

10/28

Modules over a ring §4.1

We now begin the last chapter of the semester, on modules. When we studied groups, we saw that looking at their actions on sets was very useful. A module is something that a ring acts on; but it is more than just a set: it's an abelian group.

Def'n Let R be a ring (possibly noncommutative, but with 1). A (left) R -module is an abelian group A together with a map $R \times A \rightarrow A$ (we denote $(r, a) \mapsto ra$) such that

- $r(a+b) = ra + rb \quad \forall r \in R, a, b \in A$
- $(r+s)a = ra + sa \quad \forall r, s \in R, a \in A$
- $r(sa) = (rs)a \quad \forall r, s \in R, a \in A$
- $1a = a \quad \forall a \in A$

Def'n If A and B are R -modules, a homomorphism ^(R -module) is a map $\varphi: A \rightarrow B$ such that $\varphi(x+y) = \varphi(x) + \varphi(y) \quad \forall x, y \in A$ and $\varphi(rx) = r\varphi(x) \quad \forall x \in A, r \in R$.

E.g. If $R = \mathbb{Z}$, then an R -module is the same thing as an abelian group: indeed \mathbb{Z} acts on any abelian group G by $n \cdot g = \underbrace{g + g + \dots + g}_{n \text{ times}}$ for $g \in G$ and $n \in \mathbb{Z}$ (where $(-1) \cdot g = g^{-1}$, etc.). And a \mathbb{Z} -module homo. $A \rightarrow B$ is the same as a group homo.

So modules generalize abelian groups. They also generalize vector spaces:

E.g. If $R = K$ is a field, then an R -module is the same thing as a vector space V over K , and a R -module homo. $V \rightarrow W$ is the same as a linear transformation.

So the study of modules is like a version of linear algebra for rings (but we have to be careful since linear independence does not hold...)

E.g.: If $R = M_n(K)$, matrix algebra over a field K , then one R -module is K^n , where Mv for $M \in M_n(K)$ and $v \in K^n$ is given by usual matrix multiplication, viewing v as a column vector.

E.g.: Consider $R = K[G]$, the group algebra of a group G over a field K . Then an R -module is the same thing as a vector space V over K together with a homomorphism $\varphi: G \rightarrow GL(V)$, where $GL(V)$ is the general linear group of V , the ~~set~~^{group} of all invertible linear transformations $V \rightarrow V$. This is also called a representation of group G over field K , and the study of group representations is a ~~very~~^{huge} subject!

We see that modules over noncommutative rings are very interesting, but we will mostly consider commutative rings from now on.

E.g. If R is a commutative ring and $I \subseteq R$ is an ideal, then I is an R -module (w/ the natural multiplication by elts of R) but also R/I is an R -module. In commutative algebra, quotients by ideals are a major source of modules.

E.g. Let's do a particular example. Let $R = \mathbb{C}[x]$ be the poly. ring. And let $I = \langle x^2 + 2x - 1 \rangle \subseteq R$ and $M = R/I$, as an R -module. Note that $M = \{a + bx : a, b \in \mathbb{C}\} \simeq \mathbb{C}^2$ as an abelian gp., but we have also the action of R on M to understand. Of course $1 \cdot m = m$ for all $m \in M$, but what about $x \in R$? Note that $x \cdot 1 = x$, while

$$x \cdot x = x^2 = -2x + 1 \in M \quad (\text{since } x^2 + 2x - 1 = 0)$$

From this we can deduce the action of any $f \in \mathbb{C}[x]$ on M .

Just like in linear algebra, where even more important than vector spaces are linear transformations (a.k.a. matrices), we care about module homomorphisms.

Def'n Let $\varphi: A \rightarrow B$ be an R -module homomorphism. We define its image $\text{im}(\varphi) = \{\varphi(a) : a \in A\} \subseteq B$ and kernel $\text{ker}(\varphi) = \{a \in A : \varphi(a) = 0\} \subseteq A$ as usual, and we say φ is an epimorphism if it's surjective ($\text{im}(\varphi) = B$) and a monomorphism if it's injective ($\text{ker}(\varphi) = 0$), isomorphism if both.

