MATH70033 Algebraic curves :: Lecture notes

Lecturer: Soheyla Feyzbakhsh

Last edited: 17th November 2024

Contents

1 Groundwork **1**
1.1 Definitions and theoretical background 1
1.2 Factorisation 2

2 Projective variety **3**
2.1 Motivation, definitions, basic results 3
2.2 Projective plane curves – affine plane curves 6

3 Singular point, smooth curve **7**

4 Bézout theorem **9**
4.1 Projective transformation 9
4.2 Resultant 11
4.3 Proof and applications of the theorem 14
4.4 Resultant, reprise, and a better theorem 16

Every ring in this module is commutative.

1 Groundwork

1.1 Definitions and theoretical background

Definition 1.1.1. Let $\mathbb{K}$ be a field and $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_m]$. An *affine algebraic set* is of the form

$$\mathbb{V}_{\mathbb{K}}(f_1, \ldots, f_n) = \{(x_1, \ldots, x_m) : f_1(x_1, \ldots, x_m) = \cdots = f_n(x_1, \ldots, x_m) = 0\}.$$

Example 1.1.2. $\mathbb{V}_{\mathbb{R}}(x^2 + y^2 - 1)$ is a unit circle, $\{x = 2, y = 3\}$ can be understood as $\mathbb{V}_{\mathbb{R}}(x - 2, y - 3)$, the whole $\mathbb{R}^n$ can be understood as $\mathbb{V}_{\mathbb{R}}(0)$, $\{a_1, \ldots, a_n\} \in \mathbb{C}$ can be understood as $\mathbb{V}_{\mathbb{C}}((x - a_1) \cdots (x - a_n))$.

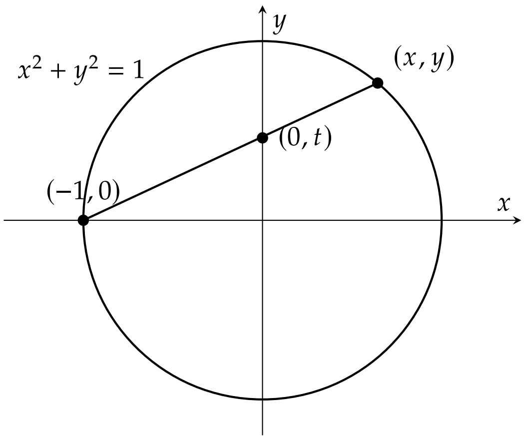
$\mathbb{Z} \subset \mathbb{C}$ is not an affine algebraic set since any nonzero polynomial has a finite number of solutions and the more polynomials one has, the less common solutions there are.

Definition 1.1.3. An *affine plane curve* over $\mathbb{K}$ is a affine algebraic set defined by $C = \mathbb{V}_{\mathbb{K}}(p) \subset \mathbb{K}^2$ where p is a nonconstant polynomial in $\mathbb{K}[x, y]$.

Definition 1.1.4. The *degree* of a plane curve $C = \mathbb{V}_{\mathbb{K}}(p)$ is the degree of the polynomial $p \in \mathbb{K}[x, y]$, i.e. write $p = \sum_{i \geq 0, j \geq 0} a_{ij} x^i y^j$ then $\deg C = \deg p = \max\{i + j : a_{ij} \neq 0\}$.

Example 1.1.5. Find all $(a, b, c) \in \mathbb{Z}^3 : a^2 + b^2 = c^2$, the Pythagorean triples. Rewrite the equation as $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$ and consider the curve $\mathbb{V}_{\mathbb{Q}}(x^2 + y^2 - 1)$. But how do we parameterise the rational points? We can consider instead $\mathbb{V}_{\mathbb{R}}(y - t(x + 1), x^2 + y^2 - 1)$ where $t \in \mathbb{Q}$. From this it's simple calculation and one finds

$$\mathbb{V}_{\mathbb{Q}}(x^2 + y^2 - 1) = \{(-1, 0)\} \cup \left\{ \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right) : t \in \mathbb{Q} \right\}.$$



Definition 1.1.6. An *ideal* $I \trianglelefteq R$ of a ring R is a subset of R such that $a, b \in I, r \in R \implies a + b, ar \in I$. For $X \subset R$, denote by $I(X)$ the ideal generated by X (the smallest ideal containing X). If $X = \{r_1, \ldots, r_n\}$ one also writes $I(X) = \langle r_1, \ldots, r_n \rangle$.

Theorem 1.1.7 (Hilbert basis theorem)**.** If R is a Noetherian ring then $R[x]$ is also Noetherian, i.e. any ideal in $R[x]$ is finitely generated if any ideal in R is finitely generated.

Corollary 1.1.8. For a field $\mathbb{K}$, any $I \trianglelefteq \mathbb{K}[x_1, \ldots, x_n]$ has a finite generating set.

Notation. $\mathbb{V}_{\mathbb{K}}(I) = \{(a_1, \ldots, a_n) : f(a_1, \ldots, a_n) = 0 \; \forall f \in I\}$.

Remark 1.1.9. By corollary above, one can write $I = \langle f_1, \ldots, f_m \rangle$. We claim $\mathbb{V}_{\mathbb{K}}(I) = \mathbb{V}_{\mathbb{K}}(f_1, \ldots, f_m)$. Indeed, $\{f_1, \ldots, f_m\} \subset I$ so clearly $\mathbb{V}_{\mathbb{K}}(I) \subset \mathbb{V}_{\mathbb{K}}(f_1, \ldots, f_m)$. But for any $g \in I$ one can write $g = g_1 f_1 + \cdots + g_m f_m$, so $\mathbb{V}_{\mathbb{K}}(I) \supset \mathbb{V}_{\mathbb{K}}(f_1, \ldots, f_m)$ as well.

Week 2, lecture 1, 7th October

Definition 1.1.10. Define the *Zariski topology* by: a set $V \subset \mathbb{K}^n$ is closed $\iff$ V is an affine algebraic set.

Remark 1.1.11. The Zariski topology is indeed a topology: $\mathbb{K}^n = \mathbb{V}_{\mathbb{K}}(0)$, $\varnothing = \mathbb{V} = \mathbb{K}(1)$, intersection of arbitrary closed sets is closed by 1.1.7 ($\mathbb{V}_{\mathbb{K}}(f_1, \dots, f_n) \cap \mathbb{V}_{\mathbb{K}}(g_1, \dots, g_m) = \mathbb{V}_{\mathbb{K}}(f_1, \dots, f_n, g_1, \dots, g_m)$), and finite union of closed sets is close ($\mathbb{V}_{\mathbb{K}}(f_1, \dots, f_m) \cup \mathbb{V}_{\mathbb{K}}(g_1, \dots, g_m) = \mathbb{V}_{\mathbb{K}}(\prod_{i,j} f_i g_j)$.
Note that Zariski topology is coarser (weaker) than the usual Euclidean topology since any polynomial is a continuous function, and closedness is preserved under preimage, but e.g. $[a, b] \subset \mathbb{R}$ is closed with respect to Euclidean norm, but not an affine algebraic set.

Definition 1.1.12. A field $\mathbb{K}$ is *algebraically closed* if $f \in \mathbb{K}[x] \implies \exists a \in \mathbb{K} : f(a) = 0$.

Theorem 1.1.13 (Fundamental theorem of algebra)**.** $\mathbb{C}$ is algebraically closed.

Lemma 1.1.14. An algebraically closed field must be infinite.

Proof. Suppose $\mathbb{K}$ is a finite field, then $f(x) = \prod_{a \in \mathbb{K}}(x - a) + 1$ has no roots in $\mathbb{K}$. □

Theorem 1.1.15. If $\mathbb{K}$ is algebraically closed, then any plane curve $C \subset \mathbb{K}^2$ has infinitely many points.

Proof. Let $C = \mathbb{V}_{\mathbb{K}}(p)$ be a plane curve and consider $p \in \mathbb{K}[x, y] = \mathbb{K}[y][x]$ as

$$Q_d(y)x^d + \cdots + Q_1(y)x + Q_0(y)$$

where WLOG $d \geq 1$ and $Q_i(y) \in \mathbb{K}[y]$. Now $Q_d(y)$ has at most $\deg_y Q_d$ roots, so since $\mathbb{K}$ is infinite by 1.1.14, there are infinitely many $y_0 : Q_d(y_0) \neq 0 \implies \deg p = d$. But again $\mathbb{K}$ is algebraically closed, hence for every such y_0, $\exists x_0 : p(x_0, y_0) = 0$. □

1.2 Factorisation

Definition 1.2.1. An *integral domain* or *domain* is a ring where product of any two nonzero elements is nonzero.
An element $a \in R$ of a ring is a *unit* if $\exists a^{-1} : a^{-1}a = 1$.
A nonzero element $a \in R$ is *irreducible* if it's not a product of two nonunit elements.
A *unique factorisation domain* is a domain R where any nonzero and nonunit element can be written uniquely (up to reordering and mutliplication by units) as product of irreducible elements.

Theorem 1.2.2. If R is a UFD, then $R[x]$ is a UFD.

Proof. See MATH70035 Algebra 3. □

Corollary 1.2.3. If $\mathbb{K}$ is a field, then $\mathbb{K}[x_1, \dots, x_n]$ is a UFD.

Theorem 1.2.4 (Weak Nullstellensatz)**.** If $\mathbb{K}$ is algebraically closed and $I \trianglelefteq \mathbb{K}[x_1, \dots, x_n]$, then $\mathbb{V}_{\mathbb{K}}(I) = \varnothing \iff 1 \in I \iff I = \mathbb{K}[x_1, \dots, x_n]$.

Proof. Let $m = \langle x1 - a_1, \dots, x_n - an \rangle \trianglelefteq \mathbb{K}[x_1, \dots, x_n]$ be a maximal ideal which has $\mathbb{V}_{\mathbb{K}}(m) = \{(a_1, \dots, a_n)\}$. But then for any ideal I other than $\mathbb{K}$ one has $I \subset m$, so $\mathbb{V}_{\mathbb{K}}(m) \subset \mathbb{V}_{\mathbb{K}}(I)$, in particular $\mathbb{V}_{\mathbb{K}}(I) \neq \varnothing$. □

Corollary 1.2.5. If $f, g \in \mathbb{K}[x_1, \dots, x_n]$ then $f \mid g \implies \mathbb{V}_{\mathbb{K}}(f) \subset \mathbb{V}_{\mathbb{K}}(g)$.

Proposition 1.2.6 (The converse)**.** Let $\mathbb{K}$ be algebraically closed and $f, g \in \mathbb{K}[x_1, \dots, x_n]$. If f is irreducible and $\mathbb{V}_{\mathbb{K}}(f) \subset \mathbb{V}_{\mathbb{K}}(g)$ then $f \mid g$.

