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.

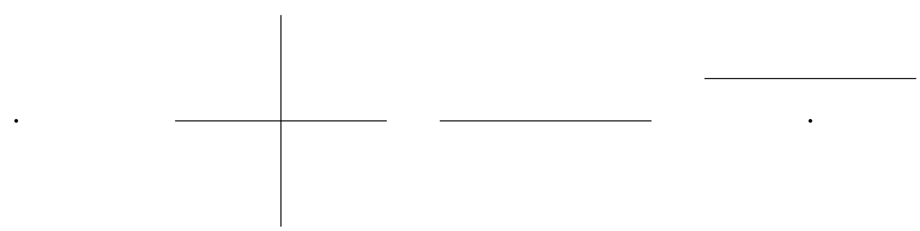
(i) $\mathbb{A}^n = Z(0)$.

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

Lemma.

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

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

(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

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

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 $J \lhd k[\mathbb{A}^n] = k[x_1, \ldots, x_n]$ 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 $k = \mathbb{C}$, $f \in \mathbb{C}[x_1, \ldots, x_n]$, 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

$$\begin{tikzcd}
\left\{\begin{matrix}\text{Zariski closed}\\ \text{subvarieties of } \mathbb{A}^n\end{matrix}\right\} \arrow[rr, bend right, hook, "I"'] & & \left\{\begin{matrix}\text{ideals in}\\ k[x_1,\dots,x_n]\end{matrix}\right\} \arrow[ll, bend right, two heads, "Z"']
\end{tikzcd}$$

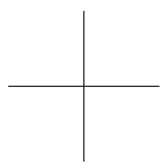
But this is not a bijection. For instance,

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

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.

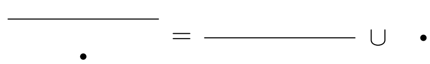
Definition (Reducible)**.** An affine variety Y is **reducible** if there are affine varieties Y_1, Y_2, $Y_i \neq Y$ with $Y = Y_1 \cup Y_2$, and **irreducible** otherwise. It is called **disconnected** if $Y_1 \cap Y_2 = \varnothing$.

Example.

$Z(xy) =$  $= Z(x) \cup Z(y)$, reducible

Also,

$$Z(y(y-1), x(y-1)) = Z(y-1) \cup Z(x,y), \text{ reducible and disconnected}$$



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

$$Y_1 = Y_2 \cup Y_2', \quad Y_2 = Y_3 \cup Y_3', \quad \ldots$$

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 ideals I_i. Let

$$W = \bigcap Y_i = Z\left(\sum I_i\right) = Z(I)$$

where $I \coloneqq \sum I_i$ is certainly an ideal. Ideals are finitely generated, by the Hilbert basis theorem, so $I = \langle f_1, \ldots, f_r \rangle$ for some f_i. $f_i \in I_{a_i}$ for some $a_1, \ldots, a_r$ so $I = I_{a_1} + \cdots + I_{a_r}$. Then $W = Y_{a_1} \cap \cdots \cap Y_{a_r}$, contradicting $Y_N \subsetneq Y_{a_1} \cap \cdots \cap Y_{a_r}$ if $N > \max(a_1, \ldots, a_r)$. $\square$

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.

Definition (Prime ideal)**.** A proper ideal I of a ring R is **prime** if $ab \in I$ for some $a, b \in R$, then either $a \in I$ or $b \in I$.

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

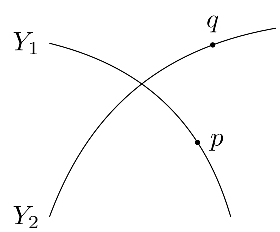
Example.

(i) $\langle xy \rangle$ is not a prime ideal.

(ii) Exercise: Let R be a UFD, $f \in R$, $f \neq 0$, then f is an irreducible polynomial $\iff$ $\langle f \rangle$ a prime ideal.

(iii) Exercise: $k[x_1, \ldots, x_n]$ is a UFD. Hence $Z(y^2 - x^3 + x)$ is irreducible, and $Z(y - x^2)$ 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 $f(p) \neq 0$. 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 $I(Y)$ is 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

$$Y_i \coloneqq Y \cap Z(f_i) = \{\, p \in Y \mid f_i(p) = 0 \,\}.$$

$Y_1 \cup Y_2 = Y$, as $p \in Y \Rightarrow f_1 f_2(p) = 0$ so either $f_1(p) = 0$ or $f_2(p) = 0$. Finally we must show $Y_i \neq Y$. But $f_i \notin I(Y)$, so $\exists p_i \in Y$ such that $f_i(p_i) \neq 0$ so $p_i \notin Y_i$. □

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

Proof. Let $Y = X - \mathcal{U}$, which is closed. Then $\overline{\mathcal{U}} \cup Y = X$, and $\mathcal{U} \neq \varnothing \Rightarrow Y \neq X$. 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. $\square$

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

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

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 is infinite.

Definition (Polynomial functions on subvariety)**.** Let

$$k[Y] \coloneqq k[x_1, \dots, x_n]/I(Y)$$

called 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 is infinite. We've also seen Y irreducible $\iff$ $I(Y)$ is prime $\iff$ $k[Y]$ is an integral domain.

Now let $p \in Y$. We have a map

$$\begin{aligned} k[Y] &\longrightarrow k \\ f &\longmapsto f(p) \end{aligned}$$

This is a k-algebra homomorphism, so the kernel

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

is an ideal. In particular, it is a maximal ideal, since here we have $k[Y]/\mathfrak{m}_p = k$, a field. (The homomorphism is surjective as constants go to constants).

A natural question to ask now is: are any other maximal ideals in $k[Y]$? In particular, what are the possible surjective k-algebra homomorphisms

$$k[x_1, \dots, x_n] \longrightarrow\!\!\!\!\!\rightarrow L$$

with L a field extension of k.

For instance, taking $k = \mathbb{R}$, we can take the homomorphism given by the quotient map $\mathbb{R}[x] \twoheadrightarrow \mathbb{R}[x]/\langle x^2 + 1\rangle$. This is surjective, and has image isomorphic to $\mathbb{C}$, so we have a new k-algebra homomorphism whose image is not just k.

Claim: If k is algebraically closed, there are no k-algebra homomorphisms $k[Y] \to k$ other than evaluating at points $p \in Y$, (so the only surjections are onto k), and if $k \neq \overline{k}$ the only additional homomorphisms have L an algebraic extension of k.

Remark. Take $\mathfrak{m} \subseteq k[x_1, \dots, x_n]$ be a maximal ideal, and take $A = k[x_1, \dots, x_n]/\mathfrak{m}$. Then A is finite dimensional as a k-vector space $\iff$ every $a \in A$ is algebraic over k.

Proof. ($\Rightarrow$) is clear, as $1, a, a^2, \dots$ can't all be linearly independent over k.

($\Leftarrow$) The images of $x_1, \dots, x_n$ in A each satisfy an algebraic relation over k and they generate A. □

Theorem (Nullstellensatz, version 1)**.** Let $\mathfrak{m} \subseteq k[x_1, \dots, x_n]$ be a maximal ideal, and set $A = k[x_1, \dots, x_n]/\mathfrak{m}$, a field extension of k. Then A is finite dimensional over k.

Proof. When k is uncountable: If the result is not true, $\exists t \in A \setminus k$ with t transcendental over k by the earlier remark. In particular, $k(t) \subseteq A$. So $\forall \lambda \in k$, $\frac{1}{t-\lambda} \in A$.

But A has countable dimension over k: Let V_d be the k-vector space which is the image of $\{\, f \in k[x_1, \dots, x_n] \mid \deg f \leq d \,\}$ in A. V_d is finite dimensional, and $\bigcup_d V_d = A$.

Now we aim to reach a contradiction by constructing an uncountable linearly independent set:

$$\left\{ \frac{1}{t - \lambda} \;\middle|\; \lambda \in k \right\} \subseteq A$$

This is certainly uncountable. Suppose it is linearly dependent, then there are $\lambda_1, \ldots, \lambda_r \in k$ distinct with

$$\sum_{i=1}^{r} \frac{a_i}{t-\lambda_i} = 0, \quad a_i \in k.$$

Then clearing denominators gives a polynomial relation in t, contradicting t is transcendental. Hence the set was linearly independent but uncountable, contradicting that A has countable dimension. $\square$

Corollary. If k is algebraically closed, then $k \hookrightarrow A$ is an isomorphism, i.e. $A \cong k$. That is, every maximal ideal is of the form $\mathfrak{m} = \langle x_1 - p_1, \ldots, x_n - p_n \rangle$ for $p \in k^n$.

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

Proof. As $\mathfrak{m}$ is a maximal ideal, A is a field. By the Nullstellensatz, A is algebraic over k, but k is algebraically closed, so $A \cong k$. Now let a_i be the image of x_i in A, and M is as stated. $\square$

Corollary. For $k = \overline{k}$, take $I \lhd k[x_1, \ldots, x_n]$ an ideal. Then

$$Z(I) \neq \varnothing \iff I \neq k[x_1, \ldots, x_n].$$

More generally, for $I \leq k[Y]$, with $Y \subset \mathbb{A}^n$ a subvariety,

$$Z(I) \neq \varnothing \iff I \neq k[Y].$$

Note if $k \neq \overline{k}$, this is obviously false (for instance, $I = \langle x^2 + 1 \rangle \in \mathbb{R}[x]$).

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

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

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

Definition (Radical of 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

$$(f+g)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} f^i g^{n+m-i}.$$

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) $\sqrt{\langle x^n \rangle} = \langle x \rangle$ in $k[x]$.

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

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

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

Theorem (Nullstellensatz, version 2)**.** If k is algebraically closed, then for any ideal $J \lhd k[x_1, \dots, x_n]$, $I(Z(J)) = \sqrt{J}$.

Proof. Let $f \in I(Z(J))$, i.e. $\forall p \in Z(J), f(p) = 0$. We must show that $\exists n$ such that $f^n \in J$. Consider $k[x_1, \dots, x_n, t]/\langle tf - 1 \rangle =: k[x_1, \dots, x_n, \frac{1}{f}]$. Let I be the ideal 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 deduce some consequences of Nullstellensatz version 2.

