More nuts and bolts on modules.

Direct products. [38.4]

Special case, R^n : a free R-module of rank n.

This is where we get linear algebra again.

Def. An R-module F is free on a subset $A \subseteq F$ if, for every nonzero $x \in F$, there are unique nonzero $r_1, \ldots, r_n \in R$ and $a_1, \ldots, a_n \in A$ s.t. $x = r_1 a_1 + \cdots + r_n a_n$ (for some $n \in \mathbb{Z}^+$)

Equivalently: Every $x \in F$ (zero or not) can be written uniquely as
$$x = \sum_{a \in A} r_a a$$
where all but finitely many of the r_a are zero.

We say A is a set of free generators or basis for F.

Not every module is free.

Example. $\mathbb{Z} \times \mathbb{Z}/5$ is not a free $\mathbb{Z}$-module.

Example. Let $R = \mathbb{Z}[x]$, $I = (2, x)$ ideal generated by 2 and x.

I is not free as an R-module.

There are R-relations between the generators.

Given (say) $x^2 + 4x + 6$, there are lots of ways to write $x^2 + 4x + 6 = 2f + xg$ for $f, g \in R$.

Same is true of any other generating set you write down.

(Note R is not a PID)

Theorem. Given a ring R and any set A.

Then there is a free module $F(A)$ on the set A with the following universal property:

Given any R-module M and map of sets $A \xrightarrow{\varphi} M$, there is a unique R-module hom $\Phi : F(A) \longrightarrow M$ making the following commute:

$$\begin{tikzcd} A \arrow[r, hook, "\iota"] \arrow[dr, "\varphi"'] & F(A) \arrow[d, "\Phi"] \\ & M \end{tikzcd}$$

(inclusion)

Proof. ~~Could construct $F(A)$ as formal R-combos of A, but do this instead.~~ (Assume $A \neq \phi$)

Let $F(A) = \{$ set fns. $f : A \longrightarrow R$ with finite support: $f(a) = 0$ for all but finitely many $a\}$.

R-module structure on $F(A)$:

$$(f+g)(a) = f(a) + g(a)$$
$$(rf)(a) = r(f(a)).$$

R-module axioms easy to check. Also freeness.

Inclusion $A \hookrightarrow F(A)$: $\quad a \longrightarrow f_a := \left\{ \begin{array}{l} a \longrightarrow 1 \\ \text{anything else} \longrightarrow 0 \end{array} \right\}$

(Note: this is a set map, A is not an R-module)

Identify this with formal R-linear combos of elts. of A

39.3

i.e. identify

$$f \longmapsto r_1 a_1 + \cdots r_n a_n$$

where $f(a_i) = r$

$f(a) = 0$ for $a \neq a_1, \ldots, a_n$.

This is a bijection.

$(\longrightarrow)$

39.~~3~~4.

The map $F(A) \xrightarrow{\Phi} M$:

$$\Phi : \sum_{i=1}^{n} r_i a_i \longrightarrow \sum_{i=1}^{n} r_i \varphi(a_i) .$$

This is :

* well defined, since $F(A)$ is free
($\sum_{i=1}^{n} r_i a_i$ can't be written some other way)

* Restriction of Φ to A equals φ.
Equivalently, $\Phi \circ \iota = \varphi$.
Says that $\Phi(a) = \varphi(a)$, which is true.

* Unique : $F(A)$ is generated by A,
Can write any elt. of $F(A)$ as above, and <u>must</u> have

$$\Phi\left(\sum r_i a_i\right) = \sum r_i \, \Phi(a_i)$$
$$= \sum r_i \, \varphi(a_i)$$ (demand that diagram commute).

<u>Cor.</u>
(1) If F_1 and F_2 are free modules on A, there is a unique iso $F_1 \to F_2$ which is the identity map on A.

(2) If F is a free R-module w/ basis A, $F \cong F(A)$.

39.5

Proof. (1)

$$\begin{tikzcd}
A \arrow[r, hook, "\iota"] \arrow[dr, hook, "\phi"'] & F_0(A) \arrow[d, "\Phi"] \\
& F_1
\end{tikzcd}$$

There is a unique map Φ making the diagram commute.

Surjective, because it maps onto $\phi(a)$ for all a and these generate F_1 as an R-module.

Injective, because if

$$\Phi\left(\sum_{i=1}^{n} r_i a_i\right) = \sum_{i=1}^{n} r_i \varphi(a_i) = 0,$$

by freeness of F_1.

So any ~~free~~ R-module which is free on A is isomorphic to $F(A)$.