Def'n Let $A \xrightarrow{\varphi_1} B \xrightarrow{\varphi_2} C$ be a sequence of R -module homomorphisms. We say this sequence is exact if $\text{im}(\varphi_1) = \text{ker}(\varphi_2)$.

Similarly if $A_1 \xrightarrow{\varphi_1} A_2 \xrightarrow{\varphi_2} A_3 \xrightarrow{\varphi_3} A_4 \dots$ is a sequence of R -mod. hom's we say it is exact if $\text{im}(\varphi_i) = \text{ker}(\varphi_{i+1})$ for all i .

Exact sequences are extremely important in the study of modules, but it can be a bit hard to understand their significance at first...

Def'n A short exact sequence is a sequence $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$ that is exact, where 0 is the trivial R -module (trivial group). What does this mean? Well since $\text{ker}(\alpha) = \text{im}(0 \rightarrow A) = 0$, we must have that α is a monomorphism, and since $\text{im}(\beta) = \text{ker}(C \rightarrow 0) = C$, must have that β is an epimorphism. Together with $\text{im}(\alpha) = \text{ker}(\beta)$, this is all we need.

Def'n Let A and B be two R -modules. The direct sum $A \oplus B$ is the direct sum as an abelian group, with $r \cdot (a, b) = (ra, rb)$ for all $r \in R$, $(a, b) \in A \oplus B$.

E.g. Given two R -modules A and B , there is a SES

$$0 \rightarrow A \xrightarrow{i} A \oplus B \xrightarrow{\pi} B \rightarrow 0$$

where $A \xrightarrow{i} A \oplus B$ is the canonical inclusion, and

$A \oplus B \xrightarrow{\pi} B$ is the canonical projection. Are all SES like that?

10/31

Def'n We say that two SES; $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$, $0 \rightarrow A' \rightarrow B' \rightarrow C' \rightarrow 0$ are isomorphic if there are iso's $f: A \rightarrow A'$, $g: B \rightarrow B'$, $h: C \rightarrow C'$ s.t.

$$\begin{array}{ccccccc} 0 & \rightarrow & A & \rightarrow & B & \rightarrow & C \rightarrow 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h \\ 0 & \rightarrow & A' & \rightarrow & B' & \rightarrow & C' \rightarrow 0 \end{array}$$

making the diagram commute (going two ways around square gives the same map).

Rmk: "Homological algebra" studies commutative diagrams ("diagram chasing").

Def'n A SES $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is split if it is isomorphic to one of the form $0 \rightarrow X \xrightarrow{i} X \oplus Y \xrightarrow{\pi} Y \rightarrow 0$

Thm If $R = K$ is a field, then any SES of vector spaces $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is split.

We will discuss the proof of this thm later, but it amounts to the fact that any set of linearly independent vectors extends to a basis.

So is every SES split? No!

E.g. Let $R = \mathbb{Z}$, so that R -modules are just abelian groups.

Let $n \geq 1$. Consider the sequence $0 \rightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \xrightarrow{\cdot} \mathbb{Z}/n\mathbb{Z} \rightarrow 0$.

Here $\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}$ is the "multiplication by n " map

$a \mapsto n \cdot a$. This is injective, so $0 \rightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}$ is exact.

And $\mathbb{Z} \xrightarrow{\cdot} \mathbb{Z}/n\mathbb{Z}$ is the quotient map $a \mapsto a \bmod n$, which is surjective, so $\mathbb{Z} \xrightarrow{\cdot} \mathbb{Z}/n\mathbb{Z} \rightarrow 0$ is exact.

