Appendix 5 Plane curves

Here we review some basic facts about algebraic curves, that are relevant to our course.

§ Plane curves

A plane curve is a set of zeroes of a polynomial $f \in \mathbb{C}[x,y]$

$$C_f := \{ (x,y) \in \mathbb{C}^2 : f(x,y) = 0 \} \subset \mathbb{C}^2$$

- C_f is said to be <u>irreducible</u> when f is irreducible, that is f is not a product of two non-constant polynomials
- C_f is <u>non-singular</u> at $P = (x_0, y_0) \in C_f$ if $\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P) \right) \neq (0,0)$.

The tangent line at P is then defined as

$$\frac{\partial f}{\partial x}(P)\,(x - x_0) + \frac{\partial f}{\partial y}(P)\,(y - y_0) = 0.$$

- $C_f \subset \mathbb{C}^2$ inherits topology from $\mathbb{C}^2$

Implicit Function Theorem $\Rightarrow$

a non-singular point has a neighbourhood homeomorphic to a disk in the complex plane e.g. $\frac{\partial f}{\partial y}(P) \neq 0 \Rightarrow \exists$ holomorphic function $h(x)$

such that $h(x_0) = y_0$ and

$$f(x, h(x)) = 0$$

in some small disk $\{x : |x - x_0| < \delta\}$

$$x \longmapsto (x, h(x)) \in C_f$$

is a local homeomorphism

If $\frac{\partial f}{\partial y}(P) = 0$, then $\frac{\partial f}{\partial x}(P) \neq 0$ and the situation is similar.

- A curve is called non-singular (or smooth) if every point on it is non-singular. Our previous observation implies that a non-singular curve is a Riemann surface.

<u>Exercise</u> Let $g \in \mathbb{C}[x]$ be a polynomial of degree ≥ 1. Check that the plane curve given by the equation

$$y^2 = g(x)$$

is non-singular if and only if $g(x)$ has no multiple roots.

§ Projective plane curves

The *projective plane* is the set of lines through the origin in $\mathbb{C}^3$:

$$\mathbb{P}^2(\mathbb{C}) = \frac{\{(x_0, x_1, x_2) \in \mathbb{C}^3 : (x_0, x_1, x_2) \neq (0,0,0)\}}{(x_0, x_1, x_2) \sim (\lambda x_0, \lambda x_1, \lambda x_2) \quad \lambda \in \mathbb{C}^\times}$$

$$= \mathbb{C}^3 \setminus \{(0,0,0)\} / \mathbb{C}^\times$$

$[x_0 : x_1 : x_2]$ denotes the equivalence class of (x_0, x_1, x_2)

$$[x_0 : x_1 : x_2] = [\lambda x_0 : \lambda x_1 : \lambda x_2]$$

homogenous (or *projective*) *coordinates*

- $\mathbb{P}^2(\mathbb{C})$ is a 2-dimensional complex manifold

The standard atlas is given by

$$\mathbb{P}^2(\mathbb{C}) = \mathcal{U}_0 \cup \mathcal{U}_1 \cup \mathcal{U}_2$$

$$\mathcal{U}_i = \{[x_0 : x_1 : x_2] : x_i \neq 0\}$$

$$\mathcal{U}_0 \xrightarrow{\sim} \mathbb{C}^2$$

$$[x_0 : x_1 : x_2] \longmapsto \left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right)$$

and similarly $\mathcal{U}_1 \simeq \mathbb{C}^2$, $\mathcal{U}_2 \simeq \mathbb{C}^2$, so $\mathbb{P}^2(\mathbb{C})$ is covered by three copies of $\mathbb{C}^2$

- a polynomial $F \in \mathbb{C}[x_0, x_1, x_2]$ is homogeneous of degree d if $F(\lambda x_0, \lambda x_1, \lambda x_2) = \lambda^d F(x_0, x_1, x_2)$

$$\Leftrightarrow \quad F = \sum_{k_0+k_1+k_2=d} a_{k_0,k_1,k_2} \, x_0^{k_0} x_1^{k_1} x_2^{k_2}$$