Isomorphic uniquely if you demand that it be the identity on A.

(Otherwise not unique: for example, could compose w/ an element of $\mathrm{Sym}(A)$.)

Def. / Theorem. Let R be a ring and M a left R-module. M is <u>Noetherian</u> if it satisfies the following three equivalent conditions.

(1) It satisfies the <u>ascending chain condition</u>:
Given a sequence of modules
$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots,$$
there exists $N \in \mathbb{Z}^+$ s.t. $M_n = M_N$ for all $n \geq N$.

(2) Every nonempty set of submodules of M contains a maximal element under inclusion.

(3) Every submodule of M is finitely generated.

A ring R is Noetherian if it is so as a left module over itself, i.e:

(a) If there are no infinite increasing chains of left ideals;

(b) If every left ideal is finitely generated.

Proof of equivalence of (1) - (2) - (3).

(1) → (2). (Uses axiom of choice)

Given S: set of submodules of M.

Choose (arbitrarily) $M_1 \in S$,

$M_2 \in S$ with $M_2 \supsetneq M_1$,

$M_3 \in S$ with $M_3 \supsetneq M_2$,

etc.

By (1) we can't keep going forever, there is some $M_N \in S$ with no $M \in S$ with $M \supsetneq M_N$.

40.2

$(2) \to (3)$.

Choose a submodule $N \subseteq M$.

Let $S = \{$ finitely generated submodules of $N\}$.

WTS $S \ni N$.

By (2), S contains a maximal element N'.

If $N \neq N'$, then there exists some $n \in N$ not in N'.

But then $N' + Rn$ is finitely generated

(with one more generator than N')

Contradicts maximality!

$(3) \to (1)$.

Given a sequence

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

The infinite union $M^* = \bigcup_{i=1}^{\infty} M_i$ is also a submodule of M.

By (3) it is finitely generated.

Write $M^* = Rm_1 + \cdots + Rm_k$ for some k.

For each m_i, it is contained in some M_{n_i}.

Choose the largest of the M_{n_i} (call it M_n)

Then $M_n = M_{n+1} = M_{n+2} = \cdots = M^*$, since it contains all the generators!

40.3. There is structure theory. Example.

Lemma. Suppose $V \geq W$ are R-modules.
Then V is noetherian iff W and V/W are.

Proof. If V is noetherian —
an ascending chain in W is also one in V
an ascending chain in V/W can be pulled back to V.
i.e. $A_1/W \leq A_2/W \leq A_3/W \leq \cdots$ corresponds to
$A_1 \leq A_2 \leq A_3 \leq \cdots$

The other way. Given a chain
$B_1 \leq B_2 \leq B_3 \leq \cdots\cdots$ in V, then
$B_1 \cap W \leq B_2 \cap W \leq B_3 \cap W \leq \cdots\cdots$ terminates
$\frac{B_1 + W}{W} \leq \frac{B_2 + W}{W} \leq \cdots\cdots$ terminates.
So $B_1 + W \leq B_2 + W \leq \cdots\cdots$ does.

Prove: $\left.\begin{cases} B_k \cap W = B_{k+1} \cap W \\ B_k + W = B_{k+1} + W \end{cases}\right\} \Longrightarrow B_k = B_{k+1}$.

If there is $x \in B_{k+1} - B_k$,
then $x \in B_k + W$.
So write $x = b + w$ $(b \in B_k,\ w \in W)$
Since $b, x \in B_{k+1}$,
$w \in B_{k+1}$ also.
So $w \in B_{k+1} \cap W = B_k \cap W$.
So $w \in B_k$ after all.

Hilbert Basis Theorem. If R is Noetherian, so is $R[x]$.

(And by induction, $R[x_1, \dots, x_n]$.)
(Vakil, FOAG)

Proof. Given $I \trianglelefteq R[x]$.

Produce a series of generators.

For each n, f_n is any elt. of $I - (f_1, \dots, f_{n-1})$ of lowest degree.

If this procedure terminates $\Rightarrow$ done.

Otherwise, let a_n be the initial coeff of each f_n.

Since R is Noetherian, $(a_1, a_2, \dots) = (a_1, a_2, \dots, a_N)$ for some N. Write $a_{N+1} = \sum_{i=1}^{N} r_i a_i$.

Then: $$f_{N+1} - \sum_{i=1}^{N} r_i f_i \, x^{\deg(f_{N+1}) - \deg(f_i)}$$

has lower degree than f_{N+1}, contradiction.

