A Discussion of Gröbner Bases and the Hilbert Scheme

Citation

Permanent link
https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37371732

Terms of Use
This article was downloaded from Harvard University’s DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA

Share Your Story
The Harvard community has made this article openly available. Please share how this access benefits you. Submit a story.

Accessibility
A DISCUSSION OF GRÖBNER BASES AND THE HILBERT SCHEME

Raluca Vlad

Advisor: Joe Harris

submitted in partial fulfillment of the requirements for a degree of Bachelor of Arts with Honors in Mathematics and Computer Science

Harvard University
March 21, 2022
1. Introduction

In this expository thesis, we want to present an introduction to computational algebraic geometry through the lens of Gr"obner bases and describe the construction and some pathological examples on the Hilbert scheme. In section 2, we introduce some algebra preliminaries and define Gr"obner bases, while in section 3 we focus on discussing Buchberger’s algorithm for computing the Gr"obner basis of a given ideal. In section 4, we give two definitions for the Hilbert polynomial associated to a subscheme, and use Gr"obner bases to prove the existence of this polynomial and to show a way of computing it. In section 5, we present an extended example and compute the Hilbert polynomial associated to smooth algebraic curves, for which we introduce Weil divisors. The Hilbert polynomial will help us introduce the Hilbert scheme in section 6, which parametrizes subschemes of the projective space with a fixed Hilbert polynomial. We also describe the construction of the Hilbert scheme in this section. Then, in sections 7 and 8, we discuss the Hilbert scheme of twisted cubics, for which we introduce the notion of extraneous component, and Mumford’s example.

I would like to thank Professor Joe Harris for helping me through the process of writing this thesis, for meeting with me, answering my questions, and being a mentor to me in the last year (and in the entire four years of my time as an undergraduate student).

2. Gr"obner Bases

The main object of study in algebraic geometry are varieties, which are defined as the vanishing locus of certain multivariable polynomials – or, more precisely, the vanishing locus of ideals of a polynomial ring. Understanding many geometric properties of varieties often translates into understanding certain algebraic properties of their corresponding ideals. Therefore, we would like to be able to understand those ideals.

When working with polynomials in one variable, this task is fairly easy. Indeed, if $k$ is a field and we work with the polynomial ring $k[x]$, then all ideals $I \subset k[x]$ are principal, i.e. generated by one element. Given any ideal $I$, say generated by $p_1, p_2, \ldots, p_m \in k[x]$, then one can find the polynomial $p$ that alone generates $I$ by finding the greatest common divisor of $p_1, p_2, \ldots, p_m$. This can be done with the Euclidean algorithm. Then, to test whether any polynomial $q \in k[x]$ belongs to $I$ amounts to testing whether $q$ is a multiple of $p$ or not, which can be done with long division.
However, things get more complicated when working with more than one variable. The purpose of Gröbner bases is to allow for a similar process of understanding ideals of polynomial rings in several variables. We try to make this precise in the following few sections. In this section, we define Gröbner bases, following chapter 2 from [CLO07] and [Gun22].

2.1. Preliminaries. We start by presenting some algebra preliminaries. The main point of this subsection is to state and prove Hilbert’s Basis Theorem, which tells us that all ideals of a polynomial ring $k[x_1, x_2, \ldots, x_n]$ over some field $k$ are finitely generated. In other words, the ideals we want to understand can be specified using fairly small (i.e. finite) amount of information. Even though we are primarily interested in ideals of polynomial rings, we state the results in this subsection for commutative rings more generally.

Definition 2.1. Given a commutative ring $R$, an ideal of $R$ is a subset $I \subseteq R$ satisfying the following two properties:

1. Under the operation of addition, $(I, +)$ is a subgroup of $(R, +);
2. $I$ is closed under multiplication by ring elements: if $i \in I$ and $r \in R$, then $ri \in I$.

Definition 2.2. Given a subset $S \subseteq R$, the ideal generated by $S$ is denoted by $\langle S \rangle$ and it equals the set of all possible $R$-linear combinations of elements of $S$:

$$\langle S \rangle = \{r_1s_1 + r_2s_2 + \cdots + r_ms_m \mid m \in \mathbb{Z}_{>0}, r_i \in R, s_i \in S\}.$$

One can fairly easily check that the set above satisfies the definition of an ideal. Moreover, we say that an ideal $I \subseteq R$ is finitely generated if there exists a finite set $S \subseteq R$ that generates it.

Definition 2.3. A commutative ring $R$ is Noetherian if it satisfies the ascending chain condition: any increasing sequence of ideals of $R$

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$$

stabilizes, i.e. there exists a non-negative integer $N$ such that $I_n = I_N$ for all $n \geq N$.

Proposition 2.1. A ring $R$ is Noetherian if and only if every ideal $I \subseteq R$ is finitely generated.

Proof. If $I \subseteq R$ were not finitely generated, then we would be able to construct a sequence $\{s_1, s_2, \ldots\}$ such that each

$$s_i \in I \setminus \langle s_1, s_2, \ldots, s_{i-1} \rangle.$$
We would thus get a strictly ascending chain of ideals of \( R \)

\[
\langle s_1 \rangle \subsetneq \langle s_1, s_2 \rangle \subsetneq \langle s_1, s_2, s_3 \rangle \subsetneq \ldots
\]

that never stabilizes, so \( R \) couldn’t be Noetherian.

Conversely, assume that every ideal is finitely generated, and consider any sequence of ascending ideals of \( R \):

\[
I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots.
\]

The union

\[
I := \bigcup_{i \geq 0} I_i
\]

is also an ideal of \( R \), and so \( I \) must be finitely generated. Let \( s_1, s_2, \ldots, s_m \in I \) be some (finitely many) elements generating it. For every such generator \( s_j \), let \( i_j \) be an index such that \( s_j \in I_{i_j} \). This means that

\[
I = \langle s_1, s_2, \ldots, s_m \rangle \subseteq \bigcup_{i=0}^{M} I_i
\]

where \( M = \max\{i_j \mid 1 \leq j \leq m\} \), so the chain of ideals above must stabilize after \( I_M \). This is true for any chain of increasing ideals of \( R \), so \( R \) is indeed Noetherian. \( \square \)

**Theorem 1** (Hilbert’s Basis Theorem). *If \( R \) is a Noetherian ring, then so is \( R[x] \).*

*Proof.* Let’s assume, for the sake of contradiction, that there exists an ideal \( I \subseteq R[x] \) that is not finitely generated. We construct a sequence of non-zero polynomials \( \{p_0, p_1, p_2, \ldots\} \subseteq R[x] \) as follows. For each \( i \geq 0 \), pick \( p_i \) to be the polynomial of minimal degree from

\[
p_i \in I \setminus \langle p_0, p_1, \ldots, p_{i-1} \rangle.
\]

Since \( I \) is not finitely generated, we will always have a choice for \( p_i \), and so we get a strictly ascending chain of ideals of \( R[x] \):

\[
\langle p_0 \rangle \subsetneq \langle p_0, p_1 \rangle \subsetneq \langle p_0, p_1, p_2 \rangle \subsetneq \ldots.
\]

Also, note that our choice of each \( p_i \) to have minimal degree implies that the degrees of the polynomials \( p_i \) are (weakly) increasing as \( i \) increases.
For each $i \geq 0$, let $d_i := \deg(p_i)$. Also, let $c_i \in R$ be the (non-zero) leading coefficient of the polynomial $p_i \in R[x]$. We get an ascending chain of ideals of $R$:

$$\langle c_0 \rangle \subseteq \langle c_0, c_1 \rangle \subseteq \langle c_0, c_1, c_2 \rangle \subseteq \ldots$$

Since $R$ is assumed to be Noetherian, this chain must stabilize, so there exists some positive integer $N$ such that

$$\langle c_0, c_1, \ldots, c_N \rangle = \langle c_0, c_1, \ldots, c_{N-1} \rangle \Rightarrow c_N \in \langle c_0, c_1, \ldots, c_{N-1} \rangle.$$

Therefore, we can write $c_N$ as an $R$-linear combination:

$$c_N = \sum_{i=0}^{N-1} r_i \cdot c_i,$$

for some $r_i \in R$. We can thus construct the following polynomial:

$$p = \sum_{i=0}^{N-1} r_i \cdot x^{d_N - d_i} \cdot p_i \in \langle p_0, p_1, \ldots, p_{N-1} \rangle.$$

The leading coefficient of $p$ is precisely $\sum r_i c_i = c_N$ and $\deg(p) = d_N = \deg(p_N)$, so the polynomial $p_N - p$ has degree strictly less than $d_N$ since the leading terms of $p_N$ and $p$ cancel each other. Moreover,

$$p_N - p \in I \setminus \langle p_0, p_1, \ldots, p_{N-1} \rangle$$

since $p$ belongs to $\langle p_0, p_1, \ldots, p_{N-1} \rangle$, but $p_N$ does not. Therefore, we constructed a polynomial $p_N - p$ of degree strictly smaller than $\deg(p_N)$, contradicting our choice of $p_N$ to have minimal degree among $I \setminus \langle p_0, p_1, \ldots, p_{N-1} \rangle$. Our assumption must have thus been false, so $R[x]$ doesn’t have ideals that are not finitely-generated, so $R[x]$ is indeed Noetherian. □

**Remark 2.1.** Any field $k$ is Noetherian since it has only two ideals, $\langle 0 \rangle$ and $k$. Therefore, repeatedly applying Hilbert’s Basis Theorem, we get that any polynomial ring $k[x_1, x_2, \ldots, x_n]$ over $k$ is Noetherian. So any ideal of such a polynomial ring is finitely generated.

### 2.2. Monomial Ordering.

The first step in generalizing the division algorithm to multiple variables is to define monomial orderings – that is, define which monomials in our polynomial ring are “larger” than the others. When working with one variable, this choice is simple – the larger monomial is that with larger degree; in fact, this is how the division algorithm works: we start by eliminating the term with largest degree, then we move to the next one and keep going. However, when working with more than one variable, it is not a priori clear
which the “largest” monomial is. In fact, we will see that there is not a unique choice for it, but we can instead fix a certain monomial ordering and work with respect to it.

**Notation.** Say we work over some field $k$ and polynomial ring $k[x_1, x_2, \ldots, x_n]$. We let

$$\mathcal{A} := \{x_1^{a_1}x_2^{a_2} \cdots x_n^{a_n} \mid a_1, a_2, \ldots, a_n \in \mathbb{Z}_{\geq 0}\}$$

denote the set of monomials in $k[x_1, x_2, \ldots, x_n]$.

**Definition 2.4.** A **monomial order** is a a total order $\leq$ on $\mathcal{A}$ satisfying the following two properties:

1. $\leq$ is a well-order – that is, every non-empty subset of $\mathcal{A}$ has a smallest element;
2. if $M \leq N$ for some monomials $M, N \in \mathcal{A}$, then $MU \leq NU$ for every $U \in \mathcal{A}$.

**Remark 2.2.** In property (1) of the definition, if we take the non-empty subset to be the whole $\mathcal{A}$, then its smallest element must be $1 = x_1^0x_2^0 \cdots x_n^0$. Otherwise, if some monomial $M \neq 1$ were the smallest monomial of $\mathcal{A}$, then $M < 1$; applying property (2) for $U = M$ would then tell us that $M^2 < M$, so $M^2$ would be an even smaller monomial, contradiction.

**Remark 2.3.** Given a monomial ordering $\leq$ on the monomial set $\mathcal{A}$ of $k[x_1, x_2, \ldots, x_n]$, then any strictly decreasing sequence of monomials $(M_i)_{i \geq 0}$ terminates. Otherwise, the set

$$\{M_i \mid i \in \mathbb{Z}_{\geq 0}\}$$

would be a non-empty subset of $\mathcal{A}$ with no smallest element, thus violating the definition of monomial order.

**Example 2.** Since 1 is always the smallest monomial of $\mathcal{A}$, repeatedly applying property (2) for $U = x$ shows that there exists a unique monomial order on the monomials of $k[x]$. This order is the one we expect:

$$1 \leq x \leq x^2 \leq \ldots$$

This uniqueness does not however persist when working with more than one variable. We give below two examples of different monomial orders that one can consider over a polynomial ring in multiple variables.
Example 3. The lexicographic order on the monomials $\mathcal{A}$ of $k[x_1, x_2, \ldots, x_n]$ is, roughly speaking, the order under which terms $x_i$ with smaller indices "weigh more" than terms with larger indices. To make this precise, this is the order defined by:

$$x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \leq x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$$

if and only if there exists some $1 \leq i \leq n$ such that $a_j = b_j$ for all $j < i$ and $a_i < b_i$.

Example 4. The degree-lexicographic order on the monomials $\mathcal{A}$ of $k[x_1, x_2, \ldots, x_n]$ is the order under which monomials with smaller degree are smaller; to break ties between monomials of the same degree, the lexicographic order is used. To make this precise, this is the order defined by:

$$x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \leq x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$$

if and only if $\sum a_i < \sum b_i$ or $\sum a_i = \sum b_i$ and there exists some $1 \leq i \leq n$ such that $a_j = b_j$ for all $j < i$ and $a_i < b_i$.

Remark 2.4. As stated earlier, the lexicographic and degree-lexicographic order on the monomials $\mathcal{A}$ of $k[x_1, x_2, \ldots, x_n]$ are not the same ordering if $n > 1$. Indeed, under the lexicographic order, we have that $x_2^5 < x_1$. However, under the degree-lexicographic order, the monomial $x_1$ is smaller since it has smaller degree.

2.3. Generalized Division Algorithm. Now that we understand how the monomials in our polynomial ring $k[x_1, x_2, \ldots, x_n]$ are ordered, we can describe a generalized division algorithm. Throughout the rest of the section, we are working with respect to some fixed monomial ordering $\leq$ on $\mathcal{A}$.

Definition 2.5. Let $f \in k[x_1, x_2, \ldots, x_n]$ be a polynomial that can be written (uniquely) as the following sum of monomials:

$$f = \sum_{M \in \mathcal{A}} c_M \cdot M,$$

where the coefficients $c_M$ are elements of the base field $k$. We say that a monomial $M \in \mathcal{A}$ occurs or appears in $f$ if $c_M \neq 0$. If $f$ is a non-zero polynomial, then we also define the following:

- the leading monomial of $f$ is

$$\text{LM}(f) := \max\{M \in \mathcal{A} \mid M \text{ occurs in } f\};$$
• the leading coefficient of $f$ is

$$\text{LC}(f) := c_{\text{LM}(f)};$$

• the leading term of $f$ is

$$\text{LT}(f) := \text{LC}(f) \cdot \text{LM}(f).$$

If $f = 0$, then set the convention that $\text{LM}(f) = \text{LT}(f) = 0$.

