Chapter 10
Dimension and Hilbert Function

The dimension of an algebraic variety can be defined in several equivalent ways. We will use an algebraic approach, and derive an algorithm for computing the dimension for an ideal I (and its corresponding variety $V(I)$) by an application of Gröbner bases. Our treatment of this subject is based on monomial ideals (such as the initial ideal of an ideal) and the concept of the Hilbert function.

Throughout this chapter we let K be a field of characteristic 0, $\overline{K}$ the algebraic closure of K, and $\mathcal{K}$ a universal domain for K, i.e. $\mathcal{K}$ is an algebraically closed superfield of K with infinite transcendence degree over K. E.g., $\mathbb{C}$ is a universal domain for $\mathbb{Q}$.

10.1. An algebraic definition of dimension

The following definition of the dimension of an ideal I can be found in [Gro68], vol. II, p. 38. We consider the coordinate ring $\Gamma(I)$ and a maximal collection of coordinate functions x_i on $V(I)$ which are independent in the coordinate ring. The number of coordinate functions in such a maximal collection is called the dimension of I.

Definition 10.1.1: Let $I \subset K[x_1, \ldots, x_n]$ be a proper ideal and $\{i_1, \ldots, i_d\}$ a subset of $\{1, \ldots, n\}$. The set $\{x_{i_1}, \ldots, x_{i_d}\}$ is said to be *independent modulo I* if

$$I \cap K[x_{i_1}, \ldots, x_{i_d}] = \{0\}.$$

We denote the set $\{X \subseteq \{x_1, \ldots, x_n\} \mid X \text{ is independent modulo } I\}$ by $\Delta(I)$. The *dimension* of I, denoted by $\dim(I)$, is the maximal number of elements in any set of variables independent modulo I, i.e.

$$\dim(I) = \max(\{|X| \mid X \in \Delta(I)\}).$$

Furthermore, for a non–empty variety $V \subseteq \overline{K}^n$ we define its dimension as

$$\dim(V) := \dim(I(V)). \qquad \square$$

Observe that for any proper ideal $I \subset K[x_1, \ldots, x_n]$ we have

$$\Delta(I) = \Delta(\sqrt{I}) \quad \text{and therefore} \quad \dim(I) = \dim(\sqrt{I}).$$

Let $\{i_1, \ldots, i_d\} \subseteq \{1, \ldots, n\}$. From the elimination property of Gröbner bases we get that

$$\{x_{i_1}, \ldots, x_{i_d}\} \in \Delta(I) \quad \text{iff} \quad G \cap K[x_{i_1}, \ldots, x_{i_d}] = \emptyset,$$

where G is the reduced Gröbner basis of I with respect to a lexicographic ordering with $x_{i_1} \prec x_{i_2} \prec \ldots \prec x_{i_d} \prec$ other variables (or, for that matter, a product ordering with $\{x_{i_1}, \ldots, x_{i_d}\} \prec X \setminus \{x_{i_1}, \ldots, x_{i_d}\}$). From these observations we can immediately derive an algorithm DIMENSION_1 for computing the dimension of an ideal I.

---

algorithm DIMENSION_1(**in:** F**; out:** d, X);
[F is a finite subset of $K[x_1, \ldots, x_n]$, with $I := \langle F \rangle \neq K[x_1, \ldots, x_n]$.
$d = \dim(I)$, and X is a set of independent variables modulo I with $|X| = d$.]
(1) **for** every permutation p of $\{1, \ldots, n\}$ **do**
{ compute the reduced Gröbner basis G_p of I w.r.t. the lexicographic ordering with $x_{p(1)} \prec \ldots \prec x_{p(n)}$;
$i_p :=$ the greatest element of $\{0, \ldots, n\}$ such that
$G_p \cap K[x_{p(1)}, \ldots, x_{p(i_p)}] = \emptyset$ };
(2) choose a permutation p' such that
$i_{p'} = \max(\{i_p \mid p \text{ a permutation of } \{1, \ldots, n\}\})$;
(3) $d := i_{p'}$;
$X := \{x_{p'(1)}, \ldots, x_{p'(i_{p'})}\}$;
return □

Example 10.1.1: Let I be the ideal generated by

$$F := \{x_1x_3 + x_1^2 + x_1x_2,\ x_2x_3 + x_1 + 1,\ x_1x_2 + x_1x_2x_3\} \subseteq \mathbb{Q}[x_1, x_2, x_3].$$