Example. $\mathbb{C}[x,y]$ is Noetherian. (any quotient too)

Given a sequence of monomials
$f_1 = x^{a_1} y^{b_1}$, $f_2 = x^{a_2} y^{b_2}$, ...
$I_1 = (f_1)$, $I_2 = (f_1, f_2)$, ...
chosen so that $f_n \notin I_{n-1}$.

Has to stop.

Corollary. Infinite Chomp terminates.

41.1. (Finals week make up)

Prehomogeneous vector spaces.

Definition. Let G be a group. A representation of G is a homomorphism $\rho : G \to GL(V)$ for some vector space V.

(Recall $GL(V) = \{ \phi \in End(V) : \phi \text{ is invertible} \}$.

Proposition. A representation $\rho : G \to GL(V)$ induces an action of G on V, given by

$$g \cdot v = \rho(g) v .$$

This is immediate. To be checked:

(1) $\rho(g_1) \cdot (\rho(g_2) \cdot v) = (\rho(g_1 g_2)) \cdot v$

(2) $\rho(1) \cdot v = v$

(2) follows because $\rho(1) = I$

(1) follows because $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$ and $End(V)$ acts on V.

Definition. Let (G, V) be a complex representation.

(i.e. given a group G

a vector space $V / \mathbb{C}$

a representation $\rho : G \to GL(V)$)

(G, V) is prehomogeneous if the action of G has a dense Zariski-open orbit.

41.2.

In practice: There exists an irreducible polynomial P defined on V s.t. $P(v) \neq 0$, $P(v') \neq 0 \Rightarrow \exists g \;\; g \cdot v = v'$.

Example. Binary cubic forms

$$V = \{au^3 + bu^2v + cuv^2 + dv^3 : a,b,c,d \in \mathbb{C}\}.$$

Action of $GL(2, \mathbb{C})$:

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \circ f(u,v) = f(\alpha u + \gamma v, \beta u + \delta v)$$

or better yet the "twisted action"

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \circ f(u,v) = \frac{1}{\alpha\delta - \beta\gamma} f(\alpha u + \gamma v, \beta u + \delta v).$$

Why is this a group action?

Proof 1. Grit it out.

Proof 2. Think of (u,v) as a row vector in $\mathbb{C}^2$.

So a binary cubic form is a function $\mathbb{C}^2 \to \mathbb{C}$.

Then $g \circ f((u,v)) = f((u,v)\,g)$.

Need: $(g_1 g_2) \circ f((u,v)) = g_1 \circ (g_2 \circ f)((u,v))$.

LHS is $f((u,v)\,g_1 g_2)$.

RHS is $(g_2 \circ f)((u,v)\,g_1)$ | $g_1 \circ f((u,v)\,g_2)$

$= f((u,v)(g_1 g_2))$ | $= f((u,v)\,g_1 g_2)$.

41.3.

If this is confusing.

$$g \circ f = \{ v \longrightarrow f(vg) \}$$

$g_1 \circ (g_2 \circ f)$

$$\text{(a)} \quad = g_1 \circ \{ v \longrightarrow f(vg_2) \}$$

$$= \{ v \longrightarrow f((vg_1)g_2) \}$$

$$\text{(b)} \quad = \{ v \longrightarrow (g_2 \circ f)(vg_1) \}$$

$$= \{ v \longrightarrow \{ w \longrightarrow f(wg_2) \} (vg_1) \}$$

$$= \{ v \longrightarrow f(vg_1g_2) \}.$$

Why the twisted action?

This ensures "scalar matrices act by scalars":

$$\begin{bmatrix} \lambda & \\ & \lambda \end{bmatrix} \circ f(u,v) = \frac{1}{\lambda^2} f(\lambda u, \lambda v)$$

$$= \frac{1}{\lambda^2} \left[a(\lambda u)^3 + b(\lambda u)^2(\lambda v) + c(\lambda u)(\lambda v)^2 + d(\lambda v)^3 \right]$$

$$= \lambda f(u,v).$$

So, for example, if $\zeta_3 = e^{2\pi i/3}$ is a primitive third root of unity,

$$\begin{bmatrix} \zeta_3 & \\ & \zeta_3 \end{bmatrix} \circ f(u,v) = \zeta_3 f(u,v).$$

Otherwise $\begin{bmatrix} \zeta_3 & \\ & \zeta_3 \end{bmatrix}$ acts trivially!

41.4.

The structure theorem.

