Algebraic Geometry Notes

Francesco Chotuck

Abstract

This is KCL undergraduate module 7CCMMS20, instructed by Dr. Dmitri Panov. The formal name for this class is "Algebraic Geometry".

Contents

1 homogeneous coordinates

We can redefine a circle to be a conic that passes through the points $(1 : -i : 0)$ and $(1 : i : 0)$.

Claim: any theorem that holds for a collections of circles and lines holds for parabolas.

The space of all conics in $\mathbb{P}^2_K$ is $\mathbb{P}^5$ (where K is algebraically closed field).

AG Point of infinity in projective space is when we set z=0.

2 Rings

The idea of this section. Let K be an algebraically closed field and an affine variety $V \subset K^n$ (by this we mean set of polys =0 or something). Consider polynomials in $K[X_1, \ldots, X_n]$ as functions on K^n. restrict these functions (polys) ot V. We get a ring and this ring knows everything about V.

Example 2.1. Suppose $x^2 + y^2 - 1 = 0$ in $\mathbb{R}^2$. Now restrict all poly on this function (a circle). What kind of functions do we get? For example if we restrict x to the circle we get sin.

We only consider commutative rings in this course.

Example 2.2. Example of maximal ideal in the ring $\mathbb{C}[X]$. First of all we conisder an interesting ideal for this ring. consider we have a set points $x_1, \ldots, x_n \in \mathbb{C}$, the set of polys which vanish at each of these points form an ideal. However, not all ideals of these type of maximal, only ideal which vanish at one point are maximal ideal in $\mathbb{C}[X]$.

Example 2.3. Example of radical. Consider the ring $\mathbb{Z}$ and take $I = 24\mathbb{Z} = 2^3 \cdot 3\mathbb{Z}$. We have that $6^3 \in 24\mathbb{Z}$ thus $Rad(I) = 6\mathbb{Z}$.

Proposition 2.4. The radical is an ideal.

3 Zarinski topology

Definition 3.1. Let $X \subset \mathbb{A}^n_k$ be any subset. The **Zarinski closure** of X is the minimal closed set containing X. (i.e. affine variety).

> **Note 3.2.** We can find such a minimal set since we are allowed to take the intersection of closed sets.

Lemma 3.3. The Zarinski closure of $X \subset \mathbb{A}^n_k$ is equal to $V(I(X))$ where $I(X)$ is the ideal of all polynomials which vanish at X.

Example 3.4. The Zarinski closure of $[0, 1]$ is $[0, 1]$ adn the Zarinski closure of $\mathbb{Z}$ is $\mathbb{Z}$.

Example 3.5. Example fo Def 7.6 $I(\{0\} \cup \{1\}) = \langle x(x-1) \rangle$.

The above is to keep notes

This would be the actual notes

4 Bezout's theorem

4.1 Definitions

Definition 4.1. An **affine space** over a field K, is the vector space K^n where the point 0 does not play a special role. We denote affine space by $\mathbb{A}^n_K$ or $\mathbb{A}^n$.

Note 4.2. An affine space captures the geometric properties of an object without the need for a fixed coordinate system or origin. It is a more flexible framework that allows for studying geometric properties independently of specific coordinate systems.

Remark 4.3. In this course K is often $\mathbb{C}$ or $\mathbb{R}$ and sometimes a finite field.

Definition 4.4. The set $K[X_1, \ldots, X_n]$ is the ring of polynomials in n variables with coefficients in the field K.

Definition 4.5. The **degree** of a polynomial is the maximal degree of its monomials.

Remark 4.6. For example the degree of the monomial $4xy$ is 2, since x and y have exponent of 1.

Definition 4.7. By $K(X_1, \ldots, X_n)$ we denote the field of rational functions.

Definition 4.8. A subset $V \subset \mathbb{A}^n_K$ is an **affine variety** if there exists polynomials $f_1, \ldots, f_M \in K[X_1, \ldots, X_n]$ such that the point $(x_1, \ldots, x_n) \in V \iff f_i(x_1, \ldots, x_n) = 0$ for all $i \in \{1, \ldots, M\}$.

Note 4.9. An affine variety is like the set of points where different polynomial equations agree. It's a way to understand the solutions to systems of equations using geometry.

Example 4.10

The simplest example of an affine variety is the affine space of dimension n over a field K.

Definition 4.11. Let $F \in K[X_1, \ldots, X_n]$ be a non-constant polynomial, then the subset $\{x \in \mathbb{A}^n_K : F(x) = 0\} \subset \mathbb{A}^n_K$ is called a **hypersurface**.

Definition 4.12. Let $F \in K[X_1, \ldots, X_n]$ be a non-constant polynomial.

- If $F(x) = 0$ we say that F **vanishes** at x.
- (More generally) if $S \subset \mathbb{A}^n_K$ and $F(x) = 0$ of any $x \in S$ we say that F **vanishes** at S.

Corollary 4.13. If F vanishes on S then S belongs to the hypersurface $F(x) = 0$.

Theorem 4.14

Each polynomial $F \in K[X_1, \ldots, X_n]$ can be represented as a product

$$F = G_1 G_2 \cdots G_k$$

of irreducible polynomials. Such a representation is unique up to changing the order of the factors G_i and multiplying them by constants.

Note 4.15. The polynomial f is irreducible over K if it cannot be expressed as the product of two polynomials of lower degree.

Remark 4.16. That is, the polynomial ring is a unique factorisation domain.

4.2 Resultant

Note 4.17. Given two polynomials $f, g \in K[X]$ the resultant of f and g is used to determine if f and g have a common root, or more generally if they have a common factor.

Definition 4.18. Given two polynomials:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$
$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$$

The **Sylvester** matrix is given by

$$S(f,g) = \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 & \cdots & 0 & \\ 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & \cdots & 0 & \\ \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \\ 0 & 0 & 0 & \cdots & a_n & a_{n-1} & \cdots & a_1 & a_0 \\ b_m & b_{m-1} & b_{m-2} & \cdots & b_0 & 0 & \cdots & 0 & \\ \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \\ 0 & 0 & 0 & \cdots & b_m & b_{m-1} & \cdots & b_1 & b_0 \end{pmatrix}$$

Example 4.19

Say we have two polynomials:

$$f(x) = 3x^2 - 2x + 1$$
$$g(x) = 2x^3 + x^2 - 3x + 4$$

Then, the Sylvester matrix would be:

$$S(f,g) = \begin{pmatrix} 3 & -2 & 1 & 0 & 0 \\ 0 & 3 & -2 & 1 & 0 \\ 0 & 0 & 3 & -2 & 1 \\ 2 & 1 & -3 & 4 & 0 \\ 0 & 2 & 1 & -3 & 4 \end{pmatrix}$$

Definition 4.20. The determinant of the Sylvester matrix is called the **resultant**. For two polynomials f and g it is denoted by $R[f, g]$.

Lemma 4.21

The polynomials f and g have a common factor if and only if $R[f, g] = 0$. In particular, if K is algebraically closed and $R[f, g] = 0$ then f and g have a common root.

Definition 4.22. A **hyperplane** is a flat surface in n-dimensional space of dimension $n - 1$. It is defined by an equation of the form $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$.

Proposition 4.23. Let $F(x_1, \ldots, x_n)$ be a polynomial vanishing on the hyperplane $a_0 + a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0$. Then $F(x_1 \ldots, x_n)$ is divisible by $a_0 + a_1x_1 + a_2x_2 + \ldots + a_nx_n$.

Remark 4.24. We take $a_0 = -b$.

Proposition 4.25 (Resultant in terms of roots)

Suppose

$$f(t) = \alpha_0(t - \alpha_1) \cdots (t - \alpha_n)$$
$$g(t) = \beta_0(t - \beta_1) \cdots (t - \beta_m)$$

then

$$R[f, g] = \alpha_0^m \beta_0^n \prod_{i,j} (\alpha_i - \beta_j).$$

Corollary 4.26

Let $f, g \in K[X]$ of degrees n and m respectively. We have the following.

1. $R[t^n, (t - 1)^m] = (-1)^{mn}$.
2. $R[\alpha f, \beta g] = \alpha^m \beta^n R[f, g]$.
3. $R[f(\alpha x), g(\alpha x)] = \alpha^{mn} R[f, g]$.

4.3 Pascal and Bézout's theorems

Note 4.27. Before we state Bézout's theorem we state a lemma necessary for its proof.

Lemma 4.28

We have the following.

1. Let K be an infinite field. If the number of solutions of $F(x,y) = G(x,y) = 0$ in K^2 is finite, then it is at most $\deg(F)\deg(G)$.
2. Let K be a field, let $f \in K[X,Y]$ be an irreducible polynomial and let $g \in K[X,Y]$ be an arbitrary polynomial. If g is NOT divisible by f then the system of equations $f(x,y) = g(x,y) = 0$ has only a finite number of solutions.

Note 4.29. Bézout's theorem is a generalisation of the following.

Proposition 4.30. Let K be a field and let $F \in K[X]$ be of degree d. Then the equation $F = 0$ has at most d solutions.

Theorem 4.31 (Bézout)

Let $F, G \in K[X,Y]$ without common factors. Then the number of points in K^2 where $F(x,y) = 0$ and $G(x,y) = 0$ is at most $\deg(F)\deg(G)$.

Proof. Let F and G be two polynomials without common factors. It follows from the lemma above (2) that the system of equations $F = G = 0$ has only a finite number of solutions. Indeed, we can decompose F into a product $F = H_1 \cdots H_k$ of irreducible polynomials and apply the lemma (2) to each pair H_i, G. Hence, we can apply lemma (1) to F and G. □

Remark 4.32. In the lemma we assume that K is an infinite field so the proof of Bézout's theorem only works for infinite fields. However, the theorem also holds in finite fields. To prove this we extend K to its algebraic closure which is always infinite.

Definition 4.33. We define a few things.

- A **plane curve** (or **curve**) is the set of points for which a polynomial $F(x,y) = 0$ in K^2.
- The **degree** of a curve $F(x,y) = 0$ is the degree of F.
- A curve $F(x,y) = 0$ is called **irreducible** if F is an irreducible polynomial.
- If $\deg(F) = 2, 3$ the curve $F(x,y) = 0$ is called a **conic** and a **cubic** respectively.

Theorem 4.34 (Pascal)
Suppose that the points $A_1, \dots, A_6 \in \mathbb{R}^2$ lie on a conic. Denote by A_iA_j the line containing A_i and A_j. Then the three points

- $A_1A_2 \cap A_4A_5$,
- $A_2A_3 \cap A_5A_6$ and
- $A_3A_4 \cap A_6A_1$

lie on one line.

Proof. We assume the conic is irreducible and given by an equation $F = 0$.

Let $L_1, M_1, L_2, M_2, L_3, M_3$ be linear functions on the plane vanishing on the lines $A_1A_2, A_2A_3, \dots, A_6A_1$ respectively. We consider the following one-parameter family of degree 3 polynomials:

$$G_\lambda = L_1L_2L_3 + \lambda M_1M_2M_3.$$

We note that $A_1, \dots, A_6$ and the three points of intersections that we study lie on the cubic curve $G_\lambda = 0$ for any λ. We choose a point p on the conic different from $A_1, \dots, A_6$ and choose λ_0 such that $G_{\lambda_0}(p) = 0$.

The intersection of the conic $F = 0$ and the cubic $G_{\lambda_0} = 0$ contains at least 7 points: six points are A_i and then p. For the sake of contradiction, suppose F and G_{λ_0} do not have any common factors, then we can apply Bézout's theorem and find that there are at most $\deg(F)\deg(G) = 2 \cdot 3 = 6$ points of intersection, but we have 7 hence, F and G must have a common factor. We assume F is irreducible so, it follows that F is a factor of G_{λ_0}, so we can write

$$G_{\lambda_0} = F \cdot L$$

where $\deg(L) = 1$ (since $\deg(G) = 3$ and $\deg(F) = 2$). The intersection points of the theorem lie on the curve

$$\{G_{\lambda_0} = 0\} = \{F \cdot L = 0\}$$

but they do not lie on the conic $F = 0$, so they must lie on $L = 0$. □

5 Polynomial method

Note 5.1. The idea of this section: let E be a finite subset of a vector space K^n. To obtain information about E we study non-zero polynomials of minimal possible degree that vanish on E. We will study two problems which make use of this method.

