

M3P20 Geometry I: Algebraic Curves

Lectured by Dr Mattia Talpo
Typeset by David Kurniadi Angdinata

Autumn 2018

Contents

1	Introduction	2
2	Complex plane curves	5
3	Projective space	9
4	Projective curves	12
5	Affine vs projective plane curves	15
6	Points at infinity	17
7	Smoothness and singularities	19
8	Projective transformations	22
9	Resultants and weak Bézout	24

1 Introduction

This course is intended as a first course in algebraic geometry, the area of mathematics that studies spaces defined by polynomial equations using algebra. It will focus on one-dimensional algebraic varieties. The reference books for the course are the following.

1. F Kirwan, Complex algebraic curves, 1992
2. W Fulton, Algebraic curves: an introduction to algebraic geometry, 1969

Geometry is the study of shapes in suitable spaces, such as sets of points on the real line \mathbb{R} , lines and circles in \mathbb{R}^2 , spheres in higher dimensional Euclidean spaces \mathbb{R}^n , etc. One way to think about shapes is to see them as the locus of zeroes defined by

$$\{(x_1, \dots, x_n) \in \mathbb{R}^n \mid f(x_1, \dots, x_n) = 0\} \iff \{f(x_1, \dots, x_n) = 0\} \subset \mathbb{R}^n$$

for some suitable function f .

Example 1.1.

1. Circles $\{f_1(x, y) = x^2 + y^2 - R^2 = 0\}$ in \mathbb{R}^2 for some $R \in \mathbb{R}$.
2. The unit square with vertices at $\{(\pm 1, 0), (0, \pm 1)\}$ in \mathbb{R}^2 defined by $\{f_2(x, y) = |x| + |y| - 1 = 0\}$.
3. Spheres $\{f_3(x_1, \dots, x_n) = x_1^2 + \dots + x_n^2 - R^2\}$ in \mathbb{R}^n for some $R \in \mathbb{R}$.

Remark 1.2. Every subset $S \subseteq \mathbb{R}^n$ is the zero-set of some function. We can define $\chi_S(x) = 1$ if $x \notin S$, $\chi_S(x) = 0$ if $x \in S$.

The class of functions used to define our shapes has great consequences on their geometry. For the circle, f_1 is a polynomial so that it is differentiable and also C^∞ . For the square, f is continuous but not differentiable at $\{(0, \pm 1), (\pm 1, 0)\}$, the vertices of the square. The function χ_S is not even continuous, unless S is empty, or the whole \mathbb{R}^n . As these examples illustrate, an underlying principle is the following equivalence.

Fact 1. Regularity properties of f are regularity properties of $\{f = 0\}$.

Such shapes are called **algebraic varieties**. Their geometric properties are intimately related to the algebraic properties of the defining polynomial equations.

Example 1.3.

1. Let $f(x)$ be a polynomial. Then the zero set of $f(x)$, $\{f(x) = 0\} \subseteq \mathbb{R}$ is a finite set of points in \mathbb{R} , and every finite set of points arises in this manner.
2. The circle is an algebraic variety.
3. Spheres in higher dimensions are algebraic varieties.

Exercise 1.

1. Is $\mathbb{Z} \subseteq \mathbb{R}$ an algebraic variety? No.
2. Is the unit square an algebraic variety? No.

Definition 1.4. Let K be a field, such as $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. For $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ a multi-index, denote by $|\alpha| = \sum_{i=1}^n \alpha_i$ and by $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$, a **monomial**. A **polynomial of degree d** in n variables with coefficients in K is a finite sum.

$$P(x_1, \dots, x_n) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha,$$

where $a_\alpha \in K$, $a_\alpha = 0$ for all $|\alpha| > d$ and $a_\alpha \neq 0$ for some α with $|\alpha| = d$. The set of polynomials of arbitrary degree in n variables with coefficients in K is denoted $K[x_1, \dots, x_n]$.

Example 1.5. Let $n = 3$. $P(x_1, x_2, x_3) = 3 + x_1^2 x_2 + x_3^{10}$ for $\alpha = (2, 1, 0)$ and $\alpha = (0, 0, 10)$ has degree ten.

Exercise 2.

1. Show that $K[x_1, \dots, x_n]$ is a ring, and that if P, Q are polynomials of degrees p, q respectively, then the degree of $\lambda P + \mu Q$ for $\lambda, \mu \in K$ is at most $\max\{p, q\}$. Give an example of polynomials $P, Q \in K[x]$ such that $\deg(P + Q) < \max\{\deg(P), \deg(Q)\}$.
2. Show that $(P \cdot Q)(x_1, \dots, x_n) = P(x_1, \dots, x_n)Q(x_1, \dots, x_n)$ is a polynomial $P \cdot Q \in K[x_1, \dots, x_n]$ with $\deg(P \cdot Q) = \deg(P) + \deg(Q)$. What if $P = 0$? What is $\deg(0)$?

Definition 1.6. An **affine plane curve** defined over K is

$$C = \{(x, y) \in K^2 \mid P(x, y) = 0\} \subset K^2,$$

where $P \in K[x, y]$. More generally, an **algebraic variety** $V \subset K^n$ is a subset of K^n defined as the locus

$$\{f_1 = \dots = f_k = 0\} \subset K^n,$$

where $f_1, \dots, f_k \in K[x_1, \dots, x_n]$ are polynomials in n variables with coefficients in K .

Example 1.7.

1. Let $a, b, c \in \mathbb{R}$ with $(a, b) \neq (0, 0)$, and let

$$f(x, y) = ax + by + c.$$

Then $\{(x, y) \in \mathbb{R}^2 \mid f(x, y) = 0\}$ is a line.

2. Let $a, b \in \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ and

$$f(x, y) = \frac{x^2}{a^2} + \frac{y^2}{b^2} - 1.$$

The curve $\{(x, y) \in \mathbb{R}^2 \mid f(x, y) = 0\}$ is an ellipse.

3. Let $a, b \in \mathbb{R}^*$ and

$$g(x, y) = \frac{x^2}{a^2} - \frac{y^2}{b^2} - 1.$$

The curve $\{(x, y) \in \mathbb{R}^2 \mid g(x, y) = 0\}$ is a hyperbola.

4. Spheres, quadrics such as ellipsoids, paraboloids, and hyperboloids in \mathbb{R}^3 are all defined via a single polynomial equation of degree two. A line in \mathbb{R}^3 can be defined by two equations in degree one.

The first property of algebraic curves is the following.

Lemma 1.8. The union of two affine plane curves is again an affine plane curve.

Proof. Let $f_1, f_2 \in K[x, y]$ and let $C_1 = \{f_1 = 0\}$ and $C_2 = \{f_2 = 0\}$. Then $f_1 \cdot f_2 \in K[x, y]$ is a polynomial and

$$C_1 \cup C_2 = \{f_1 \cdot f_2 = 0\},$$

so that $C_1 \cup C_2$ is an affine plane curve. □

Exercise 3. Write down an equation for the plane curve that is the union of the lines through any two vertices of the unit square.

Recall the following.

Definition 1.9. A polynomial $P \in K[x_1, \dots, x_n]$ is **reducible** over K if there are non-constant polynomials $Q, R \in K[x_1, \dots, x_n]$, so $\deg(Q), \deg(R) > 0$, such that $P = Q \cdot R$. A polynomial P is **irreducible** if it is not reducible.

Example 1.10. x_1x_2 is reducible, $x_1 + x_2$ is irreducible.

Fact 2. Recall also that every polynomial $P \in K[x_1, \dots, x_n]$ can be written as a product of irreducible factors $P = f_1 \dots f_k$ in an essentially unique way up to multiplication by constants. We have

$$\{P = 0\} = \{f_1 = 0\} \cup \dots \cup \{f_k = 0\} \subseteq K^n,$$

so in particular every algebraic curve is a union of algebraic curves defined by irreducible polynomials.

In the course, we will consider questions such as the following.

1. When do polynomials $f, g \in K[x, y]$ define the same affine plane curve?
2. What can be said about the intersection $\{f = 0\} \cap \{g = 0\} \subset K^2$?

Very different questions can be approached through algebraic curves. For example, we can study integer solutions to some Diophantine equations.

Example 1.11. The unit circle is the curve

$$C = \{x^2 + y^2 = 1\} \subset \mathbb{R}^2.$$

Several parametrisations are known, such as

$$t \in [0, 2\pi) \mapsto (\cos t, \sin t) \in \mathbb{R}^2.$$

We can write down another parametrisation of C by considering lines through the point $P = (-1, 0)$ using a stereographic projection. A line through P with slope $t \in \mathbb{R}$ has equation

$$L_t = \{y = t(x + 1)\} \subset \mathbb{R}^2$$

and meets C in two points, P and $P_t = (x(t), y(t))$. We can determine the coordinate of P_t by solving the system

$$L_t \cap C = \begin{cases} y = t(x + 1) \\ x^2 + y^2 = 1 \end{cases}.$$

Replacing the value of y given by the first equation into the second yields two solutions for $x(t)$. The first one is $x = -1$ and corresponds to the point $P = (-1, 0)$. The second is $(x(t), y(t))$, where

$$x(t) = \frac{1 - t^2}{1 + t^2}, \quad y(t) = \frac{2t}{1 + t^2}.$$

Note that when $t \rightarrow \infty$, $(x(t), y(t)) \rightarrow (-1, 0)$, so that $t \mapsto (x(t), y(t))$ is a parametrisation of C that identifies it with $\mathbb{R} \cup \{\infty\}$. The advantage of this parametrisation is that it is given by rational functions, that is $x(t)$ and $y(t)$ are of the form

$$t \mapsto \frac{p(t)}{q(t)},$$

where p, q are polynomials. One can use this parametrisation to get the general solution of the equation

$$x^2 + y^2 = z^2 \tag{1}$$

for $x, y, z \in \mathbb{Z}$ coprime. If $t = p/q \in \mathbb{Q}$, where $p, q \in \mathbb{Z}$ are coprime, then $x(t), y(t) \in \mathbb{Q}$ becomes

$$x(t) = \frac{p^2 - q^2}{p^2 + q^2}, \quad y(t) = \frac{2pq}{p^2 + q^2}.$$

If $x = p^2 - q^2$, $y = 2pq$, and $z = p^2 + q^2$, $x, y, z \in \mathbb{Z}$ satisfy (1). They are coprime precisely when p, q are coprime and not both odd. When p, q are coprime and both odd, then

$$x = \frac{p^2 - q^2}{2}, \quad y = pq, \quad \frac{p^2 + q^2}{2}$$

satisfy (1). Conversely, this is the general form of solutions in (1). Indeed, given $x, y, z \in \mathbb{Z}$ coprime that satisfy (1), $z \neq 0$ and

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

so that $(x/z, y/z) \in \mathbb{C}$ and if $(x, y, z) \neq (-1, 0, 1)$, there is $t \in \mathbb{R}$ such that $(x/z, y/z) = (x(t), y(t))$. But then since $x/z, y/z \in \mathbb{Q}$, we can take $t \in \mathbb{Q}$ and x, y, z have the form above.

Definition 1.12. Let $f \in \mathbb{R}[x, y]$ and let $C = \{f = 0\}$. A **rational point** of C is a point $(x, y) \in C$, that is $f(x, y) = 0$, such that $x, y \in \mathbb{Q}$.

Example 1.13. There are infinitely many rational points on the circle $\{x^2 + y^2 = 1\} \subseteq \mathbb{R}^2$, which can be described explicitly, and can be used to solve $a^2 + b^2 = c^2$ for $a, b, c \in \mathbb{Z}$, a problem in number theory. Now take $n \geq 3$ and consider

$$C = \{x^n + y^n - 1 = 0\}.$$

What are the rational points of C ? Write

$$x = \frac{a}{c}, \quad y = \frac{b}{c}, \quad a, b, c \in \mathbb{Z}, \quad c \neq 0.$$

Then

$$(x, y) \in C \iff a^n + b^n = c^n.$$

Fermat's Last Theorem by Wiles then states that there exists no solution with $a, b \neq 0$.

2 Complex plane curves

Let $P \in \mathbb{R}[x, y]$ be a polynomial with coefficients in \mathbb{R} . A priori, it is natural to study the real plane curve $C_{\mathbb{R}} = \{(x, y) \in \mathbb{R}^2 \mid P(x, y) = 0\}$. However, P can also be seen as a polynomial with coefficients in \mathbb{C} , and it will often be simpler to study the complex plane curve $C_{\mathbb{C}} = \{(x, y) \in \mathbb{C}^2 \mid P(x, y) = 0\}$. We first explain some of the properties of algebraic curves that we would like to hold and explain why these properties do not necessarily hold for real plane curves and some unpleasant things happen.

Fact 3. Many real curves are so degenerate that they do not even have points, that is $C_{\mathbb{R}} = \emptyset$. If $C_{\mathbb{R}} \neq \emptyset$, the dimension of $C_{\mathbb{R}}$ is difficult to determine.

Example 2.1. Let $t \in \mathbb{R}$ and consider $f_t(x, y) = x^2 + y^2 - t$ and the real plane curve $C_t = \{f_t(x, y) = 0\} \subseteq \mathbb{R}^2$. If $t > 0$, C_t is a circle with radius \sqrt{t} , if $t = 0$, has $C_0 = \{(0, 0)\}$, and if $t < 0$, $C_t = \emptyset$.

Fact 4. In general, it is not clear when two polynomials $f, g \in \mathbb{R}[x, y]$ define the same real plane curve, that is when

$$\{(x, y) \in \mathbb{R}^2 \mid f(x, y) = 0\} = \{(x, y) \in \mathbb{R}^2 \mid g(x, y) = 0\}.$$

Example 2.2. Let f, g denote the polynomials

$$f(x, y) = x^2y + y^2 + x^3 + x, \quad g(x, y) = x^2 + 2xy + y^2.$$

Then, since $f(x, y) = (x + 1) \cdot (x^2 + 1)$ and $g(x, y) = (x + y)^2$,

$$\{(x, y) \in \mathbb{R}^2 \mid f(x, y) = 0\} = \{(x, y) \in \mathbb{R}^2 \mid g(x, y) = 0\}.$$

Fact 5. In general, it is hard to predict when a curve intersects a fixed line, or more generally when two real curves intersect.

Example 2.3. In the notation of Example 2.1, let $C = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 - 1\} \subset \mathbb{R}^2$ be the unit circle. Consider the line $\{ax + by + c = 0\}$ for $(a, b) \neq (0, 0)$. Then, depending on $(a, b, c) \in \mathbb{R}^3$, $L \cap C$ consists of two points, one point, or is empty.

Lecture 2
Thursday
11/10/18

Most of these difficulties disappear when working with curves $C_{\mathbb{C}} \subset \mathbb{C}^2$, essentially because \mathbb{C} is algebraically closed, in other words the following theorem holds.