Corollary. If k is algebraically closed,

$$\begin{aligned} Z(I) = Z(J) &\iff I(Z(I)) = I(Z(J)) \\ &\iff \sqrt{I} = \sqrt{J}. \end{aligned}$$

So we have a bijection

$$\begin{tikzcd} \left\{ \begin{array}{c} \text{Zariski closed} \\ \text{subvarieties of } \mathbb{A}^n \end{array} \right\} \arrow[r, bend right, "I"'] & \left\{ \begin{array}{c} \text{Ideals } I \lhd k[x_1, \dots, x_n] \\ \text{such that } \sqrt{I} = I \end{array} \right\} \arrow[l, bend right, "Z"'] \end{tikzcd}$$

$$\text{irreducible varieties} \longleftrightarrow \text{prime ideals}$$

$$\text{points} \longleftrightarrow \text{maximal ideals}$$

The intrinsic definition of affine varieties is a consequence (doesn't depend on the embedding of $X \hookrightarrow \mathbb{A}^n$). To explain, we need some more definitions.

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

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

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

Definition (Algebra over a field)**.** For a field k, a k**-algebra** is a vector space with an additional commutative binary operation of multiplication which distributes in the usual way, and is compatible with scalars in the usual way. Alternatively, a k-algebra is a commutative ring which is also a vector space over k (and scalar multiplication is compatible as expected).

Definition (Algebra homomorphism)**.** For a field k, a k-algebra homomorphism between k-algebras A,B is a k-linear map $f : A \to B$ such that $f(xy) = f(x)f(y)$ for all $x, y \in A$.

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.

Finitely generated here means there is $k[x_1, \dots, x_n] \overset{\alpha}{\twoheadrightarrow} k[X]$ a surjective algebra homomorphism and we know there are no non-zero nilpotents $\iff \ker \alpha$ is a radical ideal.

We can now give an improved definition of an affine variety:

Definition (Affine variety)**.** 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, by the earlier corollary.

(ii) if $k \neq \overline{k}$, we get new examples, now $\mathbb{R}[x, y]/\langle x^2 + y^2 + 1 \rangle$ is an affine algebraic variety over $\mathbb{R}$ even though $Z(x^2 + y^2 + 1) = \varnothing$. Note Nullstellensatz says $\mathbb{R}[x, y]/\langle x^2 + y^2 + 1 \rangle$ 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 and not just corresponding to points of $Z(x^2 + y^2 + 1)$.

(iii) this definition does not explicitly refer to a choice of embedding $X \hookrightarrow \mathbb{A}^n$ (this is 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 $f : X \to Y$ 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

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

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 $\overline{y_i} \mapsto f^*(\overline{y_i})$. For each $i = 1, \dots, m$, 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

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

Now the condition that this determines an algebra homomorphism $k[Y] \to k[X]$ is the condition that

$$r_i(\Phi_1, \dots \Phi_m) = 0 \text{ in } k[X] \quad \forall i = 1, \dots, k$$

i.e. the ideal $\langle r_1, \dots, r_k \rangle$ gets 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 these polynomials is well defined, up to adding any element of $\langle s_1, \dots, s_l \rangle$).

Moreover, f^* determines a map of sets

$$\begin{aligned} f : X &\longrightarrow Y \\ x &\longmapsto (\Phi_1(x), \dots, \Phi_m(x)). \end{aligned}$$

So, a morphism of affine varieties $f : X \to Y$ is, roughly speaking, a map of sets

$$x = (X_1, \dots, X_n) \in X \longmapsto f(x) = (\Phi_1(x), \dots, \Phi_m(x)) \in Y$$

(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

$$\begin{aligned} &\exists \alpha^* : k[Y] \to k[X] \\ &\exists \beta^* : k[X] \to k[Y] \end{aligned}$$

such that $\alpha^* \circ \beta^* = \mathrm{id}$ and $\beta^* \circ \alpha^* = \mathrm{id}$.

Example.

(i) $t \mapsto (t^2, t^3)$ is a morphism $\mathbb{A}^1 \to \mathbb{A}^2$. More generally,

$$\mathrm{Mor}(\mathbb{A}^1, \mathbb{A}^n) = \{k\text{-algebra homomorphisms } k[x_1, \dots, x_n] \to k[t]\}$$

and each of these is just a tuple of polynomials $(\phi_1(t), \dots, \phi_n(t)) \in k[t]^n$.

(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 one generator t. Then 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) Take $X = \mathbb{A}^1$, $Y = \{\, (x, y) \mid x^2 = y^3 \,\} = Z(x^2 - y^3)$. 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 trivial map). Do there exist polynomials $a = a(t), b = b(t) \in k[t]$, not both constant such that $b^2 = a^3 - a$?

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

$$\text{points of } x \longleftrightarrow \text{maximal ideals } \mathfrak{m} \text{ of } k[X] \longleftrightarrow \text{algebra homomorphisms } k[X] \to k$$

Now, observe if $f^* : k[Y] \to k[X]$ and $x \in X$, we have $\mathrm{ev}_x : k[X] \to k$. Composing

$$\begin{tikzcd} k[Y] \arrow[r, "f^*"] \arrow[dr, "\mathrm{ev}_x \circ f^*"'] & k[X] \arrow[d, "\mathrm{ev}_x"] \\ & k \end{tikzcd}$$

we get an algebra homomorphism $\mathrm{ev}_x \circ f^* : k[Y] \to k$, so the kernel is a maximal ideal $\mathfrak{m}_y$ for some $y \in Y$ and $f(x) = y$. Exercise: Check $f(x) = y$.

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 projection map $Y \hookrightarrow X$ with $(p,t) \mapsto p$ is a morphism of affine algebraic varieties.

Proof. It is $k[X] \to k[Y] \coloneqq k[X][t]/\langle tf - 1\rangle$. 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 and $\dim V = n+1$ for $n \geq 0$.

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

That is, if $v \in V$, $v \neq 0$ then $kv = \{\, \lambda v \mid \lambda \in k \,\}$ is a line through 0. Conversely if $l \in \mathbb{P}V$ then $l = kv$ for some $v \in l \setminus \{0\}$.

Concretely, we can choose a basis $e_0, \ldots, e_n$ of V, and write $V \cong k^{n+1}$, under

$$\sum_{i=0}^{n} x_i e_i \longleftrightarrow (x_0, \ldots, x_n).$$

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

$$\forall \lambda \in k^\times \quad [\lambda x_0 : \ldots : \lambda x_n] = [x_0 : \ldots : x_n].$$

Lemma. $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$.

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 $\lambda \in k^\times$, 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

$$\{\, p \in \mathbb{P}^n \mid x_n \neq 0 \,\} \simeq \mathbb{A}^n,$$

using the map sending

$$[x_0 : \ldots : x_n] \longmapsto \left(\frac{x_0}{x_n}, \ldots, \frac{x_{n-1}}{x_n} \right). \qquad \square$$

Example. In the case $k = \mathbb{R}$, we have the following picture of $\mathbb{P}^1$: (currently missing, but it looks like a circle)

$$\begin{aligned} \mathbb{P}^1 &= \mathbb{A}^1 \sqcup \{\infty\} \\ \mathbb{P}^2 &= \mathbb{A}^2 \sqcup \mathbb{P}^1 = \mathbb{A}^2 \sqcup \mathbb{A}^1 \sqcup \mathbb{A}^0 \end{aligned}$$

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 lemma without coordinates, choose $H \leq V$ a vector subspace of codimension 1, and $w_0 \in V \setminus H$. For instance, we could use $H = \{\, (x_0, \ldots, x_n) \in V \mid x_n = 0 \,\}$ and $w_0 = (0, 0, \ldots, 0, 1)$. Then we have maps

$$\begin{array}{ccccc} \mathbb{P}H & \hookrightarrow & \mathbb{P}V & \hookleftarrow & H \\ kv & \longmapsto & kv & & \\ & & k(w_0 + h) & \longleftarrow\!\!\shortmid & h \end{array}$$

As the image of H is disjoint from $\mathbb{P}H$, this gives $\mathbb{P}V \setminus \mathbb{P}H \xleftarrow{\sim} H$, in particular $\mathbb{P}V \setminus \mathbb{P}H \simeq \mathbb{A}^n$. So the decomposition $\mathbb{P}V = \mathbb{P}H \sqcup$ (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 the choice of $w_0 \in V \setminus H$.

Exercise. How does changing w_0 to w_0' change the isomorphism?

We want to give $\mathbb{P}^n$ the structure of an algebraic variety, but a decomposition like this is not enough: $\mathbb{A}_1$ and $Z(x^2 = y^3)$ both decompose as $(\mathbb{A}^1 \setminus \{0\}) \sqcup \{0\}$, but they are not isomorphic. Instead, cover $\mathbb{P}^n$ with n copies of $\mathbb{A}^n$, and inherit structure from the copies.

Pictures missing

Define

$$\begin{aligned} H_i &= \{\, (x_0, \ldots, x_n) \mid x_i = 0 \,\} \subset k^{n+1} \\ \mathbb{P}H_i &= \{\, [x_0 : \ldots : x_n] \mid x_i = 0 \,\} \\ U_i &= \{\, [x_0 : \ldots : x_n] \mid x_i \neq 0 \,\} = \mathbb{P}^n \setminus \mathbb{P}H_i \end{aligned}$$

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 $U_i \cap U_j \hookrightarrow U_i$; the image is points where $x_j/x_i \neq 0$. In particular,

$$\begin{aligned} U_i &\longrightarrow \mathbb{A}^n \\ x &\longmapsto \left(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\right) \end{aligned}$$

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 (Zariski closed in projective space)**.** $X \subseteq \mathbb{P}^n$ is **Zariski closed** if $X \cap U_i$ is Zariski closed in $U_i (\simeq \mathbb{A}^n)$ for each $i = 0, \ldots, n$.

Recall $E_0 = \{\, (x, y) \in \mathbb{A}^2 \mid y^2 = x^3 - x \,\}$. Sit this inside $\mathbb{P}^2$ with coordinates $[X : Y : Z]$ by considering the map

$$\begin{aligned} U_2 = \{\, [X : Y : Z] \mid Z \neq 0 \,\} \subseteq \mathbb{P}^2 &\longrightarrow \mathbb{A}^2 \\ [X : Y : Z] &\longmapsto (X/Z, Y/Z) \\ [x : y : 1] &\longleftarrow\!\shortmid (x, y) \end{aligned}$$

We have $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$. The equation $y^2 = x^3 - x$ becomes

$$\begin{aligned} & Y^2/Z^2 = X^3/Z^3 - X/Z \\ \implies\ & Y^2 Z = X^3 - XZ^2 \qquad (\text{for } Z \neq 0) \end{aligned}$$

So we can view

$$E_0 = \{\, [X : Y : Z] \mid Y^2 Z = X^3 - XZ^2, Z \neq 0 \,\} \in \mathbb{P}^2.$$

- On U_2, we have the original equation $y^2 = x^3 - x$.
- On U_1, $Y \neq 0$, so take $x = \frac{X}{Y}$, $z = \frac{Z}{Y}$, giving $z = x^3 - xz^2$ for $z \neq 0$.
- On U_0, $X \neq 0$, so take $y = \frac{Y}{X}$, $z = \frac{Z}{X}$, giving $y^2 z = 1 - z^2$ for $z \neq 0$.