Proof. $\mathbb{V}_{\mathbb{K}}(f) \subset \mathbb{V}_{\mathbb{K}}(g) \iff \{f = 0\} \cap \{g \neq 0\} = \varnothing$, but $g(x_1, \dots, x_n) \neq 0 \iff \exists t \in \mathbb{K} : tg(x_1, \dots, x_n) = 1$ (any nonzero element of a field is a unit), so one has $\mathbb{V}_{\mathbb{K}}(f) \cap \mathbb{V}_{\mathbb{K}}(tg - 1) = \mathbb{V}_{\mathbb{K}}(f, tg - 1) = \varnothing$ where $tg - 1 \in \mathbb{K}[x_1, \dots, x_n, t]$. By 1.2.4, $1 \in \langle f, tg - 1 \rangle$, i.e. $af + b(tg - 1) = 1$ for some $a, b \in \mathbb{K}[x_1, \dots, x_n, t]$. Now write $t = \frac{1}{g}$ and multiply the above by g^N where N is large enough so that $\widetilde{a}f = g^N$ where $\widetilde{a} \in \mathbb{K}[x_1, \dots, x_n]$. In particular $f \mid g^N$, but f is irreducible, so since $\mathbb{K}[x_1, \dots, x_n]$ is a UFD by 1.2.3 f is prime, hence $f \mid g$. □

Week 2, lecture 2, 7th October

Definition 1.2.7. A topological space X is *irreducible* if for any two closed subsets $A, B \subset X$,

$$X = A \cup B \implies X = A \text{ or } X = B.$$

An affine algebraic set $\mathbb{V} \subset \mathbb{K}^n$ is *reducible* if one can write $\mathbb{V} = \mathbb{V}_1 \cup \mathbb{V}_2$ where V_i's are affine algebraic and $V_i \neq V$. Otherwise it's *irreducible*, i.e. if $\mathbb{V} = \mathbb{V}_1 \cup \mathbb{V}_2 \implies \mathbb{V} = \mathbb{V}_1$ or $\mathbb{V}_2$.

Theorem 1.2.8. Let $\mathbb{K}$ be algebraically closed. Then a plane curve $C \subset \mathbb{K}^2$ is irreducible $\iff$ $C = \mathbb{V}_{\mathbb{K}}(f)$ for some nonconstant irreducible $f \in \mathbb{K}[x, y]$.

Proof. Let $C = \mathbb{V}_{\mathbb{K}}(f)$ be irreducible and write $f = f_1^{\alpha_1} \cdots f_n^{\alpha_n}$ where f_i's are irreducible. Then $C = \mathbb{V}_{\mathbb{K}}(f_1) \cup \cdots \cup \mathbb{V}_{\mathbb{K}}(f_n)$. By definition, $\exists i : C = \mathbb{V}_{\mathbb{K}}(f_i)$.
Now let $C = \mathbb{V}_{\mathbb{K}}(p)$ where p is irreducible and suppose for a contradiction that C is reducible, i.e. $\exists p_1, p_2 : \mathbb{V}_{\mathbb{K}}(p) = \mathbb{V}_{\mathbb{K}}(p_1) \cup \mathbb{V}_{\mathbb{K}}(p_2) = \mathbb{V}_{\mathbb{K}}(p_1 p_2)$. But by 1.2.6, $p \mid p_1 p_2$, so WLOG $p \mid p_1$, so by 1.2.5 $\mathbb{V}_{\mathbb{K}}(p) \subset \mathbb{V}_{\mathbb{K}}(p_1) \subset \mathbb{V}_{\mathbb{K}}(p)$, hence $\mathbb{V}_{\mathbb{K}}(p) = \mathbb{V}_{\mathbb{K}}(p_1)$, i.e. C is irreducible. □

Theorem 1.2.9. For any affine algebraic set $\mathbb{V} \subset \mathbb{K}^n$, there are unique irreducible affine algebraic sets $\mathbb{V}_1, \ldots, \mathbb{V}_k$: $\mathbb{V} = \bigcup_{i=1}^{k} \mathbb{V}_i$ and $\mathbb{V}_i \not\subset \mathbb{V}_j \ \forall i \neq j$. The $\mathbb{V}_i$'s are called *irreducible components* of $\mathbb{V}$.

Proof. For existence, we prove that the set

$$\mathcal{F} := \{\text{affine algebraic sets } \mathbb{V} \subset \mathbb{K}^n : \mathbb{V} \text{ is not the union of a finite number of irreducible affine algebraic sets}\}$$

is empty. For a contradiction, suppose $\mathbb{V} \in \mathcal{F}$ and it's minimal with respect to inclusion. First note that $\mathbb{V}$ is reducible, so one can write $\mathbb{V} = \mathbb{V}_1 \cup \mathbb{V}_2$ where $\mathbb{V}_1, \mathbb{V}_2$ are affine algebraic, but then $\mathbb{V}_1, \mathbb{V}_2 \subset \mathbb{V}$ so by assumption $\mathbb{V}_1, \mathbb{V}_2 \notin \mathbb{F}$, i.e. $\mathbb{V}_1 = \cup_i \mathbb{V}_{1i}, \mathbb{V}_2 = \cup_j \mathbb{V}_{2j}$, but then $\mathbb{V}$ is union of these.
For the condition $\mathbb{V}_i \not\subset \mathbb{V}_j \ \forall i \neq j$ one simply needs to remove the redundant components by inclusion. It remains to show that two decompositions are the same up to reordering. Write

$$\mathbb{V} = \mathbb{V}_1 \cup \cdots \cup \mathbb{V}_k = \mathbb{W}_1 \cup \cdots \mathbb{W}_{k'}$$

then

$$\mathbb{V}_i = (\mathbb{V}_i \cap \mathbb{W}_1) \cup \cdots \cup (\mathbb{V}_i \cap \mathbb{W}_{k'})$$

which is irreducible, so $\mathbb{V}_i = \mathbb{V}_i \cap \mathbb{W}_{j(i)}$ for some $j(i)$, i.e. $\mathbb{V}_i \subset \mathbb{W}_{j(i)}$. But the argument is symmetrical, so $\mathbb{W}_{j(i)} \subset \mathbb{V}_k$ for some k, but since we got rid of redundant components, it must be $\mathbb{V}_i = \mathbb{V}_k$ and in particular $\mathbb{V}_i = \mathbb{W}_{j(i)}$. □

Corollary 1.2.10. Write $p = p_1^{d_1} \cdots p_n^{d_n} \in \mathbb{K}[x, y]$ where p_i are irreducible and $\mathbb{C} = \mathbb{V}_{\mathbb{K}}(p)$, then

1. $C = \mathbb{V}_{\mathbb{K}}(p_1) \cup \cdots \cup \mathbb{V}_{\mathbb{K}}(p_n)$, and
2. if $C = C_1 \cup \cdots \cup C_k$ is the irreducible decomposition of C, then (up to reordering) $C_i = \mathbb{V}_{\mathbb{K}}(p_i)$ and $k = n$.

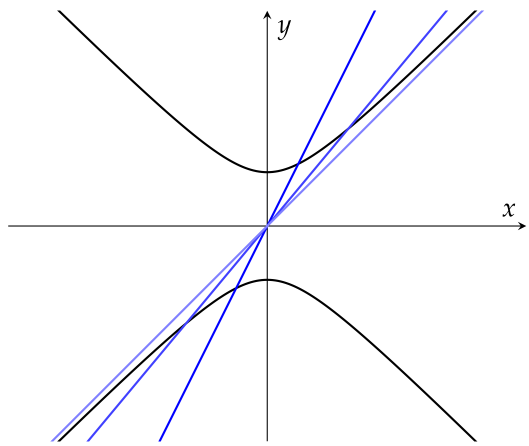
Corollary 1.2.11. If each of the irreducible decompositions of $f, g \in \mathbb{K}[x, y]$ has no repeated factors, then $\mathbb{V}_{\mathbb{K}}(f) = \mathbb{V}_{\mathbb{K}}(g) \iff f = \lambda g$ for some $\lambda \in \mathbb{K}$.

Week 2, lecture 3, 11th October

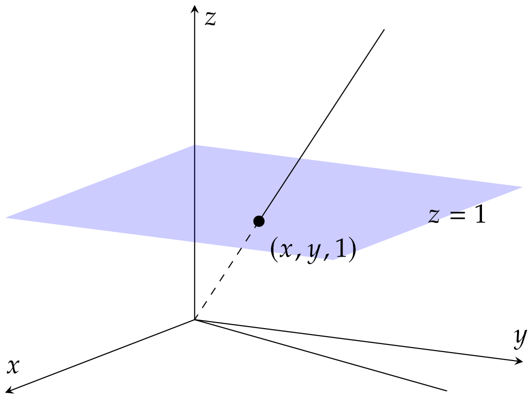
2 Projective variety

2.1 Motivation, definitions, basic results

The motivation to define projective things is we want things to be compact (in the usual Euclidean topology): consider intersection of curves $y^2 = x^2 + 1$ and $y = \alpha x$. If $\alpha \neq \pm 1$ one always has exactly two intersections, but if $\alpha = \pm 1$ the line is asymptotic so we don't have intersection – that is, if we don't consider points at infinity.



But how do we formalise "points at infinity"? That's where the word "projective" comes in.



For any point $(x, y) \in \mathbb{K}^2$, one can "project" it to the $z = 1$ plane to get a unique point $(x, y, 1)$ in the way shown above. One then consider points as lines, more speicifcally 1-dimensional subspaces. The points at infinity have z-coordinate 0, i.e. the line connecting origin and the projected point is entirely in the xy-plane so they don't reach the $z = 1$ plane.

Definition 2.1.1. The n-dimensional *projective space*, denoted by $\mathbb{P}^n$ (or more specifically $\mathbb{P}^n(\mathbb{K})$) is $\mathbb{K}^{n+1}\backslash\{0\}$ modulo the equivalence relation $p \sim q \iff p = \lambda q$ for some $\lambda \in \mathbb{K}$. An element of $\mathbb{P}^n$ is written as $[x_0, \ldots, x_n]$, which is the equivalence class for $(x_0, \ldots, x_n)$.
One equips $\mathbb{P}^n$ with the quotient topology: $U \subset \mathbb{P}^n$ is open if $\{x \in \mathbb{K}^{n+1}\backslash\{0\} : x \sim u$ for some $u \in U\}$ is open.

Example 2.1.2. $\mathbb{P}^0$ is a point, $\mathbb{P}^1$ can be understood as $\mathbb{K} \cup \mathbb{P}^0$ (the lines $y = ax$ where a is allowed to be ∞ (the y-axis)).

Remark 2.1.3. We claim $U_j := \{[x_0, \ldots, x_n] : x_j \neq 0\} \subset \mathbb{P}^n$ (the *affine charts* in manifold language) is homeomorphic to $\mathbb{K}^n$. The map φ defined by

$$\varphi : U_j \longrightarrow \mathbb{K}^n : [x_0, \ldots, x_n] \mapsto \left(\frac{x_0}{x_j}, \ldots, \frac{x_{j-1}}{x_j}, \frac{x_{j+1}}{x_j}, \ldots, \frac{x_n}{x_j}\right)$$
$$\varphi^{-1} : \mathbb{K}^n \longrightarrow U_j : (y_1, \ldots, y_n) \mapsto [y_1, \ldots, y_j, 1, y_{j+1}, \ldots, y_n]$$

is indeed bijective, and since $\mathbb{P}^n$ is equipped with quotient topology inherited from $\mathbb{K}^{n+1} \supset \mathbb{K}^n$ one has that φ preserves open sets as well, i.e. it's homeomorphic.
Now note that $\mathbb{P}^n = \bigcup_{j=0}^n U_j$, so one can understand $\mathbb{P}^n$ as $n+1$ copies of $\mathbb{K}^n$. One can also think of $\mathbb{P}^n$ as $\mathbb{K}^n \cup \mathbb{P}^{n-1}$, where $\mathbb{K}^n$ corresponds to the $x_n \neq 0$ part and $\mathbb{P}^{n-1}$ corresponds to the $x_n = 0$ part (see image above).

