University of Cambridge

Mathematics Tripos

Part II

Algebraic Geometry

Lent, 2019

Lectures by
I. Grojnowski

Notes by
Qiangru Kuang

Contents

0 Introduction

Algebraic geometry is the study of polynomial equations.

Example. $E = \{(x, y) \in \mathbb{C}^2 : y^2 = x^3 - x\}$. Sketch this.

Consider $p : E \to \mathbb{C}, (x, y) \mapsto x$. For each $x \notin \{0, \pm 1\}$, there are 2 points in $p^{-1}(x)$. So this is a double cover ramified at $0, \pm 1$, the precise meaning of these phrases will be defined later. How does this help us sketch? For x away from the three points, the preimage of a disk under p are two copies of the disk. If x is near 0, we have $x^3 - x \approx -x$ so locally it looks like $y^2 = -x$. If we project (x, y) to x we get a disk winding around twice. But if we project to y we get a bijection.

Still, how do we visualise E? First let's sketch it over $\mathbb{R}$. If $(x, y) \in \mathbb{R}^2$ then $y^2 \geq 0$ so $x(x^2 - 1) \cdot 0$. Thus $x \geq 1$ or $-1 \leq x \leq 0$. Just like in high school, we can differentiate. (graph) The infinite bit should be visualised as a circle minus a point.

Now let $(x, y) \in \mathbb{C}^2$. Let

$$\Gamma = \{(x, y) \in E : y \in \mathbb{R}, x \in [-1, 0] \cup [1, \infty)\} = p^{-1}\{[-1, 1] \cup [1, \infty)\}.$$

Claim $E \setminus \Gamma$ is disconnected and it consists of two pieces, each isomorphic via p to $\mathbb{C} \subseteq ([-1, 0] \cup [1, \infty))$. This is equivalent to the claim that if $x \in \mathbb{C} \subseteq ([-1, 0] \cup [1, \infty))$ then can choose a square root of $x^3 - x$, and then as you wander around, this remains a single-valued functions. The proof is left as an exercise.

Granting this, we have two copies of $\mathbb{C} \subseteq ([-1, 0] \cup [1, \infty))$. Turn one of them around and glue (graph).

More surprisingly, solutions of equaitons have a topology!

1 The dictionary between algebra and geometry

1.1 Basic notions

> **Definition** (k-algebra)**.** Let k be a field. A *(commutative) k-algebra* is a unital commutative ring countaining k as a subring.

Example. $k[x_1, \dots, x_n]$, the polynomial ring in n-variables.

Notation. If k is a fields, write $\mathbb{A}^n = \mathbb{A}^n(k) = k^n$, the *affine n-space.*

Observe that every $f \in k[x_1, \dots, x_n]$ defines a function

$$\begin{aligned}\mathbb{A}^n(k) &\to \mathbb{A}^1(k)\\ (p_1, \dots, p_n) &\mapsto f(p_1, \dots, p_n) = \mathrm{ev}_p(f)\end{aligned}$$

This defines a map from $k[x_1, \dots, x_n]$ to the space of all functions $\mathbb{A}^n \to \mathbb{A}^1$. If k is finite then it is surjective but not injective, and if k is infinite then it is not surjective.

More generally, if $L \supseteq k$ is an algebraic extension then one can define a function $\mathbb{A}^n(L) \to \mathbb{A}^1(L)$ by evaluating f at a point in L^n. Therefore f defines a function $\mathbb{A}^n(\overline{k}) \to \mathbb{A}^1(\overline{k})$ where $\overline{k}$ is the algebraic closure of k. So now the map $k[x_1, \dots, x_n] \to \{\mathbb{A}^n(\overline{k}) \to \mathbb{A}^1(\overline{k})\}$ is injective for all k but never surjective.

The conclusion is that we should think of $k[x_1, \dots, x_n]$ as very special functions $\overline{k}^n \to \overline{k}$, namely "polynomial with k-coefficients". As a concrete example, let $k = \mathbb{F}_q$. Then $x^q - x$ defines a function $\overline{k} \to \overline{k}$ that is *not* zero.

> **Definition** (algebraic set)**.** Let $S \subseteq k[x_1, \dots, x_n]$. Define
>
> $$Z(S) = \{p \in \mathbb{A}^p : f(p) = 0 \text{ for all } f \in S\} \subseteq \mathbb{A}^n$$
>
> which are the simultaneous zeros of equations in S. Such a subset is known as *algebraic set*, *Zariski closed subset of* $\mathbb{A}^n$.

Example.

1. $\mathbb{A}^n = Z(0)$.
2. $Z(x) = \{0\}$. Similarly $Z(x-7) = \{7\}$.
3. If $f(x) = (x - \lambda_1) \dots (x - \lambda_n)$ then $Z(f) = \{\lambda_1, \dots, \lambda_n\}$.
4. if $k = \overline{k}$ then algebraic subsets of $\mathbb{A}^1$ are $\emptyset, \mathbb{A}^1$ or finite set of points of k.
5. In $\mathbb{A}^2$, $Z(y^2 - x^3 + x) = E$ which we sketched in introduction.
6. In $\mathbb{A}^2$, $Z(x, y) = \{(0, 0)\}$, $Z(xy)$ is the union of two axes. $Z(y)$ is the x-axis and $Z(y(y-1), x(y-1))$ is the union of a point and a line.

If J is the ideal generated by S, i.e.

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

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

Recall from IB Groups, Rings and Modules

Theorem 1.1 (Hilbert basis theorem)**.** *If k is Noetherian then so is $k[x]$.*

So every ideal in $k[x_1, \dots, x_n]$ is finitely generated. Therefore there exist $f_1, \dots, f_r \in k[x_1, \dots, x_n]$ such that

$$Z(S) = Z(f_1, \dots, f_r).$$

Thus algebraic sets are solutions of finitely many polynomial equations.

Lemma 1.2.

1. *If $I \subseteq J$ then $Z(J) \subseteq Z(I)$.*
2. *$Z(0) = \mathbb{A}^n$ and $Z(k[x_1, \dots, x_n]) = \emptyset$.*
3. *$Z(\bigcup J_i) = Z(\sum J_i) = \bigcap Z(J_i)$ for any (possibly infinite) family of ideals $\{J_i\}$.*
4. *$Z(I \cap J) = Z(I) \cup Z(J)$ for ideals I, J.*

Proof. 1, 2, 3 are clear. For 4, $\supseteq$ follows from 1. For $\subseteq$, if $x \notin Z(I)$ then exists $f_1 \in I$ with $f_1(x) \neq 0$ and if $x \notin Z(J)$ then exists $f_2 \in J$ with $f_2(x) \neq 0$. Thus $f_1 f_2(x) = f_1(x) f_2(x) \neq 0$ so $x \notin Z(f_1 f_2)$. But $f_1 f_2 \in I \cap J$ as I and J are ideals. Thus $x \notin Z(I \cap J)$. □

We can define a map goes the other direction. If $Z \subseteq \mathbb{A}^n(\bar{k})$ is a subset, define

$$I(Z) = \{f \in k[x_1, \dots, x_n] : f(p) = 0 \text{ for all } p \in Z\}.$$

If $f \in I(Z), g \in k[x_1, \dots, x_n]$, $fg(p) = f(p)g(p) = 0$ if $p \in Z$ so $I(Z)$ is an ideal.

Lemma 1.3.

1. *If $Z \subseteq Z'$ then $I(Z') \subseteq I(Z)$.*
2. *For any $Y \subseteq \mathbb{A}^n$, $Y \subseteq Z(I(Y))$.*
3. *If $V = Z(J)$ is an algebraic subset then $V = Z(I(V))$.*
4. *If $J \subseteq k[x_1, \dots, x_n]$ is an ideal then $J \subseteq I(Z(J))$.*

Proof. 1, 2 and 4 are immediate. For 3, $\supseteq$ follows from $I(V) = I(Z(J) \supseteq J$ by 4 so $Z(I(V)) \subseteq Z(J) = V$ by 1. $\subseteq$ follows from 2. □

The first lemma says that algebraic subsets of $\mathbb{A}^n$ form the closed sets of a topology on $\mathbb{A}^n$. This is called the *Zariski topology.*

Example. If $X = \mathbb{A}^1(k)$ where $k = \bar{k}$, the closed subsets are finite subsets of points of $\mathbb{A}^1$.

Note that if $k = \mathbb{C}$, if $Z \subseteq \mathbb{A}^n(k)$ is Zariski closed then it is closed in the usual sense.

The second lemma says that $Z(I(Y))$ is the smallest algebraic subset of $\mathbb{A}^n$ containing Y, i.e. the closure of Y in the Zariski topology.

Example. If $k = \mathbb{C}$ and $\mathbb{Z} \subseteq \mathbb{C}$ then $Z(I(\mathbb{Z})) = \mathbb{C}$ as if a polynomial vanishes at $\mathbb{Z}$ then it must be zero.

We have a correspondence

$$\{\text{algebraic subsets of } \mathbb{A}^n\} \underset{Z}{\overset{I}{\rightleftarrows}} \{\text{ideals in } k[x_1, \dots, x_n]\}$$

Note that this is not quite a bijection. For example in $k[x]$,

$$Z(x) = Z(x^2) = Z(x^3) = \cdots$$

and more generally

$$Z(f_1^{q_1} \cdots f_r^{g_r}) = Z(f_1 \cdots f_r)$$

where $q_i > 0$. We will fix this shortly.

1.2 Hilbert's Nullstellensatz

Let $Y \subseteq \mathbb{A}^n$ be an algebraic subset so $Y = Z(I(Y))$. Recall that we have a map $k[x_1, \dots, x_n] \to \{\overline{k}^n \to \overline{k}\}$. Hence by restriction we have a map $k[x_1, \dots, x_n] \to \{Y \to \overline{k}\}$ as $Y \subseteq \overline{k}^n$. By definition $I(Y) \mapsto 0$. This motivates us to make the following definition:

> **Definition.** Let $Y \subseteq \mathbb{A}^n$ be an algebraic set. Then
>
> $$k[Y] = k[x_1, \dots, x_n]/I(Y).$$

We've just seen $k[Y] \hookrightarrow \{Y \to \overline{k}\}$ so $k[Y]$ is a special class of functions on Y, namely "polynomial functions on Y with k-coefficients".

Example.

- $k[\mathbb{A}^n] = k[x_1, \dots, x_n]$.
- $k[E] = k[x, y]/(y^2 - x^3 + x)$.

Clearly $k[Y]$ is a k-algebra. Our aim is to recover Y completely from this k-algebra.

Observe that if $p \in Y \subseteq \mathbb{A}^n(k)$ then the map

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

is an algebra homomorphism. It is surjective and its kernel, denoted

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

is a maximal ideal, as $k[Y]/\mathfrak{m}_p$ is a field. So

$$\{\text{points in } Y\} \hookrightarrow \{\text{algebra homomorphism } k[Y] \to \overline{k}\} \hookrightarrow \{\text{max ideals } \mathfrak{m} \subseteq k[Y]\}.$$

It is remarkable that if $k = \overline{k}$ then all of these coincides (it is particularly so for the first inclusion, as it gives a translation between geometry and algebra. By contrast, the second inclusion is more or less a corollary of a standard result in algebra).

What are the maximal ideals of $k[x_1, \dots, x_n]$? We've observed if $p \in k^n$ then $\{f \in k[x_1, \dots, x_n] : f(p) = 0\}$ is a maximal ideal.

Not all maximal ideals are of the form $\mathfrak{m}_p$, however. For example if $k = \mathbb{R}$ then $(x^2 + 1) \subseteq \mathbb{R}[x]$ is a maximal ideal as $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Nevertheless, notice that $\mathbb{R} \subseteq \mathbb{C}$ and this is an extension of $\mathbb{R}$.

> **Theorem 1.4** (Nullstellensatz)**.** *If $\mathfrak{m} \subseteq k[x_1, \dots, x_n]$ is a maximal ideal then $k[x_1, \dots, x_n]/\mathfrak{m} = L$ is an algebraic field extension of k, and finite-dimensional over k.*

Note that in this setting L is finite-dimensional over k if and only if every $\alpha \in L$ is algebraic over k. For the nontrivial direction, images of $x_1, \dots, x_n$ in L generate L and each satisfies a polynomial equation of degree d_i so $\dim_k L \leq d_1 \cdots d_n$.

> **Corollary 1.5.** *If $k = \overline{k}$ then the field embedding $k \to L$ is an isomorphism, that is every maximal ideal of $k[x_1, \dots, x_n]$ is of the form*
>
> $$\mathfrak{m}_p = (x_1 - p_1, \dots, x_n - p_n)$$
>
> *for $p \in k^n$.*

Proof. $L \supseteq k$ is an algebraic extension of fields so $L = k$ as $k = \overline{k}$ and p_i is the image of x_i under the map $k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]/\mathfrak{m}_p = L$. □

> **Corollary 1.6.** *Suppose $k = \overline{k}$. If $Y \subseteq \mathbb{A}^n$ is an algebraic set then we have bijections*
>
> $$\begin{array}{ccccc} \{\text{points in } Y\} & \to & \{\text{algebra homomorphisms } k[Y] \to k\} & \to & \{\text{maximal ideals of } k[Y]\} \\ p & \mapsto & \mathrm{ev}_p : f \mapsto f(p) & & \\ & & \varphi & \mapsto & \ker \varphi \\ \varphi(p) & \mapsfrom & \varphi & & \\ & & k[Y] \to k = k[Y]/\mathfrak{m} & \mapsfrom & \mathfrak{m} \end{array}$$

Proof. When $Y = \mathbb{A}^n$ this is Nullstellensatz. In general, an algebra homomorphism $\varphi : k[x_1, \dots, x_n]/I \to k$ is the same thing as an algebra homomorphism $k[x_1, \dots, x_n] \to k$ with I in its kernel. □

We will give a better proof later when we are more adept at playing with polynomial equations, but for now we'll prove a special case.

Proof of Nullstellensatz when k is uncountable. Suppose L is not algebraic. Then there exists $t \in L$ which is not algebraic over k so $k(t) \subseteq L$. But observe the following:

1. L has countable dimension as a vector space over k.

2. The set
$$\left\{\frac{1}{t-\lambda} : \lambda \in k\right\} \subseteq L$$
is linearly independent: suppose not then exist $\lambda_1, \dots, \lambda_r, a_1, \dots, a_r \in k$ with
$$\sum_{i=1}^{r} \frac{a_i}{t-\lambda_i} = 0.$$
Clear the denominators, we get an algebraic identity that t satisfies, contradicting t transcendental.

This implies that $\{\lambda : \lambda \in k\}$ is countable. Absurd. □

Corollary 1.7 (Nullstellensatz)**.** *Let $k = \overline{k}$, $I \subseteq k[x_1, \dots, x_n]$ an ideal. Then $Z(I) \neq \emptyset$ if $I \neq k[x_1, \dots, x_n]$.*

More generally, let $k = \overline{k}$, $I \subseteq k[Y]$ has $Z(I) \neq \emptyset$ if $I \neq k[Y]$.

Proof. If $I \neq k[x_1, \dots, x_n]$ then $I \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. But Nullstellensatz says that $Z(\mathfrak{m}) = \{p\}$ for some $p \in k^n$ as $\mathfrak{m} = \mathfrak{m}_p$ for some p. Thus
$$Z(I) \supseteq Z(\mathfrak{m}) = \{p\} \neq 0.$$
□

This motivates us to give an abstract, algebraic definition of algebraic set.

Definition (radical)**.** Let R be a ring and $J \subseteq R$ an ideal. The *radical* of J is
$$\sqrt{J} = \{f \in R : f^n \in J \text{ for some } n \geq 1\}.$$

Lemma 1.8. *Given an ideal $J \subseteq R$, $\sqrt{J}$ is an ideal.*

Proof. If $f, g \in \sqrt{J}$ then $f^n \in J, g^m \in J$ for some n, m. Then
$$(f+g)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{c} f^i g^{n+m-i} \in J$$
so $fg \in \sqrt{J}$.

If $r \in R, f \in \sqrt{J}$ then $rf \in \sqrt{J}$. □

Example.

1. $\sqrt{(x^n)} = (x)$ in $k[x]$.
2. If J is a prime ideal then $\sqrt{J} = J$.
3. If $f \in k[x_1, \dots, x_n]$ is irreducible then (f) is a prime ideal. As $k[x_1, \dots, x_n]$ is a UFD, $\sqrt{(f)} = (f)$.

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

Theorem 1.9 (Nullstellensatz)**.** *If $k = \overline{k}$, $J \subseteq k[x_1, \dots, x_n]$ then $I(Z(J)) = \sqrt{J}$.*

Proof. Let $f \in I(Z(J))$ so $f(p) = 0$ for all $p \in Z(J)$. We must show that $f^n \in J$ for some $n > 0$. Consider $k[x_1, \dots, x_n, t]/(tf - 1) = k[x_1, \dots, x_n, \frac{1}{f}]$. Let I be the ideal in this ring generated by the image of J. Claim that $Z(I) = \emptyset$: if not, let $p \in Z(I)$. As $J \subseteq I$, $p \in Z(J)$ so $f(p) = 0$. But $p = (p_1, \dots, p_n, p_t)$ with $p_t f(p_1, \dots, p_n) = 1$, i.e. $f(p) \neq 0$. Absurd.

Then the corollary to the Nullstellensatz implies that $I = k[x_1, \dots, x_n, \frac{1}{f}]$ (we used the fact $k = \overline{k}$). As $1 \in I = (J)$,

$$\sum_{i=1}^{N} \frac{\gamma_i}{f^i} = 1$$

for some $\gamma_i \in J$ for some $N \geq 1$. Multiply by f^N, get

$$f^N = \sum_{i=1}^{N} \gamma_i f^{N-i} \in J.$$

□

Remark. Let's try to deconstruct this mysterious proof. What are the points of $k[x_1, \dots, x_n, t]/(tf - 1) = k[Y]$? Here

$$Y = \{(p_1, \dots, p_n, p_t) \in \mathbb{A}^{n+1} : p_t f(p_1, \dots, p_n) = 1\}$$

which is isomorphic as a set to

$$\{(p_1, \dots, p_n) \in \mathbb{A}^n : f(p) \neq 0\} = \mathbb{A}^n \setminus Z(f).$$

So Y is a Zariski closed subset of $\mathbb{A}^{n+1}$ which is isomorphic as a set to $\mathbb{A}^n \setminus Z(f)$, and our proof was asking in what does

$$Z(f) \cap (\mathbb{A}^n \setminus Z(f)) = \emptyset$$

mean in terms of the ideal J.

Corollary 1.10. *Suppose $k = \overline{k}, I, J \subseteq k[x_1, \dots, x_n]$. Then $Z(I) = Z(J)$ if and only if $I(Z(I)) = I(Z(J))$ if and only if $\sqrt{I} = \sqrt{J}$. That is we have a bijection between*

$$\begin{tikzcd}
\{\textit{Zariski closed subsets of } \mathbb{A}^n\} \arrow[r, shift left, "I"] & \{\textit{radical ideal } I \subseteq k[x_1, \dots, x_n]\} \arrow[l, shift left, "Z"] \\
p & \mathfrak{m}_p
\end{tikzcd}$$

This is a hint that we may have an intrinsic characterisation of rings $k[Y]$. We'll do this shortly.

