Modules > Ideals

Isaac Cheng

August 3, 2025

1 Motivation

How can we best understand a given ring? At PROMYS, we're taught to analyze rings by characterizing important elements - units, primes, and so on. Issues distinguishing between associates in rings like $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ may lead us to define ideals, since two associate elements $a \sim b$ generate the same ideal $(a) = (b)$. Ideals also let us define quotient rings and help unify useful definitions like fields (no nontrivial ideals), PIDs (all ideals principal), and Noetherian rings (ascending chain condition). However, these ring-theoretic constructions can often feel clunky and unmotivated. Surely there is a way to phrase these constructions in a ~~more categorical~~ prettier way.

Algebraists like to say that one can understand a ring R just by examining its category R-Mod of (left-)modules. Without specifics, though, this sounds like normal unapplicable categorical nonsense. With the goal of indoctrinating as many mathematicians as possible into the cult of categorical thinking, this seminar will discuss one specific way that R-Mod sheds light on R: free resolutions of modules.

2 Understanding Modules

2.1 Modules : Rings :: Group Actions : Groups

Recall that for any object A in a category C, the automorphisms of A define a group $\mathrm{Aut}_{\mathsf{C}}(A)$. This allows us to define **group actions** on A:

Definition 2.1. *For a group G, an **action** of G on an object A of a category C is a homomorphism $\sigma : G \to \mathrm{Aut}_{\mathsf{C}}(A)$.*

Here are some examples of famous group actions:

Category	Examples of Group Actions
Set	G-Sets (G acts by permutations)
Vect_k	Group representations
Group	(Left-)multiplication, conjugation
Top	G-Spaces

It is very standard to understand groups by examining their actions — indeed, this is in some sense the purpose of representation theory! Suppose we wish to do the same for rings. The problem is then to find a categorical construction that forms a ring in the same way that automorphisms form a group.

Remark 2.2. *For any abelian group A, the endomorphisms $\mathrm{End}_{\mathsf{Ab}} A$ form a ring.*

The key here is that for abelian groups A, B, the homomorphisms $\mathrm{Hom}_{\mathsf{Ab}}(A, B)$ form an abelian group, not just a set. We say that Ab is an **Ab-enriched category**.[1] We can now define modules:

Definition 2.3. *For a ring R, a **left R-module** is an abelian group A with a ring homomorphism $\sigma : R \to \mathrm{End}_{\mathsf{Ab}}(A)$. For conciseness, we will write ra instead of $\sigma(r)(a)$.* [2]

For the purpose of this talk, all rings will be commutative, so the difference between left and right modules is irrelevant. You may have learned a different definition of module using element-wise definitions, but one can check that the two are the same.

Exercise 2.4. *Check that the following properties hold for a ring R and a left-module $\sigma : R \to \mathrm{End}_{\mathsf{Ab}}(A)$:*

1. $r(a + b) = ra + rb$
2. $(r + s)(a) = ra + sa$
3. $(rs)a = r(sa)$
4. $1a = a$

Modules may seem strange, but some examples is very familiar!

Remark 2.5. *A $\mathbb{Z}$-module is the same thing as an abelian group.*

Remark 2.6. *If R is a field, R-modules are the same things as vector spaces.*

Remark 2.7. *A ring R is a module over itself, with action by left-multiplication. Ideals of R are also modules.*

Remark 2.8. *For any indexing set A, the direct sum $R^{\oplus A}$ (viewing R as an abelian group) is an R-module with action by left-multiplication.*

[1] It is notable that Ab is enriched over itself, much like Set. We say that Ab is a **closed category**, and this gives us many nice properties to work with.

[2] A right R-module would be a ring homomorphism $R^{op} \to \mathrm{End}_{\mathsf{Ab}}(A)$.

2.2 The Category R-Mod

It should be no surprise that (left-)modules over a ring form a category, which we call R-Mod. For modules M, N over a ring R, a homomorphism of modules is a group homomorphism $\varphi : M \to N$ respecting the ring operation. Namely, we must have:

$$\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$$
$$\varphi(rm) = r\varphi(m)$$

If R and S are isomorphic rings, then R-Mod and S-Mod are isomorphic (and thus equivalent) as categories. What may be surprising is that a converse holds:

Theorem 2.9. *Let R, S be commutative rings. R-Mod and S-Mod are equivalent categories iff R and S are isomorphic.*[3]

Philosophically, this means that all the data of a commutative ring R is contained in the category R-Mod. Now we can pull out our categorical toolbox and get to work.

3 Free Resolutions of Modules

3.1 A Crash Course in Homological Algebra

A key concept ahead will be the idea of an **exact sequence** of modules.

Definition 3.1. *A sequence $\ldots \to M_i \xrightarrow{d_{i+1}} M_{i+1} \xrightarrow{d_{i+2}} M_{i+2} \xrightarrow{d_{i+3}} \ldots$ is **exact** iff im $d_n = \ker d_{n+1}$ for all n.*

We note that exact sequences easily encode several key properties of modules:

Exercise 3.2. $A \xrightarrow{\varphi} B \to 0$ *is exact iff φ is surjective.*

Exercise 3.3. $0 \to A \xrightarrow{\varphi} B$ *is exact iff φ is injective.*

Exercise 3.4. $0 \to A \xrightarrow{\varphi} B \to 0$ *is exact iff φ is an isomorphism.*

Exercise 3.5. $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ *is exact iff $C \cong B/A$.*

The ability of exact sequences to encode these properties makes them ideal[4] for what we intend ahead. They allow us to understand homomorphisms without ever using "element-wise" properties like injectivity, surjectivity, and bijectivity.