Example 5.2
If $|E| \leq n$ there is a polynomial of degree 1 that vanishes on E. On the other hand, if K is finite and $|E| > |K|^{n-1}$ then there is no non-zero polynomial of degree ≤ 1 that vanishes at E. Indeed, any degree 1 polynomial is vanishing at a hyperplane contains exactly $|K|^{n-1}$ points.

Definition 5.3. A polynomial is **identically zero** if it is zero as an element of $K[X_1, \dots, X_n]$ that is, all of its coefficients are zero.

Example 5.4

Any polynomial $F \in K[X_1, \ldots, X_n]$ with $\deg(F) = |K|$ that vanishes at all points of K^n is identically zero.

5.1 Kakeya conjecture

Definition 5.5. A **Kakeya set** is a subset of a Euclidean space that contains a unit line segment in every direction.

Note 5.6. The question regarding Kakeya sets is how big are they. Dvir proved the following conjecture.

For any n there exists $c_n > 0$ such that any Kakeya set $E \subset K^n$ has cardinality at least $c_n |K|^n$.

Proposition 5.7

We have that

- The vector space of polynomials in $K[X_1, \ldots, X_n]$ of degree $\leq d$ has dimension $\binom{n+d}{d}$.
- The dimension of the space of homogeneous degree d polynomials $\binom{n+d}{d}$.

Note 5.8. We note that the n is the one from $K[X_0, \ldots, X_n]$, so the extra coordinate of x_0 is not counted.

Sketch of proof. We do this by induction.

- **Base Case:** For $n = 1$, the vector space of polynomials in $K[X_1]$ of degree at most d has dimension $d + 1$.
- **Inductive Step:** Assume the statement holds for $n = k$. For $n = k + 1$, the dimension of the vector space is $\binom{k+d+1}{d+1}$.

□

Lemma 5.9

Let L be a linear subspace of $K[X_1, \ldots, X_n]$ and let E be a finite subset of K^n with $|E| < \dim(L)$.

- Then there is a non-zero polynomial $P \in L$ vanishing on E.
- If we denote by M the subspace of polynomials from L that vanish on E then $\dim(M) \geq \dim(L) - |E|$.

Proof. Denote by K^E the vector space of K-valued functions on E (i.e. elements in K^E are functions $f : E \to K$). We have the evaluation map

$$\text{ev} : L \to K^E.$$

This map associates to a polynomial $F \in L$ the function $F(x_1, \ldots, x_n)$ on E (i.e. $(x_1, \ldots, x_n) \in E$). The kernel of the evaluation map is M. The inequality follows from the rank-nullity theorem:

$$\begin{aligned}\dim(\ker(\text{ev})) &= \dim(L) - \dim(\text{Im}(\text{ev})) \\ &\geq \dim(L) - |E|\,.\end{aligned}$$

□

Corollary 5.10

Some corollaries.

1. Let $E \subset K^n$ be a subset such that $|E| < \binom{n+d}{d}$. Then there exists a non-zero polynomial $F \in K[X_1, \ldots, X_n]$ vanishing on E with $\deg(F) \leq d$.
2. For any subset $E \subset K^n$ there exists a non-zero polynomial $F \in K[X_1, \ldots, X_n]$ vanishing on E with $\deg(F) \leq n\,|E|^{1/n}$.

Proof. We prove each statement in turn.

1. Denote by V_d the space of polynomials in $K[X_1, \ldots, X_n]$ of degree at most d. By a proposition above we have that

$$\dim(V_d) = \binom{n+d}{d}$$

   i.e. $\dim(V_d) > |E|$ (by the hypothesis). Then applying the lemma above with $L = V_d$, the statement is proven.

2. In the proof above set $d = \left\lfloor n\,|E|^{1/n} \right\rfloor$ then,

$$\begin{aligned}\binom{n+d}{d} = \frac{(n+d)!}{d!n!} &= \frac{(d+1)\cdots(n+d)}{n!} \\ &> \frac{(n\,|E|^{1/n})\cdots(n\,|E|^{1/n} + n - 1)}{n!} \\ &\geq \frac{n^n}{n!}\,|E| \\ &\geq |E|\,.\end{aligned}$$

□

Lemma 5.11

Let $P \in K[x_1, \ldots, x_n]$ be a polynomial of degree at most $|K| - 1$ which vanishes on a Kakeya set $E \subset K^n$. Then P is identically zero.

Proof. For the sake of contradiction, assume that P is not identically zero. Then it must have positive degree, we can write

$$P = \sum_{i=0}^{d} P_i \quad \text{where } 1 \leq d \leq |K| - 1$$

for $d > 0$, and P_i is the i^{th} homogeneous component. We will come to a contradiction by showing that P_d is identically zero. Fix a vector $\boldsymbol{v} \in K^n \setminus \{0\}$. We will prove that $P_d(\boldsymbol{v}) = 0$. Since E is a Kakeya set, E contains a line with direction of $\boldsymbol{v}$ i.e. for some $\boldsymbol{x} \in K^n$ the set E contains the line $\{\boldsymbol{x} + t\boldsymbol{v} : t \in K\}$. We restrict P to this line. We obtain a polynomial of one variable in t namely, $P(\boldsymbol{x} + t\boldsymbol{v})$. We have that $P(\boldsymbol{x} + t\boldsymbol{v}) = 0$ for all $t \in K$. Since $P(\boldsymbol{x} + t\boldsymbol{v})$ is a polynomial in t of degree at most $|K| - 1$ all its coefficients are zero by the Lemma preceding Bezout's theorem. We claim the coefficient of $P(\boldsymbol{x} + t\boldsymbol{v})$ in front of t^d is $P_d(\boldsymbol{v})$ and is 0. Indeed,

$$\begin{aligned} P(\boldsymbol{x} + t\boldsymbol{v}) &= P_d(\boldsymbol{x} + t\boldsymbol{v}) + \sum_{i=0}^{d-1} P_i(\boldsymbol{x} + t\boldsymbol{v}) \\ &= \sum_{i \leq d} c_i t_i + t^d P_d(\boldsymbol{v}). \end{aligned}$$

Hence, P_d is identically zero. □

Proposition 5.12 (Kakeya conjecture)
For nay n there exists $c_n > 0$ such that any Kakeya set $E \subset K^n$ is such that $|E| \geq c_n |K|^n$.

Proof. We show that $c_n = (2n)^{-n}$ works. For the sake of contradiction, we assume $|E| < (2n)^{-n} |K|^n$. By a corollary above there is non-zero polynomial F with $\deg(F) \leq \frac{|K|}{2} < |K|$ vanishing on E. By the above lemma this is identically zero which is a contradiction. □

5.2 The joints problem

Definition 5.13. Let $\mathcal{L}$ denote a finite collection of lines in $\mathbb{R}^3$. The number of lines in $\mathcal{L}$ is denoted by $|\mathcal{L}|$.

Definition 5.14. A point $p \in \mathbb{R}^3$ is a **joint** of $\mathcal{L}$ if p lies in (at least) three lines of $\mathcal{L}$ that are not coplanar. The number of joints of $\mathcal{L}$ is denoted $J(\mathcal{L})$.

Example 5.15

The joints problem. For a given number $\ell \in \mathbb{N}$ we want to find

$$J(\ell) = \max_{|\mathcal{L}|=\ell} J(\mathcal{L}).$$

For example, we can consider $\mathbb{Z}^3 \subset \mathbb{R}^3$. Let $S = \{01, \dots, n-1\}$. We define

$$\mathcal{L} = \text{lines parallel to } x, y, z\text{-axes intersecting } S \times S \times S.$$

We have that $J(\mathcal{L}) = n^3$ and $|\mathcal{L}| = 3n^2$.

Note 5.16. This allows us to make a guess to the joints problem: $|J(\ell)| \approx \ell^{3/2}$.

Lemma 5.17. If $\mathcal{L}$ is a set of lines in $\mathbb{R}^3$ that determines J joints, then one of the lines contains at most $3J^{1/3}$ joints.

Proof. Let P be a polynomial of the lowest degree that vanishes at all joints of $\mathcal{L}$. By some previous corollary we have that $\deg(P) \leq 3J^{1/3}$. For the sake of contradiction, suppose that each line in $\mathcal{L}$ contains $> 3J^{1/3}$ joints. Then P vanishes at all lines in $\mathcal{L}$. It follows that ∇P vanishes at all joints. However, at the same time for some $i \in \{1, 2, 3\}$ we have that $\dfrac{\partial P}{\partial x_i} \neq 0$ and so $\dfrac{\partial P}{\partial x_i}$ has degree $\deg(P) - 1$ which contradicts the minimality of P. □

Theorem 5.18

We have that $J(\ell) \leq 10\ell^{3/2}$.

Proof. Let $\mathcal{L}$ be a collection of ℓ lines with $J(\ell)$ joints. By the lemma above there is a line in $\mathcal{L}$ that contains at most $3J(\ell)^{1/3}$ joints. The number of joints of $\mathcal{L}$ that do not lie on this line is at most $J(\ell - 1)$. Thus, we have

$$J(\ell) \leq J(\ell - 1) + 3J(\ell)^{1/3}.$$

Iterating this argument and using the fact that $J(\ell_1 \leq J(\ell_2))$ for $\ell_1 \leq \ell_2$ we see that

$$\begin{aligned} J(\ell) &\leq J(\ell - 1) + 3J(\ell)^{1/3} \\ &\leq J(\ell - 2) + 2 \cdot 3J(\ell)^{1/3} \\ &\leq \ell \cdot 3J(\ell)^{1/3}. \end{aligned}$$

Hence, $J(\ell)^{2/3} \leq 3\ell$. □

6 Projective space

Note 6.1. In Euclidean plane geometry, we need to separate the cases of pairs of lines which meet and parallel line which do not. Geometry becomes a lot simple if any two lines met possible "at infinity". There are various ways of arranging this and the most convenient method is to embed the $\mathbb{A}^2$ into 3-dimensional space. To each point $p \in \mathbb{A}^2$ we can associate the line OP. The lines parallel to the plane correspond to the points at infinity.

Definition 6.2. An n-dimensional **projective space** over a field K is the set of 1-dimensional subspaces of the vector space K^{n+1}. Equivalently, it is the set of lines in K^{n+1} which contain the origin. We denote this by $\mathbb{P}^n_K$ or just $\mathbb{P}^n$.

Proposition 6.3. The projective space associated to a vector space V is the set of 1-dimensional subspaces of V, and we denote it by $\mathbb{P}(V)$.

Remark 6.4. We can make this notion more precise. For any K-vector space V we can define the projective space

$$\mathbb{P}(V) = (V \setminus \{0\}) / (K^*\text{-rescaling action } v \mapsto \lambda v, \text{ for all } \lambda \in K^*).$$

This comes equipped with a quotient map $\pi : V \setminus \{0\} \to V$ such that $v \mapsto [v]$ where $[v] = [\lambda v]$. By picking a basis for V we can suppose $V = K^{n+1}$ and say

$$\begin{aligned} \mathbb{P}^n &= \mathbb{P}(K^{n+1}) \\ &= (\text{space of straight lines in } K^{n+1} \text{ through } 0). \end{aligned}$$

Note 6.5. As such we can think of points in the projective space as lines in the affine space.

Example 6.6

We provide some examples of projective space.