Finally, notice that $\text{im}(\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}) = n\mathbb{Z} = \ker(\mathbb{Z} \xrightarrow{\cdot} \mathbb{Z}/n\mathbb{Z})$,

so we indeed have a short exact sequence of abelian groups.

But it is not split! \mathbb{Z} is not isomorphic to $\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ because it has no torsion elements!

Free Modules and Vector Spaces § 4.2

Def'n For M an R -module, a submodule $N \subseteq M$ is a subset that is a sub-abelian group and is closed under the action of R : i.e., $r \cdot n \in N$ for all $n \in N$, $r \in R$.

Given a subset $X \subseteq M$, the submodule generated by X , $\langle X \rangle$, is the smallest submodule containing X ; concretely

$$\langle X \rangle = \{ r_1 a_1 + r_2 a_2 + \dots + r_n a_n : a_1, \dots, a_n \in X, r_1, \dots, r_n \in R \}$$

We say M is finitely generated if $M = \langle X \rangle$ for a finite $X \subseteq M$, and say M is cyclic if it is generated by a single element, i.e. $M = \langle x \rangle$ for some $x \in M$.

If $\langle X \rangle = M$ for some $X \subseteq M$, then we say the subset X spans M (like in linear algebra).

Def'n A subset $X \subseteq M$ is linearly independent if whenever $r_1 a_1 + r_2 a_2 + \dots + r_n a_n = 0$ for $a_1, \dots, a_n \in X$, $r_1, \dots, r_n \in R$ then we must have $r_i = 0$ for all i . (Just like linear algebra!)

We say X is a basis of M if it spans M and is linearly independent. We say the R -module M is free if it has a basis.

E.g. For any ring R , R is naturally a (left) R -module, and in fact it is a free R -module since $1 \in R$ is a basis.

More generally $R^n = R \oplus R \oplus \dots \oplus R$ is a free R -module with basis $\{(1, 0, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, 0, 0, \dots, 1)\}$.

E.g. Let $R = \mathbb{Z}/6\mathbb{Z}$. Then $\mathbb{Z}/3\mathbb{Z}$ is naturally an R -module

(viewing $\mathbb{Z}/3\mathbb{Z} = (\mathbb{Z}/6\mathbb{Z})/(\mathbb{Z}/2\mathbb{Z})$), but it is not

a free R -module because $\pm 1 \in \mathbb{Z}/3\mathbb{Z}$ would need to

be in a basis, but $3 \cdot (\pm 1) = 0 \in \mathbb{Z}/3\mathbb{Z}$ so it is not linearly independent.

Thm For any ring R (with 1), the following are equivalent for M an R -mod.:

1) M is a free R -module

2) M is isomorphic to $\bigoplus_i R$, direct sum of copies of R indexed by some (possibly infinite) set I .

Moreover, if M is a finitely generated free R -module, then $M \cong R^n$ for some $n \geq 1$. Pfi: Skipped, see book.

Free R -modules behave like vector spaces over a field.

Now we will recall some facts from linear algebra about v.s.'s.

Thm If K is a field, then every K -module is free, since it is a vector space and every vector space has a basis.

Thm Let V be a vector space over a field K .

Then: any linearly independent subset of V can be extended to a maximal linearly independent subset, which spans V , i.e., is a basis.

Moreover, all bases of V have same cardinality.

Remark: All of this remains true for a skew field K like the quaternions \mathbb{H} : see the book.

Def'n The dimension $\dim_K(V)$ of a vector space V over a field K is the cardinality of any K -basis of V .

If $\dim_K(V) < \infty$ we say V is finite dimensional,

and in this case we will have $V \cong K^{\dim_K(V)}$.

Ex. For $K = \mathbb{Z}/p\mathbb{Z}$ (p prime) a finite field with p elements,

and V a finite dimensional vector space over K

with $\dim_K(V) = n$, we have $(\mathbb{Z}/p\mathbb{Z})^n \cong V$, so

in particular $|V| = |(\mathbb{Z}/p\mathbb{Z})|^n = p^n$.

