

# Part II – Algebraic Geometry

Based on lectures by Prof. I. Grojnowski

Notes taken by Bhavik Mehta

Lent 2017

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  $p : E \rightarrow \mathbb{C}$  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 (pic) by adding a point at  $\infty$ , so it lives on the Riemann surface.

Take another copy, flip it over and glue back.

## 1 Dictionary between algebra and geometry

### 1.1 Basic notions

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

Write  $k[\mathbb{A}^n] = k[x_1, \dots, x_n]$  polynomials in  $n$  variables. Any  $f \in k[\mathbb{A}^n]$  defines a function  $f : \mathbb{A}^n = k^n \rightarrow k$  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) in  $\mathbb{A}^2$ ,  $E = Z(y^2 - x^3 + x)$  we have sketched when  $k = \mathbb{C}$  and  $k = \mathbb{R}$ .

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

Observe that if  $J$  is the ideal generated by  $S$

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

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)  $Z(0) = \mathbb{A}^n$ ,  $Z(k[x_1, \dots, x_n]) = \emptyset$ .
- (iii)  $Z(\bigcup J_i) = Z(\sum J_i) = \bigcap Z(J_i)$  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  $x \notin Z(I \cap J)$ .  $\square$

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

If  $Z \subset \mathbb{A}^n$  is any subset, let  $I(Z) = \{ f \in k[\mathbb{A}^n] \mid f(p) = 0, \forall p \in Z \}$ . 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  $J \triangleleft k[\mathbb{A}^n] = k[x_1, \dots, x_n]$  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.

Take  $\mathbb{Z} \subseteq \mathbb{C} = \mathbb{A}^1$ ,  $k = \mathbb{C}$  the closure of  $\mathbb{Z}$  in Zariski topology is  $\mathbb{C}$ .  $I(\mathbb{Z}) = \{0\}$  as if a poly vanishes at every integer it is 0. 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  $Z \implies$  closed in the usual topology. So,

$$\{\text{Zariski closed subvarieties of } \mathbb{A}^n\} \quad \{\text{ideals in } k[x_1, \dots, x_n]\}$$

But this is not a bijection  $Z(X) = Z(X^2) = Z(X^3) = \dots = \{0\} \subseteq \mathbb{A}^1$ .  $Z(\langle f_1^{a_1}, \dots, f_r^{a_r} \rangle) = Z(f_1, f_2, \dots, f_r)$ . but it turns out this kind of thing is the only problem

**Definition.** An affine variety  $Y$  is **reducible** if  $\exists$  affine varieties  $Y_1, Y_2$ ,  $Y_i \neq Y$  with  $Y = Y_1 \cup Y_2$ , and irreducible otherwise, and disconnected if  $Y_1 \cap Y_2 = \emptyset$ .

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

$$Y_1 = Y_2 \cup Y'_2, \dots$$

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

**Exercise.** If  $Y$  is a subvariety of  $\mathbb{A}^n$ ,  $Y = Y_1 \cup \dots \cup Y_r$  with  $Y_i$  irreducible, and  $r$  minimal is unique up to reordering. Call the  $Y_i$  the irreducible components of  $Y$ .

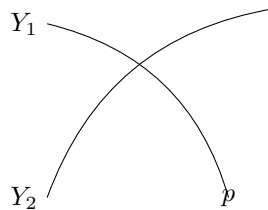
**Proposition.**  $Y$  is irreducible  $\iff I(Y)$  is a prime ideal in  $k[\mathbb{A}^n] = k[x_1, \dots, x_n]$ .

**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:  $k[x_1, \dots, x_n]$  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,  $\exists g \in Y_2 \setminus Y_1$  so  $\exists g \in I(Y_1)$  such that  $g(p) \neq 0$ . 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  $Y_i = Y_n \cap Z(f_i) = \{p \in Y \mid f_i(p) = 0\}$ .  $Y_1 \cup Y_2 = Y$ , 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.  $\exists p_i \in Y$  such that  $f_i(p_i) \neq 0$  so  $p_i \notin Y_i$ ).  $\square$

**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  $\mathcal{U} \neq \emptyset \implies Y \neq X$ . But  $X$  is irreducible, so  $\overline{\mathcal{U}} = X$ .  $\square$

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

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

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

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

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

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

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

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

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

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  $A \in \mathcal{U} \iff \text{char}_A(x) \in k[x]$  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  $A \in \mathcal{U} \iff D(\text{char}_A(x)) \neq 0$  is a polynomial in matrix coefficients of  $A$ .  $\square$

