Algebra II: Modules.

Def R ring. A (left) R-module M is an abelian group $(M,+)$ and an action $R \circlearrowright M$ s.t. $\forall r,s \in R,\ x,y \in M$.

$r\cdot(x+y) = rx+ry$

$(r+s)\cdot x = rx+sx$

$(rs)x = r(sx)$

$1x = x$.

Examples 1). R = field $\rightsquigarrow$ R-modules are R-vector spaces.

2). If $R=\mathbb{Z}$: Then R-modules are just abelian gps:

R-module structure on G:

$n>0$: $ng = \underbrace{g+\cdots+g}_{n \text{ times}}$, $0\cdot g = 0$, $(-n)g = -(ng)$.

3). $R^n = R\times\cdots\times R$ is an R-module (componentwise ring mult.)

4). If I is an ideal of R, it's an R-module.

Def M, N are R-modules. A homomorphism is $f: M \to N$ s.t. $f(rx+sy) = rf(x)+sf(y)$.

Def $N \neq \emptyset$, $N \subseteq M$ is a submodule (write $N \leq M$) if $rx+sy \in N$ $\forall r,s \in R,\ x,y \in N$.

The kernel of a hom $f: M \to N$ is a submodule of M, the image is a submodule of N.

Defs: $S \subseteq M$ is linearly independent ($/R$) if $\sum_i c_i x_i \Rightarrow c_i = 0\ \forall i$

$S \subseteq M$ spans M if $\forall x \in M\ \exists c_1,\dots,c_n \in R$, with $\forall x_1,\dots,x_n \in S,\ c_i \in R$, $\sum c_i x_i = x$.

A basis is a linearly indep. spanning set.

A module with a basis is free.

Unlike vector spaces, not all modules are free:

Ex: $R=\mathbb{Z}$, $M=\mathbb{Z}/n\mathbb{Z}$ for $n>1$.

Then $\forall g\in M$, $|M|=n \Rightarrow ng=0$. Thus, for any $\{g_1,\dots,g_m\}\subseteq M$, $ng_1+\dots+ng_m=0+\dots+0=0$
$\Rightarrow$ the set is linearly dependent $\Rightarrow$ not a basis.

The problem here was torsion (finite order elts.)

We'd like to say rank(M) = size of a basis, but this isn't even well defined!

Example: $R=\mathbb{Z}$, $M=\mathbb{Z}\times\mathbb{Z}\times\dots$ countably infinite direct product

Given a ring R and two R-modules M,N, we set $\mathrm{Hom}_R(M,N)$ to be the set of all R-mod. hom: $M\to N$.

This is an R-module under the operations:
$(\varphi+\psi)(m)=\varphi(m)+\psi(m)$; $(r\cdot\varphi)(m)=r\cdot(\varphi(m))$.

and given $\varphi\in\mathrm{Hom}_R(L,M)$, $\psi\in\mathrm{Hom}_R(M,N)$, $\psi\circ\varphi\in\mathrm{Hom}_R(L,N)$.

If $M=N$, $\mathrm{Hom}_R(M,M)=\mathrm{End}_R(M)$ is the endomorphism ring.

For $M=\mathbb{Z}\times\dots\times\mathbb{Z}$, take $\mathrm{End}_{\mathbb{Z}}(M)=:R$.

Two elements of R are: $\varphi_1(a_1,a_2,a_3,\dots):=(a_1,a_3,a_5,\dots)$
and $\varphi_2(a_1,a_2,a_3,\dots):=(a_2,a_4,a_6,\dots)$.

Define $\psi_1(a_1,\dots)=(a_1,0,a_2,0,\dots)$, $\psi_2(a_1,a_2,\dots)=(0,a_1,0,a_2,\dots)$

Then $\varphi_1(\psi_1(a_1,a_2,\dots))=\varphi_1(a_1,0,a_2,0,\dots)=(a_1,a_2,\dots)$

$\varphi_2(\psi_2(a_1,a_2,\dots))=\varphi_2(0,a_1,0,a_2,\dots)=(a_1,a_2,\dots)$

$\Rightarrow \varphi_i\psi_i=1$, $i=1,2$.

Similarly, $\varphi_1\psi_2 = \varphi_2\psi_1 = 0$.

Claim: φ_1, φ_2 are R-lin. ind.

Why: If $\exists\, \pi_1, \pi_2 \in R$, at least one non-zero, s.t. $0 = \pi_1\varphi_1 + \pi_2\varphi_2$, then mult. on the right by $\psi_1 + \psi_2$ $\rightsquigarrow$

$$0 = (\pi_1\varphi_1 + \pi_2\varphi_2)(\psi_1 + \psi_2) = \pi_1\varphi_1\psi_1 + \pi_1\varphi_1\psi_2 + \pi_2\varphi_2\psi_1 + \pi_2\varphi_2\psi_2 = \pi_1 + \pi_2 = 0.$$

Similarly, mult. on right by $\psi_1 - \psi_2 \rightsquigarrow 0 = \pi_1 - \pi_2$

Adding (subtracting) $\Rightarrow 2\pi_1 = 2\pi_2 = 0 \Rightarrow \pi_1 = \pi_2 = 0$ ☐

(↑ composition with doubling map)

Claim. φ_1, φ_2 span R:

Why: every f is $f = f\cdot\varphi_1\psi_1 = f\cdot 1 = f$.

Now we claim that $R \cong R^2 \overset{\text{induction}}{\rightsquigarrow} R \cong R^n \ \forall\, n \geq 1$.