A <u>projective plane curve</u> is the set of zeroes of a homogeneous polynomial

$$C_F := \{ [x_0 : x_1 : x_2] \in \mathbb{P}^2(\mathbb{C}) \mid F(x_0, x_1, x_2) = 0 \}$$

- C_F is <u>irreducible</u> when F is <u>irreducible</u> (we will only consider irreducible curves)
- degree of C_F := degree of F

- $C_F \cap \mathcal{U}_i$, $i = 0, 1, 2$ is a plane curve in the sense of the previous §

E.g. $(i=0)$ $\mathcal{U}_0 \xrightarrow{\sim} \mathbb{C}^2$

$$[x_0 : x_1 : x_2] \longmapsto \left(\frac{x_1}{x_0}, \frac{x_2}{x_0} \right) =: (y_1, y_2)$$

$$C_F \cap \mathcal{U}_0 = C_f \qquad f(y_1, y_2) := F(1, y_1, y_2)$$

Note that one can recover F from f: a plane curve can be extended to a projective curve. (The only exception is $F(x_0, x_1, x_2) = x_0^d \rightsquigarrow C_f = \emptyset$, but for irreducible curves this works.)

<u>Example</u> $\{ y_1^2 = y_2^d + a_1 y_2^{d-1} + \dots + a_d \} \subset \mathbb{C}^2$

$\downarrow$ sub $y_i = \frac{X_i}{X_0}$, multiply by X_0^d

$\{ X_1^2 X_0^{d-2} = X_2^d + a_1 X_2^{d-1} X_0 + \dots + a_d X_0^d \} \subset \mathbb{P}^2(\mathbb{C})$

- $\mathbb{P}^2(\mathbb{C})$ is compact (fact from topology)

$\Rightarrow C_F$ is compact

- C_F is <u>non-singular</u> (<u>smooth</u>) if $C_F \cap \mathcal{U}_i$ is non-singular for every $i = 0, 1, 2$.

We can now summarize:

a non-singular projective curve is a compact Riemann surface.

<u>Question</u>: what is the value of g? (genus of C_F)

The answer of course depends on the degree d. We will consider cases $d = 1, 2, 3$ explicitly.

$\boxed{d=1}$ curves of degree 1 are called <u>lines</u>

$$L: \quad a x_0 + b x_1 + c x_2 = 0$$
$$(a, b, c) \neq (0,0,0)$$

a line is always non-singular

w.l.o.g. $a \neq 0$
without loss of generality

consider the map

$$\varphi : L \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C})$$
$$[x_0 : x_1 : x_2] \longmapsto [x_1 : x_2] \qquad \text{bijection}$$
$$\left[-\frac{b}{a} x_1 - \frac{c}{a} x_2 : x_1 : x_2\right] \longleftarrow [x_1 : x_2] \qquad \text{(inverse)}$$

One can easily check that φ is a holomorphic map, as well as its inverse (we omit this check)

$\Rightarrow$ a line is isomorphic to $\mathbb{P}^1(\mathbb{C})$, the Riemann sphere

$g = 0$ (genus of L)

To deal with curves of higher degree, the following observation will be convenient:

<u>Proposition 1</u> Consider

C_F : $F(x_0, x_1, x_2) = 0$

irreducible curve of degree $d \geq 1$

L : $a x_0 + b x_1 + c x_2 = 0$ a line

Then $\# C_F \cap L = d$ (counting multiplicities)

<u>Proof</u> We shall see that under the isomorphism $L \simeq \mathbb{P}^1(\mathbb{C})$ given above, $C_F \cap L$ is a set of zeroes of a homogeneous polynomial of degree d.