> **Definition** ((ir)reducible, disconnected)**.** An algebraic subset Y is *reducible* if there exist algebraic subsets $Y_1, Y_2 \neq Y$ such that $Y_1 \cup Y_2$. It is *irreducible* if is not reducible. It is *disconnected if* $Y_1 \cap Y_2 = \emptyset$.

Example.

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

In other words, Y is reducible/disconnected in Zariski topology. In usual topology, such as the usual one $\mathbb{R}$, almost every set is reducible. However, in Zariski topology there are so few closed sets that this is actually a useful definition. In fact, they have a very nice algebraic characterisation:

> **Lemma 1.11.** *Y is irreducible if and only if $I(Y)$ is a prime ideal in $k[x_1, \dots, x_n]$.*

Proof. If $Y = Y_1 \cup Y_2$ is reducible then exists $p \in Y_1 \setminus Y_2$ so exists $f \in I(Y_2)$ with $f(p) \neq 0$. Similarly exists $q \in Y_2 \setminus Y_1$ so exists $g \in I(Y_1)$ with $g(q) \neq 0$. So

$$fg \in I(Y_1) \cap I(Y_1) = I(Y).$$

But $f, g \notin I(Y)$ so $I(Y)$ is not prime.

Conversely if $I(Y)$ is not prime then exists $f_1, \dots, f_2 \in k[x_1, \dots, x_n]$ with $f_1, f_2 \notin I(Y)$ but $f_1 f_2 \in I(Y)$. Set $Y_i = Y \cap Z(f_i)$. Then $Y_1 \cup Y_2 = Y$ as for $p \in Y$, $f_1 f_2(p) = 0$ so $f_1(p) = 0$ or $f_2(p) = 0$ and $Y_i \neq Y$ as $f_2 \notin I(Y)$. □

Example. $I = (x_1, \dots, x_m) \subseteq k[x_1, \dots, x_m]$ is prime, as

$$k[x_1, \dots, x_n]/(x_1, \dots, x_m) = k[x_{m+1}, \dots, x_n]$$

is an integral domain.

Exercise. Recall that if R is a UFD, $f \in R$ nonzero then if f is irreducible then (f) is a prime ideal. Furthermore as $k[x_1, \dots, x_n]$ is a UFD, it is an exercise to check that $Z(y - x^2), Z(y^2 - x^3 + x)$ are irreducible.

Zariski topology is very different from usual topology: if X is an irreducible Zariski closed subset and $U \subseteq X$ is a nonempty Zarisk open subset in X then $\overline{U} = X$, i.e. nonempty Zariski open subsets are dense.

Proof. Let $Y = X \setminus U$ which is closed. Then $\overline{U} \cup Y = X$ and $U \neq \emptyset$ so $Y \neq X$. But X is irreducible so $\overline{U} = X$. □

Application (Cayley-Hamilton)**.** Let $A \in \mathrm{Mat}_n(k)$, an $n \times n$ matrix. Define its characteristic polynomial to be

$$\chi_A(x) = \det(xI - A) \in k[x]$$

This defines a map

$$\begin{aligned} \mathrm{Mat}_n(k) &\to \mathrm{Mat}_n(k) \\ B &\mapsto \chi_A(B) \end{aligned}$$

Then for all A, $\chi_A(A) = 0$.

Proof. Strategy:

1. The set of matrices for which Cayley-Hamilton holds is a Zariski closed subset of $\mathbb{A}^{n^2}$.

2. It holds for diagonalisable matrices, which is a Zariski open subset of $\mathbb{A}^{n^2}$.

3. Hence as $\mathbb{A}^{n^2}$ is an irreducible algebraic set, it holds for all matrices.

Let $X = \mathrm{Mat}_n(k) = k^{n^2} = \mathbb{A}^{n^2}$ be the space of matrix coefficients. It is an affine space so irreducible closed. Consider

$$C = \{A \in \mathrm{Mat}_n(k) : \chi_A(A) = 0\}.$$

Claim that this is a Zariski closed subset, cut out by n^2 equations of the form $\chi_A(A)_{ij} = 0$. We must check these equations are polynomial equations in the matrix coefficients of A. Note that

$$\chi_A(x) \in k[X \times \mathbb{A}^1] = k[\mathbb{A}^{n^2+1}],$$

i.e. $\det(xI - A)$ is a polynomial equation in $n^2 + 1$ variables: matrix coefficients of A and x. Now substitute $x = A$. Note that matrix coefficients of A^r, $(A^r)_{ij}$, are polynomials in the matrix coefficients of A (of degree r). Hence $\chi_A(A)_{ij}$ are polynomial equations in coefficients of A.

As $\mathrm{Mat}_n(k) \subseteq \mathrm{Mat}_n(\overline{k})$, suffices to prove the case $k = \overline{k}$. Note that

$$\begin{aligned} \chi_A(x) &= \chi_{gAg^{-1}}(x) \\ \chi_A(gBg^{-1}) &= g\chi_A(B)g^{-1} \end{aligned}$$

for all $g \in \mathrm{GL}_n(k)$. so $\chi_A(A) = 0$ if and only if $\chi_{gAg^{-1}}(gAg^{-1}) = 0$, so A satisfies its only characteristic polynomial if and only if gAg^{-1} does for all $g \in \mathrm{GL}_n(k)$.

Now let U be the set of all matrices with distinct eigenvalues. As $k = \overline{k}$, $A \in U$ implies that there exists $g \in \mathrm{GL}_n(k)$ such that gAg^{-1} is

$$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}$$

which clearly satisfies its own characteristic polynomial. Moreover $U \neq \emptyset$ since we can always find distinct elements $\lambda_1, \dots, \lambda_n$ of k as $k = \overline{k}$.

Left to show U is Zariski open. $A \in U$ if and only $\chi_A(x) \in k[x]$ has distinct roots. But a polynomial f has distinct roots if and only if f and f' have no common root, if and only if $\Delta(f) \neq 0$, where the discriminant $\Delta(f)$ is a polynomial in the coefficients of f. Hence $A \in U$ if and only if $\Delta(\chi_A(x)) \neq 0$, so U is Zariski open. □

Now back to the abstract characterisation of algebraic varieties. We need some preliminary definitions:

> **Definition** (nilpotent)**.** Let R be a ring. $y \in R$ is *nilpotent* if exists $n > 0$ such that $y^n = 0$.

Example.

1. If $R = k[x]$ then 0 is the only nilpotent.
2. If $R = k[x]/(x^7)$ then x is nilpotent as $x^7 = 0$.

Exercise. Let $J \subseteq k[x_1, \dots, x_n]$ be an ideal and $R = k[x_1, \dots, x_n]/J$. Then $J = \sqrt{J}$ if and only if R has no nonzero nilpotents.

Corollary 1.12. *Let $k = \overline{k}$. If $Y \subseteq \mathbb{A}^n$ is a Zariski closed subset then $k[Y]$ is a finitely generated k-algebra with no nonzero nilpotents.*

Conversely, given a finitely generated reduced k-algebra A, there exists a surjection $k[t_1, \dots, t_n] \to A$. As A is reduced, the kernel is radical. This is precisely the definition of a coordinate ring.

What do we gain from this? We need not choose a generator set of the k-algebra, which is the same as an embedding $Y \hookrightarrow \mathbb{A}^n$. In this abstract formulation, the "points" in the affine space corresponds to maximal ideals of the k-algebra.

Definition (affine algebraic variety)**.** An *affine algebraic variety* over k, where k is a field, is a finitely generated k-algebra R with no nonzero nilpotent elements.

If $k = \overline{k}$, define a *point* of R to be a k-algebra homomorphism $R \to k$. More generally if $L \supseteq k$ is a field extension then an *L-point of* R is a k-algebra homomorphism $R \to L$.

Example. Let $J = \sqrt{J} \subseteq k[x_1, \dots, x_n]$ be a radical ideal and $R = k[x_1, \dots, x_n]/J$ be an affine algebraic variety.

Coversely, if R is such an algebra, choose generators $\overline{x}_1, \dots, \overline{x}_n$ of R as a k-algebra so get a surjective map $k[x_1, \dots, x_n] \to R$ where $x_i \mapsto \overline{x}_i$. Let J be the kernel and $J = \sqrt{J}$ per the exercise above.

By Nullstellensatz, points of R is $Z(J) \subseteq k^n$ given by

$$\begin{aligned} Z(J) &\to \{R \to k\} \\ p = (p_1, \dots, p_n) &\mapsto (\mathrm{ev}_p : \overline{x}_i \mapsto p_i) \end{aligned}$$

In general, choice of generators $\overline{x}_1, \dots, \overline{x}_n$ of R is the *choice* of an embedding of points of R to $\mathbb{A}^n$.

Example. $\mathbb{R}[x]/(x^2 + 1)$ has no $\mathbb{R}$-point, but it has two $\mathbb{C}$-points, given by $x \mapsto \pm i$.

We indulge in imprecision and often write "let Y be an affine algebraic variety and $R = k[Y]$ be its ring of functions". What we really mean, when spelt out, is: let R be an affine algebraic variety with $\overline{k}$-points Y.

Definition (morphism)**.** A *morphism* $\gamma : X \to Y$ of affine algebraic varieties is a k-algebra homomorphism $\gamma^* : k[Y] \to k[X]$.

An *isomorphism* $\alpha : X \to Y$ is a morphism such that there exists an inverse morphism $\beta : Y \to X$ such that $\alpha\beta = 1_Y, \beta\alpha = 1_X$.

Let's unpack the definition. Suppose X and Y are the points of R and S respectively. If $\gamma^* : S \to R$ is a k-algebra homomorphism and $p \in X$ is a point of X, that is, if $\mathrm{ev}_p : R \to \overline{k}$ is a k-algebra homomorphism, then $\mathrm{ev}_p \circ \gamma^* : S \to \overline{k}$ is a k-algebra homomorphism, so a point in Y. Thus γ^* defines a map $X \to Y$, which we denote by γ.

So this definition is a clever way of saying the map γ is defined by polynomial equations.

Example.

1. Let $X = \mathbb{A}^1, Y = \{(x, y) \in \mathbb{A}^2 : x^2 = y^3\} = Z(x^2 - y^3)$. Let $R = k[t]$. Claim $t \mapsto (t^3, t^2)$ is a morphism $X \to Y$. Unpack the definition, we have $k[Y] = k[x, y]/(x^2 - y^3)$ and a k-algebra homomorphism
$$\begin{aligned} \gamma^* : k[x, y]/(x^2 - y^3) &\to k[t] \\ x &\mapsto t^3 \\ y &\mapsto t^2 \end{aligned}$$
Check that $x^2 - y^3 \mapsto 0$ so it is well-defined.

Unravel the definition of a morphism in general, let $k[X] = k[x_1, \dots, x_n]/(s_1, \dots, s_\ell)$, $k[Y] = k[y_1, \dots, y_m]/(r_1, \dots, r_k)$ (remember choice of generators $x_1, \dots, x_n$ is choice of embeddings $X \hookrightarrow \mathbb{A}^n$). Let $\overline{y}_1, \dots, \overline{y}_m$ denote the image of $y_1, \dots, y_m$ in $k[Y]$. An algebra homomorphism $\gamma^* : k[Y] \to k[X]$ is uniquely determined by where $\overline{y}_1, \dots, \overline{y}_m$ go, i.e. by
$$\overline{\Phi}_i = \gamma^*(\overline{y}_i) \in k[X].$$
Choose a polynomial $\Phi_i \in k[x_1, \dots, x_n]$ whose reduction is $\overline{\Phi}_i$. Such a choice determines an algebra homomorphism
$$\begin{aligned} k[y_1, \dots, y_m] &\to k[x_1, \dots, x_n] \\ y_i &\mapsto \Phi_i \end{aligned}$$
i.e. a morphism $\mathbb{A}^n \to \mathbb{A}^m$, and the conditions on the polynomials Φ_i ensure the image is in Y are the condition that the ideal $(r_1, \dots, r_k)$ is sent to 0 in $k[X]$, i.e. $r_i(\Phi_1, \dots, \Phi_m) \in (s_1, \dots, s_\ell) = 0 \in k[X]$.

Question. Is the morphism in the above example an isomorphism?

Example.

1. A morphsim $\mathbb{A}^1 \to \mathbb{A}^n$ is a k-algebra homomorphism $k[x_1, \dots, x_n] \to k[t]$, which is the same as an n-tuple of polynomials $(\Phi_1(t), \dots, \Phi_n(t))$.

2. A morphism $X \to \mathbb{A}^1$ is an k-algebra homomorphism $k[t] \to k[X]$, which is an element of $k[X]$ (i.e. where t is sent to). This says that $k[X]$ is precisely the functions $X \to \mathbb{A}^1$, which is something we knew before!

3. Suppose $\mathrm{ch}\, k \neq 2$. Is there a morphism $\mathbb{A}^1 \to E = \{(x, y) : y^2 = x^3 - x\}$? Suppose $k = \mathbb{C}$, this is asking if there is a polynomial map from the punctured sphere to the punctured torus. From analytic point of view this is impossible (there is not even an analytic functions does this). Algebraically, this is asking if there exist polynomials $a(t), b(t) \in k[t]$ such that $b^2 = a^3 - a$. See example sheet 1.

4. Let X be an affine algebraic variety and let $f \in k[X]$. Consider

$$k[X] \to k[X][t]/(tf-1) = k[Y]$$

which defines a morphism $Y \to X$. What is Y and what is the morphism? By definition a point of Y is a k-algebra homomorphism $\gamma : k[X][t]/(tf - 1) \to k$. Suppose $\gamma(t) = a$ then $\gamma|_{k[X]} = \mathrm{ev}_p$ where $p \in X$ such that $af(p) = 1$, i.e. $f(p) = \frac{1}{a} \neq 0$. Conversely, if $f(p) \neq 0$, set $a = \frac{1}{f(p)}$, we get a k-algebra homomorphism. So

$$Y = \{x \in X : f(x) \neq 0\} = X \setminus Z(f)$$

which is Zariski open, and $\gamma : Y \hookrightarrow X$ is the inclusion. In general, Zariski open sets of the form $X \setminus Z(f)$ are affine varieties in their own right, and the inclusion map is a morphism of affine varieties.

By the same argument the complement of the subvariety cut out by a single polynomial is a variety. We call them

> **Definition** (hypersurface)**.** If $f \in k[x_1, \dots, x_n]$ then $Z(f) \subseteq \mathbb{A}^n$ is called a *hypersurface.*

We may ask: is every Zariski open set also an affine variety, i.e. the image of an affine variety inside some bigger affine space under an injection?. No! $\{(x, y) \in \mathbb{A}^2 : (x, y) \neq (0, 0)\}$ is not an affine variety.

2 Smooth points, dimension & Noether normalisation

Let $X \subseteq \mathbb{A}^n$ be an affine variety and $p \in X$. Let $X = Z(I)$, $I = (f_1, \dots, f_r)$. Tentatively we define

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

Translate $T_p X$ from the origin to $p \in \mathbb{A}^n$ so the equations are

$$\{v \in \mathbb{A}^n : \sum (v_i - p_i) \frac{\partial f}{\partial x_i}(p) = 0 \text{ for all } f \in I\}.$$

This is the best linear approximation to X at the point p, as

$$f(x) = f(p) + \sum (x_i - p_i) \frac{\partial f}{\partial x_i}(p) + \dots$$

If X is complex analytic then this is indeed the analytic definition of tangent space. However it's not always the case.

Example. If $I = (x^2 - y^3)$ then

$$T_{(a,b)}(X) = \{(v_1, v_2) : v_1(2a) + v_2(-3b^2) = 0\}.$$

If $(a, b) \neq (0, 0)$ this is a line and if $(a, b) = (0, 0)$ then this is $\mathbb{A}^2$.

> **Lemma 2.1.** *$\{p \in X : \dim T_p X \geq t\}$ is a Zariski closed subset of X for all $t \geq 0$.*

Proof. Write $T_p X = \ker(A : k^n \to k^r)$ where A is the matrix

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1}(p) & \cdots & \frac{\partial f_1}{\partial x_n}(p) \\ & \ddots & \\ \frac{\partial f_r}{\partial x_1}(p) & \cdots & \frac{\partial f_r}{\partial x_n}(p) \end{pmatrix}$$

By rank-nullity, $\dim \ker A \geq t$ if and only if $\text{rank} A \leq n - t$. But rank of a matrix A is greater than or equal to s if and only if there exists an $s \times s$ subminor B with $\det B \neq 0$, which is a polynomial equation in matrix coefficients. Thus $\text{rank} A \leq n - t$ if and only if all $(n + 1 - t) \times (n + 1 - t)$ subminors have zero determinant. Hence

$$\{p \in X : \dim T_p X \geq t\} = Z(f_1, \dots, f_r, \text{ determinants of subminors}).$$

□

Definition (dimension)**.** Let X be an irreducible affine variety. Then

$$\dim X = \min\{\dim T_p X : p \in X\}.$$

If $k \neq \overline{k}$ then p is taken to be $\overline{k}$-points.

In a moment we'll show $T_p X$ is independent of embedding $X \hookrightarrow \mathbb{A}^n$.

We require X to be irreducible as if not then each component can have different dimensions and $\dim X$ is not a good notion but we may as well define it anyway: we let

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

Lemma 2.2. *Suppose $k = \overline{k}$. Let $f \in k[x_1, \dots, x_n]$ be a nonconstant irreducible polynomial. Then $Z(f)$ has dimension $n - 1$.*

Proof. $\dim T_p Z(f)$ is either n or $n-1$ as there is only one equation. If $\dim T_p Z(f) = n$ then $\frac{\partial f}{\partial x_i}(p) = 0$ for all i so if $\dim Z(f) = n$ then

$$\frac{\partial f}{\partial x_i} \in I(Z(f)) = \sqrt{(f)} = (f)$$

as (f) is prime. Write $\frac{\partial f}{\partial x_i} = fg$ for some $g \in k[x_1, \dots, x_n]$. But $\deg_{x_i} \frac{\partial f}{\partial x_i} < \deg_{x_i} f$ so $g = 0$, $\frac{\partial f}{\partial x_i} = 0$. Thus we have shown $\dim Z(f) = n$ implies that $\frac{\partial f}{\partial x_i} = 0$ for all i.

If $\operatorname{ch} k = 0$ then f is a constant, $Z(f) = \emptyset$, contradiction. If $\operatorname{ch} k = p$ this implies $f \in k[x_1^p, \dots, x_n^p]$. Claim that there exists $h \in k[x_1, \dots, x_n]$ such that $f = h^p$, contradicting f being prime: write $f = \sum a_\lambda x^{p\lambda}$ for $a_\lambda \in k$. As $k = \overline{k}$, $a_\lambda^{1/p}$ exists. Set $h(x) = \sum a_\lambda^{1/p} x^\lambda$. As $\operatorname{ch} k = p$, $h^p = f$. □

Example.

