Algebraic Geometry Notes

Alexandre Daoud

May 2, 2016

1 Bézout's Theorem

Definition 1.1. Let K be a field. We define **n-dimensional affine space** over K to be

$$\mathbb{A}_K^n = \{ (a_1, \dots, a_n) \mid a_i \in K \}$$

Definition 1.2. Let K be a field. A subset $V \subseteq \mathbb{A}_n^K$ is called an **affine variety** if there exist polynomials $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ such that

$$V = \{ (a_1, \dots, a_n) \in \mathbb{A}_K^n \mid f_i(a_1, \dots, a_n) = 0 \, \forall \, 1 \leq i \leq m \}$$

Let K be a field. Recall that a polynomial $f \in K[X_1, \dots, X_n]$ is called **irreducible** if there does not exist two polynomial $g, h \in K[X_1, \dots, X_n]$ of degree greater than or equal to one such that $f = gh$. Furthermore, since K is a field, $K[X_1, \dots, X_n]$ is a principal ideal domain and, in particular, a unique factorisation domain.

Definition 1.3. Let K be a field and $f(X) = \sum_{i=0}^n a_i X^i, g(X) = \sum_{i=0}^m b_i X^i \in K[X]$ be polynomials such that $a_n b_n \neq 0$. We define the **resultant** of $f(X)$ and $g(X)$ to be

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

where the α_i and β_j are the roots of f and g respectively.

It is clear from the definition of the resultant that two polynomials f and g have a common root if and only if their resultant vanishes.

Proposition 1.4. *Let K be a field and $f = \sum_{i=0}^n a_i X^i, g = \sum_{i=0}^n b_i X^i \in K[X]$ be polynomials. Then $R[f, g]$ is equal to the determinant of the **Sylvester matrix***

$$\begin{pmatrix}
a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 & 0 \\
0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 \\
b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 & 0 \\
0 & b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & b_m & b_{m-1} & \cdots & b_1 & b_0
\end{pmatrix}$$

Proof. The resultant vanishes if and only if f and g have a common root. This means their greatest common divisor is non-trivial. Hence there exists polynomials $r(X)$ and $s(X)$ of degree at most $m-1$ and $n-1$ respectively such that $f(X)r(X)+s(X)g(X)=0$. We may consider the $m+n$ coefficients of $r(X)$ and $s(X)$ as unknowns which gives us a system of $m+n$ homogeneous equations in $m+n$ unknowns. This system of equations has a non-trivial solution if and only if the determinant of the Sylvester matrix vanishes. Now the determinant and $R[f,g]$ are homogeneous expressions of degree m in the a_i and degree n in the b_i so they must be equal up to a constant. To see that the constant is in fact 1, we need only consider the coefficient of the term $a_n^m b_0^n$. □

Proposition 1.5. *Let K be a field and $f,g \in K[X,Y]$ be polynomials of degree n and m respectively. If the number of solutions to $f(X,Y)=g(X,Y)=0$ is finite then it is at most nm.*

Proof. This is tautologically true if $|K|<\infty$. Hence suppose that K is an infinite field. Since the number of solutions to $f(X,Y)=g(X,Y)=0$ is finite, there exists a line through the origin, say l, such that any line parallel to l contains only one solution of the equation. We may thus perform a linear change of coordinates so that every solution to $f(X,Y)=g(X,Y)=0$ has a different X-coordinate. Now consider f and g as elements of $K[X][Y]$. In other words, f and g are polynomials in Y over $K[X]$. Writing this explicitly we have

$$f(X,Y)=\sum_{i=0}^{n} f_i(X)Y^i, \quad g(X,Y)=\sum_{j=0}^{m} g_j(X)Y^j$$

where $\deg(f_i)\leq n-i$ and $\deg(g_j)\leq m-j$. Now, $R[f,g]\in K[X]$. By definition, $R[f,g]$ has a root at $X=c$ if and only if $f(c,Y)$ and $g(c,Y)$ have a common root. Hence the number of solutions of the equation $f(X,Y)=g(X,Y)=0$ is at most the number of roots of $R[f,g]$. We claim that $R[f,g]$ has degree at most mn whence the theorem will follow. Indeed, for simplicity we may assume that $\deg(f_i)=n-i$ and $\deg(g_i)=m-i$. Then the diagonal of the Sylvester matrix contributes a polynomial of degree mn to the determinant. All other terms of the determinant are given by polynomials of degree at most mn. The proposition is thsu proven. □

Proposition 1.6. *Let K be a field. Suppose that $f\in K[X,Y]$ is irreducible and $g\in K[X,Y]$ is an arbitrary polynomial. If f does not divide g then $f(X,Y)=g(X,Y)=0$ has a finite number of solutions.*

Proof. Suppose that X appears with at least degree 1 in f. We claim that $f(X,Y)$ is irreducible in $K(Y)[X]$. Suppose that $f=\overline{h_1h_2}$ where $\overline{h_1h_2}\in K(Y)[X]$. Let $a_1(Y),a_2(Y)\in K[Y]$ be the denominators of $\overline{h_1},\overline{h_2}$. Let h_i represent the $\overline{h_i}$ multiplied by the a_i. Then $h_1, h_2 in K[X,Y]$ and we have

$$a_1a_2f=h_1h_2$$

Since f is irreducible and $K[X,Y]$ is a UFD, we must have that $f|h_1$ or $f|h_2$. But h_1 and h_2 both have degree of X less than f which is a contradiction. Hence f must be irreducible in $K(Y)[X]$. By similar argumentation, we see that g is not divisible by f in $K(Y)[X]$. Hence f and g have no common factors in $K(Y)[X]$. Hence there must exist two polynomials $\overline{u},\overline{v}\in K(Y)[X]$ such that

$$f\overline{u}+g\overline{v}=1$$

Let $a \in K[Y]$ be the least common multiple of all the denominators of the coefficients of $\overline{u}$ and $\overline{v}$. Denote $u = a\overline{u}$ and $v = a\overline{v}$. We then have that

$$fu + gv = a$$

Hence the Y-coordinates of all solutions of $f(X,Y) = g(X,Y) = 0$ must all be roots of $a \in K[Y]$. Since $f(X,Y)$ can have only finitely many solutions on any line $Y = c$, it must then have finitely many solutions (X,Y). □

Theorem 1.7 (Bézout's Theorem). *Let K be a field and $f, g \in K[X,Y]$ be polynomials with no common factors. Then the number of solutions to $f(X,Y) = g(X,Y) = 0$ is at most* $\deg(f)\deg(g)$.

Proof. Since $K[X,Y]$ is a UFD, we can write $f = f_1, \ldots, f_n$ for some irreducible polynomials $f_i \in K[X,Y]$. We may apply Proposition 1.6 to see that $f_i(X,Y) = g(X,Y) = 0$ has only finitely many solutions for all $1 \leq i \leq n$. Appealing to Proposition 1.5, we see that $f_i(X,Y) = g(X,Y) = 0$ has at most $\deg(f_i)\deg(g)$ solutions whence $f(X,Y) = g(X,Y) = 0$ has at most $\deg(f)\deg(g)$ solutions. □

Definition 1.8. Let K be a field and $f(X,Y) \in K[X,Y]$ a polynomial. We call the set of solutions to $f(X,Y) = 0$ a **curve**. The **degree** of a curve is the degree of the polynomial defining it. If $\deg(f) = 2$ then $f(X,Y) = 0$ is a **conic**. If $\deg(f) = 3$ then $f(X,Y) = 0$ is a **cubic**.

Theorem 1.9 (Pascal's Theorem). *Let K be a field and $f(X,Y) = 0$ a conic over K. If $A_1, \ldots, A_6$. Let A_iA_j denote the unique line passing through the points A_i and A_j. Then, up to renumbering, three points $A_1A_2 \cap A_4A_5$, $A_2A_3 \cap A_5A_6$ and $A_3A_4 \cap A_6A_1$ all lie on one line.*

Proof. Let $L_1, M_1, L_2, M_2, L_3, M_3$ be linear functions that vanish on the lines $A_1A_2, A_2A_3, A_3A_4, A_4A_5, A_5A_6, A_6A_1$ respectively. Consider the following family of polynomials indexed by λ:

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

then $G_\lambda = 0$ is a cubic that contains the points $A_1, \ldots, A_6$ and the three points listed in the theorem. Fix a point p on the conic $f = 0$ distinct from the A_i and let λ_0 be such that $G_{\lambda_0} = p$. Then $G_{\lambda_0} = 0$ and $f = 0$ have 7 points in common, namely $p, A_1, \ldots, A_6$. By Bézout's Theorem $G_{\lambda_0} = 0$ and $f = 0$ have a non-trivial greatest common divisor. We claim, in fact, that f divides G_{λ_0}. If f is irreducible then this is clear. If not then $f = 0$ is the union of two lines in the plane. We may choose p so that exactly one of $p, A_1, \ldots, A_6$ lie on the intersection of these two lines[1] hence f decomposes into two linear functions, both of which vanish at one of the points $p, A_1, \ldots, A_6$. Since G_{λ_0} also vanishes at all these points, it must be divisible by both the factors of f and is thus divisible by f itself. But f is a conic so there exists a line L such that $G_{\lambda_0} = FL = 0$. Clearly, the three points cannot lie on F so they must lie on L and we are done. □

[1]here we assume that lines always intersect, possible at a so-called **point at infinity**. The reasoning for this will be clear once we study projective space.

2 Kakeya Conjectures

Definition 2.1. Let K be a finite field and $E \subseteq K^n$. We say that E is a **Kakeya** subset of K^n if E contains a unit line in every direction.

