# Math 250A Lecture 11 Notes

Daniel Raban

October 3, 2017

# 1 Modules

## 1.1 Basic notions and examples

### 1.1.1 Modules and homomorphisms

Informally, a module $M$ over a ring $R$ is like a vector space but over a ring.

**Definition 1.1.** A *(left) module* $M$ over a ring $R$ is an abelian group with a map $R \times M \to M$ sending $(r, m) \mapsto r \cdot m$ such that for $r, s \in R$ and $x, y \in M$

1. $r \cdot (x + y) = r \cdot x + r \cdot y$.
2. $(r + s) \cdot x = r \cdot x + s \cdot x$
3. $(rs) \cdot x = r \cdot (s \cdot x)$
4. $1_R \cdot x = x$ (if $R$ has 1).

A *right module* is the same thing, except the map is $M \times R \to R$, so the actions of $R$ on $M$ is on the right.

**Definition 1.2.** Let $M$ be an $R$-module. A *submodule* $N$ is a subgroup of $M$ such that $r \cdot n \in N$ for each $r \in R$ and $n \in N$.

**Definition 1.3.** A homomorphism of modules $M_1, M_2$ is a map $f : M_1 \to M_2$ such that

1. $f(m_1 + m_2) = f(m_1) + f(m_2)$
2. $f(r \cdot m) = r \cdot f(m)$.

Better (but not standard) notation would be that homomorphisms of left modules should be written on the right (and vice versa for right modules). So we should write $mf$, not $fm$. This makes it so the second condition gives us that $(rm)f = r(mf)$, which gets rid of the needless switching of the order of $r$ and $f$. We will alternate between the two notations.

**Definition 1.4.** Let $M, N$ be modules over $R$. Then $\mathrm{Hom}_R(M, N)$ is the set of module homomorphisms from $M$ to $N$.

If $R$ is commutative, $\mathrm{Hom}_R(M, N)$ is an $R$-module.

**Definition 1.5.** An *endomorphism* of $M$ is a homomorphism from $M$ to itself.

**Definition 1.6.** A *bimodule* is a left module over one ring and a right module over another, where the left and right actions commute.

**Example 1.1.** $R$ is an $(R, R)$ bimodule.

### 1.1.2 Exact sequences of modules

Suppose we have the exact sequence

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

Are the following two sequences exact?

$$0 \to \mathrm{Hom}(M, A) \to \mathrm{Hom}(M, B) \to \mathrm{Hom}(M, C) \to 0$$

$$0 \leftarrow \mathrm{Hom}(A, N) \leftarrow \mathrm{Hom}(B, N) \leftarrow \mathrm{Hom}(C, N) \leftarrow 0$$

The answer is no.[1] Look at

$$0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Then

$$0 \to \underbrace{\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})}_{=0} \xrightarrow{\times 2} \underbrace{\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})}_{=0} \to \underbrace{\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})}_{=\mathbb{Z}/2\mathbb{Z}} \cancel{\to 0}$$

$$\cancel{0 \leftarrow} \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \xleftarrow{\times 2} \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \leftarrow \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \leftarrow 0.$$

Instead, we get exact sequences

$$0 \to \mathrm{Hom}(M, A) \to \mathrm{Hom}(M, B) \to \mathrm{Hom}(M, C)$$

$$\mathrm{Hom}(A, N) \leftarrow \mathrm{Hom}(B, N) \leftarrow \mathrm{Hom}(C, N) \leftarrow 0.$$

We leave this as an exercise.

[1] The study of homological algebra is based on the fact that these sequences are not always exact in this way.