Remark 2.1.4. Let $\mathbb{K} = \mathbb{C}$. Define

$$S^{2n+1} := \{(x_0, \ldots, x_n) \in \mathbb{C}^{n+1} \cong \mathbb{R}^{2n+2} : |x_0|^2 + \cdots + |x_n|^2 = 1\}$$

and

$$\pi : S^{2n+1} \longrightarrow \mathbb{P}^n(\mathbb{C}) : (x_0, \ldots, x_n) \mapsto [x_0, \ldots, x_n].$$

The preimage of $[x_0, \ldots, x_n]$ is then $\{(\lambda x_0, \ldots, \lambda x_n) \in S^{2n+1}\}$.
The map is clearly surjective and, similar to previous remark, continuous. We've shown $\mathbb{P}^n(\mathbb{C})$ is compact since S^{2n+1} is compact (closed and bounded) by Heine–Borel. It's also Hausdorff.

Week 3, lecture 1, 14th October

To make sense of polynomials over $\mathbb{P}^n$, we need to characterise polynomials satisfying that if $(x_0, \ldots, x_n)$ is a solution then $(\lambda x_0, \ldots, \lambda x_n)$ is also a solution for any $\lambda \in \mathbb{K}$.

Definition 2.1.5. A polynomial $f \in \mathbb{K}[x_0, \ldots, x_n]$ is *homogeneous* of degree d if

$$f(\lambda x_0, \ldots, \lambda x_0) = \lambda^d f(x_0, \ldots, x_n) \qquad \forall \lambda \in \mathbb{K}, (x_0, \ldots, x_n) \in \mathbb{K}^{n+1}.$$

Remark 2.1.6. Observe that monomial $f = cx_0^{e_0}\cdots x_n^{e_n}$ is homogeneous of degree $\sum_{i=0}^n e_i$. We claim any homogeneous polynomial is a sum of monomials of the same degree. Indeed, for any $f \in \mathbb{K}[x_0,\dots,x_n]$ with degree d one can write $f = f_d + f_{d-1} + \cdots + f_0$ where f_i only contain monomials of degree i. Then f is homogeneous of degree $d \iff f = f_d$. It's clear that $f = f_d \implies f$ is homogeneous by the observation. Now if f is homogeneous then

$$\begin{aligned} f(\lambda x_0,\dots,\lambda x_n) &= \lambda^d f_d(x_0,\dots,x_n) + \lambda^d f_{d'<d}(x_0,\dots,x_n) && \text{by definition of homogeneous}\\ &= \lambda^d f_d(x_0,\dots,x_n) + \lambda^{d-1} f_{d-1}(x_0,\dots,x_n) + \cdots + \lambda f_1(x_0+\cdots+x_n) + f_0 && \text{by calculation,} \end{aligned}$$

so it must e $f_{d'<d} = 0$.
Also a key observation is that if $p = gh$ is homogeneous then g, h are homogeneous, which can be proved easily by contradiction.

Lemma 2.1.7. If $f \in \mathbb{K}[x_0,\dots,x_n]$ is homogeneous then the set

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

is well-defined.

Proof. It suffices to show that the set does not depend the choice of representative $(x_0,\dots,x_n)$ of $[x_0,\dots,x_n]$, i.e. if $p \sim q$ and $f(p) = 0$ then $f(q) = 0$, but this is clear:

$$f(x_0,\dots,x_n) = 0 \implies f(\lambda x_0,\dots,\lambda x_n) = \lambda^d f(x_0,\dots,x_n) = \lambda^d 0 = 0.$$

□

Definition 2.1.8. A *projective variety* is a set $\mathbb{V} \subset \mathbb{P}^n(\mathbb{K})$ that can be written as

$$\mathbb{V} = \{[x_0,\dots,x_n] \in \mathbb{P}^n : f_1(x_0,\dots,x_n) = \cdots = f_k(x_0,\dots,x_n) = 0\}$$

where f_i's are homogeneous.

Proposition 2.1.9. Let $\mathbb{K}$ be algebraically closed and $f \in \mathbb{K}[x,y]$ homogeneous of degree d, then one can write $f(x,y) = \prod_{i=1}^d (a_i x + b_i y)$ where a_i, b_i not both 0, and $\mathbb{P}^1 \supset \mathbb{V}(f) = \{[-b_1,a_1],\dots,[-b_d,a_d]\}$.

Proof. Write $f = y^{d-e}g(x,y)$ where g is homogeneous of degree e and $y \nmid g(x,y)$. Write

$$\begin{aligned} g(x,y) &= c_e x^e + c_{e-1}x^{e-1}y + \cdots + c_0 y^e && \text{where } c_e \neq 0\\ &= y^e c_e\left(\left(\frac{x}{y}\right)^e + \frac{c_{e-1}}{c_e}\left(\frac{x}{y}\right)^{e-1} + \cdots + \frac{c_0}{c_e}\right)\\ &= y^e c_e \prod_{i=1}^e \left(\frac{x}{y} - t_i\right) && \text{for some } t_i \in \mathbb{K} \text{ since } \mathbb{K} \text{ is algebraically closed}\\ &= c_e \prod_{i=1}^e (x - t_i y). \end{aligned}$$

□

So projective varieties in $\mathbb{P}^1$ are not so interesting after all. To have curves we need to go one dimension higher.

Definition 2.1.10. A *projective plane curve* of degree $d > 0$ is a set of the form

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

where p is nonconstant and homogeneous of degree d.

Week 3, lecture 2, 14th October

One can define irreducibility similar for projective plane curves to 1.2.7 and analogously one has:

Proposition 2.1.11. If $\mathbb{K}$ is algebraically closed and $C \subset \mathbb{P}^2(\mathbb{K})$ is a projective plane curve, then

1. C has infinitely many points. (cf. 1.1.15)

2. C is irreducible $\iff C = \{p = 0\}$ for some irreducible homogeneous polynomial p. (cf. 1.2.8)

3. If $p, q \in \mathbb{K}[x, y, z]$ are irreducible homogeneous polynomials, then $\{p = 0\} = \{q = 0\} \iff p = \lambda q$ for some $\lambda \in \mathbb{K}$ (cf. 1.2.11)

4. If $p = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ where p_i's are irreducible, then the irreducible components of $C = \{p = 0\}$ are precisely $\{p_i = 0\}$. (cf. 1.2.10)

Proposition 2.1.12. Let $C \subset \mathbb{P}^2(\mathbb{C})$ be a projective plane curve. Then C is compact.

This is the key motivation/expectation when we defined projective spaces.

Proof. $\mathbb{P}^2(\mathbb{C})$ is compact by 2.1.4, and $C \subset \mathbb{P}^2(\mathbb{C})$ is closed since its preimage in $\mathbb{C}^3 \backslash \{0\}$ with respect to the natural quotient map is closed (since it's a preimage of a closed set of a continuous function, see 1.1.11), but any closed subset of a compact space is compact. □

2.2 Projective plane curves – affine plane curves

Again, per 2.1.3, consider $\mathbb{P}^2$ as $\{x \neq 0\} \cup \{y \neq 0\} \cup \{z \neq 0\}$, and every point $(x, y) \in \mathbb{K}^2$ corresponds uniquely to the point $[x, y, 1]$ in $\mathbb{P}^2$, i.e. the unique point where the line defined by $(0, 0, 0)$ and $(x, y, 1)$ intersects with the $z = 1$ plane.

For a projective plane curve $\overline{C} = \{p(x, y, z) = 0\}$ where $z \nmid p$ (i.e. the line $\{z = 0\}$ (the "line at infinity", denoted by L_∞) is not fully contained in $\overline{C}$), one can map it to an affine plane curve $C = \{p(x, y, 1) = 0\} \in \mathbb{K}^2$ where now $p \in \mathbb{K}[x, y]$ (since $z \nmid p$, one can make sure this p is nonconstant).

Example 2.2.1. The projective plane curve $\overline{C} = \{xy + z^2 = 0\}$ corresponds to $C = \{xy + 1 = 0\} \subset \mathbb{K}^2$, so it's a hyperbola. But it also has points at infinity, i.e. $\overline{C} \cap L_\infty = \{xy = 0\} = \{[1, 0, 0], [0, 1, 0]\}$.

How does one map an affine plane curve to a projective one? First notce that f may not be homogeneous so one needs to homogenize it, and also a polynomial over $\mathbb{P}^2$ has three variables so we need to add one more. We can do both at the same time.

Lemma 2.2.2. If $f \in \mathbb{K}[x, y]$ is of degree d, then its *homogenization* $F(x, y, z) := z^d f\left(\frac{x}{z}, \frac{y}{z}\right)$ is homogeneous of degree d such that $F(x, y, 1) = f(x, y)$ and $z \nmid F$.

Proof. Any monomial in f is of the form $cx^i y^j$ where $i + j \leq d$, which is homogenized to $z^d c \left(\frac{x}{z}\right)^i \left(\frac{y}{z}\right)^j = cz^{d-i-j} x^i y^j$, indeed a monomial in $\mathbb{K}[x, y, z]$ with degree $d - i - j + i + j = d$. Since $\deg f = d$, there is a homogenized monomial $cx^i y^j$ where $i + j = d$, so $z \nmid F$. □

We can now map $C = \{0 = f \in \mathbb{K}[x, y]\} \subset \mathbb{K}^2$ to $\overline{C} = \{F[x, y, z] = 0\}$ where F is the homogenization of f. We claim

Theorem 2.2.3. The map

$$\begin{aligned} \phi : \{\text{projective plane curves not containing } \{z = 0\}\} &\to \{\text{affine plane curves}\} \\ \overline{C} = \{p(x, y, z) = 0\} \subset \mathbb{P}^2(\mathbb{K}) &\mapsto C = \{p(x, y, 1) = 0\} \subset \mathbb{K}^2 \end{aligned}$$

is bijective with the inverse

$$\begin{aligned} \psi : \{\text{affine plane curves}\} &\to \{\text{projective plane curves not containing } \{z = 0\}\} \\ C = \{f(x, y) = 0\} \subset \mathbb{K}^2 &\mapsto \overline{C} = \{F(x, y, z) = 0\} \subset \mathbb{P}^2(\mathbb{K}) \end{aligned}$$

Proof. It suffices to see that $F(x, y, 1) = f(x, y)$ which follows from the lemma above. □

Of course this bijection is not unique, we chose in particular the $z = 1$ hyperplane.

Week 3, lecture 3, 18th October: example/exericse class

Week 4, lecture 1, 21st October

We mentioned "points at infinity" many times and let's now formalise it.

Definition 2.2.4. Let C be an affine plane curve. The *points at infinity* of C is the set $\overline{C} \cap L_\infty$.

Proposition 2.2.5. There is a bijection

$$\begin{aligned}\overline{C} \cap L_\infty &\leftrightarrow \{[x,y] \in \mathbb{P}^1 : f_d(x,y) = 0\}\\ [x,y,0] &\mapsto [x,y]\end{aligned}$$

where f_d is the homogeneous of degree d part of f.

Proof. Let $C = \{f(x,y) = 0\} \subset \mathbb{K}^2$ where $\deg f = d$. Then one can write $f = f_d + f_{d-1} + \cdots + f_0$ where each f_i is homogeneous of degree i. Then

$$F(x,y,z) = f_d(x,y) + z f_{d-1}(x,y) + \cdots + z^d f_0(x,y).$$

Hence

$$\overline{C} \cap L_\infty = \{F(x,y,z) = 0\} \cap \{z = 0\} = \{F(x,y,0) = 0\} = \{[x,y,0] : f_d(x,y) = 0\}.$$

□

Example 2.2.6. Consider $C = \mathbb{V}_{\mathbb{K}}(f)$ where $f(x,y) = x^3 + xy^2 + xy + \cdots$. Then $\overline{C} \cap L_\infty = \{[x,y,0] \in \mathbb{P}^1 : x^3 + xy^2 = 0\} = \{[0,1,0], [i,-1,0], [i,1,0]\}$.

