Part 2 - Commutative algebra & algebraic geometry

In this section we cover:

- Noetherian modules & rings,
- Hilbert's basis theorem
- k-algebras & commutative k-algebras
- Finitely generated comm k-algebras are quotients of poly rings $k[x_1, \ldots, x_n]$, & so Noetherian if k is.
- An application to invariant theory.
- Galois connection between varieties & ideals.
- Applications of algebra to decomposition results for varieties, using Noetherian property.
- The Nullstellensatz (no proof):
  & points ~ maximal ideals
  irred varieties ~ prime ideals
  varieties ~ radical ideals
- Polynomial maps & the category Var of varieties
- The comm. k-alg $k(A)$ assoc. to a variety A (ie. the co-ordinate ring)
- Functor is fully faithful
- When k alg. closed, equivalence between $(\mathrm{Var})^{op}$ & cat of f.g. reduced comm. k-algebras.

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 ⇒ 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 ⇒ 3)

3 ⇒ 1) Let $N \leq M$ & $\mathcal{F}$ 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. □

Properties of Noetherian modules

① Let M be an R-mod & $N \leq M$. Then M is Noetherian ⇔ 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. ≡ Noeth ≡ 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 $R[x_1, x_2, ----, x_n, ----]$ 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. $\square$

$\boxed{\text{Prop}^n}$ 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 $I = f(f^{-1}I) = f\langle a_1, \dots, a_n \rangle$
$= \langle fa_1, \dots, fa_n \rangle$. $\square$

After break, apply to invariant theory.

k-Algebras & Invariant Theory

- Let R be a comm. ring. An R-algebra 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 commutative 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 monoidal cat $(Mod_R, \otimes_R, R)$ & a monoid in this mon. cat. is an R-alg. / a comm. monoid is a comm. R-alg.

Example) The commutative R-alg. of polynomials $R[x_1,\dots,x_n]$ 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 free commutative R-alg. on set $\{x_1,\dots,x_n\}$.

Exercise: check this!

Def) An R-algebra A is f.g. 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 commutative R-algebra A, this is equiv. to saying that $\exists$ surj. homomorphism
$$R[x_1,\dots,x_n] \twoheadrightarrow A$$
for some n.

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

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

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

Prop^n If R is a comm. Noetherian ring, then each f.g. comm. R-algebra A is a Noetherian ring.

Proof We have surj. hom $R[x_1, \ldots, x_n] \twoheadrightarrow A$. By Hilbert's basis theorem this 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

$$G \longrightarrow k\text{-Alg}(P, P)$$

$$g \longmapsto g.- : P \xrightarrow[k\text{-alg hom}]{} P$$

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 $P^G \overset{i}{\hookrightarrow} P$.

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:

$$f_0 = 1$$

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

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

$$\vdots$$

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

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 it's powers - eg. 3 in above example.

- A poly is homogenous of degree d if all its monomials have degree .

  eg. $x_1 x_2^2 + 4x_1x_2x_3 + 7x_8^3$ 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. $x_1x_2^2 + 7x_4 + 8x_9 + 4x_1x_2x_3 + 1$

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

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

eg (12): $\underset{\substack{\cap \\ P_3}}{x_1x_2^2 + x_1x_2x_3} \longmapsto \underset{\substack{\cap \\ P_3}}{x_2x_1^2 + x_2x_1x_3}$

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 $\bar{g}_i$ 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 (eg. $\mathbb{R}$ or $\mathbb{C}$) & G a finite group acting on $P = K[x_1, \dots, x_n]$ & that the action respects the grading: ie. $g.- : P \to P$ 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.
$$= \frac{1}{|G|}\sum_g (g.b).(g.a)$$
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 $h \in G$:
$$h.p(a) = h.\frac{1}{|G|}\sum_g g.a$$
as $h.-$ K-mod map
$$= \frac{1}{|G|}\sum_g h.(g.a)$$
as G-action
$$= \frac{1}{|G|}\sum_g (hg).a$$
as elts hg run through all elts of G ie. $h.- : G \to G$ is a bij^n 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: p also preserves homog. components of degree d since each g_i 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
  $g_1 k_1 + \cdots + g_m k_m$, homog elts of degree >0 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
  $f = \underset{k}{\overset{\cap}{r}} \cdot 1 \in A$ as A a k-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
  $$f = \sum_i \rho(g_i) f_i$$ where $\rho(g_i)$ has degree lower than f.
  Hence, by induction, $\rho(g_i) \in A$ & therefore $f \in A$ too. $\square$

