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 $R \times A \to A$ (we denote $(r,a) \mapsto ra$) such that

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

Def'n If A and B are R-modules, a homomorphism (of R-modules) is a map $\varphi : A \to B$ 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 $n \cdot g = \underbrace{g + g + \cdots + g}_{n \text{ times}}$ for $g \in G$ and $n \in \mathbb{Z}$ (when $(-1)\cdot g = g^{-1}$, etc.). And a $\mathbb{Z}$-module homo. $A \to B$ 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. $V \to W$ 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 $\varphi: G \to GL(V)$, where $GL(V)$ is the general linear group of V, the group of all invertible linear transformations $V \to V$. This is also called a representation of group G over field K, and the study of group representations is a 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 $\varphi: A \to B$ be an R-module homomorphism. We define its image $\text{im}(\varphi) = \{\varphi(a) : a \in A\} \subseteq B$ and kernel $\ker(\varphi) = \{a \in A : \varphi(a) = 0\} \subseteq A$ as usual, and we say φ is an epimorphism if it's surjective ($\text{im}(\varphi) = B$) and a monomorphism if it's injective ($\ker(\varphi) = 0$), 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 $\text{im}(\varphi_1) = \ker(\varphi_2)$. Similarly if $A_1 \xrightarrow{\varphi_1} A_2 \xrightarrow{\varphi_2} A_3 \xrightarrow{\varphi_3} A_4 \cdots$ is a sequence of R-mod. hom's we say it is exact if $\text{im}(\varphi_i) = \ker(\varphi_{i+1})$ 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 $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ that is exact, where 0 is the trivial R-module (trivial group). What does this mean? Well since $\ker(\alpha) = \text{im}(0 \to A) = 0$, we must have that α is a monomorphism, and since $\text{im}(\beta) = \ker(C \to 0) = C$, must have that β is an epimorphism. Together with $\text{im}(\alpha) = \ker(\beta)$, 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

$$0 \to A \xrightarrow{\iota} A \oplus B \xrightarrow{\pi} B \to 0$$

where $A \xrightarrow{\iota} A \oplus B$ is the canonical inclusion, and $A \oplus B \xrightarrow{\pi} B$ is the canonical projection. Are all SES like this? ...

10/31

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

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

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

Thm If $R = K$ is a field, then any SES of vector spaces $0 \to A \to B \to C \to 0$ 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 $0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$.

Here $\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}$ is the "multiplication by n" map $a \mapsto n \cdot a$. This is injective, so $0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}$ is exact.

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

Finally, notice that $\operatorname{im}(\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}) = n\mathbb{Z} = \ker(\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z})$, 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., $rn \in N$ 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

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

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 $r_1 a_1 + r_2 a_2 + \cdots + r_n a_n = 0$ for $a_1, \ldots, a_n \in X$, $r_1, \ldots, r_n \in R$ 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 $R^n = R \oplus R \oplus \cdots \oplus R$ is a free R-module with basis $\{(1,0,0,\ldots,0), (0,1,0,\ldots 0), \ldots, (0,0,0,\ldots,0,1)\}$.

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 $\bigoplus_{i \in I} R$, 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 $n \geq 1$. Pf: 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.

Rmk: 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 $V \cong K^{\dim_K(V)}$.

Eg: 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 f.g. 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 $\dim_K (M \otimes_R K)$. ∎

11/4

Hom and duality § 4.4

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

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

Eg: Let's compute $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z})$. $1 \in \mathbb{Z}/3\mathbb{Z}$ is a generator, so any $\varphi: \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ 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 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}) \simeq \{x \in \mathbb{Z}/6\mathbb{Z} : 3x = 0\}$
$= \{0, 2, 4\} \simeq \mathbb{Z}/3\mathbb{Z}$.

We want to view $\mathrm{Hom}_R(A,B)$ 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 $(ra)s = r(as)$ $\forall r \in R, s \in S, a \in A$.