Lemma 2.2. *Let R be a ring. Then the vector space of polynomials in $R[X_1, \ldots, X_n]$ of degree at most d has dimension $\binom{n+d}{d}$.*

Proof. We prove the lemma by using the standard **stars and bars** argumentation of combinatorics. Clearly, the basis of such a vector space is given by all monomials in $R[X_1, \ldots, X_n]$ of degree at most d. If we homogenise these monomials using a dummy variable X_0 then, obviously, we will still have the same number of monomials. Hence it suffices to count the number of monomials in $R[X_0, X_1, \ldots, X_n]$ whose degree is d. If $X_0^{a_0} X_1^{a_1} \ldots X_n^{a_n}$ is such a monomial then we have the equation

$$a_0 + a_1 + \cdots + a_n = d$$

We seek to count the number of solutions to this equation for non-negative $a_i \in \mathbb{Z}$. To do this, we notice that this is the same as taking $n + d$ places and filling them with d 'stars' and n 'bars'. For example, if $d = 3$ and $n = 2$ then

$$\{* * | * |\}$$

corresponds to the solution $2 + 1 + 0 = 3$. But this is the same as taking $n + d$ arbitrary elements and counting the number of distinct configurations there exists with n of the elements fixed. This is equal to $\binom{n+d}{n}$ which is in turn equal to $\binom{n+d}{d}$ and we are done. $\square$

Proposition 2.3. *Let K be a field and $L \subseteq K[X_1, \ldots, X_n]$ be a linear subspace. Let $E \subseteq K^n$ be such that $|E| < \dim(L)$. Then there exists a non-zero polynomial in L that vanishes on E. Furthermore, if M is the subspace of polynomials in L that vanish on E then $\dim(M) \geq \dim(L) - |E|$.*

Proof. Let K^E denote the K-vector space of K-valued functions on E. Define the mapping

$$e : L \mapsto K^E$$

which sends a polynomial in $f(X_1, \ldots, X_n) \in L$ to the function $f(x_1, \ldots, x_n) \in K^E$. The kernel of this mapping is clearly M. By the rank-nullity theorem, we have $\dim(L) = \dim(M) + \dim(\mathrm{im}(e))$. The proposition then follows upon realising $|E| \geq \dim(\mathrm{im}(e))$. $\square$

Corollary 2.4. *Let K be a finite field and $E \subseteq K^n$ subset such that $|E| < \binom{n+d}{d}$ for some non-negative integer d. Then there exists a non-zero polynomial $f \in K[X_1, \ldots, X_n]$ that vanishes on E such that $\deg(f) \leq d$.*

Proof. Let V_d be the vector space of polynomials in $K[X_1, \ldots, X_n]$ of degree at most d. By Lemma 2.2, the dimension of V_d is $\binom{n+d}{d}$. The corollary then follows upon application of 2.3. $\square$

Lemma 2.5. *Let K be a finite field and $f \in K[X_1, \ldots, X_n]$ a polynomial of degree less than $|K|$. If f vanishes on all of K^n then f is identically zero.*

Proof. We prove the lemma by induction on the number of indeterminates n. If $n = 1$ then the lemma is true since any polynomial of degree less than $|K|$ that vanishes on all of K must be identically zero. Suppose the lemma is true for arbitrary $n-1$. We may write f in the form

$$f = \sum_{i=0}^{|K|-1} X_n^{|K|-i-1} f_i(X_1, \ldots, X_{n-1})$$

where f_i is a polynomial of degree at most i. Fix some $(x_1^0, \ldots, x_{n-1}^0) \in K^{n-1}$. Then $f(x_1^0, \ldots, x_{n-1}^0, X_n)$ is a polynomial in one variable X_n of degree less than $|K|$. This polynomial must be identically zero which means that $f_i(x_1^0, \ldots, x_{n-1}^0) = 0$ for all i. By the induction hypothesis, f_i is identically zero for all i. Hence f is also identically zero. □

Proposition 2.6. *Let K be a finite field and $f \in K[X_1, \ldots, X_n]$ a polynomial of degree at most $|K|-1$ that vanishes on some Kakeya set $E \subseteq K^n$. Then f is identically zero.*

Proof. Suppose that f is not identically zero. Then f has strictly positive degree. We may write f as a sum of its individual homogeneous components

$$f = \sum_{i=0}^{d} f_i$$

where $1 \leq d \leq |K|-1$. Let $v = (v_1, \ldots, v_n) \in K^n \backslash \{ 0 \}$. Since E is a Kakeya set, there exists some $x_v = (x_1, \ldots, x_n) \in K^n$ such that

$$\{ x_v + tv \mid t \in K \} \subseteq E$$

By hypothesis, f vanishes on E so $f(x_v + tv) = 0$ for all $t \in K$. This is a polynomial in t of degree $|K|-1$ which vanishes on all of K so it must be identically zero. We claim that the coefficient of t^d is equal to $f_d(v)$. Indeed

$$f(x_v + tv) = \sum_{i=0}^{d-1} f_i(x_v + tv) + f_d(x_v + tv) = \sum_{i<d} c_i t^i + t^d f_d(v)$$

for some $c_i \in K$. Hence for all $v \in K^n \backslash \{ 0 \}$, $f_d(v) = 0$. Furthermore, since f_d is homogeneous of degree $d > 0$, it also vanishes at 0. Hence $f_d(v)$ vanishes for all $v \in K^n$. By Lemma 2.5, $f_d(v)$ is thus identically zero which is a contradiction to the assumption that f is not identically zero. □

Theorem 2.7 (Kakeya Conjecture - Dvir's Theorem)**.** *Let K be a finite field and $E \subseteq K^n$ a Kakeya set. Then there exists a $c_n > 0$ such that $|E| \geq c_n |K^n|$.*

Proof. We claim that E has cardinality at least $\binom{|K|+n-1}{|K|-1}$. Indeed, suppose that $|E| < \binom{|K|+n-1}{|K|-1}$. Then Corollary 2.4 implies that there exists a non-zero polynomial of degree $|K|-1$ in $K[X_1, \ldots, X_n]$ that vanishes on E. But Proposition 2.6 implies that any such polynomial must be identically zero which is a contradiction. Hence the cardinality of E is at least $\binom{|K|+n-1}{|K|-1}$. Now,

$$\binom{|K|+n-1}{|K|-1} = \frac{(|K|+n-1)!}{(|K|-1)!n!} \geq \frac{|K|^n}{n!}$$

so $c_n = 1/n!$ and we are done. □

3 Projective Space

Definition 3.1. Let K be a field. Define an equivalence relation $\sim$ on $\mathbb{A}_K^{n+1} \setminus \{0\}$ where $(a_1, \ldots, a_{n+1}) \sim (b_1, \ldots, b_{n+1})$ if and only if there exists $\lambda \in K^\times$ such that $a_i = \lambda b_i$ for all $1 \leq i \leq n+1$. We define **n-dimensional projective space**, denoted $\mathbb{P}_K^n$, to be the set of all equivalence classes of this equivalence relation.

Lemma 3.2. *Let K be a field. Then $\mathbb{P}_K^n = \mathbb{A}_K^n \cup \mathbb{P}_K^{n-1}$.*

Proof. $\mathbb{A}_K^n$ embeds in $\mathbb{P}_K^n$ by the inclusion mapping $(a_1, \ldots, a_n) \mapsto [(1, a_1, \ldots, a_n)]$. The image of $\mathbb{A}_K^n$ is clearly all of $\mathbb{P}_K^n$ except for the equivalence classes of ordered pairs with zero x_0 coordinates. We shall refer to such equivalence classes as the **points at infinity** of $\mathbb{P}_K^n$. It is easy to see that the set of all points at infinity of $\mathbb{P}_K^n$ are 'isomorphic' to $\mathbb{P}_K^{n-1}$. Indeed, there is a bijection between the equivalence classes of $(0, x_2, \ldots, x_n)$ in $\mathbb{P}_K^n$ and the equivalence classes of $(x_2, \ldots, x_n)$ in $\mathbb{P}_K^{n-1}$. ☐

Corollary 3.3. $\mathbb{P}_K^n = \mathbb{A}_K^n \cup \cdots \cup \mathbb{A}_K^0$.

Definition 3.4. Let K be a field and $W^{m+1} \subseteq \mathbb{A}_K^{n+1}$ a linear subspace. Then the set of all lines through 0 in W^{m+1} is a linear subspace of $\mathbb{P}^m$ called a **projective hyperplane**. In particular, if $m = 1$ then such a subspace is a **projective line**.

Proposition 3.5. *Let K be a field. Then the intersection of any two linear subspaces $\mathbb{P}_K^l, \mathbb{P}_K^m \subseteq \mathbb{P}_K^n$ is a linear subspace of dimension at least $l + m - n$.*

Proof. $\mathbb{P}_K^l, \mathbb{P}_K^m$ and $\mathbb{P}_K^n$ are all projective spaces arising from $\mathbb{A}_K^{l+1}, \mathbb{A}_K^{m+1}$ and $\mathbb{A}_K^{n+1}$. Now,

$$\begin{aligned}\dim(\mathbb{A}_K^{l+1} \cap \mathbb{A}_K^{m+1}) &= \dim(\mathbb{A}_K^{l+1}) + \dim(\mathbb{A}_K^{m+1}) - \dim(\mathbb{A}_K^{l+1} + \mathbb{A}_K^{m+1}) \\ &\geq l + 1 + m + 1 - (n+1) = l + m - n + 1\end{aligned}$$

Hence projecting $\mathbb{A}_K^{l+1} \cap \mathbb{A}_K^{m+1}$ down we get a linear subspace of $\mathbb{P}_K^n$ of dimension at least $l + m - n$. ☐

From this proposition we see that any two hyperplanes in projective space intersect. In particular, looking back to Pascal's theorem, we may justify the assumption that all lines intersect, possibly at a so-called point at infinity.