So now take the closure of E_0 in $\mathbb{P}^2$, which effectively 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 $E_0 \sqcup *$.

More generally, if we have $I \lhd k[x_1, \dots, x_n]$ 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 $(x_1, \dots, x_n) \mapsto [1 : x_1 : \dots : x_n]$.

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

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

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 $f \in k[x_1, \dots, x_n]$ we can make f homogeneous: If $\deg f = d$, define

$$\tilde{f}(x_0, \dots, x_n) = x_0^d f(x_1/x_0, \dots, x_n/x_0)$$

so

$$\tilde{f}(1, x_1, \dots, x_n) = f(x_1, \dots, x_n)$$
$$\tilde{f}(\lambda x_0, \dots, \lambda x_n) = \lambda^d \tilde{f}(x_0, \dots, x_n) \quad \forall \lambda \in k^\times$$

and $\tilde{f}$ homogeneous of degree d.

For example, if $f = y^2 - x^3 + x$,

$$\tilde{f} = z^3((y/z)^2 - (x/z)^3 + (x/z)) = y^2 z - x^3 + xz^2$$

as in our example.

We define $\tilde{0} = 0$. Observe

(i) if $f \neq 0$, then $x_0 \nmid \tilde{f}$, and conversely

(ii) if $x_0 \nmid g$, and $g \in k[x_0, \dots, x_n]$ which is homogeneous of degree d, then homogenising $g(1, x_1, \dots, x_n)$ gives back g.

Definition (Homogenised ideal)**.** If $I \lhd k[x_1, \dots, x_n]$ an ideal, define $\tilde{I} = \langle \tilde{f} | f \in I \rangle$ the ideal generated by the $\tilde{f}$.

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

Example.

(i) Take $I = \langle x - y^2, y \rangle$. Note this is exactly $\langle x, y \rangle$ 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) Exercise: Find an example of I where $\tilde{I} \neq \langle \tilde{f}_1, \dots, \tilde{f}_r \rangle$ for any choice of $\langle f_1, \dots, f_r \rangle = I$ which has r minimal.

Notice that every polynomial $f \in k[x_0, \dots, x_n]$ can be written uniquely as $f = f_{(0)} + f_{(1)} + \dots$ 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 (by the following lemma) while $\langle xy + y^3 \rangle$ is not.

Lemma.

(i) $I \lhd k[x_0, \ldots, x_n]$ is homogeneous if and only if I is generated by a finite set of homogeneous polynomials.

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

($\Leftarrow$) Write $I = \langle g_1, \ldots, g_n \rangle$, 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 as

$$h_{(d)} = \sum_{i:\deg(g_i) = d-k} f_{i,(k)} g_i \in I.$$

(ii) ($\Leftarrow$) If $I = \langle g_1, \ldots, g_n \rangle$ 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 (codimension 1), e.g. $H = \{x_0 = 0\}$, pick $p_0 \in V \setminus H$.

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

From our earlier example, $Z = Z(I) \subseteq \mathbb{A}^n$ gives $\tilde{I}$ 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 is in the 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

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

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

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

$$\left\{\begin{matrix}\text{closed} \\ \text{subvarieties} \\ \text{of } \mathbb{A}^n\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{closed subvarities } \overline{Z} \text{ of } \mathbb{P}^n \text{ such that} \\ \text{no irreducible component of } \overline{Z} \text{ is} \\ \text{contained in } \mathbb{P}V \setminus \mathbb{A}^n = \mathbb{P}H\end{matrix}\right\}$$

$$Z \longmapsto \overline{Z} = \text{closure of } \iota(Z) \text{ in } \mathbb{P}^n$$

where $\iota : \mathbb{A}^n \hookrightarrow \mathbb{P}^n$.

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

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

Definition (Quasivarities)**.** 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 $\mathcal{U}$ which 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 $X = Z(I)$, $I = \langle f_1, \dots, f_r \rangle$. We would like to think about the tangent space to X at p, a vector space. Our tentative definition is

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

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

$$T_{(p_1,p_2)} X = \left\{ (v_1, v_2) \;\middle|\; v_1(-3p_1^2) + v_2(2p_2) = 0 \right\}.$$

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,

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

We can think of this as a linear approximation to the variety:

$$f(x) = f(p) + \sum_i (x - p_i) \frac{\partial f}{\partial x_i} + \text{ higher order terms.}$$

Lemma.

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

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

Proof. Let $X = Z(I)$, where $I = \langle f_1, \dots, f_r \rangle$. Then write

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

where $A : k^n \to k^r$ is a linear map. Recall $\dim(\ker A) + \operatorname{rank}(A) = 0$ by the rank-nullity theorem. So,

$$\begin{aligned} \dim \ker A \geq d &\iff n - \operatorname{rank} A \geq d \\ &\iff \operatorname{rank} A \leq n - d. \end{aligned}$$

But the rank of a matrix is greater than a if and only if there exists some $a \times a$ submatrix with non-zero determinant. So, $\operatorname{rank}(A) \leq d \Leftrightarrow$ all $(n-d+1) \times (n-d+1)$ subminors have zero determinant which is a collection of polynomial equations. That is,

$$I(\{ p \in X \mid \dim T_p X \geq d \}) = \langle f_1, \dots, f_r, \text{ determinants of all subminors} \rangle. \qquad \square$$

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 a k-algebra, and $\varphi : A \to k$ a homomorphism. (For example, consider $A = k[X]$, $\varphi = \mathrm{ev}_p : f \mapsto f(p)$.)

A **derivation** 'centered at φ' is a k-linear map $D : A \to k$ such that

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

Write $\mathrm{Der}(A, \varphi)$ 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 $D \in \mathrm{Der}(k[x_1, \ldots, x_n], \mathrm{ev}_p)$, we get $v_i = D(x_i)$ so $\mathrm{Der}(A, \mathrm{ev}_p) = T_p\mathbb{A}^n$.

More generally,

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

$$\begin{aligned}
\mathrm{Der}(A, \mathrm{ev}_p) &= \left\{ D = \sum_i v_i \frac{\partial}{\partial x_i}\Big|_p \;\middle|\; D\langle f_1, \ldots, f_r\rangle = 0 \text{ in } k[X] \right\} \\
&= \left\{ D = \sum_i v_i \frac{\partial}{\partial x_i}\Big|_p \;\middle|\; \sum_i v_i \frac{\partial f_j}{\partial x_i}(p) = 0 \ \forall j \right\}
\end{aligned}$$

Proof. Can be seen as above. Alternatively, $D \in \mathrm{Der}(k[X], \mathrm{ev}_p)$ has $D : k[X] \to k$, so determines $\tilde{D} \in \mathrm{Der}(k[x_1, \ldots, x_n], \mathrm{ev}_p)$ by composing with the surjection $\pi : k[x_1, \ldots, x_n] \to k[X]$.

$$\begin{tikzcd}
k[x_1, \ldots, x_n] \arrow[r, "\pi"] \arrow[dr, "\tilde{D}"'] & k[X] \arrow[d, "D"] \\
& k
\end{tikzcd}$$

Then the condition $\tilde{D}$ descends to a map $k[X] \to k$ is the condition $D\langle f_1, \ldots, f_r\rangle = 0$. □

This gives us a better definition of tangent space:

Definition (Tangent space)**.** For an affine variety X and $p \in X$,

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

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

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

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

Show that $T_pV \cong T_pX$ under a canonical isomorphism, i.e. that

$$\mathrm{Der}\left(k[X]\left[\frac{1}{f}\right], \mathrm{ev}_p\right) \xrightarrow{\sim} \mathrm{Der}(k[X], \mathrm{ev}_p)$$

for $f(p) \neq 0$.

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

Example. Take $X = \mathbb{P}^n$, $p = [p_0 : p_1 : \cdots : p_n]$. If $p_0 \neq 0$, $p = [1 : \frac{p_1}{p_0} : \cdots : \frac{p_n}{p_0}] = \iota(\bar{p})$, 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 (Dimension)**.** Let X be irreducible. Then the **dimension** of X:

$$\dim X := \min \{ \dim T_pX \mid p \in X \}$$

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 (missing picture).

Definition (General dimension)**.** If X is arbitrary,

$$\dim X := \max \{ \dim X_i \mid X_i \text{ a component of } X \}.$$

Definition (Smooth point)**.** If X is irreducible, $p \in X$ is **smooth** if $\dim T_pX = \dim X$, and singular otherwise.

We've shown singular points in X form a Zariski closed subvariety, whose complement is non-empty.

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

Proof. $T_pZ(f)$ has dimension n or $n-1$, by definition of T_pX. We know

$$T_pZ(f) = n \iff T_pZ(f) = \mathbb{A}^n \iff \forall i,\ \frac{\partial f}{\partial x_i} = 0.$$

If $\dim Z(f) = n$ then $\frac{\partial f}{\partial x_i} \in I(Z(f))$, $\forall i = 1, \ldots, n$. But $I(Z(f)) = \sqrt{f}$, by Nullstellensatz, so $I(Z(f)) = \langle f \rangle$ as f is prime. So, $\frac{\partial f}{\partial x_i} = f \cdot g_i$ for some $g_i \in k[x_1, \ldots, x_n]$. But $\deg_{x_i} \frac{\partial f}{\partial x_i} < \deg_{x_i} f$, so $g_i = 0$.

Hence $\dim Z(f) = n \implies \frac{\partial f}{\partial x_i} = 0$, $\forall i$. There are now two cases,

(i) if $\operatorname{char} k = 0$, this implies f is constant, contradicting that it is prime.

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

Proof: If $f = \sum a_\lambda x^{\lambda p}$, then set $g = \sum a_\lambda^{1/p} x^\lambda$ (for $a_\lambda \in k$) works. This requires taking pth roots of things in k, which is allowed if $k = \bar{k}$. But this contradicts f is prime! □

There are two other interesting notions of dimension:

(1) Krull dimension:

$$\dim_{\mathrm{Kr}} X = \max \{ r \mid \varnothing \neq Z_0 \subsetneq Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_r = X \}$$

where each Z_i is an irreducible Zariski closed subvariety.

For example, take $\mathbb{A}^1$. The only such chains are point $\subsetneq \mathbb{A}^1$, so $\dim_{\mathrm{Kr}} \mathbb{A}^1 = 1$. We won't have time to show $\dim_{\mathrm{Kr}} X = \dim X$.