The twisted action of $GL(2, \mathbb{C})$ on $V(\mathbb{C})$ has four orbits:

Orbit description	Stabilizer of any point
$\{f \in V(\mathbb{C}) : f \text{ has distinct roots}\}$	$\mathrm{Sym}(3)$
$\{f \in V(\mathbb{C}) : f \text{ has exactly a double root}\}$	$\mathbb{C}^\times$
$\{f \in V(\mathbb{C}) : f \text{ has a triple root}\}$	$\mathbb{C} \rtimes \mathbb{C}^\times$
$\{0\}$	$GL_2(\mathbb{C})$

How do you prove this?

Make $GL(2, \mathbb{C})$ act on linear forms.

Easier if we "mod out by scalars".

$\cancel{\gamma \cdot (\alpha x + \beta y) \in \mathbb{P}}$

<u>Definition.</u> The <u>projective line</u> $\mathbb{P}^1(\mathbb{C})$ consists of pairs $[x : y]$ with $x, y \in \mathbb{C}$ not both zero, subject to the equivalence

$$[\lambda x : \lambda y] = [x : y] \quad \text{for } \lambda \in \mathbb{C}^\times.$$

41.5.

Definition. The *projective linear group* $PGL_2(\mathbb{C})$ is $GL_2(\mathbb{C}) / Z(GL_2(\mathbb{C}))$, or equivalently equivalence classes in $GL_2(\mathbb{C})$ where $M \sim \lambda M$ for any $M \in GL_2(\mathbb{C})$ and scalar $\lambda \in \mathbb{C}^\times$.

Then $PGL_2(\mathbb{C})$ acts on $\mathbb{P}V$ and on $\mathbb{P}^1(\mathbb{C})$.

The action on $\mathbb{P}^1$ is covariant:

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} [x : y] = [\alpha x + \beta y : \gamma x + \delta y].$$

We get a WD action of $PGL_2(\mathbb{C})$ because you quotient out by scalar multiples on both sides.

Theorem. (Exercise!) $PGL_2(\mathbb{C})$ acts simply triply transitively on $\mathbb{P}^1(\mathbb{C})$.

That is: Given $z_1, z_2, z_3, w_1, w_2, w_3 \in \mathbb{P}^1(\mathbb{C})$ s.t. the z_i are all distinct and the w_j are all distinct, there exists a unique $g \in PGL_2(\mathbb{C})$ with $g \cdot z_i = w_i$ for $i = 1, 2, 3$.

Hint. Enough to choose $z_1 = [1:0]$, $z_2 = [0:1]$, $z_3 = [1:1]$.

41.6.

The roots of a binary cubic form:

If $f \in V(\mathbb{C}) - \{0\}$, then f can be factored as

$$f = (a_1 u + b_1 v)(a_2 u + b_2 v)(a_3 u + b_3 v)$$

for some $a_1, b_1, a_2, b_2, a_3, b_3 \in \mathbb{C}$.

This is unique up to:

(1) Rearrangement of factors

(2) Adjustment of scalar multiples.

The action of $GL_2(\mathbb{C})$ and $PGL_2(\mathbb{C})$ acts on the roots $[-b_1 : a_1]$ as well.

Suppose $f([-b_1 : a_1]) = 0$.

Then what are the roots of gf for some $g \in PGL_2(\mathbb{C})$?

$$gf([b:a]) = 0 \iff f(g^T [b:a]) = 0.$$

So $[b:a]$ is a root of gf

$\iff g^T[b:a]$ is a root of f.

Or: $[b:a]$ is a root of $f \iff (g^T)^{-1}$ is a root of gf.

Claim. If f, f' both have distinct roots, then $f = g \cdot f'$ for some $g \in PGl_2(\mathbb{C})$.

Sketch proof.

(1) It suffices to argue in $\mathbb{P}V$:

If f, f' are forms up to scalar multiples, there is $g \in PGL_2(\mathbb{C})$ with $gf = f'$.

This is because you can use scalar matrices to adjust the scalars.

(2) Up to scalars, f is determined by the unordered set of roots $\{\theta_1, \theta_2, \theta_3\} \in \mathbb{P}^1(\mathbb{C})$

f' is determined by $\{\tau_1, \tau_2, \tau_3\}$.

Use the theorem. Find $g \in PGL_2(\mathbb{C})$ with $g\theta_i = \tau_i$ for $i = 1, 2, 3$.

Then we win!

Moreover, if $\{\tau_1, \tau_2, \tau_3\}$ is a reordering of $\{\theta_1, \theta_2, \theta_3\}$, g will be nontrivial but $f = f'$ in $\mathbb{P}(V)$.

This is why the stabilizers are Sym(3)!