Lecture 8 - Dictionary between algebra & geometry

- Let K be a field (assumed throughout)
- A poly $f = \sum_{i_1,\dots,i_n \in \mathbb{N}} c_{(i_1,\dots,i_n)} x_1^{i_1} \dots x_n^{i_n} \in K[x_1,\dots,x_n]$

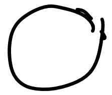
  gives rise to a function

  $f : K^n \longrightarrow K : \bar{a} \longmapsto \sum_{i_1,\dots,i_n \in \mathbb{N}} c_{(i_1,\dots,i_n)} a_1^{i_1} \dots a_n^{i_n}$.
- Given a set $S \subseteq K[x_1,\dots,x_n]$, let

  $V(S) = \{ \bar{a} \in K^n : f(\bar{a}) = 0 \text{ all } f \in S \}$.

  Subsets of this form are called varieties.
- Eg. when $K = \mathbb{R}$,

  $V(x^2+y^2-1) = \{ (a,b) \in \mathbb{R}^2 : a^2+b^2=1 \}$

  $=$  the circle.

  etc.
- Such varieties defined by poly. equations are study of algebraic geometry.
- Given $A \subseteq K^n$,

  define $I(A) = \{ f \in K[x_1,\dots,x_n] : f(a) = 0 \ \forall a \in A \}$.

  Clearly $I(A)$ is an ideal.
- If $S \subseteq T \subseteq K[x_1,\dots,x_n]$ then $V(T) \subseteq V(S)$.
- If $A \subseteq B \subseteq K^n$ then $I(B) \subseteq I(A)$.

  Thus we obtain order reversing functions

$$\begin{tikzcd} \mathrm{Sub}(K^n) \arrow[r, bend left, "I"] \arrow[r, phantom, "\perp"] & \mathrm{Sub}(K[x_1,\dots,x_n])^{op} \arrow[l, bend left, "V"] \end{tikzcd}$$

subsets

of posets, where Sub(X) means poset of subsets of X.

Observe that

$$M \subseteq IA \iff \forall (f\in M, \bar{a}\in A) : f\bar{a} = 0 \iff A \subseteq VM,$$

(or $IA \leq M$ in the opposite) so we have contravariant adjunction of posets as above:

such are called $\sum_{(i_1,\dots,i_n)} X_1^{i_1} \dots X_n^{i_n}$, $i_1,\dots,i_n \in \mathbb{N}$ Galois connections.

This is equally to say

$A \subseteq \underline{VIA}$ $\quad$ $S \subseteq \underline{IVS}$.

- The Galois connection expresses a fundamental duality between geometry (varieties) & algebra (polynomials) & allows us to translate concepts from one to the other.

Lemma

The Function $\mathrm{Sub}(k^n) \xrightarrow{VI} \mathrm{Sub}(k^n)$ sends a subset to the smallest variety containing it. In particular, X is a fixpoint for VI ($X = VIX$) if and only if X is a variety.

Proof

Certainly $X \subseteq VIX$. If $X \subseteq VY$ then, by Gal. conn., $Y \subseteq IX$ so that $VIX \subseteq VY$, as required. This proves the first claim, & second is triv. consequence.

Remark

In fact, $\mathrm{Sub}(k^n) \xrightarrow{VI} \mathrm{Sub}(k^n)$ is a closure operator in sense of topology: so there is a topology on k^n whose closed sets are precisely the varieties. This is the Zariski topology - not explored further here.

Applications of algebra to geometry

Here is a first small application.

Prop

Each variety is equal to $V(S)$ for S a finite set of polynomials.

Proof $V(S) = VIV(S)$.