(2) If X is affine and irreducible, define $k(X)$ as the field of fractions of $k[X]$, which is valid as $k[X]$ is an integral domain. This is

$$\begin{aligned} k(X) &= \{ f/g \mid f, g \in k[X] \} \\ &= \bigcup_{g \in k[X]} k[X \setminus Z(g)] \\ &= \bigcup_{g \in k[X]} k[X] \left[\frac{1}{g} \right] \\ &= \bigcup_{\substack{U \subseteq X \\ \text{Zar. open} \\ \text{affine}}} k[U] \end{aligned}$$

called the function field of X. Observe that if $U \subseteq X$ is affine and open, then $k(U) = k(X)$. But this means that if X is any irreducible variety, affine or not, can define $k(X) = k(U)$, for U any affine open subset of X.

Example.

(i) $k(\mathbb{A}^n) = k(x_1, \ldots, x_n)$

(ii) $k(\mathbb{P}^n) = k(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) \simeq k(\frac{x_0}{x_n}, \ldots, \frac{x_{n-1}}{x_n})$ since $\frac{x_i}{x_0} \cdot \frac{x_0}{x_n} = \frac{x_i}{x_n}$.

(iii) if $E = \{ (x, y) \mid y^2 = x^3 - x \}$, then $k(E) = k(x)[y]/\langle y^2 - x^3 + x \rangle$

(iv) $X = \{ (x, y) \mid y^2 = x^3 \}$, $k(X) = k(x)[y]/\langle y^2 - x^3 \rangle$

Definition (Transcendance dimension)**.** Now we can define $\operatorname{trdim} X$, the **transcendance dimension** of extension $k \subseteq k(X)$.

It is not hard to see $\operatorname{trdim} k(x_1, \ldots, x_n)/k = \operatorname{trdim} \mathbb{A}^n = \mathrm{n}$. Generally,

Theorem. For any algebraic variety X, $\operatorname{trdim} X = \dim X$.

Proof strategy: We will reduce this to $\mathbb{A}^n$ where we know $\dim \mathbb{A}^n = n = \operatorname{trdim} \mathbb{A}^n$ by looking for very special nice morphisms $X \to \mathbb{A}^n$. To motivate this, consider the following special situation.

Suppose k is algebraically closed and take a morphism $\varphi : X \to Y$ of affine varieties such that

(1) X, Y are irreducible

(2) $k[X] = k[Y][t]/\langle f(t) \rangle$ and φ^* is the inclusion

$$k[Y] \hookrightarrow k[Y][t]/\langle f \rangle = k[X]$$

where $f(t) \in k[Y][t]$ is of the form

$$f(t) = a_0(y) + a_1(y)t + \cdots + a_N(y)t^N = f(y,t) \quad \text{with } a_N \neq 0$$

(3) f is a separable polynomial, when regarded as an element of $k(Y)[t]$, i.e.

$$F(t) = \frac{f(t)}{a_N(y)} = t^N + \frac{a_{N-1}}{a_N} t^{N-1} + \cdots + \frac{a_0}{a_N}$$

is such that $F(t), F'(t)$ have no common roots. So $\varphi : X \to Y$ comes from a separable algebraic extension of function fields $k(X) \supseteq k(Y)$.

In this specific situation, we have a lemma:

Lemma.

(a) $\varphi(X)$ contains an open (hence dense!) subset of Y

(b) there exists an open non-empty subset $V \subseteq Y$ such that $\varphi^{-1}(V)$ is finite,

$$\#\varphi^{-1}(v) \leq N, \ \forall v \in V.$$

Proof.

(b)
$$X = \{ (y_0, t_0) \in Y \times \mathbb{A}^1 \mid f(y_0, t_0) = 0 \}$$
and the morphism $\varphi : X \to Y$ sends $(y_0, t_0) \mapsto y_0$. Now for fixed $y_0 \in Y \setminus Z(a_N)$, $f(y_0, t)$ is a polynomial in $k[t]$ of degree N so has at most N roots. So, take $V = Y \setminus Z(a_N)$

(a) Let $U = \{ y \in Y \mid a_N(y) \neq 0 \} = Y \setminus Z(a_N)$ is Zariski open. □

Exercise. If $f : X \to Y$ is a morphism of affine varieties then we get $\forall p \in X$, a map $df : T_p X \to T_{f(p)} Y$

Proposition. In the same situation as above, there exists a Zariski open $U \subseteq Y$ such that $\forall (y_0, t_0) \in X$ with $y_0 \in U$, the natural map $T_{(y_0,t_0)} X \to T_{y_0} Y$ is an isomorphism.

Proof. Let $Y \subseteq \mathbb{A}^n$, so

$$T_{y_0} Y = \left\{ v \in \mathbb{A}^n \;\middle|\; \sum v_i \frac{\partial h}{\partial x_i}(y_0) = 0, \forall h \in I(Y) \right\}$$

and

$$T_{(y_0,t_0)} X = \left\{ (v, \gamma) \in \mathbb{A}^n \times \mathbb{A}^1 \middle| \sum v_i \frac{\partial h}{\partial x_i}(y_0) = 0, \forall h \in I(Y), \right.$$
$$\left. \text{and } \sum v_i \frac{\partial f}{\partial x_i}(y_0, t_0) + \gamma \frac{\partial f}{\partial t}(y_0, t_0) = 1 \right\}$$

as $I(X) = \langle I(Y), f \rangle$ but this is

$$\left\{ (v, \gamma) \in T_{y_0} X \times \mathbb{A}^1 \;\middle|\; \sum v_i \frac{\partial f}{\partial x_i} + \gamma \frac{\partial f}{\partial t}(y_0, t_0) = 0 \right\}.$$

If $\frac{\partial f}{\partial t}(y_0, t_0) \neq 0$, then can divide by it, and get isomorphism $T_{y_0} X \xrightarrow{\sim} T_{(y_0,t_0)} X$. So the proposition is equivalent to $\exists$ Zariski open subset U of Y such that $\forall y_0 \in U$, $\forall t_0$ with $f(y_0, t_0) = 0$, we have $\frac{\partial f}{\partial t}(y_0, t_0) \neq 0$. But this is immediate if $\frac{\partial f}{\partial t}$ isn't the zero polynomial, and our assumption of separability implies this. $\square$

Remark.

(1) Note the assumption of separability is necessary. For instance, take $k = \overline{\mathbb{F}_p}$, $Y = \mathbb{A}^1$, $X = \{ (y, t) \mid y = t^p \}$.

$$T_{(y_0,t_0)} X = \{ (v, \gamma) \mid v - pt_0^{p-1} \cdot \gamma = 0 \} = \{ (0, \gamma) \mid \gamma \in \mathbb{A}^1 \}$$

and map

$$\begin{aligned} T_{y_0,t_0} X &\longrightarrow T_{y_0} \mathbb{A}^1 \\ (0, y) &\longmapsto 0. \end{aligned}$$

(2) $\dim X = \dim Y$, $\operatorname{trdim} X = \operatorname{trdim} Y$. The second equality is clear as this is a separable algebraic extension of fields. To prove the first, let Y^{sm} be the smooth points of Y. Y irreducible, so $Y^{\mathrm{sm}} \cap U$ is open and Zariski dense, and $\dim T_p Y = \dim Y$ if $y \in Y^{\mathrm{sm}} \cap U$. But $\varphi^{-1}(Y^{\mathrm{sm}} \cap U)$ is open in X, so $\dim X = \dim T_{(p,t)} X$ for any (p, t) in this set.

Finally, note morphisms as above with $a_N = 1$, i.e. f a monic polynomial, are even nicer as φ is surjective.

To recap: Suppose we have affine varieties X and Y with a morphism

$$k[X] = k[Y][t]/f(t) \leftarrow k[Y].$$

We noticed that if $f \in k[Y][t]$ is a monic polynomial, then the map of algebraic varities $X \xrightarrow{\varphi} Y$ is surjective with finite $\varphi^{-1}(y)$ $\forall y \in Y$.

Definition (Integral extension)**.** $B \subseteq A$ is an **integral ring extension** if $\forall a \in A$, $\exists$ a monic polynomial $f \in B[t]$ with $f(a) = 0$.

Lemma.

(i) If f is a monic polynomial, then $B \subseteq B[t]/\langle f(t) \rangle$ is an integral extension of B.

(ii) If $C \subseteq B \subseteq A$ are integral ring extensions, so is $C \subseteq A$.

Definition (Finite morphism)**.** If $\phi^* : k[Y] \to k[X]$ is an integral inclusion of rings, we say $\varphi : X \to Y$ is a **finite morphism**.

Theorem (Noether normalisation lemma)**.** Let X be an affine variety. Then there exists a finite surjective morphism $X \to \mathbb{A}^d$ for some d. More precisely, let k be such that $\operatorname{char} k = 0$ or $\operatorname{char} k = p$ and $x \mapsto x^p$ is surjective, e.g. k is finite or algebraically closed. Let A be a finitely generated algebra over k and an integral domain. Then $\exists x_1, \ldots, x_N$ which generate A as a k-algebra such that

(i) $x_1, \ldots, x_d$ algebraically independent over k

(ii) for each $i > d$, x_i is separable algebraic with monic polynomial

$$F_i[t] \in k[x_1, \ldots, x_{i-1}][t].$$

That is, $k[x_1, \ldots, x_{i-1}] \subseteq k[x_1, \ldots, x_i]$ is an integral extension for $i > d$.

Notice, by the lemma (i) and (ii), this says that $k[x_1, \ldots, x_d] \subseteq A$ is an integral ring extension.

Corollary. $\operatorname{trdim} X = \dim X$.

Proof. We showed last time $\operatorname{trdim} \mathbb{A}^d = d = \dim \mathbb{A}^d$, and that if $\varphi : X \to Y$ had this nice form, then $\operatorname{trdim} X = \operatorname{trdim} Y$, $\dim X = \dim Y$. $\square$

Example. Take $k = \mathbb{C}$, and $X = \{ (x, y) \in \mathbb{A}^2 \mid xy = 1 \}$. Notice that $X \to \mathbb{A}^1$ with $(x, y) \mapsto x$ is not a finite morphism, as $k[x] \hookrightarrow k[x, y]/xy - 1$ is not of the form $k[x][t]/(f(t))$ with f monic. However $X \to \mathbb{A}^1$ given by $(t, t^{-1}) \mapsto t + t^{-1} = z$ is finite, since $z = t + t^{-1} \implies t^2 - tz + 1 = 0$, i.e.

$$k[t, t^{-1}] = k[z][t]/t^2 - tz + 1 \tag{1}$$

and indeed any projection onto a line other than the x or y axis will work.