We obtain $\Delta(I)$ by computing lexicographic Gröbner bases of F w.r.t. every possible ordering of variables. Here are these six reduced Gröbner bases:

$$\begin{array}{lcc}
x_1 \prec x_2 \prec x_3 & : & \{x_2x_3 + x_1 + 1,\ x_1x_3 + 2x_1^2 + x_1,\ x_1x_2 - x_1^2 - x_1,\ x_1^3 + x_1^2\}, \\
x_2 \prec x_1 \prec x_3 & : & \{x_1x_3 + 2x_1x_2 - x_1,\ x_2x_3 + x_1 + 1,\ x_1^2 - x_1x_2 + x_1,\ x_1x_2^2 - x_1x_2\}, \\
x_1 \prec x_3 \prec x_2 & : & \{x_2x_3 + x_1 + 1,\ x_1x_2 - x_1^2 - x_1,\ x_1x_3 + 2x_1^2 + x_1,\ x_1^3 + x_1^2\}, \\
x_3 \prec x_1 \prec x_2 & : & \{2x_1x_2 + x_1x_3 - x_1,\ x_2x_3 + x_1 + 1,\ 2x_1^2 + x_1x_3 + x_1,\ x_1x_3^2 - x_1\}, \\
x_2 \prec x_3 \prec x_1 & : & \{x_1 + x_2x_3 + 1,\ x_2x_3^2 + 2x_2^2x_3 - x_2x_3 + x_3 + 2x_2 - 1, \\
 & & x_2^3x_3 - x_2^2x_3 + x_2^2 - x_2\}, \\
x_3 \prec x_2 \prec x_1 & : & \{x_1 + x_2x_3 + 1,\ 2x_2^2x_3 + x_2x_3^2 - x_2x_3 + 2x_2 + x_3 - 1, \\
 & & x_2x_3^3 - x_2x_3 + x_3^2 - 1\}.
\end{array}$$

Since every Gröbner basis contains a bivariate polynomial, an independent set of variables can at most contain one variable. Because of the first Gröbner basis, $\{x_1\} \notin \Delta(I)$. But $\{x_2\} \in \Delta(I)$ and $\{x_3\} \in \Delta(I)$, because the second Gröbner basis does not contain an element of $\mathbb{Q}[x_2]$, and the forth Gröbner basis does not contain an element of $\mathbb{Q}[x_3]$. Altogether,

$$\Delta(I) = \{\ \{x_2\},\ \{x_3\}, \emptyset\ \}.$$

□

Obviously this approach suffers from the fact that $n!$ Gröbner bases w.r.t. lexicographic orderings have to be computed. So our goal is to derive a more efficient approach to the computation of the dimension. The crucial fact for obtaining a faster algorithm is the following theorem, which will be proved later (for graduated orderings), after we have compiled some knowledge about Hilbert functions.

Definition 10.1.2: Let $\prec$ be an admissible ordering on $[x_1, \ldots, x_n]$, I an ideal in $K[x_1, \ldots, x_n]$. The *initial ideal* of I, denoted by $I_\prec$, is the ideal $\langle \mathrm{in}(I) \rangle$, i.e. the ideal generated by the initials or leading terms of I w.r.t. $\prec$. □

Theorem 10.1.1: *Let $\prec$ be an admissible ordering on $[x_1, \ldots, x_n]$, I a proper ideal in $K[x_1, \ldots, x_n]$. Let X be an element of maximal cardinality in $\Delta(I_\prec)$. Then X is an element of maximal cardinality in $\Delta(I)$ and therefore*

$$\dim(I_\prec) \;=\; |X| \;=\; \dim(I). \qquad \square$$

Hence, the computation of an element of maximal cardinality in $\Delta(I)$ can be reduced to the computation of an element of maximal cardinality in $\Delta(I_\prec)$.

If G is a Gröbner basis of I w.r.t. $\prec$, then $\langle \mathrm{in}(G) \rangle = I_\prec$. In fact, this is equivalent to G being a Gröbner basis w.r.t. $\prec$. So, for every subset $X = \{x_{i_1}, \ldots, x_{i_d}\} \subseteq \{x_1, \ldots, x_n\}$,

$$X \in \Delta(I_\prec) \quad \text{iff} \quad \mathrm{in}(g) \notin K[x_{i_1}, \ldots, x_{i_d}] \text{ for every } g \in G.$$

Therefore, after computing G, we can obtain an element of maximal cardinality in $\Delta(I_\prec)$ by purely combinatorial methods.

This leads immediately to the much more efficient algorithm DIMENSION_2 for computing the dimension of an ideal I.