Since k is a field, by Hilbert's basis thm, $k[x_1,..,x_n]$ is Noetherian. Hence

$IV(S) = \langle f_1,...,f_n \rangle$ so

$V(S) = V\langle f_1,...,f_n \rangle = V\{f_1,...,f_n\}$. □

Prop (dual Noetherian property)

Each sequence $\ldots A_{n+1} \subseteq A_n \ldots \subseteq A_1 \subseteq A$ of varieties stabilises.

Proof: Firstly observe that if A, B are varieties, then $A \subseteq B \iff IB \subseteq IA$. $\Rightarrow)$ we know already. For $\Leftarrow$ if $IB \subseteq IA$ then $A = VIA \subseteq VIB = B$.

Therefore, to prove the sequence stabilises is equivalently to prove $IA \subseteq IA_1 \subseteq IA_2 \subseteq \ldots\ldots$ stabilises.

Since k is a field, by Hilbert's basis thm, $k[x_1,..,x_n]$ is Noetherian so the sequence stabilises. □

Irreducibility & decompositions

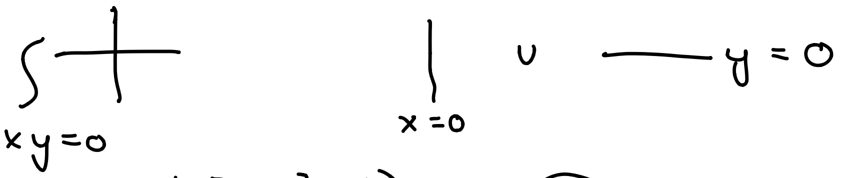
Firstly : geometry.

Def^n) - A variety A is reducible if $A = B \cup C$ where B, C are proper subvarieties (ie. proper subsets that are also varieties)

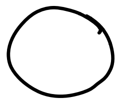
- It is irreducible if it is not reducible.

Examples ($K = \mathbb{R}$)

$V(xy) = V(x) \cup V(y)$ so $V(xy)$ is reducible.



$V(x), V(y)$ are irreducible.

$V(x^2+y^2-1) =$  is irreducible.

Now : algebra

Def^n) An ideal A is reducible if $A = B \cap C$ where B, C are ideals & $A \subset B, C$.
Otherwise A is irreducible.

Example : In $\mathbb{Z}$, $(6) = (2) \cap (3)$.
Irreducibles are (p^n) for p a prime.

Theorem

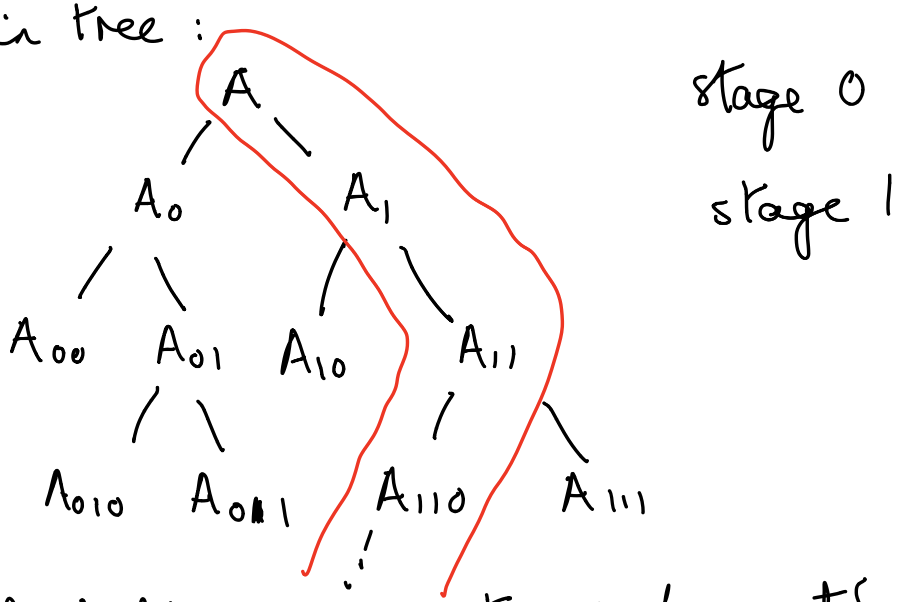
Each variety A is of form $A_1 \cup \dots \cup A_m$ for $A_1, \dots, A_m$ irreducible.