**Definition 2.6.** We say that a polynomial $f \in \mathbb{k}[x_1, x_2, \ldots, x_n]$ is reduced with respect to a subset $G \subseteq \mathbb{k}[x_1, x_2, \ldots, x_n]$ if no monomial occurring in $f$ is divisible by the leading monomial of any non-zero element of $G$.

**Remark 2.5.** The zero polynomial is vacuously reduced with respect to any set $G$.

**Definition 2.7.** Given a polynomial $f$ and a set $G$ as before, a reduction of $f$ with respect to $G$ is a polynomial $r \in \mathbb{k}[x_1, x_2, \ldots, x_n]$ which is reduced with respect to $G$ and which satisfies

$$f = g_1 h_1 + g_2 h_2 + \cdots + g_s h_s + r,$$

for some polynomials $g_i \in G$ and $h_i \in \mathbb{k}[x_1, x_2, \ldots, x_n]$ with $\text{LM}(g_i h_i) \leq \text{LM}(f)$.

**Remark 2.6.** Note that, if $r$ is the reduction of some polynomial $f$ with respect to some set $G$, then $f - r \in \langle G \rangle$. Thus, reductions with respect to a set $G$ can equivalently be thought of as reductions with respect to the ideal $\langle G \rangle$. Since ideals of polynomial rings always have a finite generating set (according to Hilbert’s Basis Theorem), it suffices to consider reductions with respect to finite sets $G$.

Given $f$ and a finite set $G$ as before, it is not a priori clear if a reduction $r$ of $f$ with respect to $G$ even exists. Below, we give an algorithm that computes such a reduction $r$, thus proving that a reduction always exists. In fact, Definition 2.7 should remind the reader of the definition of remainder from division. Therefore, it should come as no surprise that the algorithm we give below is, in fact, just a generalization of the division algorithm. To briefly summarize the algorithm in words, we want to keep dividing $f$ by elements of $G$ until we reach a reduction $r$.

**input:** polynomial $f \in \mathbb{k}[x_1, \ldots, x_n]$ and finite subset $G \subset \mathbb{k}[x_1, \ldots, x_n]$
\[ i := 0, f_0 := f, \text{updated} := \text{true} \]

repeat
\[ A(f_i) := \{ \text{monomials } M \text{ in } f_i \text{ such that } LM(g) \mid M \text{ for some } g \in G \} \tag{1} \]

if \[ A(f_i) \neq \emptyset \] then
\[ M_i := \max\{A(f_i)\} \]
\[ \text{pick } g_i \in G \text{ st } LM(g_i) \mid M_i \]
\[ f_{i+1} := f_i - \frac{c_M \cdot M_i}{LT(g_i)} \cdot g_i \tag{2}, c_M \text{ is the coefficient of } M_i \text{ in } f_i \]
\[ i = i + 1 \]
else
\[ \text{updated} = \text{false} \]
end if
until \[ \text{updated} = \text{false} \]

output: \[ f_i \in k[x_1, \ldots, x_n], \text{which is now a reduction of } f \text{ with respect to } G \]

Correctness: Let’s now explain why the output of this algorithm is indeed a reduction of \( f \) with respect to \( G \) and why the algorithm terminates after finitely many steps.

The set \( A(f_i) \) in line (1) will be empty precisely when \( f_i \) is reduced with respect to \( G \), so the output of the algorithm will indeed be a reduced polynomial. Moreover, the output \( f_i \) is obtained by repeatedly subtracting products \( g_i h_i \) in line (2), for \( h_i := \frac{c_M \cdot M_i}{LT(g_i)} \), so the output is indeed a reduction of the input \( f \) with respect to \( G \).

Finally, note that \( LM(g_i h_i) = M_i \), so the subtraction in line (2) does not affect the monomials of \( f_i \) that are larger than \( M_i \). This means that all the monomials in \( A(f_{i+1}) \) that can be further reduced are strictly smaller than \( M_i \) (the largest monomial that could be reduced in \( f_i \)). Therefore, the monomials \( M_i \) form a strictly decreasing sequence
\[ M_0 > M_1 > M_2 > \ldots, \]
which must terminate according to Remark 2.3. This proves that our algorithm must terminate as well. It also shows that \( LM(g_i h_i) = M_i \leq M_0 \leq LM(f) \), which was a condition imposed in the definition of reduction.

Remark 2.7. Note that some polynomials \( g_i \) that we pick in the algorithm might be the same. So we could keep track of them and only update their corresponding \( h_i \) instead of
creating a new one in line (2). The condition \( \text{LM}(g_i(h_i + h'_i)) \leq \text{LM}(f) \) will stay true since
\[
\text{LM}(g_i(h_i + h'_i)) = \text{LM}(g_i h_i + g_i h'_i) \leq \max\{\text{LM}(g_i h_i), \text{LM}(g_i h'_i)\}.
\]

**Remark 2.8.** Finally, we end this subsection by noting the rather disappointing fact that reductions are **not** always unique. For example, say we work with the lexicographic or degree-lexicographic monomial ordering. Take the polynomial
\[
f = x_1^4 + x_1^2 + x_2 \in \mathbb{C}[x_1, x_2]
\]
and the set
\[
G = \{x_1^3 + x_1, x_1^4, x_2\} \subset \mathbb{C}[x_1, x_2].
\]

One one hand, we can write
\[
f = x_1(x_1^3 + x_1) + (x_2)
\]
which gives us that the reduction of \( f \) with respect to \( G \) is 0.

On the other hand, we can also write
\[
f = (x_1^4) + (x_2) + x_1^2,
\]
which gives us that the reduction of \( f \) with respect to \( G \) is \( x_1^2 \neq 0 \). In the next subsection, we introduce Gröbner bases to fix this issue.

### 2.4. Gröbner Bases

We would like to find some sets \( G \) with respect to which reductions are unique. This would allow us, for example, to test whether a polynomial \( f \in k[x_1, x_2, \ldots, x_n] \) belongs to the ideal \( \langle G \rangle \) generated by \( G \) or not – indeed, if reductions are unique, then this amounts to testing whether the reduction of \( f \) with respect to \( G \) is 0 or not. It turns out that Gröbner bases have this property. We define them and present some of the properties that they have in this subsection.

**Notation.** Given a set \( S \subset k[x_1, x_2, \ldots, x_n] \), we let
\[
\text{LT}(S) := \{\text{LT}(s) \mid s \in S\}.
\]
It is not hard to see that, if \( I \subset k[x_1, x_2, \ldots, x_n] \) is an ideal, then \( \text{LT}(I) \) is also an ideal.
Definition 2.8. Given an ideal \( I \subseteq k[x_1, x_2, \ldots, x_n] \), a subset \( G \subseteq I \) is a Gröbner basis for our ideal \( I \) if

\[
\text{LT}(I) = \langle \text{LT}(G) \rangle,
\]

i.e. if the leading terms in \( I \) can be generated from the leading terms of elements of \( G \), or equivalently, if every leading term in \( I \) is a multiple of some leading term in \( G \).

Theorem 5. Given any ideal \( I \subseteq k[x_1, x_2, \ldots, x_n] \), there exists a finite Gröbner basis for \( I \).

Proof. According to Hilbert’s Basis Theorem and Remark 2.1, any ideal of \( k[x_1, x_2, \ldots, x_n] \) is finitely-generated. In particular, \( \text{LT}(I) \) must be finitely generated, so we can pick generators \( t_1, t_2, \ldots, t_m \in \text{LT}(I) \) for it. Then, for each \( 1 \leq i \leq m \), pick \( g_i \in I \) such that \( t_i = \text{LT}(g_i) \), so we can pick our Gröbner basis to be \( G := \{g_1, g_2, \ldots, g_m\} \). \( \square \)

Theorem 6. Given any ideal \( I \subseteq k[x_1, \ldots, x_n] \) and a Gröbner basis \( G \) for it, then \( I = \langle G \rangle \).

Proof. A Gröbner basis \( G \) for \( I \) is, by definition, a subset of \( I \), so the inclusion \( \langle G \rangle \subseteq I \) must hold. Conversely, let \( f \in I \), and consider the following reduction of \( f \) (whose existence is guaranteed by the generalized division algorithm from the previous subsection):

\[
f = g_1h_1 + g_2h_2 + \cdots + g_nh_s + r.
\]

Since \( f \in I \) and each \( g_i \in G \subseteq I \), we get that \( r \in I \) as well. If \( r \neq 0 \), then

\[
\text{LT}(r) \in \text{LT}(I) = \langle \text{LT}(G) \rangle.
\]

This means that \( \text{LT}(r) \) must be divisible by some \( \text{LT}(g) \in \text{LT}(G) \), so we could further reduce \( r \) with respect to \( G \), which would contradict our choice of \( r \) as a reduction of \( f \). Therefore, it must be the case that \( r = 0 \), and so \( f \in \langle G \rangle \), which proves the second inclusion \( I \subseteq \langle G \rangle \). \( \square \)

Remark 2.9. This last proof shows that, if \( f \) is an element of an ideal \( I \) and \( G \) is a Gröbner basis of \( I \), then the reduction of \( f \) with respect to \( I \) is necessarily 0. In fact, the converse also holds true: if \( f \in k[x_1, x_2, \ldots, x_n] \) and its reduction with respect to \( G \) is 0, then Remark 2.6 tells us that \( f \in \langle G \rangle = I \).

In fact, the proposition below shows that all reductions with respect to a Gröbner basis are unique, which means that Gröbner bases indeed have the property we set out to achieve:

Proposition 2.2. Given an ideal \( I \subseteq k[x_1, x_2, \ldots, x_n] \) and a Gröbner basis \( G \) for \( I \), any polynomial \( f \in k[x_1, x_2, \ldots, x_n] \) admits a unique reduction with respect to \( G \).
Proof. Let \( r_1, r_2 \in k[x_1, x_2, \ldots, x_n] \) be any two reductions of \( f \) with respect to \( G \). In particular, this means that no monomial appearing in \( r_1 \) or \( r_2 \) is divisible by any leading monomial appearing in \( \langle G \rangle = I \). However, Remark 2.6 tells us that

\[
 f - r_1, f - r_2 \in I \implies r_1 - r_2 \in I.
\]

If \( r_1 \neq r_2 \), then \( \text{LM}(r_1 - r_2) \in \text{LM}(I) \setminus \{0\} \). But \( \text{LM}(r_1 - r_2) \) must appear in at least one of \( r_1 \) and \( r_2 \), so we would get a contradiction. Therefore, it must be the case that \( r_1 = r_2 \), so \( f \) indeed has a unique reduction with respect to \( G \). \( \square \)

### 3. Buchberger’s Algorithm

In this section, we present an algorithm that can compute a Gröbner basis for a given ideal \( I \subseteq k[x_1, x_2, \ldots, x_n] \). This makes Gröbner bases the foundation for computational algebraic geometry. We keep following chapter 2 from [CLO07].

**Definition 3.1.** Given two polynomials \( f, g \in k[x_1, x_2, \ldots, x_n] \), their **S-polynomial** is defined to be the polynomial

\[
 S(f, g) := \frac{x^M}{\text{LT}(f)} \cdot f - \frac{x^M}{\text{LT}(g)} \cdot g,
\]

where the monomial \( x^M \) is the least common multiple of \( \text{LM}(f) \) and \( \text{LM}(g) \).

**Proposition 3.1** (Buchberger’s Criterion). Let \( I \subseteq k[x_1, x_2, \ldots, x_n] \) be an ideal and let \( G := \{g_1, g_2, \ldots, g_s\} \) be a generating set for \( I \). Then, \( G \) is a Gröbner basis for \( I \) if and only if the reduction of each S-polynomial \( S(g_i, g_j) \) with respect to \( G \) is zero.

**Proof.** If \( G \) is a Gröbner basis for \( I \), then the reduction of each \( S(g_i, g_j) \in \langle G \rangle = I \) must be zero according to Remark 2.9. The reverse implication is more tedious, so we will only summarize it and refer the reader to [CLO07]. Let’s thus assume that each \( S(g_i, g_j) \) has zero reduction with respect to \( G \). We want to show that \( \text{LT}(I) \subseteq \langle \text{LT}(G) \rangle \); in other words, if \( f \in I \), we want to show that \( \text{LT}(f) \in \langle \text{LT}(G) \rangle \). We know that \( G \) is a generating set for \( I \), so we can write

\[
 f = \sum_{i=1}^{s} g_i h_i,
\]

for some \( h_i \in k[x_1, x_2, \ldots, x_n] \). If \( M := \max_i \{\text{LM}(g_i h_i)\} \) is larger than \( \text{LM}(f) \), then we can rewrite the terms on the right-hand side with monomial \( M \) as a \( k \)-linear combination of S-polynomials \( S(g_i, g_j) \) with smaller leading monomial. Because the reduction of such
terms with respect to $G$ is zero, then we can further rewrite the right-hand side as $\sum g_i h_i'$ for different $h_i' \in k[x_1, x_2, \ldots, x_n]$ such that

$$\max_i \{\text{LM}(g_i h_i')\} < \max_i \{\text{LM}(g_i h_i)\}.$$  

We can keep going this way until we reach an equality $f = \sum g_i h_i$, for some $h_i \in k[x_1, \ldots, x_n]$ with $\max_i \{\text{LM}(g_i h_i)\} = \text{LM}(f)$. Such an equality then implies that

$$\text{LT}(f) \in \langle \text{LT}(g_1), \text{LT}(g_2), \ldots, \text{LT}(g_s) \rangle = \langle \text{LT}(G) \rangle,$$

as desired. □

We are now ready to describe **Buchberger’s algorithm** for computing a Gröbner basis for an ideal $I \subset k[x_1, x_2, \ldots, x_n]$

**input:** ideal $I \subset k[x_1, \ldots, x_n]$ specified by a finite generating set $G$

$G_{\text{new}} := G$, updated := $false$

**repeat**

$G = G_{\text{new}}$, updated = $false$

**for** $g_i, g_j \in G$ **do**  ▶ (1)

$r = \text{reduction of } S(g_i, g_j) \text{ wrt } G$

**if** $r \neq 0$ **then**

$G_{\text{new}} = G_{\text{new}} \cup \{r\}$, updated = $true$  ▶ (2)

**end if**

**end for**  ▶ (3)

**until** updated = $false$

**output:** $G$, which is now a Gröbner basis for $I$

**Correctness:** Let’s now explain why the output of this algorithm is indeed a Gröbner basis for $I$ and why the algorithm terminates after finitely many steps. First of all, if the algorithm terminates, then the output $G$ satisfies the property that $S(g_i, g_j)$ reduces to 0 with respect to $G$, for all $g_i, g_j \in G$. Otherwise, we would have to keep adding non-zero reductions $r$ to $G_{\text{new}}$ in line (2). Moreover, the output $G$ is a generating for $I$ since it was obtained by adding elements to the initial generating set of $I$. So Proposition 3.1 tells us that the output must indeed be a Gröbner basis, as desired.
Then, to understand why the algorithm must terminate, note that every time we reach the end of the for loop in line (3), we have that

\[ \langle \text{LT}(G) \rangle \subseteq \langle \text{LT}(G_{\text{new}}) \rangle , \]

with the inclusion being strict precisely when \( G \subsetneq G_{\text{new}} \). Indeed, \( G \subseteq G_{\text{new}} \), so the inclusion is true. And, if we updated \( G_{\text{new}} \) by adding some \( r \) to it in line (2), then \( \text{LT}(r) \in \langle \text{LT}(G_{\text{new}}) \rangle \), but \( \text{LT}(r) \notin \langle \text{LT}(G) \rangle \) since \( r \) is a reduction (and thus reduced) with respect to \( G \). Therefore, as long as we keep updating \( G_{\text{new}} \), we get a strictly ascending chain of ideals by putting together all the strict inclusions

\[ \langle \text{LT}(G) \rangle \subsetneq \langle \text{LT}(G_{\text{new}}) \rangle . \]

Since \( k[x_1, x_2, \ldots, x_n] \) is Noetherian by Hilbert’s Basis Theorem, this chain of ideals must stabilize after finitely many steps, i.e. our algorithm must terminate.