1. $\mathbb{P}^0 = \{\text{one point}\}$. In the affine space this is a line therefore, is represented by a single point in projective space. It has dimension 0.
2. We can think of $\mathbb{P}^1_{\mathbb{R}}$ as a topological circle. This space is the set one-dimensional subsets of $\mathbb{R}^2$ which is the set of lines through the origin.
3. $\mathbb{P}^2_{\mathbb{R}}$ is the sphere $x^2 + y^2 + z^2 = 1$ quotient by the central symmetry. This symmetry maps a point $P = (x, y, z)$ to $P' = (-x, -y, -z)$.
4. $\mathbb{P}^1_{\mathbb{C}}$ can be identified as the two-sphere.
5. $\mathbb{P}^3_{\mathbb{R}}$ can be identified with $SO(3, \mathbb{R})$.
6. $\mathbb{P}^1_{\mathbb{Z}/p\mathbb{Z}}$ has $p + 1$ points. The projective line over a finite field $\mathbb{Z}/p\mathbb{Z}$ consists of all one-dimensional subspaces of the vector space $(\mathbb{Z}/p\mathbb{Z})^2$, excluding the zero vector. Each non-zero vector in $(\mathbb{Z}/p\mathbb{Z})^2$ defines a unique one-dimensional subspace and thus a point on the projective line. However, scalar multiples of a vector define the same subspace, so each point corresponds to $p - 1$ distinct vectors. Thus, the total number of points on the projective line is $\frac{p^2-1}{p-1}$, which simplifies to $p + 1$.

Lemma 6.7

We have that $\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$.

Proof. Consider the vector space V^{n+1} and let $\mathbb{A}^n$ be an affine subspace of V^{n+1} that does contain 0. Consider the subset of $\mathbb{P}^n$ consisting of lines in V^{n+1} that pass through 0 and intersect $\mathbb{A}^n$. Clearly, this subset is isomorphic to $\mathbb{A}^n$ as for each point $x \in \mathbb{A}^n$ we can take the line through x and 0. The piece of $\mathbb{P}^n$ not contained in this subset consists of all lines through 0 contained in the vector subspace $V^n \subset V^{n+1}$ parallel to $\mathbb{A}^n$. This is precisely $\mathbb{P}^{n-1}$ so $\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$. □

Definition 6.8. The described hyperplane $\mathbb{P}^{n-1} \subset \mathbb{P}^n$ is called the **infinity** of $\mathbb{A}^n$.

Corollary 6.9. $\mathbb{P}^n = \mathbb{A}^n \cup \cdots \cup \mathbb{A}^0$.

Definition 6.10. Let V^{n+1} be a vector space and $W^{k+1} \subseteq V^{n+1}$ be a vector subspace. The set of lines through 0 in W^{k+1} is a subset of $\mathbb{P}^n$ isomorphic to a projective space $\mathbb{P}^k$. Such subsets of $\mathbb{P}^n$ are called **linear subspaces**. If $k = 1$ it is called a **projective line**. If $k = n - 1$ it is called a **hyperplane**.

Proposition 6.11

Assume $l + m \geq n$. We have that $\mathbb{P}^l \cap \mathbb{P}^m \subset \mathbb{P}^n$ is a linear subspace of dimension at least $l + m - n$.

Proof. Let V^{n+1} be the vector space corresponding to $\mathbb{P}^n$. Consider vector subspaces $V^{l+1}, V^{m+1} \subseteq V^{n+1}$ corresponding to $\mathbb{P}^l$ and $\mathbb{P}^m$. Then the intersection $V^{l+1} \cap V^{m+1}$ is a vector subspace of V^{n+1} of dimension at least $l + m + 1 - n$. All lines in this vector subspace going through 0 form a linear subspace of $\mathbb{P}^n$ of dimension at least $l + m - n$ and this is exactly the intersection $\mathbb{P}^m \cap \mathbb{P}^l$. □

Proposition 6.12

Suppose $k \leq n$. For any points $x_1, \ldots, x_k \subset \mathbb{P}^n$ there is a linear subspace $\mathbb{P}^{k-1} \subset \mathbb{P}^n$ containing $x_1, \ldots, x_k$.

Proof. Consider lines $l_1, l_2, \ldots, l_k$ in V^{n+1} that correspond to points $x_1, \ldots, x_k$ in $\mathbb{P}^n$. Then these lines are contained in a certain linear subspace $V^k \subseteq V^{n+1}$. All lines in V^k passing through 0 correspond to a linear subspace $\mathbb{P}^{k-1}$ in $\mathbb{P}^n$ containing $x_1, \ldots, x_k$. □

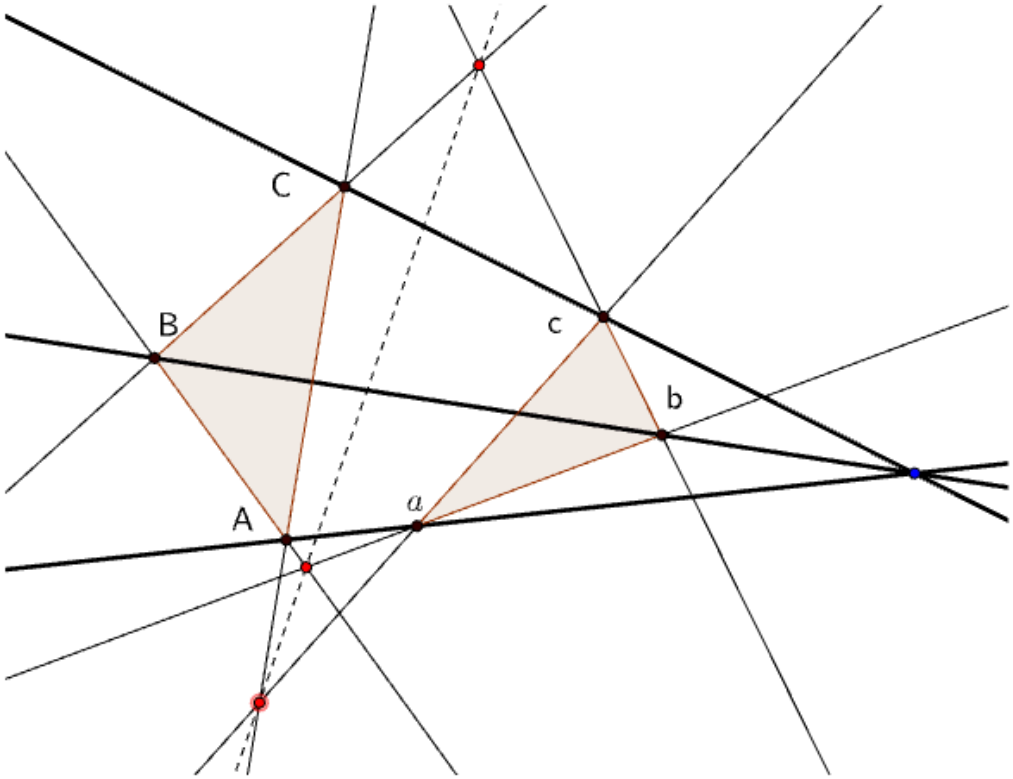
Theorem 6.13 (Desargues theorem)

Let a, b, c, A, B, C be six points in $\mathbb{P}^3$ not contained in one plane and such that no three of these points lie on one line. Suppose that the lines aA, bB and cC intersect in one point. Then the points

- $ab \cap AB$,
- $bc \cap BC$ and
- $ac \cap AC$

lie on one line.

Proof. By our assumption and the proposition above there are unique $\mathbb{P}^2$ containing points a, b, c and points A, B, C respectively i.e. $\mathbb{P}^2(abc)$ and $\mathbb{P}^2(ABC)$. Then the line $abc \cap ABC$ contains all three intersection points. Indeed, $ab \subset abc$ and $AB \subset ABC$ hence, $ab \cap AB \subset abc \cap ABC$. The same reasoning is used for the other two intersections. □



Theorem 6.14

Suppose $\mathbb{P}^k, \mathbb{P}^l, \mathbb{P}^m$ are linear subspaces in $\mathbb{P}^n$ and that $k+l+m \geq n-1$. Then there exists a projective line $\mathbb{P}^1 \subset \mathbb{P}^n$ that intersects all three subspaces.

Proof. If $\mathbb{P}^l \cap \mathbb{P}^m \neq \emptyset$ then the statement is trivial (since there is a projective line that connects a point from this intersection with a point on $\mathbb{P}^k$).

Suppose $\mathbb{P}^l \cap \mathbb{P}^m = \emptyset$. Consider the minimal linear subspace of $\mathbb{P}^n$ that contains $\mathbb{P}^l$ and $\mathbb{P}^m$. Then the following two statements hold

1. This subspace is the union of all projective lines that join a point of $\mathbb{P}^l$ with a point of $\mathbb{P}^m$.

2. Moreover, this space has dimension $l+m+1$.

We know that in $\mathbb{P}^n$ we have $\mathbb{P}^{l+m+1} \cap \mathbb{P}^k \neq \emptyset$ since $((m+l+1)+k)-n \geq 0$ by the assumptions of the theorem. Hence, there is a projective line intersecting $\mathbb{P}^m$, and $\mathbb{P}^k$. □

6.1 Projective transformations

Let V, W be vector spaces and $T : V \to W$ be a linear transformation with $\ker T = 0$. Then any one-dimensional subspace in V is sent to a one-dimensional subspace in W. Hence, T gives us a well-defined map

$$\tau : \mathbb{P}(V) \to \mathbb{P}(W).$$

Definition 6.15. A projective transformation from $\mathbb{P}(V)$ to $\mathbb{P}(W)$ is the map τ defined by an invertible linear transformation $T : V \to W$.

Example 6.16. Take $\mathbb{P}^2_K$, take two projective lines L_1, L_2 in it and a disjoint point p. The projection of L_1 to L_2 from p is the map that associates to a point $x \in L_1$ the intersection point of the unique projective line xp with L_2. This map is a projective transformation.

6.2 Homogeneous coordinates

Definition 6.17. Consider the vector space K^{n+1} with coordinate $(x_0, \dots, x_n)$ and let $\mathbb{P}^n_K = \mathbb{P}(K^{n+1})$.

Let $L \subset K^{n+1}$ be a line passing through 0. Denote $p(L)$ the corresponding point in $\mathbb{P}^n_K$. We say that $[a_0 : \cdots : a_n]$ are **homogeneous coordinates** of the point $p(L)$ if $(a_0, \dots, a_n) \in L$ and $a_0, \dots, a_n \neq 0$.

Note 6.18. Recall that $\mathbb{P}^n$ is the quotient $K^{n+1} \setminus \{(0, \dots, 0)\}$ by the equivalence relation

$$(x_0, \dots, x_n) \sim (\lambda x_0, \dots, \lambda x_n) \quad \text{where } \lambda \in K \setminus \{0\}.$$

We call a representative for an equivalence the **homogeneous coordinates** of that point in $\mathbb{P}^n$.

Remark 6.19. If $(a_0, \dots, a_n) \in L$ then points on L can be written as $(\lambda a_0, \dots, \lambda a_n)$ for $\lambda \in K$. So for $\lambda \neq 0$ we have that $[a_0 : \cdots : a_n]$ is the same point of $[\lambda a_0 : \cdots : \lambda a_n]$.

Theorem 6.20

We can embed $\mathbb{A}^n$ into $\mathbb{P}^n$ by the map

$$(x_0, \dots, x_n) \mapsto [x_0 : \cdots : x_n : 1].$$

Any other homogeneous coordinates where the first coordinate is non-zero can be re-scaled to have first coordinate 1. Points with last coordinate equal to 0 are "**points at infinity**".

Remark 6.21. A point $[x_0 : \cdots : x_n : 0]$ can be seen as a point in $\mathbb{P}^{n-1}$ by dropping the last coordinate.

6.2.1 Homogeneous equations

Definition 6.22. The **degree** of a polynomial is the highest of the degrees of the polynomial's monomials (individual terms) with non-zero coefficients.

Remark 6.23. In a multivariate polynomial, we have that $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ is also a monomial and the degree is given by the sum of the ε_i. For example, consider the polynomial $P(x, y, z) = 3x^2y + 2xyz^2 + z^3$.

- The degree of the monomial $3x^2y$ is $2 + 1 = 3$.
- The degree of the monomial $2xyz^2$ is $1 + 1 + 2 = 4$.
- The degree of the monomial z^3 is 3.