Theorem 2.4 (Fundamental theorem of algebra). Let $P \in \mathbb{C}[x]$ be a non-constant polynomial. Then P has at least one complex root, that is there exists $\alpha \in \mathbb{C}$ such that $P(\alpha) = 0$.

A consequence of the fundamental theorem of algebra is that if $P \in \mathbb{C}[x, y]$ is non-constant, then $C = \{P = 0\}$ has infinitely many points. Assume without loss of generality that the polynomials in one variable $P(\cdot, y)$ and $P(x, \cdot)$ are not constant. This means that if

$$P(x, y) = \sum_{(r,s) \in \mathbb{N}^2} c_{r,s} x^r y^s,$$

there exist (r, s) and (r', s') in \mathbb{N}^2 , which may be equal, such that $r \neq 0$ and $s' \neq 0$, and $c_{r,s} \neq 0$ and $c_{r',s'} \neq 0$. When $y_0 \neq 0$ the polynomial $P(x, y_0) \in \mathbb{C}[x]$ is non-constant and by Theorem 2.4, there exists $x_0 \in \mathbb{C}$ such that $P(x_0, y_0) = 0$. In fact, for most choices of $y_0 \neq y'_0$, the polynomials $P(\cdot, y_0)$ and $P(\cdot, y'_0)$ are different, and have some distinct roots. It follows that $\{P = 0\}$ contains infinitely many points.

Example 2.5. Let $a, b, c \in \mathbb{C}$ with $(a, b) \neq (0, 0)$, and let $f(x, y) = ax + by + c$. If $a \neq 0$, for each $y \in \mathbb{C}$, there is precisely one solution of $f(x, y) = 0$, namely

$$x = -\frac{b}{a}y - \frac{c}{a}.$$

Thus $\mathbb{C}^2 \supset \{f = 0\} = C \rightarrow \mathbb{C} \cong \mathbb{R}^2$ is an isomorphism. We will call C a **complex line**.

Remark 2.6. It is difficult to draw complex curves. Our intuition is for real vector spaces, and this makes complex curves hard to visualise. They are objects of real dimension two in $\mathbb{C}^2 \cong \mathbb{R}^4$, a four-dimensional real vector space.

Example 2.7. Let $f(x, y) = x^2 + y^2$. Then $f(x, y) = (x + iy) \cdot (x - iy)$ and, as in Lemma 1.8, $C = \{f = 0\} \subset \mathbb{C}^2$ is the union of the two complex lines $\{x + iy = 0\}$ and $\{x - iy = 0\}$. When seen as \mathbb{R} -vector spaces, these two planes meet at exactly one point corresponding to $(0, 0) \in \mathbb{R}^2 \subseteq \mathbb{C}^2$, the only real point of C . It is difficult to imagine two planes meeting in one point, because our intuition relies on three-dimensional space \mathbb{R}^3 , while $\mathbb{C}^2 = \mathbb{R}^4$.

Describing intersections is also easier.

Example 2.8. Consider $C = \{x^2 + y^2 - 1 = 0\} \subseteq \mathbb{C}^2$ and $L = \{ax + by + c = 0\} \subseteq \mathbb{C}^2$. If $b \neq 0$, we determine the intersection $C \cap L$ by solving the equation

$$x^2 + y^2 = 1, \quad y = -\frac{a}{b}x - \frac{c}{b}.$$

If $a^2 = -b^2$ or $c = 0$, there are one or two solutions. Again, it is hard to imagine a two-dimensional real surface which meets a real plane in two points.

We now turn to the question of recognising when two polynomials define the same plane curve. Here again, working in \mathbb{C} is a simplification.

Theorem 2.9 (Consequence of Hilbert's Nullstellensatz). Let $f, g \in \mathbb{C}[x, y]$ be two polynomials. Then

$$\{f = 0\} = \{g = 0\}$$

if and only if there exist $P_1, \dots, P_k \in \mathbb{C}[x, y]$, $a_1, \dots, a_k, b_1, \dots, b_k \in \mathbb{Z}_{>0}$ and $\lambda_1, \lambda_2 \in \mathbb{C}^*$ such that

$$f(x, y) = \lambda_1 P_1^{a_1} \dots P_k^{a_k}, \quad g(x, y) = \lambda_2 P_1^{b_1} \dots P_k^{b_k}. \quad (2)$$

Proof. Assume that (2) holds. Then by the proof of Lemma 1.8,

$$\{f = 0\} = \{P_1^{a_1} = 0\} \cup \dots \cup \{P_k^{a_k} = 0\} = \{P_1 = 0\} \cup \dots \cup \{P_k = 0\},$$

because if $\alpha \in \mathbb{C}$ is such that $\alpha^n = 0$, then $\alpha = 0$. The same holds for $\{g = 0\}$. Therefore $\{f = 0\} = \{g = 0\}$. The second half of the proof needs tools of commutative algebra and is omitted. \square

Remark 2.10. The theorem fails over \mathbb{R} . Let $f(x, y) = x^2 + 1$ and $g(x, y) = 1$. Then $\{f = 0\} = \{g = 0\} = \emptyset$ but the conclusion in (2) is not true.

Thus, the relation between the geometric shape $C = \{f = 0\}$ in \mathbb{C}^2 and the polynomial $f \in \mathbb{C}[x, y]$ is more transparent than in \mathbb{R} . We will always work in \mathbb{C} . Let us introduce some important notions for the study of polynomials.

Definition 2.11. A polynomial $f \in K[x, y]$ has **no repeated factors** over K if it cannot be written as a product of the form

$$f(x, y) = g(x, y)^2 \cdot h(x, y),$$

where $g, h \in K[x, y]$ and g is non-constant.

Exercise 4. Show that this is equivalent to

$$f = P_1 \dots P_k,$$

where P_1, \dots, P_k are distinct irreducible polynomials.

Corollary 2.12. Let $f, g \in \mathbb{C}[x, y]$ be polynomials with no repeated factors. Then f, g define the same complex plane curve

$$\{f = 0\} = \{g = 0\}$$

if and only if there is a non-zero constant $\lambda \in \mathbb{C}^*$ such that $f = \lambda g$.

Proof. Follows immediately from Theorem 2.9. \square

Remark 2.13. If $f = P_1^{a_1} \dots P_k^{a_k}$ with P_i irreducible for all i and $a_i \in \mathbb{N}$, then $\{f = 0\} = \{g = 0\}$ where $g = P_1 \dots P_k$. We do not lose anything by only looking at f with no repeated factors.

Let $C \subseteq \mathbb{C}^2$ be a complex plane curve. We have proved that, up to multiplication by $\lambda \in \mathbb{C}^*$, there is a unique non-constant polynomial $f \in \mathbb{C}$ with no repeated factors such that

$$C = \{f = 0\}.$$

It makes sense to define the following.

Definition 2.14. The **degree** of an affine curve $C \subseteq \mathbb{C}^2$ is the degree of any polynomial with no repeated factors f such that $C = \{f = 0\}$, that is

$$\deg(C) = \deg(f).$$

Example 2.15. Lines have degree one, since they are defined by a linear polynomial. Conics have degree two. $\{x^2y + y^2 + x + 1 = 0\}$ has degree 3, assuming it has no repeated factors.

Unless mentioned otherwise, in the first few weeks, we will assume that polynomials have no repeated factors.

Definition 2.16. Let $f_1, f_2 \in \mathbb{C}[x, y]$ be polynomials with no repeated factors and let $C_1 = \{f_1 = 0\}$ and $C_2 = \{f_2 = 0\}$ be the associated complex curves. The curves C_1 and C_2 have **no common component** if there is no non-constant polynomial P that divides both f_1 and f_2 .

This is equivalent to saying that if $f = P_1^{a_1} \dots P_k^{a_k}$ and $g = Q_1^{b_1} \dots Q_l^{b_l}$ with P_i, Q_i irreducibles, P_i distinct, and Q_i distinct, then $\lambda P_i \neq Q_j$ for all $i, j, \lambda \in \mathbb{C}^*$.

Exercise 5. Show that if C_1 and C_2 have no common component, then $\deg(C_1 \cup C_2) = \deg(C_1) + \deg(C_2)$.

Exercise 6. Let L, L' be the lines

$$L = \{ax + by + c = 0\} \subset \mathbb{C}^2, \quad L' = \{a'x + b'y + c' = 0\} \subset \mathbb{C}^2.$$

1. Show that L and L' meet at exactly one point if and only if $ab' - a'b \neq 0$.
2. Show that $L = L'$ if and only if there exists $\lambda \in \mathbb{C}$ such that $\lambda \neq 0$ and

$$a' = \lambda a, \quad b' = \lambda b, \quad c' = \lambda c.$$

Remark 2.17 (First aid topology).

1. A **topological space** is a set X with a collection of open subsets $\{U_i \subset X\}$ such that
 - (a) \emptyset and X are open,
 - (b) any union $\cup_{i \in I} U_i$ of open sets U_i is open, and
 - (c) any finite intersection $\cap_{i=1}^k U_i$ of open sets U_i is open.
2. A **metric space** X , such as $(\mathbb{C}^n, \|\cdot\|)$, is a topological space. The open sets are given by arbitrary unions and finite intersections of the familiar open balls $B(x, \epsilon) = \{z \in X \mid \|z - x\| < \epsilon\}$.
3. A subset $X \subset Y$ of a topological space Y inherits a topology from Y . The open sets of X are the sets $X \cap U$, where $U \subset Y$ is an open set of Y .
4. X is **compact** if for all open covering $X = \sum_{i \in I} U_i$ where U_i are open, there exists a finite subcovering $\cup_{i_1, \dots, i_k} U_{i_j}$ for $\{i_1, \dots, i_k\} \subseteq I$.
5. The **Heine-Borel theorem** states that a subset X of \mathbb{R}^n or of \mathbb{C}^m is compact if and only if X is closed, that is its complement is open, and bounded for the usual norm.
6. A closed subset of a compact space is compact.
7. A map $f : X \rightarrow Y$ between topological spaces is **continuous** if and only if $f^{-1}(U)$ is open in X whenever $U \subset Y$ is open. It follows that $f^{-1}(F)$ is closed whenever $F \subset Y$ is closed. In particular, if $f \in \mathbb{C}[x_1, \dots, x_n]$ is a polynomial, f defines a map $f : \mathbb{C}^n \rightarrow \mathbb{C}$ that is continuous, and

$$f^{-1}(\{0\}) = \{f = 0\} \subset \mathbb{C}^n$$

is closed because $\{0\}$ is a closed subset of \mathbb{C} .

In particular, \mathbb{C}^2 is a topological space with the Euclidean distance in \mathbb{R}^4 and the affine plane curve $C = \{f = 0\} \subseteq \mathbb{C}^2 \cong \mathbb{R}^4$ inherits a topology. Open sets of C are $U \cup C$ where $U \subseteq \mathbb{C}^2$ is open. So algebraic curves have a natural topology.

Lemma 2.18. Let $C \subset \mathbb{C}^2$ be an affine plane curve, then C is not compact.

Proof. Since f is a continuous function $\mathbb{C}^2 \rightarrow \mathbb{C}$, $C = \{f = 0\} = f^{-1}(\{0\})$, and $\{0\}$ is closed in \mathbb{C} , C is closed in \mathbb{C}^2 . We check that $C \subset \mathbb{C}^2$ is not bounded. Assume that it is, then there is a constant $M > 0$ such that $C \subset B(0, M)$, where the open ball is

$$B(0, M) = \left\{ |x|^2 + |y|^2 < M \right\}.$$

Want to show that some points in \mathbb{C} are outside this open ball. Let $y_0 \in \mathbb{C}$ be such that $|y_0| > M$ and assume we can arrange for $g = f(\cdot, y_0)$ to be a non-constant polynomial of x . By the fundamental theorem of algebra, g has a root $x_0 \in \mathbb{C}$ and the point $(x_0, y_0) \in C$. This is a contradiction, as $(x_0, y_0) \notin B(0, M)$. \square

(TODO Exercise: what if $f(x, y)$ happens to be a polynomial of y alone, so that this cannot be arranged?)

3 Projective space

Recall that it is difficult to determine when two affine plane curves $C, C' \in \mathbb{C}^2$ intersect, and some curves do not in fact intersect even over \mathbb{C} . We want to fix that, and the key is adding points at infinity.

Example 3.1.

1. Consider two distinct lines

$$L_1 = \{ax + by + c = 0\}, \quad L_2 = \{a'x + b'y + c' = 0\}.$$

Then L_1 and L_2 meet at exactly one point if and only if

$$\det \begin{pmatrix} a & b \\ a' & b' \end{pmatrix} \neq 0.$$

But we can pretend that parallel lines meet at a point at infinity corresponding to the direction vector.

2. Consider the asymptotic curve and line

$$C = \{xy - 1 = 0\}, \quad L = \{x = 0\}.$$

Then C and L do not meet, but again we can pretend that they meet at a point at infinity.

A heuristic trick is to introduce a variable z .

1. Replace x by x/z and y by y/z .
2. Solve for $z = 0$.

Example 3.2.

1. Consider the lines

$$L_1 = \{x + y + 1 = 0\}, \quad L_2 = \{x + y - 1 = 0\}.$$

Clearly L_1 and L_2 do not meet. Let us apply the trick. By 1 and 2 we get

$$\begin{cases} x/z + y/z + 1 = 0 \\ x/z + y/z - 1 = 0 \end{cases} \implies \begin{cases} x + y + z = 0 \\ x + y - z = 0 \end{cases} \implies \begin{cases} x + y = 0 \\ x + y = 0 \end{cases}.$$

We get that the point $(1, -1, 0)$ is a common solution. This will be called the point at infinity.

2. Consider the asymptotic curve and line

$$C = \{xy - 1 = 0\}, \quad L = \{x = 0\}.$$

Apply 1 and 2 to get

$$\begin{cases} xy - z^2 = 0 \\ x/z = 0 \end{cases} \implies \begin{cases} xy = 0 \\ x = 0 \end{cases}.$$

We get that $(0, 1, 0)$ is a common solution. Again, this will be called the point at infinity.