Eg: 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 $\mathrm{Hom}_R(A,B)$ is a left S-module by $s\cdot\varphi(a) = \varphi(as)$ $\forall s \in S, \varphi \in \mathrm{Hom}_R(A,B)$.
Similarly, if B is an (R,S)-module then $\mathrm{Hom}_R(A,B)$ is a left S-module by $s\cdot\varphi(a) = \varphi(a)s$ $\forall s \in S, \varphi \in \mathrm{HOM}_R(A,B)$.

E.g.: Let $R = M_2(\mathbb{C})$. Then $M = \mathbb{C}^2$ is an R-module as we saw and $\mathrm{Hom}_R(\mathbb{C}^2, \mathbb{C}^2) = \{\text{linear maps } f: \mathbb{C}^2 \to \mathbb{C}^2 : f \text{ commutes w/ all matrices in } M_2(\mathbb{C})\}$ $= \text{center of } M_2(\mathbb{C}) = \left\{\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix} : \lambda \in \mathbb{C}\right\}$. 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 $M_2(\mathbb{C})$, $\mathrm{Hom}_R(\mathbb{C}^2, \mathbb{C}^2)$ is at least a $\mathbb{C}$-vector space.

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

E.g.: If $R = \mathbb{Z}$, then for any abelian groups A, B, $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ 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 $\mathrm{Hom}_K(V, W) = \{K\text{-linear maps } f: V \to W\}$ is a K-vector space. If $V \simeq K^n$ and $W \simeq K^m$ then $\mathrm{Hom}_K(V, W) \simeq \{n \times m \text{ matrices with entries in } K\}$, so $\dim_K(\mathrm{Hom}_K(V, W)) = n \cdot m = \dim_K(V) \cdot \dim_K(W)$.

E.g.: If R is any commutative ring, then $\mathrm{Hom}_R(R^n, R^m)$ can be viewed as set of $n \times m$ matrices w/ 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, have canonical isomorphism $\mathrm{Hom}_R(R, A) \simeq A$.

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

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

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

E.g. If $R = K$ is a field, and V is a K-vector space, then $V^* = \{\text{linear functions } f: V \to K\}$ 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 $V \to V^*$. But...

Thm For any R-mod. A, there is a canonical map $A \to A^{**}$ 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. $A \to A^{**}$ 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 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0$, 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 $m \in M$ 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 $\varphi \in B^* = \mathrm{Hom}_R(B, R)$.

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

11/6

Tensor Product of modules §4.5

We now discuss an operation on R-modules called tensor product that produces a new R-mod. $A \otimes B$ from two R-mod.'s A and B. It is related to "multilinear algebra" and also intimately related to the Hom construction we discussed last class.

For convenience today we assume R is a commutative ring, although this mostly all works the same for noncom. R.

Def'n Let A and B be two R-mod.'s. Let F be the free abelian group on set $A \times B$. So the elements of F are (finite) formal sums of form $\sum n_i (a_i, b_i)$ with $a_i \in A$, $b_i \in B$, $n_i \in \mathbb{Z}$. Let S be the subgroup of F generated by elements:

$$(a+a', b) - (a, b) - (a', b) \quad \forall a, a' \in A, b \in B$$
$$(a, b+b') - (a, b) - (a, b') \quad \forall a \in A, b, b' \in B$$
$$(ra, b) - (a, rb) \quad \forall a \in A, b \in B, r \in R.$$

The quotient F/S is called the tensor product of A and B, and is denoted $A \otimes_R B$. The image of (a,b) in $A \otimes_R B$ is denoted $a \otimes b$ and is called a pure tensor.

Note: Not every element of $A \otimes_R B$ is a pure tensor. In general an element of $A \otimes_R B$ is a (formal) sum of pure tensors: $\sum n_i \, a_i \otimes b_i$ $\quad n_i \in \mathbb{Z}$, $a_i \in A$, $b_i \in B$.