The highest degree among these monomials is 4. Therefore, the degree of the polynomial $P(x, y, z)$ is 4.

Definition 6.24. A polynomial $F \in K[X_0, \ldots, X_n]$ is called **homogeneous of degree** d if all its monomials have degree d.

Example 6.25

Example and counter example.

- The polynomial $F = x + y^2$ is not homogeneous as the monomial x is of degree 1 and the monomial y is of degree 2.
- The polynomial $G = ab + c^2 + (d + e)^2$ is homogeneous, because all monomials have degree 2.

Theorem 6.26

If $[x_0 : \ldots : x_n]$ and $[y_0 : \ldots : y_n]$ represent the same point $p \in \mathbb{P}^n$, then

$$(x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n)$$

with $\lambda \in k \setminus \{0\}$. Hence, if $f \in k[X_0, \ldots, X_n]$ is a homogeneous polynomial of degree d, then

$$f(x_0, \ldots, x_n) = \lambda^d f(y_0, \ldots, y_n)$$

Thus, the actual value of f at p is not well-defined, but it is well-defined whether f is zero at p.

Definition 6.27. Let $F \in K[X_0, \ldots, X_n]$ be a degree d homogeneous polynomial. Define the subset

$$X_F = \{[a_0 : \cdots : a_n] \in \mathbb{P}^n : F(a_0, \ldots, a_n) = 0\} \subset \mathbb{P}^n.$$

We call X_F a **hypersurface** of degree d.

Remark 6.28. If $F(a_0, \ldots, a_n) = 0$ then F is zero on the whole line $(\lambda a_0, \ldots, \lambda a_n)$ for $\lambda \in K$.

Example 6.29

Some examples.

- If $\deg(F) = 1$, then $\{F = 0\} = \mathbb{P}^{n-1}$. This is a **hyperplane**.
- Consider $\mathbb{P}^1_{\mathbb{C}}$. Then $F = \sum a_i z_0^i z_1^{d-i}$. In this case F can be decomposed as a product $F = \prod_{k=1}^{d}(b_k z_0 + c_k z_1)$. So the equations $F = 0$ defines the collection of points $(c_k : -b_k)$ in $\mathbb{P}^1_{\mathbb{C}}$.

Definition 6.30. A subset $V \subset \mathbb{P}^n_K$ is said to be a **projective variety** if there exist homogeneous polynomials $f_1, \ldots, f_N \in K[X_0, \ldots, X_n]$ such that

$$[x_0 : \cdots : x_n] \in V \iff f_i(x_0, \ldots, x_n) = 0 \quad \forall i \in \{1, \ldots, N\}.$$

Example 6.31

Hypersurfaces in $\mathbb{P}^n$.

6.3 Switching coordinates

Note 6.32. We saw that $\mathbb{P}^n \setminus \mathbb{P}^{n-1} = \mathbb{A}^n$. This permits us to look at any hypersurface $X_F \subseteq \mathbb{P}^n$ from "different angles". Namely, we can choose any hyperplane $\mathbb{P}^{n-1} \subseteq \mathbb{P}^n$ and study the piece of X_F that lies in the corresponding $\mathbb{A}^n$, i.e., $X_F \cap (\mathbb{P}^n \setminus \mathbb{P}^{n-1})$.

We explain next how to derive an equation for $X_F \cap \mathbb{A}^n$ from the equation $F = 0$ defining X_F.

Definition 6.33. The subset in $\mathbb{P}^n_K$ such that $x_i \neq 0$ is denoted by U_i. We can identify with $\mathbb{A}^n_K$ by the following:

$$[x_0 : \cdots : x_i : \cdots : x_n] \in \mathbb{P}^n_K \longleftrightarrow \left(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\right) \in \mathbb{A}^n_K.$$

Definition 6.34. The subset $U_0 \subset \mathbb{P}^n$ where $x_0 \neq 0$ is given by $\mathbb{A}^n$. The points in $\mathbb{P}^n \setminus U_0$ are **points at infinity** of $U_0 = \mathbb{A}^n$.

Corollary 6.35 (Switching coordinates)

We relate homogeneous equations in $\mathbb{P}^n$ and non-homogeneous equations in U_0 as follows.

- $\mathbb{P}^n \to U_0$ we do the following substitution $x_0 \mapsto 1$.
- $U_0 \to \mathbb{P}^n$ we replace each variable by $\frac{x_i}{x_0}$ then multiply by an appropriate power of x_0 to make the polynomial homogeneous.

Example 6.36

We show some examples:

- The homogeneous polynomial $x_0^2 + x_0x_1 + x_0x_2 + x_1x_2$ is transformed into a non-homogeneous polynomial by setting $x_0 = 1$.
- The non-homogeneous polynomial $f(x_1, x_2, x_3) = x_1^2x_2^2 + x_3^3 + 1$ can be turned into a homogeneous by introducing a new variable x_0 and setting each x_i to $\frac{x_i}{x_0}$ then multiplying by x_0^4 to make it homogeneous.

  We have that $f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}, \frac{x_3}{x_0}\right) = \frac{x_1^2x_2^2}{x_0^4} + \frac{x_3^3}{x_0^3} + 1$. To make this polynomial homogeneous we multiply by x_0^4 and obtain $f(x_0, x_1, x_2, x_3) = x_1^2x_2^2 + x_0x_3^3 + x_0^4$.

6.4 Quadratic forms and conics

Note 6.37. In this section we study equations of degree 2. We assume that the field L is algebraically closed and the characteristic of K is not equal to 2.

Definition 6.38. A **quadratic form** on a vector space V is a homogeneous polynomial of degree 2.

Definition 6.39. A quadratic form F is **diagonal** in coordinates $x_1, \dots, x_n$ if $F = \sum_i a_i x_i^2$. We say F is **diagonalisable** if it is diagonal in some linear coordinates.

Definition 6.40. A **symmetric bilinear form** Q on V is a function in two variables $u, v \in V$ satisfying

$$Q(u, v) = Q(v, u) \quad \text{and}$$
$$Q(\alpha u_1 + \beta u_2, v) = \alpha Q(u_1, v) + \beta Q(u_2, v).$$

Theorem 6.41

Let F be a quadratic form on V. We can associate a symmetric bilinear form to F:

$$Q(u, v) = \frac{F(u + v) - F(u) - F(v)}{2}.$$

Furthermore, we have $F(v) = Q(v, v)$.

Lemma 6.42

For any quadratic form $F \neq 0$ on K^n there exists a basis $v_1, \dots, v_n$ such that

$$F(x_1v_1 + \cdots + x_nv_n) = x_1^2 + \cdots + x_i^2 \quad \text{for some } i \in \{1, \dots, n\}.$$

6.4.1 Conics

Definition 6.43. Let $F \in K[X, Y, Z]$ be a homogeneous polynomial of degree 2. Then the curve $\{F = 0\} \subset \mathbb{P}^2_K$ is called a **conic**.

Definition 6.44. The conic $\{F = 0\}$ is called **irreducible** if F is an irreducible polynomial.

Lemma 6.45 (Characterisation of conics)
Let $F = 0$ be an irreducible conic in $\mathbb{P}^2_K$. Then in some homogeneous coordinates $[x : y : z]$ the conic is given by the equation $xz - y^2 = 0$.

Proof. By a lemma above in some coordinates the equation for F is

- $x'^2 = 0$,
- $x'^2 + y'^2 = 0$ or
- $x'^2 + y'^2 + z'^2 = 0$.

The first two equations correspond to reducible conics, so we are in the third case. Now consider the new coordinates

- $x' = (x - z\sqrt{-1})$,
- $y' = y\sqrt{-1}$,
- $z' = (x + z\sqrt{-1})$.

□

Corollary 6.46
Any irreducible conic in $\mathbb{P}^2_K$ can be parametrised by $\mathbb{P}^1_K$.

Proof. By the lemma above we can assume that the conic C can be given by $xz - y^2 = 0$. Then the parametrisation $\phi : \mathbb{P}^1_K \to C$ can be given as follows:

$$\phi(u : v) = [u^2 : uv : v^2].$$

This map is called the **rational parametrisation** of the conic. Clearly the image of this map belongs to C and the map is injective. Moreover, the map is surjective. □

Lemma 6.47
Let $F_d \in K[X, Y, Z]$ be a homogeneous polynomial of degree d and let $C \subset \mathbb{P}^2_K$ be a conic. We have the following either

$$F_d \equiv 0 \quad \text{OR} \quad \{F_d = 0\} \cap C \text{ contains no more than } 2d \text{ points.}$$

Remark 6.48. By $F \equiv 0$ we mean that all coefficients are 0.

Note 6.49. This is an alternative proof to Bezout's theorem.

Proof. We choose coordinates $[x : y : z]$ so that the equation of C is given by $xz - y^2 = 0$. We consider the rational parametrisation

$$\begin{aligned} \mathbb{P}^1 &\to C \\ [u : v] &\mapsto [u^2 : uv : v^2]. \end{aligned}$$

We have that $F_d(u^2, uv, v^2)$ is a homogeneous polynomial of degree $2d$ in u and v. The points of intersection of C with $F_d = 0$ correspond to the points $[u : v]$ on $\mathbb{P}^1_{\mathbb{C}}$ such that $F_d(u^2, uv, v^2) = 0$. The last polynomial is a homogeneous polynomial of degree $2d$ unless it is identically zero. If it is non-zero then it factors into the product of $2d$ linear polynomials and so $\#\{C \cap \{F_d = 0\}\} \leq 2d$, otherwise clearly $C \subset F_d = 0$. □

Lemma 6.50

For any five points in $\mathbb{P}^2$ there is a conic in $\mathbb{P}^2$ that contains them.

Remark 6.51. We have that

1. The set of non-zero homogeneous polynomials of degree 2 in $K[X, Y, Z]$ up to multiplication by a constant is $\mathbb{P}^5$.
2. Each conic defines a point in $\mathbb{P}^5$.
3. All conics passing through a point in $\mathbb{P}^2$ form a hyperplane in $\mathbb{P}^5$.
4. Since any five hyperplanes in $\mathbb{P}^5$ intersect, there is a conic through any 5 points in $\mathbb{P}^5$.

Proof. Let $\mathbb{A}^3$ be the vector space corresponding to $\mathbb{P}^2$. Pick 5 non-zero points $a_1, \ldots, a_5$ on the lines in $\mathbb{A}^3$ corresponding to point $A_1, \ldots, A_5$. By a lemma in the Kakeya conjecture section, there exists a homogeneous polynomial $F(x, y, z)$ of degree 2 vanishing a_i (the space of such polynomials has dimension 6). Therefore, $F = 0$ defines on $\mathbb{P}^2$ a conic passing through A_i. □

Definition 6.52. Let V be a vector space and V^* be its dual i.e. the space of all linear functions on V. Then the space $\mathbb{P}(V^*)$ is called **dual** to $\mathbb{P}(V)$.

Proposition 6.53

Let $A_1, \ldots, A_5$ be points in $\mathbb{P}^2$.

1. If no 4 points out of $A_1, \ldots, A_5$ lie on one line then the conic passing through $A_1, \ldots, A_5$ is unique.
2. If no 3 of the A_i lie on one line then the conic is irreducible.

Proof. We prove each statement.

1. We prove each direction.

- Proof of ($\Leftarrow$). Suppose $A_1, \dots, A_4$ lie on one line $L = 0$. Then the number of conics containing $A_1, \dots, A_5$ is infinite. Indeed, for any line $L' = 0$ that contains A_5 the degenerate conic $LL' = 0$ contains all five points.
- Proof of ($\Rightarrow$). Let M be the space of polynomials of degree at most 2, vanishing at A_i. By the Lemma (Kakeya?) from the course $\dim(M) \geq 6 - 5 \geq 1$. So there is at least one conic containing $A_1, \dots, A_5$.

  Assume now that no four points out of $A_1, \dots, A_5$ lie on one line. We will prove that the conic is unique, in other words $\dim(M) = 1$. We will treat separately two cases.