To make this formal, we introduce the projective plane \mathbb{P}^2 . We will add points at infinity to \mathbb{C}^2 , in such a way that asymptotic curves meet at infinity. We will then compactify an affine plane curve C so that the two compactifications are compatible, that is

$$(C \subseteq \mathbb{C}^2) \hookrightarrow (\overline{C} \subseteq \mathbb{P}^2).$$

Notation 3.3. Fix $n \geq 0$ and \mathbb{C}^{n+1} . Let $\underline{0} = (0, \dots, 0) \in \mathbb{C}^{n+1}$ be the origin of the $(n+1)$ -dimensional complex Euclidean space. We will denote

$$W = \mathbb{C}^{n+1} \setminus \{\underline{0}\},$$

that a point $x \in W$ is given by $x = (x_0, \dots, x_n)$ where $x_0, \dots, x_n \in \mathbb{C}$ are not all zero. We define the equivalence relation on W , for any $x, y \in W$ by

$$x \sim y \iff \exists \lambda \in \mathbb{C}^* = \mathbb{C} \setminus \{0\}, x = \lambda y.$$

Exercise 7. Show that \sim is an equivalence relation on W .

Notation 3.4. Given $x \in W$, we denote

$$[x] = \{y \in W \mid x \sim y\}.$$

For simplicity, if $x = (x_0, \dots, x_n)$ we will denote $[x] = [x_0, \dots, x_n]$ instead of $x = [(x_0, \dots, x_n)]$.

Definition 3.5. The n -dimensional projective space $\mathbb{P}_{\mathbb{C}}^n$ or $\mathbb{P}^n(\mathbb{C})$ or simply \mathbb{P}^n is defined as the quotient of W by \sim , that is

$$\mathbb{P}^n = \frac{W}{\sim} = \{[x] \mid x \in W = \mathbb{C}^{n+1} \setminus \{\underline{0}\}\}.$$

The coordinates of \mathbb{P}^n are $[x] \in \mathbb{P}^n$ except $[0, \dots, 0]$ and $[\lambda x_0, \dots, \lambda x_n] = [x_0, \dots, x_n]$ for $\lambda \in \mathbb{C}^*$. In other words, in \mathbb{P}^n , two points $[x_0, \dots, x_n]$ and $[y_0, \dots, y_n]$ are the same point if and only if there exists a non-zero constant λ such that

$$x_0 = \lambda y_0, \quad \dots, \quad x_n = \lambda y_n.$$

Exercise 8. Show that $[x] = [y]$ if and only if $x \sim y$. Show that if $y \notin [x]$ then $[x] \cap [y] = \emptyset$.

Example 3.6. The point $[1, 2, i]$ is the same as the point $[i, 2i, -1]$.

Exercise 9. Show that there exists a bijection between \mathbb{P}^n and the set of all the one-dimensional subspaces of \mathbb{C}^{n+1} . In fact, if V is a finite-dimensional vector space over \mathbb{C} without the choice of a basis, we can define the associated projective space $\mathbb{P}(V)$ as the set of one-dimensional linear subspaces of V .

Example 3.7. For any non-zero $x \in \mathbb{C}$ we have $[x] = [1]$. So $\mathbb{P}^0 = \mathbb{C}^1 \setminus \{0\} / \sim$ is a point $\mathbb{C}^0 = \{[1]\}$.

Notation 3.8. For any $i = 0, \dots, n$, denote the **affine chart**

$$U_i = \{[x] = [x_1, \dots, x_n] \in \mathbb{P}^n \mid x_i \neq 0\} \subseteq \mathbb{P}^n.$$

Lemma 3.9. $\mathbb{P}^n = U_0 \cup \dots \cup U_n$.

Proof. Take $[x] = [x_0, \dots, x_n] \in \mathbb{P}^n$ in \mathbb{P}^n then $x \in W$ and in particular $x = (x_0, \dots, x_n)$ where at least one of the coefficients is non-zero, say $x_i \neq 0$. Then $[x] \in U_i$. Thus any $[x] \in \mathbb{P}^n$ is contained in the union of U_0, \dots, U_n . \square

Lemma 3.10. Pick $i = 0, \dots, n$. Define $\phi_i : \mathbb{C}^n \rightarrow U_i$ by

$$\phi_i(y_1, \dots, y_n) = [y_1, \dots, y_i, 1, y_{i+1}, \dots, y_n].$$

Then ϕ_i is a bijection and its inverse $\rho_i : U_i \rightarrow \mathbb{C}^n$ is given by

$$\rho_i[x_0, \dots, x_n] = \left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i} \right).$$

Proof. First note that both ϕ_i and ρ_i is well-defined, indeed, if

$$(y_1, \dots, y_n) \in \mathbb{C}^n$$

then

$$(y_1, \dots, y_i, 1, y_{i+1}, \dots, y_n) \in W$$

and therefore $[y_1, \dots, y_i, 1, y_{i+1}, \dots, y_n] \in \mathbb{P}^n$. Similarly, if $[x_0, \dots, x_n] = [x'_0, \dots, x'_n]$ then it follows that $\rho_i[x_0, \dots, x_n] = \rho_i[x'_0, \dots, x'_n]$. Thus, it is enough to show that both $\phi_i \circ \rho_i$ and $\rho_i \circ \phi_i$ coincide with the identity. We have

$$\rho_i(\phi_i(y_1, \dots, y_n)) = \rho_i[y_1, \dots, y_i, 1, y_{i+1}, \dots, y_n] = \left(\frac{y_1}{1}, \dots, \frac{y_{i-1}}{1}, \frac{y_i}{1}, \dots, \frac{y_n}{1}\right) = (y_1, \dots, y_n).$$

Similarly,

$$\phi_i(\rho_i[x_0, \dots, x_n]) = \phi_i\left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i}\right) = \left[\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, 1, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i}\right] = [x_0, \dots, x_n].$$

Thus they are inverses. \square

Example 3.11. Let $n = 2$ and $[x_0, x_1, x_2] \in \mathbb{P}^2$. Let $\phi_1 : \mathbb{C}^2 \rightarrow U_1$ be defined by $(0, 0) \mapsto [0, 1, 0]$ and $\phi_2 : \mathbb{C}^2 \rightarrow U_2$ be defined by $(0, 0) \mapsto [0, 0, 1]$. Check that

$$\rho_i(\phi_i(y_1, \dots, y_n)) = \rho_i([y_1, \dots, 1, \dots, y_n]) = (y_1, \dots, y_n).$$

The previous two lemmas can be used to define a topology on \mathbb{P}^n . Let $U \subseteq \mathbb{P}^n$, then U is open if and only if $\phi_i^{-1}(U \cap U_i) \subseteq \mathbb{C}^n$ is open in $U_i \cong \mathbb{C}^n$ for any $i = 0, \dots, n$.

Exercise 10. Show that $U_i \subseteq \mathbb{P}^n$ is open in \mathbb{P}^n for all $i = 0, \dots, n$.

Exercise 11. We can define another topology on \mathbb{P}^n as the quotient topology induced by the map $\pi : W \rightarrow \mathbb{P}^n$ defined by $(x_0, \dots, x_n) \mapsto [x_0, \dots, x_n]$. A subset $U \subseteq \mathbb{P}^n$ is open if and only if its preimage $\pi^{-1}(U) \subseteq W$ is open in W . Show that this indeed defines a topology, and that this topology coincides with the one defined above using the maps ϕ_i . Check that with this topology on \mathbb{P}^n , π is continuous.

Exercise 12. Prove that \mathbb{P}^n is compact. Restrict the projection π of the previous exercise to the $(n+1)$ -dimensional sphere $S^{n+1} \subseteq W$, and check that this restriction is surjective and continuous. Since S^{n+1} is compact, it follows that \mathbb{P}^n is compact as well.

Example 3.12.

1. $\mathbb{P}^1 = \{[x_0, x_1] \mid (x_0, x_1) \in \mathbb{C}^2 \setminus \{0\}\}$ is the union of two copies U_0 and U_1 of \mathbb{C}^1 . The intersection of U_0 and U_1 is $U_0 \cap U_1 = \{[x_0, x_1] \mid x_0 \neq 0, x_1 \neq 0\}$ can be identified with $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ via the map $[x_0, x_1] \mapsto x_1/x_0$. Using this identification and the maps ρ_i , the inclusion $U_0 \cap U_1 \subseteq U_0$ is the map $\mathbb{C}^* \rightarrow \mathbb{C}^1$ sending z to itself, and the inclusion $U_0 \cap U_1 \subseteq U_1$ is the map $\mathbb{C}^* \rightarrow \mathbb{C}^1$ given by $z \mapsto 1/z$. \mathbb{P}^1 is glued together from two copies of \mathbb{C} along $U_0 \cap U_1$ by these inclusions, so $\mathbb{P}^1 = \mathbb{C}^1 \cup \{\infty\}$. Over the real numbers, $\mathbb{P}^1(\mathbb{R})$ is built up in the same way from two copies of \mathbb{R}^1 , and can be identified with the circle S^1 .
2. \mathbb{P}^2 is the union of three copies of $U_0 \cong U_1 \cong U_2 \cong \mathbb{C}^2$, and the intersection can be described similarly. At infinity we will have a line. More generally, \mathbb{P}^n can be described similarly.

In practice, we will view the affine complex plane \mathbb{C}^2 as being embedded in \mathbb{P}^2 as one of the open sets U_i . For example, we identify

$$(x, y) \in \mathbb{C}^2 \iff [x, y, 1] \in \mathbb{P}^2.$$

What is the complement of this embedding, that is the points at infinity?

Notation 3.13. For any $i = 0, \dots, n$, denote

$$\mathcal{P}_i = \{[x_0, \dots, x_n] \in \mathbb{P}^n \mid x_i = 0\} \subseteq \mathbb{P}^n.$$

Lemma 3.14. For any $i = 0, \dots, n$, we have

$$\mathbb{P}^n = U_i \sqcup \mathcal{P}_i.$$

Moreover if we define $f_i : \mathbb{P}^{n-1} \rightarrow \mathcal{P}_i$ by

$$f_i [z_0, \dots, z_{n-1}] \mapsto [z_0, \dots, z_{i-1}, 0, z_i, \dots, z_{n-1}]$$

then f_i is a bijection.

Proof. TODO Exercise: both statements are easy to check. □

In conclusion, we have that

$$\mathbb{P}^n = U_i \sqcup \mathcal{P}_i \cong \mathbb{C}^n \sqcup \mathbb{P}^{n-1} = \dots = \mathbb{C}^n \cup \dots \cup \mathbb{C}^0.$$

\mathcal{P}_i is called the **hyperplane at infinity**.

Example 3.15.

1. We have already seen that \mathbb{P}^0 is a point.
2. $\mathbb{P}^1 \cong \mathbb{C}^1 \cup \mathbb{P}^0$. In other words, \mathbb{P}^1 is obtained by adding a point at infinity to the complex line \mathbb{C} . It is a way to compactify the real plane. If \mathbb{C}^1 above is U_0 , this point at infinity is the origin of the other open subset $U_1 \cong \mathbb{C}^1$. One can show that there is an bijection which is also a homeomorphism between \mathbb{P}^1 and the sphere S^1 in \mathbb{R}^3 by the identification $r \mapsto 1/r$. \mathbb{P}^1 is called the projective line.
3. $\mathbb{P}^2 \cong \mathbb{C}^2 \cup \mathbb{P}^1$. Thus \mathbb{P}^2 is obtained by adding a projective line at infinity to the complex plane \mathbb{C}^2 . \mathbb{P}^2 is called the projective plane.

Note that the point at infinity or the line at infinity is not unique, it depends on the choice of the coordinate and in our settings, it depends on i . In the future, we will often fix i , and this will give us a unique choice of the point or line at infinity.

Lecture 5
Thursday
18/10/18

4 Projective curves

Recall that an algebraic curve $C \subseteq \mathbb{C}^2$ is given by $C = \{f(x, y) = 0\}$ for $f \in \mathbb{C}[x, y]$. In this section, we want to define projective curves similarly in \mathbb{P}^2 and then compactify these affine curves. If we try to define a plane projective curve in the same way as an affine curve, that is as $\{f = 0\} \subseteq \mathbb{P}^2$, where f is a polynomial in $\mathbb{C}[x_0, x_1, x_2]$, the first hurdle we encounter is that f does not define a function on \mathbb{P}^2 .

Example 4.1.

1. Let $f(x, y, z) = x^2 + y^2 - z^2$. Then $f(1, 1, 1) = 1 + 1 - 1 = 1 \neq 4 = 4 + 4 - 4 = f(2, 2, 2)$, so that f does not define a function on \mathbb{P}^2 . It makes no sense to talk about $f(1, 1, 1)$, because in \mathbb{P}^2 , $[1, 1, 1] = [2, 2, 2]$, so the value would not be well-defined. However, the locus where f vanishes in this case is well-defined. If $f(x, y, z) = 0$, then $f(\lambda x, \lambda y, \lambda z) = 0$ for all $\lambda \in \mathbb{C}^*$, so that the subset $\{[x, y, z] \in \mathbb{P}^2 \mid f(x, y, z) = 0\}$ is well-defined.
2. Let $g(x_0, x_1, x_2) = x_0^2 + x_1$, then $g(i, 1, 0) = 0$, but $g(2i, 2, 0) \neq 0$, so that in this case, the vanishing locus $\{[x_0, x_1, x_2] \in \mathbb{P}^2 \mid g(x_0, x_1, x_2) = 0\}$ is not even well-defined.

The example shows that if we want to define projective curves as

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

then $f \in \mathbb{C}[x_0, x_1, x_2]$ has to satisfy some additional properties.

Definition 4.2. A polynomial $f \in \mathbb{C}[x_0, \dots, x_n]$ is **homogeneous** if all its monomials have the same degree $d \in \mathbb{N}$, that is

$$f(x_0, \dots, x_n) = \sum_{|\alpha| = \sum_{i=0}^n \alpha_i = d} a_\alpha x^\alpha, \quad \alpha \in \mathbb{N}^{n+1}.$$

Example 4.3.

1. The polynomial $f(x, y, z) = x^2 + y^2 - z^2$ is homogeneous of degree two. The polynomial $g(x_0, x_1, x_2) = x_0^2 + x_1$ is not homogeneous.
2. $f(x, y) = Ax^3 + Bx^2y + Cxy^2 + Dy^3$ is homogeneous of degree three, and all the homogeneous polynomials of degree three in x, y can be written in this form.
3. $g(x, y, z) = x^4 - 2x^2yz + yz^3$ is homogeneous of degree four.

Lemma 4.4. Let $P \in \mathbb{C}[x_0, \dots, x_n]$ be a polynomial. If P is homogeneous of degree d , then

$$P(\lambda x_0, \dots, \lambda x_n) = \lambda^d P(x_0, \dots, x_n),$$

for all $\lambda \in \mathbb{C}$, and all $(x_0, \dots, x_n) \in \mathbb{C}^{n+1}$.