## 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

$$\begin{array}{ccc} k[\mathbb{A}^n] & \longrightarrow & \{\text{functions from } k^n = \mathbb{A}^n \rightarrow k\} \\ & \searrow & \downarrow \\ & & \{\text{functions from } Y \rightarrow k\} \end{array}$$

where the composite is constructed by restricting a function from  $\mathbb{A}^n \rightarrow k$  to  $Y \rightarrow k$ . 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  $k[Y] \rightarrow \{\text{all functions from } Y \rightarrow k\}$  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  $k[Y] \rightarrow k$ , 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  $k = \bar{k}$ , there are no other algebra homomorphisms  $k[Y] \rightarrow k$  other than evaluating at points  $p \in Y$ , and if  $k \neq \bar{k}$  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  $k \subseteq \bar{k}$  that means  $k = \bar{k}$  algebraic over  $k$ . Now let  $a_i$  be the image of  $x_i$  in  $A$ , and  $M$  is as stated. So if  $k = \bar{k}$ , solutions of equations  $I \iff$  max ideal  $M \subseteq k[Y] \iff$  alg homomorphisms  $k[Y] \rightarrow k$  and if  $k \neq \bar{k}$ , then they are 'galois orbits of solutions over bigger fields'.  $\square$

We can interpret this in the case  $k \neq \bar{k}$  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  $\bar{k}$ .

*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  $\frac{1}{t-\lambda_1}, \dots, \frac{1}{t-\lambda_r}$  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.  $\square$

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

Note if  $k \neq \bar{k}$ , 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  $Z(I) \supseteq Z(m) = \{p\} \neq \emptyset$ .  $\square$

**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,  $J \triangleleft R$  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  $f + g \in \sqrt{J}$ .  $\square$

**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  $k = \bar{k}$ ,  $I(Z(J)) = \sqrt{J}$ .

*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  $k[x_1, \dots, x_n, t]/tf - 1 := k[x_1, \dots, x_n, \frac{1}{f}]$ . Let  $i$  be the ideal of this, generated by the image of  $J$ . Claim:  $Z(i) = \emptyset$ . 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  $k[x_1, \dots, x_n, t]/tf - 1 \leftarrow k[\mathbb{A}^{n+1}]$ . 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 let's deduce some consequences of Nullstellensatz version 2.

**Corollary.** If  $k = \bar{k}$ ,  $Z(I) = Z(J) \iff I(Z(I)) = I(Z(J)) \iff \sqrt{I} = \sqrt{J}$ . 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  $J \geq k[x_1, \dots, x_n]$  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  $k[x_1, \dots, x_n] \xrightarrow{\alpha} k[X]$  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  $k = \bar{k}$ , this coincides with our previous definition.
- (ii) if  $k \neq \bar{k}$ , we get new examples, now  $\mathbb{R}[x, y]/x^2 + y^2 + 1$  is an affine algebraic variety over  $\mathbb{R}$  even though  $Z(x^2 + y^2 + 1) = \emptyset$ . Note Nullstellensatz says  $\mathbb{R}[x, y]/x^2 + y^2 + 1$  still has lots of maximal ideals but they correspond to  $\text{Gal}(\mathbb{C}/\mathbb{R})$  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  $X \rightarrow Y$  is a  $k$ -algebra homomorphism  $f^* : k[Y] \rightarrow k[X]$ . Write  $\text{Mor}(X, Y)$  for the set of morphisms, and write  $f$  for the morphism associated to  $f^*$ .

Let us unpack this definition. Write

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

and write  $\overline{y}_1, \dots, \overline{y}_m$  for the images of  $y_i$  in  $k[Y]$ . An algebra homomorphism  $f^* : k[Y] \rightarrow k[X]$  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

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

Now the condition that this determines an algebra homomorphism  $k[Y] \rightarrow k[X]$  is the condition that  $r_i(\Phi_1, \dots, \Phi_m) = 0$  in  $k[X] \quad \forall i$  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  $X \rightarrow Y$ , denoted  $f : X \rightarrow Y$ ,  $x \mapsto (\Phi_1(x), \dots, \Phi_m(x))$ . So, a morphism of algebraic varieties  $f : X \rightarrow Y$  is, roughly speaking, a map of sets  $X = (X_1, \dots, X_n) \in X \rightarrow f(x) = (\Phi_1(x), \dots, \Phi_m(x)) \in Y$  (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  $\exists \alpha^* : k[Y] \rightarrow k[X]$ ,  $\beta^* : k[X] \rightarrow k[Y]$  such that  $\alpha^* \beta^*$  and  $\beta^* \alpha^*$  are identity.

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

(ii) Take  $\text{Mor}(X, \mathbb{A}^1) \ni \varphi^*$ , then  $\varphi^* k[t] \rightarrow k[X]$  an algebra homomorphism.  $k[t]$  is the free  $k$ -algebra on 1 generator  $t$ . That is, to specify an algebra homomorphism  $k[t] \rightarrow R$  (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  $\text{Mor}(X, \mathbb{A}^1) = k[X]$ .

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