3.1. **Improvements to Buchberger’s algorithm.** In this subsection, we mention a few improvements that one can bring to the form of Buchberger’s algorithm described above.

**Remark 3.1.** A fairly easy change that would significantly improve the complexity of the algorithm above is the following. In line (1), there is no need to check all pairs \( g_i, g_j \in G \). In particular, we do not need to consider the pairs \( (g_i, g_j) \in G \) that were already cleared in previous iterations of the algorithm – by “cleared”, I mean that the reduction of their \( S \)-polynomial \( S(g_i, g_j) \) was zero. Indeed, if the reduction of \( S(g_i, g_j) \) with respect to some set \( G \) is zero, then so is the reduction of \( S(g_i, g_j) \) with respect to \( G_{\text{new}} \supseteq G \).

Another improvement that we can bring to the algorithm above concerns the following definition of a more constraining variant of Gröbner bases:

**Definition 3.2.** Given an ideal \( I \subset k[x_1, x_2, \ldots, x_n] \), a **reduced Gröbner basis** for \( I \) is a Gröbner basis \( G \) for \( I \) satisfying the following two properties:

1. \( \text{LC}(g) = 1 \) for all \( g \in G \);
2. No monomial of any \( g \in G \) lies in \( \langle \text{LT}(G \setminus \{g\}) \rangle \).

**Remark 3.2.** The purpose of reduced Gröbner bases is to eliminate elements/terms of elements from a Gröbner basis that are redundant, in the sense that they are not needed to generate \( \text{LT}(I) \). We can adapt our algorithm so that it outputs a reduced Gröbner basis, as
follows: scale every initial element $g \in G$ and every non-zero reduction $r$ so that its leading coefficient is 1; regularly iterate over the monomials of $G$ and eliminate the monomials that violate property (2) of the definition above. Our algorithm above can potentially create very large sized Gröbner bases, so imposing these extra conditions can help us significantly reduce the data we have to keep track of. Moreover, the following proposition shows another advantage of reduced Gröbner bases, which will be useful to us in the next subsection, where we discuss applications of Gröbner bases.

**Proposition 3.2.** An ideal $I \subset k[x_1, \ldots, x_n]$ has a unique reduced Gröbner basis.

*Proof.* See section 2.7 in [CLO07].

### 3.2. Applications of Gröbner Bases

In this subsection, we discuss a few applications of Gröbner bases, following section 2.8 of [CLO07].

#### 3.2.1. Ideal Membership Problem

We briefly mentioned this application earlier. More precisely, given an ideal $I \subset k[x_1, \ldots, x_n]$, we can use a Gröbner basis to test whether a polynomial $f \in k[x_1, \ldots, x_n]$ belongs to $I$ or not. We start by finding a Gröbner basis $G$ for $I$ (for example, using Buchberger’s algorithm). Then, $f$ belongs to $I = \langle G \rangle$ if and only if its reduction with respect to $G$ is zero (see Remark 2.9).

#### 3.2.2. Ideal Equality Problem

Given ideals $I, J \subset k[x_1, \ldots, x_n]$, we can use reduced Gröbner bases to test whether the two ideals are equal. Indeed, in lieu of Proposition 3.2, we can compute reduced Gröbner bases for each of $I$ and $J$. The two ideals will be equal precisely when their reduced Gröbner bases are the same (maybe up to some permutation of the basis elements).

#### 3.2.3. Solving Polynomial Equations

Gröbner bases can be used to solve polynomial equations in multiple variables. Indeed, using Gröbner bases, one can extend the method of back-substitution from systems of linear equations to more general systems of polynomials. The name of the subject studying such methods is Elimination Theory. The name comes from the fact that, when solving a system of polynomials, we try to eliminate variables successively (just like in the linear back-substitution method) by using a lexicographic monomial ordering. We will not go into details about Elimination Theory, but instead refer the reader to chapter 3 of [CLO07].
4. The Hilbert Polynomial

To be able to understand the Hilbert scheme, we first need to define the Hilbert polynomial associated to a closed subscheme of the projective space. In this section, we give two definitions of the Hilbert polynomial and show why they are equivalent. We also show how one can use Gröbner bases to prove the existence of and compute the Hilbert polynomial of a subscheme.

4.1. Coordinate Ring Definition. One can define the Hilbert polynomial \( p_X(m) \) associated to a closed subscheme \( X \subset \mathbb{P}^n \) to be the polynomial that agrees, for large enough values of \( m \), to the dimension of the \( m^{th} \) graded piece of the coordinate ring of \( X \). We make this precise, following [Eis04] and [EH00].

**Definition 4.1.** Let \( k \) be a field and \( M \) a finitely generated graded module over the polynomial ring \( k[x_0, x_1, \ldots, x_n] \), where the polynomial ring is naturally a graded ring with grading given by the polynomial degree. The Hilbert function associated to our module \( M \) is the function \( h_M : \mathbb{Z} \rightarrow \mathbb{Z} \) defined as

\[
h_M(m) := \dim_k M_m,
\]

where the right-hand side refers to the dimension of the \( m^{th} \) graded piece of \( M \) seen as a vector space over \( k \).

**Proposition 4.1.** In the same setting from before where \( M \) is a finitely generated graded module over \( k[x_0, x_1, \ldots, x_n] \), the Hilbert function \( h_M(m) \) agrees for large enough \( m \) with a polynomial \( p_M(m) \in \mathbb{Q}[m] \) of degree at most \( n \). This polynomial is called the Hilbert polynomial associated to \( M \).

**Proof.** We proceed via induction on \( n \). For the base case, take \( n = -1 \) or, in other words, assume that the base ring is just \( k \) (the polynomial ring with no variables). In this case, \( M \) must be a finite dimensional vector space over \( k \) with an associated grading. We must have that \( M_m = \{0\} \) for all integers \( m \) that are larger than the degrees of the (finitely many) generators of \( M \). This means that \( h_M \) agrees with the constant zero polynomial for large enough \( m \).

For the inductive step, let’s assume that the proposition holds for finitely generated modules over \( k[x_0, x_1, \ldots, x_{n-1}] \) and prove that it must also hold for a finitely generated module
$M$ over $k[x_0, x_1, \ldots, x_n]$. First, for any integer $d$, we define the $d^{th}$ twist of $M$ to be the graded module $M(d)$ over $k[x_0, x_1, \ldots, x_n]$ specified by:

$$M(d)_m = M_{m+d}$$

for all integers $m$. In other words, $M(d)$ and $M$ are isomorphic modules, but they have the grading shifted by $d$. Note that this shift guarantees that multiplication by any degree $d$ polynomial $f \in k[x_0, x_1, \ldots, x_n]$ induces a map $M(-d) \to M$ that preserves grading, in the sense that any homogeneous element $x \in M(-d)_m$ is sent to a homogeneous element of the same degree $fx \in M_m$.

Going back to our inductive step, consider the map $M \xrightarrow{x_n} M$ given by multiplication by $x_n$. Let $K \subset M$ be the kernel of this map. We obtain an exact sequence

$$0 \to K(-1) \hookrightarrow M(-1) \xrightarrow{x_n} M \twoheadrightarrow M/x_nM \to 0,$$

where the twists are taken so that each map in the exact sequence preserves degrees. That is, for any integer $m$, we can restrict the sequence above to the $m^{th}$ graded piece of each module and obtain the following exact sequence of vector spaces over $k$:

$$0 \to K(-1)_m \hookrightarrow M(-1)_m \xrightarrow{x_n} M_m \twoheadrightarrow (M/x_nM)_m \to 0.$$

We now recall from linear algebra that vector space dimensions are additive (with sign) in an exact sequence. That is, if $V_1, V_2, \ldots, V_r$ are vector spaces over a field $k$ that fit into an exact sequence

$$0 \to V_1 \to V_2 \to \cdots \to V_r \to 0,$$

then their dimensions must satisfy the following relation:

$$\sum_{i=1}^r (-1)^i \cdot \dim_k V_i = 0.$$

Returning to our inductive step, we thus have that

$$\dim_k K(-1)_m - \dim_k M(-1)_m + \dim_k M_m - \dim_k (M/x_nM)_m = 0.$$

Recalling how we defined the grading of a twist above, we can rewrite this relation as

$$\dim_k K_{m-1} - \dim_k M_{m-1} + \dim_k M_m - \dim_k (M/x_nM)_m = 0.$$
In the language of Hilbert functions, we have that
\[ h_M(m) - h_M(m - 1) = h_{M/x_nM}(m) - h_K(m - 1). \]

Note that \( M/x_nM \) and \( K \) are finitely generated graded modules over \( k[x_0, \ldots, x_{n-1}] \). Indeed, they inherit a grading from \( M \). Then, \( M \) is a finitely generated module over the Noetherian ring \( k[x_0, \ldots, x_n] \), so it is a Noetherian module, so every submodule of \( M \) is finitely generated. This means that \( K \subset M \) is a finitely generated module over \( k[x_0, \ldots, x_{n-1}] \) (because \( K \) is the kernel of \( M \overset{x_n}{\to} M \), so multiplication by \( x_n \) gives 0 on \( K \)). Similarly, \( M/x_nM \) is generated over \( k[x_0, \ldots, x_{n-1}] \) by the finitely many generators of \( M \) and, in fact, these generators also generate \( M/x_nM \) over \( k[x_0, \ldots, x_n] \) (because multiplication by \( x_n \) gives 0 on \( M/x_nM \)).

Therefore, we can use our inductive hypothesis to say that the Hilbert functions \( h_K(m) \) and \( h_{M/x_nM}(m) \) agree, for large enough \( m \), to polynomials of degree at most \( n - 1 \). This means that \( h_M(m) - h_M(m - 1) \) agree, for large enough \( m \), to a polynomial of degree at most \( n - 1 \). Then, Lemma 4.1 from just below proves that \( h_M(m) \) agrees, for large enough values of \( m \), to a polynomial \( p_M(m) \in \mathbb{Q}[m] \) of degree at most \( n \), as desired. \qed

**Lemma 4.1.** Let \( h : \mathbb{Z} \to \mathbb{Z} \). If there exists an integer \( m_0 \) such that \( h(m) - h(m - 1) \) agrees with a polynomial \( q(m) \in \mathbb{Q}[m] \) for all \( m \geq m_0 \), then \( h(m) \) agrees with a polynomial \( p(m) \in \mathbb{Q}[m] \) for all \( m \geq m_0 \), and \( \deg p = \deg q + 1 \).

**Proof.** To prove this, we follow the proof of Lemma 1.12 and the suggested Exercise 1.21 from [Eis04]. We define the function \( p : \mathbb{Z} \to \mathbb{Z} \) to be given by
\[
p(m) = \begin{cases} h(m) & \text{if } m \geq m_0 \\
h(m_0) - \sum_{i=m+1}^{m_0} q(i) & \text{if } m < m_0 \end{cases}
\]
and we note that \( q(m) = p(m) - p(m - 1) \) for all integers \( m \). Thus, for all \( m \in \mathbb{Z}_{\geq 0} \), we have that \( p(m) = p(0) + \sum_{i=1}^{m} q(i) \).

Since \( p(0) \) is a constant, we want to prove that \( \sum_{i=1}^{m} q(i) \) is a polynomial in \( \mathbb{Q}[m] \) of degree \( \deg q + 1 \). Because \( q(m) \) is a rational polynomial that takes integer values on sufficiently large integers, which is a consequence of the fact that \( h(m) \) is an integer-valued function and \( q(m) = h(m) - h(m - 1) \) for all integers \( m \geq m_0 \), then it is a well-known fact that \( q(m) \) can
be written uniquely as a $\mathbb{Z}$-linear combination of the binomial functions

$$b_k(m) := \binom{m}{k} = \frac{m(m-1)\cdots(m-k+1)}{k!},$$

for integers $k$ with $0 \leq k \leq \deg q$. Therefore, it suffices to show that $\sum_{i=1}^{m} b_k(i)$ is a polynomial in $\mathbb{Q}[m]$ of degree $\deg b_k + 1 = k + 1$, for any $0 \leq k \leq \deg q$. For $k = 0$, this follows immediately because $\sum_{i=1}^{m} b_k(i) = m$. For $k \geq 1$, this follows from the combinatorial hockey-stick identity:

$$\sum_{i=1}^{m} b_k(i) = \sum_{i=1}^{m} \binom{i}{k} = \binom{m+1}{k+1},$$

which is a degree $k+1$ rational polynomial in $m$. Therefore, we proved that $p(m)$ is a rational polynomial in $m$ with $\deg q + 1$. And, by our initial definition of $p$, it agrees with $h(m)$ on all integers $m \geq m_0$. $\square$

**Remark 4.1.** It is clear that the Hilbert polynomial associated to a module $M$ is well-defined because the polynomial $p_M(m)$ satisfying the conditions of Proposition 4.1 must be unique. Indeed, if $p_M(m), p'_M(m) \in \mathbb{Q}[m]$ are distinct polynomials, then one of them grows faster as $m \to \infty$, so they cannot both agree with a fixed Hilbert function $h_M(m)$ on all (large enough values of) $m$.