Proof. Let P be a homogeneous polynomial of degree d . Then $P = M_1 + \dots + M_k$, where each M_i is a monomial of degree d , that is a product $a_i \cdot x^{\alpha_i}$ where $\alpha_i \in \mathbb{N}^{n+1}$ and $a_i \in \mathbb{C}$. For each monomial $M = a_\alpha x^\alpha = a_\alpha x_0^{\alpha_0} \dots x_n^{\alpha_n}$ of degree d , for $a_\alpha \in \mathbb{C}$ and $\alpha \in \mathbb{N}^{n+1}$, we have

$$M(\lambda x_0, \dots, \lambda x_n) = a_\alpha (\lambda^{\alpha_0} x_0^{\alpha_0}) \dots (\lambda^{\alpha_n} x_n^{\alpha_n}) = \lambda^{\sum_{i=0}^n \alpha_i} a_\alpha x^\alpha = \lambda^d a_\alpha x^\alpha = \lambda^d M(x_0, \dots, x_n),$$

because $\sum_{i=0}^n \alpha_i = |\alpha| = d$. For the arbitrary homogeneous polynomial P , write $P = \sum_{i=1}^k M_i$. Thus

$$P(\lambda x_0, \dots, \lambda x_n) = \sum_{i=1}^k M_i(\lambda x_0, \dots, \lambda x_n) = \lambda^d \sum_{i=1}^k M_i(x_0, \dots, x_n) = \lambda^d P(x_0, \dots, x_n).$$

□

Exercise 13. Prove the converse implication for the previous lemma, that is if $P \in \mathbb{C}[x_0, \dots, x_n]$ and

$$P(\lambda x_0, \dots, \lambda x_n) = \lambda^d P(x_0, \dots, x_n),$$

for all $\lambda \in \mathbb{C}$, and all $(x_0, \dots, x_n) \in \mathbb{C}^{n+1}$, then P is homogeneous of degree d .

Proposition 4.5. Let P be a homogeneous polynomial. Then

$$\{[x_0, \dots, x_n] \in \mathbb{P}^n \mid P(x_0, \dots, x_n) = 0\}$$

is well-defined.

Proof. We have to check that if $(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$, $P(x_0, \dots, x_n) = 0$ if and only if $P(y_0, \dots, y_n) = 0$. This follows immediately from Lemma 4.4, because by definition of \sim , $(y_0, \dots, y_n) = (\lambda x_0, \dots, \lambda x_n)$ for some $\lambda \in \mathbb{C}^*$, so $P(x_0, \dots, x_n) = 0$ if and only if $P(\lambda x_0, \dots, \lambda x_n) = \lambda^d P(x_0, \dots, x_n) = 0$. □

Notation 4.6. Unless mentioned otherwise, arbitrary polynomials will be denoted f, g, h, \dots while homogeneous polynomials will be denoted P, Q, R, \dots

Let $P_1, \dots, P_k \in \mathbb{C}[x_0, \dots, x_n]$ be homogeneous polynomials. Then the vanishing locus

$$\{P_1 = \dots = P_k = 0\} \subseteq \mathbb{P}^n$$

is a **projective variety**. These are the main object of study of algebraic geometry. In this class, we will focus on plane projective curves.

Definition 4.7. A complex projective plane algebraic curve is

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

where P is a non-constant homogeneous polynomial $P \in \mathbb{C}[x_0, x_1, x_2]$.

From now on $n = 2$, so consider \mathbb{P}^2 .

Example 4.8. The hyperplanes at infinity $\mathcal{P}_i = \{x_i = 0\} \subseteq \mathbb{P}^2$ for $i = 0, 1, 2$ are projective curves of degree one, where x_0 is a homogeneous polynomial of degree one.

Definition 4.9. A **projective line** is a projective curve defined by a homogeneous polynomial $ax_0 + bx_1 + cx_2 = 0$ of degree one.

We have seen that in the case of affine plane curves $\{f = 0\} \subseteq \mathbb{C}^2$, the irreducible factors of the polynomial f were important when studying curves. The next lemma ensures that the same type of results hold for projective curves.

Lemma 4.10. Let $P \in K[x_0, \dots, x_n]$ be a non-zero homogeneous polynomial. Assume that $P = Q \cdot R$, where $Q, R \in K[x_0, \dots, x_n]$. Then the polynomials Q and R are homogeneous.

Proof. TODO Exercise. □

Remark 4.11. As in the case of affine plane curves, we can therefore make sense of irreducible projective plane curves $C = \{P = 0\} \subset \mathbb{P}^2$ with P irreducible. When P is reducible $P = P_1^{a_1} \dots P_k^{a_k}$ with P_i distinct irreducible polynomials and $a_i \in \mathbb{N}_{>0}$, the projective curves $C_i = \{P_i = 0\}$ in $\{P = 0\} = \{P_1 = 0\} \cup \dots \cup \{P_k = 0\}$ are called the **irreducible components** of $C = \{P = 0\}$.

Remark 4.12. Hilbert's Nullstellensatz, and Theorem 2.9, still holds. In particular, if $P, Q \in \mathbb{C}[x, y, z]$ are homogeneous polynomials with no repeated factors, $\{P = 0\} = \{Q = 0\} \subseteq \mathbb{P}^2$ if and only if $P = \lambda Q$ for $\lambda \in \mathbb{C}^*$.

Definition 4.13. Let $C \subseteq \mathbb{P}^2$ be a projective plane curve and P any homogeneous polynomial with no repeated factor such that $C = \{P = 0\} \subseteq \mathbb{P}^2$. The degree of C is the degree of P .

Exercise 14. Show that the union of two projective curves $C_1, C_2 \subseteq \mathbb{P}^2$ is a projective curve. More generally, show that if $X_1, X_2 \subseteq \mathbb{P}^n$ are projective varieties, then $X_1 \cup X_2 \subseteq \mathbb{P}^n$ is again a projective variety.

Exercise 15. Show that if $X = \{P = 0\} \subseteq \mathbb{P}^n$ for a non-zero homogeneous polynomial $P \in \mathbb{C}[x_0, \dots, x_n]$, then

$$X = \{x_0 P = \dots = x_n P = 0\}.$$

Lemma 4.14. Let $C \subseteq \mathbb{P}^2$ be a projective curve. Then C is compact.

Recall that affine curves are never compact.

Proof. Recall that a closed subset of a compact is compact itself. Since \mathbb{P}^2 is compact by Exercise 12, we only need to prove that C is closed, or equivalently, that $\pi^{-1}(C) \subseteq W = \mathbb{C}^3 \setminus \{0\}$ is closed, where $\pi : W \rightarrow W/\sim = \mathbb{P}^2$ by $(x_0, x_1, x_2) \mapsto (x_0, x_1, x_2)$, by Remark 2.17. Assume that $C = \{P = 0\}$ for a homogeneous polynomial P . Then, $P : W \rightarrow \mathbb{C}$ is a continuous map, so that $\pi^{-1}(C) = P^{-1}(\{0\}) = \{P(x_0, x_1, x_2) = 0\} \cap W$ is a closed subset of W . □

Remark 4.15. You may have heard of the Zariski topology for algebraic varieties. The Zariski topology is defined on affine space \mathbb{C}^n or on projective space \mathbb{P}^n as the topology whose closed sets are of the form $V(S) = \{\underline{x} \in \mathbb{C}^n \mid f(\underline{x}) = 0\}$ where S is a set of polynomials or homogeneous polynomials $f \in \mathbb{C}[x_0, \dots, x_n]$. In this course, we do not work in the Zariski topology, but in the classical metric or Euclidean topology on \mathbb{C}^{n+1} and in the topology this induces on \mathbb{P}^n as outlined above. One reason for that is that the Zariski topology is not Hausdorff, or separated.

Lecture 6 is a problem class.

5 Affine vs projective plane curves

We now show how to projectivise affine curves, and study the relationship between affine and projective curves.

Notation 5.1. We will typically use coordinates x, y on \mathbb{C}^2 and x_0, x_1, x_2 on \mathbb{P}^2 .

Starting with an affine curve $C = \{f = 0\} \subseteq \mathbb{C}^2$ for $f \in \mathbb{C}[x, y]$ non-constant, want to construct a projective curve $\overline{C} \subseteq \mathbb{P}^2$, a projectivisation of C . Recall that we have identified \mathbb{C}^2 with the open subset $U_2 = \{x_2 \neq 0\} \subseteq \mathbb{P}^2$, via the function $\phi : U_2 \rightarrow \mathbb{C}^2$ defined by $[x_0, x_1, x_2] \mapsto (x_0/x_2, x_1/x_2)$ and its inverse $(x, y) \mapsto [x, y, 1]$. We now want to identify $U_2 \cap \overline{C} \subseteq \mathbb{C}^2$ with the original curve C for a suitable projective plane curve $\overline{C} = \{P = 0\} \subseteq \mathbb{P}^2$ for P homogeneous, picking $\mathbb{C}^2 \cong U_2 \subseteq \mathbb{P}^2$ to be the points not at infinity.

Example 5.2. Idea is to let $x = x_0/x_2$ and $y = x_1/x_2$. $f(x, y) = x^3 + y + 1 = (x_0/x_2)^3 + (x_1/x_2) + 1$ and clear denominators to get $P(x_0, x_1, x_2) = x_0^3 + x_1x_2^2 + x_2^3$, homogeneous of degree three. Check that restricting P to $U_2 \cong \mathbb{C}^2$ I get back f . Restricting P to $U_2 \cong \mathbb{C}^2$ gives $P(x, y, 1) = x^3 + y + 1$. $\{P = 0\} = \overline{C}$ is the projectivisation of $\{f = 0\} = C$.

Theorem 5.3. There is a bijective correspondence between

1. projective plane curves $\overline{C} = \{P = 0\} \subseteq \mathbb{P}^2$ that do not contain the line at infinity $\mathcal{P}_2 = \{x_2 = 0\}$, and
2. affine curves $C = \{f = 0\} \subseteq \mathbb{C}^2$.

The bijection $C \leftrightarrow \overline{C}$ is obtained by

$$P \mapsto [f : (x, y) \mapsto P(x, y, 1)], \quad f \mapsto [P : (x_0, x_1, x_2) \mapsto x_2^d \cdot f(x_0/x_2, x_1/x_2)],$$

for $d = \deg(f)$. The affine curve $\{f = 0\} \subseteq \mathbb{C}^2$ is $\phi(U \cap \overline{C})$, where $\overline{C} = \{P = 0\}$.

Notation 5.4. In general, P is called the **homogenisation** of the polynomial f . \overline{C} is the **projectivisation** of C .

Proof. Let $\overline{C} = \{P = 0\} \subseteq \mathbb{P}^2$ be a projective curve that does not contain $\{x_2 = 0\}$ as in the statement. $\{x_2 = 0\}$ is not contained in \overline{C} if and only if P contains at least one monomial without x_2 . Then P contains at least one monomial without x_2 , so that $f : (x, y) \mapsto P(x, y, 1)$ is a polynomial in x, y . If not, $P = x_2 \cdot Q$ and $\{P = 0\} = \{x_2 = 0\} \cup \{Q = 0\}$. So $f(x, y)$ has degree equal to $d = \deg(P)$. Under the identification $\phi : U \rightarrow \mathbb{C}^2$ defined in the previous section,

$$\phi(U \cap \overline{C}) = \{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0\}.$$

Conversely, if $C = \{f = 0\}$, then C is the image by ϕ of the intersection of U and \overline{C} , where $\overline{C} = \{P = 0\}$, where the polynomial P is defined by $P(x_0, x_1, x_2) = x_2^d \cdot f(x_0/x_2, x_1/x_2)$. Check that P is a well-defined homogeneous polynomial of degree d . \square

Look at an example where \overline{C} does contain $\{x_2 = 0\}$.

Example 5.5. Let $P = x_0x_2^2 + x_1^2x_2 = x_2(x_0x_2 + x_1^2)$. Then $f(x, y) = P(x, y, 1) = x + y^2$, so

$$P(x_0, x_1, x_2) = \left(x_0/x_2 + (x_1/x_2)^2\right) x_2^2 = x_0x_2 + x_1^2.$$

Remark 5.6. To intersect $\{P = 0\}$ and $\{Q = 0\}$ in \mathbb{P}^2 , solve $P = 0$ and $Q = 0$ in x_0, x_1, x_2 to get homogeneous coordinates of points of intersection, where $\underline{0}$ is not a valid solution and $(\lambda x_0, \lambda x_1, \lambda x_2)$ is the same as (x_0, x_1, x_2) .

Example 5.7.

1. Let \overline{C} be the projective curve $\overline{C} = \{P(x_0, x_1, x_2) = x_0^2 + x_1^2 + x_2^2 = 0\}$. Then $C = \phi(\overline{C} \cap U_2)$ is $\{f = 0\} \subseteq \mathbb{C}^2$, where $f(x, y) = x^2 + y^2 + 1$.

2. Let C be the affine curve $x^2y + y - 1 = 0$. Then \overline{C} is defined by $x_2^3 \left((x_0/x_2)^2 (x_1/x_2) + x_1/x_2 - 1 \right) = x_0^2x_1 + x_1x_2^2 - x_2^3$.

Exercise 16. Let $i = 1$ or 2 , recall that ϕ_i denotes the homeomorphism $\phi : U_i \rightarrow \mathbb{C}^2$. Show that if $\overline{C} \subseteq \mathbb{P}^2$ is a projective curve that does not contain $\mathcal{P}_i = \{x_i = 0\}$, then

$$C_i = \phi_i(\overline{C} \cap U_i) \subseteq \mathbb{C}^2$$

is an affine curve.

Intersect projectivisations to find points of intersection at infinity.

Example 5.8.

1. Consider the parallel lines

$$L_1 = \{x + y + 1 = 0\}, \quad L_2 = \{x + y - 1 = 0\}.$$

The corresponding projective lines are given by

$$\overline{L}_1 = \{x_0 + x_1 + x_2 = 0\}, \quad \overline{L}_2 = \{x_0 + x_1 - x_2 = 0\},$$

then solve to give

$$\begin{cases} x_0 + x_1 = -x_2 \\ x_0 + x_1 = x_2 \end{cases} \implies \begin{cases} x_0 + x_1 = 0 \\ x_2 = 0 \end{cases}.$$

Inside \mathbb{P}^2 , the intersection $L_1 \cap L_2$ consists of exactly one point

$$p = [1, -1, 0].$$

Thus, the two projective lines meet at one point $p \in \mathcal{P}_0$, that is p is a point at infinity.

2. Similarly, let

$$C = \{xy - 1 = 0\}, \quad L = \{x = 0\},$$

then the projectivisations are

$$\overline{C} = \{x_0 \cdot x_1 - x_2^2 = 0\}, \quad \overline{L} = \{x_0 = 0\},$$

then intersect to give

$$\begin{cases} x_0 = 0 \\ x_0x_1 - x_2^2 = 0 \end{cases} \implies \begin{cases} x_0 = 0 \\ x_2 = 0 \end{cases}.$$

As above, in \mathbb{P}^2 , $\overline{C} \cap \overline{L}$ consists of a single point

$$\{[0, 1, 0]\}$$

lying on $\mathcal{P}_2 = \{x_2 = 0\}$, the hyperplane at infinity.

