Irreducible algebraic sets

Let X be an algebraic set.

Def: X is <u>reducible</u> if $X = X_1 \cup X_2$, where $X_1, X_2 \subsetneq X$ are algebraic sets. Otherwise X is irreducible.

Ex: Let $L \subseteq \mathbb{A}^2$ be a line. Any $X \subsetneq L$ that is algebraic will be a finite set of points (see HW), so L is irreducible.

Ex: $V(xy) = V(x) \cup V(y)$ is reducible, while $V(x^2) = V(x)$ is irreducible.

Def: If $X = X_1 \cup \dots \cup X_m$, where each X_i is an irreducible algebraic set and $X_i \not\subseteq X_j$ for $i \neq j$, the X_i's are called <u>irreducible components</u> of X.

It turns out, we can always find a finite decomposition into irreducible components. To prove this, we first need some algebra.

Noetherian rings

R a commutative ring.

Def: R is <u>Noetherian</u> if every ideal $I \subseteq R$ is finitely generated.

Lemma: R is Noetherian

$\iff$ every strictly increasing sequence of ideals $I_1 \subsetneq I_2 \subsetneq \dots$ is finite.

$\iff$ every collection of ideals of R has a maximal element with respect to inclusion

Pf: On Pset

How does this relate to AG?

For a polynomial ring in finitely many variables over a field $k[x_1, \dots, x_n]$, the fact (which we will show) that every ideal is finitely generated is equivalent to the fact that every algebraic set in $\mathbb{A}^n$ is the intersection of finitely many hypersurfaces.

That is, any algebraic set can be written

$$X = V(I) = V(f_1, \dots, f_m) = V(f_1) \cap V(f_2) \cap \dots \cap V(f_m).$$

This holds by the HBT:

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

Pf: First, some terminology: If $f = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0 \in R[x]$, w/ $a_n \neq 0$, then a_n is the <u>initial coefficient</u>, $a_n x^n$ is the <u>initial term</u>.

Let $I \subseteq R[x]$ be an ideal. Choose a sequence $f_1, f_2, \dots \in I$ as follows: let $f_1 \in I$ be a nonzero elt of least degree,

and let f_{n+1} be an element of least degree in $I \setminus (f_1, \dots, f_n)$

If $(f_1, \dots, f_n) = I$, we're done.

Let a_j be the initial coefficient of f_j. Then $J = (a_1, a_2, \dots) \subseteq R$ is finitely generated. Let m be the smallest integer s.t. $J = (a_1, \dots, a_m)$.

Claim: $I = (f_1, \dots, f_m)$.

Otherwise consider $f_{m+\ell} \notin (f_1, \dots, f_m)$ Then $a_{m+\ell} = \sum_{j=1}^{m} u_j a_j$ for some $u_j \in R$.

Since $\deg f_{m+\ell} \geq \deg f_j$ for $j \leq m$, we can define

$$g = \sum_{j=1}^{m} u_j f_j x^{\deg f_{m+\ell} - \deg f_j} \in (f_1, \dots, f_m).$$

$f_{m+\ell} - g \in I \setminus (f_1, \dots, f_m)$ and has degree strictly less than the degree of f_{m+1}, which is a contradiction. $\square$

Corollary: R Noetherian $\Rightarrow R[x_1, \dots, x_n]$ Noetherian.

Cor: $k[x_1, \ldots, x_n]$ is Noetherian

Cor: Any decreasing chain of algebraic sets $X_1 \supsetneq X_2 \supsetneq \ldots$ is finite.

Now we can prove the following theorem about irreducible decompositions:

Thm: X an algebraic set.

a.) We can write $X = X_1 \cup \ldots \cup X_m$ where the X_i are irreducible components.

b.) The decomposition in a.) is unique.

Pf: a.) If X is irreducible, we're done. Otherwise $X = Y \cup Z$, Y and Z both proper algebraic subsets

We can continue by decomposing Y or Z, stopping when all alg. sets are irreducible.

If the process never stops, we get an infinite sequence

$$X \supsetneq X_1 \supsetneq X_2 \supsetneq \ldots$$

which can't happen by the Hilbert Basis Theorem.

b.) Suppose $X = X_1 \cup \dots \cup X_r$ and $X = Y_1 \cup \dots \cup Y_s$ are two irreducible decompositions.

For each X_i, we can write $X_i = \bigcup_{j=1}^{s} (Y_j \cap X_i)$.

Since X_i is irreducible, $X_i \subseteq Y_j$, some j.

Similarly, $Y_j \subseteq X_k$, some k. $\Rightarrow$ $X_i \subseteq X_k$, so $i = k$

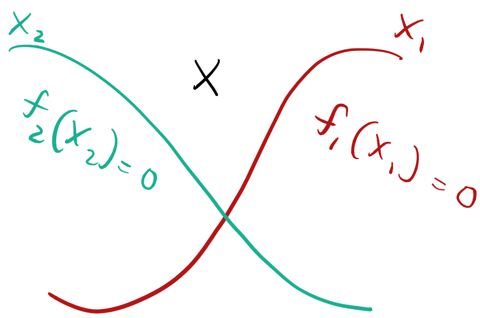
$\Rightarrow$ $X_i = Y_j$. $\square$

We already know that each algebraic set X gives us an ideal $I(X)$. If X is irreducible, we can say more:

Prop: X is irreducible $\Longleftrightarrow$ $I(X)$ is prime.