Theorem. If $k = \overline{k}$, and $\varphi : X \to Y$ is a morphism of algebraic varities, and X, Y irreducible.

(a) $\overline{\varphi(X) = Y} \iff$ algebra homomorphism $k[Y] \to k[X]$ is injective.

(b) Suppose $\overline{\varphi(X) = Y}$. Then

 (i) $\dim X \geq \dim Y$

 (ii) there exists an open subset $U \subseteq Y$, non-empty such that $\forall y \in U$, $\dim \phi^{-1} y = \dim X - \dim Y$.

 (iii) For all $y \in \varphi(X)$, $\dim \varphi^{-1}(y) \geq \dim X - \dim Y$.

Example. Take $X = \mathbb{A}^2 = Y$, and $\varphi : (x, y) \mapsto (xy, y)$. If $U = \{ (a, b) \mid b \neq 0 \}$, $\varphi^{-1}\{(a, b)\} = \{(a/b, b)\}$ a point, $\dim \varphi^{-1}(a, b) = 0 = 2 - 2$. If $b = 0$, then

$$\varphi^{-1}((a, 0)) = \begin{cases} \varnothing & \text{if } a \neq 0 \\ \mathbb{A}^1 \times \{0\} & \text{if } a = 0 \end{cases} \tag{2}$$

with dimension $1 > 0$. Notice φ is not surjective but $\overline{\varphi(X)} = Y$.

Proof. (a) Let $f \in \ker(k[Y] \to k[X])$. Then $\forall x \in X$, $f \circ \varphi(x) = 0$, so $f|_{\varphi(X)} = 0$ so $f|_{\overline{\varphi(X)}} = 0$, as f is continuous. Hence if $\overline{\varphi(X)} = y$, $f \equiv 0$ on Y, so $f = 0$. Converse is exercise.

(b) (i) $k[X]$ and $k[Y]$ are integral domains, so the fraction field $k(Y) \hookrightarrow k(X)$, hence $\operatorname{trdim} Y \leq \operatorname{trdim} X$.

(ii) Claim: Noether normalisation $\implies \exists$ open subset $V \subseteq Y$, $V \neq \varnothing$ such that if you put $U = \varphi^{-1}(V)$, the map $\varphi : U \to V$ factors as $\varphi = p \circ \alpha$, for $\alpha : U \to \mathbb{A}^d \times V$ a finite morphism and $p : A^d \times V \to V$, $p(a, v) = v$ is projection. Exercise: Show the claim shows part (ii) of the proposition. Prove the claim. Hint: Let $L = k(Y)$, set $A = L.k[X] \subseteq k(X)$ be the subalgebra of $k(X)$ generated by L and $k[X]$, so an algebra over the field L. Apply Noether to A over the field L to get $a_1, \ldots, a_d$ in A are algebraically independent over L, such that A is integral over $L[a_1, \ldots, a_d]$ and generated by $a_{d+1}, \ldots, a_N$. Put a_i over a common denominator and deduce the result.

□

Noether normalisation restate: A is a finitely generated algebra over a field k, and an integral domain. THen there exist $x_1, \ldots, x_d \in A$ algebraically independent over k, and $x_{d+1}, \ldots, x_n \in A$ such that

(i) $x_1, \ldots, x_n$ generate A

(ii) for each $i > d$, x_i satisfies a monic irreducible polynomial F_i with coefficients in $k[x_1, \ldots, x_{i-1}]$.

Moreoever, if k is perfect, then F_i can be chosen to be separable.

Definition (Perfect)**.** A field k is perfect if $\operatorname{char} k = p > 0$ and $x \mapsto x^p$ is a surjection.

Remark. In particular, $A \supseteq B \coloneqq k[x_1, \ldots, x_d]$ and $B \subseteq A$ is an integral ring extension.

Noether normalisation implies Nullstellensatz. We will need a lemma:

Lemma. If $B \subseteq A$ is an integral ring extension, then

$$\text{units of } B = \text{units of A} \cap B$$

Proof. Let $b \in B$, and suppose b has an inverse in A, i.e. $a \in A$ such that $ab = 1$. As $B \subseteq A$ is integral, $\exists c_i \in B$ such that $a^n + c_{n-1}a^{n-1} + \cdots + c_0 = 0$, (i.e. a satisfies a monic polynomial with coefficients in B). Now multiply by b^{n-1}, get $a = -c_{n-1} - c_{n-2}b - \cdots - c_0 b^{n-1} \in B$. □

Recall

Theorem (Nullstellensatz)**.** If $A = k[z_1, \ldots, z_n]/m$, m a maximal ideal (so A is a field), then all elements of A are algebraic over k.

Proof. By Noether, $A \supseteq B = k[x_1, \ldots, x_n]$ with $x_1, \ldots, x_d$ algebraically independent, and A integral over B. Assume $d > 0$. The units in B are just $k^\times$, for example x_1 is not invertible. Hence by the lemma, x_1 is not invertible in A. But A is a field, so contradiction. So $d = 0$, and A is integral over B, in particular algebraic. □

4 Algebraic Curves

From now on assume $k = \overline{k}$.

Definition. A **curve** is a quasi-projective variety X with $\dim X = 1$.

For $\dim X = 1$:

$$\begin{aligned} \operatorname{trdim} k(X) = 1 &\iff \forall p \in X \setminus \text{some finite set}, \dim T_p X = 1 \\ &\iff \text{only Zariski closed proper subvarieties of } X \text{ are finite sets of points.} \end{aligned}$$

Example. If $F = F(X_0, X_1, X_2)$, an irreducible homogeneous polynomial, then $Z(F) \subseteq \mathbb{P}^2$ is an irreducible projective curve.

Warning. Not all curves can be embedded inside $\mathbb{P}^2$ (in fact, 'most' curves are not plane curves).

Definition. If X is an algebraic variety, and $p \in X$. Define

(i) $\mathcal{O}_{X,p} = \{ f/g \in k(X) \mid g(p) \neq 0 \}$, rational functions defined in some Zariski neighbourhood of $p \in X$. This is the **local ring** of X at p.

(ii) $\mathfrak{m}_{X,p} = \{ \gamma \in k(X) \mid \gamma(p) = 0 \}$ the maximal ideal of $\mathcal{O}_{X,p}$.

Exercise.

(i) Show if $\gamma \in \mathcal{O}_{X,p} \setminus \mathfrak{m}_{X,p}$, then γ^{-1} exists in $\mathcal{O}_{X,p}$ hence $\mathfrak{m}_{X,p}$ is the unique maximal ideal.

(ii) $\mathcal{O}_{X,p}/\mathfrak{m}_{X,p} = k$

If X is a curve, $p \in X$ a smooth point ($\dim T_p X = 1$) and $k = \mathbb{C}$, then it is a fact that in the usual topology, a small neighbourhood of p looks like a small disc around 0 in $\mathbb{C}$ and the local ring $\mathcal{O}_{X,p}^{\text{analytic}} \simeq \mathbb{C}\{z\}$, convergent power series in z.

What follows is an algebraic replacement for this.

Theorem. Take a curve X, $p \in X$ a smooth point. Then

(i) $\mathfrak{m} = \mathfrak{m}_{X,p}$ is a principal ideal in $\mathcal{O}_{X,p}$

(ii) $\bigcap_{n \geq 1} \mathfrak{m}^n = \{0\}$.

(This is a replacement for implicit function theorem)

Proof. Let $X_0 \subseteq X$ be an affine open neighbourhood of p, i.e. $p \in X_0$, $k[X_0] = k[x_1, \dots, x_n]/I$ and X_0 is a curve. We can assume, by changing variables, that $p = (0, 0, \dots, 0)$.

Write $\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}$ for the image of $x_1, \dots, x_n$ in $k[X_0]$. So the local ring $\mathcal{O}_{X,p} = \mathcal{O}_{X_0,p} = \{ f/g \mid f, g \in k[X_0], g \notin \langle \overline{x_1}, \dots, \overline{x_n} \rangle \}$.

$$\mathfrak{m} = \mathfrak{m}_{X_0,p} = \mathfrak{m}_{X,p} = \overline{x}_1 \mathcal{O}_{X_0,p} + \cdots + \overline{x}_n \mathcal{O}_{X_0,p}$$

X smooth at $p \iff \dim(T_p X) = 1 = \dim(T_p X_0) = 1 \implies T_p X_0 \subseteq \mathbb{A}^n$ is a line. After a linear change of variables (act by GL_n) can assume $T_p X$ is the x_1 line, i.e. $x_2 = x_3 = \cdots = x_n = 0$.

Now if $\tilde{f}_2, \tilde{f}_3, \dots$ generate the ideal I, write $\tilde{f}_i = \sum a_{ij}x_j + \text{h.o.t.}$, put $A = (a_{ij})$ and observe that as $T_0X_0 = \langle x_2 = x_3 = \cdots = 0\rangle$ by row reduction of A can assume that $\tilde{f}_i = \lambda x_i + \text{h.o.t.}$ or $\tilde{f}_i = \text{quadratic} + \text{higher order terms}$, hence that there exists $f_2, \dots, f_n \in I$ with $f_i = x_i + h_i$ with h_i has lowest power at least 2 for $1 \leq i \leq n$.

$$\overline{x}_i = -h_i \in (\overline{x}_1^2, \overline{x}_1\overline{x}_2, \dots, \overline{x}_n^2) = \mathfrak{m}^2, \quad i \geq 2$$

so $x_i \in \mathfrak{m}^2, i \geq 2$ and so $\mathfrak{m} = \overline{x}_1\mathcal{O}_{X,p} + \overline{x}_2\mathcal{O}_{X,p} + \cdots + \mathcal{O}_{X,p}$ hence $\mathfrak{m} = \overline{x}_1\mathcal{O}_{X,p} + \mathfrak{m}$.

Invoke Nakayama's lemma: For R a ring, M a f.g. R-module, $J \subseteq R$ an ideal. Then

(i) $JM = M \implies \exists r \in J$ such that $(1+r)M + 0$.

(ii) If $N \subseteq M$ is a submodule such that $JM + N = M$ then $\exists r \in J$ such that $(1+r)M \subseteq N$.

Apply (ii) to our situation:

$$R = \mathcal{O}_{X,p}, J = M$$

Note $1 + r \in \mathcal{O}_{X,p}^\times$ for $r \in \mathfrak{m}$ so $(1+r)M = M$ in statement of Nakayama.