Why: $R \to R^2$ $\quad$ $R^2 \to R$

(inverse homs): $\vartheta \mapsto (\vartheta\varphi_1, \vartheta\varphi_2)$ $\quad$ $(\vartheta_1, \vartheta_2) \to \vartheta_1\varphi_1 + \vartheta_2\varphi_2$.

So for F-vector spaces, the "big theorem" is that every finite dimensional one is $\cong F^n$ for some unique n; that is not true for general modules!

Quotient modules: As expected; $N \leq M$ R-modules.

M/N is the R-module: ~~$r(x+N) = rx+N$~~, $x+$

elts are $x+N$; $N \leq M$ is an abelian subgp.; M/N is the quotient gp. of $(M,+)$ abelian.

and $x \mapsto r(x+N) = rx+N$.

This quotient always works, basically b/c we assume $(M,+)$ abelian.

Lemma: $R \neq 0$ a commutative rng. Then

$R^m \cong R^n \Rightarrow m = n$.

(Like in above example)

PF: Let π be a max^{m} ideal in R.
Let $M = R^m$, $N = R^n$. If $M \cong N$ as R-modules
this restricts to an isomorphism
$$M/\pi M \cong \pi N.$$
$\rightsquigarrow$ induced isomorphism $M/\pi M \cong N/\pi N$
$\Rightarrow (R/\pi)^m \cong (R/\pi)^n$ as R-modules,
hence as vector spaces $\Rightarrow m = n$ ☐

Isomorphism thms hold, as expected:

1). $M/\ker(\varphi) \cong \varphi(M)$

2). $(A+B)/B \cong A/(A \cap B)$ (sum: $A+B := \{a+b \mid a \in A, b \in B\}$)

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

4). $\{\text{submodules of } M/N\} \longleftrightarrow \{\text{submodules of } M \text{ containing } N\}$. (1:1)

It gets weirder!

Example: $R = \mathbb{Z}[x_1, x_2, \ldots]$ is a finitely generated R-module as $\{1\}$ spans. Let $S \subseteq R$ be the submodule of polys. $\ni$ 0 constant term.

S is not finitely generated as suppose $\{p_1, \ldots, p_n\}$ spans.
Let x_K be a variable not appearing in any $p_1, \ldots, p_n$.
Then no lin. comb. of the p_i can be x_K, as if
$x_K = \sum_i a_i(x) p_i(x)$, and if $a_i(x) = x_K q_i(x) + r_i(x)$,
$r_i(x)$ has no x_K
then $x_K = \sum_i (x_K q_i(x) + r_i(x)) p_i(x)$

$= x_K \sum q_i(x) p_i(x) + r \sum r_i(x)\, p_i(x)$. ← this $\sum$ has no x_K so must be $\underline{0}$.

$\Rightarrow$ ~~$\sum q_i p_i = x$~~ $\cdot \sum q_i(x) p_i(x) = 1$.

This is impossible as each p_i has no constant term.

Def A cyclic module is generated by one elt.,

$M = R \cdot a$.

Recognizing direct products (same as for gps):

$N_1, \dots, N_K$ submodules of M.

then $\pi: N_1 \times \cdots \times N_K \to N_1 + \cdots + N_K$

$(a_1, \dots, a_K) \mapsto a_1 + \cdots + a_K$

is an isomorphism

$\Updownarrow$

$N_j \cap (N_1 + \cdots + \hat{N}_j + \cdots + N_K) = 0 \ \forall j$.

$\Updownarrow$

every $x \in N_1 + \cdots + N_K$ is uniquely of the form

$x = a_1 + \cdots + a_K$, $a_i \in N_i$.

In this case, $M = N_1 \oplus \cdots \oplus N_K$ is the internal direct sum.

For commutative rings, modules that are free of rank n are just $M \cong R^n$

$M \xrightarrow{\sim} R^n$

$\sum c_i a_i \mapsto (c_i)$ uniqueness of representation as in lin. alg.

Ex: $R = \mathbb{Z} \to \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ free abelian gp. of rank n (more ex. (2)).

Def M is a **Noetherian module** if

$M_1 \subseteq M_2 \subseteq \dots$ increasing chain of submodules terminates: $M_k = M_{k+1} = M_{k+2} = \dots$ eventually.

- R is Noetherian if it is as an R-module (chains of ideals terminate)

Example: F a field, $R = F[x]$, V a vector space / F, $T: V \to V$ a linear transformation.

V is an F-module, using T, we can make V an $F[x]$-module.

$T^n = T \circ T \circ \dots \circ T$ (n times), given maps $A, B: V \to V$, $\alpha, \beta \in F$,

$\alpha A + \beta B : V \to V$, $v \mapsto \alpha(A(v)) + \beta(B(v))$

Given $p(x) = a_n x^n + \dots + a_0 \in F[x]$, define

$p(x) \cdot v = (a_n T^n + \dots + a_0)(v) = \sum_i a_i T^i(v)$.

This makes V an $F[x]$ module.

This naturally extends the action of F to $F[x]$.

The module structure depends on the choice of T.

It turns out: all $F[x]$ modules arise in this way.

Why: If V is an $F[x]$ module, V is an F-module, everything determined by what x does, which must be a lin. transf.

Further an $F[x]$ submodule W must be an F-submodule (i.e., a vector subspace of V), and we must have $T(w) \in W$ $\forall w \in W$.

That is, W is a T-stable subspace of V

$T(W) \subseteq W \Rightarrow T^n(W) \subseteq W$ $\forall n \geq 1$.