Part II – Algebraic Geometry (Rough)

Based on lectures by Prof. I. Grojnowski
Notes taken by Bhavik Mehta

Lent 2017

Contents

Introduction

Consider $E = \{ (x, y) \in \mathbb{C}^2 \mid y^2 = x^3 - x \}$. Let's first draw this when $(x, y) \in \mathbb{R}^2$. If $y \in \mathbb{R}$, $y^2 \geq 0$, so if $x \in \mathbb{R}$, $x^3 - x = x(x^2 - 1) \geq 0$ so $x \geq 1$ or $-1 \leq x \leq 0$.

Now consider $(x, y) \in \mathbb{C}$. In general, this is tricky. Here, define $p : E \to \mathbb{C}$ given by $(x, y) \mapsto x$ most of the time ($x \notin \{0, 1, -1\}$), $p^{-1}(x)$ is two points. This doesn't help us visualise.

$$\Gamma = \{ (x, y) \in \mathbb{C}^2 \mid y \in \mathbb{R}, x \in [-1, 0] \cup [1, \infty) \}$$

Claim: $E \setminus \Gamma$ is disconnected and has two pieces. Proof: Exercise.

So, $E \setminus \Gamma$ is two copies of glued together. To glue, turn one of the pieces over (this ruins the representation as a double cover, but is the right gluing). Think of (the picture below) by adding a point at ∞, so it lives on the Riemann surface.

Take another copy, flip it over and glue back. (this section is in the process of tidying)

1 Dictionary between algebra and geometry

1.1 Basic notions

Definition (Affine space)**. Affine n-space** is $\mathbb{A}^n = \mathbb{A}^n(k) \coloneqq k^n$ for k a field.

Notation. Write $k[\mathbb{A}^n] = k[x_1, \dots, x_n]$ for the polynomials in n variables.

Any $f \in k[\mathbb{A}^n]$ defines a function $f : \mathbb{A}^n = k^n \to k$ given by $(\lambda_1, \dots, \lambda_n) \mapsto f(\lambda_1, \dots, \lambda_n)$ by evaluation.

Let $S \subseteq k[x_1, \dots, x_n]$ be any subset of polynomials.

Definition (Affine variety)**.**

$$Z(S) = \{\, \lambda = (\lambda_1, \dots, \lambda_n) \in k^n \mid f(\lambda_1, \dots, \lambda_n) = 0 \text{ for all } f \in S \,\}$$

is called the **affine variety defined by** S, the simultaneous zeros of all functions in S. $Z(S)$ is called an affine subvariety of $\mathbb{A}^n$.

Example.

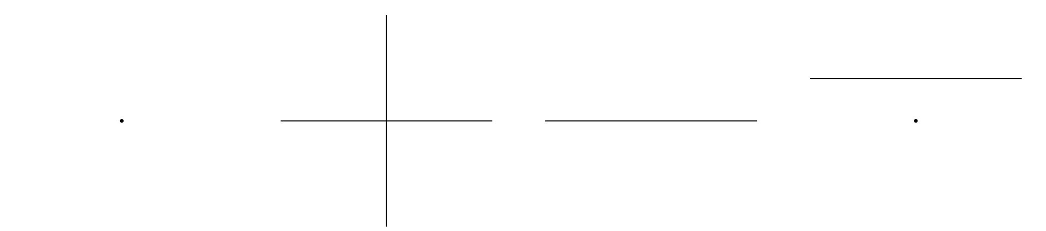
(i) $\mathbb{A}^n = Z(0)$.

(ii) On $\mathbb{A}^1$, $Z(x) = \{0\}$, $Z(x-7) = \{7\}$. If $f(x) = (x-\lambda_1)\dots(x-\lambda_n)$, $Z(f(x)) = \{\lambda_1, \dots, \lambda_n\}$. Affine subvarieties of $\mathbb{A}^1$ are: $\mathbb{A}^1$ and finite subsets of $\mathbb{A}^1$.

(iii) On $\mathbb{A}^2$, $E = Z(y^2 - x^3 + x)$ we (will) have sketched when $k = \mathbb{C}$ and $k = \mathbb{R}$ in the introduction.

(iv) For $k = \mathbb{R}$, we have

$Z(x, y) = \{(0,0)\}$ $\qquad$ $Z(xy)$ $\qquad$ $Z(y)$ $\qquad$ $Z(y(y-1), x(y-1))$



Remark. If $f \in k[\mathbb{A}^n]$ then $Z(f)$ is called a **hypersurface**.

Observe that if J is the ideal generated by S

$$J = \left\{ \sum a_i f_i \;\middle|\; a_i \in k[x_1, \dots, x_n], f_i \in S \right\}$$

then $Z(J) = Z(S)$. Hence,

Theorem. If $Z(S)$ is an affine subvariety of $\mathbb{A}^n$, there is a finite set $f_1, \dots, f_r$ of polynomials with $Z(S) = Z(f_1, \dots, f_r)$.

Proof. $J = \langle f_1, \dots, f_r \rangle$ for some $f_1, \dots, f_r$ by Hilbert basis theorem. $\square$

Lemma.

(i) if $I \subseteq J$, $Z(J) \subseteq Z(I)$

(ii) $Z(0) = \mathbb{A}^n$, $Z(k[x_1, \dots, x_n]) = \varnothing$.

(iii) $Z\left(\bigcup J_i\right) = Z(\sum J_i) = \bigcap Z(J_i)$ for any possibly infinite family of ideals

(iv) $Z(I \cap J) = Z(I) \cup Z(J)$ if I, J ideals

Proof. (i), (ii), (iii) are clear.

(iv): $\supseteq$ holds by (i). Conversely, if $x \notin Z(I)$ then $\exists f_1 \in I$ such that $f_1(x) \neq 0$. So if $x \notin Z(J)$ also, $\exists f_2 \in J$ with $f_2(x) \neq 0$ also. Hence $f_1 f_2(x) = f_1(x) f_2(x) \neq 0$, so $x \notin Z(f_1 f_2)$. But $f_1 f_2 \in I \cap J$, as I, J ideals so $x \notin Z(I \cap J)$. $\square$

Definition (Zariski topology)**.** Looking at these results, $Z(I)$ form closed subsets of a topology on $\mathbb{A}^n$, called the **Zariski topology**.

Definition. If $Z \subset \mathbb{A}^n$ is any subset, set

$$I(Z) := \{\, f \in k[\mathbb{A}^n] \mid f(p) = 0, \forall p \in Z \,\}.$$

Observe that $I(Z)$ is an ideal: if $g \in k[\mathbb{A}^n]$, $f(p) = 0$ then $(gf)(p) = 0$.

Lemma.

(i) $Z \subseteq Z' \implies I(Z') \subseteq I(Z)$

(ii) for any $Y \subseteq \mathbb{A}^n$, $Y \subseteq Z(I(Y))$,

(iii) if $V = Z(J)$ is a subvariety of $\mathbb{A}^n$, then $V = Z(I(V))$.

(iv) if $J \lhd k[\mathbb{A}^n] = k[x_1, \dots, x_n]$ an ideal, then $J \subseteq I(Z(J))$.