Example 5.9. Projective conics over \mathbb{R} are defined by degree two equations. In \mathbb{R}^2 , smooth conics are three kinds, ellipses, hyperbolas, and parabolas. Passing to $\mathbb{P}^2(\mathbb{R})$, these three kinds of curves become the same. Ellipses have no new points at infinity, hyperbolas have two new points at infinity, and parabolas have one new point at infinity.

1. Let $f(x, y) = x^2 - y^2 + 1$. Projectivising, $P(x_0, x_1, x_2) = x_0^2 - x_1^2 + x_2^2$. Restrict to $U_1 = \{x_1 \neq 0\} \subseteq \mathbb{R}^2$. $\overline{C} \cap U_1$, the equation of the unit circle $g(x, y) = x^2 - 1 + y^2 = x^2 + y^2 - 1$ is obtained by setting $x_1 = 1$.
2. Consider the parabola C with equation $y = x^2$ in \mathbb{R}^2 . Projectivising, this becomes the curve $\overline{C} = \{x_1x_2 = x_0^2\} \subseteq \mathbb{P}^2(\mathbb{R})$. The intersection with the line at infinity $x_2 = 0$ gives $x_0^2 = 0$, so the only point is $[0, 1, 0]$. The square suggests some kind of tangency, and indeed \overline{C} is tangent to $x_2 = 0$. In the chart $x_0 \neq 0$, the equation becomes $xy = 1$, and we see a hyperbola. In the chart $x_1 \neq 0$ we have again a parabola, $y = x^2$.

3. Consider the unit circle $C = \{x^2 + y^2 - 1 = 0\} \subseteq \mathbb{R}^2$. Projectivising we obtain $\overline{C} = \{x_0^2 + x_1^2 = x_2^2\} \subseteq \mathbb{P}^2(\mathbb{R})$. The intersection with the line at infinity $x_2 = 0$ is empty as we could expect. In the chart $x_0 \neq 0$ we obtain the curve $1 + x^2 - y^2 = 0$, which is a hyperbola, and similarly in $x_1 \neq 0$.

Exercise 17. Let $a, b, c, d, e, f \in \mathbb{C}$, with $(a, b, c) \neq (0, 0, 0)$, and define

$$C = \{ax^2 + bxy + cy^2 + dx + ey + f = 0\}.$$

Define the projectivisation \overline{C} of C and determine its points on the line at infinity.

Exercise 18.

1. Show that there exists a unique projective line $L \subseteq \mathbb{P}^2$ through two distinct points $P, Q \in \mathbb{P}^2$.
2. Show that two distinct projective lines in \mathbb{P}^2 meet in exactly one point.

Exercise 19. Let P_1, P_2, P_3 be three points of \mathbb{P}^2 , and denote

$$P_i = [b_{i,1}, b_{i,2}, b_{i,3}], \quad i = 1, 2, 3$$

for their coordinates. Let $B = (b_{i,j})$ be the associated 3×3 matrix. Show that P_1, P_2, P_3 lie in the same projective line if and only if $\det(B) = 0$.

6 Points at infinity

Given an affine curve $C \subseteq \mathbb{C}^2$ and its projectivisation $\overline{C} \subseteq \mathbb{P}^2$, we study the points at infinity of C , that is the points of \overline{C} that do not lie on C . Let us first recall the notation in use. Denote by U_2 the open set of \mathbb{P}^2 defined by $\mathbb{C}^2 \cong U_2 = \{x_2 \neq 0\} \subseteq \mathbb{P}^2$ and let $\mathcal{P}_2 = \mathbb{P}^2 \setminus U_2 = \{x_2 = 0\}$ be the corresponding hyperplane or line at infinity. The homeomorphism $\phi : \mathbb{C}^2 \rightarrow U_2$ is defined by $(x, y) \mapsto [x, y, 1]$, and its inverse $\psi : U_2 \rightarrow \mathbb{C}^2$ is the map $\psi : [x_0, x_1, x_2] \mapsto [x_0/x_2, x_1/x_2]$. Let C be the affine curve

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

where $f \in \mathbb{C}[x, y]$ is a polynomial of degree d with no repeated factors. The projectivisation of C is then the curve \overline{C} such that $\overline{C} \cap \{x_2 \neq 0\} = \phi(C)$, or equivalently such that $\psi(\overline{C} \cap U_2) = C$. The curve \overline{C} is

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

where P is the homogeneous polynomial

$$P(x_0, x_1, x_2) = x_2^d f(x_0/x_2, x_1/x_2).$$

Let $f_i \in \mathbb{C}[x, y]$ be the homogeneous polynomials of degree $0 \leq i \leq d$ with

$$f(x, y) = f_0(x, y) + \cdots + f_d(x, y),$$

and note that

$$P(x_0, x_1, x_2) = f_0(x_0, x_1)x_2^d + \cdots + f_d(x_0, x_1).$$

Definition 6.1. The **points at infinity** of C are the points on $\overline{C} \setminus \phi(C)$. We will often just write $\overline{C} \setminus C$.

How many points at infinity can there be? If $\{x_2 = 0\} \subseteq \overline{C}$, if and only if x_2 divides $P(x_0, x_1, x_2)$, then there are infinitely many. Assume $\{x_2 = 0\} \not\subseteq \overline{C}$. Look at $P(x_0, x_1, 0)$, and find solutions of $P(x_0, x_1, 0) = 0$ in $\mathbb{P}^1 \cong \mathcal{P}_2$. The points at infinity of C are thus

$$\overline{C} \setminus C = \overline{C} \cap \mathcal{P}_2 = \{[x_0, x_1, 0] \in \mathbb{P}^2 \mid P(x_0, x_1, 0) = 0\}.$$

From the above equation, and under the identification $\mathcal{P}_2 \cong \mathbb{P}^1$, this becomes

$$\overline{C} \setminus C = \{[x_0, x_1] \in \mathbb{P}^1 \mid f_d(x_0, x_1) = 0\},$$

that is a projective variety in $\mathcal{P}_2 \cong \mathbb{P}^1$. It is natural to expect that such a projective variety consists of a finite number of points. This is what we will prove next.

Lemma 6.2. Let $Q \in \mathbb{C}[x_0, x_1]$ be a non-zero homogeneous polynomial of degree $d \geq 1$. Then there exist $\alpha_i, \beta_i \in \mathbb{C}$ with $(\alpha_i, \beta_i) \neq (0, 0)$ for $i = 1, \dots, d$ such that

$$Q(x_0, x_1) = \prod_{i=1}^d (\alpha_i x_0 + \beta_i x_1).$$

Therefore, $\{[x_0, x_1] \in \mathbb{P}^1 \mid Q(x_0, x_1) = 0\} = \{P_i = [-\beta_i, \alpha_i]\} \subseteq \mathbb{P}^1$. Note that the P_i need not be distinct.

Proof. Let us pass to $U_1 \cong \mathbb{C}^1 \subseteq \mathbb{P}^1$, one of the two affine charts. Write $Q(x_0, x_1) = \sum_{r=0}^d a_r x_0^r x_1^{d-r}$ and let $e = \max\{r \mid a_r \neq 0\}$ so

$$Q(x_0, x_1) = x_1^d \cdot \sum_{r=0}^e a_r \left(\frac{x_0}{x_1}\right)^r.$$

Define $f \in \mathbb{C}[x]$ as $f(x) = \sum_{r=0}^e a_r x^r$. By the fundamental theorem of algebra, there are $\lambda_1, \dots, \lambda_e \in \mathbb{C}$ such that

$$f(x) = a_e \cdot \prod_{i=1}^e (x - \lambda_i),$$

where λ_i are the roots of f , and hence

$$Q(x_0, x_1) = x_1^d \cdot a_e \cdot \prod_{i=1}^e \left(\frac{x_0}{x_1} - \lambda_i\right) = a_e \cdot x_1^{d-e} \cdot \prod_{i=1}^e (x_0 - \lambda_i x_1).$$

This proves the lemma, if we set

$$(\alpha_i, \beta_i) = \begin{cases} (1, -\lambda_i) & i \leq e \\ (0, a_e) & i = e+1 \\ (0, 1) & i > e+1 \end{cases}.$$

If $e = d$, then set

$$(\alpha_i, \beta_i) = \begin{cases} (1, -\lambda_i) & i < e \\ (a_e, -a_e \lambda_e) & i = e \end{cases}.$$

The description that $\{Q = 0\} \subseteq \mathbb{P}^1$ is clear, once we note that $(\alpha_i, \beta_i) \neq (0, 0)$. □

We have proved the following.

Theorem 6.3. Let $\overline{C} \subseteq \mathbb{P}^2$ be a projective curve defined by a polynomial of degree d that does not contain \mathcal{P} . Then $\overline{C} \cap \mathcal{P}$ is a non-empty set of at most $d = \deg(Q)$ points.

Definition 6.4. Let $C = \{f = 0\} \subseteq \mathbb{C}^2$ for $f \in \mathbb{C}[x, y]$ be an affine curve of degree d and let \overline{C} be its projectivisation, where, as usual, $C = \psi(\overline{C} \cap U)$. Denote

$$f = f_d + \dots + f_0, \quad \deg f_i = i, \quad f_d \neq 0,$$

the decomposition of f into its homogeneous polynomial parts, so that

$$P(x_0, x_1, x_2) = f_d(x_0, x_1) + \dots + f_0(x_0, x_1) x_2^d = \sum_{i=0}^d x_2^{d-i} f_i(x_0, x_1).$$

Then, if $(\alpha_i, \beta_i) \in \mathbb{C}^2 \setminus \{0\}$ for $i = 1, \dots, d$ are such that

$$f_d(x_0, x_1) = \prod_{i=1}^d (\alpha_i x_0 + \beta_i x_1),$$

the affine lines $\{\alpha_i x + \beta_i y = 0\} \subseteq \mathbb{C}^2$ are the **asymptotes** of C . The points at infinity at $x_2 = 0$ of C depend on the equation $f_d(x_0, x_1) = 0$ and are

$$\overline{C} \setminus C = \{[-\beta_i, \alpha_i]\} \subseteq \mathcal{P}.$$

Each asymptote meets \overline{C} at the point $[-\beta_i, \alpha_i] \in \mathbb{P}^1$, the line at infinity. (TODO Exercise: check this)

Remark 6.5. It is clear from Lemma 6.2 that asymptotes are well-defined. Note that the asymptotes are lines in \mathbb{C}^2 because $(\alpha_i, \beta_i) \neq (0, 0)$.

Example 6.6. Consider the affine curve

$$C = \{(x, y) \in \mathbb{C}^2 \mid x^2 + y^2 - 1 = 0\}.$$

The projectivisation of C is

$$\overline{C} = \{[x_0, x_1, x_2] \in \mathbb{P}^2 \mid x_0^2 + x_1^2 - x_2^2 = 0\}.$$

so that the points at infinity of C are given by

$$\overline{C} \setminus C = \{[x_0, x_1, 0] \in \mathbb{P}^2 \mid x_0^2 + x_1^2 = 0\}.$$

This shows that C has two asymptotes, namely $L_{\pm} = \{x \pm iy = 0\}$, and two points at infinity $\{[\pm i, 1, 0]\}$.

Exercise 20. Find the asymptotes of the affine curve given by the equation $x^2y + y^3 + xy + x + 1 = 0$.

Exercise 21. Write an example of an affine curve whose asymptotes include the lines $x + 2y = 0$, $4x - 3y = 0$, and $7x + 9y = 0$.

Lecture 8
Thursday
25/10/18

7 Smoothness and singularities

Let $C \subseteq \mathbb{C}^2, \mathbb{P}^2$ be an affine or projective algebraic curve. Topologically, C is a two-dimensional object.

Example 7.1. A line $C \subseteq \mathbb{C}^2$ is a real plane $\mathbb{C} \cong \mathbb{R}^2$. $\mathbb{P}^1 \cong S^2$ is a two-dimensional sphere.

Smooth or nonsingular points of C are points where you do not have angles, pinches, etc.

Example 7.2. The union of two projective lines \mathbb{P}^1 in \mathbb{P}^2 has a non-smooth point. A pinched torus has a non-smooth point.

Idea is that can make sense of the tangent line at smooth points.

Notation 7.3. Given a function $f(x_1, \dots, x_n)$, we will denote by f_{x_i} or $\partial_{x_i} f$ the partial derivative of f with respect to x_i .

Let $C = \{f = 0\} \subseteq \mathbb{C}^2$ be an affine algebraic curve for $f \in \mathbb{C}[x, y]$ and let $(a, b) \in C$. Then the **tangent line** of C at the point $(a, b) \in C$ is the line defined by the equation

$$f_x(a, b)(x - a) + f_y(a, b)(y - b) = 0.$$

Note that this equation defines a complex line if and only if either $f_x(a, b)$ or $f_y(a, b)$ or both is not zero.

Definition 7.4. The affine curve C is **smooth** at a point $(a, b) \in C$ if at least one of $f_x(a, b)$ and $f_y(a, b)$ is not zero, so that the above equation defines a line in \mathbb{C}^2 . On the other hand if $f_x(a, b) = f_y(a, b) = 0$, then (a, b) is called a **singular** point of C . We will simply say that C is smooth if C is smooth at every point.

Example 7.5.

1. Any line in \mathbb{C}^2 is smooth.
2. $x^2 + y^2 + 1 = 0$ is smooth.
3. $y^2 - x^2(x + 1) = 0$ is singular at one point, a node.
4. $y^2 - x^3 = 0$ is singular at one point, a cusp.

What about projective curves?

