Module Theory 2
More module properties, the isomorphism theorems, exact sequences
by Ivan Aidun

These are notes interspersed with exercises. The purpose of these notes is to be more fleshed out than Evan Dummit's old notes, but shorter and more focused than a textbook treatment. Halfway between Dummit and Dummit and Foote, so to speak. I hope these are helpful to you!

Properties of general modules

In the previous set of notes, we focused on the very nice properties of modules over PIDs. In these notes, we will talk about more general modules, and how much their behavior can differ from that special case.

Free modules

We might hope that for a given free module F, the number of elements in any basis for F is the same. It turns out that for some noncommutitive rings this can actually fail, but luckily for commutative rings it is true. I am including the proof of this statement because it is one example of proving a theorem for modules over a ring by somehow reducing that theorem to a statement about vector spaces. This might seem like a tricky trick the first time you see it, but it's an important method in algebra generally.

Proposition. If R is a commutative ring, then any basis for the free module R^m has m elements.

Proof. We can prove this by reducing it to the situation of a vector space over a field. Suppose we have an isomorphism $R^m \xrightarrow{\sim} R^n$, and take any maximal ideal $\mathfrak{m} \in R$. (On the Ring Theory I sheet we asserted that every ring has a maximal ideal, and hinted at an argument involving Zorn's Lemma.) Then the isomorphism must take the submodule $\mathfrak{m}^m \subset R^m$ to $\mathfrak{m}^n \subset R^n$, so it passes to an isomorphism on the quotients $(R/\mathfrak{m})^m \xrightarrow{\sim} (R/\mathfrak{m})^n$. But now this is an isomorphism of vector spaces over the field $R/\mathfrak{m}$, so we know $m = n$.

This property is sometimes called the Invariant Basis Number (IBN) property. For rings with IBN, the number of elements in a basis for a free module is called the **rank** of the free module. For integral domains, the rank has another nice description: given a free module F, we can extend scalars to $K = \operatorname{Frac} R$ to get a vector space F_K. A basis for F remains a basis for F_K, so the rank of F is equal to the dimension of F_K.

Warning. In this context, the word "dimension" is reserved exclusively to refer to the dimension of a vector space over a field. The number of generators needed to generate a module unfortunately does not have a name of its own (at least, not one I'm aware of), but you should conceptually separate in your mind the generators of a module from any notion of dimension. Even in the case of free modules over integral domains, where the rank is equal to the dimension of some vector space, nevertheless it should be referred to as the "rank" and not the "dimension".

One reason for this is that a module might be both an R-module and *also* a vector space, for example if $R = \mathbb{C}[x]$, and the number of generators required as an R-module could be different from the dimension of the vector space. For example, $\mathbb{C}[x]/(x^4)$ is a 4-dimensional complex vector space, but it is spanned by the single element 1 as a $\mathbb{C}[x]$-module.

One might guess, based on our prior experience with vector spaces and modules over PIDs, that a submodule of a free module $G \subset R^n$ should be another free module, and that $\operatorname{rank} G \leq n$. Unfortunately, this is not necessarily the case.

Exercise 1. Let $R = \mathbb{C}[x, y]$, and consider R as a free module over itself of rank 1. Find a submodule of R that is not free.

The good news is that our proof above that any basis for a free module over a commutative ring has the same number of elements can be adapted to show that if $G \subset R^n$ happens to be a free module, then $\operatorname{rank} G \leq n$.

Any free module is torsion-free, and hence so is any submodule of a free module. However, your example in Exercise 1(b) shows that over a non-PID there can be torsion-free modules that are not free, even over a UFD, which seems like it would be the next best thing. The next exercise shows that, at the very least, for any finitely-generated torsion-free module, that module can be realized as a submodule of a free module.

Exercise 2. Let M be a finitely-generated torsion-free module over an integral domain R. We will prove that M can be injected into a free module of finite rank.

(a) Prove that M contains a finite-rank free module.

(b) Let $F \subset M$ be a maximal free module. Prove that M/F is torsion.

(c) Prove that there is some $r \in R$ so that $rM \subset F$. (Hint: look at Module Theory 1, Exercise 10.)

(d) Prove that the "multiplication by r" map above is injective, so this realizes the injection we wanted.