Proof

- We construct a tree with root A.
- Each node N is a variety with 0 or 2 children :
- if N is irreducible it has no children;
- if N is reducible, choose $N = N_0 \cup N_1$ with $N_0, N_1 \subset N$

proper subvarieties & define these to be children. We obtain tree :

eg.



& by dual Noetherian property each path down the tree from root to a leaf is finite; A is the union of the leaves of tree, each of which is irreducible. □

Remark) In fact, if we eliminate any A_i in $A_1 \cap \dots \cap A_m$ st $A_i \subseteq A_j$ another j; then expression is unique up to reordering. (Exercise!)

- We can give a similar argument on the algebra side, but here is a more compact one.

Theorem) For a comm. Noetherian ring R, each ideal is a finite intersection of irreducibles.

Proof let J be set of ideals not admitting such a decomposition. Assume it is non-empty. Then, by char. of Noetherian rings, J has a max^l element A. Clearly A is not irreducible. Hence $A = B \cap C$ for $A \subset B, C$ but then by maximality of $A \in J$, B, C are finite intersection of irreducibles; hence so is A. Contradiction. $\square$

Remark) A full understanding of such decompositions is the topic of primary decomposition.

Maximal & prime ideals

Def^n) let R a comm. ring. An ideal $I \subseteq R$ is

- proper if $0 \subset I \subset R$
- maximal if proper & $\nexists$ ideal $I \subset J \subset R$.
- prime if proper & $ab \in I \Rightarrow a \in I$ or $b \in I$.
- radical if $a^n \in I \Longrightarrow a \in I$.

Proposition

A proper ideal $I \subset R$ is

- max^l $\Leftrightarrow$ R/I a field
- prime $\Leftrightarrow$ R/I is an integral domain ($ab = 0 \Rightarrow a = 0$ or $b = 0$)
- radical $\Leftrightarrow$ R/I is reduced ($x^n = 0$ some $n \Rightarrow x = 0$)

Proof

- A comm. ring R is a field $\Leftrightarrow$ all non-zero elts are invertible $\Leftrightarrow$ only ideals are (0) & (1).

- Now ideals $J \leq R/I$ are in 1-1 correspondence with ideals $I \leq \overline{J} \leq R$. Therefore, if R/I is a field, there are just two ideals between I & R, namely I & R themselves $\Leftrightarrow$ I is max^l.

- To say R/I is integral domain is to say $(a+I)(b+I) = I \Rightarrow a+I = I$ or $b+I = I$. Since $(a+I)(b+I) = ab + I$, this says $ab \in I \Rightarrow a \in I$ or $b \in I$, ie. I is prime.

- Radical similar to prime case. □

Corollary

Maximal $\Rightarrow$ Prime $\Rightarrow$ Radical.

Proof

- By prev. prop., must show field $\Rightarrow$ integral domain $\Rightarrow$ reduced.
- Clearly integral dom. $\Rightarrow$ reduced. If a field, suppose $ab = 0$ but $a, b \neq 0$. Then $b = a^{-1}ab = a^{-1}0 = 0$ - a contradiction. □

The Nullstellensatz (Hilbert)

Def^n) For R comm., I an ideal of R, define Rad(I) = $\{x \in R : x^n \in I \text{ some } n \in \mathbb{N}\}$.

Exercise : show that Rad(I) is an ideal, and indeed a radical ideal.

- Assuming k is a field (or even just a reduced ring)

then $I(A) = \{f : f(a) = 0 \text{ all } a \in A\}$ is radical since if $f(a)^n = 0$ then $f(a) = 0$.

Hilbert's Nullstellensatz (Famous result)

If k is an algebraically closed field

$$\mathrm{Sub}(k[x_1,\dots,x_n]) \xrightarrow{IV} \mathrm{Sub}(k[x_1,\dots,x_n])$$

satisfies $IV(S) = \mathrm{Rad}\langle S\rangle$.

- we won't prove this!