We would like to define an analog of dimension, which we will call the rank, for any ^{free} R -module M for any ring R .

E.g., For $R = \mathbb{Z}$, we know every finitely generated free abelian group (i.e. free \mathbb{Z} -module) is isomorphic to \mathbb{Z}^n , where n is the rank we are talking about.

However, it is a bizarre fact that there are some noncommutative rings R which have $R \cong R \oplus R$ as R -modules, meaning there cannot be a coherent notion of rank for free modules over such R (See Exercise 13 in § 4.2 of book - example is complicated.)

Nevertheless, this cannot happen for commutative R :

Thm Let R be a commutative ring, and let M be a free R -module. Then every basis of M has the same cardinality, which we call the rank of M .

Pf sketch: The idea is to view M as a vector space over some field and then use its dimension over that field as the rank over R . More precisely, choose any maximal ideal I of R . Then we know $K = R/I$ is a field. And also,

$M \otimes_R K$ is a K -module, i.e., a vector space over K , where \otimes_R denotes tensor product of R -modules, a concept we will learn about soon. Any R -basis of M becomes a K -basis of $M \otimes_R K$, so indeed the rank of M is well defined as $\dim_K (M \otimes_R K)$. \square

11/4

Hom and duality § 4.4

Def'n For R a ring, and A and B R -modules, we use $\text{Hom}_R(A, B)$ to denote the set of R -mod. homo's $\varphi: A \rightarrow B$.

Note that $\text{Hom}_R(A, B)$ has the structure of an abelian group, where $(\varphi_1 + \varphi_2)(a) = \varphi_1(a) + \varphi_2(a)$ for all $\varphi_1, \varphi_2 \in \text{Hom}_R(A, B)$.

E.g. Let's compute $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z})$. $1 \in \mathbb{Z}/3\mathbb{Z}$ is a generator, so any $\varphi: \mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$ is determined by $\varphi(1)$. And where can we send 1? We can send it to any $x \in \mathbb{Z}/6\mathbb{Z}$ satisfying $3x = 0$ (since $3 \cdot 1 = 0 \in \mathbb{Z}/3\mathbb{Z}$). So $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}) \cong \{x \in \mathbb{Z}/6\mathbb{Z} : 3x = 0\} = \{0, 2, 4\} \cong \mathbb{Z}/3\mathbb{Z}$.

" We want to view $\text{Hom}_R(A, B)$ as not just an abelian group, but as an R -module itself. However, we will have to restrict to commutative R for this to work...

Def'n Let R and S be two rings. An (R, S) -module A is an abelian group that is simultaneously a left R -module and a right S -module, s.t. those actions of R and S commute in sense that $(r \cdot a) \cdot s = r \cdot (a \cdot s) \quad \forall r \in R, s \in S, a \in A$.

E.g. If R is a commutative ring, then any R -module A is an (R, R) -module if we set $a \cdot r = ra$ for all $r \in R, a \in A$.

Prop. Let R be a ring and A, B R -modules. Suppose that A is an (R, S) -module for some ring S . Then $\text{Hom}_R(A, B)$ is a left S -module by $s \cdot \varphi(a) = \varphi(as) \quad \forall s \in S, \varphi \in \text{Hom}_R(A, B)$. Similarly, if B is an (R, S) -module then $\text{Hom}_R(A, B)$ is a left S -module by $s \cdot \varphi(a) = \varphi(a)s \quad \forall s \in S, \varphi \in \text{Hom}_R(A, B)$.

