LECTURE 26 : MODULES

A module is roughly a vector space where we've replaced a field with a ring. Vector spaces are particular examples of modules. We follow §10.1 of Dummit & Foote 3rd Ed.

Def^{n}/ Let R be a ring (not necessarily commutative or unital). A **LEFT R-MODULE** OR **LEFT MODULE OVER R** is a set M together with

(1.) a binary operation $+$ on M under which M is an abelian group, and

(2.) an action of R on M (that is a map $R \times M \longrightarrow M$) denoted by rm, for all $r \in R$ and $m \in M$ which satisfies,

(a.) $(r+s)m = rm + sm \quad \forall r,s \in R,\ m \in M,$

(b.) $(rs)m = r(sm) \quad \forall r,s \in R,\ m \in M,$

(c.) $r(m+n) = rm + rn \quad \forall r \in R,\ m,n \in M.$

If the ring R has unity 1 we impose an additional axiom

(d.) $1m = m \quad \forall m \in M.$

A right R-module would be similarly defined by $M \times R \longmapsto mr$ etc. When R is commutative we can define a right action via $mr = rm$. for all $r \in R$ and $m \in M$. Module means left module by default in what follows.

Th^{m}/ modules over a field F and vector spaces over the field F are the same object.

Def'n Let R be a ring and M an R-module. An R-submodule of M is a subgroup N of M which is closed under the action of ring elements, meaning $rn \in N$ for all $r \in R$ and $n \in N$.

Submodules of a vector space are subspaces.

E1 $0, M$ are submodules of an R-module M

E2 Given a ring R we have $M = R$ forms an R-module where the module action is simply ring multiplication. Submodules are then left-ideals of R

E3 $R = F$ a field, then affine n-space over F is $F^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in F\}$ forms F-module indeed a vector space over F where $+$ and scalar mult.

$$(a+b)_j = a_j + b_j \quad \text{and} \quad (c\,a)_j = c a_j$$

are defined as above.

Remark: module action $(r, m) \longmapsto rm$ is the generalization of scalar multiplication $(c, V) \longmapsto c \cdot V$.

E4 R a unital ring with $1 \in R$ then for $n = 1, 2, \ldots$

$$R^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in R\}$$

and $(a+b)_j = a_j + b_j$ and $(ra)_j = r a_j$ $\forall a, b \in R^n$ and $r \in R$ make $M = R^n$ an R-module.

this defines the free module of rank n over R.

Question: what can we say about the free module R^n?
When $R = F$ (field) then we know many things from our past study of linear algebra. How do those results bend when R is not a field?

Proposition: Suppose M is an abelian group under $+$ and suppose M is an R-module for a unital ring R. Then if S is a subring of R with $1_S = 1_R$ then M is naturally an S-module via restriction of the R-module action from $R \times M \to M$ to $S \times M \to M$.

Proof: the claim of the Proposition is immediately verified since all axioms holding for R necessarily hold for $S \subset R$ where S is itself a ring with 1. //

We might recognize the application of the above Prop. to vector space theory, if V is complex vector space then V is likewise a vector space over $\mathbb{R}$ or $\mathbb{Q}$ by simply restricting the scalar multiplication.

Remark: how would we extend scalar multiplication? Or, how would we take an S-module M an elevate it to an R-module M where R extends S? (meaning S subring of R)

Def^{n}/ Given M an R-module and I a two-sided ideal of R, if $am = 0$ for all $a \in I$ and $m \in M$ then we say M is <u>annihilated</u> by I. We define an (R/I)-module structure on M by

$$(r + I)m = rm$$

for each $m \in M$ and coset $r + I \in R/I$.

We can prove M forms an (R/I)-module in the above case. Notice if $r_1 + I = r_2 + I$ then $r_2 - r_1 \in I$ and hence $(r_1 - r_2)m = 0 \quad \forall m \in M$. Thus $(r_1 + I)m = r_1 m = r_2 m = (r_2 + I)m$ and we find the (R/I)-module action is well-defined. I'll leave the axioms for the reader to check,

$$\left.\begin{aligned} (r + I) + (s + I) &= (r + s) + I \\ (rI)(sI) &= (rs)I \end{aligned}\right\} \text{ ring operations on } R/I.$$

Th^{m}/ Given a maximal ideal I in commutative ring R and an R-module M which is annihilated by I then M forms a vector space over R/I

<u>Proof</u>: given the ideal I has $IM = 0$ we find the R-module M induces an (R/I)-module structure on M via $(r + I)m = rm$. Then I maximal implies R/I is field hence (R/I)-module M is a <u>vector space</u> over R/I. //

$\mathbb{Z}$-MODULES ARE ABELIAN GROUPS

Consider $R = \mathbb{Z}$ and let A be any Abelian group where we denote the group operation by $+$. Then A can be regarded as a $\mathbb{Z}$-module as follows

$$\text{Def'n} \quad na = \begin{cases} a + a + \cdots + a \quad (n\text{-times}) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -a - a - \cdots - a \quad (-n\text{-times}) & \text{if } n < 0 \end{cases}$$

In fact, if we think about the module axioms, this is the only way to make A into a $\mathbb{Z}$-module, taking $\mathbb{Z}$ to be a unital ring for this thought. On the flip-side, every $\mathbb{Z}$-module M is an abelian group w.r.t. the module $+$ hence,

$$\mathbb{Z}\text{-modules} \iff \text{Abelian Groups}$$

Likewise, by the reasoning above,

$$\mathbb{Z}\text{-submodules of a given } \mathbb{Z}\text{-module } M \iff \text{SUBGROUPS OF } M \text{ AS AN ABELIAN GROUP}$$

Remark: given A an abelian group with $x \in A$ with finite order n we have $nx = 0$ for $n \neq 0$. Furthermore, if $|A| = m$ then $|x|$ divides m $\forall x \in A$ hence $mx = 0$ $\forall x \in A$. Thus A is annihilated by the ideal $m\mathbb{Z}$ of $\mathbb{Z}$ and so A is an $(\mathbb{Z}/m\mathbb{Z})$-module.

$F[x]$-MODULE FOR STUDY OF $T: V \to V$ LINEAR OVER F

We study the vector space V as an $F[x]$-module w.r.t. a given endomorphism $T: V \to V$

$$P(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$$

$$v \in V$$

$$P(x)v = (a_n T^n + \cdots + a_1 T + a_0)v$$

$$= a_n T^n(v) + \cdots + a_1 T(v) + a_0 v$$

where $T^2(v) = T(T(v))$ and $T^{m+1}(v) = T(T^m(v))$ defines powers of T recursively.

Remark: V is an F-module via V.C

V as an $F[x]$-module is an extension of scalars to polynomials and $F \subset F[x]$ so this is an example of the sort of extension I asked about on (3).

In summary,

$$\left\{ \begin{array}{c} V \text{ an } F[x] \\ \text{module} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} V \text{ a vector space over } F \\ \text{and} \\ T: V \to V \text{ linear} \\ \text{transformation} \end{array} \right\}$$

We can also reason that

$$\left\{ W \text{ an } F[x]\text{-submodule} \right\} \leftrightarrow \left\{ \begin{array}{c} W \text{ subspace of } V \\ \text{and } W \text{ is} \\ T\text{-stable} \end{array} \right\}$$

I call this "T-invariant" $T(W) \subseteq W$ in Math 321.