1. $\dim \mathbb{A}^n = n$.
2. Any plane curve $f(x, y)$ has dimension 1.

Definition (smooth, singular point)**.** Suppose $k = \overline{k}$. Let X be an irreducible algebraic variety and $p \in X$. p is *smooth* if $\dim T_p X = \dim X$. p is *singular* otherwise.

Thus the above lemma says that singular points form a Zariski closed subvariety and smooth points form a Zariski open subset, which is non-empty.

Proposition 2.3 (nonexaminable)**.** *If $k = \mathbb{C}$ and $\dim X = d$, then $p \in X$ is smooth if and only if there exists an isomorphism from a small ball around $0 \in \mathbb{C}^d$ to a small neighbourhood of $p \in X$ in the usual topology.*

This is obviously false in Zariski topology.

Proof. This is a consequence of implicit function theorem. □

> **Definition** (derivation)**.** Let A be a k-algebra and $\varphi : A \to k$ a k-algebra homomorphism. A *derivation centred at* φ is a k-linear map $D : A \to k$ such that
> $$D(fg) = \varphi(f)D(g) + D(f)\varphi(g)$$
> for all $f, g \in A$. Write $\operatorname{Der}(A, \varphi)$ for derivations centred at φ.

Example. $f \mapsto \frac{\partial f}{\partial x}(p)$ is a derivation centred at p.

> **Lemma 2.4.** *If $X \subseteq \mathbb{A}^n$ then for all $p \in X$,*
> $$T_pX = \operatorname{Der}(k[X], \operatorname{ev}_p).$$

Proof. If $X = \mathbb{A}^n$, $k[X] = k[x_1, \dots, x_n]$. Let $D \in \operatorname{Der}(k[X], \operatorname{ev}_p)$. Let $v_i = D(x_i)$. This gives a map

$$\begin{aligned} \operatorname{Der}(k[X], \operatorname{ev}_p) &\to \mathbb{A}^n \\ D &\mapsto (D(x_i) = v_i) \end{aligned}$$

Conversely, given $v \in \mathbb{A}^n$, define a derivation D by

$$D(f) = \sum v_i \frac{\partial f}{\partial x_i}(p).$$

In general, $k[X] = k[x_1, \dots, x_n]/(f_1, \dots, f_r)$. Let $p \in X = Z(f_1, \dots, f_r)$. Then

$$\begin{aligned} \operatorname{Der}(k[X], \operatorname{ev}_p) &= \{D \in \operatorname{Der}(k[x_1, \dots, x_n], \operatorname{ev}_p) : D|_{(f_1, \dots, f_n)} = 0\} \\ &= \{D \in \operatorname{Der}(k[x_1, \dots, x_n], \operatorname{ev}_p) : \sum v_j \frac{\partial f_i}{\partial x_j}(p) = 0 \text{ for all } i\} \end{aligned}$$

where $v_j = D(x_j)$. □

Observe that if $\alpha : X \to Y$ is a morphism of varieties, i.e. $\alpha^* : k[Y] \to k[X]$ is a k-algebra homomorphism, $D \in \operatorname{Der}(k[X], \operatorname{ev}_p)$ then $D \circ \alpha^* \in \operatorname{Der}(k[Y], \operatorname{ev}_{\alpha(p)})$. Thus we get a linear map $T_pX \to T_{\alpha(p)}Y$.

Exercise. Let $f \in k[X]$. Consider $k[X] \to k[U] = k[X][t]/(tf - 1)$. We get a morphism $U = X \setminus Z(f) \to X$. Let $p \in U$. Show this defines an isomorphism $T_pU \to T_pX$.

We have two more definitions of dimension of varieties, which agree with our current definition. To prove so we need some algebraic tools.

> **Definition** (Krull dimension)**.** Let X be an irreducible affine variety. The *Krull dimension* of X is
> $$\begin{aligned} \dim_{\mathrm{Kr}} X &= \max\{r : Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_r = X : Z_i \text{ irreducible Zariski closed}\} \\ &= \max\{r : 0 = I_r \subsetneq I_{r-1} \subsetneq \cdots \subsetneq I_0 = k[x] : I_i \text{ prime}\} \end{aligned}$$

Example.

1. If $X = \mathbb{A}^1$ then $\{\text{point}\} \subsetneq \mathbb{A}^1$ is the only such chain so X has Krull dimension 1.
2. If X is a plane curve then it has Krull dimension 1, shown in example sheet 1.

Definition (function field)**.** Let X be an irrducible affine variety. Define the *function field* of X to be

$$k(X) = \operatorname{Frac} k[X] = \bigcup_{g \in k[X]} k[X][\frac{1}{g}] = \bigcup_{g \in k[X]} k[X \setminus Z(g)]$$

which is non-zero as $k[X]$ is an integral domain.

We define the *transcendence dimension* of X to be the transcendence degree of $k(X)$ over k

$$\dim_{\mathrm{tr}} X = \operatorname{trdeg}_k k(X).$$

Example.

1. $k(\mathbb{A}^n) = k(x_1, \dots, x_n)$.
2. $E = \{(x, y) : y^2 = x^3 - x\}$. Then $k(E) = k(x)[y]/(y^2 - x^3 + x)$ which is an algebraic extension of $k(x)$, so has transcedence dimension 1.

Theorem 2.5. *Let X be an irreducible affine variety. Then*

$$\dim X = \dim_{Kr} X = \dim_{tr} X.$$

Proof. Strategy of proof: show

$$\dim \mathbb{A}^n = \dim_{\mathrm{Kr}} \mathbb{A}^n = \dim_{\mathrm{tr}} \mathbb{A}^n = n$$

then reduce to this. □

We want to describe very special maps $X \to Y$ with the property that $\dim X = \dim Y, \dim_{\mathrm{tr}} X = \dim_{\mathrm{tr}} Y$, and then show these maps exist from $X \to \mathbb{A}^n$ if $\dim X = n$.

Suppose we have X, Y affine varieties such that

1. X and Y are irreducible,
2. there exists $f \in k[Y][t]$ such that $k[X] = k[Y][t]/(f(t))$ so
$$f(t) = a_0(y) + a_1(y)t + \dots + a_N(y)t^N = f(y, t),$$
with $a_i(y) \in k[Y]$, $a_N \neq 0$. This defines a morphism $\varphi : X \to Y$.
3. f is a separable polynomial when regarded as an element of $k(Y)[t]$, i.e. let
$$F(t) = \frac{1}{a_N(y)} f(t) = t^N + \frac{a_{N-1}}{a_N} t^{N-1} + \dots + \frac{a_0}{a_N},$$
then $F(t), F'(t)$ no common roots. In other words, $k(Y) \subseteq k(X)$ is a separable algebraic extension.

Claim 1 $\varphi(X)$ contains an open, hence dense subset of Y.

Proof. By definition

$$X = \{(y_0, t_0) \in Y \times \mathbb{A}^1 : f(y_0, t_0) = 0\}$$

so if $y_0 \in Y \setminus Z(a_N)$, that is $a_N(y_0) \neq 0$, then $f(y_0, t)$ is a polynomial in t of degree N, so has exactly N roots (counting with multiplicity) over $\overline{k}$, i.e. there exists[1] $(y_0, t_0) \in X$ and $\varphi(y_0, t_0) = y_0$, in particular non-empty. □

Claim 2 There exists a non-empty Zariski open subset of Y such that the natural map $T_{(y_0,t_0)}X \to T_{y_0}Y$ is an isomorphism.

Remark. Consider $Y = \mathbb{A}^1, X = \{(y, t) : y = t^p\}$ with $\operatorname{ch} k = p$. Then

$$T_{(a,b)}X = \{(v_y, v_t) : v_y - (pt^{p-1}|_{(a,b)})v_t = 0\} = \{(0, v_t) : v_t \in \mathbb{A}^1\}$$

as $p = 0$. So $T_{(a,b)}X \to T_aY$ is the zero map. Thus separability assumption is important.

Proof. Choose generators for $k[Y]$, i.e. $Y \subseteq \mathbb{A}^n$. Then

$$\begin{aligned} T_{y_0}Y &= \{v \in \mathbb{A}^n : \sum v_i \frac{\partial h}{\partial x_i}(y_0) = 0 \text{ for all } h \in I(Y)\} \\ T_{(y_0,t_0)}X &= \{(v, \gamma) \in \mathbb{A}^n \times \mathbb{A}^1 : \sum v_i \frac{\partial h}{\partial x_i}(y_0) = 0 \text{ for all } h \in I(Y), \\ &\qquad \sum v_i \frac{\partial f}{\partial x_i}(y_0, t_0) + \gamma \frac{\partial f}{\partial t}(y_0, t_0) = 0\} \end{aligned}$$

as $I(X) = I(Y, f)$. But then

$$T_{(y_0,t_0)} = \{(v, \gamma) \in T_{y_0}Y \times \mathbb{A}^1 : \sum v_i \frac{\partial f}{\partial x_i}(y_0, t_0) + \gamma \frac{\partial f}{\partial t}(y_0, t_0) = 0\}$$

Claim this is equivalent to: there exists Zariski open subset of Y included in the above such that $\frac{\partial f}{\partial t}(y_0, t_0) \neq 0$ for all $y_0 \in U$, and this is immediate if $\frac{\partial f}{\partial t}$ is not the zero polynomial in $k[Y][t]$, but our assumption about separability implies it is not. □

$$\begin{tikzcd} \varphi^{-1}(U) \arrow[r] \arrow[d] & X \arrow[d, "\varphi"] \\ U \arrow[r] & Y \end{tikzcd}$$

where U has finite fibre and φ restricted to $\varphi^{-1}(U)$ induces isomorphism of tangent space.

Corollary 2.6.

$$\dim X = \dim Y, \dim_{tr} X = \dim_{tr} Y.$$

[1] Lecturer suddenly declares $k = \overline{k}$.

Proof. $\dim_{\text{tr}} X = \dim_{\text{tr}} Y$ is an immediate algebraic fact.

Let Y^{sm} be the smooth points of Y. As Y is irreducible, this is an open dense set and hence $U \cap Y^{\text{sm}}$ is non-empty so $\dim T_y Y = \dim Y$ if $y \in Y^{\text{sm}} \cap U$ and

$$\dim T_{(y,t)} X = \dim T_y Y = \dim Y$$

for all $(y,t) \in \varphi^{-1}(y)$. But $\varphi^{-1}(U \cap Y^{\text{sm}})$ is an open set and X is irreducible, so

$$\dim X = \dim T_x X = \dim Y$$

for all $x \in \varphi^{-1}(U \cap Y^{\text{sm}})$. □

Theorem 2.7 (Noether normalisation theorem). *Let X be an irreducible affine variety over k with $\dim X = d$. Then there exists a surjective map $p : X \to \mathbb{A}^d$ which is a composite of the above form (and in particular, $\varphi^{-1}(y)$ is a finite set for all $y \in \mathbb{A}^d$).*

Corollary 2.8.

$$\dim X = \dim \mathbb{A}^d = d = \dim_{tr} \mathbb{A}^d = \dim_{tr} X.$$

Example. Let $X = \mathbb{C}^* = \{(x,y) \in \mathbb{C}^2 : xy = 1\}$. Then Noether normalisation asserts that there is a surjection $\mathbb{C}^* \to \mathbb{C}$, i.e.

$$\begin{aligned} \mathbb{C}^* &\to \mathbb{C} \\ t &\mapsto t + t^{-1} = z \end{aligned}$$

$k[t, t^{-1}] = k[z][t]/(t^2 - zt + 1)$.

Exercise. Find a surjective map $\mathbb{A}^1 \setminus \{\lambda_1, \dots, \lambda_N\} \to \mathbb{A}^1$.

It is clear that $\varphi : X \to Y$ such that $k[X] = k[Y][t]/(f(t))$ with f monic is particularly nice. φ is surjective, the fibres are finite. Such a φ is an example of a *finite flat morphism.*

Note that $k[Y] \subseteq k[X]$ is an *integral extension* of rings.

Definition. $B \subseteq A$ is an integral extension of rings if for all $a \in A$, there exists a monic polynomial $f(t) \in B[t]$ such that $f(a) = 0$.

Lemma 2.9.

1. *If f is a monic polynomial, $B[t]/(f(t))$ is an integral extension of B.*
2. *If $C \subseteq B, B \subseteq A$ are integral extensions then so is $C \subseteq A$.*

Theorem 2.10 (Noether normalisation). *Let A be a finitely generated k-algebra where k is a field and suppose A is an integral domain. Then there exists $z_1, \dots, z_n \in A$ which generate A as a k-algebra such that*

1. *there exists d such that $z_1, \dots, z_d$ are algebraically independent over k,*
2. *for all $i > d$, z_i is algebraic over $k[z_1, \dots, z_{i-1}]$ with monic minimal polynomial F_i.*

In particular, A is integral over $k[z_1, \dots, z_d]$.

Moreover if $\operatorname{Frac} A$ *is a separable field extension of k then we can also ensure F_i's are separable polynomials, and we can always do this if $k = \overline{k}$.*

Corollary 2.11 (Nullstellensatz)**.** *If A is a finitely generated k-algebra that is also a field then $A \supseteq k$ is algebraic.*

Lemma 2.12. *If $B \subseteq A$ is an integral ring extension then*

$$B^\times = A^\times \cap B.$$

Proof. Let $b \in A^\times \cap B$. Then exists $a \in A$ such that $ab = 1$. As $A \supseteq B$ is integral, exists $c_i \in B$ such that

$$a^n + c_{n-1}a^{n-1} + \dots + c_0 = 0.$$

Multiply by b^{n-1} to get

$$a = -c_{n-1} - c_{n-2}b - \dots - c_0 b^{n-1} \in B.$$

□

Proof. Let $z_1, \dots, z_n$ be as in Noether, so A is generated by $z_1, \dots, z_n$ and $z_1, \dots, z_d$ are transcendental over k and z_i is integral over $k[z_1, \dots, z_d]$ for $i > d$. Claim that if $d > 0$ then A is *not* a field: if $d > 0$ then the units in $k[z_1, \dots, z_d]$ are just $k^\times$. So z_1 is not invertible in $k[z_1, \dots, z_d]$, so not invertible in A by the lemma. □

Proof. As A is finitely generated, there exist generators $z_1, \dots, z_n$. wlog $z_1, \dots, z_d$ are algebraically independent and A is algebraic over $k[z_1, \dots, z_d]$. If $d = n$ then done. Otherwise assume the theorem holds for all k-algebras with $\leq n-1$ generators. Let $A' = k[z_1, \dots, z_{n-1}]$. There exists nonzero $f \in k[x_1, \dots, x_n]$ such that

$$f(z_1, \dots, z_{n-1}, z_n) = 0.$$

Write $f = \sum_{i \leq N} F_i$ where $F_i \in k[x_1, \dots, x_n]$ has degree i in x_n.

Suppose k is infinite, then there exist $\lambda_1, \dots, \lambda_n \in k$ such that

$$F_N(\lambda_1, \dots, \lambda_n) \neq 0.$$

Set $x_i' = x_i - \lambda_i x_n$ for $i < n$ and $x_n' = x_n$. Note that

$$\begin{aligned} x_1^{e_1} \cdots x_n^{e_n} &= (x_1' + \lambda_1 x_n)^{e_1} \cdots (x_{n-1}' + \lambda_{n-1} x_n)^{e_{n-1}} x_n^{e_n} \\ &= \lambda_1^{e_1} \cdots \lambda_{n-1}^{e_{n-1}} x_n^{e_1 + \dots + e_n} + \text{ terms in } x_1', \dots, x_n' \text{ with lower } x_n' \text{ degree} \end{aligned}$$

Hence

$$f(x_1', \dots, x_n') = F_N(\lambda_1, \dots, \lambda_n) \cdot x_n^{e_1 + \dots + e_n} + \text{ lower } x_n \text{ degree terms.}$$

But this implies that $z_n' = z_n$ is integral over $k[z_1', \dots, z_{n-1}'] = A''$. But A'' is generated by $n-1$ elements, so inductive hypothesis gives the result.

Separability requires further argument.

If k is finite then we use an argument of Nagata: let $x_i = x_i - x_n^{\gamma_i}$ for γ_i sufficiently large. □

Exercise. Let $k = \overline{k}$ and X, Y irreducible varieties over k with $\varphi : X \to Y$ a morphism. Show that

1. $k[Y] \hookrightarrow k[X]$ if and only if $\overline{\varphi(X)} = Y$
2. If $\overline{\varphi(X)} = Y$ then $\dim X \geq \dim Y$. In fact, for all $y \in \varphi(X)$,

   $$\dim \varphi^{-1}(y) \geq \dim X - \dim Y$$

   and equality holds on a dense open subset. (hard! Require Noether normalisation)

3 Projective space

We will first define projective space as a set. Let V be a vector space over k with $\dim V = n+1$, $n \geq 0$. Define

$$\mathbb{P}V = \mathbb{P}^n = \{\text{lines through origin in } V\} = V \setminus \{0\}/k^\times.$$

Suppose $v \in V, v \neq 0$, $kv = \{\lambda v : \lambda \in k\}$ is a line. Conversely, $\ell \in \mathbb{P}V$ is a line if and only if $\ell = kv$ for any $v \in \ell \setminus \{0\}$.

Note that it is not clear that $\mathbb{P}^n$ is a variety (affine or otherwise) as it is the result of two operations, neither of which gives a variety:

1. $V \setminus \{0\}$ is not an affine algebraic variety if $\dim V > 1$.
2. quotienting a vaiety by the action of group like $k^\times$ is subtle, even if the variety is affine. This is the subject of geometric invariant theory.

The first we can do to analyse the projective space is to give it homoegeneous coordiantes. Choose a basis $e_0, \dots, e_n$ of V, i.e. an isomorphism $V \cong k^{n+1}$, write $[x_0 : \dots : x_n] \in \mathbb{P}^n$ for the line through $\sum x_i e_i$. Thus

$$[x_0 : \dots : x_n] = [\lambda x_0 : \dots : \lambda x_n]$$

for all $\lambda \in k^\times$. Claim $\mathbb{P}^n = \mathbb{A}^n \amalg \mathbb{P}^{n-1}$:

Proof. Consider $p = [x_0 : \dots : x_n]$. If $x_n = 0$, $p = [x_0 : \dots : x_{n-1} : 0]$ determines a unique point in $\mathbb{P}^{n-1}$, and conversely if $x_n \neq 0$ then

$$[x_0 : \dots : x_n] = [\frac{x_0}{x_n} : \dots \frac{x_{n-1}}{x_n} : 1].$$

This gives a bijection as required. □

Corollary 3.1.

$$\mathbb{P}^n = \mathbb{A}^n \amalg \mathbb{A}^{n-1} \amalg \dots \amalg \mathbb{A}^0.$$

This gives a nice set theoretic description of $\mathbb{P}^n$, although we still cannot quite make it into an algebraic variety by gluing together a closed and an open subset. For example, $Z(x^2 - y^3) \subseteq \mathbb{A}^2$ can be written as $k^\times \amalg \{\text{pt}\}$. On the other hand, $\mathbb{A}^1 = k^\times \amalg \{\text{pt}\}$. More data is needed.

