Modules!

Abstraction Presentation

Or: Division is Nice

David Freifeld

April 28, 2022

Aside: Fields as Vector Spaces

...over *themselves*

- Fields technically satisfy our properties of a vector space!
- For example, $\mathbb{R}$ (our vector space) over $\mathbb{R}$ (our scalars):
  1. $\mathbb{R}$ is closed under addition
  2. $\mathbb{R}$ is closed under scalar multiplication by $\mathbb{R}$
  3. $\mathbb{R}$ has an additive identity (by def. of field)
  4. $\mathbb{R}$ has an additive inverse (by def. of field)
  5. $\mathbb{R}$ has an multiplicative identity (by def. of field)
  6. $\mathbb{R}$ is associative (by def. of field)
  7. $\mathbb{R}$ is commutative (by def. of field)
  8. $\mathbb{R}$ over $\mathbb{R}$ has distributive properties
- We'll be using this type of logic for examples of modules.

What's a Module?

Let R be a commutative ring with an identity. A *module* over R (or R-module) is a nonempty set M with two operations. The first operation, addition, assigns to each pair $(u, v) \in M \times M$ an element $u + v \in M$. The second operation, juxtaposition, assigns to each pair $(r, u) \in R \times M$ an element $rv \in M$.

Additionally, the following conditions must hold:

1. M is an abelian group under addition.
2. For all $r, s \in R$ and $u, v \in M$:
   - $r(u + v) = ru + rv$
   - $(r + s)u) = ru + su$
   - $(rs)u = r(su)$
   - $1u = u$

What's a Module?

Let R be a $\overbrace{\text{commutative ring}}^{\textbf{main change}}$ with an identity. A *module* over R (or R-module) is a nonempty set M with two operations. The first operation, addition, assigns to each pair $(u, v) \in M \times M$ an element $u + v \in M$. The second operation, scalar multiplication, assigns to each pair $(r, u) \in R \times M$ an element $rv \in M$.

Additionally, the following conditions must hold:

1. M is an $\underbrace{\text{abelian group}}_{\textit{commutative group}}$ under addition.
2. For all $r, s \in R$ and $u, v \in M$:
   - $r(u + v) = ru + rv$
   - $(r + s)u) = ru + su$
   - $(rs)u = r(su)$
   - $1u = u$

~~What's a Module?~~ What's a "commutative ring"?

- A ring has all the same properties as a field with two key differences:
  1. Commutativity is not required
  2. Multiplicative inverses are not required
- We're operating on a *commutative ring* and so the only actual change is the loss of a multiplicative inverse for our scalars

What can we now do?

- There are some familiar sets we know of that don't have multiplicative inverses!
- One big one is the *integers*, $\mathbb{Z}$
- Another is the set of polynomials $\mathcal{P}^n$
- Wouldn't it be nice to be able to apply linear algebra logic to these spaces?
- We don't really divide things in linear algebra... surely it'd be fine to remove multiplicative inverses, right?

Linear Dependence

- Take the module $\mathbb{Z}$ over $\mathbb{Z}$ (think back to the first aside)
- We can easily show linearly dependent vectors where no vector is in the span of the previous vectors:

$$a_0 v_0 + a_1 v_1 = 0$$

$$\text{Let } a_0, a_1 = 2, -3 \text{ and } v_0, v_1 = 3, 2.$$

$$2(3) - 3(2) = 0$$

$$2 \notin \text{span}(3)$$

- Uh oh! The Linear Dependence Lemma no longer applies!
  - In fact, if you think back to Axler, we actually used division to prove it!

Whoops!

The Linear Dependence Lemma is important...

- We use the Linear Dependence Lemma for a lot of things, and now none of them apply!
  - Length of linearly independent lists are now not necessarily $\leq$ length of spanning lists
  - Spanning lists don't have to contain a basis
  - Linearly independent lists don't necessarily extend to a basis
- This has rippling consequences (because now everything that depended on what depended on the Linear Dependence Lemma no longer applies!), which we'll get to in a bit.

Torsion Elements

Say goodbye to the last of your intuition about linear independence.

- Modules are able to have no linearly independent elements.
- You may think "How is this possible — a list containing a single nonzero vector will always be linearly independent!"
- This is no longer true. Take the module $\mathbb{Z}/6$ over $\mathbb{Z}$.
  - Any element in $\mathbb{Z}/6$ times 6 (or any multiple of it) will equal zero.
  - As a result, there are $r \in \mathbb{Z}$ s.t. $r \neq 0$ yet $rz = 0$ for $z \in \mathbb{Z}$
  - Thus there will always be nontrivial linear combinations of a single vector v that are equal to zero.
- Nasty scalars like this are called *torsion elements*. The set of all these elements is called the *annihilator* (no relation to the other annihilator in linear algebra).