From now on we asuume our polynomials have no repeated factors, i.e. if $F = f_1^{\alpha_1} \cdots f_n^{\alpha_n}$ where each f_i is irreducible then each $\alpha_i = 1$.

3 Singular point, smooth curve

Recall in real analysis one has

Theorem 3.0.1 (Special case of implicit function theorem)**.** Let $F : \mathbb{R}^2 \to \mathbb{R}$ be a smooth (i.e. infinitely differentiable) function with $F(a,b) = 0$ and $\frac{\partial F}{\partial y}(a,b) \neq 0$. Then $\exists \delta, \varepsilon > 0$ such that $\forall x$ in the box

$$\beta = \{(x,y) \in \mathbb{R}^2 : |x - a| < \delta, |y - b| < \varepsilon\}$$

$\exists! y$ in the box such that $F(x,y) = 0$.
This correspondence gives a smooth function f over $|x - a| < \delta$ such that $F(x,y) = 0$ for $(x,y) \in \beta \iff y = f(x)$. In plain English, the theorem says a smooth curve is locally the graph of a smooth function.

Proof. WLOG assume $\frac{\partial F}{\partial y}(a,b) > 0$. Than F is increasing in y in a small enough neighbourhood of (a,b), i.e. $\exists \delta_1, \varepsilon_1 > 0 : \frac{\partial F}{\partial y}(x,y) > 0\ \forall x, y : |x - a| < \delta_1, |y - b| < \varepsilon_1$. Hence by continuity of F, $\exists \delta, \varepsilon : |x - a| < \delta \implies F(x, b + \varepsilon) > 0$ and $F(x, b - \varepsilon) < 0$. But then the intermediate value theorem says $\forall x : |x - a| < \delta$, $\exists! y : |y - b| < \varepsilon$ and $F(x,y) = 0$. □

Definition 3.0.2. Let $C = \{f(x,y) = 0\} \subset \mathbb{K}^2$ be an affine plane curve. C is *smooth* at $(a,b) \in C$ if

$$\left(\frac{\partial f}{\partial x}(a,b), \frac{\partial f}{\partial y}(a,b)\right) \neq (0,0).$$

Otherwise the point is *singular*, or a *singularity*.

One can therefore write the down the set of singular points of $C = \mathbb{V}_{\mathbb{K}}(f)$ as $\mathbb{V}_{\mathbb{K}}\left(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right)$.

C is a *smooth curve* if C is smooth at every $(a,b) \in C$.

For a smooth point $p \in C$, one can define its *tangent line* by

$$T_p C = \left\{\frac{\partial f}{\partial x}(a,b)(x - a) + \frac{\partial f}{\partial y}(a,b)(y - b) = 0\right\}$$

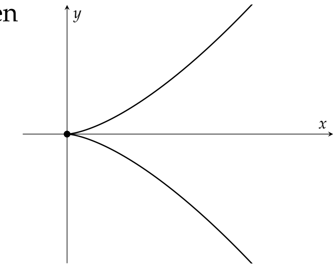
Example 3.0.3. Any affine line $\mathbb{V}_{\mathbb{K}}(f = ax + by + c)$ is smooth; since $ax + by + c$ is nonconstant, either $a = \frac{\partial f}{\partial x}$ or $b = \frac{\partial f}{\partial y}$ is nonzero.

Definition 3.0.4. A *nodal* singularity is where two smooth irreducible components intersect. We'll later see a proof of why we don't have to specifiy anything about partial derivatives.

Example 3.0.5. The curve $\{xy = 0\} = \{x = 0\} \cup \{y = 0\}$ has a nodal singularity at $(0, 0)$.

Week 4, lecture 2, 21st October

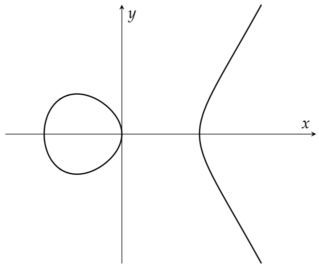
Definition 3.0.6. A *cusp* singularity is a sharp point of a curve where there's a sudden change in direction.



Example 3.0.7. The curve $C = \{f = y^2 - x^3 = 0\}$ has a singularity where

$$\frac{\partial f}{\partial x} = 3x^2 = \frac{\partial f}{\partial y} = 2y = y^2 - x^3 = 0,$$

so $(0, 0)$ is singular, which is a cusp as evident on the right.



Example 3.0.8. The *elliptic* curve $C = \{y^2 - x^3 + x = 0\}$ has singularity where

$$\frac{\partial f}{\partial x} = -3x^2 + 1 = \frac{\partial f}{\partial y} = 2y = y^2 - x^3 + x = 0,$$

which has no solutions, hence C is smooth.

Remark 3.0.9. Suppose $f = g^2 h \in \mathbb{K}[x, y]$. Then by chain rule and product rule

$$\frac{\partial f}{\partial x} = 2gh\frac{\partial g}{\partial x} + g^2\frac{\partial h}{\partial x}, \qquad \frac{\partial f}{\partial y} = 2gh\frac{\partial g}{\partial y} + g^2\frac{\partial h}{\partial y},$$

so $\{g = 0\} \subset \{\text{singularites of } f\}$, but then every point of $\{f = 0\}$ is singular, a strange behaviour. This is why we are assuming our polynomials have no repeated factors.

Definition 3.0.10. Suppose $\operatorname{char} \mathbb{K} = 0$. A projective plane curve $C = \{F(x, y, z) = 0\} \subset \mathbb{P}^2(\mathbb{K})$ is *singular* at $[a, b, c]$ if

$$\frac{\partial F}{\partial x}(a, b, c) = \frac{\partial F}{\partial y}(a, b, c) = \frac{\partial F}{\partial z}(a, b, c) = 0.$$

Otherwise the point is *smooth*.

Example 3.0.11. $C = \{F = x^d + y^d + z^d = 0\} \subset \mathbb{P}^2$ is smooth since $\frac{\partial F}{\partial x} = \frac{\partial F}{\partial y} = \frac{\partial F}{\partial z} = 0$ only at $(0, 0, 0)$, but this is not a point in $\mathbb{P}^2$.

Note that unlike the affine case, we didn't have to specify that $[a, b, c] \in C$, since $\operatorname{char} \mathbb{K} = 0$ implies that as long as the partial deriatives are zero, the point automatically lies on the curve:

Proposition 3.0.12 (Euler's identity)**.** Let $F \in \mathbb{K}[x_0, \dots, x_n]$ be homogeneous of degree d. Then

$$\sum_{i=0}^{n} x_i \frac{\partial F}{\partial x_i} = dF.$$

In particular, if $d \neq 0$ in $\mathbb{K}$ (e.g. if $\operatorname{char} \mathbb{K} = 0$) and $\frac{\partial F}{\partial x_i}(a_0, \dots, a_n) = 0 \ \forall i$, then $F(a_0, \dots, a_n) = 0$.

Proof 1. It suffices to show for a monimial $F = x_0^{i_0} \cdots x_n^{i_n}$ since a homogeneous polynomial is a sum of monomials of the same degree and one can extend the result linearly. But then

$$x_0 i_0 x_0^{i_0 - 1} x_1^{i_1} \cdots x_n^{i_n} + \cdots + x_n x_0 \cdots i_n x_n^{i_n - 1} = i_0 F + \cdots + i_n F = dF$$

as desired. □

Proof 2. Alternatively, by definition of homogeneous

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

Treat λ as a variable and differentiate both sides with respect to it:

$$\sum_{i=0}^{n} x_i \frac{\partial F}{\partial x_i}(\lambda x_0, \ldots, \lambda x_n) = d\lambda^{d-1} F(x_0, \ldots, x_n),$$

and setting $\lambda = 1$ gives the desired. □

Proposition 3.0.13. Let $\overline{C} \subset \mathbb{P}^2(\mathbb{K})$ be the projectivisation of an affine curve $C \subset \mathbb{K}^2$. Then $(a, b) \in C$ is singular $\iff [a, b, 1] \in \overline{C}$ is singular.

Proof. Since $f(x, y) = F(x, y, 1)$, clearly

$$\frac{\partial F}{\partial x}(a, b, 1) = \frac{\partial f}{\partial x}(a, b) \quad \text{and} \quad \frac{\partial F}{\partial y}(a, b, 1) = \frac{\partial f}{\partial y}(a, b),$$

so $[a, b, 1] \in \overline{C}$ is singular $\implies (a, b) \in C$ is singular. Conversely, if $(a, b) \in C$ is singular, then $[a, b, 1] \in \overline{C}$ and by above $\frac{\partial F}{\partial x}(a, b, 1) = \frac{\partial F}{\partial y}(a, b, 1) = 0$ so by 3.0.12

$$\frac{\partial F}{\partial z}(a, b, 1) = dF(a, b, 1) - a\frac{\partial F}{\partial x}(a, b, 1) - b\frac{\partial F}{\partial y}(a, b, 1) = 0.$$

□

One can therefore consider tangent lines (planes in $\mathbb{K}^3$) of projective plane curves:

$$T_p\overline{C} = \left\{ \frac{\partial F}{\partial x}(a, b, c)(x - a) + \frac{\partial F}{\partial y}(a, b, c)(y - b) + \frac{\partial F}{\partial z}(a, b, c)(z - c) = 0 \right\},$$

where the polynomial is indeed homogeneous again by 3.0.12.

Proposition 3.0.14. Let C be a projective plane curve over an algebraically closed field $\mathbb{K}$ and C_1, C_2 be two different irreducible components with $[a, b, c] \in C_1 \cap C_2$. Then C is singular at $[a, b, c]$.

Proof. By 2.1.11, one can write $C_1 = \{f_1 = 0\}, C_2 = \{f_2 = 0\}$ and $f = f_1 f_2 g$ where f_1, f_2 are irreducible. Then

$$\frac{\partial F}{x_i} = \frac{\partial f_1}{x_i} f_1 f_2 g + f_1 \frac{\partial f_2}{x_i} + f_1 f_2 \frac{\partial g}{x_i} \quad \forall i$$

which is 0 at $[a, b, c]$ since $f_1(a, b, c) = f_2(a, b, c) = 0$. □

Corollary 3.0.15. If $\mathbb{K}$ is algebraically closed, then a smooth projective plane curve must be irreducible.

This follows from Bézout's theorem, which we will later encounter and prove.

Theorem 3.0.16. Let $C = \{F(x, y, z) = 0\} \subset \mathbb{P}^2(\mathbb{C})$ be a smooth projective plane curve. Then C is a compact Riemann surface (a smooth complex manifold of complex dimension 1).

Week 4, lecture 3, 25th October

4 Bézout theorem

4.1 Projective transformation

Lemma 4.1.1. For $A \in \mathrm{GL}_{n+1}(\mathbb{K})$, there is a bijection $\phi_A : \mathbb{P}^n \to \mathbb{P}^n : [x_0, \ldots, x_n] \mapsto A \begin{bmatrix} x_0 \\ \vdots \\ x_n \end{bmatrix}$.