Proof. (i), (ii), (iv) are clear. For (iii), first show $\supseteq$. $I(V) = I(Z(J)) \supseteq J$ by (iv) so $Z(I(V)) \subseteq Z(J) = V$ by (i). $\subseteq$ follows by (iv). $\square$

Hence (ii) and (iii) show that $Z(I(Y))$ is the smallest affine subvariety of $\mathbb{A}^n$ containing Y, i.e. it is the closure of Y in the Zariski topology.

Example. Take $\mathbb{Z} \subseteq \mathbb{C} = \mathbb{A}^1$, $k = \mathbb{C}$. If a polynomial in one variable vanishes at every integer, it is 0, so $I(\mathbb{Z}) = 0$ and hence the closure of $\mathbb{Z}$ in the Zariski topology is $\mathbb{C}$.

Note if $k = \mathbb{C}$, $f \in \mathbb{C}[x_1, \dots, x_n]$, then f is continuous in the usual topology, so

$$Z(J) = \bigcap_{f \in J} Z(f) = \bigcap_{f \in J} f^{-1}(\{0\})$$

is a closed set in the usual topology, i.e. Zariski closed $\Rightarrow$ closed in the usual topology. So, the Zariski topology is coarser than the usual topology.

We now have maps

$$\begin{tikzcd} \left\{ \begin{matrix} \text{Zariski closed} \\ \text{subvarieties of } \mathbb{A}^n \end{matrix} \right\} \arrow[r, bend right, "I"'] & \left\{ \begin{matrix} \text{ideals in} \\ k[x_1, \ldots, x_n] \end{matrix} \right\} \arrow[l, bend right, "Z"'] \end{tikzcd}$$

But this is not a bijection. For instance,

$$Z(x) = Z(x^2) = Z(x^3) = \ldots = \{0\} \subseteq \mathbb{A}^1.$$

More generally, $Z(f_1^{a_1}, \ldots, f_r^{a_r}) = Z(f_1, f_2, \ldots, f_r)$, but it turns out this kind of thing is the only problem. This is called Hilbert's 'Nullstellensatz', and we will see it soon.

Definition (Reducible)**.** An affine variety Y is **reducible** if there are affine varieties Y_1, Y_2, $Y_i \neq Y$ with $Y = Y_1 \cup Y_2$, and **irreducible** otherwise. It is called **disconnected** if $Y_1 \cap Y_2 = \varnothing$.

So $Z(xy) = Z(x) \cup Z(y)$, reducible. $Z(y(y-1), x(y-1)) = Z(x, y) \cup Z(y-1)$ reducible and disconnected.

Proposition. Any affine variety is a finite union of irreducible affine varieties.

Remark. This is very different from usual manifolds.

Proof. If not, Y is not irreducible, so $Y = Y_1 \cup Y_1'$ and one of Y_1, Y_1', (say Y_1) is not the finite union of irreducible affine varieties, so

$$Y_1 = Y_2 \cup Y_2', \ldots$$

and so we get an infinite chain of affine varities $Y \supsetneq Y_1 \supsetneq Y_2 \supsetneq \cdots$. But each $Y_i = Z(I_i)$ for some ideal I_l. Let $W = \bigcap Y_l = Z(\sum I_i) = Z(I)$. $I = \sum I_i$ is an ideal. As the ideal I is finitely generated $I = \langle f_1, \ldots, f_r \rangle$ for some f_i. $f_i \in I_{a_i}$ for some $a_1, \ldots, a_r$ so $I = I_{a_1} + \cdots + I_{a_r}$, $W = Y_{i_1} \cap \cdots \cap Y_{i_r}$ contradicting $Y_N \subsetneq Y_{a_1} \cap \cdots \cap Y_{a_r}$ if $N > r$. $\square$

Exercise. If Y is a subvariety of $\mathbb{A}^N$, then we can write $Y = Y_1 \cup \cdots \cup Y_r$ with Y_i irreducible, and r minimal, uniquely up to reordering. Call the Y_i the irreducible components of Y.

Proposition. Y is irreducible $\iff$ $I(Y)$ is a prime ideal in $k[\mathbb{A}^n] = k[x_1, \ldots, x_n]$.

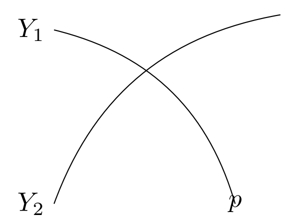
Example.

(i) (xy) is not a prime ideal.

(ii) Exercise: Let R be a UFD, $f \in R$, $f \neq 0$, f irreducible $\iff$ (f) a prime ideal.

(iii) Exercise: $k[x_1, \ldots, x_n]$ is a UFD. Hence $Z(y^2 - x^3 + x)$ is irreducible, $Z(y - x^2)$ is irreducible.

Proof. If $Y = Y_1 \cup Y_2$ is reducible, $\exists p \in Y_1 \setminus Y_2$ so $\exists f \in I(Y_2)$ such that $f(p) \neq 0$ and similarly, $\exists q \in Y_2 \setminus Y_1$ so $\exists g \in I(Y_1)$ such that $g(q) \neq 0$. Then $fg \in I(Y_1) \cap I(Y_2) = I(Y)$. But $f \notin I(Y)$, $g \notin I(Y)$ so not prime.



Conversely, if $I(Y)$ is not prime $\exists f_1 f_2 \in k[\mathbb{A}^n]$ such that $f_1, f_2 \notin I(Y)$ but $f_1 f_2 \in I(Y)$. Let $Y_i = Y \cap Z(f_i) = \{\, p \in Y \mid f_i(p) = 0 \,\}$. $Y_1 \cup Y_2 = Y$, as $p \in Y \implies f_1 f_2(p) = 0 \implies f_1(p) = 0$ or $f_2(p) = 0$. $Y_i \neq Y$ as $f_i \notin I(Y)$ (i.e. $\exists p_l \in Y$ such that $f_i(p_i) \neq 0$ so $p_i \notin Y_i$). ☐

Lemma. *X irreducible affine subvariety of $\mathbb{A}^n$, $\mathcal{U} \subseteq X$ open and non-empty $\implies \overline{\mathcal{U}} = X$.*

Proof. Let $Y = X - \mathcal{U}$, closed. Then $\overline{\mathcal{U}} \cup Y = X$, and $\mathcal{U} \neq \varnothing \implies Y \neq X$. But X is irreducible, so $\overline{\mathcal{U}} = X$. ☐

Application: Cayley-Hamilton Theorem $A \in \mathrm{Mat}_n(k)$, an $n \times n$ matrix, with

$$\mathrm{char}_A(x) = \det(xI - A) \in k[x]$$

the characteristic polynomial. This gives a function $\mathrm{char}_A : \mathrm{Mat}_n(k) \to \mathrm{Mat}_n(k)$ $B \mapsto \mathrm{char}_A(B)$. Cayley-Hamilton theorem says that $\forall A \in \mathrm{Mat}_n(k)$, $\mathrm{char}_A(A) = 0$. Notice this is an equality of matrices, so it is n^2 equations.

Proof. Let $X = \mathbb{A}^{n^2} = \mathrm{Mat}_n(k)$, affine space, hence irreducible algebraic variety. Consider $CH = \{\, A \in \mathrm{Mat}_n(k) \mid \mathrm{char}_A(A) = 0 \,\}$. Claim: this is a Zariski closed subvariety of $\mathbb{A}^{n^2}$, cut out by n^2 equations, $\mathrm{char}_A(A)_y = 0$. We must check that these equations are polynomials in the matrix coefficients of A.