Theorem 3.6 (Desargue's Theorem)**.** *Let K be a field and $a, b, c, A, B, C \in \mathbb{P}_K^3$ points not all contained in one plane. Furthermore, suppose that no three of the points all lie on one line. Suppose that the lines aA, bB, cC all intersect at a point. Then the points $ab \cap AB$, $bc \cap BC$, $ca \cap CA$ all lie on one line.*

Proof. By assumption there exists unique planes abc and ABC that contain the points a, b, c and A, B, C respectively. We claim that the intersection of abc and ABC contains the desired points. We have $ab \subseteq abc$ and $AB \subseteq ABC$ so $ab \cap AB \subseteq abc \cap ABC$. A similar argument shows that the other two points also line on such an intersection. ☐

Proposition 3.7. *Let K be a field and $\mathbb{P}^k, \mathbb{P}^l, \mathbb{P}^m$ be linear subspaces of $\mathbb{P}_K^n$ such that $m + l + k \geq n - 1$. Then there exists a projective line that intersects all three of $\mathbb{P}^k, \mathbb{P}^l, \mathbb{P}^m$.*

Proof. First suppose that $\mathbb{P}^l \cap \mathbb{P}^m = \varnothing$. Then there always exists a projective line joining a point of such an intersection to a point of $\mathbb{P}^k$ and we are done. Hence assume their intersection is trivial.

Let $\mathbb{P}$ be the minimal subspace of $\mathbb{P}^n_K$ that contains both $\mathbb{P}^l$ and $\mathbb{P}^m$. It is easy to see that such a subspace is the union of all projective lines connecting points of $\mathbb{P}^l$ and $\mathbb{P}^m$ and is of dimension of $l+m+1$. By hypothesis we have

$$\begin{aligned}\dim(\mathbb{P}\cap\mathbb{P}^k) &= \dim(\mathbb{P}) + \dim(\mathbb{P}^k) - \dim(\mathbb{P}+\mathbb{P}^k)\\ &\geq l+m+1+k-n \geq 0\end{aligned}$$

and thus $\mathbb{P}\cap\mathbb{P}^k \neq \varnothing$ so there exists a projective line intersecting all three spaces. $\square$

Definition 3.8. Let K be a field and $p \in \mathbb{P}^n_K$ a point. Let $(\lambda a_0, \ldots, \lambda a_n)$ be a representative of p in $\mathbb{A}^{n+1}_K$. Then we say that $[a_0 : \ldots : a_n]$ is a **homogeneous coordinate** of p.

Definition 3.9. Let K be a field and $f \in K[X_0, \ldots, X_n]$ a homogeneous polynomial of degree d. We define the **hypersurface** defined by f to be the subset of $\mathbb{P}^n_K$ given by

$$X_f = \{\, [a_0 : \ldots : a_n] \in \mathbb{P}^n_K \mid f(a_0, \ldots, a_n) = 0 \,\}$$

We define the **degree** of X_f to be the degree of its defining polynomial.

Example 3.10. Let K be a field and $f \in K[X_0, \ldots, X_n]$ a homogeneous polynomial of degree 1. Then $X_f = \mathbb{P}^{n-1}$.

Definition 3.11. Let K be a field and $V \subseteq \mathbb{P}^n_K$ a subset. V 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

$$V = \{\, [a_0 : \ldots : a_n] \in \mathbb{P}^n_K \mid f_i(a_0, \ldots, a_n) = 0\ \forall\, 1 \leq i \leq n \,\}$$

Definition 3.12. Let K be a field and $f \in K[X_1, \ldots, X_n]$ a polynomial of degree d. We define the **homogeneous completion** of f to be $X_0^d f(X_1/X_0, \ldots, X_n/X_0)$.

Recall that $\mathbb{P}^n_K = \mathbb{A}^n_K \cup \mathbb{P}^{n-1}_K$ and that we refer to $\mathbb{P}^{n-1}_K$ as the points at infinity of $\mathbb{A}_K$.

Homogeneous equations over $\mathbb{P}^n_K$ are related to inhomogeneous equations over $\mathbb{A}^n_K$ in the following way. Replacing X_0 with 1 in a homogeneous equation gives an inhomogeneous equation. Passing the the homogeneous completion of an inhomogeneous equation gives a homogeneous equation.

Example 3.13. Consider the two circles $X_1^2 + X_2^2 = 1$ and $X_1^2 + X_2^2 = 4$ in $\mathbb{C}^2$. It is easy to see that these two circles do not intersect in $\mathbb{C}^2$. We may pass to the homogeneous completion of these equations to get $X_1^2 + X_2^2 = X_0^2$ and $X_1^2 + X_2^2 = 4X_0^2$. It then follows that these two circles intersect at the points at infinity given by homogeneous coordinates $[0 : 1 : \pm i]$.

4 Quadratic Forms and Conics

Throughout this section, we assume all fields have characteristic different from 2.

Definition 4.1. Let K be a field. A **quadratic form** is a homogeneous polynomial of degree 2 in any number of indeterminates. A quadratic form $F(X_1, \ldots, X_n)$ is **diagonal** if $F = \sum_{i=1} a_i X_i^2$ for some $a_i \in K$. Furthermore, a quadratic form is said to be **diagonalisable** if there exists a basis for K^n in which F is diagonal.

Proposition 4.2. *Let K be an algebraically closed field and $F(X_1, \ldots, X_n)$ a non-zero quadratic form over K^n. Then there exists a K-basis of K^n, say $v_1, \ldots, v_n$, such that $F(v_1X_1 + \cdots + v_nX_n) = \sum_{i=1}^n X_1^2 + \cdots + X_i^2$ for some $1 \leq i \leq n$.*

Proof. Consider the function

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

We first claim that $Q(u,v)$ is a symmetric bilinear form on K^n.

Q is clearly symmetric by virtue of its definition. For simplicity, we shall check the calculation for bilinearity when F is in two indeterminates. We can always write F in the form

$$F(X_1, X_2) = aX_1X_2 + bX_1^2 + cX_2^2$$

and so

$$\begin{aligned} Q(u,v) &= \frac{(a+b+c)(u+v)^2 - (a+b+c)u^2 - (a+b+c)v^2}{2} \\ &= (a+b+c)uv \end{aligned}$$

which is clearly linear in both u and v. $Q(u,v)$ is also positive definite since it is a homogeneous polynomial of degree 2.

We construct the basis by a Gram-Schmidt process. Choose a $v_1 \in K$ such that $f(v_1) = 1$. This can always be done since we may take v' to be such that $F(v') \neq 0$ and then take $v_1 = v'/\sqrt{F(v_1)}$. We then have that $Q(v_1, v_1) = 1$.

Now suppose that we have constructed linearly independent vectors $(v_1, \ldots, v_k)$ such that $Q(v_i, v_j) = \delta_{ij}$. Let V_k denote the subspace of K^n that is spanned by these vectors. We claim that $K^n = V_k \oplus V_k^\perp$ where

$$V_k^\perp = \{\, v \in V \mid Q(v,u) = 0 \;\forall\, u \in V_k \,\}$$

Clearly, Q is non-degenerate on V_k so $V_k \cap V_k^\perp = \{\, 0 \,\}$. We just need to show that every element of K^n can be expressed as the sum of an element of V_k and an element of $V_k^\perp$. To this end, fix $x \in V$ and let

$$y = x - \sum_{i=1}^{k} Q(x, v_i) v_i$$

Then

$$Q(y, v_j) = Q(x, v_j) - Q(x, v_j)Q(v_j, v_j) = 0$$

whence $y \in V_k^\perp$. Hence $x = y + \sum_{i=1}^{k} Q(x, v_i)v_i \in V_k^\perp + V_k$ and thus $K^n = V_k \oplus V_k^\perp$.

Now, if the restriction of Q to $V_k^\perp$ is 0 then we can let $v_{k+1}, \ldots, v_n$ be any basis for $V_k^\perp$ and thus $v_1, \ldots, v_n$ is a basis for V satisfying $Q(v_i, v_j) = \delta_{ij}$ for all $1 \leq i \leq j \leq k$ and $Q(v_i, v_k)$ for all $i > k$. If not then we can repeat this process until Q restricts to 0 on an orthogonal subspace.

Finally, we have that

$$F\left(\sum_{i=1}^{n} v_i X_i\right) = Q\left(\sum_{i=1}^{n} v_i X_i, \sum_{i=1}^{n} v_i X_i\right) = X_1^2 + \cdots + X_k^2$$

$\square$

Corollary 4.3. *Let K be a field and C an irredicuble conic over $\mathbb{P}^2_K$. Then there exist homogeneous coordinates such that F is given by $X_0X_2 - X_1^2 = 0$.*

Proof. By Proposition 4.2, there exists coordinates such that the conic is given by one of

$$Y_0^2 = 0, \quad Y_0^2 + Y_1^2 = 0, \quad Y_0^2 + Y_1^2 + Y_2^2 = 0$$

But the first two cases are the equations for reducible conics so we must be in the third case. The coordinates $X_1 = iY_1$, $X_0 = Y_0 - iY_2$ and $X_2 = Y_0 + iY_2$ bring the conic into the desired form. □

Corollary 4.4. *Let K be a field and C an irreducible conic over $\mathbb{P}^2_K$. Then C can be put into bijection with $\mathbb{P}^1_K$. Such a mapping is called a* ***rational parametrisation*** *of C.*

Proof. By Corollary 4.3, we may assume that the conic takes the form

$$X_0X_2 - X_1^2 = 0 \tag{1}$$

We then have the map

$$\begin{aligned} \varphi : \mathbb{P}^1_K &\to C \\ [u_0 : u_1] &\mapsto [u_0^2 : u_0u_1 : u_1^2] \end{aligned}$$

We claim that this map has inverse

$$\begin{aligned} \varphi^{-1} : C &\to \mathbb{P}^1_K \\ [u_0 : u_1 : u_2] &\mapsto [u_0 : u_1] \text{ or } [u_1 : u_2] \end{aligned}$$

Note that the first of these two maps is not defined on $[0 : 0 : 1]$ and the second is not defined on $[1; 0; 0]$. They however coincide everywhere else by virtue of 1 . We now check their compositions. We have

$$\varphi^{-1} \circ \varphi([u_0 : u_1]) = \varphi^{-1}([u_0^2 : u_0u_1 : u_1^2]) = [u_0 : u_1]$$

A similar argument shows the reverse composition. □

Proposition 4.5. *Let K be a field and $A_1, \ldots, A_5 \in \mathbb{P}^2_K$ points. Then*

1. *there exists a conic over $\mathbb{P}^2_K$ that passes through them*
2. *there exists a unique conic through the A_i if and only if no 4 of the points lie on one line*
3. *the conic is irreducible if and only if no three of the points lie on one line*

Proof. Let $a_1, \ldots, a_5$ be points in $\mathbb{A}^3_K$ on the lines through the origin corresponding to $A_1, \ldots, A_5$. Note that the set of all homogeneous polynomials of degree 2, together with the 0 vector, is a linear subspace of $K[X_0, X_1, X_2]$. It is easy to see that this vector space has dimension 6 over K. Appealing to Proposition 2.3, we see that the linear subspace of $K[X_0, X_1, X_2]$ consisting of all homogeneous polynomials of degree 2 that vanish at the a_i has dimension over K at least 1. Hence there exists at least one conic passing through the a_i and thus there exists at least one conic passing through the A_i.