  - *Generic case, no three point out of $A_1, \dots, A_5$ lie on one line.* Assume by contradiction that $\dim(M) \geq 2$. Pick a point p on the line A_1A_2. Then for some non-zero $F \in M$ we have $F(p) = 0$. So the intersection of the conic $F = 0$ with the line A_1A_2 contains at least three point. From Bezout theorem it follows that if F is reducible, and $F = L_1 \cdot L_2$ where $L_1 = 0$ defines the line A_1A_2 and L_2 defines a second line. Since none of A_3, A_4, A_5 lie on A_1A_2, these three points lie on $L_2 = 0$, and we get a contradiction.
  - *Non-generic case, three points, say A_1, A_2, A_3 lie on one line $L = 0$.* Let $Q = 0$ be any conic, containing $A_1, \dots, A_5$. From Bezout theorem it follows that $Q = L \cdot L_1$, where L_1 has degree one. We see, that $L_1 = 0$ is the line passing through A_4 and A_5. So the conic Q is unique.

2. Take the conic $Q = 0$ that contains $A_1, \dots, A_5$. If Q is reducible, i.e., $Q = L_1L_2$, then it is clear that at least one of the lines $L_1 = 0$ or $L_2 = 0$ contains 3 points out of $A_1, \dots, A_5$. And also, if three points out of 5 are contained on a line $L = 0$, then by Bezout theorem L divides Q, i.e., Q is reducible.

□

6.4.2 Bitangent lines and Steiner's problem

Definition 6.54. We say that a line is **tangent** to an irreducible conic if it intersects it in exactly one point.

Theorem 6.55

There are at most 4 lines which are tangent to two distinct irreducible conics in $\mathbb{P}^2_{\mathbb{C}}$.

Proof. The set of all lines in $\mathbb{P}^2_{\mathbb{C}}$ is the dual $(\mathbb{P}^2_{\mathbb{C}})^*$. To find the number of bitangent lines we claim that the set of lines tangent to an irreducible conic $C \subset \mathbb{P}^2$ is a conic in $(\mathbb{P}^2_{\mathbb{C}})^*$. By Bézout's theorem two conics in $(\mathbb{P}^2_{\mathbb{C}})^*$ intersect in at most 4 points. It follows that the number of bitangents lines is ≤ 4. Indeed, we can write the equation of a line with $ax + by + cz = 0$ which is tangent to the conic $xz - y^2 = 0$ if and only if the equation $au^2 + buv + cv^2$ in $[u : v]$ has only one root. It follows that $b^2 - 4ac = 0$ which is a conic in $(\mathbb{P}^2_{\mathbb{C}})^*$. □

7 Cubic curves

Note 7.1. Throughout this section we assume K is an algebraically closed field of characteristic 0. The main goal will be to study curves of degree 3 in $\mathbb{P}^2_K$.

Theorem 7.2

Any two curves in $\mathbb{P}^2_K$ have a point of intersection.

7.1 Weierstrass normal form of cubic curves

Note 7.3. In this section, we will show that every irreducible cubic in $\mathbb{P}^2_K$ can be put in *Weierstrass form*.

Definition 7.4. Let $F \in K[X_1, \ldots, X_n]$ be a homogeneous polynomial. A point P on the hypersurface $F = 0$ is called **singular** if

$$\frac{\partial}{\partial x_i} F(P) = 0 \quad \text{for all } i = 0, 1, \ldots, n.$$

Furthermore,

- the point P is called **smooth** or **non-singular** if $\nabla F(P) \neq 0$.
- The hypersurface $F = 0$ is called **smooth** if all of its points are smooth.
- The **tangent plane** to a hypersurface $F = 0$ at a smooth point $P \in \{F = 0\}$ is the hyperplane defined by

$$\sum_{i=0}^{N} \frac{\partial}{\partial x_i} F(P) x_i = 0.$$

Definition 7.5. A projective line L is called **tangent** to a hypersurface $F = 0$ at a point p if the restriction of F to L has a double root at p.

Theorem 7.6. Smooth curves in $\mathbb{P}^2_{\mathbb{C}}$ are irreducible.

Definition 7.7. Let $F \in K[X_0, \ldots, X_n]$ be a polynomial. The **Hessian** of F is the determinant of the $(n+1)^2$ matrix $(\boldsymbol{H})_{i,j} = \dfrac{\partial^2 F}{\partial x_i {x_j}^2}$.

Definition 7.8. A point P on a curve $F = 0$ is called an **inflection point** if $\mathrm{Hess}(F)(P) = 0$.

Note 7.9. To find points of inflection on F, we need to find the intersection of the Hessian curve of F with F.

Theorem 7.10

Let C be an irreducible cubic in $\mathbb{P}^2_K$. Then for some homogeneous coordinates $[x : y : z]$ on $\mathbb{P}^2_K$ the equation for C is the following:

$$xz^2 = y^3 + ax^2y + bx^3$$

where $z^2 = f(y)$.

Note 7.11. This theorem is saying that a cubic of the form

$$y^2 = ax^3 + bx^2 + cx + d \quad \text{in } \mathbb{A}^3 \quad \sim \quad y^2z = ax^3 + bx^2z + cxz^2 + dz^3 \quad \text{in } \mathbb{P}^2.$$

In particular, the only point at infinity is $[0:1:0]$.

7.2 A lemma on 8 points

Theorem 7.12

Let $p_1, \ldots, p_8$ be points in $\mathbb{P}^2$ such that no 4 lie on one line and no 7 lie on one conic. Let M be the space of homogeneous polynomials of degree 3 in $K[X, Y, Z]$ vanishing at $p_1, \ldots, p_8$. Then $\dim(M) = 2$.

Proof. Without loss of generality, we can assume that the $p_i's$ are not in the plane $x = 0$. So, we consider $x \neq 0$ and also consider polynomials of degree ≤ 3 in $K[Y, Z]$. By some lemma in the Kakeya conjecture section we have $\dim(M) \geq 2$.

We will assume that $\dim(M) > 2$ and will get a contradiction. We consider 3 situations.

- Generic case: no 3 points on one line and no 6 points lie on one conic. Let $L = 0$ be the line passing through p_1 and p_2. We pick two distinct points from p_1 and p_2, say q and r. By a lemma in the Kakeya conjecture section there is an $F \in M$ vanishing at q and r. Then the cubic $F = 0$ intersects $L = 0$ in four points hence, by Bezout we have $F = L \cdot Q$, where Q is a conic i.e. $p_3, \ldots, p_8$ lie on Q which is a contradiction

- 3 points lie one line $L = 0$. Let $Q = 0$ be a conic passing through $p_4, \ldots, p_8$ by a lemma this conic is not unique. We also, note that $F = L \cdot Q$ belongs to M.

  Now, we consider polynomials $F_1, F_2 \in M$ such that F, F_1, F_2 are linearly independent. We pick a point p on $L = 0$. Then a linear combination $aF_1 + bF_2$ is vanishing on p and by Bezout $aF_1 + bF_2$ is divisible by L. Hence, is proportional to $L \cdot Q = F$ which is a contradiction.

- 6 points lie on a conic $Q = 0$. This is similar to (2), and we should consider $F = Q \cdot L$ where $L = 0$ joins p_7 and p_8.

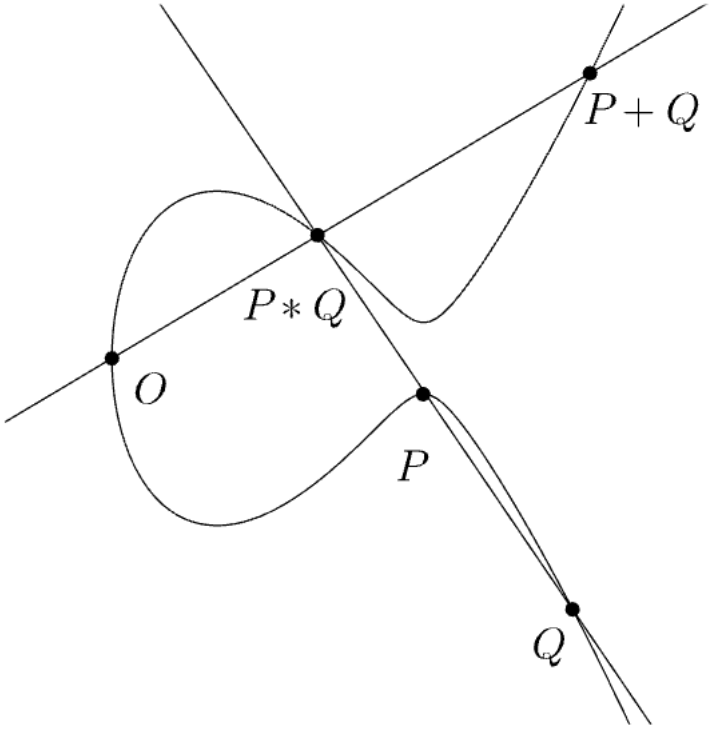
□

7.3 A group law on cubic curves

Let $C \subset \mathbb{P}^2_K$ be a cubic curve, we define on C a structure of abelian group.

- The identity element is a fixed point which we denote $O \in C$.

- The operation (addition) is defined as follows. We first need to define a different operation: take points P and Q on C and pass a line through these points. The third point of intersection on the curve is denoted by $P * Q$. TO define the addition we construct a line through O and $P * Q$ then $P + Q$ is defined as the third point of intersection of the line with C by $P + Q$. That is, $P + Q = O * (P * Q)$.



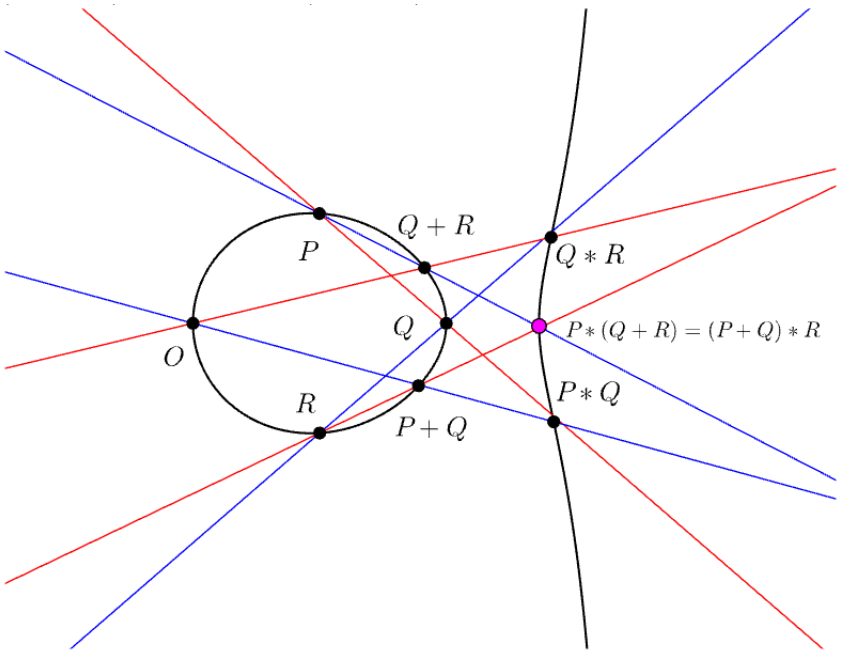
There are some special cases we need to consider when defining $P * Q$:

- If the third point of intersection does not exist then $P * Q = Q$.
- If $P = Q$ then we draw the tangent line at P then the intersection with the curve is $P * Q$.

Lemma 7.13
The operation of addition is commutative and associative.

Proof. We prove each property.

- Commutativity is clear since $P * Q$ is uniquely defined by P and Q.
- Associativity. We need to consider this figure.



Let $F = 0$ be the equation of C and let P, Q, R be three points on C it suffices to show that $(P + Q) * R = P * (Q + R)$ since this is equivalent to $(P + Q) + R = P + (Q + R)$.