Consider $\mathrm{char}_A(x) \in k[\mathbb{A}^{n^2+1}] = \det(xI - A)$, a polynomial in x and in the matrix coefficients of A.

$$\mathrm{char}_{\begin{pmatrix} a & b//c & d \end{pmatrix}}(x) = \det \begin{pmatrix} x-a & -b \\ -c & x-d \end{pmatrix} = x^2 - (a+d)x + (ad - bc)$$

The ijth coefficient of A^r is also a polynomial (of deg r) in the matrix coefficients of A, eg

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a^2 + bc & \dots \\ \vdots & \ddots \end{pmatrix}$$

hence $\mathrm{char}_A(A)_y = 0$ is a poly in the matrix coefficients of A, proving the claim.

Now, it is enough to prove the theorem when when $k = \overline{k}$, as $\mathrm{Mat}_n(k) \subseteq \mathrm{Mat}_n(\overline{k})$. Next, notice that $\mathrm{char}_A(x) = \mathrm{char}_{gAg^{-1}}(x)$, for $g \in \mathrm{GL}_n$. and $\mathrm{char}_A(gBg^{-1}) = g\,\mathrm{char}_A(B)g^{-1}$ for $g \in \mathrm{GL}_n$. Hence $\mathrm{char}_A(A) = 0 \iff \mathrm{char}_{gAg^{-1}}(gAg^{-1}) = 0$, so $A \in CH \iff gAg^{-1} \in CH$. Now, let $\mathcal{U} = \{\, A \in \mathrm{Mat}_n(k) \mid A \text{ has distinct eigenvalues} \,\}$. As $k = \overline{k}$, $A \in \mathcal{U} \implies \exists g \in \mathrm{GL}_n$ with

$$gAg^{-1} = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

and it is clear that $gAg^{-1} \in CH$. As $k = \overline{k}$, $\#k$ is infinite, so $\mathcal{U}$ is non-empty so

$$\varnothing \neq \mathcal{U} \subseteq CH \subseteq \mathbb{A}^{n^2} = X$$

hence if we show that $\mathcal{U}$ is Zariski open in X then $\mathcal{U} = X$, as X is irreducible. But CH is closed, so $\mathcal{U} \subseteq CH$, so $CH = X$.

Finally, we must show $\mathcal{U}$ is Zariski open. Observe $A \in \mathcal{U} \iff \mathrm{char}_A(x) \in k[x]$ has distinct roots. Now recall from Galois theory, if $f(x)$ is a polynomial, $\exists$ poly $D(f)$ in the coefficients of the poly f such that f has distinct roots $\iff D(f) \neq 0$.

So $A \in \mathcal{U} \iff D(\mathrm{char}_A(x)) \neq 0$ is a polynomial in matrix coefficients of A. □

1.2 Nullstellensatz

Suppose $Y \subseteq \mathbb{A}^n$ is a subvariety, let $I(Y) = \{\, f \in k[x_1, \dots, x_n] \mid f(Y) = 0 \,\}$. Recall we have maps

$$\begin{tikzcd}
k[\mathbb{A}^n] \arrow[r] \arrow[dr] & \{\text{functions from } k^n = \mathbb{A}^n \to k\} \arrow[d] \\
 & \{\text{functions from } Y \to k\}
\end{tikzcd}$$

where the composite is constructed by restricting a function from $\mathbb{A}^n \to k$ to $Y \to k$. Also note that the top map is injective if $\#k = \infty$.

Definition (Polynomial functions on subvariety)**.** Let $k[Y] = k[x_1, \dots, x_n]/I(Y)$ by the **polynomial functions on** Y, also called **regular functions**.

We just observed that $k[Y] \to \{\text{all functions from } Y \to k\}$ is injective if $\#k = \infty$. We've seen Y irreducible $\iff I(Y)$ is prime $\iff k[Y]$ is an integral domain. Now let $p \in Y$. We have a map $k[Y] \to k$, given by $f \mapsto f(p)$. This is an algebra homomorphism, so the kernel

$$m_p = \{\, f \in k[Y] \mid f(p) = 0 \,\}$$

is an ideal. (The homomorphism is surjective as constants go to constants). This is a maximal ideal, as R/M a field $\iff M$ is a maximal ideal in R and we have $k[Y]/m_p = k$.

A natural question to ask now is whether or not there are any other maximal ideals in $k[Y]$? In particular, what are the possible surjective algebra homomorphisms

$$k[x_1, \dots, x_n] \twoheadrightarrow L, \quad k \subseteq L, L \text{ field.}$$

For example, suppose $Y = Z(x^2 + 1)$ and $k = \mathbb{R}$. Then $k[Y] = \frac{\mathbb{R}[x]}{x^2+1}$ is not of the above form, since it is $\mathbb{C}$ instead of $\mathbb{R}$.

Claim: This is the only issue. If $k = \overline{k}$, there are no other algebra homomorphisms $k[Y] \to k$ other than evaluating at points $p \in Y$, and if $k \neq \overline{k}$ you just get for L algebraic extensions of k, as in the above example.

Theorem (Nullstellensatz, v1)**.** Let $m \subseteq k[x_1, \dots, x_n]$ be a maximal ideal, and $A = k[x_1, \dots, x_n]/m$. Then A is finite dimensional over k.

Remark. A is finite dimensional over $k \iff$ every $a \in A$ is algebraic over k. (Proof: $\Rightarrow$ clear, as $1, a, a^2, \dots$ can't all be linearly independent over k. $\Leftarrow$ image of $x_1, \dots, x_n$ in A each satisfy an algebraic relation over k and they generate A).

Corollary. If k is algebraically closed, then $k \hookrightarrow A$ is an iso, ie $A \cong k$, that is, every maximal ideal is of the form $M = (x_1 - p_1, \dots, x_n - p_n)$ for $p \in k^n$.

Proof. M a maximal ideal $\implies$ A a field, but if $k \subseteq \overline{k}$ that means $k = \overline{k}$ algebraic over k. Now let a_i be the image of x_i in A, and M is as stated. So if $k = \overline{k}$, solutions of equations $I \longleftrightarrow$ max ideal $M \subseteq k[Y] \longleftrightarrow$ alg homomorphisms $k[Y] \to k$ and if $k \neq \overline{k}$, then they are 'galois orbits of solutions over bigger fields'. □

We can interpret this in the case $k \neq \overline{k}$ as saying: to study solutions of algebraic equations over K, i.e. simultaneous zero of an ideal I, it is necessary to study their solutions over fields bigger than k, such as $\overline{k}$.