We want to rephrase $\mathbb{P}^n = \mathbb{A}^n \amalg \mathbb{P}^{n-1}$. Let $H \leq V$ be a hyperplane, let $w_0 \in V \setminus H$ (for example $H = \{x : x_n = 0\}, w_0 = (0, \dots, 0, 1)$). Then we have an inclusion of the projectivisation of H

$$\begin{aligned} \mathbb{P}H &\hookrightarrow \mathbb{P}V \\ kv &\mapsto kv \end{aligned}$$

as well as the affine hyperplane

$$\begin{aligned} H &\hookrightarrow \mathbb{P}V \\ h &\mapsto k(h + w_0) \end{aligned}$$

It is an exercise to show that

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

with the isomorphism depends on the choice of w_0.

Set $U_i = \{x = [x_0 : \dots : x_n] \in \mathbb{P}^n : x_i \neq 0\}, H_i = \{(x_0, \dots, x_n) : x_i = 0\} \cong \mathbb{A}^n$ so $\mathbb{P}V \setminus \mathbb{P}H_i = U_i$. It is clear that

$$U_0 \cup U_1 \cup \dots \cup U_n = \mathbb{P}^n$$

as if $x = [x_0 : \dots : x_n] \in \mathbb{P}V$, some $x_i \neq 0$ and then $x \in U_i$.

Example.

1. For $n = 1$, $U_0 = \{[1 : x_1]\}, U_1 = \{[x_0 : 1]\}$. The inclusion is

$$\begin{aligned} U_0 &\to \mathbb{P}^1 \\ [x_0 : x_1] &\to \frac{x_1}{x_0} \in \mathbb{A}^1 \cup \{\infty\} \end{aligned}$$

2. $n = 2$: $\mathbb{P}^2 = U_0 \cup U_1 \cup U_2$. $\mathbb{P}^2 = U_i \amalg \mathbb{P}^1$.

   (graph) three lines at infinity in $\mathbb{P}^2$. Exercise: the pattern of $\mathbb{P}^{n-1}$'s at ∞ in $\mathbb{P}^n$ is given by the boundary of the n-simplex.

Consider such a map $j : U \hookrightarrow \mathbb{P}^n$ where $U = U_i = \mathbb{A}^n$ for some i. This is an open embedding of topological spaces. It is an exercise to check this is an open embedding of topological spaces.

As each $U_i \cong \mathbb{A}^n$ is an affine variety, and

$$\begin{aligned} U_i \cap U_j &\to U_j \\ k^\times \times \mathbb{A}^{n-1} &\to \mathbb{A}^n \end{aligned}$$

is a morphism of affine variety, the $\mathbb{P}^n$ is a well-defined algebraic variety, and $U \to \mathbb{P}^n$ is a morphism of algebraic varieties.

Lots of maps $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$ (choose a hyperplane and a point off the hyperplane. $(x_0, \dots, x_{n-1}) \mapsto (x_0, \dots, x_{n-1}, 1)$. Call the map $i : \mathbb{A}^2 \to \mathbb{P}^2$.

Let $E^0 = \{(x, y) \in \mathbb{A}^2 : y^2 = x^3 - x\}$. What is $\overline{i(E^0)}$ in $\mathbb{P}^2$? Let's work it out. As $[x : y : 1] = [X : Y : Z]$ for $z \neq 0$, have $x = \frac{X}{Z}, y = \frac{Y}{Z}$ so $y^2 = x^3 - x$ gives

$$Y^2 Z = X^3 - XZ^2$$

so

$$i(E^0) = \{[X : Y : Z] \in \mathbb{P}^2 : Y^2 Z = X^3 - XZ^2, Z \neq 0\}.$$

From now on write E^0 for $i(E^0)$. Then the closure will be the same equation but allow $Z = 0$. This can be done as follow. There are three charts: $X \neq 0, Y \neq 0, Z \neq 0$. In chart $Z \neq 0$, $y^2 = x^3 - x$. In chart $Y \neq 0$, put $z = \frac{Z}{Y}, x = \frac{X}{Y}$ so the equation for E^0 is $z = x^3 - xz^2$ and $z \neq 0$. On chart $X \neq 0$, put $y = \frac{Y}{X}, z = \frac{Z}{X}$, equation is $y^2 = 1 - z^2$ and $z = 1$. Now taking closure of E^0 in each chart gives closure of E^0 in $\mathbb{P}^2$.

If $[X : Y : Z]$ is in the chart $Y \neq 0$ but not in chart $Z \neq 0$, must have $z = 0$. The equation says $x^3 = 0$, which has a unique solution $x = 0$, so we get an extra point $[0 : 1 : 0]$.

If $[X : Y : Z]$ is in the chart $X \neq 0$ and not in the chart $Z \neq 0$ then $z = 0$ and have $0 = 1$ which has no solution, so no extra point.

Thus the projective curve E, defined as the closure of E^0 in $\mathbb{P}^2$, is $E^0 \cup \{[0 : 1 : 0]\}$, which is what we wanted in the first lecture.

In general, given $X = Z(I) \subseteq \mathbb{A}^n$ where $I \subseteq k[x_1, \dots, x_n]$, we may ask what is the closure of X in $\mathbb{P}^n$ under the embedding $(x_1, \dots, x_n) \mapsto [1 : x_1 : \dots : x_n]$. To do so we would like to talk about varieties in projective spaces just as in affine spaces. However, note that the zero of a general polynomial in $\mathbb{P}^n$ is not well-defined as it is not invariant under the action of $k^\times$.

> **Definition** (homogeneous polynomial)**.** Given $f \in k[x_1, \dots, x_n]$, f is *homogeneous* of degree d if
>
> $$f = \sum_{c_1+\dots+c_n=d} a_{i_1\cdots i_n} x_1^{i_1} \cdots x_n^{i_n}.$$
>
> If k is infinite then this holds if and only if
>
> $$f(\lambda x_1, \dots, \lambda x_n) = \lambda^d f(x_1, \dots, x_n)$$
>
> for all $\lambda \in k^\times$.

Any $f \in k[x_1, \dots, x_n]$ can be written as $f = \sum_{r=0}^n f_{(r)}$ where $f_{(r)}$ is homogeneous of degree r.

> **Definition** (homogeneous ideal)**.** An ideal $I \subseteq k[x_1, \dots, x_n]$ is if for all $f \in I$, $f = \sum_r f_{(r)}$ then $f_{(r)} \in I$ for all I.

Example. $(xy + y^2, y^3, x^2)$ is homogeneous but $(xy + y^3)$ is not.

Given $f \in k[x_1, \dots, x_n]$, we homogenise it by defining

$$\tilde{f}(X_0, \dots, X_n) = X_0^d f(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0})$$

where $d = \deg f$. f can be recovered by

$$\tilde{f}(1, x_1, \dots, x_n) = f(x_1, \dots, x_n).$$

Example. If $f = y^2 - x^3 + x$ then

$$\tilde{f} = Z^3((Y/Z)^2 - (X/Z)^3 + (X/Z)) = ZY^2 - X^3 + XZ^2.$$

For an ideal $I \subseteq k[x_1, \dots, x_n]$, define

$$\tilde{I} = (\tilde{f} : f \in I),$$

Exercise. $\tilde{I}$ is an ideal and is homogeneous. $\tilde{I}|_{X_0=1} = I$.

> **Lemma 3.2.**
>
> 1. *$I \subseteq k[x_1, \dots, x_n]$ is homogeneous if and only if I is generated by a finite set of homogeneous polynomials.*
>
> 2. *Suppose k is infinite. $\tilde{I} \subseteq k[x_0, \dots, x_n]$ is a homogeneous ideal if*

and only if $\tilde{X} = Z(\tilde{I}) \subseteq \mathbb{A}^{n+1}$ *is invariant under the* $k^\times$*-action* $(p_0,, \dots, p_n) \mapsto (\lambda p_0, \dots \lambda p_n)$.

Proof. Exercise. □

This shows that Zariski closed subsets of $\mathbb{P}^n$, defined to be zeros cut out by homogeneous ideals in $k[x_0, \dots, x_n]$, are well-defined. They correspond to $k^\times$-invariant closed subsets of $\mathbb{A}^{n+1}$.

Note. If $I = (f_1, \dots, f_r) \subseteq k[x_1, \dots, x_n]$, it need *not* be the case that $\tilde{I} = (\tilde{f}_1, \dots, \tilde{f}_r)$. For example given $I = (x - y^2, y) = (x, y) = I(\{0\})$,

$$(xz - y^2, y) = (xz, y) \neq (x, y) = \tilde{I}.$$

Exercise. Find an ideal such that $\tilde{I} \neq (\tilde{f}_1, \dots, \tilde{f}_r)$ for any minimal generator $f_1, \dots, f_r$ of I.

Definition (quasi-projective/affine variety)**.** A *quasi-projective variety* is an open subvariety of a projective variety.

A *quasi-affine variety* is an open subvariety of an affine variety.

Example. $\mathbb{C}^2 \setminus \{(0,0)\} \subseteq \mathbb{C}^2$ is a quasi-affine variety.

Remark. If X is an affine variety, $f \in k[X]$ and X is irreducible, $k[X \setminus Z(f)] = k[X][\frac{1}{f}]$ so

$$k(X \setminus Z(f)) = \operatorname{Frac} k[X \setminus Z(f)] = \operatorname{Frac} k[X] = k(X).$$

Hence if X is an affine algebraic variety, we can define $k(X)$ to be $k(U)$ for U any open affine subvariety of X, for example for U an open set in a chart defining X.

For example in $\mathbb{P}^n$,

$$k(U_0) = k(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}) = k(U_n) = k(\frac{x_0}{x_n}, \dots, \frac{x_{n-1}}{x_n}).$$

We end this chapter with a brief discussion of compactness of projective spaces. Let $k = \mathbb{C}$. Claim

$$\mathbb{P}^n = (\mathbb{C}^{n+1} \setminus \{0\})/\mathbb{C}^\times = S^{2n+1}/S^1.$$

Proof. Define

$$S^{2n+1} = \{x \in \mathbb{C}^{n+1} : \|x\| = 1\}$$

where $\|x\| = (\sum |x_i|^2)^{1/2}$. Consider the map

$$\begin{aligned} \mathbb{C}^{n+1} \setminus \{0\} &\to S^{2n+1} \\ x = (x_0, \dots, x_n) &\mapsto \frac{1}{\|x\|}(x_0, \dots, x_n) \end{aligned}$$

$|\lambda| = 1$, i.e. $\lambda \in \mathbb{C}^*$ if and only if $\|\lambda x\| = \|x\|$ so this descends to a map

$$(\mathbb{C}^{n+1} \setminus 0)/\mathbb{C}^\times \to S^{2n+1}/S^1.$$

□

S^{2n+1} is compact in the usual topology and so is its quotient. Thus $\mathbb{P}^n$ is compact in the usual topology. Surprisingly, this has an algebraic version in the Zariski topology.

Definition (proper)**.** X is *proper* if for every continuous map $\varphi : X \to Y$, the image of a closed subset under φ is closed.

Theorem 3.3 (fundamental theorem of elimination theory)**.** *For any field k, $\mathbb{P}^n$ is proper.*

Corollary 3.4. *If $X \subseteq \mathbb{A}^n$ is an affine variety and X is proper then X is a finite set of points.*

Proof. Suppose X is not a finite set of points. Then as X is affine there exists a non-constant element $\varphi \in k[X]$, that is a morphism $\varphi : X \to \mathbb{A}^1$ which is not constant. But X is proper so $\operatorname{im} \varphi$ is closed and by assumption, $\varphi(X)$ is not a finite set of points. Hence $\varphi(X) = \mathbb{A}^1$. Define $\tilde{\varphi} : X \to \mathbb{P}^1$ to be the obvious composition. The image of $\tilde{\varphi}$ is $\mathbb{A}^1$ which is not closed in $\mathbb{P}^1$ so X is not proper. Contradiction. □

4 Curves

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

> **Definition** (curve)**.** A *curve* is a quasi-projective algebraic variety X such that $\dim X = 1$.

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

Warning: not all curves can be embedded in $\mathbb{P}^2$.

Exercise. $\dim X = 1$ means that for all $p \in X \setminus \{\text{finite set}\}$, $\dim T_p X = 1$, if and only if $\dim_{\text{tr}} k(X) = 1$, if and only if any Zariski closed subvariety of X is X or a finite set of points.

> **Definition.** Let X be an irreducible algebraic variety and $p \in X$. Define the *local ring* at p to be
>
> $$\mathcal{O}_{X,p} = \{\frac{f}{g} \in k(X) : g(p) \neq 0\},$$
>
> rational functions defined on some neighbourhood of p. Define
>
> $$\mathfrak{m}_{X,p} = \{\gamma \in \mathcal{O}_{X,p} : \gamma(p) = 0\},$$
>
> the maximal ideal of $\mathcal{O}_{X,p}$.

Exercise.

1. If $\gamma \in \mathcal{O}_{X,p} \setminus \mathfrak{m}_{X,p}$ then $\gamma^{-1} \in \mathcal{O}_{X,p}$.
2. Show $\mathfrak{m}_{X,p}$ is the unique maximal ideal of $\mathcal{O}_{X,p}$.

Suppose $k = \mathbb{C}$. Let X be a curve, $p \in X$ a smooth curve. Then a small open neighbourhood of p in the usual topology is diffeomorphic to a small open neighbourhood of 0 in $\mathbb{C}$ by implicit function theorem. The corresponding notion is convergent power series on some neighbourhood of p. It is completely analogous that here is an algebraic replacement for it.

> **Theorem 4.1.** *Let X be a curve, $p \in X$ a smooth point. Write $\mathfrak{m} = \mathfrak{m}_{X,p}$.*
>
> *1. $\mathfrak{m}$ is a principal ideal in $\mathcal{O}_{X,p}$.*
>
> *2. $\bigcap_{n \geq 1} \mathfrak{m}^n = \{0\}$.*

Example. Intuition: Consider $\{x^2 + y^2 = 1\} \subseteq \mathbb{A}^1$. If $p \neq (0, \pm 1)$ then $y - y_0$ is a “local coordinate” at p. If $k = \mathbb{C}$, $p \neq (0, \pm 1)$, then we can write x in terms of y as a convergence power series for $|y - y_0| < \varepsilon$. For example at $(1, 0)$,

$$x = (1 - y^2)^{1/2} = \sum_{n \geq 0} \binom{1/2}{n} (-1)^n y^{2n}$$

so

$$x - 1 = -\frac{1}{2}y^2 + \text{ high order terms}$$

so $x-1$ vanishes to order 2 at the point. In the theorem,

$$\mathfrak{m}_{X,p} = (y - y_0)$$

if $\frac{\partial f}{\partial x}(p) \neq 0$. Alternatively,

$$x - 1 = \frac{x^2-1}{x+1} = -\frac{y^2}{x+1}$$

and $\frac{1}{x+1} \in \mathcal{O}_{X,p} \setminus \mathfrak{m}_{X,p}$.

Proof. By definition of X there exists an affine open neighbourhood X_0 of p, i.e. an open subset $X_0 \subseteq X$ which is an affine variety. Write $k[X_0] = k[x_1, \dots, x_n]/I$. wlog $p \in X_0$ corresponds to the point $(0, \dots, 0)$. Let us write $\overline{x}_i$ for the image of x_i in $k[X_0]$. Then

$$\begin{aligned} \mathcal{O}_{X,p} &= \{\frac{f}{g} : f, g \in k[X_0], g \notin (\overline{x}_1, \dots, \overline{x}_n)\} \\ \mathfrak{m}_{X,p} &= \{\frac{f}{g} : f \in (\overline{x}_1, \dots, \overline{x}_n), g \notin (\overline{x}_1, \dots, \overline{x}_n)\} \end{aligned}$$

X is a curve smooth at p so $\dim T_p X_0 = 1$. Thus $T_p X_0 \subseteq \mathbb{A}^n$ is a line, and by changing coordinates we can assume it is the line $x_2 = x_3 = \dots = x_n = 0$. In other words, if $\tilde{f}_2, \tilde{f}_3, \dots$ generate the ideal I then write

$$\tilde{f}_i = \sum a_{ij} x_j + \text{ quadratic and higher term.}$$

Note that the higher terms do not contribute to the tangent space at 0. Thus $\dim T_0 X = 1$ implies that $\dim \ker(a_{ij}) = 1$, so by row reduction can assume that

$$\tilde{f}_i = \lambda_i x_i + \text{ high order terms}$$

for $i = 2, \dots, n$ and

$$\tilde{f}_i = \text{ quadratic and higher terms}$$

for $i > n$. So there exist $\tilde{f}_2, \dots, \tilde{f}_n \in I$, $\tilde{f}_i = x_i + h_i$ where h_i is at least quadratic.

Thus in $k[X_0]$, $\overline{x}_j = -h_j$ and

$$\overline{x}_j \in (\overline{x}_1^2, \overline{x}_1\overline{x}_2, \dots) = \mathfrak{m}^2$$

for $j \geq 2$. Thus

$$\mathfrak{m} = (\overline{x}_1, \dots, \overline{x}_n) = \overline{x}_1 \mathcal{O}_{X,p} + \dots + \overline{x}_n \mathcal{O}_{X,p} = \overline{x}_1 \mathcal{O}_{X,p} + \mathfrak{m}^2$$

We want to conclude that $\mathfrak{m} = (\overline{x}_1)$. Invoke Nakayama's lemma

Proposition 4.2. *Let R be a ring, M a finitely generated R-module, $J \subseteq R$ an ideal. Then*

1. *if $JM = M$ then exists $r \in J$ such that $(1 + r)M = 0$.*

2. *if $N \subseteq M$ is a submodule such that $JM + N = M$ then there exists*

> *$r \in J$ such that $(1+r)M = N$.*

Apply Nakayama to $R = \mathcal{O}_{X,p}, J = \mathfrak{m}_{X,p}$ and note that $1 + r \in \mathcal{O}^*_{X,p}$ if $r \in \mathfrak{m}_{X,p}$, so

$$(1+r)M = M.$$

We would like to apply Nakayama to $M = \mathfrak{m}_{X,p}, N = (x_1)$, so need to show M is finitely generated. But every ideal $J \subseteq \mathcal{O}_{X,p}$ is finitely generated,

$$J = \{\frac{f}{g} : f \in J \cap k[X_0], g \in k[X_0], g(p) \neq 0\}$$

so $g \cdot \frac{f}{g} = f \in J \subseteq k[X_0]$, but $J \cap k[X_0]$ is an ideal in $k[X_0]$, hence finitely generated by Hilbert basis theorem. As

$$\mathfrak{m} = (x_1) + \mathfrak{m}^2,$$

Nakayama 2 says that $\mathfrak{m} \subseteq (x_1)$. But $(x_1) \subseteq \mathfrak{m}$ so equality. In particular $\mathfrak{m}$ is the principal ideal generated by x_1.