Proof. First ϕ_A is well-defined: it's clear that $A \begin{bmatrix} x_0 \\ \vdots \\ x_n \end{bmatrix}$ is never zero, and $\phi_A(\lambda p) = \lambda\phi_A(p) \sim \phi_A(p)$. The bijectivity follows immediately from A is invertible. □

Remark 4.1.2. Note that ϕ_A is continuous: a map $f : \mathbb{P}^n \to X$ is continuous $\iff$ $f \circ \pi : \mathbb{C}^{n+1}\backslash\{0\} \to X$ is continuous where $\pi : \mathbb{C}^{n+1}\backslash\{0\} \to \mathbb{P}^n$ is the natural quotient map (which is by definition continuous).

Definition 4.1.3. A *projective transformation* $\phi : \mathbb{P}^n \to \mathbb{P}^n$ is $\phi = \phi_A$ for some $A \in \mathrm{GL}_{n+1}(\mathbb{K})$, which form the projective general linear group PGL_{n+1}.

Remark 4.1.4. Note that $\phi_A = \mathrm{id}_{\mathbb{P}^n} \iff A = \lambda I_{n+1}$, i.e. $\mathrm{PGL}_{n+1} \cong \mathrm{GL}_{n+1}(\mathbb{K})/\{\lambda I\}$, so one can view PGL_{n+1} as the group of equivalence classes: $A \sim B \iff A = \lambda B$ for some $\lambda \in \mathbb{K}$.

Example 4.1.5 (Möbius transformation). $f : \mathbb{C} \to \mathbb{C} : z \mapsto \frac{az+b}{cz+d}$ where $ad - bc \neq 0$. One can extend it to infinity: $\overline{f}(\infty) = \frac{a}{c}$. But $\mathbb{C} \cup \{\infty\}$ is $\mathbb{P}_1$ (recall 2.1.2), so $\overline{f}$ defines a projective transformation $\mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C}) : [x, y] \mapsto \left[ax + by, cx + dy\right]$, where the matrix can be written: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Remark 4.1.6. There is a explicit Möbius transformation that sends any three distinct points $w_1, w_2, w_3 \in \mathbb{C}$ to $0, 1, \infty$:

$$f(z) = \frac{z - w_1}{z - w_3}\frac{w_2 - w_3}{w_2 - w_1}.$$

Lemma 4.1.7. Given three distinct $w_1, w_2, w_3 \in \mathbb{P}_1$, $\exists!$ projective transformation $\phi : w_1 \mapsto [0, 1], w_2 \mapsto [1, 1], w_3 \mapsto [1, 0]$.

Proof. Write $w_i = [a_i, b_i]$ and define

$$\begin{aligned} \phi : [x, y] \mapsto & \left[\left(\frac{x}{y} - \frac{a_1}{b_1}\right)\left(\frac{a_2}{b_2} - \frac{a_3}{b_3}\right), \left(\frac{x}{y} - \frac{a_3}{b_3}\right)\left(\frac{a_2}{b_2} - \frac{a_1}{b_1}\right)\right] \\ &= [(b_1 x - a_1 y)(a_2 b_3 - a_3 b_2), (b_3 x - a_3 y)(a_2 b_1 - a_1 b_2)] \end{aligned}$$

Now suppose ϕ, ϕ' are two such projective transformations. We want to show $\phi \circ \phi'^{-1} = \lambda I_2$ for some $\lambda \in \mathbb{K}$. Note that $\phi \circ \phi'^{-1} : [0, 1] \mapsto [0, 1], [1, 0] \mapsto [1, 0]$ and $[1, 1] \mapsto [1, 1]$, so the matrix for $\phi \circ \phi'^{-1}$ has eigenvectors $(1, 0)$ and $(0, 1)$, which means the whole $\mathbb{K}^2$ is the eigenspace. □

Proposition 4.1.8. If no three of $w_1, w_2, w_3, w_4 \in \mathbb{P}^2$ are colinear, i.e. writing $w_i = [x_i, y_i, z_i]$ one has $\begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix} \neq 0$ (geometrically, the three in points in $\mathbb{K}^3$ are not on the same plane), then $\exists!$ projective transformation $\phi_A : \mathbb{P}^2 \to \mathbb{P}^2 : w_1 \mapsto [1, 0, 0], w_2 \mapsto [0, 1, 0], w_3 \mapsto [0, 0, 1], w_4 \mapsto [1, 1, 1]$.

Proof. To find this transformation, one first maps an arbitrary w_4 to $[1, 1, 1]$, and then maps w_1, w_2, w_3 to $[1, 0, 0], [0, 1, 0], [0, 0, 1]$ in the following way: we first make a map that fixes $[1, 0, 0], [0, 1, 0], [0, 0, 1]$ and sends $[x_4, y_4, z_4]$ to $[1, 1, 1]$ by the matrix

$$C = \begin{pmatrix} \frac{1}{x_4} & 0 & 0 \\ 0 & \frac{1}{y_4} & 0 \\ 0 & 0 & \frac{1}{z_4} \end{pmatrix}$$

(we know $x_4, y_4, z_4 \neq 0$ by the linear indepedency assumption), and clearly the matrix

$$A = \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix},$$

(which we assumed to be invertible) maps $[1, 0, 0], [0, 1, 0], [0, 0, 1]$ to w_1, w_2, w_3 respectively, so one needs only to find its inverse and compose it with C. □

Week 5, lecture 1, 28th October

Proposition 4.1.9. Let $C = \{F(x, y, z) = 0\} \in \mathbb{P}^2(\mathbb{K})$ be a projective plane curve and ϕ_A a projective transformation. Then

1. $\phi_A(C)$ is also a projective plane curve.
2. If C_0 is an irreducible component of C, then $\phi_A(C_0)$ is an irreducible component of $\phi_A(C)$.
3. If $p \in C$ is smooth then $\phi_A(p) \in \phi_A(C)$ is smooth. Moreover, ϕ_A preserves the tangent line, i.e. $\phi_A(T_p C) = T_{\phi_A(p)}\phi_A(C)$. In particular, if C is smooth then $\phi_A(C)$ is smooth.

Proof. Write $B = A^{-1} = (b_{ij})$ and hence $\phi_B = (\phi_A)^{-1}$.

1. Note that
$$\begin{aligned}[x_0, x_1, x_2] \in \phi_A(C) &\iff \phi_B([x_0, x_1, x_2]) \in C \\ &\iff \left[\sum_{i=0}^{2} b_{0i}x_i, \dots, \sum_{i=0}^{2} b_{ni}x_i\right] \in C \\ &\iff F\left(\sum_{i=0}^{2} b_{0i}x_i, \dots, \sum_{i=0}^{2} b_{ni}x_i\right) = 0,\end{aligned}$$
so $\phi_A(C)$ is given by the polynomial $G = F \cdot \phi_B$, which is also homomogeneous of same degree.

2. It suffices to show that if C_0 is irreducible then $\phi_A(C_0)$ is also irreducible since
$$\phi_A(C) = \phi_A(C_0 \cup \cdots \cup C_n) = \phi_A(C_0) \cup \cdot \cup \phi_A(C_n).$$
Indeed,
$$\begin{aligned}x \in \phi_A(C_0 \cup \cdots \cup C_n) &\implies \phi_B x \in C_0 \cup \cdots \cup C_n \implies \phi_B x \in C_i \text{ for some } i \\ &\implies x \in \phi_A(C_i) \implies x \in \phi_A(C_0) \cup \cdots \cup \phi_A(C_n)\end{aligned}$$
If $\phi_A(C_0) = C_1 \cup C_2$, then $C_0 = \phi_B(C_1) \cup \phi_B(C_2)$, so WLOG $C_0 = \phi_B(C_1)$ by assumption, hence $\phi_A(C_0) = C_1$ as desired.

3. Let $p \in \phi_A(C)$ with $\phi_B(p) = q \in C$ smooth. Then by chain rule
$$\begin{aligned}\left[\frac{\partial G}{\partial x_0}(p), \frac{\partial G}{\partial x_1}(p), \frac{\partial G}{\partial x_2}(p)\right] &= \left[\frac{\partial F}{\partial x_0}(\phi_B(p)), \frac{\partial F}{\partial x_1}(\phi_B(p)), \frac{\partial F}{\partial x_2}(\phi_B(p))\right] B \\ &= \left[\frac{\partial F}{\partial x_0}(q), \frac{\partial F}{\partial x_1}(q), \frac{\partial F}{\partial x_2}(q)\right] B \neq 0,\end{aligned}$$
so p is smooth. Now recall
$$T_q C = \left\{\frac{\partial F}{\partial x_0}(q)x_0 + \frac{\partial F}{\partial x_1}(q)x_1 + \frac{\partial F}{\partial x_2}(q)x_2 = 0\right\},$$
so
$$\phi_A(T_q C) = \left\{\frac{\partial F}{\partial x_0}(\phi_B p)\sum_{i=0}^{2} b_{0i}x_i + \frac{\partial F}{\partial x_1}(\phi_B p)\sum_{i=0}^{2} b_{1i}x_i + \frac{\partial F}{\partial x_2}(\phi_B p)\sum_{i=0}^{2} b_{2i}x_i = 0\right\}$$
where the coefficient for x_i is $\frac{\partial G}{\partial x_i}(p)$ again by chain rule.

□

4.2 Resultant

Let R be a UFD (and so $R[x]$ is a UFD) and $f, g \in R[x]$. We introduce an algebraic tool called resultant to tell us when do f, g have common factors.

Lemma 4.2.1. If $f, g \in R[x]$ are of degree $d, e \geq 1$ respectively, then f, g have a non-constant common factor $\iff \exists a, b \in R[x] : a, b \neq 0,\ af + bg = 0$ with $\deg a \leq e - 1,\ \deg b \leq d - 1$.

Proof. $\implies$ Suppose f, g have a non-constant common factor and write $f = hq$ and $g = hr$ where $\deg h \geq 1$ (so $\deg q \leq d - 1$ and $\deg r \leq e - 1$). Then $a = r, b = -q$ satisfy the desired.

$\impliedby$ Write $f = cf_1^{\alpha_1} \cdots f_k^{\alpha_k}$ with $\sum_{i=1}^{k} \alpha_i = d$. Since $R[x]$ is a UFD, in the factorisation of $bg = -af$ one can find $h = f_1^{\beta_1} \cdots f_k^{\beta_k}$ where $\beta_i \geq \alpha_i\ \forall i$. But then $\deg h = \sum_{i=1}^{k} \beta_i \geq d$, so $h \nmid b$ and at least some $f_i^{\gamma_i} \mid g$ where $\gamma_i \geq 1$.

□

Definition/Theorem 4.2.2. Another way to formulate the lemma: if one writes the required a, b in the general form: $a(x) = \alpha_{e-1}x^{e-1} + \cdots + \alpha_0, b(x) = \beta_{d-1}x^{d-1} + \cdots + \beta_0$ then f, g have a non-constant common factor if

$$af + bg = \alpha_{e-1}x^{e-1}f(x) + \cdot + \alpha_0 f(x) + \beta_{d-1}\beta^{d-1}g(x) + \cdots + \beta_0 g(x) = 0$$

for some $\alpha_{e-1}, \ldots, \alpha_0, \beta_{d-1}, \ldots, \beta_0 \in R$ not all zero, i.e. the $d+e$ polynomials $x^{e-1}f(x), \ldots, f(x), b^{d-1}g(x), \ldots, g(x)$ are linearly dependent over R. Now write $f(x) = a_d x^d + \cdots + a_0,\ g(x) = b_e x^e + \cdots + b_0$, then if one writes coefficients of the $d + e$ polynomials of maximum $d + e - 1$ degree (and hence have $d + e$ coefficients) in rows of a $(d + e) \times (d + e)$ matrix

$$\begin{pmatrix} a_d & \cdots & a_0 & & & \\ & a_d & \cdots & a_0 & & \\ & & \ddots & & \ddots & \\ & & & a_d & \cdots & a_0 \\ b_e & \cdots & b_0 & & & \\ & b_e & \cdots & b_0 & & \\ & & \ddots & & \ddots & \\ & & & b_e & \cdots & b_0 \end{pmatrix},$$

and consider its determinant, called the *resultant* of f and g and denoted by $\mathcal{R}_{f,g}$, then the lemma says: f, g have a non-constant common factor $\iff \mathcal{R}_{f,g} = 0$.