Proof. When k is uncountable: If the result is not true, $\exists t \in L \setminus k$ with t transcendental over k. In particular, $k(t) \subseteq L$. SO $\frac{1}{t-\lambda} \in L, \forall \lambda \in k$. But L has countable dimension over k (let V_d be the k-vector space which is the image of $\{ f \in k[x_1, \dots, x_n] \mid \deg f \leq d \}$, V_d is finite dimensional, $\bigcup V_d = L$). Now consider $\frac{1}{t-\lambda}, \dots, \frac{1}{t-\lambda_r}$ for $\lambda_1, \dots, \lambda_r \in k$ distinct. If these are linearly dependent over k, i.e. $\exists a_i \in k$ with $\sum \frac{a_i}{t-\lambda_i} = 0$, then clearing denominators gives a poly relation in t, contradicting t is transcendental. So they are linearly independent, but there are uncountably many $\lambda \in k$, a contradiction. □

Corollary. If $k = \overline{k}$, take $I \leq k[x_1, \dots, x_n]$ an ideal. Then $Z(I) \neq \varnothing \iff I \neq k[x_1, \dots, x_n]$. More generally, $I \leq k[Y]$, $Z(I) \neq \varnothing \iff I \neq k[Y]$.

Note if $k \neq \overline{k}$, this is obviously false.

Proof. For $I \leq k[Y] = k[x_1, \dots, x_n]/I(Y)$, replace I by its inverse image in $k[x_1, \dots, x_n]$ to see it suffices to prove the specific case instead of the general case.

If $I \neq k[x_1, \dots, x_n]$, then $I \subseteq m \subsetneq k[x_1, \dots, x_n]$ for m a maximal ideal. I is contained in some maximal ideal. But Nullstellensatz gives $Z(m) = \{p\}$ for some $p \in k^n$. So $Z(I) \supseteq Z(m) = \{p\} \neq 0$. □

Remark. This means, any ideal of equations which aren't all the equations have a simultaneous solutions. This is equivalent to the Nullstellensatz.

Definition (Radical ideal)**.** Take R a ring, $J \lhd R$ an ideal. The **radical** is

$$\sqrt{J} := \{ f \in R \mid \exists n \geq 1, f^n \in J \} \supseteq J$$

Lemma. $\sqrt{J}$ is an ideal.

Proof. If $\gamma \in R$, $f \in \sqrt{J}$, then $(\gamma f)^n = \gamma^n f^n \in J$ if $f^n \in J$. If $f, g \in \sqrt{J}$ with $f^n \in J$, $g^m \in J$ for some n, m then $(f+g)^{n+m} = \sum \binom{n+m}{i} f^i g^{n+m-i}$. Either $i \geq n$ so $f^i \in J$ or $n + m - i \geq m$ then $g^{n+m-i} \in J$, so $f + g \in J$. □

Example. (1) $\sqrt{(x^n)} = (x)$ in $k[x]$.

(2) if J is a prime ideal, $\sqrt{J} = J$.

(3) if $f \in k[x_1, \dots, x_n]$ is irreducible, then (f) is prime as $k[x_1, \dots, x_n]$ is a UFD, so $\sqrt{(f)} = (f)$.

Observe $Z(\sqrt{J}) = Z(J)$.

Theorem (Nullstellensatz, v2)**.** If $k = \overline{k}$, $I(Z(J)) = \sqrt{J}$.

Proof. Let $f \in I(Z(J))$, i.e. $f(p) = 0 \forall p \in Z(J)$. We must show that $\exists n$ such that $f^n \in J$. Consider $k[x_1, \dots, x_n, t]/tf - 1 \coloneqq k[x_1, \dots, x_n, \frac{1}{f}]$. Let i be the ideal of this, generated by the image of J. Claim: $Z(I) = \varnothing$. Proof: If not, let $p \in Z(I)$. As $J \subseteq I$, we have $p \in Z(J)$ and so $f(p) = 0$. But $p = (p_1, \dots, p_n, p_t)$ with $p_t \cdot f(p_1, \dots, p_n) = 1$, so $f(p) \neq 0$, contradiction. But now the corollary to Nullstellensatz version 1 gives $I = k[x_1, \dots, x_n, \frac{1}{f}]$. So, $1 \in I$. But I is generated by J, so this says $1 = \sum_1^N \gamma_i / f^i$ for some $\lambda_i \in J$, $\gamma_N \neq 0$ for some N. Clear denominators and we get

$$f^N = \sum \tilde{\gamma_i}, \tilde{\gamma_i} \in J, i.e. f^N \in J.$$

$\square$

Remark. This proof uses $k[x_1, \dots, x_n, t]/tf - 1 \twoheadleftarrow k[\mathbb{A}^{n+1}]$. This is $k[Y]$, where $Y = Z(tf - 1) \subseteq \mathbb{A}^{n+1}$ and $Z(tf - 1) = \{ (p, t_0) \mid f(p)t_0 = 1 \}$. Clearly $Y \xrightarrow{\sim} \{ p \in \mathbb{A}^n \mid f(p) \neq 0 \} = \mathbb{A}^n \setminus Z(f)$.

We will return to this, but first lets deduce some consequences of Nullstellensatz version 2.

Corollary. If $k = \overline{k}$, $Z(I) = Z(J) \iff I(Z(I)) = I(Z(J)) \iff \sqrt{I} = \sqrt{J}$. So we have a bijection

The intrinsic definition of affine varieties is a consequence (doesn't depend on the embedding of $X \hookrightarrow \mathbb{A}^n$).

Definition (Nilpotent)**.** In a ring R, an element $y \in R$ is **nilpotent** if $y^n = 0$ for some $n > 0$.

Example. In $k[x]/x^7$, x is nilpotent.

Exercise. Let $J \leq k[x_1, \dots, x_n]$ be an ideal, $R = k[x_1, \dots, x_n]/J$. Then $J = \sqrt{J} \iff R$ has no non-zero nilpotent elements.

Corollary. Let $X \subseteq \mathbb{A}^n$ be a Zariski closed subvariety. Then $k[X]$ is a finitely generated k-algebra with no non-zero nilpotent elements. As it is finitely generated, there is $k[x_1, \dots, x_n] \overset{\alpha}{\twoheadrightarrow} k[X]$ a surjective algebra homomorphism and no non-zero nilpotents $\iff \ker \alpha$ is a radical ideal.

Definition (Affine variety, v2)**.** An affine variety over a field k is a finitely generated k-algebra with no non-zero nilpotents.

Observe:

(i) if $k = \overline{k}$, this coincides with our previous definition.

(ii) if $k \neq \overline{k}$, we get new examples, now $\mathbb{R}[x, y]/x^2 + y^2 + 1$ is an affine algebraic variety over $\mathbb{R}$ even though $Z(x^2 + y^2 + 1) = \varnothing$. Note Nullstellensatz says $\mathbb{R}[x, y]/x^2 + y^2 + 1$ still has lots of maximal ideals but they correspond to $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ orbits of complex solutions, i.e. complex conjugate pairs.

(iii) this definition does not explicitly refer to a choice of embedding $X \hookrightarrow \mathbb{A}^n$ (the data of a choice of algebra generators for $k[X]$).

What is missing? We still have to define what a map of algebraic varieties is.

Definition (Morphism)**.** A **morphism** of algebraic varieties $X \to Y$ is a k-algebra homomorphism $f^* : k[Y] \to k[X]$. Write $\mathrm{Mor}(X, Y)$ for the set of morphisms, and write f for the morphism associated to f^*.

