \colon R^n \to R$ is the projection onto the nth coordinate. In other words, let N_2 be the set of elements of R that appear as the nth coordinate of some element of N. Since it's the image of a submodule under a homomorphism, it's a submodule of R, and therefore an ideal, and therefore finitely generated.

Let $x_1, \ldots, x_s$ be generators for N_1, and let $y_1, \ldots, y_t$ be elements of N whose nth coordinates are generators for N_2. For any $m \in N$, we can find an R-linear combination of the y_i whose

nth coordinate is the same as that of m. In other words, we can find $r_1, \ldots, r_t \in R$ such that the nth coordinate of the following element of M is zero:

$$m - r_1 y_1 - \ldots - r_t y_t$$

But this means that this element is in M_1! So it's a linear combination of the x_i:

$$m - r_1 y_1 - \ldots - r_t y_t = r'_1 x_1 + \ldots r'_s x_s$$

Reorganising this shows that m is in the R-linear span of the set $\{x_1, \ldots, x_s, y_1, \ldots, y_t\}$. So N is finitely generated.

Now let's do the general case. Since M is finitely generated, there is a surjective R-module homomorphism $\phi\colon R^n \to M$, mapping the standard basis vectors to the n generators $\{x_1, \ldots, x_n\}$ of M:

$$\phi(r_1, \ldots, r_n) = r_1 x_1 + \ldots + r_n x_n$$

(It's easy to check that this is indeed a surjective homomorphism. This is, by the way, a standard trick in algebra. Remember it.)

Let N be a submodule of M. Its preimage $\phi^{-1}(N)$ is a submodule of R^n, and is therefore finitely generated. The images of these generators under ϕ therefore generate N, and so N is finitely generated. ♣