Lecture 7 - Noetherian rings & Invariant Theory

Noetherian modules & rings

Def^n) An R-module M is finitely generated if $\exists\, a_1, \dots, a_n$ st. each $a \in M$ is of form
$a = r_1 a_1 + \dots + r_n a_n$.

- Equivalently, if $\exists\, n \in \mathbb{N}$ & surjective hom.

$$R^n \longrightarrow M$$

free R-mod on n elements

Def^n) An R-module M is Noetherian if all its submodules are f.g.

- In partic., M itself must be f.g.
- Below are some equiv. descriptions of the Noetherian property.

Proposition

TFAE:

① M is Noetherian

② M sat the ascending chain condition (acc): each sequence $M_0 \subseteq M_1 \subseteq \dots \subseteq M_n \subseteq \dots \subseteq M$ stabilises - ie. $\exists\, k \in \mathbb{N}$ st $M_k = M_{k+i}$ $\forall i \in \mathbb{N}$.

③ Every non-empty set $\mathcal{F}$ of submodules of M has a maximal elements, ordered by inclusion.

Proof

$1 \Rightarrow 2$) The union $\bigcup_{i \in \mathbb{N}} M_i \subseteq M$ is a submodule, so by ① it is fg by $a_1, \dots, a_n$. Since each $a_i \in \bigcup M_i$ belongs to some A_{k_i}, then $a_1, \dots, a_n \in A_k$ where $k = \max(k_1, \dots, k_n)$.
Hence $A_k = \bigcup A_i$ & the sequence stab. @ A_k.

$2 \Rightarrow 3$) For a contradiction, suppose $\mathcal{F}$ is non-empty set of submodules of M not having max^l element. Choose $M_0 \in \mathcal{F}$. As M_0 not max^l, $\exists M_0 \subset M_1 \subset M$ where $M_1 \in \mathcal{F}$. Continue in this way to create chain

$$M_0 \subset M_1 \subset M_2 \subset \dots \subset M_n \subset \dots \subset M$$

that doesn't stabilise. Hence $2 \Rightarrow 3$)

$3 \Rightarrow 1$) Let $N \subseteq M$ & $\mathcal{F}$ the set of f.g. submods. of N. Then $\{0\} \in \mathcal{F}$ so non-empty; hence has max^l elt $A = \langle a_1, \dots, a_n \rangle \leq N$. We claim $A = N$. Indeed, if $b \in N - A$ then $A = \langle a_1, \dots, a_n \rangle \subset \langle a_1, \dots, a_n, b \rangle \leq N$ but this contradicts maximality of A. $\square$

Properties of Noetherian modules

(1) Let M be an R-mod & $N \leq M$. Then M is Noetherian $\Leftrightarrow$ N is Noeth. & M/N is Noeth.

(2) If M is Noeth so is M^n.

- Proofs left as an exercise.

Noetherian rings

Def^n) A ring R is left Noetherian if R is Noetherian as a left R-module,
right Noetherian ...... R ...... right R-module,
Noetherian if both left & right Noetherian.

- For R commutative, R-Mod $\cong$ Mod$_R$ so left Noeth. $\equiv$ Noeth $\equiv$ right Noeth.
- A submodule of R (as a left R-module)

is a left ideal of R; hence R is (left) Noeth. if left ideals are fin. gen.

Examples

- If R is a field, it's only ideals are $\{0\}$ & R - hence R is Noetherian.
- If R is a principal ideal domain - eg. $\mathbb{Z}$ - all of its ideals are gen by a single element. Therefore R is Noetherian.

Non-example

- Note R is free R-module on 1 - $r = r.1$ - & so finitely generated. Hence a non-Noetherian it gives an example of a f.g. module with a non-f.g. submodule.
- An example of such a ring is $R[x_1, x_2, \ldots, x_n, \ldots]$ the ring of polys in inf. many variables. It has sequence of ideals $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \langle x_1, x_2, x_3 \rangle \subset \ldots R[x_1, \ldots, x_n]$ which never stabilises so this is a non-Noeth. ring; indeed the non f.g. ideal $\bigcup_{n \in \mathbb{N}} \langle x_1, \ldots, x_n \rangle =$ ideal of polynomials with no scalar term.

Theorem (Hilbert's basis Theorem)

Let R be (left) Noetherian. Then so is the polynomial ring $R[x_1, \dots, x_n]$.