Let us unpack this definition. Write

$$k[X] = k[x_1, \dots, x_n]/\langle s_1, \dots, s_l \rangle \qquad k[Y] = k[y_1, \dots, y_m]/\langle r_1, \dots, r_k \rangle$$

and write $\overline{y_1}, \dots, \overline{y_m}$ for the images of y_i in $k[Y]$. An algebra homomorphism $f^* : k[Y] \to k[X]$ takes $\overline{y_i} \mapsto f^*(\overline{y_i})$. Choose a poly $\Phi_i = \Phi_i(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$ which mod the ideal $\langle s_1, \dots, s_l \rangle$ equals $f^*(\overline{y_i})$. This defines an algebra homomorphism

$$\begin{aligned} k[y_1, \dots, y_m] &\longrightarrow k[x_1, \dots, x_n] \\ y_l &\mapsto \Phi_i(x_1, \dots, x_n). \end{aligned}$$

Now the condition that this determines an algebra homomorphism $k[Y] \to k[X]$ is the condition that $r_i(\Phi_1, \dots \Phi_m) = 0$ in $k[X]$ $\forall i$ i.e. the ideal $\langle r_1, \dots, r_l \rangle$ get sent to zero in $k[X]$. That is, f^* is the data of polynomials $\Phi_1, \dots, \Phi_m$ in $k[x_1, \dots x_n]$ such that $r_i(\Phi_1, \dots \Phi_m) = 0$ (and the choice of such polynomials is well defined, up to adding any element of $\langle s_1, \dots, s_i \rangle$). Moreover, f^* determines a map of sets $X \to Y$, denoted $f : X \to Y$, $x \mapsto (\Phi_1(x), \dots, \Phi_m(x))$. So, a morphism of algebraic varieties $f : X \to Y$ is, roughly speaking, a map of sets $X = (X_1, \dots, X_n) \in X \longrightarrow f(x) = (\Phi_1(x), \dots, \Phi_m(x)) \in Y$ (where $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$) given by polynomials $\Phi_1, \dots, \Phi_m \in k[\mathbb{A}^n]$. The condition that $(\Phi_1(x), \dots, \Phi_m(x)) \in Y$ is the condition $r_i(\Phi_1, \dots, \Phi_m) = 0$. But, we gave this definition in a way which didn't require choosing $X \hookrightarrow \mathbb{A}^n$ etc.

Definition (Isomorphic)**.** X is **isomorphic** to Y if $\exists \alpha^* : k[Y] \to k[X]$, $\beta^* : k[X] \to k[Y]$ such that $\alpha^* \beta^*$ and $\beta^* \alpha^*$ are identity.

Example. (i) $t \mapsto (t^2, t^3)$ is a morphism $\mathbb{A}^1 \to \mathbb{A}^2$. More generally, $\mathrm{Mor}(\mathbb{A}^1, \mathbb{A}^n) = k$-algebra homomorphims $k[x_1, \dots, x_n] \to k[t]$ is just a tuple of polys $(\phi_1(t), \dots, \phi_n(t)) \in k[t]^n$.

(ii) Take $\mathrm{Mor}(X, \mathbb{A}^1) \ni \varphi^*$, then $\varphi^* k[t] \to k[X]$ an algebra homomorphism. $k[t]$ is the free k-algebra on 1 generator t. That is, to specify an algebra homomorphism $k[t] \to R$ (for any ring R), it is enough to say where t gets mapped to, and conversely any element of R determines such a homomorphism. So $\mathrm{Mor}(X, \mathbb{A}^1) = k[X]$.

(iii) $X = \mathbb{A}^1$, $Y = \{ (x, y) \mid x^2 = y^3 \} = Z(x^2 - y^3)$. Consider $t \mapsto (t^3, t^2)$. This is a morphism $(t^3)^2 = (t^2)^3$. Exercise: Is this an isomorphism? Is $Y \cong \mathbb{A}^1$?

(iv) Take $\operatorname{char} k \neq 2$. Is there a morphism $\mathbb{A}^1 \to \{ (x, y) \mid y^2 = x^3 - x \}$ (which isn't a trival map). Do there exist polynomials $a = a(t), b = b(t) \in k[t]$, not both constant such that $b^2 = a^3 - a$.

If $k = \overline{k}$, we can also reconstruct f as follows

Proposition. Let X be an affine algebraic variety, and $f \in k[X]$. Then set

$$Y = \{ (p,t) \in X \times \mathbb{A}^1 \mid tf(p) = 1 \}$$

. This is an affine algebraic variety, and the map $Y \hookrightarrow X$ with $(p,t) \mapsto p$ is a morphism of affine algebraic varieties.

Proof. It is $k[X] \to k[Y] =: k[X][t]/tf - 1$. Exercise: $k[Y]$ has no non-zero nilpotents. $\square$

This means you should think of $Y \xrightarrow{\sim} X \setminus Z(f) \hookrightarrow X$. That is, you should think of this as saying the Zariski open $X \setminus Z(f)$ is also an affine algebraic variety and the inclusion map $Y \hookrightarrow X$ is a morphism of algebraic varieties.

Warning. Take $\{ (x,y) \in \mathbb{A}^2 \mid (x,y) \neq (0,0) \}$. This is Zariski open in $\mathbb{A}^2$ as $\{(0,0)\}$ is a closed set. But, this is not an affine algebraic variety.

2 Projective space

We will define it first as a set, then as an algebraic variety (but not an affine one). Take V a vector space over k, $\dim V = n+1$ for $n \geq 0$.

$$\begin{aligned} \mathbb{P}V = \mathbb{P}^n &= \{\text{set of lines through 0 in } V\} \\ &= (V \setminus \{0\})/k^\times \end{aligned}$$

That is, if $v \in V$, $v \neq 0$ then $kv = \{\, \lambda v \mid \lambda \in k \,\}$ is a line through 0, and conversely if $l \in \mathbb{P}V$ is a line, $l = kv$ for any $v \in l \setminus 0$. Choose a basis $e_0, \ldots, e_n$ of V, write $V \xleftarrow{\sim} k^{n+1}$, $\sum x_i e_i \leftarrow\!\shortmid (x_0, \ldots, x_n)$. If $(x_0, \ldots, x_n) \neq (0, \ldots, 0)$, write $[x_0 : \ldots : x_n]$ for the corresponding point in $\mathbb{P}^n$ so $[\lambda x_0 : \ldots : \lambda x_n] = [x_0 : \ldots : x_n]$. Claim: $\mathbb{P}^n = \mathbb{A}^n \amalg \mathbb{P}^{n-1}$. Proof: Consider $[x_0 : \ldots : x_n] \in \mathbb{P}^n$. Either $x_n = 0$ or $x_n \neq 0$. If $x_n = 0$, $p = [x_0 : \ldots : x_{n-1} : 0]$, and $p = p' = [x'_0 : \ldots : x'_n]$ if and only if $x'_n = 0$ and $\lambda(x_0, \ldots, x_{n-1}) = (x'_0, \ldots, x'_{n-1})$ for some $\lambda \in k^\infty$, i.e. $p = p' \in \mathbb{P}^{n-1}$. If $x_n \neq 0$, then we can rescale $(x_0, \ldots, x_n) = x_n \cdot (\frac{x_0}{x_n}, \ldots, \frac{x_{n-1}}{x_n}, 1)$, so get $\{\, p \in \mathbb{P}^n \mid x_n \neq 0 \,\} \cong \mathbb{A}^n$. sending $[X_0 : \ldots : X_n] \to (\frac{X_0}{X_n}, \ldots, \frac{X_{n-1}}{X_n})$.