[3] If R,S are general rings, then R-Mod and S-Mod are equivalent iff their centers are isomorphic. This result for commutative rings is a corollary.

[4] No pun intended.

3.2 Free Modules

Definition 3.6. *A module M is* ***finitely generated*** *iff there exists an integer m and homomorphism $\pi : R^m \to M$ such that $R^m \xrightarrow{\pi} M \to 0$ is exact. This encodes that $M = R^m / \ker \pi$.*

Definition 3.7. *A module M over a ring R is* ***free*** *if there exists a basis B such that $R^{\oplus B} \cong M$ as modules; that is, if there exists $\varphi : R^{\oplus B} \to M$ such that $0 \to R^{\oplus B} \xrightarrow{\varphi} M \to 0$ is exact. In this case, every element of M can be written as a linear combination of elements of B with coefficients in R.*

These two definitions let us characterize fields in a completely element-free and ideal-free way.

Lemma 3.8. *Let R be an integral domain. R is a field iff every finitely generated R-module is free.*

Proof. Let R be a field and M be an R-module. Let $S \subseteq M$ be a linearly independent subset. Now there exists a maximal linearly independent subset B containing S by Zorn's Lemma.[5] This must generate all of M by a maximality argument, so it is a basis, so $R^{\oplus B} \cong M$ and M is free.

Let R be a ring such that every finitely generated R module is free. Let $r \in R$ nonzero. If r is not a unit, then $R/(c)$ is nonzero. Since it is generated by 1, it is finitely generated and thus free. This means all elements are linearly independent, but $1 \cdot c = c = 0$, a contradiction. Thus c is a unit so R is a field. □

At first glance, this seems like a whole lot of machinery for a simple statement we all already knew — that vector spaces are free. But we can generalize.

Definition 3.9. *For an R-module M, a* ***free resolution of length*** *i is an exact sequence $0 \to R_1^m \to \ldots \to R^{m_{i+1}} \to M \to 0$.*

Before going into results, let's do some exercises.

Exercise 3.10. *Find a free resolution of $\mathbb{Z}$ over $R = \mathbb{Z}[x, y]$, where x, y act by 0.*[6]

Exercise 3.11. *Find a free resolution of the ideal $(2, x)$ over $R = \mathbb{R}[x]$, where x acts by 0.*[7]

It seems like the more complicated the ring, the longer our free resolution may need to be. This turns out to be true in a very precise way.

[5] This is not actually necessary for the finitely generated case.

[6] ANSWER: $0 \to R \xrightarrow{d_2} R^2 \xrightarrow{d_1} R \xrightarrow{\pi} \mathbb{Z} \to 0$, where $d_1(m, n) = mx + ny, d_2(m) = (ym, -xm)$.

[7] ANSWER: $0 \to R \xrightarrow{d_2} R^2 \xrightarrow{d_1} (2, x) \to 0$, where $d_1(m, n) = 2m + xn$ and $d_2(m) = (xm, -2m)$.

Remark 3.12. *R is a field iff every R-module has a free resolution of length* 0.

Now, it's time to generalize. For what rings R does every R-module have a free resolution of length 1? That is, if fields are the nicest rings, what are the second-nicest rings?

Theorem 3.13. *An integral domain R is a PID iff for every finitely generated R-module M, every exact sequence $R^{m_0} \to M \to 0$ can be completed to a free resolution $0 \to R^{m_1} \to R^{m_0} \to M \to 0$.*[8]

Proof. Suppose the latter statement holds. Let I be an ideal of R and let $M = R/I$, so $R \xrightarrow{\pi} M \to 0$ is exact. This can be completed to a free resolution $0 \to R^m \xrightarrow{\psi} R \xrightarrow{\pi} M \to 0$, so $\operatorname{im} \psi = R^m / \ker \psi = \ker \pi = I$. This gives an exact sequence $R^m \to I \to 0$, so I is free. Since I is a free submodule of R, which is free of rank 1, rank $I \leq R$, so I is principal.

The converse follows from the classification of finitely generated modules over PIDs.[9] $\square$

In conclusion, fields are the rings that allow us to complete resolutions of length 0, and PIDs are the rings that allow us to complete resolutions of length 1. We could now ask about rings that let us complete longer resolutions, although they don't have such familiar names.

4 Concluding Thoughts

Inspired by how groups are characterized by their actions, we defined modules as ring actions on abelian groups. We discovered that the category R-Mod contains the data of R up to isomorphism, and wondered how to extract this data using our categorical toolbox. One option wound up being free resolutions, where we were able to use exact sequences of modules to characterize both fields and PIDs. There is much left to learn on this topic, which we encourage the reader to explore!

[8]This may seem like a strange way of phrasing the statement. But note that a module M is the same as an exact sequence $M \to 0$, and for fields we wanted to be able to complete these to exact sequences $0 \to R^m \to M \to 0$.

[9]Translation: we drop a giant nuke on the problem and it works.