Now let $M = \bigcap_{n \geq 1} \mathfrak{m}^n$, $J = \mathfrak{m} \subseteq \mathcal{O}_{X,p}$ so a finitely generated ideal. But $\mathfrak{m}M = M$ so by Nakayama 1 $M = 0$. □

Exercise. Apply this to the circle.

Let $X = Z(f) \subseteq \mathbb{A}^2$ be a plane curve, $p = (x_0, y_0) \in X$ a smooth point. Then $x - x_0$ generate $\mathfrak{m}_{X,p}$ if and only if $\frac{\partial f}{\partial y}(x_0, y_0) \neq 0$, and a similar statement holds for y. Thus if

$$\frac{\partial f}{\partial x}(p) = \frac{\partial f}{\partial y}(p) = 0$$

then p is not a smooth point. Thus we can either write y in terms of x locally or vice versa near a smooth point.

Exercise: check this is immediate from the theorem and its proof.

> **Definition.** A function $t \in \mathfrak{m}_{X,p}$ such that $\mathfrak{m}_{X,p} = (t)$ is called a *local parameter* or *local coordinate* at p.

Such is not unique but if t is a local parameter so is ut if $u \in \mathcal{O}^*_{X,p}$ and all other local parameters are of this form.

> **Corollary 4.3** (order of vanishing/pole)**.** *Every $f \in k(X)^*$ can be written uniquely as*
>
> $$f = t^n \cdot u$$
>
> *where $n \in \mathbb{Z}, u \in \mathcal{O}^*_{X,p}$. We call $n = \nu_p(f)$ the* order of vanishing/pole *of f at p.*
>
> $$\mathcal{O}_{X,p} = \{f \in k(X) : \nu_p(f) \geq 0\} \cup \{0\}$$
> $$\mathfrak{m}_{X,p} = \{f \in k(X) : \nu_p(f) \geq 1\} \cup \{0\}$$

This is independent of the choice of t.

Proof. Given $f \in \mathcal{O}_{X,p}$, as $\bigcap_{n\geq 0} \mathfrak{m}^n = 0$, there exists a unique $n \geq 0$ such that $f \in \mathfrak{m}^n \backslash \mathfrak{m}^{n+1}$. Define $\nu_p(f) = n$. As $\mathfrak{m}^n = (t^n)$, $f = t^n u$ with $u \in \mathcal{O}_{X,p} \backslash \mathfrak{m}_{X,p} = \mathcal{O}^*_{X,p}$. Note if $t^n u' = t^m u$ where $n \geq m$ then $t^{n-m} = u' u^{-1} \in \mathcal{O}^*_{X,p}$ so $n = m$.

If $f \in k(X)^*$, $f \notin \mathcal{O}_{X,p}$ then f^{-1} is. Apply the above and define $\nu_p(f) = -\nu_p(f^{-1})$. □

Example. $X = \mathbb{P}^1$ so $k(X) = k(x)$. Let $f \in k(x), f \neq 0$. Then $f = \prod (x - a_i)^{n_i}$, where a_i's are distinct. Consider $\nu_p(f)$.

1. If $p = a \in \mathbb{A}^1$, i.e. $p \neq \infty$, then a local coordinate t is $x - a$ so
$$\nu_a(f) = \begin{cases} 0 & a \notin \{a_1, \dots, a_m\} \\ n_i & a = a_i \end{cases}$$
2. If $p = \infty$ then $\frac{1}{x}$ is a coordinate.
$$f(x) = (\frac{1}{x})^{-\sum n_i} \underbrace{\prod (1 - \frac{a_i}{x})^{n_i}}_{\text{regular at } \infty}$$
so $\nu_\infty(f) = -\sum n_i$.

Proof of Nakayama. Let M be generated by $m_1, \dots, m_n$ as an R-module. As $JM = M$, there exists $x_{ij} \in J$ such that $m_i = \sum x_{ij} m_j$, i.e.
$$\sum_j \underbrace{(\delta_{ij} - x_{ij})} m_j = 0$$
for all i. Recall that
$$X \cdot \operatorname{adj} X = \det X \cdot I,$$
so multiply the above by $\operatorname{adj}(I - X)$ to get $dm_i = 0$ for all i, where
$$d = \det(I - X) = 1 + r$$
for some $r \in J$. expanding out the det, i.e. $(1 + r)M = 0$ as required.

The second part is immediate by applying Nakayama's lemma to M/N. □

Exercise. Show
$$\mathcal{O}_{X,p}/\mathfrak{m}^n = \mathcal{O}_{X,p}/(t^n) = k[t]/(t^n).$$
(inverse limit)

Discussion on projective space having no holes:

> **Proposition 4.4.** *Let X be a curve, $U = X \setminus \{\text{finite set of points}\}$ and $\alpha : U \to Y$ a morphism with Y a projective variety. Let $p \in X$ be smooth. Then α extends to a morphism $U \cup \{p\} \to Y$.*

Proof. wlog $Y = \mathbb{P}^m$ (by continuity). In some neighbourhood of p, $\alpha = [f_0 : \cdots : f_m]$ where $f_i \in k(X)$. Let t be a local coordinate at p. Let $n_i = \nu_p(f_i)$ so either $f_i(p) = 0$ or $f_i = t^{n_i} u_i$ where $u_i \in \mathcal{O}^*_{X,p}$. Let $N = \min\{n_1, \dots, n_m\}$, say it is attained at n_j, that is $N = n_j$ for some j. Then
$$\alpha = [t^{-N} f_0 : \cdots : t^{-N} f_m]$$
but $f_i t^{-N} \in \mathcal{O}_{X,p}$ has no pole at p and $f_j t^{-N} = u_j$ which does not vanish at p. □

> **Definition** (rational map)**.** Let X, Y be arbitrary algebraic varieties. A *rational map* $\varphi : X \dashrightarrow Y$ is a pair of a Zariski open $U \subseteq X$ and a morphism $\varphi : U \to Y$ (i.e. it is a partially defined map).

Using this terminology, the proposition is saying that a rational map to a projective variety extends to a smooth point.

Example. If $F_0, \dots, F_m$ are homogeneous polynomials of degree d in $X_0, \dots, X_n$ then

$$[X_0 : \cdots : X_n] \mapsto [F_0(X) : \cdots : F_m(X)]$$

is a rational map $\mathbb{P}^n \dashrightarrow \mathbb{P}^m$ defined on the open set where some F_i is nonzero, i.e. on the complement of $Z(F_0, \dots, F_n)$.

> **Definition.** Two rational maps $\varphi_1, \varphi_2 : X \dashrightarrow Y$ defined on U_1, U_2 are *equal* if there exists a Zariski open $V \subseteq U_1 \cap U_2$ with $\varphi_1|_V = \varphi_2|_V$. That is, the rational map defined by φ doesn't depend on U — we can shrink and think of them as the same rational map.

> **Definition.** X, Y are *birational* if there exist rational maps $\varphi : X \dashrightarrow Y, \psi : Y \dashrightarrow X$ such that
>
> $$\begin{aligned} \psi\varphi &= \mathrm{id}_X \\ \varphi\psi &= \mathrm{id}_Y \end{aligned}$$
>
> as rational maps.

Remark. The proposition is false if $\dim X > 1$ or $p \in X$ is not smooth. For example

$$\begin{aligned} \mathbb{A}^2 &\dashrightarrow \mathbb{P}^1 \\ (x, y) &\mapsto \frac{x - y}{x + y} \end{aligned}$$

cannot be extended to $(0, 0)$. More interestingly, consider

$$[X : Y : Z] \mapsto [YZ : XZ : XY] \text{``}=\text{''} [\frac{1}{X} : \frac{1}{Y} : \frac{1}{Z}]$$

which cannot be extended to three points. This is the beginning of high dimensional algebraic geometry.

> **Proposition 4.5.** *Let $\alpha : X \to Y$ be a nonconstant morphism of irreducible curves.*
>
> 1. *For all $q \in Y$, $\alpha^{-1}(q)$ is a finite set.*
> 2. *α induces an embedding of fields $k(Y) \hookrightarrow k(X)$ such that $[k(X) : k(Y)]$ is finite.*

Definition (degree)**.** The degree of the extension is called the *degree* of α.

Proof.

1. $\alpha^{-1}(q)$ is a closed subset of X. But the only closed subsets are fintie set of points and X. As α is nonconstant the result follows.

2. If $f \in k(Y)$ then exists $U \subseteq Y$ affine such that $f \in k[U]$. Then $f \circ \alpha : \alpha^{-1}(U) \to k$ is well-defined in $k[\alpha^{-1}(U)] \subseteq k(X)$ so we have a map of fields $k(Y) \to k(X)$. Have $k \subseteq k(Y) \subseteq k(X)$ where $k(X)$ and $k(Y)$ are both algebraic over k. Thus $k(X)/k(Y)$ is algebraic.

□

Example. Consider the morphism

$$\begin{aligned} \alpha : \mathbb{A}^1 &\to \mathbb{A}^1 \\ z &\mapsto z^r \end{aligned}$$

which induces a filed extension $k(Y) = k(y) \subseteq k(X) = k(x), y \mapsto x^r$ so $k(x^r) \subseteq k(x)$. The degree of α is r.

Let $\alpha : X \to Y$ be a nonconstant morphism of smooth irreducible projective curves. Then α is surjective (as $\alpha(X) \subseteq Y$ is a closed subvariety (?) and not a finite set of points). Let $y \in Y, t \in \mathcal{O}_{Y,y}$ a local coordinate. If $x \in X, \alpha(x) = y$. Then $t \circ \alpha \in \mathcal{O}_{X,x}$, i.e. $t \circ \alpha$ is a function defined in some neighbourhood of $x \in X$. So we can ask what is the order of vanishing of $t \circ \alpha$ at x, i.e. $\nu_x(t\alpha)$. Call this the *multiplicity* or *ramification index* of α at x, denote it $e_\alpha(x)$. How to calculate this? Choose a local parameter s at x then $t\alpha = s^n \cdot u$ for some $n \geq 0, u \in \mathcal{O}^*_{X,x}$. Then $n = \nu_x(t\alpha) = e_\alpha(x)$.

Example. Assume $\operatorname{ch} k \nmid r$ and consider

$$\begin{aligned} \alpha : \mathbb{A}^1 &\to \mathbb{A}^1 \\ z &\mapsto z^r \end{aligned}$$

Let's compute $e_\alpha(x)$. Suppose $a \in \mathbb{A}^1$. A local parameter at $\alpha(a) = a^r$ is $t = x - a^r$. Now

$$t \circ \alpha(x) = x^r - a^r = \prod_{i=0}^{r-1} (x - \zeta^i a)$$

where ζ is a primitive rth root of unity (here we used the assumption $\operatorname{ch} k \nmid r$). Hence

$$\nu_a(x^r - a^r) = \begin{cases} 1 & a \neq 0 \\ r & a = 0 \end{cases}$$

as $x - a$ is a local parameter at a.

Notice that $\#\alpha^{-1}(a) = r$ for all $a \in \mathbb{A}^1$ if we count the points with multiplicity. This is a general phenomenon.

Theorem 4.6 (finiteness theorem)**.** *Let $\alpha : X \to Y$ be a morphism of smooth projective irreducible curves. Then*

1. *for all $y \in Y$,*
$$\sum_{x\in\alpha^{-1}(y)} e_\alpha(x) = \deg\alpha.$$

2. *if $k(X)/k(Y)$ is separable then $e_\alpha(x) = 1$ for all but finitely many $x \in X$.*

Exercise. Check the separability assumption in 2 is necessary.

Proof. Omitted. □

Corollary 4.7. *Let nonzero $f \in k(X)$ where X is a smooth projective curve. Then the number of zeros of f equals to the number of poles of f. More precisely, there are only finitely many zeros and poles, $\{p \in X : \nu_p(f) \neq 0\}$ is finite and*
$$\sum_{p\in X} \nu_p(f) = 0.$$

Cauchy's theorem implies this if $k = \mathbb{C}$.

Proof. $f \in k(X)$ is a rational map $X \dashrightarrow \mathbb{P}^1$. As X is smooth this extends to a well-defined morphism of algebraic varieties $X \to \mathbb{P}^1$. Now $x \in k(\mathbb{P}^1)$ is a local coordinate around $0 \in \mathbb{P}^1$, so if $f(p) = 0$ then $e_f(p) = \nu_p(f)$. $\frac{1}{x}$ is a local coordinate around $\infty \in \mathbb{P}^1$ so if $f(p) = \infty$ then $e_f(p) = -\nu_p(f)$. If $f(p) \neq 0$ or ∞ then $\nu_p(f) = 0$. Thus finiteness theorem says that
$$\deg f = \sum_{p:f(p)=0} \nu_p(f) = \sum_{p:f(p)=\infty} -\nu_p(f)$$
and hence the result. □

The rest of this course aims to answer the question, given a curve and points on the curve, can we find a function with prescribed order of vanishing at these points?

Definition (divisor)**.** A *divisor* D on a curve X is a formal sum $D = \sum n_i P_i$ where $n_i \in \mathbb{Z}, P_i \in X$ and only finitely many nonzero terms. $\mathrm{Div}(X)$ is the abelian group of all divisors on X, i.e. the free abelian group generated by points of X.

There is a homomorphism
$$\begin{aligned}\deg : \mathrm{Div}(X) &\to \mathbb{Z}\\ \sum n_i P_i &\mapsto \sum n_i\end{aligned}$$

If $f \in k(X)$, define
$$\mathrm{div}(f) = \sum_{p\in X} \nu_p(f) p.$$

We just saw that
$$\deg \mathrm{div}(f) = 0.$$

Define $\mathrm{Div}^n(X) = \{D \in \mathrm{Div}(X) : \deg D = n\}$. Divisors of the form $\mathrm{div}(f)$ are called *principal divisors*, denoted $\mathrm{div}\, k(X)^*$. We will study

$$\mathrm{Cl}(X) = \mathrm{Pic}(X) = \mathrm{Div}(X)/\,\mathrm{div}\, k(X)^*,$$

the class group, Picard group or group of line bundles on X. Note that we have an induced homomorphism $\deg : \mathrm{Cl}(X) \to \mathbb{Z}$.

Proposition 4.8. *If $X = \mathbb{P}^1$ then $\mathrm{Cl}(X) = \mathbb{Z}$.*

Remark. We will show this characterises $\mathbb{P}^1$.

Proof. For any curve X, $\deg : \mathrm{Cl}(X) \to \mathbb{Z}$ is surjective so we must show $\ker(\deg : \mathrm{Cl}(X) \to \mathbb{Z}) = 0$, i.e. any degree 0 divisor is of the form $\mathrm{div}(f)$.

Let

$$D = \sum_{a \in \mathbb{A}^1} n_a(a) + n_\infty(\infty)$$

so $0 = \deg D = \sum n_a + n_\infty$ implies that $n_\infty = -\sum n_a$. Consider $f(x) = \prod_{a \in \mathbb{A}^1}(x-a)^{n_a}$. It is clear that $\mathrm{div}(f) = D$. □

Write $[D]$ for the class of $D \in \mathrm{Div}(X)$ in $\mathrm{Cl}\, X$ and $D \sim D'$ if $[D] = [D']$, i.e. if $D = D' + \mathrm{div}(f)$ for some $f \in k(X)^*$.

If $D = \sum n_i P_i$, say D is *effective* if $n_i \geq 0$ for all i. Write $D \geq 0$.

Example. Let $\alpha : X \to Y$ be a morphism. Then $\sum_{x \in \alpha^{-1}(y)} e_\alpha(x)(x)$ is an effective divisor of degree $\deg \alpha$.

Suppose $k = \overline{k}$ and let X be a smooth irreducible projective curve. Let $D = \sum_{i=1}^n n_i P_i$ be a divisor. Let

$$\begin{aligned} L(D) &= \{f \in k(X)^* : D + \mathrm{div}(f) \geq 0\} \cup \{0\} \\ &= \{f \in k(X)^* : \nu_{p_i}(f) \geq -n_i, \nu_p(f) \geq 0 \text{ for } p \notin \{p_1, \dots, p_r\}\} \cup \{0\} \end{aligned}$$

As $\nu_p(f+g) \geq \min\{\nu_p(f), \nu_p(g)\}$, $L(D)$ is a vector space (usual notation: $\Gamma(X, \mathcal{O}(D))$).

Example.

1. $L(nP) = \{f \in k(X)$ with a pole of order $\leq n$ at p and no other poles$\}$
2. If $X = \mathbb{P}^1$, $L(n(\infty))$ is the set of polynomials of degree $\leq n$. $L(n(\infty) - (a))$ where $a \in \mathbb{A}^1$ equals to $(x-a) \cdot \{$polynomials of deg $\leq n-1\}$.

Lemma 4.9.

1. *If $\deg D < 0$ then $L(D) = 0$.*
2. *$L(0) = k$.*
3. *If $D \sim D'$, i.e. $D = D' + \mathrm{div}(g)$ where $g \in k(X)^*$ then*

$$\begin{aligned} L(D) &\to L(D') \\ f &\mapsto fg \end{aligned}$$

is an isomorphism.

> 4. *If* $L(D) \neq 0$ *then there exists* $D' \geq 0$ *with* $D' \sim D$.
>
> 5. $\dim L(D) \leq \deg D + 1$ *if* $\deg D \geq 0$. *Indeed,*
>
> $$\dim L(D) \leq \dim(L(D-p)) + 1$$
>
> *for all* $p \in X$.

Proof.

1. If $f \in L(D)$ then $\deg f \leq \deg D$ from the definition. But $\deg f \geq 0$.

2. Exercise.

3. As $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g)$ since $\nu_p(fg) = \nu_p(f) + \nu_p(g)$.

4. Obvious from definition.

5. Induct on $\deg D$. If $\deg D < 0$ then $L(D) = 0$ by 1. Pick $p \notin \{p_1, \dots, p_r\}$. Consider the map $\lambda : L(D) \to k, f \mapsto f(p)$. This is well-defined as f has no pole at p. Then $f \in \ker \lambda$ if and only if $f \in L(D)$ and $\nu_p(f) \geq 1$, if and only if $f \in L(D-p)$. Note that λ need not be surjective. As $\ker \lambda = L(D-p)$, induction gives

$$\dim L(D) \leq 1 + \dim L(D-p) \leq 1 + (\deg D - 1) + 1$$

by induction. More generally, if $D = n_p \cdot p + \sum_{q \neq p} n_q \cdot q$ then define

$$\begin{aligned} \lambda : L(D) &\to k \\ f &\mapsto (t^{n_p} f)(p) \end{aligned}$$

if t is a local coordinate at p.