**Remark 4.2.** This definition of the Hilbert polynomial extends naturally to closed subschemes $X \subset \mathbb{P}^n$. In particular, for each such subscheme $X$, there exists a homogeneous ideal $I(X) \subset k[x_0, x_1, \ldots, x_n]$ that determines the ideal sheaf of $X$: $\mathcal{I}(X) = \mathcal{I}_X$. For example, see [EH00] for an explicit construction. Then, we define the **homogeneous coordinate ring** of $X$ to be

$$S(X) := k[x_0, x_1, \ldots, x_n]/I(X),$$

which is clearly a finitely generated graded module over $k[x_0, x_1, \ldots, x_n]$. Finally, the Hilbert function $h_X(m)$ and polynomial $p_X(m)$ associated to the scheme $X$ are defined to be the Hilbert function and corresponding polynomial associated to the coordinate ring $S(X)$, as described above.

**Example 7.** Let’s take the base field to be $k = \mathbb{C}$ and let’s compute the Hilbert polynomial associated to the twisted cubic curve $C \subset \mathbb{P}^3$. Recall that the twisted cubic is defined as the vanishing locus of the homogeneous ideal

$$I := (x_0x_2 - x_1^2, x_1x_3 - x_2^2, x_0x_3 - x_1x_2) \subset k[x_0, x_1, x_2, x_3].$$
Consider the hyperplane section $D : C \cap V(x_3)$ of the twisted cubic. Note that $D$ equals the vanishing locus of the homogeneous ideal $J := (I, x_3) = (x_3, x_0x_2 - x_1^2, x_2^2, x_1x_2) \subset k[x_0, x_1, x_2, x_3]$, so the coordinate ring of $D$ equals $S(D) = k[x_0, x_1, x_2]/J \cong k[x_0, x_1, x_2]/(x_0x_2 - x_1^2, x_2^2, x_1x_2)$.

Thus, the Hilbert polynomial associated to our hyperplane section $D$ is the constant polynomial $h_D(m) = 3$. This follows because, for each positive integer $m$, the $m$th graded piece $S(D)_m$ is generated as a $k$-vector space by the monomials $x_0^\alpha x_1^\beta x_2^\gamma$ for $\alpha + \beta + \gamma = m$. However, note that such a monomial is equal mod $J$ to

$$x_0^\alpha x_1^\beta x_2^\gamma = \begin{cases} 0 & \text{if } \gamma \geq 2 \text{ or } \beta, \gamma \geq 1 \\ x_0^{\alpha+1}x_1^{\beta-2}x_2^{\gamma+1} & \text{if } \beta \geq 2 \end{cases},$$

so $S(D)_m$ is in fact generated by the three monomials $x_0^m, x_0^{m-1}x_1,$ and $x_0^{m-1}x_2$.

Finally, note that multiplication by $x_3$ is injective on the coordinate ring $S(C) = k[x_0, x_1, x_2, x_3]/I$, so we have a short exact sequence

$$0 \to S(C)(-1) \xrightarrow{x_3} S(C) \to S(D) \to 0,$$

where the $-1$ twist is taken so that all the maps in the exact sequence preserve degrees. For every positive integer $m$, we can restrict the short exact sequence above to the $m$th graded piece of each space (similarly to how we proceeded in the proof of Proposition 4.1) and obtain that

$$h_C(m) = h_C(m - 1) + h_D(m) = h_C(m - 1) + 3.$$

All we have to do is note that $h_C(0) = \dim_k S(C)_0 = \dim_k k = 1$, and so a quick induction tells us that $h_C(m) = 3m + 1$ for all non-negative integers $m$. As the Hilbert function $h_C(m)$ that we computed for $m \geq 0$ is already in polynomial form, the Hilbert polynomial associated to the twisted cubic must be the same:

$$p_C(m) = h_C(m) = 3m + 1.$$
Remark 4.3. Since the twisted cubic in the example above has degree 3 and genus 0, this small example agrees with the more general computation of Hilbert polynomials of curves that we carry out later, in section 5.

4.2. Hilbert Polynomials through Gröbner Bases. The method above for proving the existence of Hilbert polynomials is the one usually used, and is going to help us later in the exposition. However, there is also a rather neat way of proving the existence of Hilbert polynomials using Gröbner bases. We take some time to present this approach here, following a proposition and a suggested exercise from [Gun22].

Proposition 4.2. Let $X \subset \mathbb{P}^n$ be a subscheme and $I := I(X) \subset k[x_0, x_1, \ldots, x_n]$ its corresponding ideal. The set of monomials $M := \{M \in k[x_0, x_1, \ldots, x_n] \mid M \notin LM(I)\}$ form a basis for the coordinate ring $S(X)$ of $X$, seen as a vector space over $k$.

Proof. First, we want to show that each element of $S(X)$ can be generated by monomials in $M$. Consider thus any polynomial $f \in k[x_0, x_1, \ldots, x_n]$ and take $r \in k[x_0, \ldots, x_n]$ to be a reduction of $f$ with respect to the ideal $I$. By Remark 2.6, we know that $f \equiv r \mod I$, so $f$ and $r$ represent the same equivalence class in the quotient $S(X)$. Then, since $r$ is reduced with respect to $I$, it must be a $k$-linear combination of monomials not in $LM(I)$, i.e. a $k$-linear combination of elements of $M$.

Then, we also want to show that the monomials in $M$ are linearly independent. Consider any non-trivial $k$-linear combination of elements in $M$:

$$f := \sum_{i=1}^{s} c_i \cdot M_i,$$

where each $c_i \in k \setminus \{0\}$ and $M_i \in M$ are distinct monomials. Since the monomials appearing in $f$ are distinct and appear with constant coefficients, they cannot cancel each other, so

$$LM(f) = \max \{ M_i \mid 1 \leq i \leq s \}.$$

In particular, this means that $LM(f) \in M$, so $LM(f) \notin LM(I)$, so $f \notin I$. Therefore, $f \neq 0$ in $S(X)$, proving that non-trivial $k$-linear combination of elements in $M$ are non-zero. □

Remark 4.4. Assume the same setting as in the previous proposition. If $h : \mathbb{Z} \to \mathbb{Z}$ is the Hilbert function associated to $S(X)$, then for any positive integer $m$, $h(m)$ equals the number
of monomials in $\mathcal{M}$ that have degree $m$. If we pick a Gröbner basis $G = \{g_1, g_2, \ldots, g_s\}$ for $I$, then $\text{LM}(I) = \langle \text{LM}(G) \rangle$, so $h(m)$ equivalently equals the number of monomials of degree $m$ that are not divisible by $\text{LM}(g_i)$, for any $g_i \in G$. We know that the total number of monomials in $k[x_0, x_1, \ldots, x_n]$ that have degree $m$ equals $\binom{m+n}{m}$, by a simple stars and bars argument. Therefore,

$$h(m) = \binom{m+n}{m} - \# \{ M : \deg(M) = m \text{ and } \exists g \in G \text{ such that } \text{LM}(g) \mid M \}.$$ 

Now, given any polynomial $g \in k[x_0, \ldots, x_n]$, the number of monomials in $k[x_0, \ldots, x_n]$ of degree $m \geq \deg(g)$ that are divisible by $\text{LM}(g)$ is

$$\binom{m - \deg(g) + n}{m - \deg(g)} \quad (*)$$

again by a stars and bars argument.

Finally, for every tuple $i_1, i_2, \ldots, i_r$, we denote

$$g_{i_1i_2\cdots i_r} := \text{LCM}(\text{LM}(g_{i_1}), \text{LM}(g_{i_2}), \ldots, \text{LM}(g_{i_r}))$$

and we denote by $\mathcal{M}_{m,i_1i_2\cdots i_r}$ the set of monomials of $k[x_0, \ldots, x_n]$ that have degree $m$ and that are divisible by $g_{i_1i_2\cdots i_r}$. The inclusion and exclusion principle then tells us that our Hilbert function is given by

$$h(m) = \binom{m+n}{m} - \sum_{i=1}^{s} |\mathcal{M}_{m,i}| - \sum_{1 \leq i < j \leq s} |\mathcal{M}_{m,ij}| - \cdots + (-1)^s |\mathcal{M}_{m,12\cdots s}|.$$

For $m \geq \deg(g_{12\cdots s})$, this function equals the polynomial obtained by replacing each cardinality $|\mathcal{M}_{m,i_1i_2\cdots i_r}|$ by the appropriate binomial function, according to $(*)$, thus proving the existence of the Hilbert polynomial.

**Remark 4.5.** The method described in the previous remark also offers a way of computing the Hilbert polynomial of a subscheme $X$. More precisely, to compute $p_X(m)$, one can use Buchberger’s algorithm to find a Gröbner basis $G$ for $I(X)$ and then look at the degrees of elements $g \in G$ and the degrees of their least common multiples to write down the binomial functions that make up $p_X(m)$.

**4.3. Cohomological Definition.** A second way in which one can define the Hilbert polynomial associated to a subscheme $X \subset \mathbb{P}^n$ is via the Euler characteristic of the structure
sheaf $\mathcal{O}_X$ of $X$. We make this precise and explain why our two definitions are equivalent, following the results and suggested exercises from chapter III.5 in [Har77].

**Definition 4.2.** Let $X$ be a projective scheme over a field $k$ and $\mathcal{F}$ a coherent sheaf on $X$. We define the **Euler characteristic** of $\mathcal{F}$ to be

$$
\chi(\mathcal{F}) := \sum_{i \geq 0} (-1)^i \dim_k H^i(X, \mathcal{F}),
$$

where the right-hand side refers to the dimension of the $i^{th}$ sheaf cohomology group, seen as a vector space over $k$.

**Remark 4.6.** The Euler characteristic described above is a well-defined finite number, and we explain here why this is the case. According to a vanishing theorem due to Grothendieck (Theorem III.2.7 in [Har77]), if $X$ is a Noetherian topological space of dimension $\dim X$, then the cohomology group $H^i(X, \mathcal{F})$ is 0 for any $i > \dim X$ and any sheaf $\mathcal{F}$ of abelian groups on $X$. This result shows that we can rewrite our definition of the Euler characteristic as

$$
\chi(\mathcal{F}) = \sum_{i=0}^{\dim X} (-1)^i \dim_k H^i(X, \mathcal{F}).
$$

Moreover, a vanishing theorem due to Serre (Theorem III.5.2 in [Har77]) states that, if $X$ is a projective scheme over a Noetherian ring $A$ and $\mathcal{F}$ any coherent sheaf on $X$, then $H^i(X, \mathcal{F})$ is a finitely-generated $A$-module. In the setting of our definition, this result shows that each $H^i(X, \mathcal{F})$ is a finite dimensional vector space over $k$, so $\chi(\mathcal{F})$ is indeed finite.

**Notation.** We will use $h^i(X, \mathcal{F})$ to denote $\dim_k H^i(X, \mathcal{F})$.

A useful result about the Euler characteristic of sheaves is that it is compatible with short exact sequences of coherent sheaves in the following sense:

**Lemma 4.2.** If $X$ is a projective scheme over a field $k$ and $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ are coherent sheaves over $X$ satisfying the short exact sequence

$$
0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0,
$$

then the Euler characteristics of the three sheaves must satisfy

$$
\chi(\mathcal{F}_2) = \chi(\mathcal{F}_1) + \chi(\mathcal{F}_3).
$$
Proof. The given short exact sequence of sheaves induces a long exact sequence of vector spaces over \(k\) on the cohomology groups:

\[
0 \to H^0(X, \mathcal{F}_1) \to \cdots \to H^i(X, \mathcal{F}_1) \to H^i(X, \mathcal{F}_2) \to H^i(X, \mathcal{F}_3) \to H^{i+1}(X, \mathcal{F}_1) \to \cdots.
\]

Note that this exact sequence terminates eventually because each \(\mathcal{F}_j\) has only finitely many non-zero cohomology groups (according to the Grothendieck vanishing theorem mentioned earlier). Then, because vector space dimensions are additive (with sign) in a long exact sequence, we get that

\[
\sum_{i \geq 0} (-1)^i \cdot (h^i(X, \mathcal{F}_1) - h^i(X, \mathcal{F}_2) + h^i(X, \mathcal{F}_3)) = 0.
\]

Moving the \(\mathcal{F}_2\) cohomology groups to the other side of this equality, we get that

\[
\sum_{i \geq 0} (-1)^i \cdot h^i(X, \mathcal{F}_2) = \sum_{i \geq 0} (-1)^i \cdot h^i(X, \mathcal{F}_1) + \sum_{i \geq 0} (-1)^i \cdot h^i(X, \mathcal{F}_3),
\]

which is precisely the equality that we wanted to prove. \(\Box\)

Remark 4.7. The result of the lemma above can be extended to arbitrary (finite) numbers of sheaves. Indeed, if \(X\) is a projective scheme over \(k\) and \(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_r\) are coherent sheaves over \(X\) (for some integer \(r \geq 3\)) satisfying the exact sequence

\[
0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \cdots \to \mathcal{F}_r \to 0,
\]

then the lemma and induction on \(r\) prove that

\[
\sum_{i=1}^{r} (-1)^i \cdot \chi(\mathcal{F}_i) = 0.
\]

We are now ready to define the Hilbert polynomial associated to a coherent sheaf \(\mathcal{F}\) on a projective scheme \(X\), and explain that this is the same as the Hilbert polynomial defined previously when \(\mathcal{F}\) is the structure sheaf of \(X\). We make this precise by stating and proving Exercise III.5.2 in [Har77].