Week 5, lecture 2, 28th October

Example 4.2.3. An easy example makes it clear: consider $f(x) = x-a, g(x) = x-b \in R[x]$. Then $\deg f = \deg g = 1$ so one has a 2×2 matrix with

$$\mathcal{R}_{f,g} = \det \begin{pmatrix} 1 & -a \\ 1 & -b \end{pmatrix} = -b + a,$$

so f, g have a common factor $\iff a = b$.

Proposition 4.2.4. If the field of fractions of R has characteristic 0, then $f \in R[x]$ has repeated factors $\iff$ $\mathcal{R}_{f,f'} = 0$.

Proof. $\implies$ Write $f = g^2 h$ where $g, h \in R[x]$ and $\deg g \geq 1$. Then $f' = 2gg'h + g^2h'$, so f, f' have the nonconstant common factor g, so by 4.2.2 one has $\mathcal{R}_{f,f'} = 0$.

$\impliedby$ For any f with $\mathcal{R}_{f,f'} = 0$ and an irreducible factor g of f, write $f = gh$ and $g \mid f'$. Then $f' = g'h + gh'$, so $g \mid f' - gh' = g'h$. But $\deg g' < \deg g$, so $g \nmid g'$ (one can rule out $g' = 0$ since characteristic is 0), hence $g \mid h$ and $g^2 \mid f$.

□

Since this module deals with curves, we are interested in polynomials in more variables.

Proposition 4.2.5. Consider $\mathbb{K}[x, y, z]$ as $\mathbb{K}[y, z][x]$ and let $R = \mathbb{K}[y, z]$. Any homogeneous polynomial $F(x, y, z)$ of degree d can be written as

$$x^d f_0(y, z) + \cdots + f_d(y, z) \in R[x] \qquad \text{where each } f_i \text{ is homogeneous of degree } i.$$

The leading coefficient is $f_0(y, z) = F(1, 0, 0)$. To make sure it has the same degree over $\mathbb{K}$ and R as we would expect, assume $F(1, 0, 0) \neq 0$.

Now similarly write another polynomial $G(x, y, z)$ as $y^e g_0(y, z) + \cdots + g_e(y, z) \in R[x]$ with $g_0(y, z) = G(0, 0, 1) \neq 0$. Then $\mathcal{R}_{FG} \in R$ is well-defined, and we claim: $\exists A, B \in \mathbb{K}[x, y, z] : \deg_x A \leq e - 1, \deg_x B \leq d - 1$ and $\mathcal{R}_{F,G} = AF + BG$.

Moreover, if $\mathcal{R}_{F,G} \neq 0$ then it's homogeneous of degree de (as an element of $\mathbb{K}[y, z]$).

Proof. Write $\mathcal{R}_{F,G} = \det M$ where M is by definition

$$\begin{pmatrix} f_0(y,z) & \cdots & f_d(y,z) & & & \\ & f_0(y,z) & \cdots & f_d(y,z) & & \\ & & \ddots & & \ddots & \\ & & & f_0(y,z) & \cdots & f_d(y,z) \\ g_0(y,z) & \cdots & g_e(y,z) & & & \\ & g_0(y,z) & \cdots & g_e(y,z) & & \\ & & \ddots & & \ddots & \\ & & & g_0(y,z) & \cdots & g_e(y,z) \end{pmatrix}$$

and do the following column operations to get a new matrix N: add $x^{d+e-j}\times$ the jth column to the last $d+e$th column for each j from 1 to $d+e-1$. The last column of N is then

$$\begin{pmatrix} f_0x^{d+e-1}+\cdots+f_dx^{e-1} \\ \vdots \\ f_0x^d+\cdots+f_d \\ g_0x^{d+e-1}+\cdots+g_ex^{d-1} \\ \vdots \\ g_0x^e+\cdots+g_e \end{pmatrix} = \begin{pmatrix} x^{e-1}F \\ \vdots \\ F \\ x^{d-1}G \\ \vdots \\ G \end{pmatrix}.$$

Since column operation doesn't change determinant, $\det N = \mathcal{R}_{F,G}$, which is a R-linear combination of

$$x^{e-1}F,\ldots,F,x^{d-1}G,\ldots,G.$$

This proves $\mathcal{R}_{F,G} = AF+BG$ where A,B satisfy the desired properties.

Now by definition (write $M=(a_{i,j})$)

$$\mathcal{R}_{F,G} = \det M = \sum_{\sigma\in S_{d+e}} (-1)^\sigma a_{1,\sigma(1)}\cdots a_{d+e,\sigma(d+e)},$$

and it remains to see each summand A_σ is homogeneous of degree de. Forget the sign (not relevant considering homogeneity or degree) and split it to two parts: the first e rows (the ones with f) and the last d rows (the ones with g):

$$A_\sigma = \prod_{i=1}^{e} a_{i,\sigma(i)} \prod_{j=e+1}^{d+e} a_{j,\sigma(j)}.$$

Then for $1\le i\le e$, $a_{i,\sigma(i)} = f_{\sigma(i)-i}(y,z)$ which by construction is homogeneous of degree $\sigma(i)-i$, and for $e+1\le j\le d+e$, $a_{j,\sigma(j)} = g_{\sigma(j+e)-j}(y,z)$, homogeneous of degree $\sigma(j+e)-j$. So

$$\begin{aligned}\deg A_\sigma &= \sum_{i=1}^{e}(\sigma(i)-i) + \sum_{j=1}^{d}(\sigma(j+e)-j)\\ &= \sum_{i=1}^{d+e}\sigma(i) - \sum_{i=1}^{d} i - \sum_{i=1}^{e} i\\ &= \frac{(d+e)(d+e+1)}{2} - \frac{e(e+1)}{2} - \frac{d(d+1)}{2}\\ &= \frac{d^2+d(e+1)+de}{2} - \frac{d(d+1)}{2}\\ &= \frac{de+de}{2} = de.\end{aligned}$$

□

Week 5, lecture 3, 1st November

Corollary 4.2.6. $R_{F,G}$ is the zero polynomial $\iff$ F and G share a nonconstant common factor.

Proof. By 4.2.4, $R_{F,G}=0 \iff F,G$ have a nonconstant common factor as polynomials in x, so it remains to ensure that they don't have a common factor that is considered to be "constant" in the ring $R=\mathbb{K}[y,z]$. Suppose that $F(x,y,z)=H(y,z)F'(x,y,z)$. But then $F(1,0,0)\neq 0$ and $H(y,z)=0$ (since any factor of a homogeneous polynomial must be homogeneous, recall 2.1.6), a contradiction.

Conversely it's a more direct application or 4.2.4. □

The above discussion about common factors relies on the a priori restrictive condition that $[1,0,0]$ is not on the curves C_F, C_G, but this turns out to be not restrictive: we claim that for any F,G, one can always find a projective transformation such that $\{F=0\}$ and $\{G=0\}$ do not pass through $[1,0,0]$, by the following lemma.

Lemma 4.2.7. Let $\mathbb{K}$ be algebraically closed and $C_1,\ldots,C_n\in\mathbb{P}^2(\mathbb{K})$ projective plane curves. Then $C_1\cup\cdots\cup C_n$ is a proper subset of $\mathbb{P}^2(\mathbb{K})$.

Proof. If $C_i=\{F_i(X,Y,Z)=0\}$ then $C_1\cup\cdots\cup C_n = \left\{\prod_{i=1}^n F_i(X,Y,Z)=0\right\}$. For a contradiction, suppose $\{x-cy=0\}\subset\left\{\prod_{i=1}^n F_i(X,Y,Z)=0\right\}$ $\forall c\in\mathbb{K}$. This would imply $C_1\cup\cdots\cup C_n=\mathbb{P}^2(\mathbb{K})$. But $\mathbb{K}$ is algebraically closed, so in particular it's infinite, and it's impossible for $\prod_{i=1}^n F_i(X,Y,Z)$ to have infinite irreducible factors, which would follow from our assumption. □

4.3 Proof and applications of the theorem

Theorem 4.3.1 (Weak Bézout)**.** Let $\mathbb{K}$ be algebraically closed and $C, C' \subset \mathbb{P}^2(\mathbb{K})$ two projective plane curves with degree $d \geq 1, e \geq 1$ respectively. Then $C \cap C' \neq \emptyset$ and moreover, either $|C \cap C'| \leq de$ or $C \cap C'$ contains a plane curve.

Proof. Write $C = \{F_d(X, Y, Z) = 0\}$ and $C' = \{G_e(X, Y, Z) = 0\}$, and WLOG assume $[1, 0, 0] \notin C, C'$. Consider $\mathcal{R}_{F,G} \in \mathbb{K}[y, z]$ of degree de.

If $\mathcal{R}_{F,G} = 0$ then F, G have a nonconstant common factor, i.e. $C \cap C' \neq \emptyset$ and contain a plane curve given by the zero set of the common factor.

If $\mathcal{R}_{F,G} \neq 0$, since $\mathbb{K}$ is algebraically closed, one has $a_i, b_i \in \mathbb{K} : \mathcal{R}_{F,G} = \prod_{i=1}^{de}(a_i y + b_i z)$. Now fix $[y_0, z_0]$ and consider $F(x, y_0, z_0), G(x, y_0, z_0) \in \mathbb{K}[x]$. Then they have a common root $\iff$ $\mathcal{R}_{F(x,y_0,z_0),G(x,y_0,z_0)} = 0$, so $\mathcal{R}_{F,G}$ vanishes on $[y_0, z_0]$, i.e. $[y_0, z_0] = [b_i, -a_i]$ for some i. We've proved that for any fix $[y_0, z_0]$, $\exists x_0 : [x_0, y_0, z_0] \in C \cap C' \iff [y_0, z_0] = [b_i, -a_i]$ for some i, so $C \cap C' \neq \emptyset$. It remains to show $|C \cap C'| \leq de$, so suppose $|C \cap C'| > de$ and let $S \subset C \cap C' : |S| = de + 1$. Consider the finite collection of curves

$$\{C, C', \text{lines through any pair of distinct points in } S\},$$

and again WLOG assume none of them passes through $[1, 0, 0]$. Since $|C \cap C'| > de$, we know for some $1 \leq i \leq de$, there are two distinct solutions $[x_0, y_i, z_i], [x_0', y_i, z_i] \in S$, but then the line through them $\{a_i y + b_i z = 0\}$ passes through $[1, 0, 0]$. □

Week 6, lecture 1, 4th November

We have already seen an application of Bézout, which is 3.0.15:

Proof of 3.0.15. Write $C = C_1 \cup C_2$, then C is singular at points in $C_1 \cap C_2$ (3.0.14), which is nonempty by Bézout. □

What about the converse?

Proposition 4.3.2. Let $\mathbb{K}$ be algebraically closed with char $\mathbb{K} = 0$ and $\{F = 0\} = C \subset \mathbb{P}^2(\mathbb{K})$ be irreducible of degree d. Then C has finitely many singular points.