Proof

- Since $R[x_1, x_2] = R[x_1][x_2] \dots$ it suffices, by induction, to show that $R[x]$ is Noeth if R is.
- Suppose $I \subseteq R[x]$ which is not f.g. — we will derive a contradiction.
- Given a poly. $c_n x^n + \dots + c_1 x + c_0$ we say its degree is n & leading term is c_n.
- Choose $f_0 \in I$ of minimal degree. As I is not f.g. $\exists f_1 \in I - \langle f_0 \rangle$ of min. degree.
- Continuing in this way, we obtain $f_{n+1} \in I - \langle f_0, \dots, f_n \rangle$ of min deg. for each n.
- By construction $\deg(f_0) \leq \deg(f_1) \leq \deg(f_2) \leq \dots$
- Let a_i be leading term of f_i.
- Then we have chain of ideals of R $\langle a_0 \rangle \subseteq \langle a_0, a_1 \rangle \subseteq \dots$.
- As R is Noetherian, it stabilises at $\langle a_0, a_1, \dots, a_m \rangle$. Then $a_{m+1} = r_0 a_0 + \dots + r_m a_m$ for some $r_i \in R$.
- Since $\deg(f_{m+1}) \geq \deg(f_i)$ all $i \leq m$, we can form the polynomial

$$g = \sum_{i=0}^{m} r_i \, x^{(d(f_{m+1}) - d(f_i))} f_i \in \langle f_0, \dots, f_m \rangle$$

- This poly. is a sum of polys of degree

$d(f_{m+1})$ & so g has deg $d(f_{m+1})$.

- If $f_{m+1} - g \in \langle f_0, \dots, f_m \rangle$ then we would have $f_{m+1} = (f_{m+1} - g) + g \in \langle f_0, \dots, f_m \rangle$ too as ideal closed under sums, which is false. Hence $f_{m+1} - g \in I - \langle f_0, \dots, f_m \rangle$.
- Therefore its degree $\geqslant$ degree $\langle f_{m+1} \rangle$.
- However,

$$f_{m+1} - g = f_{m+1} - \left(\sum_{i=0}^{m} r_i \, x^{(d(f_{m+1}) - d(f_i))} f_i \right)$$

has term of top degree $d(f_{m+1})$ & this is $a_{m+1} - \sum_{i=0}^{m} r_i a_i = 0$.

Therefore $f_{m+1} - g$ has lower degree than f_{m+1}, which is a contradiction. $\square$

Prop^n If $f : R \twoheadrightarrow S$ a surj. hom. of rings. If R is Noetherian so is S.

Proof

For $I \subseteq S$ an ideal, then $f^{-1}(I) \subseteq R$ an ideal with $f(f^{-1} I) = I$.

As R is Noeth, $f^{-1} I = \langle a_1, \dots, a_n \rangle$.

Therefore $I = f(f^{-1} I) = f \langle a_1, \dots, a_n \rangle$
$= \langle f a_1, \dots, f a_n \rangle$. $\square$

After break, apply to invariant theory.

k-Algebras & Invariant Theory

- Let R be a comm. ring. An <u>R-algebra</u> is a R-module $(A,+,0)$ with a ring str. $(A,+,0,\cdot,1)$ such that $\cdot$ is R-bilinear function: that is, $r(a.b) = ra.b = a.rb$.
- The R-alg A is <u>commutative</u> if $\cdot$ is commutative.
- A homom. of R-algs is a function preserving both ring & R-module structure.

Categorical remark) R commutative $\Rightarrow$ Mod_R is a <u>monoidal cat</u> $(Mod_R, \otimes_R, R)$ & a <u>monoid</u> in this mon. cat. is an R-alg. / a comm. monoid is a comm. R-alg.

Example) The commutative R-alg. of <u>polynomials</u> $R[x_1,\dots,x_n]$ with coefficients in R

eg. $x_1x_2 + \underset{\in R}{r}x_7^{10}\dots$ is our main example.

This is in fact the <u>free commutative R-alg.</u> on set $\{x_1,\dots,x_n\}$.

Exercise : <u>check this!</u>

Def) An R-algebra A is <u>f.g.</u> if $\exists a_1,\dots,a_n$ st each element of A is a R-linear comb. of products of the a_i ~

eg. $r_1a_1a_2 + 5a_4a_7^6\dots$

For a <u>commutative R-algebra</u> A, this is equiv. to saying that $\exists$ surj. homomorphism $R[x_1,\dots,x_n] \longrightarrow A$ for some n.