E.g.: Let $R = M_2(\mathbb{C})$. Then $M = \mathbb{C}^2$ is an R -module as we saw and $\text{Hom}_R(\mathbb{C}^2, \mathbb{C}^2) = \{ \text{linear maps } f: \mathbb{C}^2 \rightarrow \mathbb{C}^2: f \text{ commutes w/ all matrices in } M_2(\mathbb{C}) \}$
 $= \text{center of } M_2(\mathbb{C}) = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}: \lambda \in \mathbb{C} \right\}$. There is no natural action of $M_2(\mathbb{C})$ on this set of diagonal matrices, but since \mathbb{C}^2 has a right action of \mathbb{C} commuting w/ left action of $M_2(\mathbb{C})$, $\text{Hom}_R(\mathbb{C}^2, \mathbb{C}^2)$ is at least a \mathbb{C} -vector space.

Cor If R is a commutative ring, then $\text{Hom}_R(A, B)$ is naturally an R -module for any R -modules A and B . We have $r \cdot \varphi(a) = r\varphi(a) = \varphi(ra) \forall r \in R, \varphi \in \text{Hom}_R(A, B)$.

E.g.: If $R = \mathbb{Z}$, then for any abelian groups A, B , $\text{Hom}_{\mathbb{Z}}(A, B)$ is an abelian group, a.k.a. \mathbb{Z} -module.

E.g.: If $R = K$ is a field and V and W are two K -vector spaces then $\text{Hom}_K(V, W) = \{ K\text{-linear maps } f: V \rightarrow W \}$ is a K -vector space. If $V \cong K^n$ and $W \cong K^m$ then $\text{Hom}_K(V, W) \cong \{ n \times m \text{ matrices with } \text{entries} \text{ in } K \}$, so $\dim_K(\text{Hom}_K(V, W)) = n \cdot m = \dim_K(V) \cdot \dim_K(W)$.

E.g.: If R is any commutative ring, then $\text{Hom}_R(R^n, R^m)$ can be viewed as set of $n \times m$ matrices w/ ~~coeffs~~ ^{entries} in R . We'll discuss this more (especially when R is a PID) later.

Prop. Let R be a commutative ring. Then for any R -mod. A , we have canonical isomorphism $\text{Hom}_R(R, A) \cong A$.

PS: The isomorphism is given by $\varphi \mapsto \varphi(1)$ for $\varphi \in \text{Hom}_R(R, A)$. This works since 1 generates R as an R -module.

So $\text{Hom}_R(R, A) = A$. What about other direction, i.e., $\text{Hom}_R(A, R)$?

Def'n For R a com. ring and A an R -mod., its dual module is $A^* = \text{Hom}_R(A, R)$.

E.g. If $R = K$ is a field, and V is a K -vector space, then $V^* = \{\text{linear functions } f: V \rightarrow K\}$ is the dual space, also often called the space of linear functionals on V . You might know that if V is finite dimensional then $\dim_K(V) = \dim_K(V^*)$. However, there is no canonical isomorphism $V \rightarrow V^*$. But...

Thm For any R -mod. A , there is a canonical map $A \rightarrow A^{**}$ to the double dual given by $a \mapsto (f \mapsto f(a))$ for $a \in A$, $f \in A^*$.

Def'n A module A is reflexive if the canonical homo. $A \rightarrow A^{**}$ is an isomorphism.

E.g. For any field K and finite dimensional vector space V over K , V is reflexive, i.e. canonically isomorphic to V^{**} .

E.g. On next HW you will show $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0$, hence the dual of $\mathbb{Z}/n\mathbb{Z}$, and also the double dual, as a \mathbb{Z} -mod., $= 0$. Notice how these non-reflexive come from torsion in the module (where we recall torsion element means an elem with $rm = 0$ for some non zero divisor $r \in R$).

One last thing about duality is how it interacts with module homo's:

Thm Let $A \xrightarrow{f} B$ be two R -mod. with a homomorphism between them. Then we have a hom. $B^* \xrightarrow{f^*} A^*$ given by $(f^* \varphi)(a) = \varphi(f(a))$ for all $\varphi \in B^* = \text{Hom}_R(B, R)$.

Rmk: This means duality is a "contravariant functor"; i.e., it reverses direction of arrows in category of R -modules. //