□

> **Definition.**
> $$\ell(D) = \dim L(D).$$

Example. If $X = \mathbb{P}^1$ and $\deg D = n \geq 0$ then $\ell(D) = \deg D + 1$.

Proof. By 3, this only depends on $[D] \in \mathrm{Cl}(\mathbb{P}^1) \cong \mathbb{Z}$, so may as well take $D = n(\infty)$ and we have $\ell(n(\infty)) = n + 1$. □

Example. Let $E^0 = \{(x, y) \in \mathbb{A}^2 : y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)\}$ where λ_i's are distinct and $\lambda_1\lambda_2\lambda_3 \neq 0$. Let E be the plane curve contained in $\mathbb{P}^2$ defined by this, i.e. the closure of E^0 in $\mathbb{P}^2$. (Recall that E is the projective variety given by

$$ZY^2 = (X - \lambda_1 Z)(X - \lambda_2 Z)(X - \lambda_3 Z).$$

It has an extra point when $Z = 0$, which implies $X = 0, Y \neq 0$, so a unique point at ∞, $P_\infty = [0 : 1 : 0]$)

We will compute $L(nP_\infty)$ for n small. Start by computing $\operatorname{div}(x), \operatorname{div}(y)$. $x = 0$ when $y = \pm\sqrt{\lambda_1\lambda_2\lambda_3} = \pm c$. $x = \infty$ at P_∞. Note that at $(x, y) = (0, \pm c)$, $\frac{\partial f}{\partial y} \neq 0$ so x is a local parameter at these points and so

$$\operatorname{div}(x) = aP_\infty + \underbrace{[0 : c : 1] + [0 : -c : 1]}_{\text{vanishes of order 1 at these points}}$$

To find a we can either take a local coordinate, or use the fact that $\deg(\operatorname{div}(x)) = 0$ so $a = -2$. Similarly

$$\operatorname{div}(y) = -3P_\infty + \sum_{i=1}^{3} [\lambda_i : 0 : 1]$$

as $\frac{\partial f}{\partial x} \neq 0$ at $[\lambda_i : 0 : 1]$ so y is a local parameter there. Thus $x \in L(2P_\infty), y \in L(3P_\infty)$. This is similar to computation of Weierstrass $\wp$-function.

Claim that $L(P_\infty) = k$. Granting the claim, lemma 5 implies that $\dim L(nP_\infty) \leq n$, but

$$\begin{aligned} 1, x &\in L(2P_\infty) \\ 1, x, y &\in L(3P_\infty) \\ 1, x, y, x^2 &\in L(4P_\infty) \\ 1, x, y, x^2, xy &\in L(5P_\infty) \end{aligned}$$

Note that all these are linearly independent. But

$$1, x, y, x^2, xy, x^3, y^2 \in L(6P_\infty),$$

which are *not* linearly indepedent as

$$y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3).$$

Exercise. $\{x^i, x^i y : i \geq 0\}$ are linearly independent in $k(X)$ and hence $\dim L(nP_\infty) = n$ for all $n \geq 1$.

Compare this with $X = \mathbb{P}^1$, $\dim L(n\infty) = n + 1$ when $n \geq 0$.

Note that λ_i's being distinct is essential as it ensures the curve is smooth. On the other hand, $\lambda_1\lambda_2\lambda_3 \neq 0$ is just a convenience (without which x vanishes at $[0 : c : 1]$ with order 2).

Proof of claim. If $L(P_\infty) \neq k$ then $L(P_\infty) = k + kt$ for some function $t \in k(E)$. Then $t^n \in L(nP_\infty) \setminus L((n-1)P_\infty)$ so $1, t, \dots, t^n$ are a basis of $L(nP_\infty)$. But $x \in L(2P_\infty), y \in L(3P_\infty)$ so exist $g_2(t), g_3(t)$ polynomials of degree 2 and 3 such that $x = g_2(t), y = g_3(t)$, so $x = (at + b)^2 + d$, $a \neq 0, b, d \in k$. By a change of variable (replacing t by $at + b$), the defining equation

$$y^2 = \prod (x - \lambda_i)$$

becomes

$$g_3(t)^2 = \prod (t^2 - (\lambda_i - d)).$$

But λ_i's distinct implies that $\lambda_i - d$ distinct so RHS is not a square in $k(t)$, contradiction. □

Suppose X is a smooth projective curve, $D \in \text{Div}(X)$ with $\ell(D) \geq 1$. Set $m = \ell(D) - 1$. Choose a basis $f_0, \dots, f_m$ of $L(D)$. We get a rational map

$$\begin{aligned} X &\dashrightarrow \mathbb{P}^m = \mathbb{P}(L(D)^*) \\ p &\mapsto [f_0(p) : \dots : f_m(p)] \end{aligned}$$

which, as X is smooth, extends to a morphism $\alpha_D : X \to \mathbb{P}^m$.

Moreover if $D \sim D'$, i.e. $D' = D + \text{div}(g)$ then $f_0 g, \dots, f_m g$ is a basis of $L(D')$ by part 3 of the lemma and

$$[(gf_0)(p) : \dots : (gf_n)(p)] = [f_0(p) : \dots : f_m(p)]$$

so we get the same map to projective space. Thus the map $\alpha_D : X \to \mathbb{P}^m$ depends only on $[D] \in \text{Cl}(X)$.

Example. $X = \mathbb{P}^1, D = n\infty, \ell(D) = n + 1$. Choose basis $1, t, \dots, t^n$ of $L(D)$. Have

$$\alpha_D(t) = [1 : t : \dots : t^n] : \mathbb{P}^1 \to \mathbb{P}^n$$

Write $t = \frac{x_1}{x_0}$,

$$\alpha_D[x_0 : x_1] = [1 : \frac{x_1}{x_0} : \dots : \left(\frac{x_1}{x_0}\right)^n] = [x_0^n : x_0^{n-1}x_1 : \dots : x_1^n]$$

> **Definition** (embedding). $\alpha : X \to Y$ is an *embedding* of X if it is a morphism which induces an isomorphism between $\alpha(X)$ and X.

Exercise.

1. Show $\alpha_{n\infty} : \mathbb{P}^1 \to \mathbb{P}^n$ is an embedding if $n \geq 1$.

2. Show that the map

$$\begin{aligned} \alpha : \mathbb{P}^1 &\to \mathbb{P}^2 \\ t &\mapsto [1 : t^2 : t^3] \end{aligned}$$

is *not* an embedding.

Exercise. Let

$$X = E = \text{Cl}\{(x, y) : y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)\} \subseteq \mathbb{P}^2.$$

Show

$$\begin{aligned} \alpha_{P_\infty} &: E \to \mathbb{P}^0 = \text{pt} \\ \alpha_{2P_\infty} &: E \to \mathbb{P}^1 = \mathbb{P}(\langle 1, x \rangle^*) \\ (x, y) &\mapsto x \\ \alpha_{3P_\infty} &: E \to \mathbb{P}^2 = \mathbb{P}(\langle 1, x, y \rangle^*) \\ (x, y) &\mapsto (x, y) \end{aligned}$$

Theorem 4.10 (embedding criterion)**.** *Let X be a smooth projective curve and $D \in \operatorname{Div}(X)$. Then $\alpha_D : X \to \mathbb{P}^m$ is an embedding if and only if for all $p, q \in X$,*

$$\ell(D - p - q) = \ell(D) - 2.$$

Intuition: if $p \neq q$ then this ensures this is an injection. If $p \neq q$ then this gives a criterion for singular point.

Proof. Omitted for now. Instead, we will define the degree of a curve in $\mathbb{P}^m$. □

When this happens, X is a curve in $\mathbb{P}^m$ of *degree* $\deg D$.

$X \subseteq \mathbb{P}^m = \mathbb{P}V$ where $\dim V = m + 1$, X a smooth curve. Let $H \subseteq \mathbb{P}^m$ be a hyperplane such that $X \not\subseteq H$ (otherwise take $m - 1$)). Define

$$[H \cap X] \in \operatorname{Cl}(X)$$

as $H \cap X$ "counted with multiplicity". (picture) There exists a linear function $x_0 \in V^*$ such that $H = \{p : x_0(p) = 0\}$. Write this as $x_0 = 0$. x_0 is not a well-defined function in $k(X)$. To get a rational function on X, pick $x_1 \in V^*$ such that $x_1(p) \neq 0$. Now $\frac{x_0}{x_1} \in k(X)$ and $\nu_p(\frac{x_0}{x_1})$ is defined and we set it to be n_p. If x_1' is another line with $x_1'(p) \neq 0$ then

$$\nu_p(\frac{x_0}{x_1'}) = \nu_p(\frac{x_0}{x_1}) + \underbrace{\nu_p(\frac{x_1}{x_1'})}_{=0}$$

so n_p is independent of the choice of x_1. We thus define

$$[H \cap X] = \sum_{p \in H \cap X} n_p p \in \operatorname{Div}(X).$$

Notice that $n_p \geq 0$ for all p, i.e. $[H \cap X] \geq 0$. Moreover, if we picked another hyperplane $H' = \{x_0' = 0\}$ with $X \not\subseteq H'$ then

$$\nu_p(\frac{x_0}{x_1}) = \nu_p(\frac{x_0'}{x_0}) + \nu_p(\frac{x_0}{x_0'})$$

hence

$$[H \cap X] = [H' \cap X] + \operatorname{div}(\frac{x_0}{x_0'}),$$

so image in the class group is independent of the choice of H. Thus we define

Definition.

$$\deg X = \deg[H \cap X]$$

for any hyperplane H not containing X.

Theorem 4.11. *Let $F(X_0, X_1, X_2)$ be a homogeneous polynomial of degree d and suppose $Z(F) \subseteq \mathbb{P}^2$ is smooth irreducible. Then*

$$\deg Z(F) = d.$$

Proof. Linearly change coordinates if necessary so $[0 : 1 : 0] \notin Z(F)$. Then

$$F = \sum_{i+j+k=d} a_{ijk} X_0^i X_1^j X_2^k$$

and $F[0 : 1 : 0] \neq 0$ implies that $a_{0,d,0} \neq 0$. Thus set $x = \frac{X_0}{X_1}, z = \frac{X_2}{X_1}$ and

$$f(x,z) = \frac{1}{a_{0,d,0}} F(x,1,z) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

where $a_i = a_i(z)$ is a polynomial in z of degree $\leq d - i$. $f(x,z)$ is a polynomial of degree d in variable x. In picture $z = 0$ is the hyperplane H (yellow line) and we are computing $H \cap X$ using chart $X_1 \neq 0$ (complement of green line).

We will now compute $\nu_p(z)$ for all $p \in \mathcal{X}_0$ where $\mathcal{X}_0 = Z(F) \cap \{X_1 \neq 0\} = \{(x,z) : f(x,z) = 0\}$. Note the last expression is affine. But

$$k[\mathcal{X}_0]/(z) = k[x,z]/(z, f(x,z)) = k[x]/(f(x,0)).$$

Now write

$$f(x,0) = (x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r}$$

with α_i's distinct and $\sum n_i = d$ and notice that points $(\alpha_i, 0)$ are exactly the intersections $\mathcal{X}_0 \cap \{z = 0\}$. But Chinese remainder theorem says

$$k[x]/(x-\alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r} \cong \bigoplus k[x]/(x-\alpha_i)^{n_i}.$$

Let $\mathcal{X} = Z(F)$. Claim

$$\nu_p(z) = \dim \mathcal{O}_{\mathcal{X},p}/(z) = \dim \mathcal{O}_{\mathcal{X}_0,p}/(z)$$

by definition: as if t is a local parameter at p, $z = t^n \cdot u$ where $n = \nu_p(z)$, and we've seen

$$\mathcal{O}_{\mathcal{X}_0,p}/(z) = k[t]/(t^n)$$

which has dimension n. So

$$k[\mathcal{X}_0]/(z) \cong \bigoplus_{p \in \mathcal{X} \cap H} \mathcal{O}_{\mathcal{X},p}/(z) \cong \bigoplus_{i=1}^{r} \mathcal{O}_{\mathcal{X}_0,(\alpha_i,0)}/(z).$$

Have

$$\dim k[\mathcal{X}_0]/(z) = \sum n_i = \sum \nu_{p_i}(z) = d.$$

□

Remark (quadrics). $x^2 + y^2 = 1$, $xy = 1$ and $y = x^2$ are three type of curves over $\mathbb{R}$, and two types over $\mathbb{C}$. But they all correspond to curves in $\mathbb{P}^2$: $XY = Z^2$ has two points $[1 : 0 : 0]$ and $[0 : 1 : 0]$ at infinity while for $YZ = X^2$, there is one point (with multiplicity 2) at infinity. There is only one family of quadric (degree 2 curve) in $\mathbb{P}^2$, isomorphic to $\mathbb{P}^1$.

Corollary 4.12 (Bezout's theorem)**.** *If $X = Z(F), W = Z(G)$ with $\deg F = d, \deg G = d'$ are two curves in $\mathbb{P}^2$ such that $X \not\subseteq W, W \not\subseteq X$ then they intersect in $\leq dd'$ points.*

Proof. Given a curve $\mathcal{X}$ in $\mathbb{P}^m$ and $G \in k[X_0, \dots, X_n]$ homogeneous of degree d' such that $X \nsubseteq W = Z(G)$. Define

$$[\mathcal{X} \cap W] = \sum_{p \in \mathcal{X} \cap W} m_p p$$

where $m_p = \nu_p(G/X_1^{d'})$ for any linear function X_1 such that $X_1(p) \neq 0$. As

$$\frac{G}{X_1^{d'}} = \left(\frac{X_0}{X_1}\right)^{d'} \cdot \left(\frac{G}{X_0^{d'}}\right)$$

but $\nu_p(X_0/X_1)$ is the order of vanishing of $\mathcal{X}$ along X_0 so

$$[\mathcal{X} \cap W] = d'[\mathcal{X} \cap H] + \operatorname{div} \frac{G}{X_0^{d'}}$$

hence

$$[\mathcal{X} \cap W] = d'[\mathcal{X} \cap H] \in \mathrm{Cl}(\mathcal{X})$$

with $\deg[\mathcal{X} \cap W] = d' \deg[\mathcal{X} \cap H]$. So if $m = 2$ and $W, \mathcal{X} \subseteq \mathbb{P}^2$, $\deg[\mathcal{X} \cap H] = d$, by the theorem. Hence $\#(\mathcal{X} \cap W) \leq dd'$. □

5 Differentials

Let B be a ring, $A \subseteq B$ a subring.

Definition (Kähler differential)**.** The *Kähler differential*, 1*-form* or *relative cotangent bundle* $\Omega^1_{B/A}$ is the free B-module generated by B, which we denote by $\mathrm{d}b$ for $b \in B$, quotiented by the submodule generated by

$$\begin{aligned}&\mathrm{d}(fg) - f\mathrm{d}g - g\mathrm{d}f\\&\mathrm{d}(b+b') - \mathrm{d}b - \mathrm{d}b'\\&\mathrm{d}a\end{aligned}$$

where $b, b', f, g \in B, a \in A$.

Exercise.

1. Let X be an affine algebraic variety over k, $x \in X$ and $\mathrm{ev}_x : k[X] \to k$ the corresponding k-algebra homomorphism. Show that
$$\mathrm{Hom}_{k[X]}(\Omega^1_{k[X]/k}, k) \cong \mathrm{Der}(k[X], \mathrm{ev}_x)$$
where on LHS k is regarded as a $k[X]$-module via ev_x.
2. More generally, for any B-module M,
$$\mathrm{Hom}_B(\Omega^1_{B/A}, M) \cong \{A\text{-linear derivations } B \to M\}.$$
Hence $\Omega^1_{k[X]/k}$ is dual to the tangent bundle, hence called the *cotangent bundle.*

Definition (rational differential)**.** The *rational differentials* on X is defined to be $\Omega^1_{k(X)/k}$.

If you prefer the language of complex geometry, this is the space of meromorphic differential forms.

Usual rules of calculus apply so for example

$$0 = \mathrm{d}(1) = \mathrm{d}(\frac{g}{g}) = \frac{1}{g}\mathrm{d}g + g\mathrm{d}\frac{1}{g}$$

by Leibniz so

$$\mathrm{d}\frac{1}{g} = -\frac{1}{g^2}\mathrm{d}g.$$

Similarly

$$\mathrm{d}(fg) = \frac{g\mathrm{d}f - f\mathrm{d}g}{g^2}.$$

Corollary 5.1.

1. $\Omega^1_{k(x)/k} = \Omega^1_{k(\mathbb{P}^1)/k} = k(x)\mathrm{d}x$ *where x is transcendental over k.*

2. *If $L \supseteq k$ is a separable algebraic extension then $\Omega^1_{L/k} = 0$.*

Proof. If $\alpha \in L$ then by definition there exists a monic $f(z) \in k[z]$ such that $f(\alpha) = 0$ and $f'(\alpha) \neq 0$. Differentiate the relation $f(\alpha) = 0$ to get $(\mathrm{d}f)(\alpha) = 0$. But $\mathrm{d}f(\alpha) = f'(\alpha)\mathrm{d}\alpha$ and $f'(\alpha) \neq 0$ so $\mathrm{d}\alpha = 0$. □

Combining these, get

Lemma 5.2. *If X is a curve, $p \in X$ smooth and t a local parameter at p then*

$$\Omega^1_{k(X)/k} = k(X)\mathrm{d}t.$$

Proof. If t is a local parameter then the extension $k(X)/k(t)$ is algebraic and separable (the first one is obvious by transcendence degree and the second requires proof, but we omit it). Thus if $\alpha \in k(X)$ there exists $f \in k(t)[z]$ such that $f(\alpha) = 0$, $\frac{\partial f}{\partial z}(\alpha) \neq 0$. Write $f(z) = \sum f_i(t)z^i$ where $f_i(t) \in k(t)$. Differentiate,

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

by linearity and Leibniz rule. We get

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

□

Definition (regular)**.** If $\omega \in \Omega^1_{k(X)/k}$, $p \in X$ smooth and t a local parameter at p so $\omega = f\mathrm{d}t$ for some $f \in k(X)$. Define the order of vanishing of ω at p to be

$$\nu_p(\omega) = \nu_p(f)$$

and the divisor of ω to be

$$\mathrm{div}(\omega) = \sum_p \nu_p(\omega)p.$$

Say ω is *regular* at p if $\nu_p(\omega) \geq 0$.

Need to show that $\nu_p(\omega)$ is independent of choice of local parameter t.

Lemma 5.3.

1. *If $f \in \mathcal{O}_{X,p}$ then $\nu_p(\mathrm{d}f) \geq 0$.*
2. *If t_1 is any local coordinate at p then $\nu_p(\mathrm{d}t_1) = 0$. In particular, $\nu_p(\omega)$ is well-defined and*

$$\nu_p(f\mathrm{d}t_1) = \nu_p(f) + \nu_p(\mathrm{d}t_1).$$

3. *If $f \in k(X)$ has $\nu_p(f) = n < 0$ then $\nu_p(\mathrm{d}f) = \nu_p(f) - 1$ if $\mathrm{ch}\, k \nmid n$.*

Proof.

