Chapter 10: Modules.

Informal Definition of a module:

a module is a vector space, but over a ring instead of a field.

This means we can add and multiply by scalars, but scalars come from a ring R.

Some (but not all) of what you know about vector spaces will carry over to modules.

Examples: A vector space over F is a module over F.

An abelian group is a module over the ring $\mathbb{Z}$.

We can define scalar multiplication on A:

if $n > 0$ $\quad na = \underbrace{(a + a + \cdots + a)}_{n \text{ times}}$

$n = 0$ $\quad na = 0 \in A$.

$n < 0$ $\quad na = \underbrace{(-a) + (-a) + \cdots + (-a)}_{|n| \text{ times}}$

Examples (cont'd): Let V be a vector space over F and let $T: V \to V$ be a linear transformation. Let $R = F[x]$.

Then V is a $F[x]$-module as follows:

if $a_0 + a_1 x + \cdots + a_n x^n \in R$ and $v \in V$.

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

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

Remark: if a V.S. over F V is an $F[x]$ module then the action of x on V $(x \cdot v \in V)$ is a linear transformation by the definition of module (see parts (b), (c) of def'n on page 337) and the correspondence on p. 341.

Q: Why is a module? What is the benefit of studying such things?

A: We can unify two theorems:

Fundamental Theorem of. f.g. Abelian Grps.

Jordan Canonical Form.

Both of these are special case of the structure theorem for finitely generated modules over a P.I.D.

Recall that $\mathbb{Z}$ and $F[x]$ are PIDs.

A f.g. ab.gp. is a $\mathbb{Z}$-module

A vector space over $\mathbb{C}$ and a linear trans. $T: V \to V$ give us a $\mathbb{C}[x]$-module, as before.

Modules also encompass some earlier concepts.

If R is a (possibly non-commutative) ring.

and $I \subset R$ is a left ideal in R,

then I is an (left) R-module.

also R/I is a left-R-module.

Some things about vector spaces do NOT carry over.

Example: Every FDVS / F has a basis.

It is not true that every f.g. module over R has a basis. $\mathbb{Z}/2\mathbb{Z}$ is a $\mathbb{Z}$-module.

But there is the linear relation:

$$\begin{array}{ccccc} 2 & \cdot & 1 & = & 0 \\ \cap & & \cap & & \cap \\ \mathbb{Z} & & \mathbb{Z}/2\mathbb{Z} & & \mathbb{Z}/2\mathbb{Z} \end{array}$$

There is a concept of "free" module for which a basis exists, and there are no linear relations.

Def. Defn of linear relation for R-modules: M: a linear combination

$$a_1 m_1 + \cdots + a_n m_n = 0 \in M.$$

$a_i \in R \quad m_i \in M.$

Canonical example:

$$\underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{n \text{ times}} = \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ times}}.$$

is a free $\mathbb{Z}$-module on n generators.

The distinction between $\times$ and $\oplus$ comes mainly in the infinite case. Example from vector spaces

Let $V = \{(a_1, a_2, \ldots) \mid a_i \in \mathbb{R}\}$

Let $V_i \subset V$ be $V_i = \{(a_1, \ldots, a_i, 0 \cdots)\}$.

Let $U = \bigcup_{i=1}^{\infty} V_i$.

$U \neq V$. U is more like $\oplus$

V is more like $\times$.

$\underbrace{R \times \cdots \times R}_{n \text{ times}}$ is an R-module, free on n generators

This is written $R \oplus \cdots \oplus R$.

Notice that if R is a field F, all f.g. modules are of this form.

But $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ is a $\mathbb{Z}$-module NOT of this form.

Similarly $F[x]/(x^2)$ is a $F[x]$-module not of the form $F[x] \oplus \cdots \oplus F[x]$.

Many analogies to groups carry over:

Concept of a "homomorphism" (similar to linear transformation)

Concept of a "quotient module" similar to quotient group / vector space.

The sum of two submodules is a submodule.

There are "isomorphism theorems" e.g.

if $A \subset B \subset M$ are s.b modules

$$(M/A)/(B/A) \cong M/B.$$

You learned in the linear algebra class that if V, W are vector spaces / F then $\mathrm{Hom}(V, W)$ = linear trans $V \to W$ is also a vector space.

If M and N are R-modules, then

$\mathrm{Hom}_R(M, N)$ = R-module homomorphisms $M \to N$

is an abelian group

And if R is commutative then

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

[Of course we have not yet written down the definition of R-module homomorphism.]

What must the def'n be?

It must preserve scalar mult (by elts of R) and addition (of elts of M).

[Much like def'n of lin trans.]

If we have two such things, θ, φ we can add them.

Define $(\theta+\varphi)(m) = \theta(m) + \varphi(m)$

$$(\theta+\varphi)(m+m') = \theta(m+m') + \varphi(m+m')$$
$$= \theta(m) + \theta(m') + \varphi(m) + \varphi(m')$$
$$= \theta(m) + \varphi(m) + \theta(m') + \varphi(m')$$
$$= (\theta+\varphi)(m) + (\theta+\varphi)(m')$$

Similarly $(\theta+\varphi)(rm) = r \cdot (\theta+\varphi)(m)$.

Thus $\mathrm{Hom}_R(M, N)$ is an ab. gp.

Q: Where does showing $\mathrm{Hom}_R(M,N)$ is an R-module require the commutativity of R?

We need to show.

$r \cdot \varphi$ is an R module hom.

where $\varphi \in \mathrm{Hom}_R(M,N)$

This requires that we show

$$(r\cdot\varphi)(sm) = s(r\cdot\varphi)(m).$$

The defn of $(r\cdot\varphi)(m)$ is $r\varphi(m)$.

Thus we must show

$$r\varphi(sm) = rs\varphi(m) = sr\varphi(m).$$

Homework will be posted Due Wed Oct 25.

Quiz monday Oct. 23 Covering 10.1, 10.2.