### 1.1.3 Examples of modules

**Example 1.2.** Vector spaces over fields are modules.

**Example 1.3.** Abelian groups are modules over $\mathbb{Z}$.

**Example 1.4.** Left ideals of $R$ are the same as left submodules of a module $R$.

**Example 1.5.** Let $G$ be a group acting on a set $S$. Form the vector space $V$ over $K$ with basis $S$, and form the group ring $K[G]$. $G$ acts on $V$ by acting on the basis elements. So $V$ is a module over the ring $K[G]$.[2]

**Example 1.6.** Suppose $M$ is a left module over a ring $R$. Then $\mathrm{Hom}_R(M, M)$, the endomorphisms of $M$, is a ring, where the product is composition of endomorphisms. $M$ is a right module over $\mathrm{Hom}_R(M, M)$. Furthermore, the right action of $\mathrm{Hom}_R(M, M)$ commutes with the left action of $R$ on $M$ (follows from the definition of a homomorphism). So $M$ is a $\mathrm{Hom}_R(M, M)$ bimodule.

$\mathrm{Hom}_R(M, M)$ is analogous to the permutations of a set $S$. If we have a group, we can represent it as the permutations of the set $S$. Similarly, a ring is often studied as a subring of $\mathrm{Hom}_T(M, M)$ for some $T$-module $M$.

**Example 1.7.** Take an algebraic number field such as $\mathbb{Q}[i]$, where $i^2 = -1$. Think of $Q[i]$ as a vector space over $\mathbb{Q}$, and think of the ring $\mathbb{Q}[i]$ as endomorphisms of this vector space. So we can represent elements of $\mathbb{Q}[i]$ as matrices. Matrices are linear transformations of vector spaces or equivalently homomorphisms of modules.

Pick a basis of $\mathbb{Q}[i]$: $\{1, i\}$. The action of 1 is $1 \to 1$ and $i \to i$ and the action of $u$ is $1 \to i$ and $i \to -1$. So we have the matrices

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad i = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

So $\mathbb{Q}[i]$ can be thought of as the matrices

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

with $a, b \in \mathbb{Q}$.

Look at the invariants of matrices, the trace and the determinant. Here, $\mathrm{tr}(a+bi) = 2a$, and $\det(a + bi) = |a + bi|$.

[2] The study of these modules is very important in representation theory.

## 1.2 Free modules

**Definition 1.7.** The *direct sum* of modules $M_\alpha$ over $R$ is the abelian group $\bigoplus M_\alpha$ with the action of $R$ on each component $\alpha$ determined by the action of $R$ on $M_\alpha$.

**Definition 1.8.** A *free module* is a module that is a direct sum of copies of $R$.

In some sense, free modules are the simplest sort of module.

**Example 1.8.** Any vector space is a free module.

**Example 1.9.** $\mathbb{Z}$ is a free module over $\mathbb{Z}$. However, $\mathbb{Z}/2\mathbb{Z}$ is not free.

We want to define the *rank* of a free module as the number of copies of $R$ in the sum. Is this well defined? We must check that if $R^m \cong R^n$, then $m = n$. However this is not always true. When is this true?

- This is true when $R$ is a field.
- This is false if $R$ is the 0 ring.
- This is true if $R$ is commutative with $R \neq 0$.

  Pick a maximal ideal $I$ in $R$ and suppose $R^m \cong R^n$. Reduce mod $I$, so $(R/I)^m \cong (R/I)^n$ as modules over a field $R/I$. So $m = n$ because $R/I$ is a field.
- This is sometimes true if $R$ is not commutatative (see below).
- There exist rings $R \neq 0$ such that $R \cong R \oplus R$ as $R$ modules (see below).

**Example 1.10.** Take $R = M_n(K)$, the $n \times n$ matrices over a field $K$, and suppose $R^a \cong R^b$. These are vector spaces of dimension $an^2$ and $bn^2$, respectively, so $a = b$.

**Example 1.11.** Here is an example of a ring $R \neq 0$ such that $R \cong R \oplus R$ as $R$ modules. This is a possibly unsettling result. Homomorphisms from $R^m$ to $R^n$ can be identified with $m \times n$ matrices, as in linear algebra. If $R \cong R \oplus R$, we have a $1 \times 2$ invertible matrix!

Pick an abelian group $A$ such that $A \cong A \oplus A$, such as $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$. Put $R = \mathrm{End}(A)$; in our example, this is the set of $\infty \times \infty$ matrices with only finitely many nonzero entries in each row. Then $R = \mathrm{Hom}(A, A) = \mathrm{Hom}(A, A \oplus A) = R \oplus R$.