Remark: The pure tensors in $A \otimes_R B$ satisfy these relations:

$$(a+a') \otimes b = a \otimes b + a' \otimes b$$
$$a \otimes (b+b') = a \otimes b + a \otimes b'$$
$$ra \otimes b = a \otimes rb \quad \forall r \in R$$

This is the sense in which the tensor product is "multilinear," i.e., linear in both components.

Prop: $A \otimes_R B$ has the structure of an R-mod. where
$r\left(\sum_i n_i\, a_i \otimes b_i\right) = \sum_i n_i\, ra_i \otimes b_i = \sum_i n_i\, a_i \otimes rb_i$

Prop. The $\otimes$ operation is associative and commutative in sense that $(A \otimes_R B) \otimes_R C \cong A \otimes_R (B \otimes_R C)$
and $A \otimes_R B \cong B \otimes_R A$.

Prop: We have $A \otimes_R R \cong A \cong R \otimes_R A$ for any R-mod A.

Pf: All of these propositions are relatively straightforward. Let's prove the last one about $A \otimes_R R \cong A$. First note that $a \otimes r = ra \otimes 1$ for any pure tensor, hence every pure tensor is of form $a \otimes 1$ for $a \in A$. Then any element of $A \otimes_R R$ is of form $\sum_i n_i\, a_i \otimes 1$ but this is $= \left(\sum_i n_i\, a_i\right) \otimes 1 = a' \otimes 1$ for some $a' \in A$. So $A \otimes_R R = \{a \otimes 1 : a \in A\} \cong A$, as claimed. ∎

Eg: Let's do an example of tensor products for $R = \mathbb{Z}/2\mathbb{Z}$. Let $A = R^2 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} = B$. What does $(\mathbb{Z}/2\mathbb{Z})^2 \otimes_{\mathbb{Z}/2\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})^2$ look like? Let's consider some elements:

$(0,0) \otimes (1,1) = 0 \cdot (0,0) \otimes (1,1) = (0,0) \otimes 0 \cdot (1,1) = (0,0) \otimes (0,0)$

So in fact $(0,0) \otimes a = 0$ for any $a \in A$. Also we have

$(1,1) \otimes (1,0) = ((1,0) + (0,1)) \otimes (1,0) = (1,0) \otimes (1,0) + (0,1) \otimes (1,0)$.

In fact we can see that a basis over $\mathbb{Z}/2\mathbb{Z}$ of $A \otimes_R A$ is $\{(1,0) \otimes (1,0),\ (1,0) \otimes (0,1),\ (0,1) \otimes (1,0),\ (0,1) \otimes (0,1)\}$.

Note that $\dim_R(A \otimes_R A) = 4 = 2 \cdot 2 = \dim_R(A) \cdot \dim_R(A)$.
Also note that $(1,0) \otimes (1,0) + (0,1) \otimes (0,1)$ is an element in $A \otimes_R A$ which is not a pure tensor. =

Thm Let $R=K$ be a field and V and W two K-vector spaces. Suppose $\{e_i : i\in I\}$ and $\{f_j : j\in J\}$ are bases of V and W, then $\{e_i \otimes f_j : i\in I, j\in J\}$ is a basis of $V\otimes_K W$. In particular if V and W are finite dimensional with $n=\dim_K(V)$ and $m=\dim_K(W)$ then $\dim_K(V\otimes_K W)=n\cdot m=\dim_K(V)\cdot\dim_K(W)$.

Pf: Exercise for you, similar to the example we saw. ☐

However when R is *not* a field, $\otimes_R$ behaves differently, especially if there are torsion elements in the modules.