W.l.o.g. $a \neq 0$

$$C_F \cap L : \underbrace{F\left(-\frac{b}{a}x_1 - \frac{c}{a}x_2 , x_1 , x_2\right)}_{\substack{\| \\ G(x_1, x_2)}} = 0 \qquad \deg G = d$$

By the main theorem of algebra, G has d roots in $\mathbb{P}^1(\mathbb{C})$ counting multiplicities. ⊠

$\boxed{d=2}$ (non-singular $\Leftrightarrow$ irreducible when $d=2$, we omit the check) irreducible curves of degree 2 are called <u>conics</u>

Let $C \subset \mathbb{P}^2(\mathbb{C})$ be a conic and $P = [x_0^* : x_1^* : x_2^*]$ be a point on C

We will sketch a construction of a bijective map $C \simeq \mathbb{P}^1(\mathbb{C})$.

(Again, we omit the check of holomorphicity.)

The set of all lines in $\mathbb{P}^2(\mathbb{C})$

$$L: \ aX_0 + bX_1 + cX_2 = 0$$

is parametrized by $[a:b:c] \in \mathbb{P}^2(\mathbb{C})$.

Consider the subset of lines passing through $P = [x_0^*: x_1^*: x_2^*]$:

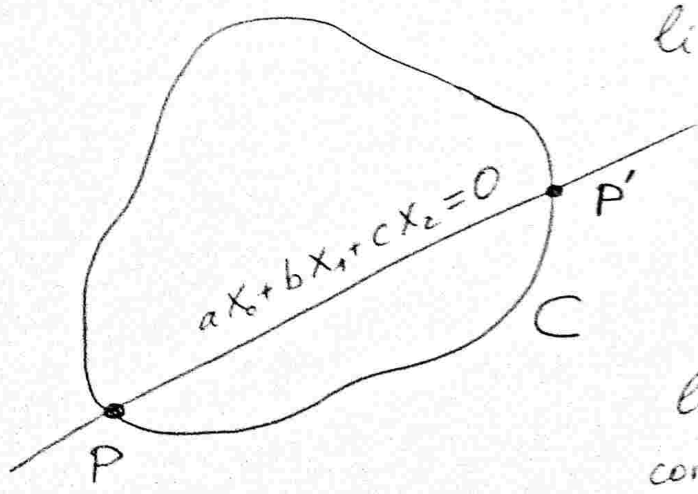
$$S := \{ [a:b:c] \in \mathbb{P}^2(\mathbb{C}) \mid ax_0^* + bx_1^* + cx_2^* = 0 \} \simeq \mathbb{P}^1(\mathbb{C})$$

because this subset is a line itself

By proposition 1, every such line intersects C in some other point $P' \in C$, which gives a bijective map

$$\mathbb{P}^1(\mathbb{C}) \simeq S \xrightarrow{\sim} C$$

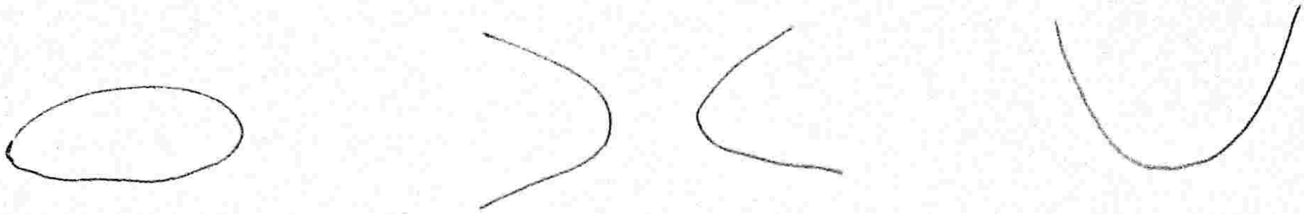
$$\text{line} \longmapsto \text{the second intersection point } P'$$



Remark: the tangent line at P will correspond to the case $P' = P$ (intersection of multiplicity 2)

We conclude that a conic is a Riemann surface of genus 0 (it is isomorphic to the Riemann sphere)

Remark: in geometry over the real numbers, irreducible curves of degree 2 in the plane $\mathbb{R}^2$ are classified into three classes



ellipses, hyperbolas and parabolas.