Example. $\mathbb{P}^1 = \mathbb{A}^1 \amalg \{\infty\}$ Also, $\mathbb{P}^2 = \mathbb{A}^2 \amalg \mathbb{P}^1 = \mathbb{A}^2 \amalg \mathbb{A}^1 \amalg \mathbb{A}^0$. If $k = \mathbb{F}^q$, the number of points in $\mathbb{P}^n$ is $1 + q + \ldots + q^n = \frac{q^{n+1}-1}{q-1}$.

To phrase the above claim without coordinates, choose $H \leq V$ a vector subspace of codimension 1, and $w_0 \in V \setminus H$. Then we have maps $\mathbb{P}H \hookrightarrow \mathbb{P}V \hookleftarrow H$ where the first map is $kv \mapsto kv$ and the second has $k(w_0 + h) \leftarrow\!\shortmid h$. This gives $\mathbb{P}V \setminus \mathbb{P}H \xleftarrow{\sim} H$, in particular $\mathbb{P}V \setminus \mathbb{P}H \cong \mathbb{A}^n$. So decomposition $\mathbb{P}V = \mathbb{P}H \amalg$ a space isomorphic to $\mathbb{A}^n$ depends only on the choice of a hyperplane H but the isomorphism $\mathbb{A}^n \to \mathbb{P}V \setminus \mathbb{P}H$ depends on choice of $w_0 \in V \setminus H$. Exercise: How does changing w_0 to w'_0 change the isomorphism?

So, $P^2 \twoheadleftarrow U_0 \amalg U_1 \amalg U_2$. We have $U_i \cap U_j = \{\, [x_0 : \cdots : x_n] \mid x_i \neq 0, x_j \neq 0 \,\} \cong \mathbb{A}^{n+1} \times (\mathbb{A}^1 \setminus \{0\})$. The congruence here follows by embedding $U_i \cap U_j \hookrightarrow U_i$, and the image is points where $x_j / x_i \neq 0$. In particular, we have $U_i \xrightarrow{\sim} \mathbb{A}^n$, with $x \mapsto (\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i})$, where $1 = x_i / x_i$ is omitted. So, this lets us see projective space as covered by open sets (analogous to charts on a manifold).

Definition. $X \subseteq \mathbb{P}^n$ is Zariski closed if $X \cap U_i$ is Zariski closed in $U_i = \mathbb{A}^n$ for each $i = 0, \ldots, n$.

Recall $E_0 = \{\, (x, y) \in A^2 \mid y^2 = x^3 - x \,\}$. Sit this inside $P^2 = [X : Y : Z]$ via $\mathbb{A}^2 \xrightarrow{\sim} U_2 = \{Z \neq 0\} \subseteq \mathbb{P}^2$. That is, $[X : Y : Z] \mapsto (x/z, y/z)$. So, $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$. The equation $y^2 = x^3 - x$ becomes $Y^2/Z^2 = X^3/Z^3 - X/Z$, and $Z \neq 0$ so the equation is $Y^2 Z = X^3 - XZ^2$ (for $Z \neq 0$). Hence, $E_0 = \{\, [X : Y : Z] \mid Y^2 Z = X^3 - XZ^2, Z \neq 0 \,\} \in \mathbb{P}^2$.

On the chart $Z \neq 0$, we have the original equation $y^2 = x^3 - x$. On $Y \neq 0$, take $x = \frac{X}{Y}$, $z = Z/Y$, i.e. set $Y = 1$, get $z = x^3 - xz^2$ for $z \neq 0$. For the chart $X \neq 0$, take $y = Y/X$, $z = Z/X$ get $y^2 z = 1 - z^2$ and $z \neq 0$. So now take the closure of E^0 in $\mathbb{P}^2$, which means ignore the condition $z \neq 0$. What, if any, extra points have we added? On the chart $Y \neq 0$, if $Z = 0$ get $x^3 = 0$ the unique extra point $[0 : 1 : 0]$ On the chart $X \neq 0$, if $Z = 0$ get $1 = 0$, no solutions, so no extra points are added. So, the closure of E^0 is $E_0 \amalg *$, just as we wanted.

More generally, if we have $I \leq k[x_1, \ldots, x_n]$ an ideal, $Z = Z(I) \subseteq \mathbb{A}^n$, we can ask what the closure of Z is in $\mathbb{P}^n$ using $\mathbb{A}^n \to \mathbb{P}^n$ given by $(x_1, \ldots, x_n) \mapsto [1 : x_1 : \cdots : x_n]$.

Definition. $f \in k[x_0, \ldots, x_n]$ is **homogeneous** of degree d (for $d \geq 0$) if

$$f = \sum a_{i_0,\ldots,i_n} x_0^{i_0} \cdots x_n^{i_n}$$

If k is infinite, this is equivalent to $f(\lambda x) = \lambda^d f(x)\ \forall \lambda \in k^\times$.

As we saw in the example, given $f \in k[x_1, \ldots, x_n]$ make f homogeneous: If $\deg f = d$, define $\tilde{f}(x_0, \ldots, x_n) = x_0^d f(x_1/x_0, \ldots, x_n/x_0)$ and then $\tilde{f}(1, x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$ and $\tilde{f}(\lambda x_0, \ldots, \lambda x_n) = \lambda^d \tilde{f}(x_0, \ldots, x_n)\ \forall \lambda \in k^\infty$ homogeneous of degree d. For example, if $f = y^2 - x^3 + x$, $\tilde{f} = z^3((y/z)^2 - (x/z)^3 + (x/z))$ as in our example. Define $\tilde{0} = 0$. Observe (i) if $f \neq 0$, then $x_0 \nmid \tilde{f}$, and conversely (ii) if $x_0 \nmid g$, $g \in k[x_0, \ldots, x_n]$ which is homogeneous of degree d, then $\tilde{g}(1, x_1, \ldots, x_n) = g$.

Definition. If $I \leq k[x_1, \ldots, x_n]$ an ideal, define $\tilde{I} = \langle \tilde{f} | f \in I \rangle$ the ideal generated by the $\tilde{f}$.

Warning. If $I = \langle f_1, \ldots, f_r \rangle$ it need not be the case that $\tilde{I} = \langle \tilde{f}_1, \ldots, \tilde{f}_r \rangle$

Example. (i) Take $I = \langle x - y^2, y \rangle$. Note this is $\langle x, y \rangle$ and so the zero set is $\{0\}$. Now, $\langle \widetilde{x - y^2}, \tilde{y} \rangle = \langle xz - y^2, y \rangle = \langle xz, y \rangle$ but $\tilde{I} = \langle \tilde{x}, \tilde{y} \rangle = \langle x, y \rangle$. (ii) Can you find an example of I where $\tilde{I} \neq \langle \tilde{f}_1, \ldots, \tilde{f}_r \rangle$ for any choice of $\langle f_1, \ldots, f_r \rangle = I$ which has r minimal.

Notice that every polynomial $f \in k[x_0, \ldots, x_n]$ can be written uniquely as $f = f_{(0)} + f_{(1)} + \ldots$ where $f_{(i)}$ is homogeneous of degree i.

Definition. An ideal I is homogeneous if whenever $f \in I$, then $f_{(d)} \in I$ for all d.