Theorem 7.6 (Euler relation). Let $P \in \mathbb{C}[x_0, x_1, x_2]$ be a homogeneous polynomial of degree d . Then the following relation holds at each point $[x_0, x_1, x_2] \in \mathbb{P}^2$.

$$x_0 \cdot P_{x_0} + x_1 \cdot P_{x_1} + x_2 \cdot P_{x_2} = d \cdot P.$$

Example 7.7. Let $P(x_0, x_1, x_2) = x_0^2 + x_1^2 + x_2^2$.

$$P_{x_0} = 2x_0, \quad P_{x_1} = 2x_1, \quad P_{x_2} = 2x_2 \quad \implies \quad x_0 \cdot P_{x_0} + x_1 \cdot P_{x_1} + x_2 \cdot P_{x_2} = 2(x_0^2 + x_1^2 + x_2^2) = d \cdot P.$$

Proof. By Lemma 4.4, for any $\lambda \in \mathbb{C}$ we have

$$P(\lambda x_0, \lambda x_1, \lambda x_2) = \lambda^d \cdot P(x_0, x_1, x_2).$$

We now compute the derivative with respect to λ of both sides of this equation,

$$\partial_\lambda (\lambda^d \cdot P(x_0, x_1, x_2)) = d\lambda^{d-1} P(x_0, x_1, x_2), \quad \partial_\lambda (P(\lambda x_0, \lambda x_1, \lambda x_2)) = \sum_{i=0}^2 x_i P_{x_i}(\lambda x_0, \lambda x_1, \lambda x_2).$$

By the equality above we have

$$\sum_{i=0}^2 x_i P_{x_i}(\lambda x_0, \lambda x_1, \lambda x_2) = d\lambda^{d-1} P(x_0, x_1, x_2),$$

for all $\lambda \in \mathbb{C}$. Thus, if we plug in $\lambda = 1$, we get the claim. \square

Definition 7.8. If a point $p = [z_0, z_1, z_2]$ of a projective curve $C = \{P = 0\} \subseteq \mathbb{P}^2$ for $P \in \mathbb{C}[x_0, x_1, x_2]$ homogeneous satisfies

$$P_{x_i}(z_0, z_1, z_2) = 0, \quad i = 0, 1, 2,$$

then we will say that C is singular at p . C is smooth at p if it is not singular. C is said to be smooth if it does not admit any singular point, so it is smooth at every point.

Lemma 7.9. Let $C = \{P = 0\}$ be a projective curve for $\mathbb{C}^2 \cong U_2 \subseteq \mathbb{P}^2$ which does not contain the line $\{x_2 = 0\}$ and let $C_0 = \{f = 0\} \subseteq \mathbb{C}^2$ be the associated affine curve, where $f(x, y) = P(x, y, 1)$. Then (a, b) is a singular point of C_0 if and only if $[a, b, 1]$ is a singular point of C .

Proof. If $(a, b) \in C_0$ is a singular point of C_0 , it is a singular point for C . Note that $P(x, y, 1) = f(x, y)$ by construction, so $P_{x_0}(x, y, 1) = f_x(x, y)$, $P_{x_1}(x, y, 1) = f_y(x, y)$. Then, since $f(a, b) = 0$ we have

$$P(a, b, 1) = 0.$$

Since $f_x(a, b) = f_y(a, b) = 0$, we have

$$P_{x_0}(a, b, 1) = P_{x_1}(a, b, 1) = 0.$$

Finally by Theorem 7.6, we have

$$P_{x_2}(a, b, 1) = x_0 \cdot P_{x_0}(a, b, 1) + x_1 \cdot P_{x_1}(a, b, 1) + x_2 \cdot P_{x_2}(a, b, 1) = dP(a, b, 1) = 0,$$

since everything is zero except $P_{x_2}(a, b, 1)$. Thus, we have

$$P_{x_i}(a, b, 1) = 0, \quad i = 0, 1, 2.$$

The converse implication is similar. \square

Exercise 22. Show that

1. $C = \{x_0^2 + x_1^2 + x_2^2 = 0\}$ is smooth,
2. $C = \{x_1^2 x_0^2 - x_2^3 = 0\}$ is singular at the point $[1, 0, 0]$, and

3. any projective line is smooth.

Definition 7.10. Let $p = [z_0, z_1, z_2]$ be a smooth point of the projective curve $C = \{P = 0\}$. The **projective tangent line** of the curve $C = \{P = 0\}$ at the point p is given by the equation

$$\sum_{i=0}^2 P_{x_i}(z_1, z_2, z_3) \cdot x_i = 0.$$

Note that the line is well-defined since the curve C is smooth at the point p .

Proposition 7.11. Let $C \subseteq \mathbb{P}^2$ be a projective algebraic curve not containing the line $\{x_2 = 0\}$. Then the affine line in U_2 associated to the projective tangent line at $[a, b, 1] \in C$ is the tangent line at (a, b) of the affine curve C_0 associated to C in U_2 , for (a, b) a smooth point in C_0 .

Equivalently, the projectivisation of the tangent line to $C_0 \subseteq \mathbb{C}^2$ at $(a, b) \in C_0$ is the projective tangent line to the projectivisation C of C_0 at $[a, b, 1]$.

Proof. Assume $C = \{P = 0\} \subseteq \mathbb{P}^2$ does not contain the line $\{x_2 = 0\}$. Let $f(x, y) = P(x, y, 1)$ and let $C_0 = \{f = 0\}$. The affine line associated to the projective tangent line of C at the point $(a, b) \in C_0$ is given by the equation

$$P_{x_0}(a, b, 1) \cdot x_0 + P_{x_1}(a, b, 1) \cdot x_1 + P_{x_2}(a, b, 1) \cdot x_2 = 0.$$

Since $P(a, b, 1) = 0$, by Theorem 7.6 we have

$$P_{x_2}(a, b, 1) = -a \cdot P_{x_0}(a, b, 1) - b \cdot P_{x_1}(a, b, 1).$$

Moreover, as above we have $f_x(a, b) = P_{x_0}(a, b, 1)$ and $f_y(a, b) = P_{x_1}(a, b, 1)$. Combining everything together we get

$$f_x(a, b)(x - a) + f_y(a, b)(y - b) = 0,$$

which is the equation of the tangent line of C_0 at (a, b) . \square

Theorem 7.12. Let C be a smooth projective curve. Then C is irreducible.

Assume that any two projective curves in \mathbb{P}^2 intersect in at least one point, so there exists $p \in C_1 \cap C_2$. Later on we will prove this.

Proof. Suppose not. Then $\{P = 0\} = C = C_1 \cup C_2$ where $C_i = \{P_i = 0\}$ is a projective curve for $i = 1, 2$. In particular, $C = \{P = Q \cdot R = 0\}$, where Q and R defines C_1 and C_2 respectively. We want to show that $A = \{a, b, c\} \in C_1 \cap C_2 \neq \emptyset$ is a singular point for C , which contradicts the assumption on C . We have

$$P_{x_i}(A) = (Q \cdot R)_{x_i}(A) = Q(A) \cdot R_{x_i}(A) + R(A) \cdot Q_{x_i}(A) = 0, \quad i = 1, 2.$$

The last equality follows from the fact that $Q(A) = R(A) = 0$. Thus C is singular at A as claimed, a contradiction. \square

Example 7.13. Example of a reducible curve, where the two pieces have the same tangent line where they intersect. $C_1 = \{y - x^2\}$ and $C_2 = \{y + x^2\}$ has $(0, 0)$ as the only point of intersection. Tangent line at $(0, 0)$ to both C_1 and C_2 is $y = 0$. The definition gives that $C = C_1 \cup C_2 = \{(y - x^2)(y + x^2) = 0\} = \{y^2 - x^4 = 0\}$ is not smooth at $(0, 0)$. Note that the tangent line at $(0, 0) \in C$ for some affine curve C is given by the linear part of $f = 0$ where $\{f = 0\} = C$. Equation $f_x(0, 0)(x - 0) + f_y(0, 0)(y - 0) = 0$ is a linear approximation of C around $(0, 0)$. Now $y^2 - x^4 = 0$ does not have a linear part. The best possible approximation is a double line $y^2 = 0$, the term of lowest degree of f . Thus $(0, 0) \in \{y^2 - x^4 = 0\}$ should not be a smooth point.

Remark 7.14. When talking about smoothness, take f for $C = \{f = 0\}$ without repeated factors. Otherwise if $f = g^2 \cdot h$ for g non-constant, then $\{f = 0\}$ would be singular along $\{g = 0\}$. We do not want this.

Lecture 9
Friday
26/10/18

Theorem 7.15. Let C be an irreducible projective curve of degree d . Then the number of singular points of C is at most

$$d \cdot (d - 1).$$

In particular it is finite.

We will prove this later on, after seeing some results on intersections of curves.

Exercise 23. For which values of $\lambda \in \mathbb{C}$ does the algebraic curve

$$y^2 - x(x-1)(x-\lambda) = 0$$

admit at least one singular point? For each of those values of λ , what are the singular points?

8 Projective transformations

How do we move around points or change coordinates in \mathbb{P}^n ? In linear algebra, that is in \mathbb{C}^n , we do that with linear maps $L : \mathbb{C}^n \rightarrow \mathbb{C}^n$, that is functions such that $L(\lambda v + \mu w) = \lambda L(v) + \mu L(w)$ for all $v, w \in \mathbb{C}^n$ and $\lambda, \mu \in \mathbb{C}$. These correspond to $n \times n$ matrices $A = (a_{ij})$ with coefficients in \mathbb{C} . Given such a matrix, we can define a linear function $L : \mathbb{C}^n \rightarrow \mathbb{C}^n$, by

$$L(x_1, \dots, x_n) = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^n a_{1j}x_j \\ \vdots \\ \sum_{j=1}^n a_{nj}x_j \end{pmatrix},$$

and a linear function L gives a matrix by setting a_{ij} as the i -th coefficient of the vector $L(e_j) \in \mathbb{C}^n$. How about in $\mathbb{P}^n = \mathbb{C}^{n+1} \setminus \{0\} / \sim$? Use matrices or linear transformations in \mathbb{C}^{n+1} .

Lemma 8.1. Assume that A is an $(n+1) \times (n+1)$ matrix with coefficients in \mathbb{C} such that

$$\det(A) \neq 0,$$

if and only if it is invertible. Then the function $\Phi : \mathbb{P}^n \rightarrow \mathbb{P}^n$, defined by

$$\Phi[x_1, \dots, x_n] = \left[A \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix} \right],$$

is well-defined and a bijection.

Proof. Since $\det(A) \neq 0$, we know from linear algebra that if

$$A \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix} = 0,$$

then $x = (x_0, \dots, x_n) = 0$. If A is not invertible there is no associated Φ . Thus if $x \in W = \mathbb{C}^{n+1} \setminus \{0\}$, then $A \cdot x \in W$. Moreover, if $x, y \in W$ are such that $[x] = [y]$, then there exists a non-zero $\lambda \in \mathbb{C}$ such that $x = \lambda y$ and

$$A \cdot x = \lambda A \cdot y,$$

which implies that $[A \cdot x] = [A \cdot y]$. It follows that Φ is well-defined. It is a bijection, with inverse given by the same kind of transformation obtained from the inverse matrix A^{-1} . \square

Definition 8.2. Any such function like Φ in Lemma 8.1 is called a **projective transformation**.

Remark 8.3. Note that an arbitrary $(n+1) \times (n+1)$ matrix A does not define a well-defined function as above, because there might be non-zero vectors $v \in \mathbb{C}^{n+1}$ such that $A \cdot v = \underline{0}$, and thus $[A \cdot v]$ would not define a point of projective space.

Example 8.4. You probably have encountered Möbius transformations in complex analysis. They are rational functions $f : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ of one complex variable z

$$f : z \mapsto \frac{az + b}{cz + d}, \quad a, b, c, d \in \mathbb{C}, \quad ad - bc \neq 0.$$

In terms of geometry, these are the projective transformations of \mathbb{P}^1 to itself. Indeed, if $[x_0, x_1]$ are the homogeneous coordinates on \mathbb{P}^1 , a projective transformation ϕ associated to a 2×2 invertible matrix T is given by

$$\Phi[x_0, x_1] = [A \cdot (x_0, x_1)] = [ax_0 + bx_1, cx_0 + dx_1], \quad T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad ad - bc \neq 0.$$

If, as in Lemma 3.14, we write $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$, where $\{\infty\} = \{x_1 = 0\} = \{[1, 0]\}$, then if $x_1 \neq 0$, $[x_0, x_1] = [x_0/x_1, 1] = [z, 1]$ for $z = x_0/x_1$ and

$$\Phi[z, 1] = [ax_0 + bx_1, cx_0 + dx_1] = [az + b, cz + d],$$

and if $cz + d \neq 0$, that is $[z, 1] \neq [-d, c]$, this is

$$\Phi[z, 1] = \left[\frac{az + b}{cz + d}, 1 \right] = [f(z), 1].$$

Here, unlike in complex analysis, the point $\{\infty\} = [1, 0]$ plays no special role, and we see right away that $\Phi[1, 0] = [a, c]$ and $\Phi[-d, c] = [1, 0]$.

Theorem 8.5. Assume that P_1, P_2, P_3 are three non-collinear points in \mathbb{P}^2 , that is not on the same line. Then there exists a projective transformation

$$\Phi : \mathbb{P}^2 \rightarrow \mathbb{P}^2$$

such that

$$\Phi(P_1) = [1, 0, 0], \quad \Phi(P_2) = [0, 1, 0], \quad \Phi(P_3) = [0, 0, 1].$$

Remark 8.6. Every projective transformation $\Phi = [A]$ is invertible. Just take $\Phi^{-1} = [A^{-1}]$.

Proof. Let $P_i = (a_{1i}, a_{2i}, a_{3i}) \in \mathbb{C}^3$ and $A = (a_{ij})$. Then, since P_1, P_2, P_3 are not collinear, it follows that $\det(A) \neq 0$ and A is invertible. Let B be the inverse matrix of A and let $\Phi = [B] : \mathbb{P}^2 \rightarrow \mathbb{P}^2$ be the projective transformation associated to the matrix B . Then

$$BP_i = e_i \quad \implies \quad \Phi(P_i) = [e_i],$$

as desired. □

Exercise 24. When do two linear transformations $L, L' : \mathbb{C}^{n+1} \rightarrow \mathbb{C}^{n+1}$ give rise to the same projective transformation $\mathbb{P}^n \rightarrow \mathbb{P}^n$?

Can do better.

Exercise 25. Show that if $P_1, P_2, P_3 \in \mathbb{P}_{\mathbb{C}}^1$ are distinct points, there exists a unique projective transformation $\Psi : \mathbb{P}_1 \rightarrow \mathbb{P}_1$ such that

$$\Psi(P_1) = [1, 0], \quad \Psi(P_2) = [0, 1], \quad \Psi(P_3) = [1, 1].$$

Exercise 26. Assume that $P_1, P_2, P_3, P_4 \in \mathbb{P}_{\mathbb{C}}^2$ are four points such that no three of them lie in the same line. Show that there exists a unique projective transformation $\Psi : \mathbb{P}^2 \rightarrow \mathbb{P}^2$ such that

$$\Psi(P_1) = [1, 0, 0], \quad \Psi(P_2) = [0, 1, 0], \quad \Psi(P_3) = [0, 0, 1], \quad \Psi(P_4) = [1, 1, 1].$$

Take a Φ as in the previous theorem. I can scale the representatives of the P_i , so $[v_i] = P_i$. Choose v_4 such that $P_4 = [v_4]$ and $v_4 = \sum_{i=1}^3 \lambda_i v_i = \lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \lambda_3 \cdot v_3$ for $\lambda_i \in \mathbb{C}^*$. We are in \mathbb{C}^2 , and the v_1, v_2, v_3 are linearly independent, so they are a basis. If $\lambda_i = 0$ for some i , the remaining vectors are in the same two-dimensional subspace of \mathbb{C} , contradicting non-collinearity in \mathbb{P}^2 . Take $\lambda_i \cdot v_i$ as representatives for P_i for $i = 1, 2, 3$ and v_4 for P_4 . Get matrix A as before, so $A \cdot e_i = P_i$ and $A \cdot \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} = \sum_{i=1}^3 \lambda_i v_i = v_4$, so $B = A^{-1}$, $\Phi = [B]$ and

$$\Phi(P_i) = [e_i], \quad i = 1, 2, 3, \quad \Phi(P_4) = [1, 1, 1].$$

There is a version of the previous statement in higher dimensions.

