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 (R-module) homomorphism is a map $\varphi: A \to B$ such that $\varphi(x+y) = \varphi(x) + \varphi(y) \ \forall x,y \in A$ and $\varphi(rx) = r\varphi(x) \ \forall x \in A,\ r \in R.$

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 ~~set~~ 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 $M = \{a \cdot 1 + bx : a, b \in \mathbb{C}\} \simeq \mathbb{C}^2$ 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.

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

<u>Def'n</u> Let $A \xrightarrow{\varphi_1} B \xrightarrow{\varphi_2} C$ be a sequence of R-module homomorphisms. We say this sequence is <u>exact</u> if $im(\varphi_1) = ker(\varphi_2)$. 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 $im(\varphi_i) = ker(\varphi_{i+1})$ 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...

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

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

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

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

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

Def'n We say that two SES; $0 \to A \to B \to C \to 0$, $0 \to A' \to B' \to C' \to 0$ are <u>isomorphic</u> 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 <u>commute</u> (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 <u>split</u> 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 <u>field</u>, 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? <u>No</u>!

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

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

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

Finally, notice that $\mathrm{im}(\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}) = n\mathbb{Z} = \ker(\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z})$, 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 <u>no</u> <u>torsion elements</u>!