Let $G = 0$ be the cubic composed of the lines $(P, Q), (O, Q + R), (R, P + Q)$ and let $H = 0$ be the cubic composed of the lines $(Q, R), (O, P + Q), (P, Q + R)$. We note that the 8 points

$$O, P, Q, R, (P * Q), (P + Q), (Q * R), (Q + R)$$

lie on cubics, $C, G = 0, H = 0$. We assume that all of these points are different, so we can use the lemma on 8 points. This theorem implies that F, G, H are linearly dependent: $H = aF + bG$. We note that F and G vanish at $(P + Q) * R$ so by the linear dependence H vanishes as it as well. We also assume $(P + Q) * R$ is different from the 8 points. Then by the linear dependence $(P, Q + R)$ contains $(P + Q) * R$.

□

Theorem 7.14

If O is a point at infinity (i.e. $[0 : 1 : 0]$) then for a point $P = (u, v)$ on the cubic we have $-P = (u, -v)$.

Proof. Lines passing through xy-plane are vertical i.e. P and $-P$ lie on a single vertical line. □

7.4 Harnack's curve theorem

Note 7.15. The main result is the Harnack's curve theorem which gives an exact upper bound on the number of connected components of a smooth curve of fixed degree.

Definition 7.16. Let $F \in \mathbb{R}[X, Y, Z]$ be a homogeneous polynomial of degree d. Suppose that the curve $F = 0$ in $\mathbb{R}P^2$ is smooth. Then this curve is composed of several connected components (in the usual topology) which are all homeomorphic to a circle. We call such connected components **ovals**.

Definition 7.17. There are two types of ovals:

- Even ovals cut $\mathbb{R}P^2$ into a union of a disc and a Mobius band.
- Odd ovals do not cut it. The complement of such curves in $\mathbb{R}P^2$ is connected.

Example 7.18. An example of an odd oval is the real projective line.

Theorem 7.19

The number of ovals of an irreducible smooth plane curve of degree d is $\leq \frac{(d-1)(d-2)}{2} + 1$.

Remark 7.20. From topology it follows that a smooth curve can have at most one odd oval. Indeed, any two odd ovals intersect, and so a curve with two odd ovals cannot be smooth.

Example 7.21

We can ask how many ovals there can be in a smooth curve of degree d.

- If $d = 1$ corresponds to a line so, there is 1 oval.
- If $d = 2$ the number is 1 or 0 (for the latter a pair of distinct lines which do not intersect).
- If $d = 3$ the number is 1 or 2.

8 Higher dimensional projective varieties

Definition 8.1. We call the **Segre map** the map

$$\sigma : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{(n+1)(m+1)-1}$$
$$([x_0 : \cdots : x_n], [y_0 : \cdots : y_m]) \mapsto [x_0y_0 : x_0y_1 : \cdots : x_0y_m : x_1y_0 : \cdots : x_iy_j : \cdots x_ny_m]$$

The image of the embedding is called the **Segre variety** $\Sigma_{n,m}$.

Theorem 8.2

The image of the Segre embedding can be identified with the set of rank one $(m+1) \times (n+1)$ matrices (up to proportionality). Indeed, for each rank 1 matrix (z_{ij}) there exists vectors $(x_0, \ldots, x_n) \in K^{n+1}$ and $(x_0, \ldots, x_m) \in K^{m+1}$ such that $z_{ij} = x_iy_j$ for all i and j.

Proposition 8.3. The image of the Segre map is a projective variety in $\mathbb{P}^{(n+1)(m+1)-1}$ given by the system of homogeneous quadratic equations $z_{ij}z_{kl} - z_{il}z_{kj} = 0$.

Corollary 8.4. Let $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ be projective varieties. Then the image $\sigma(X \times Y) \subset \mathbb{P}^{(n+1)(m+1)-1}$ of the Segre map is a projective variety.

9 Rings recap

Note 9.1. The idea of section is to consider an algebraically closed field K and an affine variety $V \subset K^n$. We will consider polynomials from $K[X_1, \ldots, X_n]$ as functions on K^n and restrict these functions to V. These restricted functions form a ring. We **claim** that if we understand this ring we understand V.

9.1 Rings and ideals

Remark 9.2. We will only consider commutative rings in this course.

Definition 9.3. For a field K a **K-algebra** is a commutative ring containing K as a subring.

Example 9.4
A typical example of a K-algebra is $K[X_1, \ldots, X_n]$.

Definition 9.5. Let R be a ring and $I \subseteq R$ be a proper ideal.

- The ideal I is said to be a **maximal ideal** of R if there is no ideal J of R such that $I \subsetneq J \subsetneq R$.
- The ideal I is called **prime** if for any a, b with $ab \in I$ we have that $a \in I$ or $b \in I$.

Example 9.6
We provide an example of a maximal ideal in the ring $\mathbb{C}[X]$. Consider the set points $x_1, \ldots, x_n \in \mathbb{C}$, now the set of polynomials which vanish at each of these points forms an ideal. However, not all ideals of this type are maximal; we have a maximal ideal when we consider the set of polynomial which vanish at one point — this is a maximal ideal.

Definition 9.7. The **radical** of an ideal I in a commutative ring R is defined as

$$\mathrm{Rad}(I) = \sqrt{I} = \{r \in R : r^n \in I \text{ for some positive integer } n\}.$$

An ideal I is called **radical** if $I = \mathrm{Rad}(I)$.

9.2 Finitely generated / Noetherian

Definition 9.8. Let R be a commutative ring and let $A \neq \varnothing$ be a subset. The **ideal generated** by A is the smallest ideal of R containing A. Equivalently, it is the collection of all finite linear combinations of elements of A:

$$(A) = \left\{ \sum_{i=1}^{N} b_i x_i : b_i \in R, x_i \in A \right\}.$$

An ideal generated by the elements $\{x_1, \ldots, x_n\}$ is denoted as $(x_1, \ldots, x_n)$.

Definition 9.9. An ideal $I \subset R$ is said to be **finitely generated** if there exists a finite subset $A = \{x_1, \ldots, x_n\} \subset R$ such that $I = (x_1, \ldots, x_n)$.

Definition 9.10. A ring R is called **Noetherian** if every ideal of R is finitely generated.

Lemma 9.11 (Characterisation of Noetherian rings)
Let R be a ring. The following conditions are equivalent:

1. The ideals of R satisfy the **Ascending chain condition** (ACC) i.e. if for the chain $I_1 \subset I_2 \subset \cdots$ are proper ideals of R, then there exists an N such that for all $n > N$ we have $I_n = I_N$.
2. Every ideal of R is finitely generated.

Proof. We prove each direction in turn. We prove the **contrapositive** statements.

- Proof of (1) $\Rightarrow$ (2). Suppose an ideal $I \subset R$ is not finitely generated. We will construct by induction an infinite sequence of elements $x_1, \ldots, x_n, \ldots \in I$ such that the ideals $I_n = (x_1, \ldots, x_n)$ form an infinite strictly increasing chain (which will contradict the ACC condition). Suppose we have already constructed $x_1, \ldots, x_N$. Since $(x_1, \ldots, x_n) \neq I$ we can find $x_{n+1} \in I$ such that $x_{n+1} \notin (x_1, \ldots, x_n)$.
- Proof of (2) $\Rightarrow$ (1). If $I_1 \subsetneq I_2 \subsetneq \cdots$ are proper ideal in R then $I = \bigcup_{i \in \mathbb{N}} I_i$ is a proper ideal in R (since it does not contain 1). This ideal cannot be finitely generated. Indeed, for any collection of elements $x_1, \ldots, x_n \subset I$ there exists a k such that $x_1, \ldots, x_n \in I_k$. Therefore, $x_1, \ldots, x_n$ do not generate I_{k+1}. Hence, they do not generate I.

□

Example 9.12

We provide some examples and counterexamples of Noetherian rings.

- The ring $\mathbb{Z}$ and $K[X]$ are Noetherian since they are principal ideal domains, i.e. every ideal is generated by one element.
- The ring of continuous functions on $[0,1]$ is not Noetherian. Indeed, we can consider the sequence of ideals I_n of functions vanishing on $\left[0, \frac{1}{n}\right]$.
- The ring of analytic functions in one variable is not Noetherian. Indeed, we can consider the chain of ideals $(\sin x)$, $\left(\frac{\sin x}{x}\right)$, $\left(\frac{\sin x}{(x(x-\pi))}\right)$, …, this clearly does not stabilise.

9.3 Hilbert's basis theorem

Theorem 9.13

Let R be a commutative ring. If R is Noetherian then so is $R[X]$.

Proof. Suppose I is an ideal of $R[X]$. We will prove that I is finitely generated.

First, we construct a sequence of embedded ideals in $I_0 \subseteq I_1 \subseteq \ldots \subseteq I_n \subseteq \ldots \subseteq R$. The ideal I_i is generated by the leading coefficients of all polynomials of degree i in I, i.e., if $a_i x^i + a_{i-1}x^{i-1} + \ldots + a_0 \in I$, then $a_i \in I_i$.

Let's show that $I_i \subseteq I_{i+k}$ for $k \geq 0$. Indeed, if we multiply $a_i x^i + a_{i-1}x^{i-1} + \ldots + a_0$ by x^k, the leading coefficient doesn't change. Also, since R is Noetherian, the chain of ideals I_i stabilizes for some n so that $I_n = I_{n+1} = \ldots$.

We will now construct a finite set of polynomials, generating I.

For each $i = 0, \ldots, n$ choose S_i to be a finite set of polynomials in $I \subset R[X]$ of degree i whose leading coefficients generate I_i. We claim that the finite union $S = S_0 \cup \ldots \cup S_n$ generates I, in other words $(S) = I$.

Proof of $I = (S)$. Indeed, take a polynomial $f = a_m x^m + a_{m-1}x^{m-1} + \ldots \in I$. Let's first show that there exists a polynomial $g \in (S)$, of degree m with leading coefficient a_m. If $m \leq n$, then $a_m \in I_m$ and so there is $g \in (S_m)$ of degree m and with leading coefficient a_m. If $m > n$ then $a_m \in I_n$, so we can find $a_m x^n + \ldots + a_0 \in (S_n)$ and set $g = x^{m-n}(a_m x^n + \ldots + a_0)$.

Now, $f - g$ has degree at most $m-1$ and $g \in (S)$. Repeating the above procedure m times, we see $f \in (S)$. I.e., $(S) = I$. □

Corollary 9.14. For any Noetherian ring R the ring $R[X_1, \ldots, X_n]$ is Noetherian. In particular, we can take R to be equal to any field K.

Proof. We prove this by induction on n. The base case is trivial since R is Noetherian. Suppose $R[X_1, \ldots, X_n]$ is Noetherian we have an isomorphism

$$R[X_1, \ldots, X_{n+1}] = R[X_1, \ldots, X_n][X_{n+1}],$$

i.e. the polynomial ring in $n+1$ variables with coefficients in R can be seen as the polynomial ring in X_{n+1} with coefficient in $R[X_1, \ldots, X_n]$. Hence, it is Noetherian by induction. □

Definition 9.15. A commutative ring R is **finitely generated over its subring** A if there exists elements $r_1, \ldots, r_n \subset R$ such that for any $r \in R$ there is a polynomial $P \in A[X_1, \ldots, X_n]$ such that $r = P(x_1, \ldots, x_n)$.

Corollary 9.16. Let A be a Noetherian ring, and let R be a ring finitely generated over A, then R is Noetherian.

Proof. Suppose that R is generated by elements $(r_1, \ldots, r_n)$. Take the ring $A[X_1, \ldots, X_n]$ (which is Noetherian) and consider the surjective homomorphism $\phi : A[X_1, \ldots, X_n] \to R$ such that $x_i \mapsto r_i$. Since, the ACC holds for ideals in $A[X_1, \ldots, X_n]$ it must also hold for ideals in R because ϕ is surjective and the pre-image of an ideal under ϕ is an ideal. □

10 Varieties

Note 10.1. The goal of this section is to discuss the following equivalence for an algebraically closed field K:

$$\text{Affine varieties in } K^n \iff \text{Radical ideals in } K[X_1, \ldots, X_n].$$

10.1 From ideals to affine varieties

Note 10.2. We construct a map that associates each ideal $I \subset K[X_1, \ldots, X_n]$ the affine variety $V(I)$ in $\mathbb{A}^n_K$.

