Lecture 8 - Dictionary between algebra & geometry

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

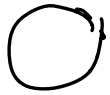
  gives rise to a function

  $f: K^n \longrightarrow K : \bar{a} \longmapsto \sum_{i_1,\dots,i_n \in \mathbb{N}} c_{(i_1,\dots,i_n)} a_1^{i_1} \cdots a_n^{i_n}$.
- 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

$$\underset{\text{subsets}}{\text{Subs}(K^n)} \underset{V}{\overset{I}{\rightleftarrows}} \text{Subs}(K[x_1,\dots,x_n])$$

of posets, where $\mathrm{Sub}(X)$ means poset of subsets of X.

Observe that

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

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

such are called Galois connections.

This is equally to say

$A \subseteq VIA$ $\quad S \subseteq IVS$.

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

Proof

Certainly $X \subseteq VIX$. If $X \subseteq V4$ then, by Gal. corr., $4 \subseteq IX$ so that $VIX \subseteq V4$, as required. This proves the first claim, & second is triv. consequence.

Remark

In fact, $Sub(k^n) \xrightarrow{VI} Sub(k^n)$ 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 $V(S) = V(IV(S))$.

Since k is a field, by Hilbert's basis thm, $k[x_1,\dots,x_n]$ is Noetherian. Hence $IV(S) = \langle f_1,\dots,f_n\rangle$ so

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

Prop (dual Noetherian property)

Each sequence $\dots A_{n+1} \subseteq A_n \dots \subseteq A_1 \subseteq A$ 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 $IA \subseteq IA_1 \subseteq IA_2 \subseteq \dots$ stabilises.

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

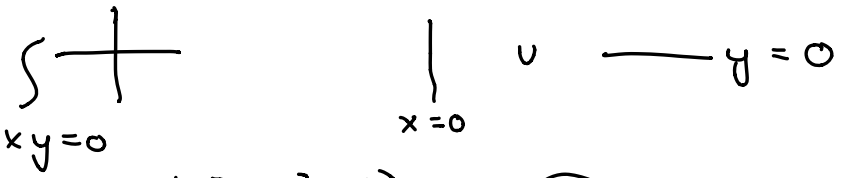
Irreducibility & decompositions

Firstly : geometry.

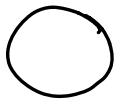
Def^n) - A variety A is reducible if $A = B \cup C$ where B, C are proper subvarieties (i.e. proper subsets that are also varieties)
- it is irreducible if it is not reducible.

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

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



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

$U(x^2+y^2-1) =$  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 $\mathbb{Z}$, $(0) = (2) \cap (3)$.
Irreducibles are (p^n) for p a prime.

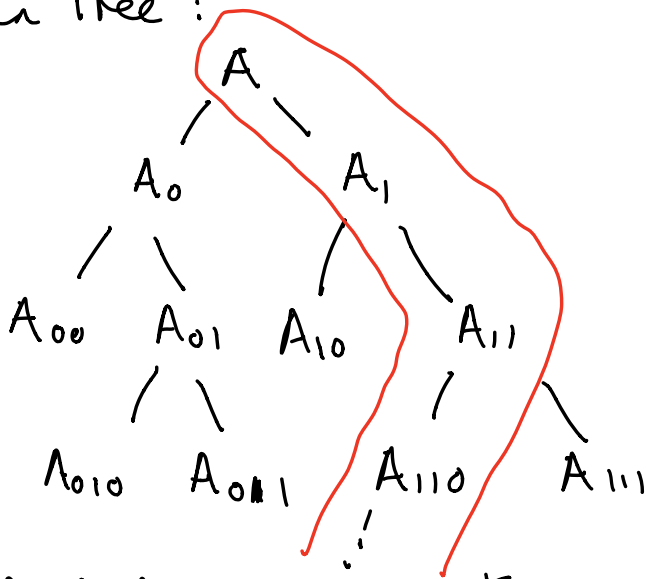
Theorem

Each variety A is of form $A_1 \cup \ldots \cup A_m$ for $A_1, \ldots, A_m$ 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 $A_{i_1} \cap \dots \cap A_{i_m}$ 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 $\mathcal{J}$ be set of ideals not admitting such a decomposition. Assume it is non-empty. Then, by char. of Noetherian rings, $\mathcal{J}$ 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 $A \in \mathcal{J}$, B, C are finite intersection of irreducibles; hence so is A. Contradiction. $\square$

Remark) A full understanding of such decomposition 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 $a^n \in I \Rightarrow a \in I$.

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 $b \in I$, i.e. 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 $\mathrm{Rad}(I) = \{x \in R : x^n \in I \text{ some } n \in \mathbb{N}\}$.

Exercise: show that $\mathrm{Rad}(I)$ 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

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

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

- we won't prove this!

Hilbert's Nullstellensatz (main version)

The Galois connection

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

restricts to an iso of posets

$$\text{Varieties} \underset{V}{\overset{I}{\rightleftarrows}} (\text{Radical Ideals})^{op}$$

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 $M = \text{Rad}(\langle M \rangle) = IV(M)$ by Nullstellensatz. Hence radicals are precisely the IV-fixpoints.
- Like any Galois connection, the above restricts to a bijⁿ between fixpoints on either side. □

Theorem
Under the above correspondence

$$\text{Varieties} \underset{V}{\overset{I}{\rightleftarrows}} (\text{Radical Ideals})^{op}$$

we have a correspondence between

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

and

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

Proof

- Clearly each point $\bar{a} = (a_1, \ldots, a_n) \in k^n$ is a variety since it is

$$V\{x_1 - a_1, \ldots, x_n - a_n\}.$$

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

To see maximality, suppose $I(\bar{a}) \subset J \subset k[x_1, \ldots, x_n]$. Then $I(\bar{a}) \subset J \subseteq \mathrm{Rad}(J) \subset k[x_1, \ldots, x_n]$ so $\phi \subset V(\mathrm{Rad}(J)) \subset VI(\bar{a}) = \{a\}$ 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 $VI(\bar{a}) = \{\bar{a}\} \subset V(M)$ 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

$A_1 = V(IA \cup \{f_1\})$, $A_2 = V(IA \cup \{f_2\})$.

Since f_1, f_2 don't vanish on A,

$A_1, A_2 \subset \mathbf{A}$. 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. $\square$