Hilbert's Nullstellensatz (main version)

The Galois connection

$$\begin{tikzcd}
\mathrm{Sub}(k^n) \arrow[r, shift left, "I"] \arrow[r, phantom, "\perp"] & \mathrm{Sub}(k[x_1,\dots,x_n])^{op} \arrow[l, shift left, "V"]
\end{tikzcd}$$

restricts to an iso of posets

$$\begin{tikzcd}\text{Varieties} \arrow[r, shift left=2, "I"] \arrow[r, phantom, "\perp"] & (\text{Radical Ideals})^{op} \arrow[l, shift left=2, "V"]\end{tikzcd}$$

between varieties & radical ideals.

Proof - We've seen IV-fixpoints are precisely the varieties.

- Certainly each IA is radical, and if M is radical, then $M = \mathrm{Rad}(\langle M \rangle) = IV(M)$ by Nullstellensatz. Hence radicals are precisely the IV-fixpoints.
- Like any Galois connection, the above restricts to a bij^n between fixpoints on either side. $\square$

Theorem

Under the above correspondence

$$\begin{tikzcd}\text{Varieties} \arrow[r, shift left=2, "I"] \arrow[r, phantom, "\perp"] & (\text{Radical Ideals})^{op} \arrow[l, shift left=2, "V"]\end{tikzcd}$$

we have a correspondence between

- points of K^n $\equiv$ maximal ideals

and

- non-empty irreducible varieties $\equiv$ prime ideals.

Proof

- Clearly each point $\bar{a} = (a_1, \ldots, a_n) \in k^n$ is a variety since it is
$$V\{x_1 - a_1, \ldots\ldots, x_n - a_n\}.$$
Indeed, $I(\bar{a}) = \langle x_1 - a_1, \ldots\ldots, x_n - a_n \rangle$ & this is a maximal ideal.

To see maximality, suppose
$$I(\bar{a}) \subset J \subset k[x_1, \ldots, x_n]. \text{ Then}$$
$$I(\bar{a}) \subset J \subseteq Rad(J) \subset k[x_1, \ldots, x_n] \text{ so}$$
$$\phi \subset V(Rad(J))] \subset VI(\bar{a}) = \{a\}$$
by order-rev. bij between varieties & radicals, and this is impossible.

- Suppose $0 \subset M \subset k[x_1, \ldots, x_n]$ is max^l; then this gives
$$\phi \subset V(M) \subset k^n.$$
If $V(M)$ contained two points $\bar{a}, \bar{b}$, then
$$VI(\bar{a}) = \{\bar{a}\} \subset V(M) \text{ so } M \subset I(\bar{a})$$
contradicting maximality of M.

- For second part, will show
A irreducible $\Leftrightarrow$ $I(A)$ is prime.

- Suppose I is not prime, so $\exists f_1, f_2 \notin I(A)$ st $f_1 f_2 \in I(A)$. Consider varieties
$$A_1 = V(IA \cup \{f_1\}), \quad A_2 = V(IA \cup \{f_2\}).$$
Since f_1, f_2 don't vanish on A,

$A_1, A_2 \subset A$. However as $f_1 f_2 \in I(A)$, $f_1(a) f_2(a) = 0$ all $a \in A$ so $\forall a \in A$ $f_1(a) = 0$ or $f_2(a) = 0$; hence $A_1 \cup A_2 = A \Rightarrow$ A is reducible.

Conversely, suppose $A = A_1 \cup A_2$ prop. subvarieties.
So $I(A) \subset I(A_1), I(A_2)$.
Choose $f_j \in I(A_j) / I(A)$ for $j = 1, 2$.
Then $f_1 f_2(a) = 0$ all $a \in A = A_1 \cup A_2$
so $f \in I(A) \Rightarrow I(A)$ not a prime ideal.

$\square$

Lecture 9 - Varieties & commutative algebras

last time : varieties vs ideals of poly. rings

varieties & maps of varieties vs commutative k-algs

Def^n) Let k be a field & $A \leq k^n$ & $B \leq k^\ell$ be varieties. A polynomial map $f : A \to B$ is a function such that $\exists$ polys $f_1, \ldots, f_\ell \in k[x_1, \ldots, x_n]$ with $\forall a \in A$ $f(a) = (f_1(a), \ldots, f_\ell(a))$.