Proposition 4.3. Let \(k\) be a field and \(X\) a projective scheme over \(k\). Let \(\mathcal{F}\) be a coherent sheaf on \(X\) and \(\mathcal{O}_X(1)\) a very ample invertible sheaf on \(X\) over \(k\). Define a function \(p : \mathbb{Z} \to \mathbb{Z}\) by taking

\[
p(m) = \chi(\mathcal{F}(m)).
\]
The function \( p(m) \) agrees with a rational polynomial in \( \mathbb{Q}[m] \) for all integer values of \( m \).

This polynomial is called the **Hilbert polynomial** associated to \( \mathcal{F} \), with respect to the very ample invertible sheaf \( \mathcal{O}_X(1) \).

**Proof.** We proceed via induction on the dimension of the support of \( \mathcal{F} \). For the base case, let’s assume that \( \mathcal{F} \) is supported on a point \( p \in X \). Consider the inclusion \( j : \{p\} \hookrightarrow X \) and the sheaf of abelian groups \( \mathcal{G} \) on \( \{p\} \) with global sections \( \mathcal{G}(\{p\}) = \mathcal{F}_p \). Then, if we take the sheaf \( j_* \mathcal{G} \) on \( X \) to be the extension of \( \mathcal{G} \) by zero outside \( \{p\} \), we have \( H^i(\{p\}, \mathcal{G}) = H^i(X, j_* \mathcal{G}) \). (The proof that a sheaf and its extension by zero under an inclusion of a closed subset have the same cohomology can be found in [Har77].) Moreover, we have that \( \mathcal{F} \cong j_* \mathcal{G} \) via the isomorphism defined by: for every \( V \subseteq X \) open, the map \( \mathcal{F}(V) \to (j_* \mathcal{G})(V) \) sends each element \( v \in \mathcal{F}(V) \) to its germ in \( \mathcal{F}_p \). Therefore, we get that

\[
H^i(X, \mathcal{F}) = H^i(\{p\}, \mathcal{G}) = \begin{cases} \mathcal{F}_p & \text{if } i = 0 \\ 0 & \text{otherwise} \end{cases},
\]

which means that \( \chi(\mathcal{F}) = \dim_k \mathcal{F}_p \). Then, for \( \mathcal{F}(m) \) we must have

\[
H^i(X, \mathcal{F}(m)) = H^i(X, (j_* \mathcal{G})(m)) = H^i(X, j_* (\mathcal{G}(m))) = H^i(\{p\}, \mathcal{G}(m))
\]

and we have that

\[
H^i(\{p\}, \mathcal{G}(m)) = \begin{cases} \mathcal{F}_p \otimes \mathcal{O}(m)(\{p\}) \cong \mathcal{F}_p & \text{if } i = 0 \\ 0 & \text{otherwise} \end{cases},
\]

which means that \( \chi(\mathcal{F}(m)) = \dim_k \mathcal{F}_p \) as well. Therefore, \( p(m) \) is the constant \( \dim_k \mathcal{F}_p \) polynomial, proving our base case.

For the inductive step, let’s assume that the statement of our proposition holds for all sheaves \( \mathcal{F} \) with \( r \)-dimensional support, and let’s prove that the statement must hold for a sheaf \( \mathcal{F} \) with \( (r+1) \)-dimensional support. That is, we can pick coordinates such that \( \text{supp} \mathcal{F} \) is contained in \( \mathbb{P}^{r+1} \) (the space where only the first \( r+2 \) coordinates are potentially non-zero), but is not contained in \( \mathbb{P}^r \) (where only the first \( r+1 \) coordinates are potentially non-zero).

Then, we consider the map \( \mathcal{F} \xrightarrow{x_{r+1}} \mathcal{F}(1) \cong \mathcal{F} \otimes \mathcal{O}_X \mathcal{O}_X(1) \) given by multiplication by \( x_{r+1} \), which is a section of \( \mathcal{O}_X(1) \). We can let \( \mathcal{R} \) and \( \mathcal{L} \) be the kernel and, respectively, cokernel...
of this map, so we get the following exact sequence of sheaves:

\[ 0 \to R \to \mathcal{F} \xrightarrow{x_{r+1}} \mathcal{F}(1) \to L \to 0. \]

Because multiplication by \( x_{r+1} \) is an isomorphism away from the hyperplane \( V(x_{r+1}) \), the support of the sheaves \( R \) and \( L \) is contained in \( \mathbb{P}^{r+1} \cap V(x_{r+1}) \cong \mathbb{P}^r \), so the inductive hypothesis applies to them. Finally, we can tensor the exact sequence above by \( \mathcal{O}_X(m) \) and get the exact sequence

\[ 0 \to R(m) \to \mathcal{F}(m) \to \mathcal{F}(m+1) \to L(m) \to 0. \]

Taking the Euler characteristic in this exact sequence gives us

\[ \chi(\mathcal{F}(m+1)) - \chi(\mathcal{F}(m)) = \chi(L(m)) - \chi(R(m)). \]

The right-hand side agrees with a polynomial by our inductive hypothesis, so Lemma 4.1 proves that \( \chi(\mathcal{F}(m)) \) also agrees with a rational polynomial for all integers \( m \). \( \square \)

We now want to show that the Hilbert polynomial associated to the structure sheaf \( \mathcal{O}_X \) agrees with the Hilbert polynomial associated to the coordinate ring \( S(X) \) of \( X \) that we discussed in subsection 4.1. For this, we state the following vanishing theorem due to Serre (Theorem III.5.2 in [Har77]):

**Theorem 8.** Let \( X \) be a projective scheme over a Noetherian ring \( A \), \( \mathcal{F} \) a coherent sheaf on \( X \), and \( \mathcal{O}_X(1) \) a very ample invertible sheaf on \( X \). Then, there exists an integer \( m_0 \) depending on \( \mathcal{F} \) such that \( H^i(X, \mathcal{F}(m)) = 0 \) for all positive integers \( i \) and for all integers \( m \geq m_0 \).

**Remark 4.8.** This theorem implies that, for large enough values of \( m \), the Hilbert polynomial associated to \( \mathcal{O}_X \) is given by:

\[ p(m) = \chi(\mathcal{O}_X(m)) = h^0(X, \mathcal{O}_X(m)). \]

The cohomology group \( H^0(X, \mathcal{O}_X(m)) \) can be identified with the space of global sections of \( \mathcal{O}_X(m) \) which, by the definition of the structure sheaf, are given precisely by \( S(X)_m \). Therefore, on large enough values of \( m \), the Hilbert polynomial associated to \( \mathcal{O}_X \) agrees with the Hilbert polynomial associated to the coordinate ring \( S(X) \), so the two polynomials must be the same, as desired.
Example 9. Let’s take \( X \subset \mathbb{P}^n \) to be a degree \( d \) hypersurface and let’s compute the Hilbert polynomial \( p(m) \) associates to its structure sheaf \( \mathcal{O}_X \). Let \( f \in k[x_0, x_1, \ldots, x_n] \) be the degree \( d \) polynomial defining \( X \). This means that multiplication by \( f \) gives an isomorphism \( \mathcal{O}_{\mathbb{P}^n}(-d) \cong \mathcal{I}_X \), where \( \mathcal{I}_X \subset \mathcal{O}_{\mathbb{P}^n} \) denotes the ideal sheaf of \( X \). Moreover, we know that this ideal sheaf \( \mathcal{I}_X \) fits into the following short exact sequence of sheaves:

\[
0 \to \mathcal{I}_X \to \mathcal{O}_{\mathbb{P}^n} \to \mathcal{O}_{\mathbb{P}^n}/\mathcal{I}_X \to 0,
\]

where \( \mathcal{O}_{\mathbb{P}^n}/\mathcal{I}_X \) is just (the extension by zero of) the structure sheaf \( \mathcal{O}_X \). Therefore, for any integer \( m \), we can tensor this exact sequence by \( \mathcal{O}_{\mathbb{P}^n}(m) \) and get the exact sequence

\[
0 \to \mathcal{O}_{\mathbb{P}^n}(m-d) \to \mathcal{O}_{\mathbb{P}^n}(m) \to \mathcal{O}_X(m) \to 0.
\]

Taking the Euler characteristic in this sequence, we get that

\[
\chi(\mathcal{O}_X(m)) = \chi(\mathcal{O}_{\mathbb{P}^n}(m)) - \chi(\mathcal{O}_{\mathbb{P}^n}(m-d)).
\]

Using Theorem 8, we get that for large enough \( m \) the right-hand side equals:

\[
h^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(m)) - h^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(m-d)).
\]

To compute this expression, we recall the following result stated and proven in chapter III.5 of [Har77]:

**Theorem 10.** The polynomial ring \( k[x_0, x_1, \ldots, x_n] \) is isomorphic, as graded \( k \)-module, to

\[
\bigoplus_{r \in \mathbb{Z}} H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(r)).
\]

This means that, for any integer \( r \), we have that \( H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(r)) \) is generated by the degree \( r \) monomials of \( k[x_0, x_1, \ldots, x_n] \). In particular, a simple stars and bars argument shows that

\[
h^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(r)) = \binom{n+r}{r}.
\]

Therefore, for large enough \( m \), we have that

\[
\chi(\mathcal{O}_X(m)) = \binom{n+m}{m} - \binom{n+m-d}{m-d},
\]

which is a polynomial of degree \( n - 1 \) in \( m \), and so this must be the Hilbert polynomial \( p(m) \) that we are looking for.
5. AN EXAMPLE: THE HILBERT POLYNOMIAL OF A CURVE

In this section, we show that the Hilbert polynomial of a smooth projective algebraic curve of degree \( d \) and genus \( g \) is \( h(m) = dm - g + 1 \). This requires us to first introduce Weil divisors. Also, in this section, we assume we are working over the field \( k = \mathbb{C} \).

5.1. Divisors. We introduce divisors and their associated invertible sheaves. I am mostly following my lecture notes from [Har21], as well as [Kar20] for their discussion of divisors associated to higher dimensional varieties.

**Definition 5.1.** Let \( C \) be a smooth projective algebraic curve. A (Weil) divisor \( D \) on \( C \) is a formal \( \mathbb{Z} \)-linear combination of points of the curve:

\[
D = \sum_{\alpha} m_{\alpha} \cdot p_{\alpha},
\]

with each \( m_{\alpha} \in \mathbb{Z} \) and \( p_{\alpha} \in C \). Equivalently, we can write

\[
D = \sum_{p \in C} m_{p} \cdot p,
\]

where the coefficients \( m_{p} \) are integers and all but finitely many of them equal 0. The degree of such a divisor \( D \) is defined to be the sum of these integer coefficients:

\[
\deg(D) = \sum_{p \in C} m_{p}.
\]

*Notation.* The formal linear combinations described above form an abelian group under formal addition, which we denote by \( \text{Div}(C) \).

**Definition 5.2.** Given a smooth projective algebraic curve \( C \) and a rational function \( f : C \to \mathbb{C} \), we define the divisor associated to \( f \) to be

\[
(f) := \sum_{p \in C} \text{ord}_{p}(f) \cdot p,
\]

where \( \text{ord}_{p}(f) \) is the vanishing order of \( f \) at \( p \) – this means that \( \text{ord}_{p}(f) > 0 \) if and only if \( p \) is a zero of \( f \) and \( \text{ord}_{p}(f) < 0 \) if and only if \( p \) is a pole of \( f \). Here, the vanishing order \( \text{ord}_{p} \) is defined to be the valuation of the local ring \( \mathcal{O}_{C,p} \), which is a discrete valuation ring whose fraction field is the field \( K(C) \) of rational functions on \( C \).

These divisors of the form \( (f) \) that arise from rational functions \( f \) on \( C \) are called principal divisors.
Definition 5.3. Given a smooth projective algebraic curve $C$ and two divisors $D, D' \in \text{Div}(C)$, we say that $D$ and $D'$ are **linearly equivalent** if their difference is a principal divisor:

$$D - D' = (f),$$

for some rational function $f : C \to \mathbb{C}$.

*Notation.* It is often convenient to consider divisors on a curve $C$ up to linear equivalence, which also form a group called the **Divisor Class Group**. We denote this group of equivalence classes of divisors on $C$ by $\text{Cl}(C) := \text{Div}(C)/\sim$.

Definition 5.4. Let $C$ be a curve like before and $D = \sum m_\alpha \cdot p_\alpha$ a divisor on $C$. We define the **associated sheaf** of $D$ to be the sheaf $\mathcal{O}_C(D)$ on $C$ defined as follows: for every open subset $U \subseteq C$, take

$$\mathcal{O}_C(D)(U) := \{ f \in K(C) \mid \text{ord}_{p_\alpha}(f) \geq -m_\alpha \text{ for all } p_\alpha \in U \},$$

where $K(C)$ denotes the set of rational functions on $C$.

Remark 5.1. Sheaves associated to divisors behave well under tensoring, in the sense that

$$\mathcal{O}_C(D) \otimes_{\mathcal{O}_C} \mathcal{O}_C(D') \cong \mathcal{O}_C(D + D') \quad \text{via} \quad f \otimes g \mapsto fg.$$

In particular, the relation above shows that each $\mathcal{O}_C(D)$ is an invertible sheaf on $C$ since we have that $\mathcal{O}_C(D) \otimes \mathcal{O}_C(-D) \cong \mathcal{O}_C(0) = \mathcal{O}_C$, the sheaf of regular functions of $C$.

*Notation.* Given a curve $C$ as before, we define the **Picard group** of $C$ to be the group of isomorphism classes of invertible sheaves on $C$. We denote this group by $\text{Pic}(C)$.

Remark 5.2. Given a projective algebraic curve $C$ and two divisors $D, D' \in \text{Div}(C)$, it turns out that $D$ and $D'$ are linearly equivalent if and only if their associated invertible sheaves are isomorphic. Given this and the result of Remark 5.1, we see that the association $D \mapsto \mathcal{O}_C(D)$ induces a group isomorphism $\text{Cl}(C) \to \text{Pic}(C)$.

In fact, the definitions in these section can be extended to smooth projective varieties $X$ of higher dimension, as follows. A divisor $D$ on $X$ becomes a formal $\mathbb{Z}$-linear combination $\sum m_Y \cdot Y$ of codimension 1 irreducible closed subsets $Y \subset X$ and its associated invertible sheaf $\mathcal{O}_X(D)$ is defined by taking $\mathcal{O}_X(D)(U)$ to be the rational functions on $X$ whose vanishing order along $Y$ is at least $-m_Y$ (where here the vanishing order is defined by taking
the generic point $\eta \in Y$ and looking at the valuation of $O_{X, \eta}$ at $f$). We say that two divisors $D, D'$ on $X$ are linearly equivalent if their difference is the divisor generated by a rational function on $X$. As before, the association $D \mapsto O_{X}(D)$ gives an isomorphism of the group $\text{Cl}(X)$ of equivalence classes of divisors on $X$ and the group $\text{Pic}(X)$ of isomorphism classes of invertible sheaves on $X$.