Take $M = \mathfrak{m}$, $N = \langle x_1\rangle$. We need M is finitely generated. But $M \subseteq \mathcal{O}_{X,p}$ and every ideal in $\mathcal{O}_{X,p}$ is finitely generated: Proof: If $J \subseteq \mathcal{O}_{X,p}$ is an ideal, $J = \{\, f/g \mid f \in J \cap k[X_0], g \in k[X_0], g(p) \neq 0\,\}$. Observe $J \cap k[X_0]$ is finitely generated by Hilbert basis and if $\frac{f}{g} \in J$, then $f = g \cdot \frac{f}{g} \in J$ also.

So Nakayama (ii) says

$$\mathfrak{m} = \langle x_1\rangle + \mathfrak{m} \cdot \mathfrak{m} \implies \mathfrak{m} \subseteq \langle x_1\rangle$$

but $\langle x_1\rangle \subseteq \mathfrak{m}$, so $\mathfrak{m} = \langle x_1\rangle$, i.e. $\mathfrak{m}$ is a prime ideal, generated by x_1. For part (ii) of the theorem, let $M = \cap_{n \geq 0}\mathfrak{m}^n$. Again, $M \subseteq \mathcal{O}_{X,p}$ so is finitely generated and $\mathfrak{m}M = M$, so Nakayama (i) says $M = 0$. □

Definition. Any $t \in \mathfrak{m}_{X,p}$ such that $\mathfrak{m} = \langle t\rangle$ is called a local coordinate (or local parameter) at p.

It is not unique, but if t' is any other, it is of the form $t' = ut$, $u \in \mathcal{O}_{X,p}^\times$, a unit. So x_1 is a local coordinate in the above proof, and the proof showed

Corollary. Let $X = Z(f) \subseteq \mathbb{A}^2$, $p = (x_0, y_0) \in \mathbb{A}^2$. Then $x - x_0$ is a local coordinate at $p \iff \frac{\partial f}{\partial y}(x_0, y_0) \neq 0$ 'you can write the y coordinate as a function of x', and similarly for $y - y_0$ with $\frac{\partial f}{\partial x}(x_0, y_0) \neq 0$. And if both $\frac{\partial f}{\partial x}(x_0, y_0)$ and $\frac{\partial f}{\partial y}(x_0, y_0)$ are zero, p is not a smooth point.

Example. Take $x^2 + y^2 = 1$. $\frac{\partial f}{\partial x} = 2x \implies y - y_0$ is a local parameter if $p \neq \pm(0,1) \in X$. If $k = \mathbb{C}$, for $p \neq \pm(0,1)$ can write x in terms of y as a convergent power series (in a small neighbourhood)

$$x = (1 - y^2)^{\frac{1}{2}} = \sum \binom{\frac{1}{2}}{n}(-1)^n y^{2n}.$$

For example with $p = (1,0)$, $x - 1 = (1-y^2)^{\frac{1}{2}} - 1 = \sum_{n \geq 1}\binom{\frac{1}{2}}{n}(-1)^n y^{2n} = -\frac{1}{2}y^2 + \cdots$. Here, y is a local parameter at $(1,0)$. Our proposition is a substitute for this.

Corollary.

(i) Every $f \in k(X)$, $f \neq 0$ can be written uniquely as $f = t^n u$, $n \in \mathbb{Z}$, $u \in \mathcal{O}^*_{X,p}$, t a local parameter.

Write $n = \nu_p(f)$, the 'valuation of f at p', order of vanishing or $-$order of pole of f at p. It is independent of the choice of t.

(ii)

$$\mathcal{O}_{X,p} = \{0\} \cup \{\, f \in k(X) \mid \nu_p(f) \geq 0 \,\} \quad \mathfrak{m} = \{0\} \cup \{\, f \in k(X) \mid \nu_p(f) \geq 1 \,\}$$

We say $\mathcal{O}_{X,p}$ is a discrete valuation ring, and ν_p is a valuation.

For example, in the circle, $\nu_{1,0}(x-1) = 2$.

Proof. If $f \in \mathcal{O}_{X,p}$, $f \neq 0$, as $\bigcap \mathfrak{m}^n = \{0\}$ there exists a $n \geq 0$ such that $f \in \mathfrak{m}^n - \mathfrak{m}^{n+1}$. Define $\nu_p(f) = n$. As $\mathfrak{m}^n = \langle t^n \rangle$, this means $f = t^n u$, some $u \in \mathcal{O}^*_{X,p} = \mathcal{O}_{X,p} \setminus \mathfrak{m}$. So now if $f \in k(X), f \neq 0$, write $f = \frac{t^n u}{t^m v}$, put $\nu_p(f) = n - m$, and this is unique as if $f = t^a u = t^b v$, $a, b \in \mathbb{Z}$, $u, v \in \mathcal{O}^*_{X,p}$. Wlog $a \geq b$, $t^{a-b} = vu^{-1} \in \mathcal{O}^*_{X,p}$, so $a = b$. □

Proof of Nakayama. Let M be generated by $m_1, \ldots, m_n$ as an R-module, i.e. map $R^n \twoheadrightarrow M$, $\langle r_i \rangle \mapsto \sum_1^n r_i m_i$ is surjective. Then $JM = M \implies \exists x_{ij} \in J$ such that $m_i = \sum x_{ij} m_j$, i.e.

$$(I - X) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0 \quad \text{when } X = (x_{ij}) \tag{$*$}$$

Now recall $X\mathrm{adj}(X) = \det(X)I$ where $\mathrm{adj}(X)$ is the matrix of determinants of minors. Mulitply $(*)$ by $\mathrm{adj}(I - X)$, get $dm_i = 0$ for $i = 1, \ldots, n$ where $d = \det(I - X) = 1 + r$ with $r \in J$ by expanding out the determinant, use J ideal i.e. $(1 + r)M = 0$.

(ii) is immediate from (i), by applying (i) to M/N. □

If we shrink U, want to consider this the same rational map, so given

$$\varphi_1, \varphi_2 \dashrightarrow Y$$

say φ_1 equal to φ_2 if $\exists V \subseteq U_1 \cap U_2$ Zariski open.

Definition. X and Y are

Proposition. Take X a projective curve, $\alpha : X \dashrightarrow Y$ a rational map, Y projective and $p \in X$ a smooth point. Then we can extend α so it is well defined in a neighbourhood of p.

Remark. Cremona transform shows this is false for $X = \mathbb{P}^2$.

Proof. X is a curve, α defined on an open subset of X, so it is defined eexcept possibly at a finite set of points. SO it is enough to show α is defined at p. Y is projective, $Y \subseteq \mathbb{P}^m$ for some m, enough to prove this for $Y = \mathbb{P}^m$.

$$\alpha = [f_0 : \cdots : f_m]$$

So each $f_i = t^{n_i} u_i$, where $n_i = \nu_p(f_i)$. $u_i(p) \neq 0$, i.e. $u_i \in \mathcal{O}_{X,p}$. Let $N = \min(n_0, \ldots, n_m)$, say minimum happens at j, i.e. $N = n_j$. Then $t^{-N} f_i \in \mathcal{O}_{X,p}$ has no pole at p and $t^{-N} f_j = u_j \in \mathcal{O}_{X,p}$ does not vanish, and

$$\alpha = [t^{-N} f_0 : \cdots : t^{-N} f_m] : X \dashrightarrow \mathbb{P}^m$$

is now defined at p also. □

Recall, if $f : X \to Y$ a morphism of algebraic varieties such that $\overline{f(X)} = Y$, then

$$\dim f^{-1}(y) \geq \dim X - \dim Y, \quad \text{with equality on an open dense set.}$$

(Noether normalisation).

If X, Y curves, this can be proved directly, it states:

Proposition. Let $\alpha : X \to Y$ be a non-constant morphism of irreducible curves.

(i) $\forall q \in Y$, $\alpha^{-1}(q)$ is a finite set.

(ii) α induces an embedding fo fields $k(Y) \subseteq k(X)$ such that $k(X)/k(Y)$ is a finite extension.

Definition. The **degree of** α is defined to be the degree of the field extension.

Proof.

(i) If X is an irreducible curve, $Z \subsetneq X$ closed proper subvariety, then Z is a finite set of points. (Proof: Exercise. Note this is saying Krull dim = dim) So $\alpha^{-1}(q)$ is a closed subvariety of X. As α is not a constant map, it is a proper subvariety $\Rightarrow$ it is a finite set of points.

(ii) If $f \in k(Y)$, means $f \in k[U]$ for some affine open subvariety of Y (since $k(Y)$ is the set of rational maps $Y \dashrightarrow \mathbb{A}^1$, analogously to $k[Y]$ being the set of morphisms $Y \to \mathbb{A}^1$.) So $f \circ \alpha : \alpha^{-1}(U) \to \mathbb{A}^1$ is well defined, in $k[\alpha^{-1}U] \subseteq k(X)$ be definition of morphism. So this gives a ring homomorphism $k(X) \to k(Y)$, but the rings are fields so the homomorphism is injective. Finally

$$k \hookrightarrow k(Y) \hookrightarrow k(X)$$

but $k \hookrightarrow k(Y)$ has transcedance dimension 1, and $k \hookrightarrow k(X)$ has transcedance dimension 1, therefore $k(Y) \hookrightarrow k(X)$ has trdim $= 0$, i.e. is an algebraic extension.

$\square$

Example. Take $X = \mathbb{A}^1$, $Y = \mathbb{A}^1$, $\alpha : X \to Y$ given by $z \mapsto z^n$. On function fields, this has $k(Y) \hookrightarrow k(X)$ sending $y \mapsto x^n$ (write $k(Y) = k(y)$, $k(X) = k(x)$). So $k(x^n) \hookrightarrow k(x)$ has degree n (as $1, x, \ldots, x^{n-1}$ is a basis of $k(x)$ over $k(x^n)$).

For $\alpha : X \to Y$ a morphism of smooth irreducible curves, let $y \in Y$, $t \in \mathcal{O}_{Y,y}$ a local parameter. So $t =$(some neighbourhood of y in Y) $\to \mathbb{A}^1$. Let $x \in X$ with $\alpha(x) = y$. Then $t\alpha$ is defined on some neighbourhood of x and is a morphism to $\mathbb{A}^1$, i.e. $t\alpha \in \mathcal{O}_{X,x}$.

So we can ask: what is the order of vanishing of $t\alpha$ at x? Choose $s \in \mathcal{O}_{X,x}$ a local coordinate at x, write $t\alpha = s^n u$, with $u \in O^*_{X,x}$, $u(x) \neq 0$. $n = \nu_x(t\alpha)$ is called the multiplicity (ramification index) of α at x denoted $e_\alpha(x) \coloneqq \nu_x(t\alpha)$.

Example. $\alpha : \mathbb{A}^1 \to \mathbb{A}^1$ sending $z \mapsto z^n$, and say $\operatorname{char} k \not| n$. Compute $e_\alpha(p)$, $\forall p \in \mathbb{A}^1$.