Definition 8.7. A **hyperplane** in \mathbb{P}^n is the image of a subspace of dimension n in \mathbb{C}^{n+1} via the map $\Pi : \mathbb{C}^{n+1} \setminus \{0\} \rightarrow \mathbb{P}^n$. Equivalently, it is the locus of points $[x_0, \dots, x_n]$ of \mathbb{P}^n satisfying some linear equation $\sum_{i=1}^n a_i x_i = 0$, where $(a_0, \dots, a_n) \neq 0$.

Example 8.8. Projective lines are precisely the hyperplanes of \mathbb{P}^2 .

Exercise 27. Let $\mathcal{S} = \{p_0, \dots, p_n, q\} \subseteq \mathbb{P}^n$ be a collection of $n+2$ distinct points such that no $n+1$ points of \mathcal{S} lie in a hyperplane. Denote by e_i , for $i = 0, \dots, n$, the vectors of the standard basis of \mathbb{C}^{n+1} . Then there is a unique projective transformation $f : \mathbb{P}^n \rightarrow \mathbb{P}^n$ such that

$$f(p_i) = [e_i] = [0, \dots, 0, 1, 0, \dots, 0], \quad i = 0, \dots, n, \quad f(q) = [1, \dots, 1].$$

Sometimes such a set of points is called a **projective basis**, in analogy with bases of vector spaces.

Exercise 28. Let L be a line in \mathbb{P}^2 . Then given $i \in \{0, 1, 2\}$, there exists a projective transformation $f : \mathbb{P}^2 \rightarrow \mathbb{P}^2$ such that $f(L) = \mathcal{P}_i = \{x_i = 0\}$.

Exercise 29. Let $C = \{P = 0\} \subseteq \mathbb{P}^2$ be a projective curve and let $\Phi = [A] : \mathbb{P}^2 \rightarrow \mathbb{P}^2$ be a projective transformation, a 3×3 matrix A . Show that

1. $\Phi(C)$ is again a projective curve of degree $\deg(\Phi(C)) = \deg(C)$, in particular C is a line if and only if $\Phi(C)$ is a line,
2. $\Phi(C)$ is irreducible if and only if C is, and there is a natural bijection between the sets of components of the two curves,
3. C is smooth if and only if $\Phi(C)$ is smooth, and
4. if $p \in C$ is a smooth point and l is the tangent line of C at p then $\Phi(C)$ is smooth at the point $\Phi(p)$ and $\Phi(l)$ is the tangent line of $\Phi(C)$ at $\Phi(p)$.

What is the equation of $\Phi(C)$?

Remark 8.9. As this last exercise suggests, one should think of curves only differing from each other via a projective transformation to be the same curve, since projective transformations preserve their properties. These transformations should be thought of as a change of projective coordinate system.

Lecture 10
Monday
29/10/18

9 Resultants and weak Bézout

Now we start studying how projective curves intersect in the projective plane, heading towards Bézout's theorem. Let $C = \{P = 0\}$ and $D = \{Q = 0\}$ be two projective curves of degree n and m defined by homogeneous polynomials $P, Q \in \mathbb{C}[x_0, x_1, x_2]$.

Theorem 9.1 (Bézout's theorem). $C \cap D$ has $n \cdot m$ points, unless C and D have a common component, and count points with multiplicity.

Example 9.2. If you do not use multiplicity, there might be less than $n \cdot m$ points.

1. Tangencies. Let $C = \{y = x^2\}$ and $D = \{y = 0\}$. In \mathbb{P}^2 , they intersect in $1 \neq (2)(1) = \deg(C) \deg(D)$ point in this case.
2. Singularities of C and D . Let C be two lines and D be a line passing through the intersection of C . $1 \neq (2)(1) = \deg(C) \deg(D)$ point of intersection.

Think of perturbing the equations.

We first have to develop some algebraic tools, the resultant. We want to study $C \cap D = \{P = 0\} \cap \{Q = 0\}$, where P, Q no repeated factors, that is points $[x_0, x_1, x_2]$ that are solutions up to scaling of the equations for C and D

$$P(x_0, x_1, x_2) = 0, \quad Q(x_0, x_1, x_2) = 0,$$

where $(x_0, x_1, x_2) \neq (0, 0, 0)$. We first take a step back to the case of polynomials in one variable and study solutions of $p(x) = q(x) = 0$ for polynomials $p, q \in \mathbb{C}[x]$. Let p, q be

$$p(x) = a_0 + \cdots + a_n x^n = \sum_{i=0}^n a_i x^i, \quad q(x) = b_0 + \cdots + b_m x^m = \sum_{i=0}^m b_i x^i, \quad a_n, b_m \neq 0,$$

for $a_i, b_i \in \mathbb{C}$, and $\deg(P) = n$ and $\deg(Q) = m$. When does $p(x) = q(x) = 0$ have solutions? Transform this question into linear algebra. The polynomials p and q have a common root, that is there is $\lambda \in \mathbb{C}$ such that $p(\lambda) = q(\lambda) = 0$, precisely if there is a non-constant polynomial $l \in \mathbb{C}[x]$ such that

$$p(x) = l(x)r(x), \quad q(x) = l(x)s(x),$$

where r and s are non-zero polynomials, which thus have $\deg(r) \leq n - 1$ and $\deg(s) \leq m - 1$.

Lemma 9.3. The polynomials p and q have a common root if and only if there are non-zero polynomials r, s with $\deg(r) \leq n - 1$ and $\deg(s) \leq m - 1$ with

$$p(x)s(x) - q(x)r(x) = 0, \tag{3}$$

the zero polynomial

Proof. By taking r and s in the previous discussion, it is clear that if p and q have a common root, then (3) holds. Conversely assume that (3) holds. There is a unique decomposition $p(x) = c p_1(x)^{a_1} \cdots p_k(x)^{a_k}$, where $c \in \mathbb{C}^*$, p_1, \dots, p_k are monic non-constant irreducible polynomials, and $a_i \in \mathbb{N}^*$. Since $p_1(x)^{a_1} \cdots p_k(x)^{a_k} \mid q(x)r(x)$ and $\deg(r) \leq n - 1 < \sum_{i=1}^k \deg(p_i)$, at least one of the irreducible polynomials p_i divides $q(x)$, by irreducibility. It follows that p and q have a common factor and, by the fundamental theorem of algebra, that p and q have a common root. \square

We now show that (3) is a system of $m + n$ equations in $m + n$ variables. Now write $r(x)$ and $s(x)$ in terms of unknown coefficients. Let $\underline{v} = (v_0, \dots, v_{n+m-1}) \in \mathbb{C}^{n+m}$ be defined by

$$s(x) = v_0 + \cdots + v_{m-1} x^{m-1} = \sum_{i=0}^{m-1} v_i x^i, \quad -r(x) = v_m + \cdots + v_{n+m-1} x^{n-1} = \sum_{i=0}^{n-1} v_{m+i} x^i.$$

Substitute these into $p(x) \cdot s(x) - q(x) \cdot r(x) = 0$. Get a big system of equations. Then (3) is

$$(v_0 a_0 + v_m b_0) + \cdots + \left(\sum_{k=0}^i (v_k a_{i-k} + v_{m+k} b_{i-k}) \right) x^i + \cdots + (v_{m-1} a_n + v_{n+m-1} b_m) x^{n+m-1} = 0.$$

Since this is a polynomial of degree $n + m - 1$, we thus have a system of $n + m$ equations in $n + m$ variables of the form

$$A \cdot v = 0, \quad (4)$$

where A is an $(n + m) \times (n + m)$ matrix

$$A = \begin{pmatrix} a_0 & & 0 & b_0 & & 0 \\ \vdots & \ddots & & \vdots & \ddots & \\ a_n & & a_0 & b_m & & b_0 \\ & \ddots & \vdots & & \ddots & \vdots \\ 0 & & a_n & 0 & & b_m \end{pmatrix},$$

where there are m columns of a_i and n columns of b_i . From linear algebra, we know that (4) has a non-trivial solution if and only if $\det(A) = 0$. This motivates the following definition.

Definition 9.4. Let $p, q \in \mathbb{C}[x]$ be as above. Then the **resultant** of p and q is the determinant of the $(n + m) \times (n + m)$ matrix A^T ,

$$R_{f,g} = \det(A^T) = \det \begin{pmatrix} a_0 & \dots & a_n & & 0 \\ & \ddots & & \ddots & \\ 0 & & a_0 & \dots & a_n \\ b_0 & \dots & b_m & & 0 \\ & \ddots & & \ddots & \\ 0 & & b_0 & \dots & b_m \end{pmatrix}.$$

Thus, Lemma 9.3 can be reformulated as the following.

Theorem 9.5. Let $p, q \in \mathbb{C}[x]$ be two non-zero polynomials. Then, p and q have a common root if and only if $R_{p,q} = 0$.

Example 9.6.

1. Let $p(x) = x^2 - 1$ and $q(x) = x^2 + 2x + 1$, so

$$a_0 = 1, \quad a_1 = 0, \quad a_2 = -1, \quad b_0 = 1, \quad b_1 = 2, \quad b_2 = 1.$$

Then the resultant of f and g is the 4×4 matrix

$$R_{f,g} = \det \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

(TODO Exercise: Check that the determinant is $R_{f,g} = 0$) Thus, f and g have a common solution $x = -1$.

2. Let $n = 1$ and $m = 4$, so $p(x) = a_0 + a_1x$ and $q(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4$. Then A is a 5×5 matrix

$$A = \begin{pmatrix} a_0 & 0 & 0 & 0 & b_0 \\ a_1 & a_0 & 0 & 0 & b_1 \\ 0 & a_1 & a_0 & 0 & b_2 \\ 0 & 0 & a_1 & a_0 & b_3 \\ 0 & 0 & 0 & a_1 & b_4 \end{pmatrix}.$$

3. Recall that $p \in \mathbb{C}[x]$ has a repeated root if and only if p and p' have a common root, that is by what precedes if and only if $R_{p,p'} = 0$. If $p(x) = ax^2 + bx + c$, where $a \neq 0$, then

$$R_{p,p'} = \det \begin{pmatrix} c & b & a \\ b & 2a & 0 \\ 0 & b & 2a \end{pmatrix} = a(4ac - b^2).$$

We see that $-R_{p,p'} = a \cdot \Delta$, where Δ is the discriminant of the quadratic equation $p(x) = 0$.

4. Let $n = 2$ and $m = 3$, so $p(x) = a_0 + a_1x + a_2x^2$ and $q(x) = b_0 + b_1x + b_2x^2 + b_3x^3$. Then A is a 5×5 matrix

$$A = \begin{pmatrix} a_0 & 0 & 0 & b_0 & 0 \\ a_1 & a_0 & 0 & b_1 & b_0 \\ a_2 & a_1 & a_0 & b_2 & b_1 \\ 0 & a_2 & a_1 & b_3 & b_2 \\ 0 & 0 & a_2 & 0 & b_3 \end{pmatrix}.$$

In general, the resultant is useful because it tends to be easier to compute the determinant of a matrix than to factorise polynomials in order to determine whether they have a common root. Assume now that $P, Q \in \mathbb{C}[x_0, x_1, x_2]$ are homogeneous polynomials of degrees n and m respectively. We write P and Q as polynomials in x_0 , with coefficients in $\mathbb{C}[x_1, x_2]$.

$$P(x_0, x_1, x_2) = \sum_{i=0}^n a_i(x_1, x_2) x_0^i, \quad Q(x_0, x_1, x_2) = \sum_{j=0}^m b_j(x_1, x_2) x_0^j,$$

where $a_i \in \mathbb{C}[x_1, x_2]$ is a homogeneous polynomial of degree $n - i$, and $b_j \in \mathbb{C}[x_1, x_2]$ is homogeneous of degree $m - j$. In particular, $a_n = P(1, 0, 0)$ and $b_m = Q(1, 0, 0)$ are constants.

Definition 9.7. Assume that $P(1, 0, 0) \neq 0$ and $Q(1, 0, 0) \neq 0$. The resultant of P and Q is the determinant of the $(n + m) \times (n + m)$ matrix

$$R_{P,Q}(x_1, x_2) = \det \begin{pmatrix} a_0(x_1, x_2) & \dots & a_n(x_1, x_2) & & 0 \\ & & \ddots & \ddots & \\ 0 & & a_0(x_1, x_2) & \dots & a_n(x_1, x_2) \\ b_0(x_1, x_2) & \dots & b_m(x_1, x_2) & & 0 \\ & & \ddots & \ddots & \\ 0 & & b_0(x_1, x_2) & \dots & b_m(x_1, x_2) \end{pmatrix}.$$

The entries of the matrix above are homogeneous polynomials in $\mathbb{C}[x_1, x_2]$. If you specify $x_1 = a$, $x_2 = b$ for $a, b \in \mathbb{C}$, then $R_{P,Q}$ is the resultant of $P(x_0, a, b)$ and $Q(x_0, a, b)$. We admit the following theorem, which follows from commutative algebra.

Theorem 9.8. Let $P, Q \in \mathbb{C}[x_0, x_1, x_2]$ be homogeneous polynomials of degrees n and m , and assume that $a_n, b_m \neq 0$. Then P and Q have a common factor if and only if $R_{P,Q} \equiv 0$, that is if

$$R_{P,Q}(x_1, x_2) = 0, \quad x_1, x_2 \in \mathbb{C}.$$

In fact, slightly more is true.

Theorem 9.9. Let $P, Q \in \mathbb{C}[x_0, x_1, x_2]$ be homogeneous polynomials such that $P(1, 0, 0), Q(1, 0, 0) \neq 0$. Then $R_{P,Q} \in \mathbb{C}[x_1, x_2]$ is a homogeneous polynomial of degree nm .

