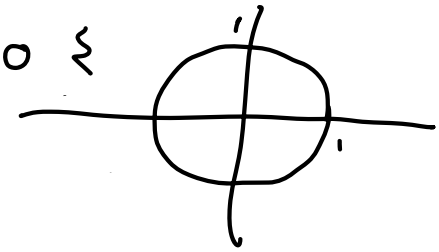
L8 - The dictionary between algebra & geometry

- Let k be a Field.
- Polynomial $f = \sum m_{(i_1,\dots,i_n)} x_1^{i_1} \cdots x_n^{i_n} \in k[x_1,\dots,x_n]$ gives rise to gives rise to function $f : k^n \to k : \bar{a} \mapsto \sum m_{(i_1,\dots,i_n)} a_1^{i_1} \cdots a_n^{i_n}$ & so we can investigate its zeroes : those $\bar{a} \in k^n$ at which $f(\bar{a}) = 0$.
- Given a set S of polys in $k[x_1,\dots,x_n]$, let $V(S) = \{ \bar{a} \in k^n : f(\bar{a}) = 0 \ \forall f \in S \}$.

Subsets of this form are called varieties

Eg. When $k = \mathbb{R}$,

$V(x^2+y^2-1) = \{(a,b) : a^2+b^2-1 = 0\}$



Such varieties defined by poly. equations are the study of algebraic geometry.

- On the other hand, given a subset $A \subseteq k^n$, let $I(A) = \{ f \in k[x_1,\dots,x_n] : f(\bar{a}) = 0 \text{ all } \bar{a} \in A \}$.

Clearly $I(A)$ is an ideal.

- If $S \subseteq T$ then $V(T) \subseteq V(S)$ & if $A \subseteq B$ then $I(B) \subseteq I(A)$;

thus we obtain order reversing functions

$$\mathrm{Sub}(k^n) \underset{V}{\overset{I}{\rightleftarrows}} \mathrm{Sub}(k[x_1,\dots,x_n])^{op}$$

of posets, where $\mathrm{Sub}(X)$ is the poset of subsets of X. Observe that

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

$\iff A \subseteq VM$, so we have an adjunction of posets as above:

such relationships between posets are called Galois connections.

This is equally to say $A \subseteq VI(A)$ & $S \subseteq IV(S)$.

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

Lemma The function

$$\mathrm{Sub}(k^n) \xrightarrow{\mathbb{V}\mathbb{I} = \overline{(-)}} \mathrm{Sub}(k^n)$$

sends a subset X to the smallest variety containing it. In particular, X is a fixpoint for $\mathbb{V}\mathbb{I}$ (i.e. $\mathbb{V}\mathbb{I}X = X$) iff X is a variety.

Proof - Certainly $X \subseteq \mathbb{V}\mathbb{I}X$.

If $X \subseteq \mathbb{V}Y$ then, by adjointness, $Y \subseteq \mathbb{I}X$ so that $\mathbb{V}\mathbb{I}X \subseteq \mathbb{V}Y$.

- This proves the first claim & the second follows immediately.

Remark: The function

$$\mathrm{Sub}(k^n) \xrightarrow{\mathbb{V}\mathbb{I} = \overline{(-)}} \mathrm{Sub}(k^n)$$

is a closure operator in the sense of topology; therefore there is a topology on k^n whose closed sets are precisely the varieties: this is called the Zariski topology.

- We won't explore it further here.

Applications of algebra to geometry

Proposition (dual Noetherian prop.)
Each sequence $\dots A_{n+1} \subseteq A_n \subseteq \dots \subseteq A_1 \subseteq A$ of varieties stabilises.

Proof

- Firstly, observe that for varieties A, B we have $A \subseteq B \iff \mathbb{I}B \subseteq \mathbb{I}A$. The $\Rightarrow$) we know.
Suppose $\mathbb{I}B \subseteq \mathbb{I}A$. Then $A = V\mathbb{I}A \subseteq V\mathbb{I}B = B$ since varieties are fixpoints, as required.
- Therefore, to prove the sequence stabilises is equivalent to showing
$\mathbb{I}A \subseteq \mathbb{I}A_1 \subseteq \dots \subseteq \mathbb{I}A_n \subseteq \dots$
stabilises, & this is true since by the Hilbert basis theorem, $k[x_1, \dots, x_n]$ is Noetherian. $\square$

Here is a small application of algebra to geometry:

Proposition

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

Proof

$V(S) = V \mathcal{I} V(S)$ but by Hilbert basis theorem $k[x_1, \ldots, x_n]$ is Noetherian.