Proof. Since char $\mathbb{K} = 0$, not all partial derivatives are zero, so WLOG assume $\frac{\partial F}{\partial x} \neq 0$. Then the set of singular points of C

$$\operatorname{sing}(C) \subset \left\{[a, b, c] \subset \mathbb{P}^2(\mathbb{K}) : F(a, b, c) = 0, \frac{\partial F}{\partial x}(a, b, c) = 0\right\},$$

and $\gcd\left(F, \frac{\partial F}{\partial x}\right) = 1$ since F is irreducible and $d = \deg F > \deg \frac{\partial F}{\partial x} = d - 1$, so $|\operatorname{sing}(C)| \leq d(d-1)$. □

Definition 4.3.3. A *conic* is a projective plane curve of degree 2. In particular, it's of the form

$$\{F = ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0\} \subset \mathbb{P}^2(\mathbb{K}).$$

Theorem 4.3.4. Let $\mathbb{K}$ be algebraically closed and $C \subset \mathbb{P}^2(\mathbb{K})$ an irreducible conic. Then C is projectively equivalent to $\{x^2 = yz\}$, in particular C is smooth.

Proof. By 4.3.2, $\exists$ a smooth point $P \in C$. Let $q \in T_pC$ be another point. Then we claim $\exists$ a projective transformation ϕ that sends p to $[1, 0, 0]$ and q to $[0, 1, 0]$. We now work with the "nice" curve $\phi(C)$ and replace C with it. Note that now T_pC is the unique line that goes through $[1, 0, 0]$ and $[0, 1, 0]$, which is $\{z = 0\}$ (see coursework 1, question 2). Now $[1, 0, 0] \in C$ implies $a = 0$, and

$$T_pC = \left\{\frac{\partial F}{\partial x}(1, 0, 0)x + \frac{\partial F}{\partial y}(1, 0, 0)y + \frac{\partial F}{\partial z}(1, 0, 0)z\right\} = \left\{by + dz = 0\right\} = \{z = 0\}$$

implies $b = 0$ and $d \neq 0$. Now $c \neq 0$ since if $c = 0$ then $dxz + eyz + fz^2$ is reducible with the factor z. So we now have the polynomial $(\sqrt{c}y)^2 + (dx + ey + fz)z$. After the projective transformation $\sqrt{c}y \mapsto y, dx + ey + fz \mapsto x$ and $z \mapsto -z$ we have the desired form. □

Remark 4.3.5. If $\mathbb{K}$ is algebraically closed and $\{F = 0\} = C \subset \mathbb{P}^2(\mathbb{K})$ is reducible of degree 2, then by definition it must be a union of two lines $L_1 \cup L_2$. If F has no repeated factor, then C is projectively equivalent to $\{x^2 + y^2 = 0\}$.

A motivating question in algebraic geometry is, to uniquely determine a curve, how many points do I need? We already know two points determine a line (again see coursework 1, question 2). Knowing how many points determine a conic is very hard using high school level maths, but it's quite easy now with all the buildup.

Proposition 4.3.6. Any five points in $\mathbb{P}^2(\mathbb{K})$ lie on a conic. If no three of them are colinear, then this conic is unique.

Proof. Write $p_i = [x_i, y_i, z_i] \in \mathbb{P}^2(\mathbb{K})$ for $i = 1, \ldots, 5$, and let $\{F = ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0\} \subset \mathbb{P}^2(\mathbb{K})$ be a conic. By substituting F with the p_i's, we get five linear equations for six variables $a, \ldots, f$, which has at least one nonzero solution.

Now assume no three of them are colinear and for a contradiction, suppose distinct conics C, C' pass through the p_i's. Consider $C, C' \subset \mathbb{P}^2(\overline{\mathbb{K}})$ where $\overline{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$. If we can prove $C = C'$ in $\mathbb{P}^2(\overline{\mathbb{K}})$ then surely $C = C'$ in $\mathbb{P}^2(\mathbb{K})$. Now $p_1, \ldots, p_5 \in C \cap C' \subset \mathbb{P}^2(\overline{\mathbb{K}})$, so by 4.3.1 $C \cap C'$ must contain a plane curve since if it doesn't it contains at most 4 points. Since $C \neq C'$, $C \cap C'$ must be some line L, but this implies p_i's are colinear, contradicting our assumption. □

Week 6, lecture 2, 4th November

Definition 4.3.7. A *cubic* a projective plane curve of degree 3.

Theorem 4.3.8 (Cayley–Bacharach)**.** Let $\mathbb{K}$ be algebraically closed. Suppose two projective plane cubics $C = \{F(x, y, z) = 0\}$, $C' = \{G(x, y, z) = 0\}$ intersect at exactly 9 points $p_1, \ldots, p_9$. If a cubic $C'' \subset \mathbb{P}^2(\mathbb{K})$ passes through $p_1, \ldots, p_8$, then C'' belongs to the *pencil* (2-dimensional family of cubics) $\left\{C_{[a,b]} = \{aF + bG = 0\} : [a, b] \in \mathbb{P}^1\right\}$. In particular, $p_9 \in C''$.

Proof. Let's first understand more about the 9 points, which are intersections of two arbitrary cubics:

1. No four of the p_i's can be colinear: suppose $p_1, \ldots, p_4$ lie on L, in particular $|L \cap C| > 3$, then by 4.3.1 one has $L \cap C$ contains a plane curve, so $L \subset C$, hence similarly $L \subset C'$, but then $L \subset C \cap C'$, contradicting that C and C' intersect at and only at 9 points.

2. No seven of the p_i's lie on the same conic: suppose $p_1, \ldots, p_7$ lie on D, in particular $|L \cap C| > 6$, then by 4.3.1 $C \cap D$ and $C' \cap D$ contain a plane curve. If D is irreducible then $C \cap D = C' \cap D = D$, again a contradiction. If D is reducible, write $D = L \cup \widetilde{L}$, but then one has 7 points on union of two lines, so one of them has at least 4 points, contradicting our first observation.

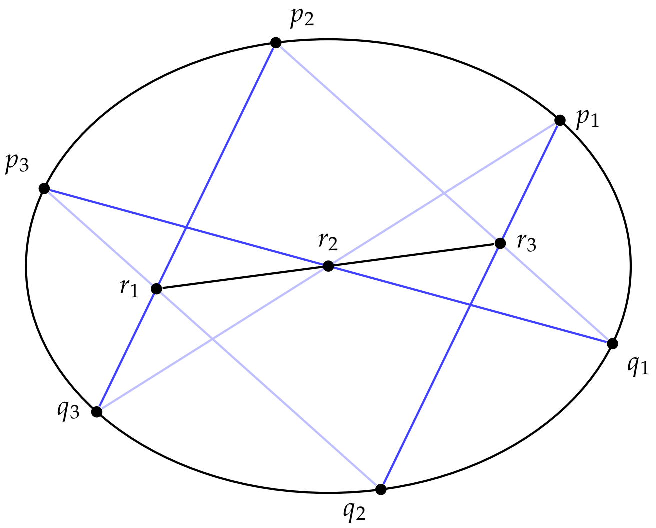
3. Any five of the p_i's determine a unique conic: if no three are colinear, one can use 4.3.6, so suppose $p_1, p_2, p_3 \in L$ for some line L, and let L' be the unique line that goes through $p_4, p_5 \notin L$ (by 1). Then $D = L \cup L'$ is a conic, which we want to prove is unique, so suppose a distinct D' also goes through $p_1, \ldots, p_5$. But $|D \cap D'| > 4$, so $D \cap D'$ must contain a plane curve by 4.3.1, which is either L or L', but if $L \subset D'$ then since $p_4, p_5 \in D'$, one must have $D' = L \cup L'$, and if $L' \subset D'$, then at most one of p_1, p_2, p_3 lies on L' by 1, so WLOG assume $p_1 \in L'$, then D contains the unique line that goes through p_2, p_3, which is L. Hence $D' = L \cup L' = D$.

Now we prove the theorem by contradiction. Suppose $\exists$ a cubic $C'' = \{H = 0\}$ that goes through $p_1, \ldots, p_8$ but H is not a linear combination of F and G. We claim in this case, no three of $p_1, \ldots, p_8$ are colinear. For a contradiction, suppose $p_1, p_2, p_3 \in L$ for some line L. Then by 1, $p_4, \ldots, p_8 \notin L$. By 3, they uniquely determine a conic D. By 2, at most one of p_1, p_2, p_3 lies on D. Let $\widetilde{C} = L \cup D$ be the cubic containing all 8 points.

If $q_1, q_2 \in \mathbb{P}^2(\mathbb{K})$, note that $\exists (a, b, c) \neq (0, 0, 0) : \{P = 0\}$ goes through q_1, q_2 where $P = aF + bG + cH$, since F, G, H are assumed to be linearly independent, so 2 equations gives at least one nonzero solutions to 3 variables. Now choose $q_1 \in L$ with $q_1 \neq p_1, p_2, p_3$ and $q_2 \in \mathbb{P}^2(\mathbb{K}) \backslash \widetilde{C}$. Then $\{P = 0\}$ is distinct from $\widetilde{C}$ by constuction, but this is a contradiction: again, apply 4.3.1 to L and $\{P = 0\}$ to see that $L \subset \{P = 0\}$, so $\{P = 0\} = L \cup D'$ for some conic D', which contains $p_4, \ldots, p_8$, but five points uniquely determine a conic, so $D = D'$ and $\widetilde{C} = \{P = 0\}$. □

Week 6, lecture 3, 8th November

Theorem 4.3.9 (Pascal's)**.** Let $C \subset \mathbb{P}^2$ be a conic and $p_1, p_2, p_3, q_1, q_2, q_3 \in C$ with no three of them colinear. Denote the line that goes through p_i and q_j by L_{ij}, and the intersection point of L_{ij} and L_{ji} where $i \neq j$ by r_{6-i-j} (i.e. the one in $\{1, 2, 3\}$ that's not i or j). Then r_1, r_2, r_3 are colinear.



Proof. Consider the two cubics $L_{12} \cup L_{23} \cup L_{31}$ and $L_{21} \cup L_{32} \cup L_{13}$, which intersect at exactly the 9 points $p_1, p_2, p_3, q_1, q_2, q_3, r_1, r_2, r_3$, and the cubic $C \cup L$ where L is the line that goes through r_1 and r_2, which passes through $p_1, p_2, p_3, q_1, q_2, q_3, r_1, r_2$. Applying Cayley–Bacharach to the three cubics gives us $r_3 \in C \cup L$, so it remains to show $r_3 \notin C$, but this is trivial: if $r_3 \in C$ then $L_{12} \subset C$, but then $C = L_{12} \cup \widetilde{C}$ is a union of two lines, so there must be three of $p_1, p_2, p_3, q_1, q_2, q_3$ being colinear, contradicting assumption. □

Week 7, lecture 1, 11th November

4.4 Resultant, reprise, and a better theorem

Proposition 4.4.1. Let $f, g \in R[x]$ and write $f(x) = a(x-\lambda_1)\cdots(x-\lambda_d)$ and $g(x) = b(x-\mu_1)\cdots(x-\mu_e)$ where $d, e > 0$. Then

$$\mathcal{R}_{f,g} = a^e b^d \prod_{\substack{1\le i\le d\\1\le j\le e}} (\lambda_i - \mu_j) = a^e \prod_{i=1}^{d} g(\lambda_i)$$

Proof. First observe that for any arbitrary $f, g \in R[x]$ and $a, b \in R$, one has $\mathcal{R}_{af,bg} = a^e b^d \mathcal{R}_{f,g}$ by the fact that multiplying one row of the matrix M by λ changes $\det M$ by a factor of λ as well, so it suffices to prove the case where $a = b = 1$.