Prop^n] Varieties & polynomial maps form a category Var.

Proof) Consider

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "g"] & C \\ k^\ell \arrow[u, phantom, sloped, "\subseteq"] & k^n \arrow[u, phantom, sloped, "\subseteq"] & k^m \arrow[u, phantom, sloped, "\subseteq"] \end{tikzcd}$$

rep. by polynomials $(f_1, \ldots, f_n)$ & $(g_1, \ldots, g_m)$: then gf is represented by polys $h_1, \ldots, h_m$ where

$$h_i(x_1, \ldots, x_\ell) = g_i(f_1(x_1, \ldots, x_\ell), \ldots, f_n(x_1, \ldots, x_\ell)).$$

The identity

$$\begin{tikzcd} A \arrow[r, "id"] & A \\ k^n \arrow[u, phantom, sloped, "\subseteq"] & k^n \arrow[u, phantom, sloped, "\subseteq"] \end{tikzcd}$$

is polynomial since rep. by $(x_1, \ldots, x_n)$.

Clearly associative & unital since just function composition. □

Def) For A a variety, the co-ordinate ring $k(A) = \mathrm{Var}(A, k)$ is a commutative k-algebra whose elements are polynomial maps $A \to k$ with operations pointwise as in k:

- $f+g\,(a) = f(a)+g(a)$
- $f.g\,(a) = f(a).g(a)$
- $\lambda f\,(a) = \lambda . f(a)$.

- $K(A)$ can also be described more algebraically.

Proposition

There is an iso of k-algebras

$$k[x_1,\dots,x_n]/I(A) \cong K(A)$$

where $I(A)$ is ideal of polys vanishing at A.

~~Proof~~ The function $k[x_1,\dots,x_n] \to K(A)$

$$f \longmapsto A \hookrightarrow k^n \xrightarrow{f} k$$

is a surjective k-algebra homomorphism & its kernel consists exactly of $I(A)$.

Hence we obtain iso, by first iso thm, $k[x_1,\dots,x_n]/I(A) \cong K[A]$.

□

Properties: ① As k is a field, $k[x_1,\dots,x_n]$

is Noetherian ; hence so is quotient $k[A]$.

② As $I(A)$ is radical, the quotient $k[A]$ is reduced: (ie. $f^n=0 \Rightarrow f=0$).

③ The comm. k-alg $k[x_1,\dots,x_n]$ is freely generated by $x_1,\dots,x_n$; therefore $k(A)$ is generated by the image of thes under

$$\begin{aligned} k[x_1,\dots,x_n] &\twoheadrightarrow K(A) \; : \\ x_i &\longmapsto p_i : A \hookrightarrow k^n \xrightarrow{x_i} K \\ & \qquad\quad a=(a_1,\dots,a_n) \longmapsto a_i \; ; \end{aligned}$$

ie. $K(A)$ is finitely generated by the n projections $p_i : A \longrightarrow k$.

- Given a morphism $f : A \longrightarrow B \in Var$ we obtain

$$\begin{aligned} K(B) = Var(B,K) &\xrightarrow{f^*} Var(A,K) = K(A) \\ B \xrightarrow{g} K &\longmapsto A \xrightarrow{f} B \xrightarrow{g} K \end{aligned}$$

which is a k-algebra homomorphism since operations are component-wise as in k.

-This makes $K(-) : Var^{op} \longrightarrow Comm\text{-}k\text{-}Alg$ a functor.

Theorem

$K(-) : \mathrm{Var}^{op} \longrightarrow \text{Comm-}k\text{-Alg}$ is fully faithful.

(ie. given $K(A) \xrightarrow{\alpha} K(B) \in \text{Comm.}k\text{-Alg}$ $\exists !\ B \xrightarrow{f} A \in \mathrm{Var}$ st $\alpha = f^*$.)