Therefore $\mathcal{I} V(S) = \langle f_1, \ldots, f_n \rangle$

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

□

Irreducibility & decompositions

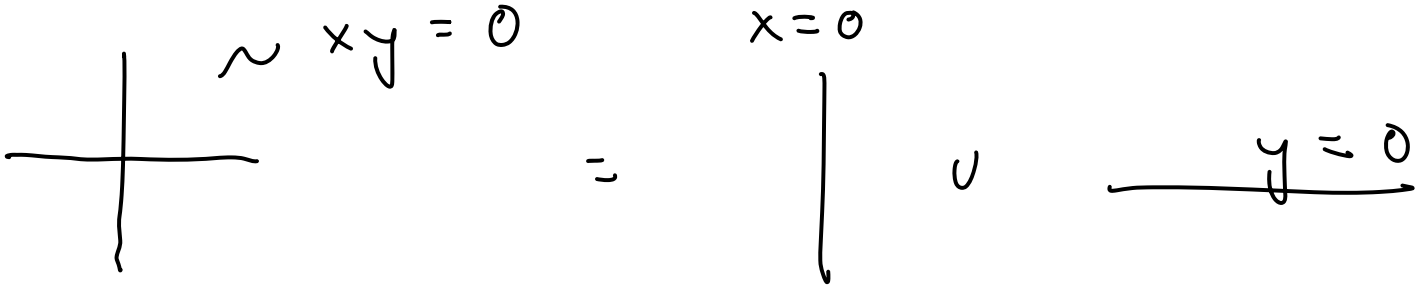
- Firstly, on the geometry side:

Def^n - A variety A is reducible if it can be written as $A = B \cup C$ where B, C are varieties that are proper subsets of A (aka subvarieties)

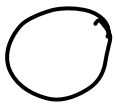
- A variety is irreducible if it is not reducible.

Example ($k = \mathbb{R}$)

- $Z(xy) = Z(x) \cup Z(y)$



so $Z(xy)$ is reducible.

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

- On the algebra side :

Def) An ideal I is reducible if $\exists$ ideals $I \subset A, B$ such that $I = A \cap B$.
Otherwise I 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

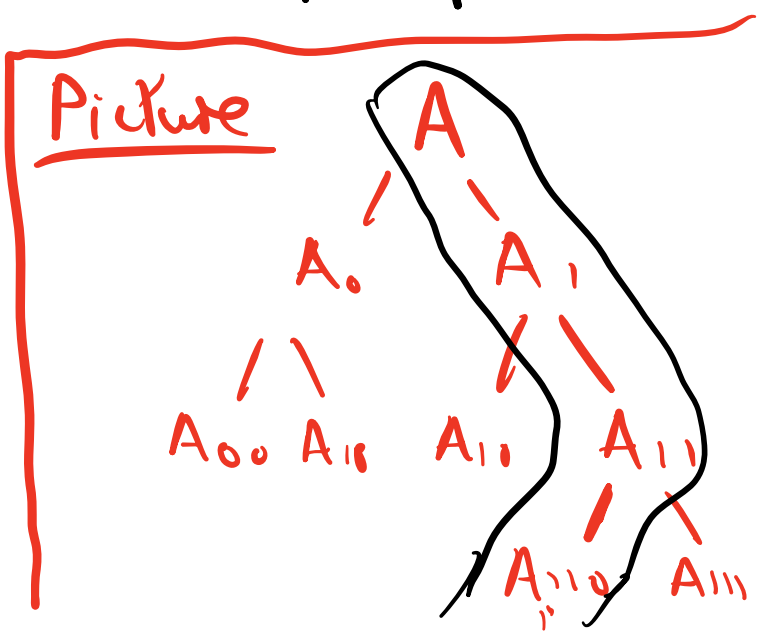
- Let W be the set of varieties not of this form.
- Suppose $A \in W$. Then A not irreducible.
- So $A = A_0 \cup A_1$ with $A_0, A_1 \subset A$ varieties.
- Since $A \in W$, either $A_0 \in W$ or $A_1 \in W$.
- Wlog assume $A_1 \in W$.
- Now repeat argument to get

$$\dots\dots \subset A_2 \subset A_1 \subset A$$

which does not stabilise.