E.g. Let's consider $R=\mathbb{Z}$, so R-mod.'s are just abelian gp.s. In particular let's consider $\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Z}/2\mathbb{Z}$, where $\mathbb{Q}$ is the (additive) group of the rational numbers. Notice that for any pure tensor $x\otimes b$ for $x\in\mathbb{Q}$, $b\in\mathbb{Z}/2\mathbb{Z}$ we have $x\otimes b = 2(\frac{x}{2})\otimes b = (\frac{x}{2})\otimes 2b = \frac{x}{2}\otimes 0 = 0$ since $2b\in\mathbb{Z}/2\mathbb{Z}=0$ and since $\frac{x}{2}$ exists for any $x\in\mathbb{Q}$. Since any pure tensor $=0$, $\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Z}/2\mathbb{Z}=0$. Exercise: what is different with $\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/2\mathbb{Z}$?

(On HW #6 you will take this example further...)

Thm Let A, B, C be R-mod's and $A \xrightarrow{f} B$ a homo. R-mod. Then $\exists$ a homo. R-mod. $A\otimes_R C \xrightarrow{f\otimes 1_C} B\otimes_R C$ where $f\otimes 1_C(\sum_i n_i\, a_i\otimes c_i) = \sum_i n_i\, f(a_i)\otimes c_i$.

Rmk: Since $-\otimes_R C$ preserves the direction of the arrows we say it is a "covariant functor" on category of R-mod's

Finally, let's discuss the relationship between tensor and hom.

Theorem (Tensor-Hom Adjunction) For A, B, C R-mod's, have $\mathrm{Hom}_R(A \otimes_R B, C) \simeq \mathrm{Hom}_R(A, \mathrm{Hom}_R(B, C))$.

This says $\otimes_R$ and $\mathrm{Hom}_R(-,-)$ are "opposite" or "dual" in a certain sense... Let's focus on one special case.

Cor $(A \otimes_R B)^* \simeq \mathrm{Hom}_R(A, B^*)$

Pf: Take $C = R$ in the tensor-hom adjunction. ☒

Cor Suppose B is reflexive, i.e., $B^{**} = B$.
Then $\mathrm{Hom}_R(A, B) \simeq (A \otimes_R B^*)^*$.

Rmk: Recall that every finite-dimensional v.s. V over a field K is reflexive. Hence $\mathrm{Hom}_K(V, W) \simeq (V \otimes_K W^*)^* \simeq V^* \otimes_K W$ for any two fin.-dim'l v.s.'s. This shows that we can build up all hom spaces between fin.-dim'l vector spaces just using $\otimes$ and duality.

Pf sketch for tensor-hom adjunction:
See the book for details, but key point is that

$$\mathrm{Hom}_R(A \otimes_R B, C) \simeq \mathrm{Bil}_R(A \times B, C)$$

where $\mathrm{Bil}_R(A \times B, C)$ is the set of "bilinear maps" $A \times B \to C$. Then $\mathrm{Bil}_R(A \times B, C) \simeq \mathrm{Hom}_R(A, \mathrm{Hom}_R(B, C))$ via the map $f \mapsto (a \mapsto (b \mapsto f(a, b)))$.

☒

11/13

Modules over a PID §4.6 ("cultural lesson")

A while back we explained the classification of finitely generated abelian groups. A very similar classification holds for f.g. R-modules, whenever R is a PID.

Lemma Let R be a PID and M a free R-module. Then any submodule $M' \subseteq M$ is also free, with rank$(M') \leq$ rank(M).

Pf sketch: Let's restrict to the case when rank(M) is finite, so $M \cong R^n$. Let $\pi_i : M \to R$ for $i = 1, \dots, n$ denote the projection onto the i^{th} component of $M = R^n$. For each $i = 1, \dots, n$, $\pi_i(M')$ is a submodule of R, hence an ideal, hence of the form (a_i) for some $a_i \in R$ (since R is a PID). Choose $u_i \in M$ such that $\pi_i(u_i) = a_i$. Then, throwing out the u_i with $u_i = 0$, $\{u_1, \dots, u_n\}$ is a basis of M' (exercise) so indeed M' is free with rank$(M') \leq n$. ∎