The above exercise actually gives us the power to prove part of the classification theorem for finitely-generated modules over PIDs. (I stated this as a consequence of the classification theorem, but I don't know of a proof of the classification theorem that doesn't use this fact.)

Exercise 3. Suppose R is a PID. Let $G \subset R^n$ be a submodule. Use the above exercise to show that G is free.

Other important properties a module can have

A module is **simple**, or sometimes **irreducible**, if it has no nonzero proper submodules. Note that a ring is simple iff it is a simple module over itself. For a module M, the **annihilator** of M, $\operatorname{Ann}(M)$, is the set of all $r \in R$ that kill every $m \in M$. In symbols: $\operatorname{Ann}(M) = \{r \in R : \forall m \in M, rm = 0\}$.

Exercise 4. Prove that $\operatorname{Ann}(M)$ is an ideal of R.

Exercise 5.

(a) Prove that a module M is simple if and only if it is cyclic and any nonzero $m \in M$ is a generator.

(b) Prove that if M is simple, then $\operatorname{Ann}(M)$ is a maximal ideal.

(c) Prove that if M is simple, then $M \cong R/\operatorname{Ann}(M)$.

(d) Give an example of two non-isomorphic simple $\mathbb{Z}$-modules.

(e) Give an example of two non-isomorphic simple $\mathbb{R}[x]$-modules.

(f) **(Frequent Problem 1 example)** How many non-isomorphic simple (left) $M_2(\mathbb{C})$-modules can you think of? Prove that you found them all.

A module is **Noetherian** if its submodules satisfy the Ascending Chain Condition. As with "simple", a ring is Noetherian iff it is a simple module over itself.

Example 1.

- Similar to rings, a module is Noetherian iff all of its submodules are finitely generated.
- Any finitely-generated module over a Noetherian ring is also Noetherian.
- There can be Noetherian modules over non-Noetherian rings. The zero module is always Noetherian, as is any simple module, and we showed above that every ring has a simple module since every ring has a maximal ideal.
- There can be non-Noetherian modules over Noetherian rings. **Exercise 6.** Prove that $\mathbb{Q}$ is not a Noetherian $\mathbb{Z}$-module by demonstrating an infinite ascending sequence of submodules. (Incidentally, this proves that $\mathbb{Q}$ is not a finitely-generated $\mathbb{Z}$-module.)

The isomorphism theorems

Below, all modules are modules over a single ring R.

Theorem (first isomorphism theorem)**.** Let $\phi\colon M \to N$ be a homomorphism of R-modules. Then $\ker\phi$ is a submodule of M, $\operatorname{im}\phi$ is a submodule of N, and the induced homomorphism $M/\ker\phi \to \operatorname{im}\phi$ is an isomorphism. In particular, if ϕ is surjective, then $N \cong M/\ker\phi$.

Theorem (second isomorphism theorem)**.** Let M be an R-module, $N_1, N_2 \subset M$ submodules. Then $N_1 + N_2 = \{n_1 + n_2 : n_1 \in N_1,\ n_2 \in N_2\}$ is a submodule of M, N_2 is a submodule of $N_1 + N_2$, $(N_1 + N_2)/N_2$ is a submodule of M/N_2, $N_1 \cap N_2$ is a submodule of N_1, and the composition $N_1 \hookrightarrow M \twoheadrightarrow M/N_2$ induces an isomorphism $N_1/(N_1 \cap N_2) \xrightarrow{\sim} (N_1 + N_2)/N_2$.

Theorem (third isomorphism theorem)**.** Let M be an R-module, N a submodule. Then if P is an submodule of M such that $N \subset P \subset M$, then P/N is a submodule of M/N, and the composition $M \twoheadrightarrow M/N \twoheadrightarrow (M/N)/(P/N)$ induces an isomorphism $M/P \xrightarrow{\sim} (M/N)/(P/N)$.

Theorem (lattice theorem)**.** The correspondence that takes a submodule $P \subset M$ containing N to the quotient P/N gives a bijection

$$\{\text{submodules of } M \text{ containing } N\} \xrightarrow{\sim} \{\text{submodules of } M/N.\}$$

Furthermore, this bijection preserves inclusions, sums, and intersections.

