What the "hell" is a module?

Sachin Kumar
University of Waterloo, Faculty of Mathematics

Modules play a major part in modern mathematical research. It is a key character in the field of representation theory, also in the major area of Langland's program. A fun fact, a vector space is acually a module over a field. I hope this gives a motivation to explore this amazing field. In this essay, I will mostly try to talk above modules over Ring, (or you could say vector spaces over rings), which is kind of restrictive and non-trivial, but more elegant than, over fields. I would request the reader to know, what a group, ring and an ideal is, at a minimum!

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 are pure mathematicians, though, so we will give a rigorous definition.

Definition. Let R be a commutative ring. A R-module is an Abelian group M and a function $\cdot : R\times M \to M$ satisfying the following axioms: For all $r, r_1, r_2 \in R$ and $m, m_1, m_2 \in M$,

1. $r(m_1 + m_2) = rm_1 + rm_2$
2. $(r_1 + r_2)m = mr_1 + mr_2$
3. $r_1(r_2m) = (r_1r_2)m$
4. $1m = m$

So for a module to make sense, you need to have a ring and a group. This 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 non-trivial, 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 (yeh!), and you can multiply it by elements of $\mathbb{Z}$ (heck yeh!). 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 a R-module. In fact, you can define an ideal to be an R-submodule of R. (An R-submodule of M is exactly what you think it is: it's a 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). 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 the reader 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 generally, if $\phi : R \to T$ is a homomorphism, then T is an R-module. This explains that R/I example too.

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

Definition. Let M and N be R-modules. An R-module homomorphism, $M \to N$ is a homomorphism $f : M \to N$ 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 thats admit a two-sided inverse that is also an R-module homomorphism, a bijective one.

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. Proving this is trivial, just use some theories in linear algebra.

Complex conjugation defines a $\mathbb{Z}$-module homomorphism, $\mathbb{Z}[i] \to \mathbb{Z}[i]$. This is also a homomorphism of rings. The function $x \mapsto 2x$ 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, that the proof here is very easy and that the image and pre-image 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. Let M be a R-module, $S \subset M$. 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. 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. □

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

Theorem. 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,

$$M = R^n = \underbrace{R \times R \times \cdots \times R}_{n \text{ times}}$$

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 a 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. 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}, ie., $N_1 \cong R^{n-1}$, and so it is finitely generated.
Let $N_2 = \pi_n(N) \subset R$, where $\pi_n : R^n \to R$ is the projection onto the n-th coordinate. In other words, let N_2 be the set of elements of R that appear as the n-th 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 the generators for N_1, and let $y_1, \ldots, y_t$ be elements of N whose n-th coordinates are generators for N_2. For any $m \in N$, we can find an R-linear combination of the y_i whose n-th coordinate is the same as that of m. In other words, we can find $r_1, \ldots, r_t \in R$ such that the n-th coordinate of the following element of M is zero:

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

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

$$m - r_1 y_1 - \cdots - r_t y_t = r_1' x_1 + \cdots + r_s' x_s$$

Reorganizing 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 $\phi : R^n \to M$, mapping the standard basis vectors to the n generators $\{x_1, \ldots, x_n\}$ of M:

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

It's easy to check that this is indeed a surjective homomorphism. This is, by the way, a standard trick in algebra. Let N be a submodule of M. It's preimage $\phi^{-1}(N)$ is 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. Hence we are done! □