1. Choose an affine open neighbourhood X_0 of X so $p \in X_0 \subseteq \mathbb{A}^N$. Then $f \in \mathcal{O}_{X,p}$ means that $f = \frac{g}{h}$ where $g, h \in k[x_1, \dots, x_N]$, $h(p) \neq 0$. So

$$\mathrm{d}f = \frac{h\mathrm{d}g - g\mathrm{d}h}{h^2} = \sum_{i=1}^{N} \gamma_i \mathrm{d}x_i$$

for some $\gamma_i \in \mathcal{O}_{X,p}$, that is $\nu_p(\gamma_i) \geq 0$. Hence

$$\nu_p(\mathrm{d}f) \geq \min\{\nu_p(\mathrm{d}x_i) : i = 1, \dots, N\}.$$

Hence $\{\nu_p(\mathrm{d}f) : f \in \mathcal{O}_{X,p}\}$ is bounded below. Choose $f \in \mathcal{O}_{X,p}$ with $\nu_p(\mathrm{d}f)$ minimal. Write $f - f(p) = tf_1$, $f_1 \in \mathcal{O}_{X,p}$. Hence

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

If $\nu_p(f) < 0$ then as $\nu_p(f_1 \mathrm{d}t) = \nu_p(f_1) \geq 0$ by definition, then $(*)$ implies that

$$\nu_p(\mathrm{d}f_1) = \nu_p(\mathrm{d}f) - 1,$$

contradicting minimality of $\nu_p(\mathrm{d}f)$.

2. $t_1 = ut$ for some $u \in \mathcal{O}^*_{X,p}$ and hence

$$\mathrm{d}t_1 = u\mathrm{d}t + t\mathrm{d}u.$$

By 1, $\mathrm{d}u = g\mathrm{d}t$ with $\nu_p(g) \geq 0$. So $\mathrm{d}t_1 = (u + tg)\mathrm{d}t$ and $\nu_p(u + tg) = \nu_p(u) = 0$.

3. $f = t^n u$ then $\mathrm{d}f = nt^{n-1}u\mathrm{d}t + t^n \mathrm{d}u$ and 2 implies the result.

□

Proposition 5.4. *Let $\omega \in \Omega^1_{k(X)/k}$. Then $\nu_p(\omega) = 0$ for all but finitely many $p \in X$.*

Proof. Choose $t \in k(X)$ such that $k(X)/k(t)$ is separable algebraic (for example t is a local parameter at some point p, or t is obtained from Noether normalisation). Then t defines a rational map $\alpha = [1 : t] : X \dashrightarrow \mathbb{P}^1$, hence extends to a map $\alpha : X \to \mathbb{P}^1$ as X is smooth projective. Finiteness theorem says that only finitely many points p with $\alpha(p) = \infty$, or with $e_\alpha(p) > 1$. For any other $p \in X$, $t - t(p)$ is a local coordinate at p, and so $\nu_p(\mathrm{d}t) = 0$ for all but finitely many p. Thus the proposition holds if $\omega = \mathrm{d}t$.

For any arbitrary $\omega \in \Omega^1_{k(X)/k}$, $\omega = f\mathrm{d}t$ and

$$\nu_p(f\mathrm{d}t) = \nu_p(f) + \nu_p(\mathrm{d}t)$$

and $\nu_p(f) = 0$ for all but finitely many p, proving the result. □

Definition. The divisor of a Kähler form is defined to be

$$\operatorname{div}\omega = \sum_{p\in X} \nu_p(\omega)p \in \operatorname{Div}(X).$$

We have just shown that this is a finite sum and indeed well-defined.

As $\operatorname{div}(f\omega) = \operatorname{div} f + \operatorname{div}\omega$, the class of $\operatorname{div}(\omega)$ in $\operatorname{Cl}(X)$ is *independent* of ω. This is called the *canonical class* $\mathcal{K}_X = [\operatorname{div}\omega]$ for any $0 \neq \omega \in \Omega^1_{k(X)/k}$.

Pick $0 \neq \omega_0 \in \Omega^1_{k(X)/k}$. Recall that

$$\begin{aligned} L(\mathcal{K}_X) &= L(\operatorname{div}(\omega_0)) \\ &= \{f \in k(X) : \operatorname{div}(\omega_0) + \operatorname{div}(f) \geq 0\} \\ &= \{f \in k(x) : \operatorname{div}(f\omega_0) \geq 0\} \\ &= \{\omega \in \Omega^1_{k(X)/k} : \operatorname{div}\omega \geq 0\} \end{aligned}$$

Definition (genus)**.** We define the *genus* of X to be

$$\ell(\mathcal{K}_X) = \dim L(\mathcal{K}_X).$$

Example.

1. Let $X = \mathbb{P}^1$. Let x be a coordinate on $\mathbb{P}^1$ and choose $\omega = \mathrm{d}x$. Must compute $\nu_p(\mathrm{d}x)$ for $p \in \mathbb{P}^1$. If $p \in \mathbb{A}^1$ then $x - p$ is a local coordinate and $\mathrm{d}(x-p) = \mathrm{d}x$ has $\nu_p(\mathrm{d}x) = 0$.

   If $p = \infty$ then $t = \frac{1}{x}$ is a local coordinate and

   $$\mathrm{d}x = \mathrm{d}\left(\frac{1}{t}\right) = -\frac{1}{t^2}\mathrm{d}t$$

   so $\nu_\infty(\mathrm{d}x) = -2$ so $\operatorname{div}(\mathrm{d}x) = -2\infty = \mathcal{K}_X$. Thus $\deg \mathcal{K}_X = -2$. Then by a lemma $\ell(\mathcal{K}_X) = 0$ so $\mathbb{P}^1$ has genus 0.

2. $y^2 = f(x) = (x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$ where λ_i's distinct. This gives $X = E \subseteq \mathbb{P}^2$ with a unique point at ∞, $P_\infty = [0:1:0]$. Take derivative, $2y\mathrm{d}y = f'(x)\mathrm{d}x$. Let's consider the 1-form

   $$\omega = \frac{\mathrm{d}x}{y} = \frac{2\mathrm{d}y}{f'(x)} \in \Omega^1_{k(E)/k}.$$

   Need to compute $\operatorname{div}\omega$. Given $p = (x_0, y_0) \in \mathbb{A}^2$, if $f'(x_0) \neq 0$ then $y - y_0$ is a local coordinate so

   $$\omega = \frac{2}{f'(x_0)}\mathrm{d}y = \frac{2}{f'(x_0)}\mathrm{d}(y-y_0)$$

   and thus $\nu_p(\omega) = 0$.

   If $y_0 = \frac{1}{2}\frac{\partial}{\partial y}(y^2 - f(x))|_p \neq 0$ then $x - x_0$ is a local parameter so

   $$\omega = \frac{1}{y}\mathrm{d}(x-x_0)$$

has $\nu_p(\omega) = 0$. Since λ_i's are distinct and the curve is smooth at p, at least one of these happens.

At $p = P_\infty$, have

$$Y^2Z = (X - \lambda_1 Z)(X - \lambda_2 Z)(X - \lambda_3 Z).$$

Consider the chart $Y \neq 0$. Write

$$\begin{aligned} u &= \frac{x}{y} = \frac{X}{Y} \\ v &= \frac{1}{y} = \frac{Z}{Y} \end{aligned}$$

In this chart, E becomes $\{(u, v) : g(u, v) = 0\}$ where

$$g(u, v) = v - (u - \lambda_1 v)(u - \lambda_2 v)(u - \lambda_3 v).$$

In this chart P_∞ corresponds to $(u, v) = (0, 0)$. As

$$\frac{\partial g}{\partial v}\Big|_{(0,0)} = 1 \neq 0$$

u is a local parameter at $(0, 0)$. Thus $\nu_{P_\infty}(u) = 1$ and $\nu_{P_\infty}(v) \geq 1$. Here is an ad hoc way of computing it:

$$\nu_{P_\infty}(u - \lambda_i v) \geq 1$$

so $\nu_{P_\infty}(v) \geq 3$. Thus $\nu_{P_\infty}(u - \lambda_i v) = 1$ and $\nu_{P_\infty}(v) = 3$. But then $y = \frac{1}{v}$ so $\nu_{P_\infty}(y) = -3$. So

$$\nu_{P_\infty}(x) = \nu_{P_\infty}(ux) = 1 - 3 = -2.$$

So

$$\nu_{P_\infty}(\mathrm{d}x) = -2 - 1 = -3$$

if $\operatorname{ch} k \neq 2$ by lemma 3. Thus

$$\nu_{P_\infty}\left(\frac{\mathrm{d}x}{y}\right) = -3 - (-3) = 0$$

so $\operatorname{div} \omega = 0$, i.e. $\mathcal{K}_X = 0$. Thus $g = \ell(0) = 1$. E has genus 1.

Definition (elliptic curve)**.** A curve of genus 1 is called an *elliptic curve.*

We showed $y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$ has genus 1.

Proposition 5.5. *Let $\mathcal{X} = Z(F) \subseteq \mathbb{P}^2$ be an irreducible smooth projective curve, $F = F(X, Y, Z)$ homogeneous of degree d. Then*

$$\mathcal{K}_X = (d - 3)[\mathcal{X} \cap H]$$

where $\mathcal{X} \cap H$ is the divisor of the intersection of any line H (i.e. hyperplane) with $\mathcal{X}$. In particular

$$\deg \mathcal{K}_X = d(d - 3).$$

Proof. Let $x = \frac{X}{Z}, y = \frac{Y}{Z}$ and $f(x,y) = F(x,y,1)$ be the equation of $\mathcal{X}$ on $\mathbb{A}^2$ which is the chart $Z \neq 0$ in $\mathbb{P}^2$. Differentiate,

$$\mathrm{d}f = \frac{\partial f}{\partial x}\mathrm{d}x + \frac{\partial f}{\partial y}\mathrm{d}y = 0 \in \Omega^1_{k(X)/k}$$

as $f = 0 \in k(X)$. Take

$$\omega = \frac{\mathrm{d}x}{\partial f/\partial y} = -\frac{\mathrm{d}y}{\partial f/\partial x}$$

and need to compute $\nu_p(\omega)$ for all $p \in \mathcal{X}$.

Let $p = (x_0, y_0) \in \mathbb{A}^2 \cap \mathcal{X}$. If $\frac{\partial f}{\partial y}(p) \neq 0$ then $x - x_0$ is a local coordinate at p so $\omega = \frac{\mathrm{d}(x-x_0)}{\partial f/\partial y}$ has $\nu_p(\omega) = 0$. If $\frac{\partial f}{\partial x}(p) \neq 0$ then $y - y_0$ is a local coordinate so $\nu_p(\omega) = 0$. As $\mathcal{X}$ is smooth by hypothesis, at least one of this is nonzero, so $\nu_p(\omega) = 0$ for all $p \in \mathbb{A}^2 \cap \mathcal{X}$, i.e. with the choice of ω, all contributions occur at the line at ∞, which is $z = 0$.

If necessary, change coordinates on the $z = 0$ line so $[1 : 0 : 0] \notin \mathcal{X}$. Then $\mathcal{X} \cap \{z = 0\}$ is contained in the chart $Y \neq 0$. (the only case in which we can't do this operation is $\{z = 0\} \subseteq \mathcal{X}$, but in this case X is just $\mathbb{P}^1$). Let

$$u = \frac{Z}{Y} = \frac{1}{y}$$
$$v = \frac{X}{Y} = \frac{x}{y}$$

so u, v are coordinates on $Y \neq 0$ chart. Now the equation of $\mathcal{X}$ is given by

$$g(u,v) = F(v,1,u) = F(\frac{x}{y}, 1, \frac{1}{y}) = y^{-d}F(x,y,1) = y^{-d}f(x,y),$$

that is

$$f(x,y) = y^d g(u,v).$$

Now differentiate and use chain rule,

$$\frac{\partial f}{\partial x} = y^d\left(\frac{\partial g}{\partial v}\frac{\partial v}{\partial x} + \frac{\partial g}{\partial u}\underbrace{\frac{\partial u}{\partial x}}_{=0}\right) = y^{d-1}\frac{\partial g}{\partial v}$$

Also $\mathrm{d}y = -\frac{1}{u^2}\mathrm{d}u$ so

$$\omega = -\frac{\mathrm{d}y}{\partial f/\partial x} = u^{d-3}\frac{\mathrm{d}u}{\partial g/\partial v} = u^{d-3}\eta$$

where

$$\eta = \frac{\mathrm{d}u}{\partial g/\partial v} = -\frac{\mathrm{d}v}{\partial g/\partial u}$$

For exactly the same reason as before, $\nu_p(\eta) = 0$ for all $p \in \mathbb{A}^2_{(u,v)} \cap \mathcal{X}$. Thus

$$\nu_p(\omega) = (d-3)\nu_p(u) + \nu_p(\eta) = (d-3)\nu_p(u).$$

Finally observe that

$$\nu_p(u) = \nu_p(\frac{Z}{Y})$$

is just the contact order of the line $Z = 0$ with $\mathcal{X}$, i.e. $[\mathcal{X} \cap \{Z = 0\}] = \sum_{p \in \mathcal{X} \subseteq \{Z=0\}} \nu_p(\omega)p$, by definition. □

6 Riemann-Roch theorem

Theorem 6.1 (classical Riemann-Roch)**.** *Let X be a smooth projective curve with genus $g = g(X) = \ell(\mathcal{K}_X)$. Let $D = \sum n_i P_i \in \operatorname{Div}(X)$. Then*

$$\ell(D) - \ell(\mathcal{K}_X - D) = 1 - g + \deg D.$$

We will not prove this theorem but will spend the rest of the course understanding the statement and its consequences. Immediate consequences are:

1. take $D = 0$. As $\ell(0) = 1$, this says that $\ell(\mathcal{K}_X) = g$, which is the definition of genus.
2. take $D = \mathcal{K}_X$, we get $\deg \mathcal{K}_X = 2g - 2$.
3. If $\deg D > 2g - 2$ then $\deg(\mathcal{K}_X - D) < 0$ so $\ell(\mathcal{K}_X - D) = 0$ so by Riemann-Roch,
$$\ell(D) = 1 - g + \deg D.$$
Warning: if $0 < \deg D \leq 2g - 2$, the behaviour of $\ell(D)$ is complicated as you vary D in $\operatorname{Cl}^a(X)$, $a = \deg D$ fixed, ℓ can jump. In fact $\operatorname{Cl}^a(X)$ is an algebraic variety and it stratifies into subvarieties according to $\ell(D)$. This is *Brill-Noether loci*.
4. If $\deg D > 2g$ then for all $p, q \in X$,
$$\ell(D - p - q) = \ell(D) - 2 = 1 - g - 2 + \deg D.$$
Hence by embedding criterion
$$\alpha_D : X \to \mathbb{P}(L(D)^*) \cong \mathbb{P}^n$$
is an embedding, with image a curve of degree $\deg D$.

Corollary 6.2. *If $\mathcal{X}$ is a smooth plane curve of degree d, then as $\deg \mathcal{K}_X = d(d-3)$, have*

$$g = \frac{1}{2}(d-1)(d-2).$$

For example if $d = 1$ or 2, correponding to line and conics respectively, we have $g = 0$. If $d = 3$ then $g = 1$. In general we have a progression

$$0, 0, 1, 3, 6, 10, \cdots$$

which does not have every natural number in there. Thus smooth projective curves of genus $2, 4, 5, 7, \cdots$ cannot occur inside $\mathbb{P}^2$.

Let's study curves of small genus using Riemann-Roch.

Proposition 6.3. *X has genus 0 if and only if $X = \mathbb{P}^1$.*

Proof.

- $\Longleftarrow$: done earlier.

- $\implies$: suppose X has genus 0. Let $p \in X$. The divisor (p) has degree 1. As $1 > -2 = 2g-2$, by Riemann-Roch $\ell((p)) = 2$. But $k = L(0) \subseteq L((p))$ so exists $f \in L((p)) \setminus k$. Have $\operatorname{div}(f) + (p) \geq 0$, i.e. f has a pole at p and no other pole. But $\operatorname{div}(f)$ has degree 0, so $\deg(\operatorname{div}(f) + (p)) = 1$, which is saying $\operatorname{div}(f) = -(p) + (q)$ for some $q \in X$. In addition $p \neq q$ as f is not constant. As $p \neq q$, f is not constant so $\alpha = [1 : f] : X \dashrightarrow \mathbb{P}^1$ is a nonconstant rational map, hence a morphism (as X is smooth) of degree 1. Thus by an exercise on example sheet 3 α is an isomorphism.

□

Note that there are two parts of the proof: we showed that if $\ell((p)) = 2$ for some $p \in X$ then $X \cong \mathbb{P}^1$, and we used Riemann-Roch to show such p exists.

6.1 Curves of genus 1

Let X be a smooth projective curve with genus $g = 1$. Then by Riemann-Roch, if $\deg D > 0$ then $\ell(D) = \deg D$.

Fix a point $p_\infty \in X$. Have

$$\underbrace{L(0)}_{k} \subseteq \underbrace{L(p_\infty)}_{k} \subsetneq \underbrace{L(2p_\infty)}_{k\langle 1,x\rangle} \subsetneq \underbrace{L(3p_\infty)}_{k\langle 1,x,y\rangle} \subsetneq \cdots$$

where we choose $x \in L(2p_\infty) \setminus k, y \in L(3p_\infty) \setminus L(2p_\infty)$. As before, $L(6p_\infty)$ contains $1, x, y, x^2, xy, x^3, y^2$. But $\dim L(6p_\infty) = 6$ so there exist a linear relation between these monomials, with x^3, y^2 appearing with non-zero coefficients (as $1, x, y, x^2, xy \in L(5p_\infty)$ are linearly independent, and we cannot have only one of x^3, y^2 with nonzero coefficient by considering the degree of pole at ∞). Rescale $x \mapsto \lambda x, y \mapsto \mu y$, we get a relation in $k(X)$

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

for some $a_i \in k$. This equation defines a curve C_0 in $\mathbb{A}^2$ (exericse: this is irreducible) with a unique point at ∞, call it p_∞, so $C = C^0 \cup \{p_\infty\} \subseteq \mathbb{P}^2$, and

$$\alpha_{3p_\infty} = [1 : x : y] : X \to \mathbb{P}^2$$

maps X into C. As α_{3p_∞} is not constant and C is irreducible, this map is surjective. The embedding criterion tells us α_{3p_∞} is an isomorphism $X \cong C$.