- Contradicts dual Noeth. prop.
- Hence $W = \emptyset$.

Picture



Algebra side

- We can give a similar argument on the algebra side, as in the exercise class.
- Here is another compact one.

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

Proof Let J be the set of ideals not admitting such a decomposition. Assume it is non-empty. Since R is Noetherian, it has a max^{l} elt A (recall char. of Noetherian rings).

Clearly A is not irreducible; so $A = B \cap C$ for $A \subset B, C$ but then B, C admit such a **decomposition**, **whence so does A**.

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

Flavours of ideal

Let R be a commutative ring. An ideal $I \subseteq R$ is

- proper if $I \subset R$
- maximal if proper & there is no ideal $I \subset J \subset R$
- prime if proper & $ab \in I \Rightarrow a \in I$ or $b \in I$.
- radical if $a^n \in I \Rightarrow a \in I$.

Proposition

A proper ideal $I \subset R$ is:

① maximal $\Leftrightarrow$ R/I is a Field

② prime $\Leftrightarrow$ R/I is an integral domain ($ab=0 \Rightarrow a=0$ or $b=0$)

③ radical $\Leftrightarrow$ R/I is reduced ($a^n=0 \Rightarrow a=0$).

Proof ① R/I is a Field $\Leftrightarrow$ only ideals are (0) & (1).

- Now ideals J in R/I are in 1-1 correspondence with ideals $I \subseteq \bar{J} \subseteq R$.

Therefore, R/I has just (0) & (1) as ideals $\Leftrightarrow$ any such $\bar{J} = I$ or R - ie. I is maximal.

② To say R/I an integral domain (no zero divisors)

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 $b \in I$, as required.

③ Similar to ②.

Corollary

Maximal $\Rightarrow$ prime $\Rightarrow$ radical.

Proof / • If I is maximal, R/I a Field.

If $ab = 0 \in R/I$ for $a, b \neq 0$, then $a^{-1}ab = b = 0$.

Contradiction. Hence R/I integral domain $\Rightarrow$ I prime.

• If I prime, R/I integral domain $\Rightarrow$ R/I reduced $\Rightarrow$ I radical.

Def^) Let I be an ideal. Let $\mathrm{Rad}(I) = \{a \in R : a^n \in I \text{ some } n \in \mathbb{N}\}$

Lemma) $\mathrm{Rad}(I)$ is a radical ideal, the smallest radical ideal containing I.

Proof) The only non-trivial bit to check is that $\mathrm{Rad}(I)$ is an ideal.

- Let $a, b \in \mathrm{Rad}(I)$. Then $a^n, b^m \in I$ some m, n

Then $(a+b)^{n+m-1}$ (binomial expansion)

$$= \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} a^i b^{n+m-1-i}$$

For each i, $i \geq n$ or $n+m-1-i \geq m$ so each terms has exponent $a^i \in I$ or $b^{n+m-1-i} \in I \Rightarrow$

$(a+b)^{n+m-1} \in I$.

- If $a^n \in I$, $(\lambda a)^n = \lambda^n a^n \in I \Rightarrow \lambda a \in \mathrm{Rad}(I)$.

□

Remark

If K is a field, then

$I(A) = \{f : f(a) = 0 \text{ all } a \in A\}$

is radical since if $f(a)^n = 0$ then $f(a) = 0$ as K has no zero divisors.

Hilbert's Nullstellensatz

If k is algebraically closed field (eg. $\mathbb{C}$) then $IZ(S) = Rad(\langle S \rangle)$, where $\langle S \rangle$ is the ideal generated by S.

We will not prove it. It implies

Nullstellensatz Main

For k alg. closed, the Galois connection

$$Sub(k^n) \underset{V}{\overset{I}{\underset{\longleftarrow}{\overset{\longrightarrow}{}}}} Sub(k[x_1, \ldots, x_n])^{op}$$

restricts to an iso of posets

$$Var^{op} \underset{I}{\overset{Z}{\underset{\longrightarrow}{\overset{\longleftarrow}{}}}} Rad$$

between varieties & radical ideals.