Now suppose, without loss of generality, that $A_1, \ldots, A_4$ all lie on one projective line $L = 0$. If $L' = 0$ is any line containing A_5 then $LL' = 0$ is a conic that contains $A_1, \ldots, A_5$. Hence there are more than one conics that pass through $A_1, \ldots, A_5$ in this case.

Conversely, suppose that there does not exist a projective line passing through any four of $A_1, \ldots, A_5$. To prove the conic is unique, we shall consider the case where no three of $A_1, \ldots, A_5$ lie on line separately.

First suppose that no three of $A_1, \ldots, A_5$ lie on one line and that C_1 and C_2 are two conics, given by $F_1 = 0$ and $F_2 = 0$ respectively, containing $A_1, \ldots, A_5$. We first claim that given any point $p \in \mathbb{P}^2_K$, there exists a point $[s : t] \in \mathbb{P}^1_K$ such that $(sF_1 + tF_2)(p) = 0$. Indeed, if $F_2(p) = 0$ then we may take $[s : t] = [0 : 1]$. Else we can take $s = 1$ and

$$t = -\frac{F_1(p)}{F_2(p)}$$

Now choose p on the line L_1 joining A_1 and A_2 and let $F = sF_1+tF_2 = 0$ be the corresponding conic. The intersection of F with L_1 contains the three points p, A_1 and A_2. By Bézout's Theorem, F must be reducible and we have $F = L_1L$ for some line L. Since L_1 cannot contain any of the A_3, A_4, A_5, they must be on L. But this contradicts the assumption that no three of the A_i lie on one line. Hence the conic must be unique.

Finally, let $F = 0$ be a conic passing through the five A_i. If F were reducible then it would decompose into two lines $F = L_1L_2 = 0$. Clearly, one of the L_i must contain three of the points. Conversely, if three of the points lie on one line L then Bézout's Theorem implies that L divides F and thus F is reducible. $\square$

5 Cubic Curves

Proposition 5.1. *Let K be an algebraically closed field of characteristic zero. Then any two curves over $\mathbb{P}^2_K$ intersect.*

Proof. Let C_1 and C_2 be two curves over $\mathbb{P}^2_K$ given by the homogeneous polynomials $F, G \in K[X_0, X_1, X_2]$. We need to exhibit a non-zero $(a_0, a_1, a_2) \in \mathbb{A}^3_K$ such that $F(a_0, a_1, a_2) = G(a_0, a_1, a_2) = 0$. In order to do this, we shall consider the resultant of these two polynomials. Without loss of generality, we may assume that $F(1, 0, 0)$ and $G(1, 0, 0)$ are non-zero. Furthermore, we may write (scaling if necessary)

$$F(X_0, X_1, X_2) = \sum_{i=0}^{n} F_i(X_1, X_2)X_0^i, \quad G(X_0, X_1, X_2) = \sum_{i=0}^{m} G_i(X_1, X_2)X_0^i$$

for some $F_i, G_i \in K[X_1, X_2]$. By definition, it is easy to see that the resultant of F and G with respect to X_0 is a homogeneous polynomial in X_1 and X_2 of degree nm. Hence if we fix non-zero $a_2 \in K$, we get a polynomial in X_0. Since K is algebraically closed, such a polynomial must have a root, say a_0. Then $R[F, G](a_1, a_2) = 0$ so the polynomials $F[X_0, a_1, a_2]$ and $G[X_0, a_1, a_2]$ must have a root in common. This means that there exists non-zero (a_0, a_1, a_2) such that $F[a_0, a_1, a_2] = G[a_0, a_1, a_2] = 0$ and we are done. $\square$

Definition 5.2. Let K be a field and $F \in K[X_0, X_1, \ldots, X_n]$ be a homogeneous polynomial. A point P of the hypersurface $F = 0$ is said to be **singular** if

$$\frac{\partial F}{\partial X_i}(P) = 0$$

for all $0 \leq i \leq n$. If some of the derivatives are non-zero then P is said to be **smooth**. If all the points of $F = 0$ are smooth then the hypersurface itself is said to be **smooth**

Proposition 5.3. *Let K be an algebraically closed field of characteristic 0. Then any smooth curve over $\mathbb{P}^2_K$ is irreducible.*

Proof. Let C be a smooth curve over $\mathbb{P}^2_K$ given by $F \in K[X_0, X_1, X_2]$. Suppose, for a contradiction, that C is reducible. Then F decomposes as $F = GH$ for some $G, H \in K[X_0, X_1, X_2]$. By Proposition 5.1, G and H intersect at some point, say P. Now,

$$\frac{\partial F}{\partial X_0}(P) = \left[\frac{\partial G}{\partial X_0}H + \frac{\partial H}{\partial X_0}G\right](P) = 0$$

and so $F = 0$ is singular at P which is a contradiction to the smoothness of C. Hence C must be irreducible. □

Definition 5.4. Let K be a field and L a projective line over $\mathbb{P}^n_K$. If $F = 0$ is a hypersurface over $\mathbb{P}^n_K$ then L is said to be **tangent** to $F = 0$ if the restriction of F to L has a double root at some point p.

Definition 5.5. Let K be a field and $f \in K[X_0, X_1, \ldots, X_n]$ a polynomial. We define the **Hessian** of f to be

$$\mathrm{Hess}_f = \det\left(\frac{\partial f}{\partial X_i \partial X_j}\right)_{0 \le i \le j \le n}$$

Theorem 5.6 (Weierstrass Normal Form)**.** *Let K be a field an algebraically closed field of characteristic 0. Let C be a smooth cubic curve over $\mathbb{P}^2_K$. Then there exist homogeneous coordinates so that C is given by an equation of the form*

$$X_0 X_2^2 = X_1^3 + aX_0^2 X_1 + bX_0^3$$

for some $a, b \in K$. In other words, any smooth cubic curve over $\mathbb{A}^2_K$ is projectively equivalent to a cubic curve given by

$$X_2^2 = X_1^3 + aX_1 + b$$

Proof. Let C be given by the homogeneous polynomial of degree 3 $F \in K[X_0, X_1, X_2]$. By Proposition 5.1, there exists $P \in \mathbb{P}^2_K$ such that

$$F(P) = \mathrm{Hess}_F(P) = 0 \tag{2}$$

We may choose coordinates so that $P = [0 : 0 : 1]$ and the line $X_0 = 0$ is tangent to the curve C at P. Now write F in the following form:

$$F = F_1(X_0, X_1)X_2^2 + F_2(X_0, X_1)X_2 + F_3(X_0, X_1)$$

where the $F_i \in K[X_0, X_1]$ are homogeneous of degree i. Since C is smooth, F must be smooth at P and it is thus clear from the above form of the equation that the tangent line to F at P must be given by $F_1[X_0, X_1] = 0$. But the coordinates were chosen so that $X_0 = 0$ is the tangent line of F at P so we must have that $F_1[X_0, X_1] = cX_0$. Without loss of generality, we may assume that $c = -1$. We now have the curve in the following form:

$$0 = -X_0 X_2^2 + (aX_0^2 + bX_0 X_1 + cX_1^2)X_2 + F_3(X_0, X_1)$$

By Equation 2 we have

$$\mathrm{Hess}_F(P) = \det \begin{pmatrix} 2a & b & -2 \\ b & 2c & 0 \\ -2 & 0 & 0 \end{pmatrix} = -8c$$

We must therefore have that $c = 0$. Passing to affine space, we have the equation

$$X_2^2 = aX_2 + bX_1X_2 + F_3(1, X_1)$$

Completing the square in X_2 and rearranging gives us

$$\left(X_2 - \frac{a + bX_1}{2}\right)^2 = \left(\frac{a + bX_1}{2}\right)^2 = F_3(1, X_1)$$

We may finally make a linear change of coordinates to bring the equation into the form

$$X_2^2 = X_1^3 + aX_1 + b$$

for some $a, b \in K$. Passing to the homogeneous completion of this equation gives us the desired equation for the cubic curve over projective space. $\square$

Definition 5.7. Let K be a field and $F \in K[X_0, X_1, X_2]$ be a homogeneous polynomial. We say that a point P on the curve $F = 0$ is an **inflection point** if $\mathrm{Hess}_F(P) = 0$.

Proposition 5.8. *Let K be a field and $p_1, \ldots, p_8 \in \mathbb{P}^2_K$ be points such that no 4 lie on one line and no 7 lie on one conic. If M is the linear subspace of $K[X_0, X_1, X_2]$ consisting of homogeneous polynomials of degree 3 that vanish at the p_i then* $\dim(M) = 2$.