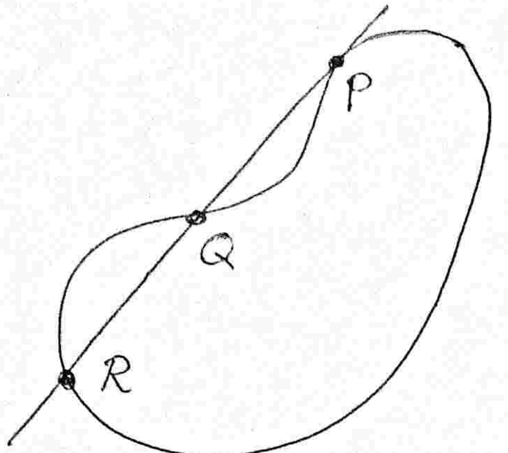
As we saw above, when one extends from $\mathbb{R}$ to the algebraically closed field $\mathbb{C}$ (to have the main theorem of algebra working) and from the plane to its projectivization $\mathbb{P}^2$ (here we have Proposition 1), then all conics become isomorphic.

Conics over $\mathbb{R}$ are called conic sections.

$\boxed{d=3}$ $C : F(x_0, x_1, x_2) = 0$ smooth

irreducible homogeneous polynomial of degree 3

In the case of degree 3, Proposition 1 can be used to define a group law on C. Rougly, this works as follows: for any two points $P, Q \in C$ we "draw" a line through P and Q; this line must have the third point of intersection, call it $R = R(P, Q)$.



So we get a binary operation

$$\begin{aligned} C \times C &\longrightarrow C \\ (P, Q) &\longmapsto R \end{aligned}$$

Note: $R(Q,P) = R(P,Q)$ the operation is commutative

To define a group law one actually needs some assumptions. In particular, there should be the neutral element (zero of the group law):

Def A point $O \in C$ is called a <u>point of inflection</u> if the tangent line at O intersects C only at O (this means multiplicity 3, by Proposition 1)

Example Consider

$C: \quad X_1^2 X_2 = X_0^3 + a X_0^2 X_2 + b X_0 X_2^2 + c X_2^3.$

Then $O = [0:1:0] \in C$ is an inflection point.

$U_1 = \{X_1 \neq 0\}$ $\quad y_0 = \frac{X_0}{X_1} \quad y_2 = \frac{X_2}{X_1}$ coordinates

$C \cap U_1 = \{ \underline{y_2 = y_0^3 + a y_0^2 y_2 + b y_0 y_2^2 + c y_2^3} \}$ call this $f(y_0, y_2)$

$\cup$

$O = (0,0)$ $\quad \frac{\partial f}{\partial y_2}(0) = 1 \quad \frac{\partial f}{\partial y_0}(0) = 0$

$\Rightarrow y_2 = 0$ tangent line

$\Rightarrow$ in $\mathbb{P}^2(\mathbb{C})$ the tangent line to C at O is given by $X_2 = 0$

Its intersection with C must have $X_0 = 0$ (see the equation of C), so the only intersection pt. is $O = [0:1:0]$.

On a smooth cubic curve C with an inflection point $O \in C$ one can define a commutative group law as follows:

- O is the zero $\quad (P + O = P \quad \forall P \in C)$
- for each $O \neq P \in C$ its inverse $-P$ is defined as the third intersection point of the line through O and P with C
- for $P, Q \in C$ define $P + Q = -R(P,Q)$, where $R = R(P,Q)$ is the third intersection point

Remark: In the last property, when $P = Q$ one takes the tangent line at P to define $2P = P + P = -R(P,P)$. This requires the smoothness assumption on C.

We omit the check that the above defined addition law satisfies the respective axioms.

One can prove that the situation described in the last example is in fact general:

Proposition 2 Consider a smooth projective cubic curve $C \subset \mathbb{P}^2(\mathbb{C})$ which has an inflection point $\mathcal{O} \in C$. Then there is a linear change of coordinates in $\mathbb{P}^2(\mathbb{C})$

$$(X_0, X_1, X_2) \to (X_0, X_1, X_2)M, \quad M \in GL_3(\mathbb{C})$$

such that in the new coordinates $\mathcal{O} = [0:1:0]$ and the equation of C becomes

$$X_1^2 X_2 = X_0^3 + a X_0^2 X_2 + b X_0 X_2^2 + c X_2^3 \qquad (*)$$

for some $a, b, c \in \mathbb{C}$.