Cor Let M be a finitely generated R-module, where R is a PID. Then there is an exact sequence of the form:

$$0 \to R^m \to R^n \to M \to 0 \quad \text{for some } m \leq n.$$

Pf: Let $x_1, \dots, x_n$ be generators of M as an R-mod. Then there is an epimorphism $R^n \xrightarrow{f} M$ given by $f(e_i) = x_i$ where $e_i \in R^n$ is $e_i = (0, 0, \dots, \overset{i}{1}, \dots, 0)$ i^{th} standard basis vector. Let $N = \ker(R^n \xrightarrow{f} M)$. Then N is a submodule of R^n, hence by previous lemma is isomorphic to R^m for some $m \leq n$, giving sequence $0 \to R^m \to R^n \to M \to 0$ as claimed. ∎

Remark: Just as we saw w/ f.g. abelian groups, the $R^n \to M$ gives the generators of the module M and the $R^m \to R^n$ gives the relations among the generators.

From this corollary we deduce a classification of finitely generated modules over a PID.

Theorem (Classification of f.g. modules over a PID)
Let R be a PID and M a f.g. module over R.
Then i) $\exists!\ f \geq 0$ and nonzero nonunits $d_1 | \cdots | d_m \in R$ such that
$$M \simeq R^f \oplus R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_m)$$
ii) $\exists!\ f \geq 0$ and prime powers $p_1^{k_1}, p_2^{k_2}, \ldots, p_\ell^{k_\ell} \in R$ such that
$$M \simeq R^f \oplus R/(p_1^{k_1}) \oplus \cdots \oplus R/(p_\ell^{k_\ell}).$$

Notice how the statement is almost exactly the same as the classification of f.g. abelian groups, and indeed we can follow exactly the same proof we sketched then. Namely, we fix a resolution $0 \to R^m \to R^n \to M \to 0$ of M, and view the map $R^m \to R^n$ as a matrix ($m \times n$ matrix with coefficients in R), whose cokernel gives us the module M. Then, as before, putting the matrix representing $R^m \to R^n$ in Smith Normal Form gives us the invariant factors $d_1 | \cdots | d_m$ of module M.
(The very technical point being that SNF of a matrix over a PID exists...) The conversion between invariant factors $d_1 | \cdots | d_m$ and elementary divisors $p_1^{k_1}, \ldots, p_\ell^{k_\ell}$ exactly parallels case of $\mathbb{Z}$-modules, i.e., abelian groups.

One of the most important examples of a PID is $R = K[x]$, polynomial ring in one variable over a field K. We might wonder what can be said about modules over polynomial rings $K[x_1, \ldots, x_n]$ in multiple variables. This is the starting point of commutative algebra.

Theorem (Hilbert's syzygy theorem) Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring in n variables over a field K, and M a f.g. R-module. Then there is an exact sequence

$$0 \to L_m \to L_{m-1} \to \cdots \to L_1 \to L_0 \to M \to 0$$

with $m \leq n$, where all the L_i are free R-modules. This is called a free resolution of the module M.

Rmk: Notice the case $n = 1$ says we have a free resolution $0 \to L_1 \to L_0 \to M \to 0$ of a module M over $R = K[x]$, which we saw since R is a PID.

Just as the map $L_1 \to L_0$ determines the relations among the generators of the module M, the map $L_2 \to L_1$ determines the relations among the relations, which are called the (higher) syzygies of the module M. The content of Hilbert's theorem is that eventually these syzygies are zero.

The importance of free resolutions is that we can use linear algebra to study nonlinear things like polynomial rings and their modules. We may come back to this next semester...

11/18 Algebras over a field §4.7 ("cultural lesson")

An algebra is an algebraic structure that is simultaneously a ring and a module (over another ring).

Def'n: Let R be a commutative ring. An algebra over R is a ring A (not necessarily commutative, but w/ a 1) such that:

i) $(A,+)$ is a (left) R-module.

ii') $r(ab) = (ra)b = a(rb)$ for all $r \in R$, and $a,b \in A$.