**Example 11.** We take $X = \mathbb{P}^n$ and describe $\text{Cl}(\mathbb{P}^n) \cong \text{Pic}(\mathbb{P}^n)$, following a similar example in section 4 of [Mat10]. First of all, note that any two hyperplanes $H_1, H_2 \subset \mathbb{P}^n$ give rise to linearly equivalent divisors $H_1 \sim H_2$; indeed, this follows because, if $H_1 = V(f_1)$ and $H_2 = V(f_2)$ for some degree 1 homogeneous polynomials $f_1, f_2 \in \mathbb{C}[x_0, x_1, \ldots, x_n]$, then

$$H_1 - H_2 = \left(\frac{f_1}{f_2}\right),$$

where $\frac{f_1}{f_2}$ is a rational function on $\mathbb{P}^n$, being just a ratio of two degree 1 homogeneous polynomials. Therefore, we can talk about the hyperplane class $[H] \in \text{Cl}(\mathbb{P}^n)$.

Then, we have that $\text{Cl}(\mathbb{P}^n) \cong \mathbb{Z}$ and, moreover, $\text{Cl}(\mathbb{P}^n)$ is generated by the hyperplane class $[H]$. Indeed, let $S_1 = V(g_1)$ and $S_2 = V(g_2)$ be any two hypersurfaces in $\mathbb{P}^n$ defined by the homogeneous degree $d_1$ and, respectively, $d_2$ polynomials $g_1, g_2 \in \mathbb{C}[x_0, x_1, \ldots, x_n]$. If $e_1d_1 = e_2d_2$ for some integers $e_1, e_2$, then we have a linear equivalence $e_1H_1 \sim e_2H_2$ because

$$e_1H_1 - e_2H_2 = \left(\frac{g_1^{e_1}}{g_2^{e_2}}\right).$$

Therefore, the hyperplane class generates $\text{Cl}(\mathbb{P}^n)$ since every hyperplane has degree 1. Moreover, $\text{Cl}(\mathbb{P}^n) \cong \mathbb{Z}$ because the hyperplane class has infinite order; indeed, if $H \subset \mathbb{P}^n$ is any hyperplane, we cannot have $nH \sim 0$ or, equivalently, $nH = (f)$ for some rational function $f$, because $f$ is the ratio of two homogeneous polynomials of the same degree, and thus gives rise to a divisor of degree 0.

Finally, under the isomorphism $\text{Cl}(\mathbb{P}^n) \cong \text{Pic}(\mathbb{P}^n)$ described earlier, the hyperplane class $[H]$ corresponds to the twisting sheaf $O_{\mathbb{P}^n}(1)$, which is a generator $\text{Pic}(\mathbb{P}^n)$.

Our example above shows that, if $H \subset \mathbb{P}^n$ is a hyperplane, then $O_{\mathbb{P}^n}(H) \cong O_{\mathbb{P}^n}(1)$. Below, we show how this results extends to hyperplane sections of curves.

**Proposition 5.1.** Let $C \subset \mathbb{P}^n$ be a smooth projective algebraic curve and $D \in \text{Div}(C)$ a hyperplane section of $C$ – that is, take $H$ to be a general hyperplane of $\mathbb{P}^n$ and define the
divisor $D$ to be given by the points of intersection in $H \cap C$. The sheaf $\mathcal{O}_C(D)$ associated to this hyperplane section is isomorphic to the twisting sheaf $\mathcal{O}_C(1)$. More generally, if $m$ is any integer, then the sheaf associated to the divisor $mD \in \text{Div}(C)$ is isomorphic to $\mathcal{O}_C(m)$.

Proof. First, we know that, for any effective divisor (i.e. a $\mathbb{Z}$-linear combinations using only non-negative coefficients) $D$ on some variety $X$, the sheaf $\mathcal{O}_X(-D)$ is isomorphic to the ideal sheaf $\mathcal{I}_D$ of $D$ (thought of as a subscheme of $X$). Therefore, we have the following short exact sequence of sheaves (described in section 5 of [Kar20]):

$$0 \to \mathcal{O}_X(-D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0.$$ 

Back to our proposition, consider the divisor $H$ on $\mathbb{P}^n$. We saw in Example 11 that $\mathcal{O}_{\mathbb{P}^n}(H) \cong \mathcal{O}_{\mathbb{P}^n}(1)$, so $\mathcal{O}_{\mathbb{P}^n}(-H) \cong \mathcal{O}_{\mathbb{P}^n}(-1)$ and we get the short exact sequence:

$$0 \to \mathcal{O}_{\mathbb{P}^n}(-1) \to \mathcal{O}_{\mathbb{P}^n} \to \mathcal{O}_H \to 0.$$ 

Then, we can tensor this exact sequence by $\mathcal{O}_C$ (which corresponds to restricting everything to $C$) and get

$$0 \to \mathcal{O}_C(-1) \to \mathcal{O}_C \to \mathcal{O}_{H\cap C} = \mathcal{O}_D \to 0.$$ 

Therefore, the ideal sheaf of the subscheme $D \subset C$ is isomorphic to $\mathcal{O}_C(-1)$, which means that $\mathcal{O}_C(-1) \cong \mathcal{O}_C(-D)$. Thus, the sheaf associated to the divisor $D$ is precisely the twisting sheaf $\mathcal{O}_C(1)$. Then, the sheaf associated to the divisor $mD$ must be isomorphic to $\mathcal{O}_C(1)^\otimes m \cong \mathcal{O}_C(m)$. □

5.2. The Hilbert Polynomial of a Curve. We are now ready to compute the Hilbert polynomial of a smooth projective algebraic curve. For this, we follow section IV.1 in [Har77].

**Theorem 12.** Let $C \subset \mathbb{P}^n$ be a smooth projective algebraic curve of genus $g$ and degree $d$. Then, its Hilbert polynomial is given by

$$h_C(m) = dm - g + 1.$$ 

Proof. We want to prove that, for any non-negative integer $m$

$$\chi(\mathcal{O}_C(m)) = dm - g + 1.$$ 

Equivalently, if $H \subset \mathbb{P}^n$ is a general hyperplane and $D := H \cap C$ is the corresponding hyperplane section of our curve, then $\deg(D) = \deg(C) = d$ and $\mathcal{O}_C(mD) \cong \mathcal{O}_C(m)$ according
to Proposition 5.1, so we want to prove that

$$\chi(\mathcal{O}_C(mD)) = \deg(mD) - g + 1.$$ 

In fact, we prove a slightly stronger result: if $D$ is any divisor on our curve $C$, then

$$\chi(\mathcal{O}_C(D)) = \deg(D) - g + 1. \quad (*)$$

We proceed via induction on the number of points appearing in $D$. For the base case, take $D = 0$. We want to prove that $\chi(\mathcal{O}_C) = -g + 1$, which follows just from the definition of the (arithmetic) genus of the curve $C$.

For the inductive step, we prove that the relation $(*)$ holds true for a divisor $D \in \text{Div}(C)$ if and only if it holds true for the divisor $D + p$, where $p$ is any point on our curve. Recalling the exact sequence of sheaves discussed in the proof of Proposition 5.1, we have:

$$0 \to \mathcal{O}_C(-p) \to \mathcal{O}_C \to \mathcal{O}_p \to 0.$$ 

We tensor this exact sequence by $\mathcal{O}_C(D + p)$. Note that

$$\mathcal{O}_p \otimes_{\mathcal{O}_C} \mathcal{O}_C(D + p) \cong \mathcal{O}_p$$

because (the extension by zero of) $\mathcal{O}_p$ is a skyscraper sheaf and $\mathcal{O}_C(D + p)$ is invertible, thus locally free of rank 1. We get the following exact sequence of sheaves:

$$0 \to \mathcal{O}_C(D) \to \mathcal{O}_C(D + p) \to \mathcal{O}_p \to 0.$$ 

Using the fact that $\chi(\mathcal{O}_p) = h^0(\{p\}, \mathcal{O}_p) = 1$ and the fact that the Euler characteristic is additive (with sign) in an exact sequence, we get that

$$\chi(\mathcal{O}_C(D + p)) = \chi(\mathcal{O}_C(D)) + \chi(\mathcal{O}_p) = \chi(\mathcal{O}_C(D)) + 1.$$ 

This proves our inductive step since $\deg(D + p) = \deg(D) + 1$. \hfill \qed

**Remark 5.3.** In the proof above, the only place where we used the fact that $C$ is embedded into $\mathbb{P}^n$ is when we considered its hyperplane section. In particular, our proof that $\chi(\mathcal{O}_C(D)) = \deg(D) - g + 1$ for any divisor $D \in \text{Div}(C)$ is true for any curve (not necessarily tied to an embedding).

32
5.3. **The Riemann-Roch Theorem.** While not strictly necessary to our discussion of the Hilbert polynomial and the Hilbert scheme, we mention here the famous Riemann-Roch theorem. The result of this theorem is used to compute the dimension of $H^0(C, \mathcal{O}_C(D))$ – that is, the dimension of rational functions on a smooth projective algebraic curve $C$ whose zeros and poles are no worse than the coefficients of the given divisor $D \in \text{Div}(C)$; alternatively, if we think of $C$ as a compact Riemann surface, this is the dimension of meromorphic functions on $C$ whose zeros and poles are again controlled by the coefficients of $D$. In fact, our proof of Theorem 12 was adapted from [Har77]'s proof of Riemann-Roch, which contains only one extra step in addition to our our discussion so far. We present this additional step below to complete the proof of Riemann-Roch.

**Notation.** Given a curve $C$ like before and a divisor $D$ on $C$, we let $l(D)$ denote $h^0(C, \mathcal{O}_C(D))$. Also, we let $K$ denote the divisor (i.e. one of the divisors in that linear equivalence class of divisors) on $C$ whose associated invertible sheaf $\mathcal{O}_C(K)$ is isomorphic to the canonical sheaf $\omega_C$ of relative differentials on $C$.

**Theorem 13** (Riemann-Roch). Let $C$ be a smooth projective algebraic curve. Given any divisor $D \in \text{Div}(C)$ and $K \in \text{Div}(C)$ the canonical divisor on $C$, then

$$l(D) - l(K - D) = \deg(D) - g + 1.$$  

**Proof.** The associated invertible sheaf of the canonical divisor $K \in \text{Div}(C)$ is the canonical sheaf $\omega_C$ on $C$, so the associated invertible sheaf of $K - D$ is $\omega_C \otimes \mathcal{O}_C(-D)$. Then, Serre duality (which is proven in [Har77]) shows that

$$H^0(C, \omega_C \otimes \mathcal{O}_C(-D)) \cong H^1(C, \mathcal{O}(D)).$$

We get that

$$l(D) - l(K - D) = h^0(C, \mathcal{O}(D)) - h^0(C, \omega_C \otimes \mathcal{O}_C(-D))$$

$$= h^0(C, \mathcal{O}(D)) - h^1(C, \mathcal{O}(D))$$

$$= \chi(\mathcal{O}_C(D)).$$

This reduces the Riemann-Roch theorem to the relation ($\ast$) that we showed holds true in the proof of Proposition 5.1.\qed
6. The Hilbert Scheme

After describing the Hilbert polynomial associated to a subscheme, we are now ready to define the Hilbert scheme. For its definition as a fine moduli space, we follow [Mac] and [Bel19]. We also discuss the construction of the Hilbert scheme as a subscheme of the Grassmannian, following [HM98] and [Str96].

**Definition 6.1** (Informal Definition). We want the Hilbert scheme $\mathcal{H}_{p,n}$ to parametrize all the closed subschemes $X \subset \mathbb{P}^n$ whose Hilbert polynomial equals $p \in \mathbb{Q}[m]$. The disjoint union $\mathcal{H}_n := \sqcup_p \mathcal{H}_{p,n}$ will then be a parameter space for all closed subschemes $X \subset \mathbb{P}^n$.

**Remark 6.1.** Before we sketch the construction of the Hilbert scheme $\mathcal{H}_{p,n}$, we remark that there could be multiple schemes parametrizing subschemes of the projective space – that is, schemes whose closed points are in bijection with closed subschemes of $\mathbb{P}^n$. Therefore, in order to have a well-defined Hilbert scheme, we need to impose an additional condition: we require that the Hilbert scheme $\mathcal{H}_{p,n}$ is a fine moduli space for the moduli problem defined by the Hilbert functor. We make this precise in the following subsection.


**Definition 6.2.** Given a scheme $X$ over $k$, its functor of points is defined to be the contravariant functor

$$h_X : (\text{schemes}/k)^{\text{op}} \to (\text{sets})$$

sending each $Y \in (\text{schemes}/k)^{\text{op}}$ to the set $\text{Mor}(Y, X)$ of morphisms $Y \to X$ over $k$; additionally, $h_X$ sends each morphism $f : Y \to Z$ of schemes over $k$ to the map of sets $h_X(f) : \text{Mor}(Z, X) \to \text{Mor}(Y, X)$ given by precomposition by $f$: for every $\varphi \in \text{Mor}(Z, X)$

$$h_X(f)(\varphi) = \varphi \circ f \in \text{Mor}(Y, X).$$

**Definition 6.3.** A functor $F : (\text{schemes}/k)^{\text{op}} \to (\text{sets})$ is representable or a moduli problem if there exists a scheme $X$ over $k$ such that $F$ and the functor of points $h_X$ are naturally isomorphic. If such a scheme $X$ exists, say that $X$ is a fine moduli space for $F$.

**Note.** Definitions 6.2 and 6.3 work the same for the opposite of the category of schemes over any base scheme, but for our purposes it suffices to restrict our attention to schemes over a field $k$.  

34
**Definition 6.4.** The **Hilbert functor** is the functor

\[ \text{Hilb}_{p,n} : (\text{schemes}/k)^{\text{op}} \to (\text{sets}) \]

sending a scheme $B$ over $k$ to the set of subschemes $X \subset \mathbb{P}^n$ that are flat over $B$ and that have Hilbert polynomial equal to $p \in \mathbb{Q}[m]$.