5 Differentials

Take a ring B and a subring $A \subseteq B$.

Definition. Define $\Omega^1_{B/A}$ symbols $f\,\mathrm{d}g$ subject to the relations

$$\begin{aligned} \mathrm{d}(fg) &= g\,\mathrm{d}f + f\,\mathrm{d}g \quad \forall f, g \in B \\ \mathrm{d}(b + b') &= \mathrm{d}b + \mathrm{d}b' \quad \forall b, b' \in B \\ \mathrm{d}a &= 0 \quad \forall a \in A \end{aligned}$$

i.e. it is the free B-module generated by B, quotiented by the above relations:

$$\bigoplus_{b \in B} B\ \mathrm{d}b / R$$

We call these Kahler differentials, 1-forms or the relative cotangent bundle.

Exercise.

(a) let X be an affine algebraic vairety, $x \in X$ and consider the ring homomorphism $\mathrm{ev}_x : kX \to k$ given by $f \mapsto f(x)$. Show

$$\mathrm{Hom}_{k[X]}(\Omega^1_{k[X]/k}, k) \xrightarrow{\sim} \mathrm{Der}(k[X], k) = T_x X$$

regarded as $k[X]$-module via ev_X.

(b) More generally, show that if M is a B-module, then $\mathrm{Hom}_B(\Omega^1_{B/A}, M) = A$-linear derivations from $B \to M$.

So $\Omega^1_{k[X]/k}$ is dual to the tangent bundle TX on X, called the cotangent bundle of X.

Definition. Define rational differentials on X as $\Omega^1_{k(X)/k}$.

Our usual rules of calculus apply:

$$0 = \mathrm{d}1 = \mathrm{d}\left(\frac{g}{g}\right) = \frac{1}{g}\,\mathrm{d}g + g\,\mathrm{d}\left(\frac{1}{g}\right) \implies \mathrm{d}\left(\frac{1}{g}\right) = -\frac{\mathrm{d}g}{g^2}$$

so we have the usual quotient rule.

Corollary.

(1) $\Omega^1_{k(x)/k} = k(x)\,\mathrm{d}x$, if x is transcendental over k.

(2) L/k a separable algebraic extension. Then $\Omega^1_{L/k} = 0$.

Proof. If $\alpha \in L$, $\exists$ a monic polynomial $f(z) \in k[z]$ with $f(\alpha) = 0$ and $f'(\alpha) \neq 0$. But now $0 = f(\alpha)$, differentiate to get $\mathrm{d}f(\alpha) = 0$, but $\mathrm{d}f(\alpha) = f'(\alpha)\,\mathrm{d}\alpha$ so $f'(\alpha) \neq 0 \implies \mathrm{d}\alpha = 0$. ☐

Combining these two examples, we get

Lemma. Let X be a curve, $p \in X$ a smooth point on X, t a local parameter at p. Then $\Omega^1_{k(X)/k)} = k(X)\,\mathrm{d}t$

Hence if $\alpha \in k(X)$, $\exists f \in k(t)[z]$, i.e. $f = \sum f_i(t) z^i$

$$\text{s.t.} f(\alpha) = 0 \text{ and } \frac{\partial f}{\partial z} \neq 0.$$

Hence

$$0 = \mathrm{d}f(\alpha) = \mathrm{d}(\sum f_i(t)\alpha^i) = (\sum f_i'(t)\alpha^i)\,\mathrm{d}t + \underbrace{(\sum f_i(t) i\alpha^{i-1})}_{=\frac{\partial f}{\partial z}(\alpha)\neq 0\,\mathrm{d}\alpha}$$

so

$$\mathrm{d}\alpha = \frac{-\sum f_i'(t)\alpha^i}{\frac{\partial f}{\partial z}(\alpha)}\,\mathrm{d}t \in k(X)\,\mathrm{d}t.$$

Let $w \in \Omega^1_{k(X)/k}$, $p \in X$ smooth point on curve X, t local parameter at p so $w = f\,\mathrm{d}t$, some $f \in k(X)$.

Definition. $\nu_p(w) \coloneqq \nu_p(f)$ is the other of vanishing of w at p. Also, we have

$$div(w) = \sum_p \nu_p(w) p \in Div(w)$$

We say w is 'regular at p' if $\nu_p(w) \geq 0$.

We need to show this definition makes sense: (i) $\nu_p(w)$ is independent of t and (ii) the above sum only has finitely many non-zero terms.

Lemma. (a) If $f \in \mathcal{O}_{X,p}$, then $\nu_p(\mathrm{d}f) \geq 0$.

(b) If t_1 is any local parameter at p, then $\nu_p(\mathrm{d}t_1) = 0$. Hence $\nu_p(f\,\mathrm{d}t) = \nu_p(f) + \nu_p(f\,\mathrm{d}t)$ does not depend on choice of local parameter t.

(c) If $f \in k(X)$, $n = \nu_p(f) < 0$, then $\nu_p(\mathrm{d}f) = \nu_p(f) - 1$, if $n \neq 0$ in k, i.e. if $\mathrm{char}(k) \nmid n$.

Proof. (a) Let $p \in X_0 \subseteq X$, X_0 an affine neighbourhood of p, i.e. $X_0 \subseteq \mathbb{A}^N$ is an affine curve so $f = \frac{g}{h}$, $g, h \in k[x_1, \ldots, x_N]$, $h(p) \neq 0$ and

$$\mathrm{d}f = \frac{h\,\mathrm{d}g - g\,\mathrm{d}h}{h^2} = \sum_1^N \gamma_i\,\mathrm{d}x_i \quad \text{where } \gamma_i \in \mathcal{O}_{X,p} \quad \text{is well defined at } p.$$

hence $\nu_p(\mathrm{d}f) \geq \min\{\nu_p(\mathrm{d}x_1), \ldots, \nu_p(\mathrm{d}x_N)\}$ which is bounded below. Choose $f \in \mathcal{O}_{X,p}$ with $\nu_p(\mathrm{d}f)$ minimal, which certainly exists.

Recall t is our local parameter at p. Now $f - f(p) = t \cdot f_1$ where $f_1 \in \mathcal{O}_{X,p}$. Differentiating, get

$$\mathrm{d}f = \mathrm{d}(f - f(p)) = f_1\,\mathrm{d}t + t\,\mathrm{d}f_1.$$

Now, if $\nu_p(\mathrm{d}f) < 0$, then as $\nu_p(f_1\,\mathrm{d}t) = \nu_p(f_1) \geq 0$, ((a)) $\implies \nu_p(\mathrm{d}f_1) = \nu_0(\mathrm{d}f) - 1$. But this contradicts minimality of $\nu_p(\mathrm{d}f)$.

(b) We have $t_1 = tu$, $u \in \mathcal{O}^*_{X,p}$.

Then $\mathrm{d}t_1 = u\,\mathrm{d}t + t\,\mathrm{d}u$. By (i), $\mathrm{d}u = g \cdot \mathrm{d}t$ with $\nu_p(g) \geq 0$. So $\mathrm{d}t_1 = (u + tg)\,\mathrm{d}t$. But $\nu_p(u + tg) = \nu_p(u) = 0$, proving the result.

(c) If $f = t^n u,\ \mathrm{d}f = nt^{n-1}u \cdot \mathrm{d}t + t^n \,\mathrm{d}u$, as required.

$\square$

Lemma. Let $w \in \Omega^1_{k(X)/k}$, then $\nu_p(\omega) = 0$ for all but finitely many $p \in X$.

Proof. Choose $t \in k(X)$, such that $k(X) \supseteq k(t)$ finite separable (e.g. t a local parameter or use Noether normalisation). Then $\alpha = [1 : t] : X \dashrightarrow \mathbb{P}^1$ defines a rational map, and as X is smooth this extends to a morphism $\alpha : X \to \mathbb{P}^1$. Then the finiteness theorem $\Rightarrow$ only finitely many $p \in X$ with $\alpha(p) = \infty$ or $e_\alpha(p) > 1$. For all other p, $t - t(p)$ is a local parameter at p and hence, by lemma above $\square$

E a curve of genus 1, $P_\infty \in E$.

$$\begin{aligned} E &\xrightarrow{\sim} Cl^0(E) \\ P &\mapsto [P - P_\infty] \end{aligned}$$

Therefore E is an abelian group, define $P \boxplus Q = R$ if $(P - P_\infty) + (Q - P_\infty) = (R - P_\infty)$ in $Cl^0(E)$ i.e. $P + Q \sim R + P_\infty$. Note P_∞ is the zero element.

In fact this group law is algebraic. Consider $\alpha_{3P_\infty} : E \to \mathbb{P}^2$. We know $E \cap (Z = 0) = 3P_\infty$, as we computed this when E was a plane curve of the form (**).

We also know that $[E \cap L] = P_1 + P_2 + P_3$, if $l \subseteq \mathbb{A}^2$ defined a line L in $\mathbb{P}^2$ and these are equivalent in $Cl(E)$, as $\mathrm{Div}(z/l) = P_1 + P_2 + P_3 - 3P_\infty$.

This is all immediate from the definition of $[X \cap H] \in Cl(X)$ for X a curve and H a hyperplane and the proof it was independent of choice of hyperplane H.

So $P_1 + P_2 + P_3 \sim 3P_\infty \implies P_1 \boxplus P_2 \boxplus P_3 = \square * P_\infty + \square * 0$. That is, $P \boxplus Q \boxplus R = \square * 0 \iff P, Q, R$ lie on a line $\in E$.

Exercise.

(i) Show that for fixed $P \in E$, the map $E \dashrightarrow E$, $e \mapsto e \boxplus P$ is a rational map, hence a morphism and even an isomorphism, i.e. defining $P \boxplus Q \boxplus R = P_\infty$ if P, Q, R lie on a line, show that given P, can write the coords of $e \boxplus P$ as rational functions of the coordinates of $e \in E$, and show also the coords of $\boxminus e$ are rational functions.

(ii) We have shown the addition is associative, as $Cl^0(E)$ is a group. Can you show it directly?

Suppose $\mathrm{char}(k) \neq 2$, and E is the closure of $\{\, (x, y) \mid y^2 = (x - \_lambda_1)(x - \lambda_2)(x - \lambda_3) \,\}$ in $\mathbb{P}^2$ for λ_i distinct.

Consider the line $x = a$ in $\mathbb{P}^2$. It intersects E at 3 points: at P_∞, and at $(a, b), (a, -b)$ some $b \in k$, i.e. $(a, b) \boxplus (a, -b) = P_\infty = \square * 0$. So $\boxminus(a, b) = (a, -b)$.