Remark) If A is f.g. as an R-module, it is f.g. as an R-alg, but <u>not</u> conversely.

$R[x]$ not f.g. as an R-module as have

$x, x^2, x^3, \ldots$ & none are R-lin. dep.

$\boxed{\text{Prop}^n}$ If R is a comm. Noetherian ring, then each f.g. R-algebra A is a Noetherian ring.

$\boxed{\text{Proof}}$ We have surj. hom $R[x_1, \ldots, x_n] \twoheadrightarrow A$. By Hilbert's basis theorem lhs is Noetherian &, from last time, a surj. quotient of Noeth. ring is Noetherian; hence A is. $\square$

Invariant theory

Problem: understand functions invariant under action of a group G.

- We will look at the case k a field & G acting on comm. k-alg $P = k[x_1, \ldots, x_n]$: that is, we have a group hom

$$G \longrightarrow k\text{-Alg}(P, P)$$
$$g \longmapsto \underset{k\text{-alg hom}}{g.- : P \longrightarrow P}$$

s.t. $e.f = f$ where $e \in G$ is unit & $(g.h).f = g.(h.f)$ for $g, h \in G$.

- The invariants of the action are its fixpoints: those polys f s.t. $g.f = f$ $\forall g \in G$.

- These form a subalgebra $P^G \xhookrightarrow{i} P$.

Fundamental problem of invariant theory

- Determine whether P^G has a finite set of generators (ie. is a f.g. K-algebra).
- We will show this is true in wide generality.

First,

Example

- The symmetric group S_n acts on $\{x_1, \dots, x_n\}$ by permuting them.
- Taking free commutative K-alg $F\{x_1, \dots, x_n\} = P$ we obtain an action of S_n on P by permuting variables:

eg. $(12)(2x_1x_2^2 + 3) = 2x_2x_1^2 + 3$.

- Then P^{S_n} = K-alg. of symmetric functions.

Examples are the elementary symm. functions:

$$f_0 = 1$$

$$f_1 = x_1 + \dots + x_n$$

$$f_2 = \sum_{1 \le i \le j \le n} x_i x_j$$

$$\vdots$$

$$f_n = x_1 . x_2 \dots x_n$$

In fact, P^{S_n} is f.g. as a K-alg by the el. s.f.'s : in fact, each $f \in P^{S_n}$ is uniquely a lin comb of multiples of the esf.

Graded algebras & homogenous polynomials

- A graded K-alg A is one of the form $\bigoplus_{n \in \mathbb{N}} A_n$ where the $A_n \subseteq A$ are K-submodules whose elements are called homogenous of degree n, and where $1 \in A_0$ & if $a \in A_n, b \in A_m$ then $a.b \in A_{n+m}$.
- A morphism $f: A \longrightarrow B$ of graded K-algebras is a K-alg map pres homog. components: ie $F(A_n) \subseteq B_n$ for $n \in \mathbb{N}$.

Example

$P = K[x_1, \ldots, x_n]$ is a graded K-alg. To see this, recall:

- a monomial is a product of the $x_1, \ldots, x_n$ - eg. $x_1 x_2^2$.
- Each polynomial is uniquely a lin. comb. of monomials ~ ie. they form a basis for P as K-module.
- The degree of a monomial is sum of its powers - eg. 3 in above example.

- A poly is homogenous of degree d if all its monomials have degree.
eg. $x_1x_2^2 + 4x_1x_2x_3 + 7x_8^3$ is homogenous of degree 3.

- let $P_d \subseteq P$ consist of homogenous polys of degree d; then as each poly is a sum of hom. components, this makes P a graded K-algebra:

eg. $x_1x_2^2 + 7x_4 + 8x_9 + 4x_1x_2x_3 + 1$

$$= \underset{\overset{\cup}{P_0}}{1} + (\underset{\overset{\cup}{P_1}}{7x_4 + 8x_9}) + (\underset{\overset{\cup}{P_3}}{x_1x_2^2 + 4x_1x_2x_3})$$

- Observe also that the action of S_n on P in previous example preserves the graded algebra structure:

eg $(12): \underset{\overset{\cup}{P_3}}{x_1x_2^2 + x_1x_2x_3} \mapsto \underset{\overset{\cup}{P_3}}{x_2x_1^2 + x_2x_1x_3}$