We can do better: if $\operatorname{ch} k \neq 3$, we can complete the cube by $x \mapsto x - \frac{a_2}{3}$ so the equation becomes (by renaming the coefficients)

$$y^2 + a_1 xy + a_3 y = x^3 + a_4 x + a_6.$$

If $\operatorname{ch} k \neq 2$, we can complete the square by $y \mapsto y - \frac{a_1 x + a_3}{2}$ to get

$$y^2 = x^3 + q_2 x^2 + a_4 x + a_6.$$

Combining these two, if $\operatorname{ch} k \neq 2, 3$, do them in this order to get

$$y^2 = x^3 + a_4 x + a_6 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$$

for λ_i's distinct (by smoothness).

Theorem 6.4. *Every curve of genus* 1 *is isomorphic to a smooth plane curve of the form*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Amazingly, every curve of genus 1 is a group by the following:

Proposition 6.5. *Let E be a curve of genus* 1*, $p_\infty \in E$. Then the map*

$$\begin{aligned} E &\to \mathrm{Cl}^0(E) \\ p &\mapsto [p - p_\infty] \end{aligned}$$

is a bijection.

Proof. For injectivity, if $p - p_\infty = q - p_\infty$ in $\mathrm{Cl}(E)$ the $p - q = \mathrm{div}(f)$ for some $f \in k(E)$. But then $[1 : f] : E \to \mathbb{P}^1$ is an isomorphism, contradicting E having genus 1.

For surjectivity, if $D \in \mathrm{Div}(E)$ and $\deg D = 0$, then

$$\deg(D + p_\infty) = 1 > 2g - 2 = 0$$

so by Riemann-Roch $\ell(D + p_\infty) = 1$. Let $0 \neq f \in L(D + p_\infty)$ so

$$D + p_\infty + \mathrm{div}(f) \geq 0.$$

But the degree of this is 1, implying that $D + p_\infty + \mathrm{div}(f) = q$, i.e. $D = q - p_\infty$ in $\mathrm{Cl}(E)$. □

Corollary 6.6. *E is an algebraic group, where the group operation $\boxplus$ is define by*

$$p \boxplus q = r \iff (p - p_\infty) + (q - p_\infty) = (r - p_\infty)$$

in $\mathrm{Cl}(E)$, i.e. if $p + q = r + p_\infty$ in $\mathrm{Cl}(E)$.

Notice that the identity of the group is p_∞.

Definition (elliptic curve)**.** An *elliptic curve* is a pair (E, p_∞) where E is a curve of genus 1 and $p_\infty \in E$.

In fact, the group law is algebraic: consider $\alpha_{3p_\infty} : E \to \mathbb{P}^2$ and let X, Y, Z be coordinates on $\mathbb{P}^2$. As we know $E \cap \{Z = 0\} = 3p_\infty$ and if $L = \{\ell = 0\}$ is any line in $\mathbb{P}^2$, $[L \cap E] = p_1 + p_2 + p_3$ and $\mathrm{div}(\ell/z) = p_1 + p_2 + p_3 - 3p_\infty$. Note $\ell/z \in k(E)$. Thus $p_1 + p_2 + p_3 = 3p_\infty$ in $\mathrm{Cl}(E)$, i.e.

$$p_1 \boxplus p_2 \boxplus p_3 = p_\infty \boxplus p_\infty \boxplus p_\infty = p_\infty.$$

Thus geometrically the group law can be characterised as follow: any line L intersects E at three points, and the sum of the three points in the group is p_∞.

Exercise.

1. Show that for fixed $p \in E$, the map
$$\begin{aligned} E &\dashrightarrow E \\ e &\mapsto e \boxplus p \end{aligned}$$
is a rational map, hence a morphism, hence an isomorphism.

2. Show the map $y \mapsto \boxminus y$ is a morphism (i.e. it is a rational function).

3. Show that $\boxplus : E \times E \to E$ defines a morphism so E is a group object in the category of smooth projective varieties.

Suppose $E = \{y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)\} \cup \{p_\infty\}$ and $\operatorname{ch} k \neq 2, 3$. Consider the line $\{x = a\}$ in $\mathbb{P}^2$. It intersects E at p_∞ and at $(a, \pm b)$ for some $b \in k$. Hence
$$(a, b) \boxplus (a, -b) \boxplus p_\infty = p_\infty$$
i.e.
$$(a, b) \boxplus (a, -b) = p_\infty,$$
that is $\boxminus(a, b) = (a, -b)$, so this proves a special case of 2. This implies that $[2]p = 0$, that is $p \boxplus p = p_\infty$ if and only if $b = 0$ or $p = p_\infty$, i.e. $p = (\lambda_i, 0)$ or $p = p_\infty$. These are exactly the ramification points of the morphism $\alpha_{2p_\infty} = [x : 1] : E \to \mathbb{P}^1$. That is, E is a double cover of $\mathbb{P}^1$, ramified at 4 points, and these four points are just the points of order 2 on E, i.e. $\mathbb{P}^1 = E/(\mathbb{Z}/(2))$ where $\mathbb{Z}/(2)$ acts on E by $p \mapsto \boxminus p$. These 4 points are well-defined, independent of choices, up to a coordinate change on $\mathbb{P}^1$, i.e. up to action of PGL_2 on $\mathbb{P}^1$.

Let $j(E)$ be the cross ratio of these 4 points $\infty, \lambda_1, \lambda_2, \lambda_3$. It is an invariant of $(\mathbb{P}^1)^2/\mathrm{PGL}_2$. For example if we scale (change of coordinates?) so that $y^2 = x(x - 1)(x - \lambda)$, then
$$j(E) = j(\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2 (l - 1)^2}.$$

Thus $j(E) = j(E')$ if and only if $E \cong E'$: only if because given $\lambda_1, \lambda_2, \lambda_3, \infty$, we can define E, if by the discussion above.

Corollary 6.7. *There is a three way correspondence*
$$\begin{aligned} &\{\textit{genus 1 curves up to isomorphism}\} \\ \leftrightarrow &\{4 \textit{ distinct points in } \mathbb{P}^1\}/\mathrm{PGL}_2 \\ \leftrightarrow &\mathbb{A}^1 \quad \textit{given by } j \end{aligned}$$

6.2 Riemann-Hurwitz

Theorem 6.8 (Riemann-Hurwitz)**.** *Let $\alpha : X \to Y$ be a nonconstant morphism of smooth projective curves such that $k(X)/k(Y)$ is a separable algebraic extension (for example if $\operatorname{ch} k = 0$). Set $\chi(X) = 2 - 2g(X)$. Then*
$$\chi(X) = \chi(Y) \deg \alpha - \sum_{p \in X} (e_p(\alpha) - 1).$$

Proof. α defines a map

$$\begin{aligned}\alpha^* : \Omega^1_{k(Y)/k} &\to \Omega^1_{k(X)/k} \\ f\mathrm{d}g &\mapsto (f\alpha)\mathrm{d}(g\alpha)\end{aligned}$$

Separability implies that α^* is injective (as α is nonconstant). Pick $0 \neq \omega \in \Omega^1_{k(Y)/k}$, then by Riemann-Roch

$$\deg \omega = 2g(Y) - 2 = -\chi(Y).$$

Let $p \in X, q = \alpha(p) \in Y$ and pick local coordinates t_p, t_q at p, q respectively, so $t_q \circ \alpha = ut_p^{e_p(\alpha)}$ where u is a unit. Write $\omega = f\mathrm{d}t_q$ for some $f \in k(Y)$, so $\alpha^*\omega = f\alpha\mathrm{d}(ut^{e_p})$. Hence

$$\begin{aligned}\nu_p(\alpha^*\omega) &= \nu_p(f\alpha) + \nu_p(\mathrm{d}(ut^{e_p})) \\ &= \nu_q(f)e_p + \nu_p(ut^{e_p}) - 1 \quad \text{if } \operatorname{ch} k \nmid e_p \\ &= \nu_q(\omega)e_p + e_p - 1\end{aligned}$$

Therefore

$$\begin{aligned}-\chi(X) &= \deg \alpha^*\omega \\ &= \sum_{q \in Y}(\sum_{p \in \alpha^{-1}(q)} e_p)\nu_q(\omega) + \sum_{p \in X}(e_p - 1) \\ &= \deg \alpha \sum_{q \in Y} \nu_q(\omega) + \sum_{p \in X}(e_p - 1)\end{aligned}$$

□

Corollary 6.9. *Let $k = \mathbb{C}$. Then the topological Euler characteristic of a smooth projective curve X is $2 - 2g$, i.e. g is the "number of holes".*

Proof. The topological characteristic of $\mathbb{P}^1$ is $2 = 2 - 0$ so the statement holds for $X = \mathbb{P}^1$. In general, let $f \in k(X)$ nonconstant. Then f defines a morphism $\alpha : X \to \mathbb{P}^1$. Now Riemann-Hurwitz for f as a Riemann surface and as an algebraic curve coincide. □

Corollary 6.10. *If $g(X) < g(Y)$ then there are no non-constant maps $X \to Y$. In particular if $g(Y) > 0$ then there are no non-constant maps $\mathbb{P}^1 \to Y$.*

c.f. exercise proving the non-existence of non-constant map from $\mathbb{P}^1$ to an elliptic curve.

Proof. By Riemann-Hurwitz for any $\alpha : X \to Y$ non-constant,

$$0 \leq 2(g(X) - g(Y)) + (-2g(Y) + 2)(\deg \alpha - 1) < 0,$$

absurd. □

Definition (hyperelliptic)**.** If a curve X admits a degree 2 map $X \to \mathbb{P}^1$, we say X is *hyperelliptic.*

For example an elliptic curve is hyperelliptic.

Suppose X is hyperelliptic, $\pi : X \to \mathbb{P}^1$ is a degree 2 map and $\operatorname{ch} k \neq 2$. If $p \in X$, either $e_p = 1$ and p is unramified, or $e_p = 2$ and p is ramified (constrast this with the case $\alpha : X \to \mathbb{P}^1$ with degree ≥ 3, where there are more than one type of ramification). Then Riemann-Hurwitz says that

$$2 - 2g = 2 \times 2 - \#\{\text{ramification points}\}$$

so there are $2 + 2g$ ramification points, which in particular is always even. For example if $g = 1$ then there are 4, if $g = 2$ then there are 6.

6.3 Curves of genus 2

If a curve X has $g(X) > 0$ then we can then consider the map $\alpha_{\mathcal{K}} : X \to \mathbb{P}^{g-1}$, the *canonical morphism*. This is not very interesting for $g(X) = 1$. Suppose X has genus 2.

Proposition 6.11. *$\alpha_{\mathcal{K}}$ is a map of degree 2, so X is a hyperelliptic curve and $\alpha_{\mathcal{K}}$ is ramified at 6 points.*

Proof. Only thing needs proving is that $\alpha_{\mathcal{K}}$ has degree 2. As $\ell(\mathcal{K}_X) = g(X) = 2 > 0$, $\mathcal{K}_X = p + q$ in $\operatorname{Cl}(X)$ and

$$\ell(p + q) = \ell(\mathcal{K}_X) = 2 > 1$$

so there exists a non-constant function $h \in L(p+q)$, i.e. $\operatorname{div}(h) + p + q \geq 0$. As h has poles at most at p and q, $\deg h = 1$ or 2. But $\deg h = 1$ would imply $X \cong \mathbb{P}^1$, contradicting X has genus 2. Thus $\deg h = 2$ and $\alpha_{\mathcal{K}_X} = [1 : h] : X \to \mathbb{P}^1$ has degree 2. □

Corollary 6.12. *There is a map from*
the set of isomorphism classes of curves of genus 2 embeds
to
{tuples of 6 points in $\mathbb{P}^1$}/PGL_2,

We'll see in a moment these 6 points determine the curve, so this is an open embedding, suggesting that $\dim \{\text{curves of genus } 2\}$ is $6 - 3 = 3$.

Remark. For $g \geq 2$, $\alpha_{2\mathcal{K}_X} : X \to \mathbb{P}^n$ is always an embedding by Riemann-Roch and embedding theorem.

Proposition 6.13. *Let X be a smooth curve of genus g, $g \geq 2$. Then*

1. *either X is hyperelliptic, i.e. admits a degree 2 map to $\mathbb{P}^1$, in which case the canonical map factors*

$$\alpha_{\mathcal{K}_X} : X \twoheadrightarrow \mathbb{P}^1 \hookrightarrow \mathbb{P}^{g-1}$$

and $\alpha_{\mathcal{K}_X} : X \to \mathbb{P}^1$ has degree 2.

> 2. *or X is not hyperelliptic, in which case $\alpha_{\mathcal{K}_X} : X \to \mathbb{P}^{g-1}$ is an embedding, called the* canonical embedding.
>
> *Moreover, 2 happens for most curves of genus g, $g \geq 3$. The set of all curves of genus g, i.e. the moduli space of curves of genus g, denoted $\mathcal{M}_g$, is an algebraic variety of dimension $3g-3$, and the set of all hyperelliptic curves of genus g is a subvariety, isomorphic to $(\mathbb{P}^1)^{2g+2}/\operatorname{PGL}_2$, of dimension $2g-1$.*

Proof. We prove 2 first. The embedding criteria says $\alpha_{\mathcal{K}_Z}$ is an embedding if and only if for all $p, q \in X$,

$$\ell(\mathcal{K}_X - p - q) = \ell(\mathcal{K}_X) - 2 = g - 2.$$

Riemann-Roch says $\ell(\mathcal{K}_X - p - q) = \ell(p+q) + g - 3$ so the embedding criteria is equivalent to $\ell(p+q) = 1$. But $\ell(p+q) > 1$ implies that X is hyperelliptic by the argument last time on $g = 2$ curves. Conversely if X is hyperelliptic there exist p, q with $\ell(p+q) > 1$ (obvious). Thus $\ell(p+q) = 1$ if and only if X is not hyperelliptic and $\alpha_{\mathcal{K}_X}$ is an embedding.

For the first part, suppose X is hyperelliptic, i.e. there exists a double cover (degree 2 map) $X \to \mathbb{P}^1$. This gives an embedding $k(x) = k(\mathbb{P}^1) \hookrightarrow k(X)$ which makes $k(X)/k(x)$ an algebraic extension of degree 2. Assume $\operatorname{ch} k \neq 2$, there exists $y \in k(X)$ such that $y^2 = f(x)$ for some $f \in k(x)$ (by completing the square). This gives a rational function $f : X \dashrightarrow \mathbb{P}^1$. As X is smooth, get a morphism $f : X \to \mathbb{P}^1$, ramified at ∞ and at points $a_1, \dots, a_r$ if $f(x) = (x-a_1)\cdots(x-a_r)$. But we say that Riemann-Roch implies that there are $2g+2$ ramification oints, so $\deg f = 2g+1$. Need to show that $\alpha_{\mathcal{K}_X}$ factors through $\mathbb{P}^1$. To finish choose $\omega = \frac{\mathrm{d}x}{y}$, and check that X^0, defined to be

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\subseteq"] & \mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\} \arrow[d, "\subseteq"] \\
X^0 = f^{-1}(A) \arrow[r] & \mathbb{A}^1
\end{tikzcd}$$

has $X^0 = \{(x,y) : y^2 = f(x)\}$ and $L(\mathcal{K}_X) = \langle \omega, x\omega, \dots, x^{g-1}\omega \rangle$ and $f|_{X^0} : X^0 \to \mathbb{A}^1$ is $(x,y) \mapsto x$, so that

$$\alpha_{\mathcal{K}_X} = [1 : x : x^2 : \cdots : x^{g-1}] : X \to \mathbb{P}^{g-1}$$

Indeed factors through $\mathbb{P}^1$ as

$$\begin{aligned} X &\to \mathbb{P}^1 && \to \mathbb{P}^{g-1} \\ (x,y) &\mapsto x && \mapsto [1 : x : \cdots : x^{g-1}] \end{aligned}$$

Finally we will not prove 3. See what happens when you restrict f to $f^{-1}(\mathbb{P}^1 \setminus \{0\})$. □

7 Abel-Jacobi theorem

Let $k = \mathbb{C}$ and X a smooth curve. Pick $\omega \in L(\mathcal{K}_X)$. For concreteness, consider

$$\begin{aligned} y^2 &= x^3 - a_2 x + a_4 \\ \omega &= \frac{\mathrm{d}x}{y} = \frac{\mathrm{d}x}{\sqrt{x^3 - a_2 x + a_4}} \end{aligned}$$

For $P, Q \in X$, we would like to define $\int_P^Q \omega$, but this is not defined unless unless we choose a path γ from P to Q. If γ is a loop and the loop is contractible then $\int_\gamma \omega = 0$, but if we choose γ to be γ_1, γ_2, two elements giving independent classes in homology, then the integral is not zero. Thus $\int_P^Q$ is not well-defined, but it is well-defined up to multiples

$$k_1 \int_{\gamma_1} \omega + k_2 \int_{\omega_2} \omega,$$

i.e. up to an element of $\mathbb{Z}\tau_1 + \mathbb{Z}\tau_2$. Thus there is a well-defined pairing

$$\begin{aligned} H_1(X; \mathbb{Z}) \times L(\mathcal{K}_X) &\to \mathbb{C} \\ ([\gamma], \omega) &\mapsto \int_\gamma \omega \end{aligned}$$

which is linear, so defines a map

$$L(\mathcal{K}_X) \to \mathrm{Hom}_{\mathbb{Z}}(H_1(X, \mathbb{Z}), \mathbb{C}) \cong H^1(X; \mathbb{C})$$

If $\ell(\mathcal{K}_G) = g$ then $H_1(X, \mathbb{Z}) \cong \mathbb{Z}^{2g}$, so the cohomology group is $\mathbb{C}^{2g}$. It is a fact that this is an injection, and RHS does not depende on the complex structure on X (and in particular, on the algebraic structure of X). However the map does change so we get a faimly of $\mathbb{C}^g$ sitting inside a fixed $\mathbb{C}^{2g}$.

Theorem 7.1 (Abel-Jacobi)**.** *Pick a basis $\omega_1, \dots, \omega_g$ of $L(\mathcal{K}_X)$. Then the map*

$$P - Q \mapsto (\int_P^Q \omega_1, \dots, \int_P^Q \omega_g)$$

extends to a well-defined map

$$\mathrm{Cl}^0(X) \to \mathbb{C}^g / \mathbb{Z}^{2g}$$

which is an isomorphism, so

$$\mathrm{Cl}^0(X) \cong \mathbb{C}^g / \mathbb{Z}^{2g} = (S^1)^{2g}.$$

The number $\int_\gamma \omega$ for $\gamma \in H_1(X; \mathbb{Z})$ are called periods*.*

Moreover $\mathrm{Cl}^0(X)$ *is a projective algebraic variety, so an* abelian variety*.*

Elementary application: we can do integrals

$$\int_\gamma \frac{\mathrm{d}x}{x^2 + ax + b}$$

by writing in elementary terms. but we cannot integrate

$$\int_\gamma \frac{\mathrm{d}x}{x^3 - x + 1}.$$

The former is a quadric so isomorphic to $\mathbb{P}^1$. The failure in doing so for cubic gives a point in $\mathrm{Cl}^0(X)$.

Index