Notice that this says

$$\square * 2P = 0 (\iff P \boxplus P = P_\infty) \tag{3}$$

$$\iff P = (a, 0) \tag{4}$$

i.e. $b = 0 \iff P = (\lambda_i, 0)\ i = 1, 2, 3$ or $P = P_\infty \iff P$ is a ramification point of $\alpha_{2P_\infty} : E \to \mathbb{P}^1$ $((a, b) \mapsto a)$.

That is, E is a double cover of $\mathbb{P}^1$, ramified at 4 points and these 4 points are the points of order 2 in E.

Let $j(E) =$ cross ratio of $\lambda_1, \lambda_2, \lambda_3, \infty$ four distinct points. This is invariant of $\{\lambda_1, \lambda_2, \lambda_3, \infty\}$ over PGL_2 actions, so independent of the choice of coordinates of $\mathbb{P}^1$.

So $j(E) = j(E') \iff E \cong E'$.

Proof. ($\Leftarrow$) is done above, (check it didn't depend on P_∞). ($\Rightarrow$) Given $\lambda_1, \lambda_2, \lambda_3, \infty$, define a curve, it is isomorphic to E by what we have done. $\square$

We have proved

Corollary. {genus 1 curves} up to isomorphism $= \{4 \text{ distinct points in } \mathbb{P}^1\}/PGL_2 \xrightarrow{\sim} \mathbb{A}^1$.

Explicitly, if $y^2 = x(x-1)(x-\lambda)$, $j(E) = \frac{2^8(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$.

5.1 Curves of genus > 1

Take X a smooth projective curve, genus $g > 0 \iff \deg K_X > 0$ We can study $\alpha_{K_X} : X \to \mathbb{P}^{g-1}$, the 'canonical map'.

Example. Take $g = 2$, $\alpha_{K_X} : X \to \mathbb{P}^1$. (Recall $X \not\subseteq \mathbb{P}^2$, as smooth plane curves have genus $0, 1, 3, 6, 10, \dots$)

Lemma. α is a map of degree 2, X is a 'hyperellptic curve'.

Proof. Let $K_X = \sum n_l P_l$, and $f \in \mathcal{L}(\mathcal{K}_X)$. Then $\mathcal{K}_X + \div(f) \geq 0$ is effective and of degree 2, so $\mathcal{K}_X + \div(f) = P + Q$, for some $P, Q \in X$. So $K_X \sim P + Q$, and $l(\mathcal{K}_X) = 2 = l(P+Q) > 1$ so exists a non-constant $h \in \mathcal{L}(\mathcal{K}_X)$ such that $\div(h) + P + Q \geq 0 \implies$ degree of h is 1 or 2. But X genus 2, so isn't $\mathbb{P}^1$ so $\deg h \neq 1$, so $\alpha_{\mathcal{K}_X} = [1 : h] : X \dashrightarrow \mathbb{P}^1$ has degree 2. $\square$

Note that the embedding theorem (+Riemann-Roch) shows $\alpha_{d\mathcal{K}_X} : X \to \mathbb{P}^{2d-2}$ is an embedding if $d > 2$.

Proposition. Take X a smooth projective curve of genus g. Either

(i) X admits a degree 2 map $\pi : X \to \mathbb{P}^2$ 'X is hyperelliptic' in which case the image $\alpha_{\mathcal{K}_X}(X) \subseteq \mathbb{P}^{g-1}$ is a $\mathbb{P}^1$ sitting inside $\mathbb{P}^{g-1}$ and $X \to \alpha(X) (\hookrightarrow \mathbb{P}^{g-1})$ is a degree 2 map.

(ii) X is not hyperellptic, and $\alpha_{\mathcal{K}} : X \to \mathbb{P}^{g-1}$ is an embedding.

Moreover, (ii) happens 'most of the time'. Specifically, $\dim \mathscr{M}_g = 3(g-1)$ where $\mathscr{M}_g$ is the set of algebraic curves of genus g up to isomorphism. $\dim(hyperellipticcurvesofgenusg) = \ldots < 3(g-1)$.

RH: $\chi(X) \coloneqq 2 - 2g$. For $\alpha : X \to Y$, non-constant, separable,

$$\chi(X) = \chi(Y) \cdot \deg \alpha - \sum_{p \in X} (e_\alpha(p) - 1)$$

'conservation of Euler characteristic'.

Proof. Recall α defines a map $k(Y) \to k(X)$, with $f \mapsto f \cdot \alpha$, and so a map

$$\alpha^* : \Omega^1_{k(Y)/k)} \longrightarrow \Omega^1_{k(X)/k} f \, \mathrm{d}g \longmapsto f\alpha \, \mathrm{d}(g\alpha)$$

α is separable and non-constant, so α^* is injective.

Pick $\omega \in \Omega^1_{k(Y)/k}$, $\omega \neq 0$. $\deg \omega = 2g(Y) - 2 = -\chi(Y)$. We want to compute $\deg \alpha^* \omega$, as this is $-\chi(X)$.

Let $p \in X$, $q = \alpha(p) \in Y$. Choose a local parameter t_p at $p \in X$ and t_q at $q \in Y$. Recall $t_q \circ \alpha = ut_p^{e_\alpha(p)}$ by definition of $e_\alpha(p)$.

Hence if $\omega = f\,\mathrm{d}t_q$, $\alpha^*\omega = f\alpha\,\mathrm{d}(ut_p^{e\alpha(p)})$ this vanishes at p to order

$$\nu_p(\alpha^*\omega) = \underbrace{\nu_p(f\alpha)}_{=e_\alpha(p)\nu_q(f)} + \underbrace{\nu_p(\,\mathrm{d}(ut^{e_\alpha(p)}))}_{\nu_p(ut^{p})+1=e_\alpha(p)-1}$$

by the lemma when we defined $\nu_p(\omega)$.

If $\nu_q(f) = s$, $f = u^p t_q^s$ and $f\alpha = u' \circ \alpha . t_q^{se_\alpha(p)}$ and observe $\nu_q(f) = \nu_q(\omega)$, by definition. Hence

$$\begin{aligned}
-\chi(X) = \deg \alpha^*\omega &= \sum_{q \in Y} \left(\sum_{\substack{p \in X \\ \alpha(p)=y}} e_\alpha(p) \right) \cdot v_q(\omega) + \sum_{p \in X} (e_\alpha(p) - 1) \\
&= \sum_{q \in Y} \deg \alpha \cdot \nu_q(\omega) + \sum_{p \in X} (e_\alpha(p) - 1) \\
&= \deg \alpha \cdot \deg \omega + \sum_{p \in X} (e_\alpha(p) - 1). \qquad \square
\end{aligned}$$

We return to prove

Proposition. (i) Take $\pi : X \to \mathbb{P}^1$ a map of degree 2, X a smooth projective curve, $\operatorname{char} k \neq 2$, i.e. X is hyperelliptic. Then the image of $\alpha_{\mathcal{K}_X}$ is isomorphic to the inclusion $\mathbb{P}^1 \hookrightarrow \mathbb{P}^{g-1}$, and $X \to \alpha_{\mathcal{K}_X}(X)$ has degree 2.

Proof. $\deg \pi = 2 \implies 2 + 2g$ ramification points by RH. Choose $\infty \in \mathbb{P}^1$ to be one of them, and the others are $a_1, \ldots, a_{2g+1}$. Now π defines $k(\mathbb{A}^1) = k(\mathbb{P}^1) = k(x) \hookrightarrow k(X)$.

π is of degree 2, so this is a quadratic extension, so by Galois theory $\exists y \in k(X)$, $f \in k(x)$ such that

$$k(X) = k(x)[y]/\langle y^2 - f(x) \rangle$$

.

So $f : X \dashrightarrow \mathbb{P}^1$ extends to a morphism $f : X \to \mathbb{P}^1$ with $X^0 = X \setminus \{\infty\}$

$$\begin{tikzcd}
X^0 \arrow[r, "f"] \arrow[d, hook] & \mathbb{A}^1 \\
\{\, (x, y) \in \mathbb{A}^2 \mid y^2 = f(x) \,\} \subseteq \mathbb{A}^2 &
\end{tikzcd}$$

and $f(x) = (x - a_1) \cdots (x - a_{2g+1})$.

Sketch remainder of proof:

1) it must be the case that $f = \pi : X \to \mathbb{P}^1$

2) take $\omega = \frac{\mathrm{d}x}{y}$ on X^0. Show

$$\mathcal{L}(\mathcal{K}_X) = \langle \omega, x\omega, x^2\omega, \ldots, x^{g-1}\omega \rangle$$

so

$$\begin{tikzcd} \alpha_{\mathcal{K}_X} = [1 : x : x^2 : \cdots : x^{g-1}] : X \arrow[rr] \arrow[dr, "f"] & & \mathbb{P}^{g-1} \\ & \mathbb{P}^1 & \end{tikzcd}$$ $\square$

Remark. Quadrics in two variables x, y are of the form Once we know about $\mathbb{C}$, the algebraic closure of $\mathbb{R}$, the first two are the same: $(x, y) \mapsto (x - iy, x + iy)$.

We learned that we should consider these in $\mathbb{P}^2$, not $\mathbb{A}^2$.

The equation $xy = 1$ becomes $xy = z^2$, giving two points at ∞: $[1 : 0 : 0]$ and $[0 : 1 : 0]$.

Now consider $y = x^2$. Its completion is $yz = x^2$, which has one point at ∞.

Now you interpret the algebraic fact that there is one equivalence class of homogeneous non-degenerate quadratic forms in n variables to say

$$\text{parabola} = \text{hyperbola} = \text{circle} = \mathbb{P}^1$$

up to a change of coordinates. Only the position of the line at ∞ has changed.

Take X a smooth projective curve, $k = \mathbb{C}$. If $g \geq 1$, $\mathcal{L}(\mathcal{K}_X) = \langle \omega_1, \ldots, \omega_g \rangle$ by choosing a basis. We showed $X \hookrightarrow Cl^0(X)$.

Consider map

$$\begin{aligned} Cl^0(X) &\longrightarrow \mathbb{C}^g/\mathbb{Z}^{2g} \\ D = \sum P_i - Q_i &\longmapsto \left(\sum \int_{P_i}^{Q_i} \omega_1, \ldots, \sum \int_{P_i}^{Q_i} \omega_g \right) \end{aligned}$$

Example. If X is an elliptic curve, $\mathcal{L}(\mathcal{K}_X) = k \cdot \omega$,

Proposition. If $X = Z(F) \subseteq \mathbb{P}^2$, $F = F(X_0, X_1, X_2)$ homogeneous of degree d, then $\deg[H \cap X] = d$.