The proof is left as an exercise.

Remark: A smooth plane cubic C with a fixed point $O \in C$ can be transformed into (*) by a rational change of coordinates in $\mathbb{P}^2(\mathbb{C})$. In particular, this transformation will make O an inflection point.

Def A smooth plane cubic curve $C \subset \mathbb{P}^2(\mathbb{C})$ with an inflection point $O \in C$ is called an *elliptic curve*. Equation (*) is called the Weierstrass equation.

Note that (*) is non-unique. For example, changing $X_0 \to X_0 + \frac{a}{3} X_2$ we get (*) with $a = 0$. There is more freedom left. We will consider this question later.

Observe that O is the only solution of (*) with $X_2 = 0$. It follows that $C \setminus \{O\}$ is the plane curve $C \cap U_2$, which is given in the coordinates $x := \frac{X_0}{X_2}$, $y := \frac{X_1}{X_2}$ by

$$y^2 = x^3 + a x^2 + b x + c. \qquad (**)$$

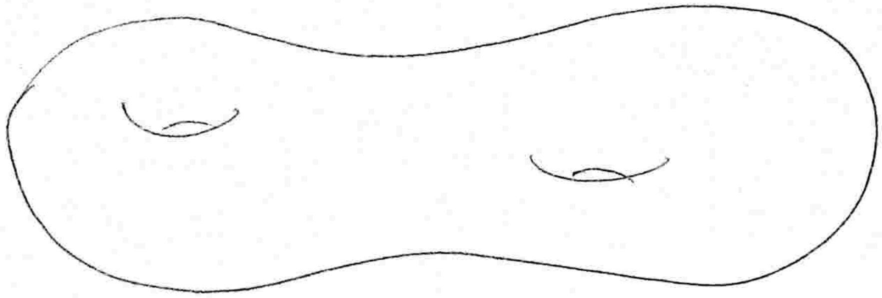
The curve (*) is smooth if and only (**) is smooth. Indeed, we constructed the tangent line at O in the above example, and every other point of C belongs to (**). By the exercise given earlier, (**) is a smooth curve if and only if $g(x) = x^3 + ax^2 + bx + c$ has no multiple roots.

Corollary 3 A smooth projective cubic is a Riemann surface of genus 1.

Proof Consider the holomorphic map

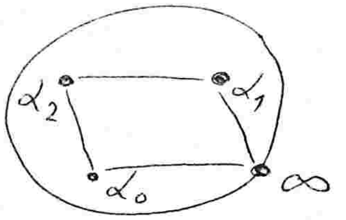
$$f : C \longrightarrow \mathbb{P}^1(\mathbb{C})$$

given by $f = \frac{X_0}{X_2}$ (we assume that C is given by the Weierstrass equation (*)). Then f has degree 2 (in the chart (**) f is given by $f(x,y) = x$, so a generic point has 2 preimages). The only points with 1 preimage are $\infty = [1:0]$ ($f^{-1}(\infty) = O$) and the three roots of $g(x) = x^3 + ax^2 + bx + c$.



C

$$\Big\downarrow\ f(X_0:X_1:X_2) = \frac{X_0}{X_2}$$



$\mathbb{P}^1(\mathbb{C})$

Consider the graph on $\mathbb{P}^1(\mathbb{C})$ with vertices ∞ and α_i, $i = 0, 1, 2$ (the roots of $g(\alpha_i) = 0$), joined by four edjes. This graph has $V = 4$ vertices, $E = 4$ edjes, $F = 2$ faces. Its preimage in C will have

$$V' = 4, \quad E' = 2 \cdot E = 8, \quad F' = 2 \cdot F = 4$$

and therefore the genus g of C satisfies

$$2 - 2g = V' - E' + F' = 0$$

$$\Rightarrow \quad g = 1$$

(see Lecture 4 about genus computation using graphs.) $\boxtimes$