Consider the ring homomorphism

$$\begin{aligned} \psi : S := R[y_1, \dots, y_d, z_1, \dots, z_e] &\to R \\ y_i &\mapsto \lambda_i \\ z_j &\mapsto \mu_j, \end{aligned}$$

which extends to a homomoprhism $\overline{\psi} : S[x] \to R[x]$, under which $\overline{f} = \prod_{i=1}^{d}(x - y_i)$ is mapped to f and $\overline{g} = \prod_{j=1}^{e}(x - z_j)$ is mapped to g. It's then clear that $\psi\left(\mathcal{R}_{\overline{f},\overline{g}}\right) = \mathcal{R}_{f,g}$.

Now if $y_i - z_j = 0$, then $(x - y_i)$ and $(x - z_j)$ are common factors of $\overline{f}, \overline{g}$, hence $\mathcal{R}_{\overline{f},\overline{g}} = 0$ by 4.2.2. Hence $(y_i - z_j) \mid \mathcal{R}_{\overline{f},\overline{g}}$. Apply this to any pair i, j and compare degrees, one has

$$\mathcal{R}_{\overline{f},\overline{g}} = c \prod_{\substack{1\le i\le d\\1\le j\le e}} (y_i - z_j)$$

for some contant c. Substituting $y_i = 1, z_j = 0$ for all i, j, one has $\overline{f} = (x-1)^d$ and $\overline{g} = x^e$, so

$$c = c(1-0)^{de} = \mathcal{R}_{(x-1)^d, x^e} = \det \left(\begin{array}{c|ccccc} * & (-1)^d & 0 & 0 & \cdots & 0 \\ * & * & (-1)^d & 0 & \cdots & 0 \\ * & * & * & (-1)^d & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & * & \cdots & (-1)^d \\ \hline I_d & 0 & 0 & 0 & \cdots & 0 \end{array}\right),$$

now, moving the last d row to the top requires de exchange of two rows, with the resulting matrix with determinant $1^d \cdot \left((-1)^d\right)^e = (-1)^d e$, so $(-1)^{de} c = (-1)^d e$, i.e. $c = 1$. ◻

Proposition 4.4.2. If $g \in R[x]$ has $\deg g \geq 1$, then $R_{x-c,g(x)} = g(c)$.

Proof. Applying (the second equality of) 4.4.1 one has

$$R_{x-c,g(x)} = \prod_{i=1}^{1} g(c) = g(c).$$

But g may not completely split into linear factors, so it remains to show that resultant is invariant in $\overline{k}$, the algebraic closure of the field of fractions k of R, which is clear. ◻

Proposition 4.4.3. For nonconstant $f, g, h \in R[x]$, $\mathcal{R}_{f,gh} = \mathcal{R}_{f,g}\mathcal{R}_{f,h}$.

Proof. Use the same trick to consider $f, g, h \in \overline{k}[x]$ where $\overline{k}$ is algebraically closed, and write $f(x) = a(x - \lambda_1)\cdots(x - \lambda_d)$, then by 4.4.1

$$\mathcal{R}_{f,gh} = a^{\deg gh} \prod_{i=1}^{d} gh(\lambda_i) = \left(a^{\deg g} \prod_{i=1}^{d} g(\lambda_i)\right)\left(a^{\deg h} \prod_{i=1}^{d} h(\lambda_i)\right) = \mathcal{R}_{f,g}\mathcal{R}_{f,h}.$$

◻

Proposition 4.4.4. For $f, g, h \in R[x]$ such that $f, g, hf + g$ are nonconstant and f is monic, $\mathcal{R}_{f,g} = \mathcal{R}_{f,hf+g}$.

Proof. Again applying 4.4.1 and writing $f = \prod_{i=1}^{d}(x - \lambda_i)$ one has

$$\mathcal{R}_{f,g+hf} = \prod_{i=1}^{d}(hf + g)(\lambda_i) = \prod_{i=1}^{d}(h(\lambda_i)f(\lambda_i) + g(\lambda_i)) = \prod_{i=1}^{d} g(\lambda_i) = \mathcal{R}_{f,g}.$$

◻

Week 7, lecture 2, 11th November

Remark 4.4.5. Consider the curves $C : y = x^2 - t$ and $D : y = 0$. By 4.3.1, they have at most two intersection points. But when $t = 0$, naively they have only one intersection at the origin. This is messy and we want to refine our formation of the theorem so that these exceptions don't appear by associate a number $I_p(C, D)$, intersection multiplicity, for the intersection of C and D at p so that we have the universal form $\sum_{p \in C \cap D} I_p(C, D) = \deg f \cdot \deg g$.

Naively we want $I_p(C, D)$ to satisfy:

1. $I_p(C, D) = I_p(D, C)$
2. $p \notin C \cap D \implies I_p(C, D) = 0$
3. If a curve $C_0 \subset C \cap D$ and $p \in C_0$, then $I_p(C, D) = \infty$
4. If C, D are distinct lines intersecting at p, then $I_p(C, D) = 1$
5. $D = D_1 \cap D_2 \implies I_p(C, D) = I_p(C, D_1) + I_p(C, D_2)$
6. For $C = \{F = 0\}$ and $D = \{G = 0\}$, one has $I_p(C, D) = I_p(C, D')$ where $D' = \{FQ + G = 0\}$. In English, if I perturb my curve a little bit, the multiplicity shouldn't change

So, how do we uniquely define $I_p(C, D)$ so that it always satisfy the above?

Example 4.4.6. By the properties above, for $p = [0, 0, 1]$,

$$I_p(y^2z - x^3, x) = I_p(x, y^2z - x^3) = I_p(x, y^2z) = 2I_p(x, y) + I_p(x, z) = 2,$$

so from the properties without any explicit formula, one can uniquely determine (at least in this case) $I_p(C, D)$!

Definition/Theorem 4.4.7. There's one and only one way to define the *intersection multiplicity* $I_p(C, D)$ that satisfies the 6 properties above.

Proof. For uniqueness, see Frances Kirwan's *Complex algebraic curves*, in which she proved by induction on $k = I_p(C, D)$ (express $I_p(C, D) = k$ by intersection multiplicities strictly less than k by the 6 properties).
We define $I_p(C, D)$ as follows:

1. If $p \notin C \cap D$ then $I_p(C, D) = 0$.
2. If p lies on a common component of C, D, then $I_p(C, D) = \infty$.
3. Now consider $C' \subset C$ and $D' \subset D$ such that C', D' have no common components. Observe that in the 6 properties above, we didn't mention any specific coordinates, which means for any projective transformation ϕ, one has
$$I_{\phi(p)}(\phi(C'), \phi(D')) = I_p(C', D'),$$
so WLOG suppose $[1, 0, 0] \notin \{C', D' \text{ lines through pairs of intersections of } C', D'\}$.
If $\mathbb{K}$ is algebraically closed, recall proof of 4.3.1 and write $C' = \{F = 0\}, D' = \{G = 0\}$ and $\mathcal{R}_{F,G} = \prod_{i=1}^{de}(a_i y + b_i z)$. We proved that $\exists x_0 \in \mathbb{K} : [x_0, y_0, z_0] \in C \cap D \iff [y_0, z_0] = [-b_i, a_i]$ for some i, and such x_0 is unique. Moreover, every intersection corresponds to one such x_0.
Then, write $p = [a, b, c]$ and define $I_p(C, D)$ as the usual multiplicity of $[b, c]$ as a root of $\mathcal{R}_{F,G}(y, z)$, i.e. the largest k such that $(cy - bz)^k \mid \mathcal{R}_{F,G}(y, z)$.

Week 7, lecture 3, 15th November

It remains to check this definition satisfies the 6 properties.

1. This is clear since $R_{F,G}(y, z) = \pm R_{G,F}(y, z)$, so their roots are exactly the same.
2. By definition.
3. By definition.
4. Write $\ell_1 = \{f_1(x) = ax + by + cz = 0\}$ and $\ell_2 = \{f_2(x) = dx + ey + fz = 0\}$, then $p = [bf - ce, cd - af, ae - bd]$. Since $(a, b, c) \neq (d, e, f)$, indeed $p \in \mathbb{P}^2(\mathbb{K})$. By applying a projective transformation, we can assume $p \neq [1, 0, 0]$ and write
$$R_{f_1,f_2} = \det\begin{pmatrix} a & by + cz \\ d & ey + fz \end{pmatrix} = (ae - bd)y + (af - cd)z,$$
and clearly the root $[]cd - af, ae - bd]$ has multiplcity 1.
5. By 4.4.3.
6. By 4.4.4

$\square$

Theorem 4.4.8 (Bézout)**.** If $\mathbb{K}$ is algebraically closed and $C, D \subset \mathbb{P}^2(\mathbb{K})$ are two curves of degree $d, e \geq 1$ with no common component, then
$$\sum_{p \cap D} I_p(C, D) = de.$$

Proof. Repeat the proof 4.3.1 and apply the definition above. $\square$

Definition 4.4.9. $C, D \subset \mathbb{P}^2(\mathbb{K})$ are *transverse* at $p \in C \cap D$ if p is smooth on both curves and $I_p(C, D) = 1$.

Then, 4.4.8 says two smooth curves C, D has $\deg C \deg D$ intersections $\iff$ C, D intersect transversely at every intersection.

Proposition 4.4.10. C, D are transverse at $p \iff T_pC$ and T_pD are different.

Proof. Since p is smooth, there is a unique irreducible component C' of C that passes through p by 3.0.14, and since $I_p(C, D) = I_p(C', D)$, one can assume C, and symmetrically D are irreducible. Moreover C and D can be assumed to be different since if $C = D$ then $I_p(C, D) = \infty$ and of course $T_pC = T_pD$. WLOG suppose $\deg c = d \geq e = \deg d$
By 4.3.1, $|C \cap D| < \infty$. Apply a projective transformation so that $p = [0, 0, 1]$, $T_pD = \{x = 0\}$ and none of C, D or lines through pairs of intersections of C and D passes through $[1, 0, 0]$. Now we can write $I_p(C, D)$ using

resultants. Write $F(x,y,z) = f_0(y,z)^d + \cdots + f_d(y,z)$ and $G(x,y,z) = g_0(y,z)^e + \cdots + g_e(y,z)$ where f_i, g_i are homogeneous of degree i. Then $I_p(C,D)$ is the largest k such that $y^k \mid \mathcal{R}_{F,G}(y,z)$.

By 3.0.12, $0 = dF(0,0,1) = \frac{\partial F}{\partial z}(0,0,1)$, so since p is smooth, $\left(\frac{\partial F}{\partial x}(0,0,1), \frac{\partial F}{\partial y}(0,0,1)\right) \neq (0,0)$. Now write $f_d(y,z) = az^d + bz^{d-1}y + \cdots$ where $y^2 \mid \cdots$. Note that $F(0,0,1) = 0 = f_d(0,1) = a$, and $b = \frac{\partial F}{\partial y}(0,0,1)$. Hence if $y^2 \mid f_d(y,z) \iff b = 0 \iff T_p = \{x = 0\}$. □

Corollary 4.4.11. For a smooth point $p \in C \subset \mathbb{P}^2$ and a line L, one has $I_p(C,L) \geq 2 \iff L = T_p(C)$.