Example. $I = \langle xy + x^2, y^3, x^2 \rangle$ is homogeneous (follows from following lemma) while $\langle xy + y^3 \rangle$ is not.

Lemma.

(i) $I \leq k[x_0, \ldots, x_n]$ is homogeneous $\iff$ I is generated by a finite set of homogeneous polynomials.

(ii) Suppose k is infinite. $\tilde{Z} = Z(I)$ is Zariski clsoed and invariant under multiplication by $k^\times$ i.e. $p \in \tilde{Z} \iff \lambda p \in \tilde{Z},\quad \forall \lambda \in k^\times$ if and only if $I = I(\tilde{Z})$ is a homogeneous ideal.

Proof. (i) $\Rightarrow$. I is generated by some polynomials $g_1, \ldots, g_n$. If I is homogeneous, then the homogeneous parts $g_{i(j)}$ are in I, and they generate I.
$\Leftarrow$. If $I = \langle g_1, \ldots, g_n \rangle$, g_i homogeneous of degree d_i. Let $h \in I$, so $h = \sum f_i g_i$. We have to show that $h = \sum h_{(d)}$ has each piece $h_{(d)} \in I$. But write $f_i = \sum f_{i,(k)}$, each $f_{i,(k)}$ homogeneous of degree k. Then regroup the sum $\sum f_{i,(k)} g_k$ as $h_{(d)} = \sum_{i:\deg(g_i)=d-k} f_{i,(k)} g_i \in I$.

(ii) $\Leftarrow$. If $I = \langle g_1, \ldots, g_n$ with g_i homogeneous of degree d, then $g_i(\lambda p) = \lambda^{d_i} g_i(p) = 0$ if $g_i(p) = 0$, so $\tilde{Z}$ is invariant under $k^\times$.
$\Rightarrow$. The group $k^\times$ acts on $k[x_0, \ldots, x_n]$ as algebra automorphisms $\lambda * x_i = \lambda x_i$, with $(\lambda * f)(x_0, \ldots, x_n) = f(\lambda x_0, \ldots, \lambda x_n)$ and $Z(I)$ is $k^\times$ stable $\iff$ I is preserved by this action. That is, $f \in I \implies \lambda * f \in I$. So, let $f \in I$, $f = f_{(0)} + f_{(1)} + \cdots$ with $\deg f_{(i)} = i$. We must show $f_{(i)} \in I$. But $\lambda * f = f_{(0)} + \lambda f_{(1)} + \lambda^2 f_{(2)} + \cdots$ so if we pick $\lambda_0 = 1$,

$\lambda_1, \ldots, \lambda_n \in k^\times$.

$$\begin{aligned} f = &\lambda_0 * f = f_{(0)} + f_{(1)} + f_{(2)} + \cdots + f_{(n)} \\ &\lambda_1 * f = f_{(0)} + \lambda_1 f_{(1)} + \lambda_1^2 f_{(2)} + \cdots + \lambda_1^n f_{(n)} \\ &\vdots \lambda_n * f = f_{(0)} + \lambda_n f_{(1)} + \lambda_n^2 f_{(2)} + \cdots + \lambda_n^n f_{(n)} \end{aligned}$$

That is,

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & \lambda_1 & \ldots & \lambda_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_n & \ldots & \lambda_n^n \end{pmatrix} \begin{pmatrix} f_{(0)} \\ f_{(1)} \\ \vdots \\ f_{(n)} \end{pmatrix} = \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} * f$$

So if we choose $\lambda_i \neq \lambda_j$ for all $i \neq j$ (possible as $\#k$ infinite), the determinant is

$$\pm \prod_{i<j} (\lambda_i - \lambda_j) \neq 0$$

so we can invert the matrix and write $f_{(d)}$ as a linear combination of $\lambda_0 * f, \ldots, \lambda_n * f$ all of which are in I. Hence I is a homogeneous ideal. $\square$

Recall $V = \mathbb{A}^{n+1}$, $H \leq \mathbb{A}^{n+1}$ a hyperplane, e.g. $H = \{x_0 = 0\}$, pick $p_0 \in V \setminus H$.

$$\mathbb{A}^n = \mathbb{P}V \setminus \mathbb{P}H \hookrightarrow \mathbb{P}^n = \mathbb{P}V$$

$Z = Z(I) \subseteq \mathbb{A}^n \rightsquigarrow \tilde{I}$ a homogeneous ideal in $n+1$ variables, which generated the closure of Z inside $\mathbb{P}^n$. In particular, the homogeneous ideal can be seen as defining a closed subvariety $\tilde{Z}$ of $\mathbb{A}^{n+1}$ such that $p \in \tilde{Z}$, then $\lambda p \in \tilde{Z}$ $\forall \lambda \in k^\times$. This corresponds to a closed subvariety of $\mathbb{P}^n$ where $l \in$subvariety $\iff$ $l = kp = \langle p \rangle$ for $p \in \tilde{Z}$, $p \neq 0$. If $k = \overline{k}$, Nullstellensatz says this subvariety $\subseteq \mathbb{P}^n$ is non-empty.

$$\iff \tilde{Z} \supsetneq \{(0)\} \iff \text{ homogeneous ideal } I \subsetneq \langle x_0, \ldots, x_n \rangle$$

i.e. Zariski closed subvarieties of $\mathbb{P}^n$ $\leftrightarrow$ homogeneous ideals in $x_0, \ldots, x_n$ different from $\langle x_0, \ldots, x_n \rangle$.

Exercise. Show that (***) defines a bijection

Definition. A projective variety is a closed subvariety of $\mathbb{P}^n$, some n

An affine variety is $k[X] = k[x_1, \ldots, x_n]/I$, $I = \sqrt{I}$.

Definition. A quasi-affine variety is an open subvariety of an affine variety A quasi-projective variety is an open subvariety of a projective variety.

Exercise. If $\mathcal{U} \subseteq X$ an open subset of a variety X, $\exists$ structure of a variety on $\mathcal{U}$ makes the embedding a morphism of varieties.

3 Smooth points, dimension, Noether normalisation

Let $X \subseteq \mathbb{A}^n$ be an affine variety, $p \in X$. Write $X = Z(I)$, $I = \langle f_1, \ldots, f_r \rangle$. We would like to think about the tangent space to X at p, a vector space. Our tentative definition is

$$\begin{aligned} T_p X &= \{\, v \in \mathbb{A}^n \mid \sum v_i \frac{\partial f_j}{\partial x_i}(p) = 0, j = 1, \ldots, r \,\} \\ &= \{\, v \in \mathbb{A}^n \mid \sum v_i \frac{\partial f}{\partial x_i}(p) = 0, \forall f \in I \,\} \end{aligned}$$

For example, take $I = \langle y^2 - x^3 \rangle$. Then

$$T_{(p_1,p_2)} X = \{\, (v_1, v_2) \mid v_1(-3p_1^2) + v_2(2p_2) = 0, -3p_1^2 v_1 + 2p_2 v_2 = 0 \,\}$$

So if $(p_1, p_2) \neq (0,0)$ then $T_{(p_1,p_2)}X$ is a line, and if $(p_1,p_2) = (0,0)$ then $T_{(p_1,p_2)}X = \mathbb{A}^2$.