The most important case is when $R = K$ is a field, and then the algebra A over K is a vector space, hence has a well-defined dimension, etc.

E.g.: Every ring R is a $\mathbb{Z}$-module since $(R,+)$ is an abelian group, and it's easy to see that any R is in fact a $\mathbb{Z}$-algebra.

E.g.: For any commutative ring R, the polynomial ring $R[x]$ and formal power series ring $R[[x]]$ are R-algebras.

In fact, there is another way to describe algebras:

Prop: A ring A has the structure of an R-algebra if and only if there is a ring homomorphism $\varphi : R \to Z(A)$, where $Z(A) = \{a \in A : ab = ba \ \forall b \in A\}$ is the center of A.

Pf: Given such a homomorphism $\varphi : R \to Z(A)$, we define the R-mod. structure on A by $r \cdot a = \varphi(r)a$. Conversely, if A has a compatible R-mod. structure, then we can define such a φ by $\varphi(r) = r \cdot 1_A$. ∎

Rmk: We often want this φ to be a monomorphism, i.e., we have a copy of R inside the center of A.

Many of the examples of noncommutative rings we've seen are algebras over fields:

E.g. Let K be a field and G a group. Recall the group algebra $K[G]$ consists of formal (finite) linear combinations $\sum_{i=1}^{n} k_i g_i$, $k_i \in K$, $g_i \in G$ with multiplication $g \cdot h = gh \in G$ extended linearly. This is a K-algebra: $\{k \cdot e : k \in K\}$ is a copy of K inside of $K[G]$

E.g. Let $n \geq 1$, K be a field, and recall that $M_n(K)$ denotes the ring of $n \times n$ matrices with entries in K. This is a K-algebra with $\{k \cdot \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} : k \in K\}$ being a copy of K inside of $M_n(K)$.

Rmk: The dimension of $K[G]$ is $|G|$, and the dimension of $M_n(K)$ is n^2.

Recall that a (possibly noncommutative) ring R is called a division ring (or skew field) if every nonzero element is a unit. A division algebra is a division ring over a field.

E.g. The complex numbers $\mathbb{C}$ are a division algebra over $\mathbb{R}$, as are the quaternions $\mathbb{H}$. In fact...

Thm (Frobenius) The only finite dimensional division algebras over $\mathbb{R}$ are:
- $\mathbb{R}$ itself (dimension 1)
- $\mathbb{C}$ (dimension 2)
- $\mathbb{H}$ (dimension 4).

Rmk: If we consider non-associative algebras, there is another one, the octonions $\mathbb{O}$ which have dimension 8 over $\mathbb{R}$. Their (non associative) multiplication can be encoded by this picture ("Fano plane"):

← 7 points correspond to 7 basis elements other than 1

One of the most important things we can do with algebras is extend scalars of a module. What this means is that if R is a commutative ring and A is a (commutative) algebra over R, then any R-module M can be "extended" to $A \otimes_R M$, which is naturally an A-module.

E.g. When we explained why the rank of a free module M over a commutative ring R is well-defined, we let K be the field of fractions of R, which is naturally an R-algebra, and then extended scalars to view $K \otimes_R M$ as a K-vector space, which has a well-defined dimension.

What if K is a field and L is a K-algebra which is also a field? Note that any homomorphism $\varphi: K \to L$ between fields is injective (because the kernel must be an ideal, which can only be $\{0\}$ or K, but since $\varphi(1) = 1$ the kernel must be $\{0\}$). Hence if L is a field that is an algebra over another field K, we can view this as an inclusion $K \subseteq L$, which we call an extension of the base field K.

Next semester we will study extensions of fields in depth. For example, we have $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, but are there other things in between? Well, yes, for example $\mathbb{Q}(\sqrt{2})$ = smallest subfield of $\mathbb{R}$ containing $\sqrt{2}$.

In fact, this is a finite dimensional extension of $\mathbb{Q}$ (we have $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$) and we can understand these kinds of extensions using "Galois theory"!