Exercise: let f be homogenous & $f = \sum g_i f_i$ where the f_i are homogenous. Show that $f = \sum_i \bar{g}_i f_i$ where $\bar{g}_i f_i$ is

homogeneous of degree $\deg f - \deg f_i$.
(Hint: let $\overline{g_i}$ be the homog. component of g_i in degree $\deg f - \deg f_i$)

Theorem (Hilbert's finite gen. of invariants)

Let K be a field of char 0 (e.g. $\mathbb{R}$ or $\mathbb{C}$) & G a finite group acting on $P = K[x_1, \dots, x_n]$ & that the action respects the grading: i.e. $g.- : P \to P$ maps P_d into P_d $\forall d \in \mathbb{N}$.
Then P^G is a fin. gen. K-algebra.

Proof

- Consider the inclusion $i : P^G \hookrightarrow P$ of comm K-algs.
- As this is a ring. hom, we can view P as a P^G-module & $i : P^G \hookrightarrow P$ as a P^G-module map.
- The key is $\exists$ a P^G-module map
  $p : P \longrightarrow P^G$ with $pi = 1$.
  This is the averaging map:
  $$p(a) = \frac{1}{|G|} \sum_{g \in G} g.a$$
  which we will meet again in Maschke's Thm in group representation theory.
- As $g.-$ is ab. group homomorphism, so is the finite sum of such maps, hence so is p.

- To see it is a P^G-module map, let $b \in P^G$.

Then $p(b.a) = \frac{1}{|G|} \sum_g g.(b.a)$ as $g.-$ a K-alg hom.

$$= \frac{1}{|G|} \sum_g (g.b).(g.a) \quad \text{as } b \in P^G$$

$$= \frac{1}{|G|} \sum_g b.(g.a)$$

$$= b.\frac{1}{|G|} \sum_g (g.a) = b.p(a)$$

as required.

- To see $p(a) \in P^G$, let $h \in G$:

$$h.p(a) = h.\frac{1}{|G|} \sum_g g.a \quad \text{as } h.- \text{ K-mod map}$$

$$= \frac{1}{|G|} \sum_g h.(g.a) \quad \text{as } G\text{-action}$$

$$= \frac{1}{|G|} \sum_g (hg).a \quad \text{as elts } hg \text{ run through all elts of } G \text{ ie. } h.- : G \to G \text{ is a bij}^n \text{ of sets.}$$

$$= \frac{1}{|G|} \sum_g g.a$$

$$= p(a).$$

- Finally, let $a \in S^G$ & consider

$$pi(a) = \frac{1}{|G|} \sum_g g.a$$

$$= \frac{1}{|G|} \sum_g a = \frac{1}{|G|} |G| a = a,$$

as required.

Remark: ρ also preserves homog. components of degree d since each g - does & homog. comps of degree closed under k-linear sums.

- Now let $I \subseteq P$ be the ideal generated by homogenous elements of P^G of degree >0:

i.e. elts of form

$$g_1 k_1 + \cdots + g_m k_m, \quad \text{homog elts of degree } >0 \text{ in } P^G,$$

& $g_i \in P$.

- As k is field, it is Noetherian; hence by Hilb. basis thm P is Noetherian. Hence I is finitely generated by finitely many sums as above; hence can choose the generators $f_1, \ldots, f_m$ to be homogenous elts of P^G of degree >0.
- Now let $A \leq P^G$ be the k-subalgebra generated by $f_1, \ldots, f_m$. Will prove each $f \in P^G$ belongs to A.
- It suffices to prove this for homogenous a, since each $f \in P^G$ is a sum of its homogenous components, & these also

belong to P^G (as g.- pres. homog. comps)

- For a homog., argue by induction.
- If f has degree 0, then
$$f = \underset{K}{\underset{\cap}{r}} \cdot 1 \in A \text{ as } A \text{ a } K\text{-alg}.$$

- If $\deg f > 0$, then $f \in I$. Hence
$$f = \sum_{i=1}^{m} g_i . f_i .$$
- From the exercise, can assume g_i is homogenous of degree $\deg f - \deg f_i < \deg f$.
- Then applying ρ, since $f, f_i \in P^G$, & ρ a P^G-module map, we get
$$f = \sum_i \rho(g_i) f_i \quad \text{where } \rho(g_i) \text{ has}$$
degree lower than f.

Hence, by induction, $\rho(g_i) \in A$ & therefore $f \in A$ too. $\square$