**Theorem 14.** The Hilbert functor is representable by some projective scheme $\mathcal{H}_{p,n}$, and this is what we define to be the Hilbert scheme.

**Proof.** We sketch the construction of $\mathcal{H}_{p,n}$ in the next subsection. \qed

**Remark 6.2.** By Yoneda’s lemma, if a functor is representable by a scheme, then that scheme is unique (up to natural isomorphism). Therefore, Theorem 14 indeed gives a well-defined definition of the Hilbert scheme.

We state a couple useful results about the Hilbert scheme.

**Remark 6.3.** The Hilbert scheme $\mathcal{H}_{p,n}$ is connected. This result is proven in [Mac].

**Remark 6.4.** The Zariski tangent space to the Hilbert scheme $\mathcal{H}_{p,n}$ at the point corresponding to a subscheme $X \subset \mathbb{P}^n$ can be identified with the space of global sections of the normal sheaf $\mathcal{N}_{X/\mathbb{P}^n}$:

\[ T_X \mathcal{H}_{p,n} \cong H^0(X, \mathcal{N}_{X/\mathbb{P}^n}) . \]

A full description of this identification can be found in [EH16].

### 6.2. Construction of $\mathcal{H}_{p,n}$

In this subsection, we give a sketch of the construction of the Hilbert scheme $\mathcal{H}_{p,n}$ as a subscheme of the Grassmannian. While we will not rigorously explain all the details needed to prove Theorem 14, these can be found in [Str96].

**Definition 6.5 (Mumford-Castelnuovo regularity).** Given an integer $r$, we say that a coherent sheaf $\mathcal{F}$ on $\mathbb{P}^n$ is $r$-regular if

\[ H^i(\mathbb{P}^n, \mathcal{F}(r-i)) = 0 \quad \text{for all} \; i > 0. \]

**Remark 6.5.** This $r$-regularity controls when the Hilbert polynomial $p(m)$ of a subscheme $X \subset \mathbb{P}^n$ becomes equal to the dimension of the space of global sections $H^0(X, \mathcal{O}_X(m))$ — this will hold true for all $m \geq r$. In fact, there exists an integer $r$ such that the Hilbert
polynomial $p(m)$ stabilizes to $h^0(X, \mathcal{O}_X(m))$ after $m \geq r$ simultaneously for all subschemes $X \subset \mathbb{P}^n$ with that Hilbert polynomial. The following two propositions taken from [Str96] help us make this precise.

**Proposition 6.1.** If $\mathcal{F}$ is an $r$-regular coherent sheaf on $\mathbb{P}^n$, then

1. The map $H^0(\mathbb{P}^n, \mathcal{F}(s)) \otimes H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(1)) \to H^0(\mathbb{P}^n, \mathcal{F}(s+1))$ is surjective for all $s \geq r$;
2. $\mathcal{F}$ is $r'$-regular for all $r' \geq r$.

**Proof.** We simultaneously prove the two statements via induction on $n$. For the base case, take $n = 0$. The sheaf $\mathcal{F}$ is supported on a point, so statement (1) is clearly true, while statement (2) is true by Serre’s vanishing theorem.

For the inductive step, let $H \subset \mathbb{P}^n$ be a hyperplane. We will show that the restriction $\mathcal{F}_H = \mathcal{F} \otimes_{\mathcal{O}_{\mathbb{P}^n}} \mathcal{O}_H$ is $r$-regular, and then assume the two statements hold true for $\mathcal{F}_H$ for our inductive hypothesis. We saw in section 5 that the ideal sheaf of a hyperplane is given by $\mathcal{I}_H \cong \mathcal{O}_{\mathbb{P}^n}(-1)$, so we have a short exact sequence of sheaves

$$0 \to \mathcal{O}_{\mathbb{P}^n}(-1) \to \mathcal{O}_{\mathbb{P}^n} \to \mathcal{O}_H \to 0.$$ 

We can tensor it by $\mathcal{F}(s)$ for any $s$, and get

$$0 \to \mathcal{F}(s-1) \to \mathcal{F}(s) \to \mathcal{F}_H(s) \to 0.$$ 

When $s = r - i$, we can take the long exact sequence of cohomology groups induced by this short exact sequence, and the portion

$$0 = H^i(\mathbb{P}^n, \mathcal{F}(r - i)) \to H^i(H, \mathcal{F}_H(r - i)) \to H^{i+1}(\mathbb{P}^n, \mathcal{F}(r - i - 1)) = 0$$

tells us that $H^i(H, \mathcal{F}_H(r - i)) = 0$ for all $i > 0$, proving that $\mathcal{F}_H$ is $r$-regular.

Back to our inductive step, we can assume that $\mathcal{F}_H$ is $r'$-regular for all $r' \geq r$ since it is supported on $H \cong \mathbb{P}^{n-1} \subset \mathbb{P}^n$. We look at the same long exact sequence of cohomology groups, this time for $s = r - i + 1$, and have

$$0 = H^i(\mathbb{P}^n, \mathcal{F}(r - i)) \to H^i(\mathbb{P}^n, \mathcal{F}(r - i + 1)) \to H^i(H, \mathcal{F}_H(r - i + 1)) = 0.$$ 

This means that $H^i(\mathbb{P}^n, \mathcal{F}_H(r - i + 1)) = 0$ for all $i > 0$, so $\mathcal{F}$ is $(r + 1)$-regular. We can keep going this way to prove that $\mathcal{F}$ is $r'$-regular for all $r' \geq r$. 


We now prove that statement (1) must hold for $\mathcal{F}$. Let thus $s \geq r$. We know that $\mathcal{F}$ is $s$-regular, so $H^1(\mathbb{P}^n, \mathcal{F}(s-1)) = 0$, so the exact sequence of cohomology groups contains:

$$H^0(\mathbb{P}^n, \mathcal{F}(s)) \to H^0(H, \mathcal{F}_H(s)) \to H^1(\mathbb{P}^n, \mathcal{F}(s-1)) = 0,$$

which means that the map $\alpha : H^0(\mathbb{P}^n, \mathcal{F}(s)) \to H^0(H, \mathcal{F}_H(s))$ is surjective. We also know that the map

$$\beta : H^0(H, \mathcal{F}_H(s)) \otimes H^0(H, \mathcal{O}_H(1)) \to H^0(H, \mathcal{F}_H(s+1))$$

is surjective by the inductive hypothesis that (1) holds for $\mathcal{F}_H$.

Note then that the two maps $\alpha, \beta$ fit into a commutative diagram

$$
\begin{array}{ccc}
H^0(\mathbb{P}^n, \mathcal{F}(s)) \otimes H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(1)) & \xrightarrow{\alpha} & H^0(H, \mathcal{F}_H(s)) \otimes H^0(H, \mathcal{O}_H(1)) \\
\downarrow{\gamma} & & \downarrow{\beta} \\
H^0(\mathbb{P}^n, \mathcal{F}(s+1)) & \xrightarrow{\delta} & H^0(H, \mathcal{F}_H(s+1))
\end{array}
$$

Therefore, $\delta \circ \gamma = \beta \circ \alpha$ is surjective, being a composition of two surjective maps. Note also that $\ker(\delta) \subset \im(\gamma)$ because $\ker(\delta)$ comes from $H^0(\mathbb{P}^n, \mathcal{F}(s))$ via

$$0 \to H^0(\mathbb{P}^n, \mathcal{F}(s)) \to H^0(\mathbb{P}^n, \mathcal{F}(s+1)) \xrightarrow{\delta} H^0(H, \mathcal{F}_H(s+1)).$$

This means that $\gamma$ must be surjective, because if there is an element $x \notin \im(\gamma)$, then $\delta(x) \notin \im(\delta \circ \gamma)$, which is impossible since $\delta \circ \gamma$ is surjective. This finalizes the proof that statement (1) holds for $\mathcal{F}$, so we proved the induction we wanted. \hfill \Box

**Proposition 6.2.** Given any fixed Hilbert polynomial $p(m) \in \mathbb{Q}[m]$, there exists an integer $r_p$ depending only on the polynomial $p(m)$ such that, for any subscheme $X \subset \mathbb{P}^n$ with Hilbert polynomial equal to the given $p(m)$, the ideal sheaf $\mathcal{I} := \mathcal{I}_X$ of $X$ is $r_p$-regular.

**Proof.** The proof of this proposition also proceeds via induction on $n$. We only mention that, as in the previous proof, we can take a hyperplane $H \subset \mathbb{P}^n$ and get a short exact sequence of ideal sheaves

$$0 \to \mathcal{I}(-1) \to \mathcal{I} \to \mathcal{I} \otimes \mathcal{O}_H \to 0.$$  

From here, the inductive hypothesis for $\mathcal{I} \otimes \mathcal{O}_H$ proves the statement for $\mathcal{I}$. See [Str96] for more details. \hfill \Box
Remark 6.6. We can now make Remark 6.5 precise. If $X \subset \mathbb{P}^n$ is any subscheme with some Hilbert polynomial $p(m) \in \mathbb{Q}[m]$ and $r := r_p$ is the integer that Proposition 6.2 guarantees, then the Hilbert polynomial $p(m)$ stabilizes to equal the dimension of sections $h^0(X, \mathcal{O}_X(m))$ for all $m \geq r$. This can be seen because $\mathcal{I}_X$ is $r'$-regular for all $r' \geq r$, so all higher cohomology groups of $\mathcal{I}_X(m)$ vanish for $m \geq r$. Therefore,

$$q_X(m) := \chi(\mathcal{I}_X(m)) = h^0(\mathbb{P}^n, \mathcal{I}_X(m))$$

for all $m \geq r$, where $q_X(m) \in \mathbb{Q}[m]$ denotes the Hilbert polynomial $p_I(m)$ associated to the sheaf $\mathcal{I}_X$. Then, looking at the short exact sequence of sheaves

$$0 \to \mathcal{I}_X(m) \to \mathcal{O}_{\mathbb{P}^n}(m) \to \mathcal{O}_X(m) \to 0,$$

we get that

$$h^0(X, \mathcal{O}_X(m)) = h^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(m)) - h^0(\mathbb{P}^n, \mathcal{I}_X(m)) = \binom{n+m}{m} - q_X(m),$$

is a polynomial for all $m \geq r$, so it must be the Hilbert polynomial $p_X(m)$ of $X$. This means that both Hilbert polynomials $p_X(m)$ and $q_X(m)$ stabilize to equal just the dimension of global sections for $m \geq r$ and, moreover, these two polynomials are related via

$$p_X(m) + q_X(m) = \binom{n+m}{m}.$$

Proposition 6.3. Let $p(m) \in \mathbb{Q}[m]$ be a fixed Hilbert polynomial and $r$ be the integer that Proposition 6.2 guarantees. Also, let $q(m) := \binom{n+m}{m} - p(m) \in \mathbb{Q}[m]$. There exists a map

$$\varphi : \mathcal{H}_{n,p} \to \text{Gr} \left( q(r), \binom{n+r}{r} \right)$$

that realizes the Hilbert scheme $\mathcal{H}_{n,p}$ as a subscheme of the Grassmannian.

Proof. Let $X \subset \mathbb{P}^n$ be a subscheme. As a set map, $\varphi$ associates to every subscheme $X$ the point in the Grassmannian corresponding to the $r$th graded piece $I(X)_r$ of the ideal of $X$.

Let’s now give the equations that cut out $\varphi(\mathcal{H}_{n,p})$. Let $T := k[x_0, x_1, \ldots, x_n]$ and let $T_i$ denote the $i$th graded piece of $T$, for any $i$. Also, let $S(T_i)$ denote the set of vector subspaces
of $T_i$. Consider the multiplication map:

$$f : \text{Gr}(q(r), T_r) \overset{\otimes T_1}{\longrightarrow} T_{r+1}$$

sending a $q(r)$-dimensional subspace $V$ of $T_r$ to the subspace of $T_{r+1}$ obtained by tensoring $V$ with all linear forms $T_1$ of $T$.

Note that statement (1) of Proposition 6.1 guarantees that

$$f(I(X)_r) = I(X)_{r+1}$$

for all ideals $I(X)$ of subschemes $X \subset \mathbb{P}^n$ with Hilbert polynomial $p(m)$. And thus $f(I(X)_r)$ is a $q(r+1)$-dimensional subspace of $T_{r+1}$. It turns out that the image $f(V)$ has the expected dimension $q(r+1)$ if and only if the vector space $V$ we start with is the $r^{th}$ graded piece of some ideal $I(X)$ of a subscheme $X \subset \mathbb{P}^n$ with Hilbert polynomial $p(m)$. Therefore, we can realize $\varphi(\mathcal{H}_{n,p})$ as the subscheme of the Grassmannian given by the vanishing locus of $(q(r+1) + 1)$-dimensional minors under the map $f$. \hfill \Box

7. The Hilbert Scheme of Twisted Cubics in $\mathbb{P}^3$

Let’s now restrict our attention to the Hilbert scheme

$$\mathcal{H}_{g,n,d} := \mathcal{H}_{dm-g+1,n}$$

parametrizing subschemes $X \subset \mathbb{P}^n$ whose Hilbert polynomial equals $p(m) = dm - g + 1$, for some fixed constants $d$ and $g$. According to Theorem 12, these include smooth projective algebraic curves $C \subset \mathbb{P}^n$ of genus $g$ and degree $d$.

Definition 7.1. The restricted Hilbert scheme $\mathcal{H}_{0,3,3}^\circ$ is the open subset of $\mathcal{H}_{0,3,3}$ that parametrizes smooth, irreducible, nondegenerate projective algebraic curves $C \subset \mathbb{P}^n$.

In this section, we restrict our attention to the case when $n = 3$, $d = 3$, and $g = 0$, and describe the components of $\mathcal{H}_{0,3,3}$, including their smoothness and dimension. It turns out that $\mathcal{H}_{0,3,3}^\circ$, which parametrizes twisted cubics, is irreducible, but $\overline{\mathcal{H}_{0,3,3}^\circ}$ is not the only component of $\mathcal{H}_{0,3,3}$. We follow [EH] and [PS85].

7.1. Twisted Cubics Component. In this subsection, we look at the restricted Hilbert scheme component, $\overline{\mathcal{H}_{0,3,3}^\circ}$, whose general point corresponds to a twisted cubic.
Proposition 7.1. The restricted Hilbert scheme $H_{0,3,3}$ is irreducible and has dimension 12.