Proof. Let L be the linear subspace of $K[X_0, X_1, X_2]$ consisting of all homogeneous polynomials of degree 3. By Lemma 2.2, this has dimension 10. Hence by Lemma 2.3, we have $\dim(M) \geq 2$. Hence assume that $\dim(M) > 3$. We shall consider 3 seperate cases.

First suppose that no 3 points lie on one line and no 6 points lie on one conic. Let $L = 0$ denote the line passing through p_1 and p_2. Let q and r be two distinct points, neither of which are equal to p_1 or p_2. We can always construct an $F \in M$ that vanishes at both q and r. Hence the cubic $F = 0$ intersects $L = 0$ in 4 points. By Bézout's Theorem, F must be reducible and we have $F = LQ$ where Q is some conic. We cannot have that $p_3, \ldots, p_8$ lie on L so they must lie on Q. But by assumption, no 6 points lie on one conic whence we arrive at a contradiction.

Now suppose that 3 points $p_1, \ldots, p_3$ lie on one line, say $L = 0$. Let Q be the unique conic passing through $p_4, \ldots, p_8$. Note that $F = LQ \in M$. Since $\dim(M) > 2$, we can find F_1 and F_2 such that F, F_1 and F_2 are linearly independent. Now let p be a point on L distinct from $p_1, \ldots, p_3$. We can always find a linear combination of F_1 and F_2 that vanishes at p. By Bézout's Theorem, we must have that such a linear combination is divisible by L. But then this linear combination is proportional to F which is a contradiction to their pairwise linear independence.

Finally, suppose that 6 of the points $p_1, \ldots, p_6$ lie on one conic. Here the argumentation follows the previous case where we take L to be the line through p_7 and p_8.

We see that in all cases, we arrive at contradictions so we must have that $\dim(M) = 2$. $\square$

6 Group Law for Cubics

Let K be a field and C a cubic curve over $\mathbb{P}_K^2$. We shall define the structure of an abelian group on C as follows:

Fix a distinguished point $O \in C$. This will act as the identity. Let P and Q be arbitrary points on C. Let L be the line through P and Q. If L intersects C at a third point, then denote it $P * Q$. If not then L is tangent to C at P so let $P * Q = P$. Now let M be the line through O and $P * Q$. We let $P + Q$ be the third point of intersection of this line with C. In other words, $P + Q = O * (P * Q)$.

Proposition 6.1. *Let K be a field and C a smooth cubic curve over $\mathbb{P}_K^2$. Then $(C, +)$ is an abelian group.*

Proof. The commutativity is clear from the definition of $+$. Furthermore, it is clear that $O + P = P$. Indeed, $O + P = O * (O * P)$. Now, the line joining O and P contains a point, say M. But the line joining M and O must also contain P.

We must now check associativity of $+$. Let $F \in K[X_0, X_1, X_2]$ be the polynomial defining C. Let $P, Q, R \in C$. We need to show that $P + (Q + R) = (P + Q) + R$. In other words, $O*(P*(Q+R)) = O*((P+Q)*R)$. This reduces to showing that $P*(Q+R) = (P+Q)*R$.

Let $F_1 = 0$ be the cubic given by the composition of the three lines $(P, Q), (O, Q + R), (R, P + Q)$. Let $F_2 = 0$ be the cubic given by the composition of the three lines $(Q, R), (O, P + Q), (P, Q + R)$. We note that $O, P, Q, R, (P * Q), (P + Q), (Q * R), (Q + R)$ all lie on the three cubics $F = 0$, $F_1 = 0$ and $F_2 = 0$.

Now if 4 of those points were to lie on the same line then C would contain the line that passess through these points and C would be reducible which is a contradiction to the fact that C is smooth. The same argumentation shows that no 7 of the points lie on one conic. Appealing to Proposition 5.8, we see that F, F_1 and F_2 must be linearly dependent over K. Hence we may write

$$F_2 = aF + bF_1$$

for some $a, b \in K$. Now, both F and F_1 vanish at the point $(P + Q) * R$ whence F_2 does too. But this is only possible if $(P + Q) * R = P * (Q + R)$.

Finally, we must prove that inverses exist. Let $P \in C$. If O is not an inflection point of C then the tangent line to C at O intersects C in some other point, say O^*. Then we have $-P = O^* * P$. If O is an inflection point then $-P = O * P$. □

7 Higher Dimensional Varieties

Definition 7.1. Let K be a field. We define the **Segre map** to be

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

The image of this map is written $\sum_{n,m}$.

Proposition 7.2. *Let K be a field. Then the image of the Segre embedding $\sum_{n,m} \subseteq \mathbb{P}_K^{(n+1)(m+1)-1}$, given in homogeneous coordinates $[Z_{00} : \ldots : Z_{ij} : \ldots : Z_{nm}]$ is a projective variety given by the system of homogeneous equations*

$$Z_{ij}Z_{kl} - Z_{il}Z_{kj} = 0$$

Proof. Let M be the set of all $(n+1)\times(m+1)$-dimensional matrices over K. Define an equivalence relationship on M, say $\sim$, where $A\sim B$ if and only if $A=\lambda B$ for some $\lambda\in K^{\times}$. It is easy to see that $\sum_{n,m}$ is the set of all $\sim$-equivalence classes of matrices of rank 1. Indeed, any element of $\mathbb{P}_K^{(n+1)(m+1)-1}$ is given by homogeneous coordinates which are invariant under multiplication by scalars. To see that the equivalence classes we are considering are of rank 1, we need only consider the matrix $Z_{ij}=X_iY_j$. Any row is necessarily a linear combination of some other row in this matrix whence the rank is at most 1. But we cannot have that all entries of the matrix are 0 since we are working in projective space so the matrix cannot have rank 0.

Now, any 2×2 minor in a rank 1 matrix must be 0 and we therefore must have that $Z_{ij}Z_{kl}-Z_{il}Z_{kj}=0$. Conversely, if any 2×2 minor of a matrix is 0 then such a matrix must have rank 1. It then follows that $\sigma_{n,m}$ is a projective variety given by $Z_{ij}Z_{kl}-Z_{il}Z_{kj}=0$. □

Corollary 7.3. *Let K be a field and $X\subseteq\mathbb{P}_K^n$ and $Y\subseteq\mathbb{P}_K^m$ projective varieties. Then $\sigma(X\times Y)\subseteq\mathbb{P}_K^{(n+1)(m+1)-1}$ is a projective variety.*

Proof. We first observe that we can write $X\times Y=X\times\mathbb{P}_K^m\cap\mathbb{P}_K^n\times Y$. It thus suffices to prove the corollary for the product $X\times\mathbb{P}_K^m$. Furthermore, we may assume that X is a hypersurface since any variety is necessarily the intersection of hypersurfaces. Hence X is given by some $F\in K[X_0,\dots,X_n]$. It then follows that $\sigma(X\times\mathbb{P}_K^m)$ is given by the intersection of $\sigma(\mathbb{P}_K^n\times\mathbb{P}_K^m)$ with the hypersurfaces $F(Z_{0i},\dots,Z_{ni})$ for $0\le i\le m$. □

Recall that given a field K, we can construct the space of so-called **bivectors** of a vector space V of dimension n over K, denoted Λ^2V. If vectors are line segments then bivectors can be geometrically interpreted as plane segments. Such bi-vectors are constructed using the wedge product $\wedge$ on two vectors $u,v\in V$ subject to the relations

$$(\alpha\cdot u)\wedge v=\alpha(u\wedge v),\quad u\wedge v=-v\wedge u$$

If $e_1,\dots,e_n$ is a K-basis for V then any bivector w can be expressed as

$$w=\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}e_i\wedge e_j$$

for some $a_{ij}\in K$. Note that the properties of a bivector impose the condition $w\wedge w=0$ for any bivector w.

Definition 7.4. Let K be a field. We define the **Grassmannian** $(\mathbf{m},\mathbf{n})$ over K to be the set of all m-dimensional linear subspaces of $\mathbb{A}_K^n$. This is equivalent to all the $m-1$-dimensional linear subspaces of $\mathbb{P}_K^{n-1}$.

Proposition 7.5. *Let K be a field. Then the Grassmannian $(2,4)$ over K can be naturally identified with a quadratic hypersurface in $\mathbb{P}_K^5$.*

Proof. To each two dimensional subspace of $\mathbb{A}_K^4$, we may associate a bivector $w=u\wedge v$ where $u,v\in\mathbb{A}_K^4$ are non-proportional vectors. We may write

$$w=a_{12}e_1\wedge e_2+\dots+a_{34}e_3\wedge e_4$$

Since $w\wedge w=0$, we arrive at the following:

$$a_{12}a_{34}(e_1\wedge e_2\wedge e_3\wedge e_4)+a_{13}a_{24}(e_1\wedge e_3\wedge e_2\wedge e_4)+a_{14}a_{23}(e_1\wedge e_4\wedge e_2\wedge e_3)=0$$

Using the fact that $u\wedge v=-v\wedge u$ we have

$$(a_{12}a_{34}-a_{13}a_{24}+a_{14}a_{23})(e_1\wedge e_2\wedge e_3\wedge e_4)=0$$

and so we have $a_{12}a_{34}-a_{13}a_{24}+a_{14}a_{23}=0$. Passing to the coordinate system of $\mathbb{P}_K^5$ we can write this as $X_0X_1-X_2X_3+X_4X_5=0$. □

8 Hilbert's Basis Theorem

Definition 8.1. Let R be a ring and $I \lhd R$ an ideal. We define the **radical** of I to be

$$\sqrt{I} = \{ r \in R \mid r^n \in I \text{ for some } n \in \mathbb{N} \}$$

We say that I is **radical** if $I = \sqrt{I}$.

Definition 8.2. Let R be a ring. Then R is **Noetherian** if every ideal of R is finitely generated.