Proof

- Firstly, we show faithfulness:

consider

$$\begin{tikzcd} A \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] \arrow[d, phantom, sloped, "\subseteq"] & B \arrow[d, phantom, sloped, "\subseteq"] & \in \mathrm{Var} \\ k^n & k^m & \end{tikzcd}$$

& suppose

$$\begin{tikzcd} K(B) \arrow[r, shift left, "f^*"] \arrow[r, shift right, "g^*"'] \arrow[r, phantom, "="] & K(A) \end{tikzcd}$$

. Must show $f = g$.

- So given $B \xrightarrow{h} k$ we have $f^* h = g^* h$, ie. $hf = hg$.
- In partic, consider $p_i : B \longrightarrow k$, $a \longmapsto a_i$ for $i \in \{1, \ldots, m\}$
- Then $p_i f(a) = f_i(a)$ where $f(a) = (f_1(a), \ldots, f_n(a))$.
- Therefore $p_i f = p_i g$ all i says
  $f_i(a) = g_i(a)$ all i so
  $f(a) = g(a)$ all $a \in B$; hence $f = g$.

- For fullness, consider $\alpha : K(B) \longrightarrow K(A)$.

We must find f such that $\alpha = f^*$, but then $\alpha(p_i) = f^*(p_i) = p_i \circ f$.

Therefore, we must define f by

$F(a) = (\alpha(p_1)a, -----, \alpha(p_m)a)$.

Certainly this is polynomial since each $\alpha(p_i) \in K(A)$ is polynomial map.

It remains to show that if $a \in A$ then $fa \in B$:
indeed, suppose $B = V(g_1, ----, g_r) =$

$$\{b \in k^m : g_i b = 0 \text{ all } i \in \{1, .., r\}\}.$$

- We must show $g_i f(a) = 0$ all $a \in A$:

ie. $g_i F(a) = g_i(\alpha(p_1)a, -----, \alpha(p_m)a)$

$$= (g_i\alpha(p_1)a, ..., g_i\alpha(p_m)a) = 0 \text{ all } a \in A.$$

- This is equally to say

$$g_i(\alpha(p_1), ..., \alpha(p_m)) = 0 \text{ in } K(A)$$

- But as $\alpha : K(B) \longrightarrow K(A)$ is a homomorphism of k-algebras, we have this equals

$$\alpha(g_i(p_1, -------, p_m)) \quad \text{so it suff.}$$

to show $g_i(p_1, ---, p_m) = 0 \in K(B)$.

- But this is precisely to show

$$g_i(p_1(b), ..., p_m(b)) = 0 \text{ all } b \in B$$

$$\parallel$$

$$g_i(b_1, ..., b_m) \quad \text{where } b = (b_1, ---, b_m)$$

& this is zero by assumption : ie. $B = V\{g_1, ---, g_r\}$.

□

Corollary

Two varieties A & B are iso $\Longleftrightarrow$ $K(A)$ & $K(B)$ are iso as comm. k-algebras.

Proof : (Exercise : Fully faithful functor reflects isos.)

Corollary

- If k is algebraically closed, then a comm. k-algebra S is iso to some $K(A)$ $\Leftrightarrow$ S is a finitely gen. reduced k-alg.

Proof

- Certainly $k[A]$ is reduced, as we have seen & f.g.
- Conversely suppose S is f.g. reduced. As f.g., have surj. alg. hom.

$$k[x_1, \dots, x_n] \xrightarrow{p} S$$

whose kernel $\ker(p)$ is radical since

$$S \cong k[x_1, \dots, x_n]/\ker(p)$$

is reduced, Hence by the Nullstellensatz,

$$\ker(p) = IV\ker(p);$$

so

$$S \cong k[x_1, \dots, x_n]/IV\ker(p) = k(V\ker p).$$

□

Remark : Therefore we have a fully faithful

Functor $\mathrm{Var}^{op} \xrightarrow{k(-)}$ Red-Comm-k-Alg which if k is algebraically closed is essentially surjective (surj. up to iso): in other words, for k alg. closed we have an equivalence of categories

$$\mathrm{Var}^{op} \xrightarrow{k(-)} \text{Red-Comm-}k\text{-Alg}\,.$$