Proof. We look at quadric surfaces containing a twisted cubic $C$. We want to show that, if $Q, Q' \subset \mathbb{P}^3$ are two distinct quadric surfaces, then $Q \cap Q'$ contains a twisted cubic $C$ if and only if $Q \cap Q'$ also contains a line $L$; if this is the case, then $Q \cap Q' = C \cup L$. On one hand, let $Q, Q'$ be two quadrics containing a twisted cubic curve $C$. Bézout’s theorem tells us that $Q \cap Q'$ has degree 4, so the intersection must contain a line $L$ in addition to the degree 3 curve $C$. On the other hand, let $Q, Q'$ be two quadrics containing a given line $L$; moreover, for the purposes of our dimension calculation, it suffices to assume that these quadrics are general – that is, smooth and irreducible. Such a quadric $Q$ is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$; this is because, under a suitable change of coordinates, we can assume that $Q = V(x_0 x_3 - x_1 x_2)$, which is exactly the image $\sigma(\mathbb{P}^1 \times \mathbb{P}^1)$ of $\mathbb{P}^1 \times \mathbb{P}^1$ under the Segre embedding:

$$\sigma : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3 \quad \text{sending} \quad (x_0 : x_1) \mapsto [x_0 y_0 : x_0 y_1 : x_1 y_0 : x_1 y_1].$$

Then, $Q'$ will intersect $Q \cong \mathbb{P}^1 \times \mathbb{P}^1$ in bidegree $(2, 2)$ – where this bidegree comes from the degrees of the intersection of $Q'$ with a general $\mathbb{P}^1 \times \{\text{pt}\}$ and $\{\text{pt}\} \times \mathbb{P}^1$, respectively. Therefore, given that $L \subset Q \cap Q'$, we must have that $Q \cap Q' = L \cup C$, for some curve $C$ of bidegree $(2, 1)$ or $(1, 2)$. Moreover, by Bertini’s theorem, $C$ will be smooth, so it will be a twisted cubic curve.

Let $\text{Gr}(1, 3)$ denote the Grassmannian of lines in $\mathbb{P}^3$. Also, let $\mathbb{P}^9$ be the space of quadric surfaces in $\mathbb{P}^3$; what we mean by this is the following: we can identify a quadric in $\mathbb{P}^3$ with the homogeneous degree 2 polynomial $f \in \mathbb{C}[x_0, x_1, x_2, x_3]$ that defines it (taking $f$ up to scalar multiplication), and we can identify such homogeneous degree 2 polynomials with points in $\mathbb{P}^9$ via the map

$$f(x_0, x_1, x_2, x_3) = a_0 \cdot x_0^2 + a_1 \cdot x_0 x_1 + a_2 \cdot x_0 x_2 + \cdots + a_{10} \cdot x_4^2 \mapsto [a_0 : a_1 : \cdots : a_{10}] \in \mathbb{P}^9.$$

Then, consider the incidence scheme:

$$\Phi := \{(C, L, Q, Q') \mid Q \cap Q' = C \cup L\} \subset H_{0,3,3} \times \text{Gr}(1, 3) \times \mathbb{P}^9 \times \mathbb{P}^9$$

and look at the two projection maps $\pi_1 : \Phi \to H_{0,3,3}$ and $\pi_2 : \Phi \to \text{Gr}(1, 3)$.

First, consider the projection $\pi_2 : \Phi \to \text{Gr}(1, 3)$, which is easily seen to be surjective. Given any line $L \in \text{Gr}(1, 3)$, I claim that the space of quadrics containing $L$ is isomorphic to $\mathbb{P}^6$.
Indeed, pick any three distinct points \( p_1, p_2, p_3 \in L \). A quadric surface \( Q \) contains \( L \) if and only if it contains the three chosen points because, if \( Q \) contains the three points, then

\[
\#(Q \cap L) \geq 3 > 2 = \deg(Q) \cdot \deg(L),
\]

so \( Q \) must contain the whole line \( L \). Since each requirement that \( p_i \in Q = V(f) \) removes one degree of freedom by imposing that the coefficients \( a_0, a_1, \ldots, a_{10} \) of \( f \) satisfy \( f(p_i) = 0 \), the space of quadrics containing \( L \) is thus isomorphic to \( \mathbb{P}^{9-3} = \mathbb{P}^6 \). Therefore, the preimage \( \pi_2^{-1}(L) \) comes from all general quadrics \( Q, Q' \) containing \( L \) and so is an open subset of \( \mathbb{P}^6 \times \mathbb{P}^6 \).

Therefore, \( \Phi \) is irreducible and has dimension

\[
\dim(\Phi) = \dim(\Gr(1, 3)) + \dim(\pi_2^{-1}(L)) = \dim(\Gr(1, 3)) + \dim(\mathbb{P}^6 \times \mathbb{P}^6) = 4 + 12 = 16.
\]

Then, consider the projection \( \pi_1 : \Phi \to \mathcal{H}^{0}_{0,3,3} \), which is again surjective. Given any twisted cubic \( C \in \mathcal{H}^{0}_{0,3,3} \), the space of quadrics containing \( C \) is isomorphic to \( \mathbb{P}^2 \). This follows by a similar argument, noting that we can pick any distinct points \( p_1, p_2, \ldots, p_7 \in C \) and a quadric \( Q \) contains the curve \( C \) if and only if it contains these seven points. We get that the space of quadrics containing \( C \) is isomorphic to \( \mathbb{P}^2 \) and so the fiber \( \pi_2^{-1}(C) \) is an open subset of \( \mathbb{P}^2 \times \mathbb{P}^2 \). Therefore, \( \mathcal{H}^{0}_{0,3,3} \) is irreducible and has dimension

\[
\dim(\mathcal{H}^{0}_{0,3,3}) = \dim(\Phi) - \dim(\pi_2^{-1}(C)) = \dim(\Phi) - \dim(\mathbb{P}^2 \times \mathbb{P}^2) = 16 - 4 = 12.
\]

\[\square\]

**Proposition 7.2.** Given any twisted cubic \( C \subset \mathbb{P}^3 \), the Zariski tangent space \( T_C \mathcal{H}^{0}_{0,3,3} \) to the Hilbert scheme at the corresponding point \( C \in \mathcal{H}^{0}_{0,3,3} \) is 12-dimensional, so the restricted Hilbert scheme is smooth.

**Proof.** By Remark 6.4, we can identify the tangent space of interest with \( H^0(C, N_{C/\mathbb{P}^3}) \). We can then take a smooth, irreducible quadric surface \( Q \subset \mathbb{P}^3 \) that contains the twisted cubic \( C \), and get a short exact sequence of normal sheaves:

\[
0 \to N_{C/Q} \to N_{C/\mathbb{P}^3} \to N_{Q/\mathbb{P}^3}|_C \to 0.
\]

First, \( N_{C/Q} \) has degree 4 because \( C \) is a curve of bidegree \((1, 2)\) or \((2, 1)\) on the quadric \( Q \cong \mathbb{P}^1 \times \mathbb{P}^1 \) and the degree of the normal sheaf \( N_{C/Q} \) is just given by the self-intersection of the curve \( C \) on the surface \( Q \). Also, \( N_{Q/\mathbb{P}^3}|_C \cong \mathcal{O}_C(2) \), so it has degree 6. Then \( N_{C/\mathbb{P}^3} \)
must have degree $4 + 6 = 10$. This means that

$$\mathcal{N}_{C/\mathbb{P}^3} \cong \begin{cases} \mathcal{O}_{\mathbb{P}^1}(4) \oplus \mathcal{O}_{\mathbb{P}^1}(6) & \text{if the exact sequence above splits} \\ \mathcal{O}_{\mathbb{P}^1}(5) \oplus \mathcal{O}_{\mathbb{P}^1}(5) & \text{otherwise} \end{cases}.$$ 

Regardless which case it is, we get that the dimension of $H^0(C, \mathcal{N}_{C/\mathbb{P}^3})$ is 12, as desired. □

Remark 7.1. In fact, one can show that $\mathcal{N}_{C/\mathbb{P}^3} \cong \mathcal{O}_{\mathbb{P}^1}(5) \oplus \mathcal{O}_{\mathbb{P}^1}(5)$. We won’t prove this rigorously, but we briefly explain how one obtains this. For any point $p \in C$, we define a subsheaf $L_p \subset \mathcal{N}_{C/\mathbb{P}^3}$ by specifying its fibers: if $q \in C \setminus \{p\}$, then we take the fiber $(L_p)_q$ to be the 1-dimensional subspace of $\mathcal{N}_{C/\mathbb{P}^3}$ defined by the line $pq$; to specify the fiber $(L_p)_p$, we take the closure of the previous fibers as $q$ approaches $p$. It turns out that, for any two distinct points $p, q \in C$, we can write

$$\mathcal{N}_{C/\mathbb{P}^3} \cong L_p \oplus L_q,$$

which means that we must be in the case when $\mathcal{N}_{C/\mathbb{P}^3} \cong \mathcal{O}_{\mathbb{P}^1}(5) \oplus \mathcal{O}_{\mathbb{P}^1}(5)$.

7.2. Extraneous Component. The restricted Hilbert scheme $\mathcal{H}_{0,3,3}$ is not the only component of $\mathcal{H}_{0,3,3}$ – that is, not every subscheme of $\mathbb{P}^3$ with Hilbert polynomial $p(m) = 3m + 1$ is a flat limit of twisted cubics. Indeed, we can take unions $C' := C \cup \{p\}$ of a plane cubic curve $C \subset \mathbb{P}^2 \subset \mathbb{P}^3$ and a point $p \in \mathbb{P}^3 \setminus C$. Indeed, the Hilbert polynomial of such a union $C'$ equals $p(m) = 3m + 1$ because: a plane cubic curve $C$ has degree 3 and genus 1, and adding a point to it leaves the degree unchanged, but decreases the genus by 1.

Definition 7.2. We let $\mathcal{H}' \subset \mathcal{H}_{0,3,3}$ be the open subset of the Hilbert scheme parametrizing unions of a plane cubic curve and a point not on the curve. This $\mathcal{H}'$ gives another irreducible component of $\mathcal{H}_{0,3,3}$. Such additional components of the Hilbert scheme are called extraneous components.

Proposition 7.3. The component $\mathcal{H}'$ just defined is irreducible and has dimension 15.

Proof. It suffices to prove that the Hilbert scheme $\mathcal{H}$ parametrizing plane cubic curves in $\mathbb{P}^3$ is irreducible and has dimension 12. Once we know this, it follows immediately that $\mathcal{H}'$ is irreducible and has dimension 15 since it is an open subset of $\mathcal{H} \times \mathbb{P}^3$. 

42
To compute the dimension of $\mathcal{H}$, consider the map

$$\varphi: \mathcal{H} \to (\mathbb{P}^3)^*,$$

sending each plane cubic curve $C \subset \mathbb{P}^3$ to the (unique) hyperplane $H \subset \mathbb{P}^3$ containing it. Given any hyperplane $H \in (\mathbb{P}^3)^*$, the space of cubic curves contained in $H \cong \mathbb{P}^2$ can be identified with the space of degree 3 homogeneous polynomials on $\mathbb{P}^2$, which can be identified with $\mathbb{P}^9$ (by an argument similar to the one we gave in the proof of Proposition 7.1). Therefore, $\mathcal{H}$ is irreducible and has dimension:

$$\dim(\mathcal{H}) = \dim ((\mathbb{P}^3)^*) + \dim (\varphi^{-1}(H)) = 3 + 9 = 12.$$

□

In the remarks below, we state a few facts that help fully describe the Hilbert scheme $\mathcal{H}_{0,3,3}$. We refer the reader to [PS85] for proofs.

**Remark 7.2.** The two components described in this section are the only two irreducible components of the Hilbert scheme $\mathcal{H}_{0,3,3}$:

$$\mathcal{H}_{0,3,3} = \overline{\mathcal{H}_{0,3,3}} \cup \overline{\mathcal{H}}.$$

In particular, this means that any subscheme of $\mathbb{P}^3$ that has Hilbert polynomial $p(m) = 3m+1$ is either a twisted cubic, a union of a plane cubic curve and a point, or a flat limit of such subschemes.

**Remark 7.3.** At the intersection of the two components, $\overline{\mathcal{H}_{0,3,3}} \cap \overline{\mathcal{H}}$, a general point corresponds to a nodal plane cubic curve $C \subset \mathbb{P}^2 \subset \mathbb{P}^3$ with an embedded point at the node.

**Remark 7.4.** The Hilbert scheme $\mathcal{H}_{0,3,3}$ is everywhere smooth. However, the computation for this gets very cumbersome very soon. For example, in order to show that the Hilbert scheme is smooth at the points of the intersection $\overline{\mathcal{H}_{0,3,3}} \cap \overline{\mathcal{H}}$, [PS85] looks at second order deformations to see that it has the expected dimension.

8. **Mumford’s Example**

While the Hilbert scheme $\mathcal{H}_{0,3,3}$ from the previous section behaved as nicely as one can hope, this nice behavior does not persist. We thus end by mentioning Mumford’s example of a
rather unexpected pathology occurring on the Hilbert scheme. Full details and computations for this result can be found in [EH].

**Example 15.** Consider the restricted Hilbert scheme $\mathcal{H}_{24,3,14}$, parametrizing smooth, irreducible curves $C \subset \mathbb{P}^3$ with genus 24 and degree 14. It turns out that the subspace $\mathcal{H} \subset \mathcal{H}_{24,3,14}$ that parametrizes curves that are residual to two conic surfaces in the intersection of a sextic and a cubic surface gives an irreducible component of $\mathcal{H}_{24,3,14}$. In particular, $\mathcal{H}$ is irreducible and has dimension 56. However, if we pick a general point $C \in \mathcal{H}$, then the tangent space to $\mathcal{H}$ at $C$ is 57-dimensional. Therefore, the component $\mathcal{H}$ of $\mathcal{H}_{24,3,14}$ is singular at its generic points. This example thus offers a stark contrast with the nicely-behaved components of $\mathcal{H}_{0,3,3}$ from the previous section.

**Remark 8.1.** In fact, the pathological behavior of the Hilbert scheme extends far beyond Mumford’s example. In [Vak06], Ravi Vakil proves that every type of singularity appears on the Hilbert scheme of smooth curves in projective space. In other words, every complete local ring appears as the completion of a local ring of a Hilbert scheme. While I do not fully understand the proof given in [Vak06], I think this result is really nice and unexpected, so I figured it’s a good way to end our discussion of the Hilbert scheme.
References