Lemma 8.3. *Let R be a ring. Then the following conditions are equivalent:*

1. *R is Noetherian*
2. *Every ascending chain of ideals of R is stationary*
3. *Every non-empty set of ideals of R has a maximal element.*

Proof. We first show that (1) $\implies$ (2). Suppose that R is Noetherian and let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

be an ascending chain of ideals in R. Let I be the union of the I_j for all $j \geq 1$. Then I is an ideal and, since R is Noetherian, it is finitely generated say by $a_1, \dots, a_n \in R$. Now, for all $1 \leq i \leq n$ there exists a $j \geq 1$ such that $a_i \in I_j$. Let I_k be the largest such ideal. Then I_k contains all $a_1, \dots, a_n$ whence $I \subseteq I_k$. We also have the trivial inclusion $I_k \subseteq I$ and we see that the chain is stationary.

We now show that (2) $\implies$ (3). Let $\mathcal{I}$ be a non-empty set of ideals of R. Choose an ideal $I_1 \in \mathcal{I}$. If I_1 is maximal then we are done. If not then $\mathcal{I} \backslash I_1$ is non-empty and we may choose I_2 such that $I_1 \subseteq I_2$. We may continue in this fashion, forming an ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \dots$. By assumption, this chain is stationary at some I_k. Then this I_k is the desired maximal element of $\mathcal{I}$.

Finally, we show that (3) $\implies$ (1). Suppose that every non-empty set of ideals of R has a maximal element. Let $I \lhd R$ be an ideal. Denote

$$\mathcal{I} = \{ J \subseteq I \mid J \lhd R \text{ and } J \text{ is finitely generated} \}$$

Clearly $\mathcal{I}$ is non-empty since it contains the zero ideal. By assumption, we may choose a maximal element of $\mathcal{I}$, say J. If $I = J$ then we are done. If not then consider $a \in I \backslash J$. Then $(J, \{ a \})$ is a finitely generated ideal contained in I which contains J. This is a contradiction to the maximality of J. Hence $I = J$ and I is Noetherian. $\square$

Theorem 8.4 (Hilbert's Basis Theorem)**.** *Let R be a Noetherian ring. Then $R[X]$ is Noetherian.*

Proof. Let $I \lhd R[X]$ be an ideal. We need to show that I is finitely generated. To this end, let I' be the ideal in R generated by the leading coefficients of polynomials from I. Since R is Noetherian, we must have that $I' = (a_1, \dots, a_s)$ for some $a_i \in R$.

Let $f_1, \dots, f_s \in I$ be polynomials whose leading coefficients are the a_i. Let N be the maximal degree of the polynomials f_i.

Let $J = (f_1, \dots, f_n) \lhd R[X]$. Then for all $f \in I$, there exists a $g \in J$ such that $\deg(f-g) < N$. Hence if $R[X]^{<N}$ is the linear subspace of $R[X]$ consisting of all polynomials of degree less than N, we see that I is generated by $f_1, \dots, f_s$ and $I \cap R[X]^{<N}$. We can then repeat the same process restricted to $R[X]^{<N}$ to see that there exist some $f_{s+1}, \dots, f_t$ such that I is generated by $f_1, \dots, f_t$ and $I \cap R[X]^{<N-1}$. Continuing in this way, we obtain finitely many generators for I. □

Corollary 8.5. *Let R be a Noetherian ring. Then $R[X_1, \dots, X_n]$ is Noetherian.*

Corollary 8.6. *Let R be a ring and M a finitely generated R-module. Then M is Noetherian.*

9 Varieties and Hilbert Nullstellensatz

Definition 9.1. Let K be a field and $V \subseteq \mathbb{A}^n_K$ a subset. We say that V is a **affine variety** if there exist polynomials $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ such that

$$V = \{ (a_1, \dots, a_n) \in \mathbb{A}^n_K \mid f_i(a_1, \dots, a_n) = 0 \text{ for } 1 \le i \le m \}$$

Definition 9.2. Let K be a field and $I \lhd K[X_1, \dots, X_n]$ an ideal. We can define an affine variety attached to I by

$$V(I) = \{ (a_0, \dots, a_n) \in \mathbb{A}^n_K \mid f(a_0, \dots, a_n) = 0 \; \forall \, f \in I \}$$

Remark. The above definition makes sense since Hilbert's Basis Theorem guarantees that every ideal of $K[X_1, \dots, X_n]$ is finitely generated and thus there exist finitely many polynomials defining $V(I)$.

Proposition 9.3. *Let K be a field and denote $I, J \lhd R = K[X_1, \dots, X_n]$ ideals. Then*

1. $V(\{0\}) = \mathbb{A}^n_K, V(R) = \varnothing$
2. *If* $I \subseteq J$ *then* $V(J) \subseteq V(I)$
3. $V(I) \cup V(J) = V(I \cap J)$
4. $\bigcap_n V(I_n) = V(\prod_n I_n)$

Proof.

Part 1: $V(\{0\}) = \mathbb{A}^n_K$ holds since the zero polynomial will vanish at any point of $\mathbb{A}^n_K$. Conversely, the ring R cannot be generated by finitely many non-constant polynomials so we must have that $V(R) = \varnothing$.

Part 2: If $I \subseteq J$ then, clearly, J has at least the same number of generators as I. In the case that $I = J$, it is clear that $V(J) = V(I)$. In the case that $I \subsetneq J$ then J must have more generators and thus there are more polynomials which define the variety $V(J)$. Having more polynomials means the freedom of choice of elements of $\mathbb{A}^n_K$ is reduced so we must have that $V(J) \subseteq V(J)$.

Part 3: We have $I \cap J \subseteq I$ and so, Part 2 implies that $V(I) \subseteq V(I \cap J)$. Similarly, $V(J) \subseteq V(I \cap J)$. Hence $V(I) \cup V(J) \subseteq V(I \cap J)$.

Conversely, suppose that $P \in V(I \cap J)$ and assume that $P \notin V(I)$. Then there exists $f \in I$ such that $f(P) \neq 0$. By a similar argumentation, there exists $g \in J$ such that $g(P) \neq 0$. Then $f \circ g \in I \cap J$ but $(f \circ g)(P) \neq 0$ which is a contradiction.

Part 4: Suppose $P \in \bigcap_n V(I_n)$. Then for each n, there exists a finite number of polynomials in I_n, say $f_1^{(n)}, \ldots, f_N^{(n)}$ which vanish at P. Clearly, any finite linear combination of such polynomials must vanish at P whence $P \in V(\prod_n I_n)$.

Conversely, suppose that $P \in V(\prod_n I_n)$. Clearly, $I_n \subseteq \prod_n I_n$. It then follows by Part 2 that $V(\prod_n I_n) \subseteq V(I_n)$ for all n. Hence $V(\prod_n I_n) \subseteq \bigcap_n V(I_n)$.

$\square$

Proposition 9.4. *Let K be a field. Then defining the $V(I)$ to be closed sets of $\mathbb{A}_K^n$ defines a topology τ_Z on $\mathbb{A}_K^n$ called the* ***Zariski Topology****.*

Proof. In order to show that the Zariski Topology is indeed a Topology, we need to prove

1. $\mathbb{A}_K^n, \varnothing \in \tau_Z$
2. Any intersection of elements of τ_Z is again an element of τ_Z
3. Finite unions of elements of τ_Z is again an element of τ_Z

By 9.3 we know that $V(\{0\}) = \mathbb{A}_K^n$ and thus $\mathbb{A}_K^n \in \tau_Z$. Furthermore, the empty set is vacuously an affine variety so also $\varnothing \in \tau_Z$.

Now let $\{V_n\}_{n \in \mathbb{N}}$ be a collection of elements of τ_Z. We have $\bigcap_n V_n = V(\prod_n I_n)$ and so $\bigcap_n V_n \in \tau_Z$.

Finally, let $V(I_1), \ldots, V(I_n) \in \tau_Z$. Then $V(I_1) \cup \cdots \cup V(I_n) = V(I_1 \cup \cdots \cup I_n)$ and so $V(I_1) \cup \cdots \cup V(I_n) \in \tau_Z$. $\square$

Proposition 9.5. *Let K be a field. Then any polynomial mapping on $\mathbb{A}_K$ is continuous with respect to the Zariski Topology.*

Proof. Recall that a mapping is continuous with respect to some topology if and only if the preimage of any closed set is closed. Let $f \in K[X_1, \ldots, X_n]$ be a polynomial. Let $X \in \tau_Z$ be a closed set. We need to show that the preimage of $f(X)$ is in τ_Z. Recall that the closed sets of τ_Z are exactly the affine varieties. Hence X is defined by some polynomials $h_1, \ldots, h_N \in K[X_1, \ldots, X_n]$. Now, $x \in f^{-1}(X)$ if and only if $f(x) \in X$ if and only if $h_i(f(x)) = 0$ for all $1 \leq i \leq N$. This then means that $f^{-1}(X)$ is defined by the equations $h_1 \circ f, \ldots, h_N \circ f$ which means that $f^{-1}(X)$ is an affine variety and is thus in τ_Z. Hence f is a continuous mapping with respect to the Zariski Topology. $\square$

Definition 9.6. Let K be a field and $V \subseteq \mathbb{A}_K$ an affine variety. We define the **vanishing ideal** of V to be

$$I(V) = \{ f \in K[X_1, \ldots, X_n] \mid f(a_1, \ldots, a_n) = 0 \; \forall \, (a_1, \ldots, a_n) \in V \}$$

Proposition 9.7. *Let K be a field and $V \subseteq \mathbb{A}_K^n$ a variety. Then $I(V)$ is a radical ideal.*

Proof. Suppose that $f \in \sqrt{V(I)}$. Then $f^n \in V(I)$ for some $n \in \mathbb{N}$. Hence there exists a point $P \in V$ at which f^n vanishes. But then so f also vanishes at P and thus $f \in V(I)$ as required. $\square$

Proposition 9.8. *Let K be a field and $V \subseteq \mathbb{A}_K^n$ an affine variety. Then*

1. $V(I(V)) = V$

2. $I(V(I)) \subseteq I$

3. If I *is non-radical then* $I(V(I)) \subsetneq I$

Proof.