(Recall J is <u>prime</u> if for $fg \in J$, $f \in J$ or $g \in J$).

Pf: Assume X is reducible. Then $X = X_1 \cup X_2$, and



$I(X_1), I(X_2) \underset{\substack{\uparrow \\ \text{since } X_i \neq X}}{\supsetneq} I(X)$.

Let $f_i \in I(X_i) \setminus I(X)$.

Then for $P \in X$, $f_1(P) = 0$ or $f_2(P) = 0$ $\Rightarrow$ $(f_1 f_2)(P) = 0$.

$\Rightarrow \quad f_1 f_2 \in I(X)$ so $I(X)$ is not prime.

Now assume $I(X)$ is not prime. Then $\exists\ f, g \notin I(X)$ s.t. $fg \in I(X)$.

$\Rightarrow X \subseteq V(fg) = V(f) \cup V(g)$, but $X \not\subseteq V(f)$ or $V(g)$.

$$\Rightarrow X = \underbrace{(V(f) \cap X)}_{\neq X} \cup \underbrace{(V(g) \cap X)}_{\neq X} \Rightarrow X \text{ is reducible. } \square$$

We'll soon show that if J is a prime ideal, $V(J)$ is irreducible. For this, it is necessary that $k = \bar{k}$!

Ex: Consider $f = y^2 + x^2(x-1)^2 \in \mathbb{R}[x,y]$

f is irreducible, so (f) is prime (exer)

But the zeros of f are $\{(0,0),(1,0)\}$.

Dimension

If $X \subseteq \mathbb{A}^n$ is an alg. set, we can write $X \supseteq X_d \supsetneq X_{d-1} \supsetneq \cdots \supsetneq X_0 \supsetneq \emptyset$.
where X_i is an irr. alg. set.

The maximum such d is the dimension of X.

Ex: $\dim \mathbb{A}^1 = 1$. We know $\dim \mathbb{A}^n \geq n$, but showing equality is hard, and involves a lot of CA machinery.

Equivalently, $\dim X$ = maximum length of chain of prime ideals containing $I(X)$.

Irreducible algebraic sets in $\mathbb{A}^2$

What are the irreducible sets in $\mathbb{A}^2$? So far, we know:

1.) $\emptyset = V(1)$
2.) $\mathbb{A}^2 = V(0)$
3.) A point $(a,b) = V(x-a,\ y-b)$
4.) Irreducible <u>plane curves</u> $= V(f)$, f irreducible ← (Need to prove this is always irreducible.)

In order to show that these are all the possibilities, it suffices to prove the following:

Proposition: Let $f, g \in k[x,y]$ with no common factors. Then $V(f,g) = V(f) \cap V(g)$.

Note that if $f = f'a$, $g = g'a$, then $V(f,g) = V(f',g') \cup V(a)$, so we can reduce to situation in the theorem.

Before we prove this, we need some...

Algebra preliminaries:

Def: Let R be an integral domain. The <u>field of fractions</u> of R

is the set

$$\left\{ \frac{a}{b} \;\middle|\; a, b \in R,\ b \neq 0 \right\}$$

s.t. $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = cb$ and $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}$.

Note that this is in fact a field.

The field of fractions of $k[x_1, \ldots, x_n]$ is called the <u>field of rational functions</u>, denoted $k(x_1, \ldots, x_n)$.

Elements are of the form $\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}$, $f, g \in k[x_1, \ldots, x_n]$.

Recall the following:

<u>Gauss' Theorem:</u> If R is a UFD with field of fractions K, then if f is irreducible in $R[x]$, it's irreducible in $K[x]$.

Using this, we can now prove the proposition.

<u>Proof of proposition:</u> If f and g have no common factors in $k[x,y] = k[x][y]$, then by Gauss' Theorem, the don't have common factors in $k(x)[y]$.

$k(x)$ is a field $\Rightarrow k(x)[y]$ is a PID. Thus,

$(f, g) = (h) \subseteq k(x)[y]$, for some h. But h divides f and g,

so $(f, g) = (1)$. Thus, $rf + sg = 1$ for some $r, s \in k(x)[y]$.

Clearing denominators, we get

$$\underset{\text{in } k[x,y]}{a} f + \underset{\text{in } k[x,y]}{b} g = \underset{\text{in } k[x]}{d}$$

Let $P = (\alpha, \beta) \in V(f,g)$. Then $d(\alpha) = 0$. Thus, only finitely many x-coordinates appear in $V(f,g)$.

By an analogous argument, only finitely many y-coordinates appear, so $V(f,g)$ is finite. $\square$

Finally, we can show the following:

<u>Cor</u>: If $f \in k[x,y]$ is irreducible, then $I(V(f)) = (f)$, so $V(f)$ is irreducible.

<u>Pf</u>: We know $(f) \subseteq I(V(f))$. If $g \in I(V(f))$, then

$V(f) \subseteq V(g)$.

Note that since k is algebraically closed, $V(f)$ is infinite: WLOG, f has positive degree d in x. Write

$$f = a_d(y)\, x^d + \cdots + a_1(y)\, x + a_0(y).$$

For each of the infinitely many $\alpha \in k$ s.t. $a_d(y)$ doesn't vanish, $f(x, \alpha)$ has at least one root.

Thus, $V(f, g)$ is infinite, so f and g have a common factor. f is irreducible, so it divides $g \Rightarrow g \in (f)$. $\square$