So the rank of a free $R$-module is not necessarily well-defined.

### 1.3 Projective modules

Given a free module $M$, we can recover the underlying set $S_M$; this is via a forgetful functor $F$ from the category of modules to the category of sets. Likewise, given a set $S$, we can form the free module $M_S$ with basis $S$; this is also via a functor, $F'$. These functors commute with morphisms in the following way:

$$\begin{tikzcd} M \arrow[r, "F"] \arrow[d, "f"] & S_M \arrow[d, "F(f)"] \\ N & S_N \arrow[l, "F'"] \end{tikzcd}$$

We say that the functors $F$ and $F'$ are *adjoint*. As a consequence, free modules are projective.

**Definition 1.9.** A *projective module* $P$ is a module with the following property. If the sequence $M \to N \to 0$ is exact, then any map $P \to N$ lifts to a map $P \to M$.

$$\begin{tikzcd} M \arrow[r] & N \arrow[r] & 0 \\ & P \arrow[u] \arrow[ul, dashed] & \end{tikzcd}$$

**Proposition 1.1.** *The following are equivalent:*

1. *$P$ is projective.*
2. *$P \oplus Q$ is free for some module $Q$.*

*Proof.* (1) $\implies$ (2) : Pick a free module $F$ so $\varphi : F \to P$ is onto. Then $F \to P \to 0$, so we can find a map $P \to F$.

$$\begin{tikzcd} F \arrow[r, "\varphi"] & P \arrow[r] & 0 \\ & P \arrow[u, "\mathrm{id}"] \arrow[ul, dashed] & \end{tikzcd}$$

But then $F$ splits as $P \oplus \ker(\varphi)$.

(2) $\implies$ (1): Exercise. $\square$

**Example 1.12.** $R = \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, so $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3/Z$ are projective over $\mathbb{Z}/6\mathbb{Z}$ but not free.

**Example 1.13.** Let $R$ be the ring of continuous functions on a circle $S^1$, and let $M = R$. Then we can think of $M$ as continuous functions $S^1 \to S^1 \times \mathbb{R}$. $M$ is sections of $S^1 \times \mathbb{R} \to S^1$, which equals the real valued functions on $S^1$. This is a *vector bundle*[3] over $S$.

[3] We won't be going over vector bundles in detail in this course. If you don't know what a vector bundle is, see a topology course.

Consider a Möbius band, and view it as a vector bundle over $S^1$, so each fiber is isomorphic to $\mathbb{R}$. Now define a module $N$ to be the sections of this twisted vector bundle. Then $N$ is projective but not free.

$N$ is not free because the orientations of the fibers change as you go around $S^1$. It is projective because $N \oplus N = M \oplus M$. At each point of $S^1$, consider the normal bundle. Now take the orthogonal complement. So we get 2 Möbius bands so at each point, and their fibers intersect at every point. So we can think of $N \oplus N$ as the sum of 2 Möbius bands.

In effect, we can think of projective modules as "twisted free modules."

**Example 1.14.** Let $R = \mathbb{Z}[\sqrt{-5}]$; we can think of this as a rectangular lattice in $\mathbb{C}$. Let $M = (2, 1 + \sqrt{-5})$. The principal ideals here are rectangular with respect to this lattice picture. Non-principal ideals are diamond shaped. Principal ideals here are free modules, and nonprincipal ideals are not free.

We want to show that $M$ is projective, and we do so by showing that $M = R \oplus R$. We map $g : R \oplus R \xrightarrow{\text{onto}} M$ by sending $(1,0) \mapsto 2$ and $(0,1) \mapsto 1 + \sqrt{-5}$. We want to construct a section $f : M \to R \oplus R$, where $g(f(m)) = m$. So $R \oplus R = M \oplus \ker(g)$. Let $f(x) = (-x, x(1 + \sqrt{-5})/2)$, and check that $f(x) \in R \oplus R$. So $M$ is projective.