Part 1: Suppose that $f \in I(V)$. Then by definition, f vanishes on V so $V \subseteq V(I(V))$.

Conversely, suppose $P \notin V$. Then, since V is given by some $f_1, \ldots, f_n \in K[X_1, \ldots, X_n]$, there must exist an f_i such that $f_i(P) \neq 0$. But $f_i \in I(V)$ so we must have that $P \notin V(I(V))$.

Part 2: Suppose that $f \in I(V(I))$. Then, by definition, there exists a $P \in V(I)$ such that $f(P) = 0$. It then follows that $f \in I$.

Part 3: By Part 2 we have that $I(V(I)) \subseteq I$. By Proposition 9.7 we know that $I(V(I))$ is radical. Hence if I is not radical, we cannot have that $I(V(I)) = I$ so we must have that $I(V(I)) \subsetneq I$.

□

Theorem 9.9 (Hilbert's Nullstellensatz)**.** *Let* K *be an algebraically closed field and* $I \triangleleft K[X_1, \ldots, X_n]$ *an ideal. Then* $I(V(I)) = \sqrt{I}$*.*

This theorem has the following meaning. If K is an algebraically closed field and $F_1, \ldots, F_m, G \in K[X_1, \ldots, X_n]$ are such that G vanishes whenever all the F_i vanish then there exists an $N > 0$ such that

$$G^N = A_1F_1 + \cdots + A_mF_m$$

for some $A_i \in K[X_1, \ldots, X_n]$.

Corollary 9.10. *Let* K *be algebraically closed and* $I \triangleleft K[X_1, \ldots, X_n]$ *an ideal. Then* $V(I)$ *is empty if and only if there exist* $f_1, \ldots, f_k \in I$ *and* $g_1, \ldots, g_k \in K[X_1, \ldots, X_n]$ *such that*

$$\sum_{i=1}^{k} f_i g_i = 1$$

Proof. If we are able to write 1 as a linear combination of the f_i then, clearly, the f_i cannot vanish simultaneously and so $V(I) = \varnothing$.

Conversely, suppose that $V(I) = \varnothing$. We need to show that $1 \in I$. By the Nullstellensatz we have that $\sqrt{I} = I(V(I)) = I(\varnothing) = K[X_1, \ldots, X_n]$. Hence $1^n \in I$ for some $n > 0$ whence $1 \in I$. □

Corollary 9.11. *Let* K *be an algebraically closed field. Then every maximal ideal of* $K[X_1, \ldots, X_n]$ *is of the form*

$$\mathfrak{m}_a = (X_1 - a_1, \ldots, X_n - a_n)$$

for some $a_i \in K$*.*

Proof. It is clear that $K[X_1, \ldots, X_n]/\mathfrak{m}_a = K$ and thus $\mathfrak{m}_a$ is a maximal ideal.

Conversely, suppose that $I \triangleleft K$ is a maximal ideal. Then $1 \notin I$. Appealing to Corollary 9.10 we see that $V(I)$ contains at least one point $a = (a_1, \ldots, a_n) \in \mathbb{A}_K^n$. hence we must have that $I \subseteq \mathfrak{m}_a$. But I is maximal so $I = \mathfrak{m}_a$. □

Corollary 9.12. *Let K be an algebraically closed field and $f, g \in K[X_1, \dots, X_n]$. If f is irreducible and g vanishes on the hypersurface $f(X_0, \dots, X_n) = 0$ then f divides g.*

Proof. We have that $I(V(f)) = \sqrt{(f)}$. Since g vanishes on $f = 0$ we have that $g \in \sqrt{(f)}$. Then $g^n \in (f)$ for some $n > 0$. But $K[X_1, \dots, X_n]$ is a UFD so $g \in (f)$. $\square$

Definition 9.13. Let K be a field and $V \subseteq \mathbb{A}^n_K$ an affine variety. We say that V is **irreducible** if it cannot be expressed as $V = V_1 \cup V_2$ where $V_i \subsetneq$ are proper affine V-subvarieties.

Proposition 9.14. *Let K be a field and $V \subseteq \mathbb{A}^n_K$ a variety. Then V is irreducible if $I(V)$ is prime.*

Proof. Suppose that $I(V)$ is not prime. We can then find $f_1, f_2 \notin I(V)$ such that $f_1 f_2 \in I(V)$. Then for all $P \in V$ we have $f_1(P) f_2(P) = 0$. But $K[X_1, \dots, X_n]$ is an integral domain so either $f_1(P) = 0$ or $f_2(P) = 0$. This implies that either $P \in V(F_1)$ or $P \in V(F_2)$. Furthermore, $f_i \notin V$ means that $V(f_i) \neq V$ so we have a decomposition

$$V = (V \cap V(f_1)) \cup (V \cap V(f_2))$$

and thus V is reducible.

Conversely, suppose that $I(V)$ is prime and assume, for a contradiction, that $V = V_1 \cup V_2$ for some proper affine V-subvarieties V_1, V_2. Let $I_i = I(V_i)$. Then $V(I_i) = V_i$ and thus $V(I(V)) = V = V_1 \cup V_2 = V(I_1) \cup V(I_2) = V(I_1 \cap I_2)$. Now, $V(I), I_1$ and I_2 are all radical so by the Nullstellensatz, we must have that $I(V) = I_1 \cap I_2$. Furthermore, $I(V) \subsetneq I_1, I_2$ so there exists $f_1 \in I_1 \backslash I(V)$ and $f_2 \in I_2 \backslash I(V)$. Then $f_1 f_2 \in I_1 \cap I_2 = I(V)$ which is a contradiction to the fact that $I(V)$ is prime. $\square$

Definition 9.15. Let K be a field and $V \subseteq \mathbb{A}^n_K$ an affine variety. We define the **coordinate ring** of V to be

$$K[V] = K[X_1, \dots, X_n]/I(V)$$

Proposition 9.16. *Let K be an algebraically closed field and $V \subseteq \mathbb{A}^n_K$ an affine variety. Then there is a one-to-one correspondence between the elements of V and the maximal ideals of $K[V]$.*

Proof. Recall that there is a one-to-one correspondence between the ideals of $K[X_1, \dots, X_n]/I(V)$ and the ideals of $K[X_1, \dots, X_n]$ containing $I(V)$. This in turn implies that there is a one-to-one correspondence between the maximal ideals of $K[X_1, \dots, X_n]/I(V)$ and the maximal ideals of $K[X_1, \dots, X_n]$ containing $I(V)$. By Corollary 9.11 every maximal ideal of $K[X_1, \dots, X_n]$ is of the form $\mathfrak{m}_a = (X - a_1, \dots, X - a_n)$ for some $a = (a_1, \dots, a_n) \in \mathbb{A}^n_K$. But $\mathfrak{m}_a$ contains $I(V)$ if and only if $a \in V$. Putting these facts together gives us the one-to-one correspondence between points of V and maximal ideals of $K[V]$. $\square$

10 Hilbert Functions and Hilbert Polynomials

Definition 10.1. Let R be a ring. We say that R is **graded** if there exist a collection of abelian groups $\{ R_i \}$ such that

$$R = \bigoplus_i R_i$$

and the following properties hold:

1. $R_i R_j \subseteq R_{i+j}$
2. Any $r \in R$ can be expressed as a finite sum of elements in some of the R_i

Any element $r \in R_i$ is said to be a **homogeneous element**. A **homogeneous ideal** is one generated by a homogeneous element of a graded ring.

Example 10.2. Let K be a field. Then $K[X_1, \ldots, X_n]$ is a graded ring. Indeed

$$K[X_1, \ldots, X_n] = \bigoplus_i R_i$$

where R_i is the vector space of homogeneous polynomials of degree i.

Definition 10.3. Let R be a graded ring such that R_0 is a field K, R is generated by $R_0 \oplus R_1$ and R_1 is finite-dimensional over K. Then we shall refer to R as an **admissible** graded ring.

Definition 10.4. Let R be an admissible graded ring. We define the Hilbert function of R to be

$$h_R(d) = \dim_{R_0}(R_d)$$

Example 10.5. Consider $R = K[X_0, X_1, \ldots, X_n]$. Then R is admissible and

$$h_R(d) = \binom{n+d}{d} = \frac{(d+1)\ldots(d+n)}{n!}$$

Definition 10.6. Let K be a field and $X \subseteq \mathbb{P}^n_K$ a projective variety. We define the **homogeneous vanishing ideal** of X to be

$$I(X) = \{\, f \in K[X_0, \ldots, X_n] \mid f(a_0, \ldots, a_n) = 0 \;\forall\, [a_0 : \ldots : a_n] \in \mathbb{P}^n_K \,\}$$

We define the **homogeneous coordinate ring** of X to be

$$S(X) = K[X_0, \ldots, X_n]/I(X)$$

Proposition 10.7. *Let K be a field and $X \subseteq \mathbb{P})K^n$ a projective variety. Then the homogeneous ideal and homogeneous coordinate ring of X admissible graded rings.*

Proof. The homogeneous components of $I(X)$, say $I(X)_d$ are exactly the homogeneous polynomials of degree d that vanish on X.

Let K_n be the space of all homogeneous polynomials of degree d. Then the homogeneous components of $S(X)$ are $K_d/I(X)_d$. □

Definition 10.8. Let K be a field and $X \subseteq \mathbb{P}^n_K$ a projective variety. Let $I = I(X)$ be the homogeneous ideal of X. We define the **Hilbert function** of X, denoted $h_X(d)$ to be the Hilbert function of its homogeneous coordinate ring. More generally, if I is a homogeneous ideal then we define its Hilbert function to be the Hilbert function of $K[X_0, \ldots, X_n]/I$.