Proof. Let A be the $(n + m) \times (n + m)$ matrix above, that is such that $R_{P,Q} = \det(A)$. Recall from linear algebra that

$$\det(A) = \sum_{\sigma \in S_{n+m}} \text{sign}(\sigma) \prod_{k=1}^{n+m} A_{k, \sigma(k)}.$$

Lecture 11
Thursday
01/11/18

The entries of A are either zero or are homogeneous polynomials, we thus only need to check that for each $\sigma \in S_{n+m}$ such that $A_{k,\sigma(k)} \neq 0$ for all k , $\prod_{k=1}^{n+m} A_{k,\sigma(k)}$ is of degree nm . By definition of A , the non-zero entries of A are

$$A_{k,l} = \begin{cases} a_{l-k}(x_1, x_2) & k \leq m, 0 \leq l-k \leq n \\ b_{l-k+m}(x_1, x_2) & k \geq m+1, 0 \leq l-k+m \leq m \end{cases}.$$

$\deg(a_{l-k}) = n - (l-k)$ and $\deg(b_{l-k+m}) = m - (l-k+m) = k-l$, so that when non-zero, $\prod_{k=1}^{n+m} A_{k,\sigma(k)}$ has degree

$$\deg\left(\prod_{k=1}^{n+m} A_{k,\sigma(k)}\right) = \sum_{k=1}^m (n - (\sigma(k) - k)) + \sum_{k=m+1}^{m+n} (k - \sigma(k)) = mn + \sum_{k=1}^{m+n} k - \sum_{k=1}^{m+n} \sigma(k).$$

The last two terms are equal because σ is a permutation, so this is equal to mn for all permutations $\sigma \in S_{m+n}$, and this proves that $R_{P,Q}$ is a homogeneous polynomial of degree mn . \square

Recall that homogeneous polynomials in two variables always factor as a product of linear homogeneous polynomials. We can now prove a weak form of Bézout's theorem. We will refine the statement later on.

Theorem 9.10 (Weak Bézout theorem). Let $C, D \subseteq \mathbb{P}^2$ be projective curves of degrees $\deg(C) = n$ and $\deg(D) = m$ respectively. Then

1. C and D intersect in at least one point, that is $C \cap D$ is not empty, and
2. C and D have at most $\# \{C \cap D\} \leq nm$ distinct points of intersection, if they do not have a common component.

Proof.

1. Let $P, Q \in \mathbb{C}[x_0, x_1, x_2]$ be homogeneous polynomials of degrees n and m with no repeated factors that define C and D , that is

$$C = \{P = 0\}, \quad D = \{Q = 0\}.$$

$P(1, 0, 0) \neq 0$ and $Q(1, 0, 0) \neq 0$ if and only if $p = [1, 0, 0]$ is not in C and not in D . Use a projective transformation to ensure this. Let $q \in \mathbb{P}^2$ be a point that lies neither on C nor on D , so not on $C \cup D$. (TODO Exercise: such a point always exists) There is a projective transformation $\Phi : \mathbb{P}^2 \rightarrow \mathbb{P}^2$ that sends p to $[1, 0, 0]$, that is $\Phi(p) = [1, 0, 0]$. Transform C and D using Φ , so replace them with $\Phi(C)$ and $\Phi(D)$. We have seen that $\Phi(C), \Phi(D)$ are projective curves of the same degrees $\deg(\Phi(C)) = \deg(C)$ and $\deg(\Phi(D)) = \deg(D)$, and that $\# \{C \cap D\} = \# \{\Phi(C) \cap \Phi(D)\}$. Thus, after replacing C with $\Phi(C)$ and D with $\Phi(D)$ we may assume that $[1, 0, 0] \notin C \cup D$, so $P(1, 0, 0) \neq 0$ and $Q(1, 0, 0) \neq 0$. We assume that C and D have no common component, as the result is trivial if they do. Denote by R the resultant polynomial of P and Q , $R(x_1, x_2) = R_{P,Q}(x_1, x_2)$ for all $x_1, x_2 \in \mathbb{C}$, and factor it. By Theorems 9.8 and 9.9, R is a homogeneous polynomial of degree nm that is not identically zero, since C and D have no common component. By Lemma 6.2, there are $(\alpha_i, \beta_i) \in \mathbb{C}^2 \setminus \{(0, 0)\}$ for $i = 1, \dots, nm$ such that

$$R(x_1, x_2) = \prod_{i=1}^{nm} (\alpha_i x_1 + \beta_i x_2).$$

Fix $(a, b) \in \mathbb{C}^2 \setminus \{(0, 0)\}$, and let $p, q \in \mathbb{C}[x]$ be the polynomials defined by

$$p(x) = P(x, a, b), \quad q(x) = Q(x, a, b).$$

Then, $R(a, b) = R_{p,q}$. In particular, if $(a, b) = (\beta_1, \alpha_1)$, $R(-\beta_1, \alpha_1) = 0$, and by Theorem 9.5, there is $\lambda \in \mathbb{C}$ such that

$$P(\lambda, -\beta_1, \alpha_1) = p(\lambda) = q(\lambda) = Q(\lambda, -\beta_1, \alpha_1) = 0,$$

so $p(x_0), q(x_0)$ have a common root λ . Since $(-\beta_1, \alpha_1) \neq (0, 0)$, $(\lambda, \beta_1, \alpha_1) \neq (0, 0, 0)$, so that $p = [\lambda, -\beta_1, \alpha_1]$ is a well-defined point of \mathbb{P}^2 and is on both C and D , so $p \in C \cap D$.

2. We will show that if $C \cap D$ contains at least $nm+1$ distinct points, C and D have a common factor. Let $\mathcal{S} = \{p_1, \dots, p_{nm+1}\}$ be any set of $nm+1$ distinct points and denote by $L_{i,j}$ the unique line containing p_i and p_j for $1 \leq i, j \leq nm+1$. For each i , denote by $[x_0^i, x_1^i, x_2^i]$ the coordinates of p_i . The point $x = [x_0, x_1, x_2] \in \mathbb{P}^2$ belongs to $L_{i,j}$ if and only if $\det(A) = 0$, where

$$A_{i,j} = \begin{pmatrix} x_0 & x_0^i & x_0^j \\ x_1 & x_1^i & x_1^j \\ x_2 & x_2^i & x_2^j \end{pmatrix}. \quad (5)$$

Let $p \in \mathbb{P}^2$ be any point that lies neither on C, D nor on any $L_{i,j}$, that is $p \notin C \cup D \cup (\cup_{i,j} L_{i,j})$. Can apply a projective transformation $\Phi : \mathbb{P}^2 \rightarrow \mathbb{P}^2$ that sends p to $[1, 0, 0]$. Taking images along Φ , the image of \mathcal{S} is a set of $nm+1$ distinct points and the image of $L_{i,j}$ by Φ is the unique line through $\Phi(p_i)$ and $\Phi(p_j)$. As in the proof of 1, after replacing C, D , and \mathcal{S} by their images by Φ , we may assume that $[1, 0, 0] \notin C \cup D$ and that $[1, 0, 0]$ lies on no line through two points $p_i, p_j \notin \mathcal{S}$. In particular, by (5),

$$\det \begin{pmatrix} 1 & x_0^i & x_0^j \\ 0 & x_1^i & x_1^j \\ 0 & x_2^i & x_2^j \end{pmatrix} \neq 0,$$

that is, $(x_1^i, x_2^i) \neq (0, 0)$ for all i , otherwise determinant is zero, so that $[x_1^i, x_2^i]$ is a well-defined point of \mathbb{P}^1 , and $[x_1^i, x_2^i] \neq [x_1^j, x_2^j]$ for all $i \neq j$. Let $P, Q \in \mathbb{C}[x_0, x_1, x_2]$ be homogeneous polynomials of degrees n and m that define C and D , that is

$$C = \{P = 0\}, \quad D = \{Q = 0\}.$$

Since $[1, 0, 0] \notin C \cup D$, $P(1, 0, 0) \neq 0$ and $Q(1, 0, 0) \neq 0$. Denote by R the resultant $R_{P,Q}$ of P, Q . This is homogeneous of degree nm and factors into linear factors $R(x_1, x_2) = \prod_{i=1}^{nm} (\alpha_i x_1 + \beta_i x_2)$ for $(\alpha_i, \beta_i) \neq (0, 0)$, so $\{R = 0\} \subseteq \mathbb{P}^1$ has at most nm distinct elements. Now assume $C \cap D$ contains at least $nm+1$ points and let $\mathcal{S} \subseteq C \cap D$ be a set of $nm+1$ distinct points. Set $(\alpha_i, \beta_i) = (-x_2^i, x_1^i)$ for $i = 1, \dots, nm+1$. By construction, for all i , $p(x) = P(x_0, x_1^i, x_2^i)$ and $q(x) = Q(x_0, x_1^i, x_2^i)$ have a common root so that $\det(R_{p,q}) = 0$. But we have

$$\det(R_{p,q}) = R(x_1^i, x_2^i),$$

so that $(\alpha_i x_1 + \beta_i x_2)$ is a factor of the polynomial $R(x_1, x_2)$. Since $[x_1^i, x_2^i] \neq [x_1^j, x_2^j]$ these factors are distinct, so $\{[x_1^i, x_2^i]\} \subseteq \mathbb{P}^1$ has at least $nm+1$ distinct points and

$$R(x_1, x_2) = \prod_{i=1}^{nm+1} (\alpha_i x_1 + \beta_i x_2) S(x_1, x_2), \quad (6)$$

for some possibly constant homogeneous polynomial S . If $R(x_1, x_2)$ is not identically zero, by Theorem 9.9, it has degree nm . Thus, (6) shows that R is identically zero, because the degree of the polynomial on the right hand side of (6) is at least $nm+1$ if this polynomial is not identically zero. Thus, by Theorem 9.8, P and Q have a common factor and C and D have a common component. □

This finishes the proof of Theorem 7.12, and now we can also prove Theorem 7.15, stated before.

Proof of Theorem 7.15. Use Bézout's theorem. Let $C = \{P = 0\}$ for P a polynomial of degree d defining C . Singular points are solutions $[x_1, x_2, x_3]$ at

$$P = 0, \quad P_{x_0} = 0, \quad P_{x_1} = 0, \quad P_{x_2} = 0.$$

Without loss of generality we may assume that there exists $i = 0, 1, 2$ such that $Q = P_{x_i}$ is not zero, otherwise P is constant. Thus Q is a homogeneous polynomial of degree $d-1$. If p is a singular point of C

then $P(p) = Q(p) = 0$. Clearly the opposite is not true. Let $D = \{Q = 0\}$. Then D is another projective curve of degree $d - 1$ and the intersection $C \cap D$ contains all the singular points of C . Moreover, since C is irreducible, it follows that C and D do not have any common component. By Theorem 9.10, it follows that the number of intersection points of C and D is at most $\deg(C) \deg(D) = d \cdot (d - 1)$ and the claim follows. \square

Proposition 9.11 (Pascal's mystic hexagon). Let $C \subseteq \mathbb{P}^2$ be an irreducible conic and let $p_1, \dots, p_6 \in C$ be six distinct points that form a hexagon, that is no three of the points p_1, \dots, p_6 lie on a projective line. Then the points of intersection of lines passing through opposite sides are collinear.

Proof. Assume that p_1, \dots, p_6 are ordered such that the lines L_1, \dots, L_6 , with L_i the unique line through p_i and p_{i+1} , form the sides of a hexagon. Denote by D_1 the cubic curve $L_1 \cup L_3 \cup L_5$ and by D_2 the cubic curve $L_2 \cup L_4 \cup L_6$. Both cubic curves are reducible by definition, and both contain the points p_1, \dots, p_6 . Let $q_1 = L_1 \cap L_4$, $q_2 = L_3 \cap L_6$, and $q_3 = L_5 \cap L_2$ be the not necessarily distinct points of intersection of opposite sides. We want to prove that there is a projective line L through q_1, q_2, q_3 . First note that if q_1, q_2, q_3 are not distinct, there is a projective line through q_1, q_2, q_3 by Exercise 18. We therefore assume that q_1, q_2, q_3 are three distinct points. The points q_1, q_2, q_3 are not in the set $\{p_1, \dots, p_6\}$ because otherwise, one of the lines L_1, \dots, L_6 would have to contain at least three of the points p_1, \dots, p_6 . Since C is irreducible, it contains none of the lines L_1, \dots, L_6 , in particular, C has no common component with D_1 or with D_2 . Since $C \cap D_1 \supset \{p_1, \dots, p_6\}$ and $C \cap D_2 \supset \{p_1, \dots, p_6\}$, and since C and D_1 and C and D_2 have no common component, their intersections consist of at most $(2)(3) = 6$ points and therefore $C \cap D_1 = C \cap D_2 = \{p_1, \dots, p_6\}$. This shows that the points q_1, q_2, q_3 do not lie on C . I will construct another cubic, having seven points of intersection with C . Let $p_0 \in C$ be a point that does not belong to the set $\{p_1, \dots, p_6\}$. In particular, the point p_0 does not lie on D_1 or on D_2 . Let P, Q be homogeneous polynomials that define the cubic curves D_1 and D_2 , products of the equations of the lines, that is

$$D_1 = \{P = 0\}, \quad D_2 = \{Q = 0\}.$$

Since $p_0 \notin D_1 \cup D_2$, $P(p_0) \neq 0$ and $Q(p_0) \neq 0$, so that there exists $[\lambda, \mu] \in \mathbb{P}^1$ such that $\lambda P(p_0) + \mu Q(p_0) = 0$, such as $[-Q(p_0), P(p_0)]$. Consider the cubic curve

$$D = \{\lambda P + \mu Q = 0\} \subseteq \mathbb{P}^2,$$

where $\lambda P + \mu Q$ is a homogeneous polynomial of degree three. The points p_1, \dots, p_6 lie on $D_1 \cap D_2$, hence they satisfy $P(p_i) = Q(p_i) = 0$ for all i , so $(\lambda P + \mu Q)(p_i) = 0$ and $p_1, \dots, p_6 \in D$. Since $p_0 \in D$, the intersection $C \cap D$ thus contains at least seven distinct points p_0, \dots, p_6 . By Bézout's theorem, this implies that C and D have a common component, and since C is irreducible, that has to be C and $C \subseteq D$. If Q is a homogeneous polynomial of degree two that defines C , there is a homogeneous polynomial S of degree one such that

$$D = \{Q \cdot S = 0\} = C \cup \{S = 0\},$$

of which $\{S = 0\}$ has to be a line. Let L be the projective line $L = \{S = 0\}$ that I was looking for. Since the points $q_1, q_2, q_3 \in D_1 \cap D_2$, they also lie on D . We have seen that $q_1, q_2, q_3 \notin C$, thus, they lie on L . \square