Definition 10.3. For each ideal $I \subset K[X_1, \ldots, X_n]$ define

$$V(I) = \{p \in \mathbb{A}^n_K : f(p) = 0 \; \forall f \in I\}.$$

Proposition 10.4. We have that $V(I)$ is an affine variety.

Proof. By Hilbert's basis theorem each ideal in $K[X_1, \ldots, X_n]$ is generated by a finite number of elements $f_1, \ldots, f_N$. □

Proposition 10.5

The map $I \to V(I)$ from ideals in $R = K[X_1, \ldots, X_n]$ to affine varieties in $\mathbb{A}^n_K$ has the following properties:

1. $V(\{0\}) = \mathbb{A}^n_K$ and $V(R) = \varnothing$;
2. If $I \subset J$ then $V(J) \subset V(I)$;
3. $V(I) \cup V(J) = V(I \cap J)$;
4. $\bigcap_m V(I_m) = V(\sum_m I_m)$ where $\sum_m I_m$ denotes the ideal consisting of finite linear combinations of elements in I_m with coefficients in R.

Proof. We prove each statement in turn.

1. We have.

- Let $I = \{0\}$, the ideal consisting only of the zero polynomial. Any point in affine space $\mathbb{A}^n$ satisfies all polynomials in I, including the zero polynomial. Therefore, $V(\{0\}) = \mathbb{A}^n$.
- Let $I = K[X_1, \ldots, X_n]$, the ideal consisting of all polynomials with coefficients in field K. Since I includes the constant polynomial 1, no point in affine space $\mathbb{A}^n$ can satisfy all polynomials in I, including the constant polynomial 1. Thus, $V(K[X_1, \ldots, X_n]) = \varnothing$.

2. The more constraints in the form of equations we add, then we will have fewer solutions.

   Given $I \subset J$, let P be a point in $V(J)$. This means that every polynomial in J vanishes at P. Since I is a subset of J, every polynomial in J is also in I. Therefore, every polynomial in I vanishes at P, which implies that P is also in $V(I)$. Thus, we've shown that if P is in $V(J)$, then P is in $V(I)$, which means $V(J) \subset V(I)$.

3. We have to prove the double inclusion.

   - We prove $V(I) \cup V(J) \subset V(I \cap J)$. Since $I \cap J \subset I$ by (2) we have $V(I) \subset V(I \cap J)$ and similarly $V(J) \subset V(I \cap J)$.
   - We prove $V(I \cap J) \subset V(I) \cup V(J)$. Take a point $p \in V(I \cap J)$. If $p \notin V(I)$ then $f(p) \neq 0$ for some element $f \in I$. Similarly, if $p \notin V(J)$ then $g(p) \neq 0$ for some element $g \in J$. Then $f \cdot g \in I \cap J$ and $(f \cdot g)(p) \neq 0$, which contradicts the assumption that $p \in V(I \cap J)$.

4. Take a point $p \in \bigcap_m V(I_m)$ then $f_m(p) = 0$ for all $f_m \in I_m$. It follows that $f(p) = 0$ for all finite linear combinations of elements of I_m. So, $p \in V\left(\sum I_m\right)$ and we conclude $\bigcap_m V(I_m) \subset V(\sum I_m)$.

   On the other hand, $I_n \subset \sum I_m$ for every n, hence $V(\sum_m I_m) \subset V(I_n)$ for every n and therefore $V(\sum_m I_m) \subset \bigcap_n V(I_n)$.

□

10.2 From varieties to ideals: the vanishing ideal

Definition 10.6. Let $V \subset \mathbb{A}^n$ be an affine variety. The **vanishing ideal** of V in $K[X_1, \ldots, X_n]$ is

$$I(V) = \{f \in K[X_1, \ldots, X_n] : f(p) = 0 \ \forall p \in V\}.$$

Lemma 10.7. For any affine variety V the ideal $I(V)$ is radical.

Proof. If $f \in \mathrm{Rad}(I(V))$ then $f^n \in I(V)$ for some n i.e. f^n vanishes at V for some n. Therefore, f must vanish at V which implies that $f \in I(V)$ hence, $I(V)$ is radical. □

Lemma 10.8
We have the following.

1. For any affine variety V we have $V(I(V)) = V$.
2. For any ideal I we have $I \subset I(V(I))$.
3. If I is not radical $I \subsetneq I(V(I))$.

Proof. We prove each statement in turn.

1. We have to prove the double inclusion.
   - $\subset$. Take a point $p \notin V$ since V is an affine variety we have that V is given by a set of equations $f_1 = \cdots = f_n = 0$. So, for some i we have that $f_i(p) \neq 0$. Since $f_i \in I(V)$ it follows that $p \notin V(I(V))$.
   - $\supset$. By definition of $I(V)$ any $f \in I(V)$ vanishes on V.
2. Any $f \in I$ vanishes on $V(I)$.
3. This follows from (2) and some lemma.

□

10.3 Hilbert's Nullstellensatz

Theorem 10.9 (Hilbert's Nullstellensatz)
If K is an algebraically closed field, then for each ideal J in $K[X_1, \ldots, X_n]$ we have $I(V(J)) = \mathrm{Rad}(J)$.

Note 10.10. This theorem provides a bijection between affine varieties and radical ideals.

Corollary 10.11
The following two equivalent statements are called the **weak Nullstellensatz theorem**.

1. If K is an algebraically closed field, then for any ideal $J \subset K[X_1, \ldots, X_n]$ we have that $V(J) = \varnothing \iff J = K[X_1, \ldots, X_n]$.
2. Every maximal ideal of $K[X_1, \ldots, X_n]$ is of the form $m_a = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$, where $a_1, \ldots, a_n \in K$.

Proof. We prove each statement in turn.

1. We prove each direction.
   - Proof of ($\Rightarrow$). Suppose $V(J) = \varnothing$ then by the Nullstellensatz we have that $\mathrm{Rad}(J) = I(V(J)) = I(\varnothing) = K[X_1, \ldots, X_n]$. Therefore, $1 \in \mathrm{Rad}(J)$ which implies $1 \in J$ as well.

- Proof of ($\Leftarrow$). If $1 \in J$ then $V(J) = \varnothing$.

2. Consider the evaluation map $K[X_1 \ldots, X_n] \to K$ that sends any polynomial f to its value at a. The kernel of this map is precisely m_a. It follows that the quotient $K[X_1, \ldots, X_n]/m_a = K$ is a field hence, m_a is maximal.

□

Example 10.12

Take the polynomials $p, q \in \mathbb{C}[X_1, \ldots, X_n]$. If p is irreducible and q vanishes at the hypersurface $p(x_1, \ldots, x_n) = 0$ then p divides q. Indeed, q vanishes on $p = 0$ so by the Nullstellensatz $q \in \mathrm{Rad}((p))$ i.e. $q^n \in (p)$ for some n. At the same time $\mathbb{C}[X_1, \ldots, X_n]$ is a UFD so $q \in (p)$.

10.4 The coordinate ring $K[V]$

Note 10.13. We want to associate a ring to every variety as we did with ideals and varieties.

Definition 10.14. Let $V \subset \mathbb{A}^n_K$ be an affine variety. We define the **coordinate ring** of V as the quotient $K[V] = K[X_1, \ldots, X_n]/I(V)$. The quotient map is $\varphi : K[X_1, \ldots, X_n] \to K[V]$.

Example 10.15

The coordinate ring $\mathbb{C}[\{0\}] = \mathbb{C}$. Clearly $I(\{0\}) = (x)$ so $\mathbb{C}[X]/(x) \cong \mathbb{C}$.

Definition 10.16. A K-valued function f on V is **regular** if there is a polynomial $F \in K[X_1, \ldots, X_n]$ such that restriction of F to V is f, i.e. $F|_V = f$.

Proposition 10.17. Let $V \subset \mathbb{A}^n_K$ be an affine variety. Then regular functions on V form a ring which is isomorphic to $K[V]$.

Proposition 10.18

Let V be an affine variety. Points of V are in one-to-one correspondence with maximal ideals in $K[V]$.

Proof. We prove each correspondence in turn.

- Points to maximal ideals. Take a point $a \in V$ and let $m_a \subset K[V]$ be the ideal of elements vanishing at a. Consider the homomorphism $K[V] \to K$ that takes a regular function $f \in K[V]$ to $f(a)$. Clearly, m_a is the kernel of the homomorphism, so $K[V]/m_a \cong K$ and m_a is maximal.

- Maximal ideals to points. For any maximal ideal $m \subset K[V]$ we find a point $a \in V$ where all elements of m vanish. Since $\varphi : K[X_1, \ldots, X_n] \to K[V]$ is surjective, we can consider the composition of the quotient homomorphism $K[X_1, \ldots, X_n] \to K[V] \to K[V]/m$. The kernel of the map $K[X_1, \ldots, X_n] \to K[V]/m$ is given by $\phi^{-1}(m)$ (the pre-image) so, by the isomorphism theorem we have that

$$K[X_1, \ldots, X_n]/\varphi^{-1}(m) \cong K[V]/m.$$

  Since m is maximal we have that $K[V]/m$ is a field which implies the following ring $K[X_1, \ldots, X_n]/\varphi^{-1}(m)$ is also a field hence, $\varphi^{-1}(m)$ is maximal. Using the weak Nullstellensatz we know that

$$\varphi^{-1}(m) = ((X_1 - a_1), \ldots, (X_n - a_n)),$$

  for some $a \in K^n$.

  We prove that $a \in V$. Indeed, the above, all element of $\varphi^{-1}(m)$ vanish at a. At the same time, we have $I(V) = \varphi^{-1}(0) \subset \varphi^{-1}(m)$. So all elements of $I(V)$ vanish at a which implies $a \in V$. Finally, $m \subset K[V]$ is generated by restrictions of $X_i - a_i$ to V so all the elements of m vanish at $a \in V$.

□

10.5 Regular maps

Definition 10.19. Let $X \subset \mathbb{A}^n_K$ and $Y \subset \mathbb{A}^m_K$ be affine varieties. A map $f : X \to Y$ is **regular** if there exists m polynomials $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ such that $f(x) = (f_1(x), \ldots, f_m(x))$ for all $x \in X$.

Definition 10.20. A regular map $f : X \to Y$ is called an **isomorphism** if it has a regular inverse. That is there exists a regular map $g : Y \to X$ such that $f \circ g = \mathrm{id}_X$ and $g \circ f = \mathrm{id}_Y$. In this case we say that X and Y are isomorphic.

Example 10.21 (Exam Question)
Is there an isomorphism between $\mathbb{C}^1$ and the conic $xy = 1 \in \mathbb{C}^2$.

Solution. It suffices to establish that $\mathbb{C}[X] \ncong \mathbb{C}[X, Y]/(xy = 1)$. In the RHS we have that $xy = 1$ if this was an isomorphism then in LHS there must exist two polynomials whose product is 1 which is not possible unless they are constants.

Definition 10.22. Let $f : X \to Y$ be a regular map between algebraic varieties X and Y. Then for any regular function u on Y, define the **pull-back** of u, denoted $f^*(u)$, as a function on X by the rule $f^*(u)(x) = u(f(x))$, for each $x \in X$.

It follows that $f^*(u)$ is also a regular function on X.

Example 10.23
Let $X \subset \mathbb{A}^n_K$ be an affine variety and let $f = (f_1, \ldots, f_m) : X \to \mathbb{A}^m_K$ be a regular map. Let $y_1, \ldots, y_m$ be coordinates on $\mathbb{A}^m_K$ then $f^*(y_i) = f_i$.

Lemma 10.24. Let X and Y be affine varieties. Any homomorphism $\varphi : K[Y] \to K[X]$ (as K-algebras) is of the form $\varphi = f^*$ for some regular map $f : X \to Y$.