Example 10.9. Let K be a field and consider $X = \mathbb{P}^n_K$ as a variety over itself. Then $I(X) = \varnothing$. Indeed, there does not exist finitely many polynomials that simultaneously vanish at all points of $\mathbb{P}^n_K$. Then $S(X) = K[X_0, X_1, \ldots, X_n]/\varnothing = K[X_0, X_1, \ldots, X_n]$.

Example 10.10. Let K be a field and $p_1, p_2, p_3 \in \mathbb{P}^2_K$ distinct points. Let $I = I(X)$. We are interested in determining $h_I(d)$. First suppose that $d = 1$. If K_n is the n^{th} homogeneous component of $K[X_0, X_1, X_2]$ we have that

$$h_I(1) = \dim_K(K_1/I_1) = \dim_K(K_1) - \dim_K(I_1) = 3 - \dim)K(I_1)$$

Now I_1 is the space of homogeneous polynomials of degree 1 that vanish at p_1, p_2, p_3. This space is non-trivial, and has dimension 1, if and only if p_1, p_2, p_3 are colinear. Hence we have that

$$h_I(1) = \begin{cases} 2 & \text{if } p_1, p_2, p_3 \text{ are colinear} \\ 3 & \text{if otherwise} \end{cases}$$

Now suppose that $d = 2$. We claim that $h_I(2) = 3$ regardless of whether the points are colinear or not. Fix representatives $v_1, v_2, v_3 \in \mathbb{A}^3_K \setminus \{0\}$. We define a mapping

$$\varphi : K_2 \to \mathbb{A}^3_K$$

where we evaluate a polynomial in K_2 at each of the points v_1, v_2, v_3. Now, we can multiply a linear homogeneous polymnomial vanishing at p_1 but not p_3 by a linear homogeneous polynomial vanishing at p_2 but not p_3 to get a homogeneous quadratic polynomial vanishing at p_1 and p_2 but not p_3. We can repeat this process to find homogeneous quadratic polynomials that vanish at any 2 of the 3 points. Hence the image of φ contains the standard basis vectors whence the image of φ is all of $\mathbb{A}^3_K$. We then have that

$$\begin{aligned} h_I(2) = \dim_K(K_2/I_2) = \dim_K(K_2) - \dim_K(I_2) &= \dim_K(K_2) - \dim_K(\ker(\varphi)) \\ &= \dim_K(\mathrm{im}(\varphi)) = 3 \end{aligned}$$

The same proof shows that $h_I(d) = 3$ for all $d \geq 3$. We have those completely determined the Hilbert function for this projective variety.

Theorem 10.11. *Let K be a field and $X \subseteq \mathbb{P}^n_K$ a projective variety (I a homogeneous ideal). Then for large enough d, $h_X(d)$ ($h_I(d)$) is a polynomial.*

Definition 10.12. Let K be a field and $X \subseteq \mathbb{P}^n_K$ a projective variety. The unique polynomial $p_X(d) = h_X(d)$ is called the **Hilbert polynomial** of X. If $p_X(d) = a_k d^k + \cdots + a_0$ then the **dimension** of $\dim X$ is k. Furthermore, the **degree** of X is defined to be $\deg X = k! a_k$.

Proposition 10.13. *Let K be an algebraically closed field and $F \in K[X_0, X_1, \ldots, X_n]$ an irreducible homogeneous polynomial of degree d. Let $X_F \subseteq \mathbb{P}^n_K$ be the hypersurface given by $F = 0$. Then the Hilbert polynomial of X_F is*

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

Proof. The first term in the formula is the K-dimension of the space of homogeneous polynomials of degree m. It thus suffices to prove that the second term is the K-dimension of $I(X_F)_m$.

$I(X_F)_m$ consists of all homogeneous polynomials of degree m that vanish at the hypersurface $F = 0$. By the Nullstellensatz we have

$$I(X_F) = \sqrt{(F)}$$

Now, F is irreducible so $\sqrt{(F)} = (F)$. Indeed, if $G^k \in (F)$ then $G^k = HF$ for some $H \in K[X_0, X_1, \ldots, X_n]$. Since $K[X_0, X_1, \ldots, X_n]$ is a unique factorisation domain, we must have that $G = H'F$ for some for some $H' \in K[X_0, X_1, \ldots, X_n]$. Letting K_n be the n^{th} homogeneous component of $K[X_1, \ldots, X_n]$, we see that $I(X_F)_m = FK_{m-d}$ and we are done. $\square$

Remark. Note that the above proof relies on the fact that $\sqrt{(F)} = (F)$. This in fact holds for any F of the form $F = F_1 \cdots F_n$ where each F_i is irreducible and pair-wise distinct.

Example 10.14. Let K be a field and $X \subseteq \mathbb{P}^2_K$ be the hypersurface given by a curve. Then

$$h_X(m) = \binom{m+2}{2} - \binom{m+2-d}{2} = dm - \frac{d(d-3)}{2}$$

11 Bézout's Theorem in Higher Dimensions

Lemma 11.1. *Let K be a field and U, V, W vector spaces over K. If*

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

is an exact sequence for some linear maps $f : U \to V$ and $g : V \to U$ then $\dim_K(V) = \dim_K(U) + \dim_K(W)$.

Proof. We have

$$\begin{aligned} \dim_K(V) = \dim_K(\ker(g)) + \dim_K(\operatorname{im}(g)) &= \dim_K(\operatorname{im}(f)) + \dim_K(\operatorname{im}(g)) \\ &= \dim_K(U) + \dim_K(W) \end{aligned}$$

$\square$

Proposition 11.2. *Let K be a field and $I, J \lhd K[X_0, X_1, \ldots, X_n]$ homogeneous ideals. Then $h_{I\cap J} + h_{I+J} = h_I + h_J$.*

Proof. We have the following exact sequence

$$0 \longrightarrow R/(I\cap J) \longrightarrow R/I \times R/J \longrightarrow R/(I+J) \longrightarrow 0$$

with the second map sending $\overline{f}$ to $(\overline{f}, \overline{f})$ and the third map sending $(\overline{f}, \overline{g})$ to $\overline{f} - \overline{g}$. Passing to the d^{th} homogeneous component in this sequence and applying Lemma 11.1 yields the formula. $\square$

Proposition 11.3. *Let K be a field and $I \lhd K[X_0, X_1, \ldots, X_n]$ a homogeneous ideal. Let $f \in K[X_0, X_1, \ldots, X_n]$ be a homogeneous polynomial of degree e. Assume there exists a $d_0 \in \mathbb{N}$ such that for all $g \in K[X_0, X_1, \ldots, X_n]$ of degree at least d_0 with $fg \in I$ we have $g \in I$. Then $h_{I+(f)}(d) = h_I(d) - h_I(d-e)$ for almost all $d \in \mathbb{N}$.*

Proof. Denote $R = K[X_0, X_1, \ldots, X_n]$. Then for all d such that $d - e \geq d_0$ we have the following exact sequence

$$0 \longrightarrow R_{d-e}/I_{d-e} \longrightarrow R_d/I_d \longrightarrow R_d/(I+(f))_d \longrightarrow 0$$

with the first map given by multiplication by f and the second map given by the quotient map. The injectivity of the second map is guaranteed by the hypothesis of the theorem. The surjectivity of the third map is guaranteed by it being a quotient map. Appealing to Lemma 11.1 yields the formula. $\square$

Remark. Let K be a field and $X \subseteq \mathbb{P}_K^n$ a projective variety. Let $I = I(X)$ be the corresponding homogeneous ideal. Consider the irreducible decomposition $X = X_1 \cup \dots \cup X_r$ so that $I(X) = I(X_1) \cap \dots I(X_n)$. Suppose that $F \in K[X_0, \dots, X_n]$ does not vanish on any X_i. We shall show that the assumption of the previous proposition holds.

If f does not vanish on any of the X_i then $\overline{f}$ is non-zero in $S(X_i)$ for all i. If $gf \in I$ then $gf \in I(X_i)$ for all i. So $\overline{g}\overline{f} \in S(X_i)$. But $S(X_i)$ is an integral domain and $\overline{f}$ is non-zero so $\overline{g} = 0$. This means that $g \in I(X_i)$ and thus $g \in I$.

Theorem 11.4. *Let K be a field and $X \subseteq \mathbb{P}_K^n$ a projective variety of dimension at least 1. Let $f \in K[X_0, X_1, \dots, X_n]$ be a homogeneous polynomial that does not vanish on any irreducible component of X. Then*

$$\deg(I(X) + (f)) = \deg(X)\deg(f)$$

Proof. Let $m = \dim(X)$. By definition, the Hilbert polynomial of X is

$$p_X(d) = \frac{\deg X}{m!}d^m + a_{m-1}d^{m-1} + \dots + a_0$$

for some $a_i \in \mathbb{Q}$. Let $e = \deg(f)$. By the previous remark we can apply the lemma to see that

$$\begin{aligned} p_{I(X)+f}(d) &= p_X(d) - p_X(d-e) \\ &= \frac{\deg(X)}{m!}(d^m - (d-e)^m) + am - 1(d^{m-1} - (d-e)^{m-1}) + \dots \\ &= \frac{e\deg(X)}{(m-1)!}d^{m-1} + \dots \end{aligned}$$

Hence $\deg(I(X) + (f)) = \deg(X)e = \deg(X)\deg(f)$. $\square$

Theorem 11.5. *Let K be a field and $X_1, \dots, X_k \subseteq \mathbb{P}_K^n$ projective varieties of dimensions $n_1, \dots, n_k$ and degrees $d_1, \dots, d_k$ respectively. Suppose that $\sum_i n - n_i$ and $X_1 \cap \dots \cap X_k$ has finite cardinality. Then this number is at most $d_1 \cdots d_k$.*