Proof

- we've seen IV-fixed points are the varieties.
- Also IA is radical, and if M is radical

  $M = Rad(\langle M \rangle) = IZ(M)$ by Nullstellensatz

  so M a fixpoint. In particular IZ-fixpoints $\equiv$ radicals. $\square$

Theorem Under the correspondence

$$\text{Var}^{\text{op}} \underset{I}{\overset{Z}{\rightleftarrows}} \text{Rad}$$

points of k^n $\equiv$ maximal ideals

and

non-empty irreducible varieties $\equiv$ prime ideals

Proof Clearly each point $\bar{a} = (a_1, \ldots, a_n)$ is a variety since it is the set of sol^{n}s of the polys $\{x_1 - a_1, \ldots, x_n - a_n\}$.

Indeed, $I(\bar{a}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ a maximal ideal (exercise)

Conversely, if M is a maximal ideal $0 \subset M \subset k[x_1, \ldots, x_n]$;
then applying the order rev. bij^n Z gives
$\phi \subset Z(M) \subset k^n$.

- If $Z(M)$ contained two points $\bar{a}, \bar{b}$ or more then $ZI(\bar{a}) = \{\bar{a}\} \subset Z(M)$ so $M \subset I(\bar{a})$ contradicting maximality of M;
hence $Z(M)$ is a single point.

• For the second part, we will show

A is irreducible $\iff$ $I(A)$ is prime.

- Suppose $I(A)$ not prime, so $\exists f_1, f_2 \notin I(A)$ s.t. $f_1 f_2 \in I(A)$. Consider the alg sets $A_1 = Z(I(A) \cup \{f_1\})$ & $A_2 = Z(I(A) \cup \{f_2\})$.

Since f_1, f_2 don't vanish on A, $A_1, A_2 \subset A$ are proper subsets.

On the other hand, as $f_1 f_2 \in I(A)$ then $f_1(a) f_2(a) = 0$ 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 $A = A_1 \cup A_2$ proper alg. subsets.

So $I(A) \subset I(A_1), I(A_2)$.

(Indeed, if $I(A_j) = I(A)$ then $A = VI(A) = V(I(A_j)) = A_j$)

- Choose $f_1 \in I(A_1) \setminus I(A)$ & $f_2 \in I(A_2) \setminus I(A)$.

Then $f_1 f_2(a) = 0$ all $a \in A = A_1 \cup A_2$ so $f_1 f_2 \in I(A)$

$\Rightarrow I(A)$ not a prime ideal.

□

Co-ordinate rings

Def^n) Let k be a field & $A \subseteq k^n$ & $B \subseteq k^\ell$ 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 $A \xrightarrow{f} B \xrightarrow{g} C$ with $A \subseteq k^\ell$, $B \subseteq k^n$, $C \subseteq k^m$

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 $A \xrightarrow{id} A$ with $A \subseteq k^n$ is polynomial since rep. by $(x_1, \ldots, x_n)$.

Clearly associative & unital since just function composition. $\square$

Def) For A a variety, the co-ordinate ring $K(A) = Var(A, k)$ is a commutative k-algebra whose elements are polynomial maps $A \longrightarrow k$ 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 $k[x_1, \ldots, x_n]/I(A) \cong K(A)$ where $I(A)$ is ideal of polys vanishing at A.

Proof

The function $k[x_1, \ldots, x_n] \twoheadrightarrow K(A)$

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

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

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

Properties: ① As k is a field, $k[x_1, \ldots, x_n]$ is Noetherian; hence so is quotient $I(A) = \langle f_1, \ldots, f_n \rangle$ & $K(A)$ is **finitely generated**.

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

In Fact,

Theorem

If k is algebraically closed a commutative k-alg X is isomorphic to some $k[A]$ for A an algebraic set $\Leftrightarrow$ X is finitely generated & reduced.

Proof $k[A]$ is reduced & f.g.

- Conversely suppose S is f.g. reduced. As f.g., have surj. alg. hom.

$$k[x_1, \ldots, x_n] \xrightarrow{\rho} S$$

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

$$S \cong k[x_1, \ldots, x_n]/\ker(\rho)$$

is reduced, Hence by the Nullstellensatz,

$$\ker(\rho) = I V \ker(\rho);$$

so $S \cong k[x_1, \ldots, x_n]/I V \ker(\rho) = k(V\ker\rho)$. □

In fact, there is equiv of categories between Var & cat of f.g reduced comm k-algs.