Whoooops!

Even more things fall apart now.

- We no longer necessarily have linearly independent elements!
  - Modules need not have bases
  - Anything that depends on bases, like FToLM, is gone!

Submodules & Finitely-Generated Modules

- We can define submodules in a similar manner to subspaces:
  - A submodule of an R-module M is a nonempty subset S of M that is also an R-module under the operations obtained by restricting the operations of M to S
- There's a few formal vocabulary switches:
  - The submodule *generated* (or spanned) by a subset S of a module M is the set of all linear combinations of elements of S.
  - A module is *finitely-generated* if it contains a finite set that generates M.

Infinite submodules

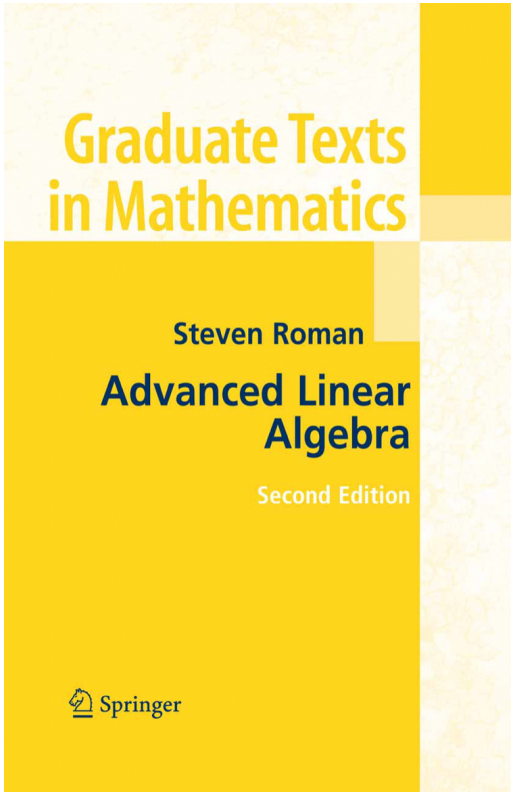
...of *finite* modules!?

- You can have finite modules with infinite submodules!
- Let R be the ring of polynomials with infinite variables $x_1, x_2, ...$ over a field F. Each element in R is however comprised of finite amount of these variables.
- Then, consider R as a module over R.
  - This module will be finitely generated by the identity element 1. Intuitively, since our scalars are also polynomials, you can think of this as saying every polynomial can be generated by multiply every polynomial by 1.
  - Consider the submodule S of all polynomials with no constant term. What do you multiply all the polynomials (your scalars) by s.t. you will get all polynomials with no constant term? The variables $x_1, x_2, ...$ themselves.
  - $x_1, x_2, ...$ is an infinite set, and thus S is not finitely generated.

Submodule Complements Need Not Exist

- In Axler, we proved that every subspace S has a complement U s.t. $S \oplus U = V$.
- This isn't the case with submodules!
- Take the set $\mathbb{Z}$ as a $\mathbb{Z}$-module. One of the properties of $\mathbb{Z}$ is that all of its submodules are *cyclic* (generated by one element), and as a result each submodule is the set of multiples of an integer.
- Hence, any two proper submodules N, M of $\mathbb{Z}$ have a nonzero intersection equal to $\text{lcm}(n, m)$, where n and m are the elements generating N and M.
- As a result, the only submodules that could ever have a complement are $\mathbb{Z}$ and $\{0\}$.

Where To From Here?



- I've been summarizing the fourth chapter of Steven Roman's *Advanced Linear Algebra*.
- There's another two chapters about modules!
- Most of them (and some of chapter 4!) is dedicated to reasoning about how we actually *work* with these things and make rules such that they're usable.

It Could Be Worse

We've only discussed "well behaved" modules.

- The requirement that our modules be over *commutative* rings is something we imposed for convenience.
- We can also have modules over *noncommutative* rings, which causes more problems.
  - Modules over noncommutative rings can have bases of different sizes
  - If $v_1, \ldots, v_n$ is linearly independent over R, this is not necessarily true for $r_1 v_1, \ldots, r_n v_n$ in the case of noncommutative rings.

It Could Be *Even* Worse

- We can generalize further.
- You can consider modules over *semirings*.
  - Semirings don't need to have additive inverses.
- You can consider modules over *near-rings*.
  - Near-rings are the general term for sets satisfying less axioms than a ring. All this fuss was only the removal of *one* rule, so things get even more broken if you remove more core ones.
- You can also describe this even more abstractly with category theory, but my eyes started to glaze over when reading about that.