Exact sequences

It feels like about time to talk about exact sequences. If A, B, C are R-modules, a sequence of homomorphisms $A \xrightarrow{f} B \xrightarrow{g} C$ is called **exact** if $\operatorname{im} f = \ker g$. A longer sequence of homomorphisms

$$A_1 \to A_2 \to A_3 \to A_4 \to \dots$$

is called exact if every three-module sequence (two-arrow sequence) is exact.

Example 2.

- For every module A, there is only one homomorphism from the zero module to A. A sequence of the form $0 \to A \xrightarrow{f} B$ is exact if and only if $\ker f = 0$, that is, iff f is injective.

- For every module C, there is only homomorphism from C to the zero module. A sequence of the form $B \xrightarrow{g} C \to 0$ is exact if and only if $\operatorname{im} g = C$, that is, iff g is surjective.

- Combining the above, saying that $\phi\colon A \to A'$ is an isomorphism is the same as saying that the sequence $0 \to A \xrightarrow{\phi} A' \to 0$ is exact.

- A situation common enough to get its own name is the situation where you have an exact sequence that looks like
$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0.$$

  Such a sequence is called a **short exact sequence** (often abbreviated SES), not because it's the shortest possible exact sequence, but because in practice it's the shortest exact sequence that really matters. By the above, saying that this is a short exact sequence is the same as saying that

  - f is injective,
  - g is surjective, and
  - $\operatorname{im} f = \ker g$.

You should think about a short exact sequence as encapsulating all the information of the first isomorphism theorem: the first isomorphism theorem can be rephrased as saying that for any short exact sequence as above, we have that $C \cong B/\operatorname{im} f$.

- We said earlier that a module is finitely generated iff it admits a surjective map from a finite-rank free module. We could recast this as saying a module is finitely generated iff there exists an exact sequence

  $$R^n \xrightarrow{f} M \to 0$$

  If R is a PID, then the kernel of this map is a submodule of R^n, and hence is free and of rank $k \leq n$, so we get a short exact sequence

  $$0 \to \ker f \cong R^k \to R^n \xrightarrow{f} M \to 0.$$

  One way to prove the classification theorem for modules over a PID is to prove that any map $R^k \xrightarrow{g} R^n$ can be written in a special form that reveals information about the quotient $R^n/\operatorname{im} g$. This is the theory of **Smith Normal Form**, which I love but will not discuss further in these notes.

- If R is not a PID, then the kernel of the surjection $R^n \to M \to 0$ need not be another free module, but it will be a finitely-generated module, so we can get another surjection $R^{n_2} \to \ker f \to 0$. Then we can look at the kernel of f_2, and get a surjection from a free module onto that, and so on. In the end, we get what is called a "free resolution" of the module M, which is an exact sequence:

  $$0 \leftarrow M \xleftarrow{f_1} R^{n_1} \xleftarrow{f_2} R^{n_2} \xleftarrow{f_3} R^{n_3} \leftarrow \ldots.$$

  (I sometimes write long sequences like this "backwards", which is a habit I learned from Daniel Erman, and which many of his students do as well. Among the benefits of writing it this way is that the indexing on the page goes in the correct order.)

The concept of exact sequences is more general than modules, you can also talk about exact sequences of groups, or pretty much any other algebraic thing. For example, there is a short exact sequence of groups

$$1 \to \{\pm 1, \pm i\} \to Q \to \mathbb{Z}/2\mathbb{Z} \to 1,$$

where here I'm writing 1 to mean the trivial group, and Q is the quaternion group $\{\pm 1, \pm i, \pm j, \pm k\}$.

You can find a nice visual metaphor for exact sequences in Ravi Vakil's lovely Puzzling Through Exact Sequences. It might be helpful to read, but don't feel bad if at some point you get lost because it does get quite advanced (eventually discussing spectral sequences).

Splitting short exact sequences

A short exact sequence

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is said to **split on the right** if there is a map $s\colon C \to B$ so that $g \circ s = \mathrm{id}_C$ (that is, for every $c \in C$, $g(s(c)) = c$). The map s is called a **(right) splitting homomorphism/map**, or often just a **splitting**. You will often see splittings notated in the following way:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] \arrow[l, bend left, "s"] & 0. \end{tikzcd}$$

Similarly, a SES is said to **split on the left** if there is a map $\sigma\colon B \to A$ so that $\sigma \circ g = \mathrm{id}_A$.