Remark. You can think of T_pX as sitting at $p \in X$, by translating $v \mapsto v + p$. So,

$$\simeq \{\, v \in \mathbb{A}^n \mid \sum (v_i - p_i) \frac{\partial f}{\partial x_i}(p) = 0, \forall f \in I \,\}$$

We can think of this as a linear approximation to the variety, $f(x) = f(p) + \sum (x_i - p_i) \frac{\partial f}{\partial x_i} +$ higher order terms.

Lemma.

$$\{\, p \in X \mid \dim T_p X \geq d \,\}$$

is a Zariski closed subvariety of X, for all $d \geq 0$.

Proof.

$$T_p X = \ker \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_r}{\partial x_1} & \cdots & \frac{\partial f_r}{\partial x_n} \end{bmatrix}$$

and recall $\dim(\ker A) + r(A) = 0$. So, $\dim \ker \geq d \iff n - \mathrm{rank} \geq d \iff rank \leq n - d$. But the rank of a matrix is greater than $a \iff$ exists some $a \times a$ submatrix with non-zero determinant. So, $\mathrm{rank}(\frac{\partial f_j}{\partial x_i}) \leq d \iff$ all $(n-d+1) \times (n-d+1)$ subminors have zero determinant which is a collection of polynomial equations. That is, $I\{\, p \in X \mid \dim T_p X \geq d \,\} = \langle f_1, \ldots, f_r, \text{ determinants of all subminors} \rangle$. $\square$

The problem with the definition from earlier was that it depends on an embedding, and we want a definition of T_pX which doesn't depend on embedding $X \hookrightarrow \mathbb{A}^n$.

Definition. Take A an algebra over k, and $\phi : A \to k$ a homomorphism. (For example, take $A = k[X]$, $\phi = \mathrm{ev}_p : f \mapsto f(p)$.) A **derivation** 'centered at ϕ' is a k-linear map $D : A \to k$ such that

$$D(fg) = Df\phi(g) + \phi(f)Dg \qquad \text{(Leibniz rule)}$$

Write $\mathrm{Der}(A, \phi)$ for the set of such derivations, a vector space over k.

Example. Take $A = k[x_1, \ldots, x_n]$, $p \in \mathbb{A}^n$. If $(v_1, \ldots, v_n) \in \mathbb{A}^n$, then $D(f) = \sum v_i \frac{\partial f}{\partial x_i}(p)$ is a derivation centered at ev_p. Moreover, it is the unique derivation with $D(x_i) = v_i$.

Exercise. Show it is unique.

Conversely, given $D \in \operatorname{Der}(k[x_1,\dots,x_n],\mathrm{ev}_p)$, get $v_i = D(x_i)$ so $\operatorname{Der}(k[x_1,\dots,x_n],\mathrm{ev}_p) = T_p\mathbb{A}^n$. More generally,

Lemma. Let $A = k[x_1,\dots,x_n]/\langle f_1,\dots,f_r\rangle = k[X]$ and take $p \in X$.

$$\operatorname{Der}(A,\mathrm{ev}_p) = \{\, D = \sum v_i \frac{\partial}{\partial x_i} \mid {}_p|D\langle f_1,\dots,f_r\rangle = 0 \text{ in } k[X] \,\}$$

Proof. Can be seen as above. Alternatively, $\operatorname{Der}(k[X],\mathrm{ev}_p)$ determines $\tilde{D} \in \operatorname{Der}(k[x_1,\dots,x_n],\mathrm{ev}_p)$ and then the condition $\tilde{D}$ descends to a map $k[X] \to k$ is the condition $D\langle f_1,\dots,f_r\rangle = 0$. $\square$

This gives us a better definition of tangent space:

Definition (Intrinsic definition of tangent space)**.**

$$T_pX = \operatorname{Der}(k[X],\mathrm{ev}_p).$$

We can almost immediately conclude that this gives a definition for any algebraic variety.

Exercise. Let $V = X \setminus Z(f)$, $f \in k[X]$ be a Zariski open affine subvariety of X, i.e.

$$k[V] = k[X][\frac{1}{f}].$$

Show $T_pX \cong T_pX$ a canoncial isomorphism, i.e. that $\operatorname{Der}(k[X][\frac{1}{f}],\mathrm{ev}_p) \xrightarrow{\sim} \operatorname{Der}(k[X],\mathrm{ev}_p)$.

So now $T_pX = T_pU$, for U any Zariski open subvariety: the tangent space is Zariski local.

Example. Take $X = \mathbb{P}^n$, $p = [p_0 : p_1 : \dots : p_n]$. If $p_0 \neq 0$, $p = [1 : \frac{p_1}{p_0} : \dots : \frac{p_n}{p_0}] = \iota(\bar{p})$, the embedding of some $\bar{p} \in \mathbb{A}^n \hookrightarrow \mathbb{P}^n$. THen

$$T_p\mathbb{P}^n = T_{\bar{p}}\mathbb{A}^n = \mathbb{A}^n$$

Definition. Let X be irreducible. Then the **dimension** of X:

$$\dim X \coloneqq \min\{\, \dim T_pX \mid p \in X \,\}$$

Example. $\dim A^n = n = \dim \mathbb{P}^n$, $\dim\{\, (x,y) \mid y^2 = x^3 \,\} = 1$.

If X is not irreducible, the dimension is not such a great concept.

Definition. If X is arbitrary, $\dim X \coloneqq \max \dim X_i | X_i$ a component of X.

Definition. If X is irreducible, $p \in X$ is **smooth** if $\dim T_pX = \dim X$, and singular otherwise and we've shown singular points in X form a Zariski closed subvariety, whose complement is non-empty.

Lemma. Let $f \in k[x_1,\dots,x_n]$ be prime. Then $\dim Z(f) = n-1$. Call this a 'hypersurface'.

Proof. $T_pZ(f)$ has dimension n or $n-1$, and $T_pZ(f) = \mathbb{A}^n \iff \forall i\ \frac{\partial f}{\partial x_i} = 0$. So $T_pZ(f)$ has dimension n for all $p \in Z(f) \implies \frac{\partial f}{\partial x_i} \in I(Z(f)) \quad \forall i = 1,\dots,n$. But $I(Z(f)) = \sqrt{f}$, by Nullstellensatz, so $= (f)$ as f is prime. So, $\frac{\partial f}{\partial x_i} = f.g$ for some g. But $\deg x_i \frac{\partial f}{\partial x_i} < \deg_{x_i} f \implies g = 0$. So $\dim Z(f) = 0 \implies \frac{\partial f}{\partial x_i} = 0 \quad \forall i$. There are now two cases,

(i) if $\operatorname{char} k = 0$, this implies $f = 0$.

(ii) if $\operatorname{char} k = p$, this implies $f \in k[x_1^p, \ldots, x_n^p]$ as $\frac{\partial(x^p)}{\partial x} = px^{p-1} = 0$.

Claim: $\exists g \in k[x_1, \ldots, x_n]$ such that $g(x)^p = f(x)$. Proof: If $f = \sum a_\lambda x^{\lambda p}$, $g = \sum a_\lambda^{1/p} x^\lambda$ (for $a_\lambda \in k$) which requires can take pth roots of things in k, which is allowed if $k = \bar{k}$. But this contradicts f is prime! $\square$