Proof. Let $y_1, \dots, y_m$ be coordinates in the space $\mathbb{A}^m_K$ of Y. We have that $y_i \in K[Y]$ hence $\varphi(y_i) \in K[X]$. Set $\varphi(y_i) = f_i$ and consider the map $f(x) = (f_1(x), \dots, f_m(x))$. The map $f : X \to \mathbb{A}^m_K$ is regular, and it satisfies the property $f^*(y_i) = f_i = \varphi(y_i)$.

We now prove that $f(X) \subset Y$. Take any point $x \in X$ and any polynomial $H \in I(Y)$. We show that $H(f(x)) = 0$. Since $H \in I(Y)$ we have that $H(y_1, \dots, y_m)$ is the zero element in $K[Y]$. Then, clearly $0 = \varphi(H(y_1, \dots, y_n)) = H(f_1, \dots, f_m) \in K[X]$ i.e. this expression vanishes on X. We conclude,

$$H(f(x)) = H(f_1(x), \dots, f_m(x)) = 0.$$

The claim holds for any $H \in I(Y)$ so $f(x) \in Y$. □

Theorem 10.25

Let $X \subset \mathbb{A}^n_K$ and $Y \subset \mathbb{A}^m_K$ be affine varieties. We have that X and Y are isomorphic if and only if their coordinate rings $K[X]$ and $K[Y]$ are isomorphic as K-algebras.

Proof. Suppose $f : X \to Y$ is an isomorphism and g is its inverse. We prove that $f^* : K[Y] \to K[X]$ and $g^* : K[X] \to K[Y]$ are isomorphisms i.e. inverse to each other.

Indeed, fg is identical on Y so $(fg)^* = g^* f^*$ is the identity homomorphism from $K[Y] \to K[Y]$ (by the definition of pullback). The same holds for $f^* g^*$.

We now suppose that $\varphi : K[Y] \to K[X]$ is an isomorphism the by the lemma above $\varphi = f^*$ for some regular map $f : X \to Y$ and $\varphi^{-1} = g^*$ for some regular map $g : Y \to X$. Note that gf induces the identity map $f^* g^* = \varphi\varphi^{-1} : K[X] \to K[X]$. We also conclude that gf is identical and so f and g are inverse. □

Example 10.26

Consider $\mathbb{C}^1$ and the parabola $y = x^2$. These two spaces are isomorphic. Clearly, the maps $(x, y) \mapsto x$ and $x \mapsto (x, y)$ establish this.

11 Hilbert's functions and Hilbert polynomials

11.1 Graded rings and modules and the Hilbert function

Definition 11.1. A **graded ring** is a ring with a direct sum decomposition

$$S = S_0 \oplus S_1 \oplus \cdots$$

satisfying the following properties:

1. Each S_i is closed under addition;
2. $S_i S_j \subset S_{i+j}$ for $i, j \geq 0$;
3. An element of S is a finite sum of elements from different S_i.

Definition 11.2. An element $s \in S$ is **homogeneous** if $s \in S_i$ for some i. A **homogeneous ideal** of S is an ideal generated by homogeneous elements.

Example 11.3. $S = K[X_1, \dots, X_n]$ graded by degree

$$S = S_0 \oplus S_1 \oplus \cdots$$

where S_d is the vector space of homogeneous polynomials of degree d.

Remark 11.4. We will only consider rings such that

1. $S_0 = K$,
2. S is generated by $S_0 \oplus S_1$,
3. S_1 is a finite-dimensional vector space over K.

In such rings each S_i is a finite-dimensional vector space over K.

Definition 11.5. Let S be a graded ring finitely generated over $S_0 = K$. The **Hilbert function of** S is defined as $h_S(d) = \dim(S_d)$.

Example 11.6
Let $S = K[X_0, \dots, X_N]$ then $h_S(d) = \binom{n+d}{d}$.

Definition 11.7. Let $X \subset \mathbb{P}^n_K$ be a projective variety. The **homogeneous ideal** $I(X)$ is the ideal in $K[X_0, \dots, X_n]$ generated by all homogeneous polynomials vanishing on X.

Definition 11.8. The **homogeneous coordinate ring** $S(X)$ of X is the quotient ring $K[X_0, \dots, X_n]/I(X)$.

Proposition 11.9
We have that:

- $I(X)$ is a graded ring, namely $I(X) = \bigoplus_d I(X)_d$ where $I(X)_d$ is the space of degree d polynomials in $K[X_0, \dots, X_n]$ vanishing on X.
- $S(X)$ is graded, namely $S(X)_d = S_d/I(X)_d$.

Proposition 11.10. Let $X_F \subset \mathbb{P}^n$ be a hypersurface defined by a homogeneous polynomial F. We have that $I(X_F) \subset K[X_0, \dots, X_n]$ is the vanishing ideal of the variety $V((F))$.

Note 11.11. In other words, every polynomial vanishing on $\{F = 0\} \subset \mathbb{A}^{n+1}$ is a sum of homogeneous polynomials vanishing on $\{F = 0\}$.

Proof. We prove the double inclusion of $I(X_F) = I(V((F)))$.

- $\subset$. Let $f \in I(X_F)$. This means that f vanishes on the hypersurface X_F. Thus, f vanishes at every point of X_F, which implies that f vanishes on the variety $V((F))$ as well. Hence, $f \in I(V((F)))$.
- $\supset$. Let $G \in K[X_0, \ldots, X_n]$ and let

$$G = G_1 + \cdots + G_k$$

be its decomposition into homogeneous components. Suppose G vanishes on $V((F))$. Then each G_i vanishes on $V((F))$. So each G_i vanishes on the hypersurface X_F. So $G = \sum_i G_i \subset I(X_F)$ i.e. $I(V((F))) \subset I(X_F)$.

□

Definition 11.12. The **Hilbert function** h_X of a projective variety X is the Hilbert function of its homogeneous coordinate ring i.e. $h_X(m) = \dim(S(X)_m)$.

Example 11.13

The Hilbert function of $\mathbb{P}^n$ is $h_{\mathbb{P}^n}(d) = \binom{n+d}{n}$. Indeed, by definition the homogeneous coordinate ring $S(\mathbb{P}^n)$ of $\mathbb{P}^n$ is $K[X_0, \ldots, X_n]$.

Definition 11.14. By **Hilbert function of an ideal** h_I we denote the Hilbert function on the ring $K[X_0, \ldots, X_n]/I$.

Note 11.15. The Hilbert function $h_I(t)$ of an ideal I in a polynomial ring measures the vector space dimension consisting of all polynomials of a given degree t modulo the ideal.

Example 11.16

For the given ideal $I = (x_1^5, x_1x_2^2, x_2^3) \subset K[x_1, x_2]$, the Hilbert function counts the number of independent monomials of degree t that are not in I.

To determine $h_I(t)$, we count such monomials for each degree t:

- For $t = 0$, the monomial is 1, which gives $h_I(0) = 1$.
- For $t = 1$, the monomials are x_1 and x_2, thus $h_I(1) = 2$.
- For $t = 2$, the monomials are x_1^2, x_1x_2, and x_2^2, yielding $h_I(2) = 2$.
- For $t = 3$, the monomials are $x_1^3, x_1^2x_2$, and $x_1x_2^2$ (since $x_1x_2^2$ is in I), giving $h_I(3) = 2$ (not 1 as incorrectly stated).
- For $t = 4$, $x_1^4, x_1^3x_2$, and $x_1^2x_2^2$ are the monomials not in I, so $h_I(4) = 3$.
- For $t \geq 5$, all monomials of that degree are divisible by at least one generator of I, hence $h_I(t) = 0$.

Therefore, the corrected Hilbert function should be:

$$\begin{aligned} h_I(0) &= 1, \\ h_I(1) &= 2, \\ h_I(2) &= 2, \\ h_I(3) &= 2, \\ h_I(4) &= 3, \\ h_I(t) &= 0 \text{ for } t \geq 5. \end{aligned}$$

11.2 Hilbert polynomials

Theorem 11.17

For any projective variety X (or a homogeneous ideal $I \subset K[X_0, \ldots, X_n]$) the Hilbert function $h_X(d)$ (or $h_I(d) = \dim(S_d/I_d)$) is equal to a certain polynomial for large enough $d > 0$.

Definition 11.18. Let $X \subset \mathbb{P}^n$ be a projective variety. The unique polynomial p_X such that $p_X(d) = h_X(d)$ for large d is called the **Hilbert polynomial** of X.

Definition 11.19. Suppose $p_X(d) = a_kd^k + \cdots a_0$ with $a_k \neq 0$. The **dimension** of X is defined to be $\dim(X) = k$. The **degree** of X is defined to be $\deg(X) = k! \cdot a_k$.

Remark 11.20. The geometric definition. Suppose $X \subset \mathbb{P}^n$ is a projective variety, then $\dim(X) = n - (\text{maximal dimension of } \mathbb{P}^k \text{ such that } \mathbb{P}^k \cap X = \varnothing) - 1$. Moreover, the degree of X is given by $\deg(X) = \#\text{of points intersection of } X \text{ with a generic plane } \mathbb{P}^{n-\dim(X)}$.

11.2.1 The Hilbert polynomial of a hypersurface

Lemma 11.21
Let $F \in K[X_0, \ldots, X_n] = R$ be an irreducible, homogeneous polynomial of degree d. Let X_F be the hypersurface in $\mathbb{P}^n$ given by the equation $F = 0$. The Hilbert polynomial of X_F is

$$p_{X_F}(m) = \binom{m+n}{n} - \binom{m+n-d}{n}.$$

12 Higher dimensional Bézout's theorem

12.1 Exact sequences and Hilbert functions

Lemma 12.1 (Exact sequences)**.** Let $f : U \to V$ and $g : V \to W$ be linear maps of K-vector spaces. Assume that f is injective, g is surjective, and that $\mathrm{Im}(f) = \ker(g)$. That is,

$$0 \to U \xrightarrow{f} V \xrightarrow{g} W \to 0$$

is an exact sequence. Then $\dim(V) = \dim(U) + \dim(W)$.

Proof. This follows from the rank-nullity theorem. We have

$$\begin{aligned} \dim(V) &= \dim(\ker(g)) + \dim(\mathrm{Im})(g) \\ &= \dim(\mathrm{Im}(f)) + \dim(W) \\ &= \dim(U) + \dim(W). \end{aligned}$$

□

Proposition 12.2
Let $I, J \subset K[X_0, \ldots, X_n]$ be two homogeneous ideals. Then $h_{I\cap J} + h_{I+J} = h_I + h_J$.

Proof. Set $R_i = K[X_0, \ldots, x_i]$. For each m we have the following exact sequence

$$0 \to R_m/(I_m \cap J_m) \to R_m/I_m \times R_m/J_m \to R_m/(I_m + J_m) \to 0.$$

The first non-trivial map sends $[f] \to ([f], [f])$ and the second map $([f], [g]) \to [f] - [g]$. Now apply the lemma above. □

Lemma 12.3. Let $I \subset K[X_0, \ldots, X_n]$ be a homogeneous ideal and let $f \in K[X_0, \ldots, X_n]$ such that $f \notin I$ be a homogeneous polynomial of degree N. Assume that $K[X_0, \ldots, X_n]/I$ is an integral domain. Then

$$h_{I+(f)}(d) = h_I(d) - h_I(d - N) \quad \text{for } d > N.$$

12.2 Higher dimensional Bézout's theorem

Theorem 12.4
Let $X \subset \mathbb{P}^n_K$ be an irreducible projective variety of dimension at least 1 and let $f \in K[X_0, \ldots, X_n]$ be a homogeneous polynomial that does not vanish on X. Then $\deg(I(X) + (f)) = \deg(X)\deg(f)$.

13 Interesting results for the exam

Theorem 13.1

Let $F = \sum a_i z_0^i z_1^{d-i}$ be a homogeneous polynomial in two variables, $a_i \in \mathbb{C}$. We can write $F = \prod_{k=1}^{d}(b_k z_0 + c_k z_1)$