Exercise 7. Let

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

be a short exact sequence of R-modules.

(a) Show that the sequence splits on the right if and only if there is a submodule $C' \subset B$ so that $g\colon C' \to C$ is surjective and B is the internal direct sum of $f(A)$ and C'. (This is why the map s is called a "splitting". Its existence "splits" B up into the direct sum of two smaller things.)

(b) Show that the sequence splits on the left if and only if it splits on the right.

Thus, for modules, actually people will usually just say a sequence **splits** (or sometimes "is split" or sometimes "is split exact") if it splits on either side, since they are the same.. You might be confused about why I told you about splitting on the left versus right at all if I was just going to turn around and tell you they're the same. The reason is that they happen to be the same for modules, but they are not the same for groups (to be discussed in the notes on groups), and they may not be the same in some other algebraic context you encounter later in life. In general, splitting on the right is the less restrictive notion, and it's usually what people will default to when they talk about a SES "splitting".

Exercise 8.

(a) (Low ball) Give an example of an exact sequence of abelian groups ($\mathbb{Z}$-modules) that splits.

(b) Give an example of an exact sequence of abelian groups that does *not* split.

(c) Give an example of an exact sequence of $\mathbb{C}[x]$-modules that does not split.

Exact sequences that don't split are frequently asked-for examples in Problem 1s on the qual. See August 2021 Problem 1 (e) and August 2018 Problem 1 (a).

Exercise 9. If you don't remember much group theory, come back to this question later.

(a) Prove that the exact sequence of groups

$$1 \to \{\pm 1, \pm i\} \to Q \to \mathbb{Z}/2\mathbb{Z} \to 1$$

does not split on either the right or the left.

(b) Prove that the exact sequence of groups

$$1 \to \langle r \rangle \to D_5 \to \mathbb{Z}/2\mathbb{Z} \to 1$$

splits on the right but not on the left. (Here, D_5 is the dihedral group of order 10, presented as $\langle r,\, s \mid r^5 = s^2 = srsr = e\rangle$.)

Exercise 10. Let A, B be R-modules, and suppose there is a short exact sequence

$$0 \to A \xrightarrow{f} B \xrightarrow{g} R^n \to 0.$$

(a) Prove that this sequence splits. (Hint: show it splits on the right.)

(b) Suppose $R = k$ is a field, so that A, B are k-vector spaces. Show that part (a) is the same thing as the rank-nullity theorem. (In fact, your argument is also the argument used to prove the rank-nullity theorem, but saying "module" everywhere instead of "vector space".)

Exercise 11. Suppose you had a function λ that took in a module and output some integer. We say λ is **additive** if for every SES

$$0 \to A \to B \to C \to 0$$

we have $\lambda(B) = \lambda(A) + \lambda(C)$.

(a) Show that the function $\dim V$ is additive on finite-dimensional k-vector spaces.

(b) Let λ be an additive function, and let

$$0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$$

be an exact sequence of modules. Show that we can do a sort of "inclusion-exclusion" on the sequence to get

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0.$$

Why are they called "exact" sequences?

The terminology of exactness originally came from algebraic topology. In topology, you come across the situation in which you have a sequence of homomorphisms of abelian groups (a.k.a. $\mathbb{Z}$-modules)

$$0 \leftarrow C_0 \xleftarrow{\partial_1} C_1 \xleftarrow{\partial_2} C_2 \xleftarrow{\partial_3} \dots$$

and for geometric reasons these maps satisfy $\partial_i \circ \partial_{i+1} = 0$. Another way of saying that is that $\operatorname{im} \partial_{i+1} \subset \ker \partial_i$. One thing that matters in this situation is when it is the case that $\operatorname{im} \partial_{i+1} = \ker \partial_i$, that is, you care about when the image of one is *exactly* the kernel of the next, not just some smaller thing inside the kernel. That is to say, you want to know if the above sequence is exact at i, and if it isn't you want to quantify in some way how not-exact it is.