---

algorithm DIMENSION_2(**in:** F; **out:** d, X);
[F is a finite subset of $K[x_1, \ldots, x_n]$, with $I := \langle F \rangle \neq K[x_1, \ldots, x_n]$.
$d = \dim(I)$, and X is a set of independent variables modulo I with $|X| = d$.]
(1) choose an admissible ordering $\prec$ on $[x_1, \ldots, x_n]$;
    $G := \mathrm{GB}(F)$ w.r.t. $\prec$;
(2) for all subsets $X = \{x_{i_1}, \ldots, x_{i_m}\}$ of $\{x_1, \ldots, x_n\}$ check whether
    (*) $X \in \Delta(I_\prec)$, i.e. whether
    $\mathrm{in}(g) \notin K[x_{i_1}, \ldots, x_{i_m}]$ for every $g \in G$;
(3) X := a set of maximal cardinality satisfying this condition (*);
    $d := |X|$;
    return □

A proof of Theorem 10.1.1 can be found in [KaS95]. In [KrW91] a different proof for lexicographic orderings is given. We will restrict ourselves to another special case: we will prove Theorem 10.1.1 under the additional assumption that $\prec$ is a *graduated ordering*, i.e.

$$\deg(u) < \deg(v) \Longrightarrow u \prec v \qquad \text{for all } u, v \in [x_1, \ldots, x_n].$$

Our proof is based on the important concept of Hilbert functions.

Example 10.1.2: Let F be defined as in the previous example and let G be the reduced Gröbner basis of F w.r.t. the lexicographic ordering with $x_1 \prec x_2 \prec x_3$. Then

$$I_\prec = \langle \mathrm{in}(G) \rangle = \langle x_2x_3,\ x_1x_3,\ x_1x_2,\ x_1^3 \rangle.$$

Hence,

$$\Delta(I_\prec) = \{\ \{x_2\},\ \{x_3\},\ \emptyset\ \} \quad \text{and} \quad \dim(I) = \dim(I_\prec) = 1. \qquad \square$$

The initial ideal $I_\prec$ of an ideal I has the special property of being generated by monomials. Such ideals have a structure very similar to homogeneous ideals. Of course, they are particular homogeneous ideals.

Definition 10.1.3: An ideal I in $K[x_1, \ldots, x_n]$ is a *monomial ideal* iff it has a monomial basis, i.e. a basis B s.t. every $f \in B$ is a monomial $ax_1^{j_1} \cdots x_n^{j_n}$, $a \in K$. $\square$

Theorem 10.1.2: *Let I be an ideal in $K[x_1, \ldots, x_n]$. Then the following are equivalent:*

(i) I is a monomial ideal.

(ii) If $f \in I$ and m is a monomial occurring in f, then $m \in I$.

(iii) I is generated by a finite monomial basis.

Proof: (i) $\Longrightarrow$ (ii): By definition, for every $f \in I$ there exist finitely many monomials $m_1, \ldots, m_r$ in a monomial basis B such that

$$f = h_1m_1 + \cdots + h_rm_r$$

for some $h_1, \ldots, h_r \in K[x_1, \ldots, x_n]$. Hence, every monomial in f is divisible by one of the m_i and therefore in I.

(ii) $\Longrightarrow$ (iii): By Hilbert's Basis Theorem the ideal I has a finite basis B'. Then the set

$$B := \{\ m \mid m \text{ occurs in some } f \in B'\ \}$$

is a finite monomial basis of I.

(iii) $\Longrightarrow$ (i): Trivial. $\square$

10.2. The Hilbert function

Let W be a subspace of a finite–dimensional vector space V. Recall that in this case W and the quotient space V/W are also finite–dimensional and

$$\dim(V) = \dim(W) + \dim(V/W). \tag{10.2.1}$$

Definition 10.2.1: Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal. For a non–negative integer s we let

$$K[x_1, \ldots, x_n]_{\leq s}$$

denote the set of polynomials of total degree $\leq s$ in $K[x_1, \ldots, x_n]$ and we define

$$I_{\leq s} := I \cap K[x_1, \ldots, x_n]_{\leq s}.$$

Note that we can consider $K[x_1, \ldots, x_n]_{\leq s}$ as a finite–dimensional vector space over K and $I_{\leq s}$ as a finite–dimensional subspace. The *(affine) Hilbert function* of I is the function on the non–negative integers s defined by (using (10.2.1))

$$\begin{aligned} HF_I(s) :&= \dim(K[x_1, \ldots, x_n]_{\leq s}/I_{\leq s}) \\ &= \dim(K[x_1, \ldots, x_n]_{\leq s}) - \dim(I_{\leq s}). \end{aligned}$$

□

Example 10.2.1: Consider the ideal

$$I = \langle x^2 \rangle \subset \mathbb{Q}[x, y, z].$$

By a simple inspection we see that for $s = 0, 1, 2, 3$ the Hilbert function of I is as follows:

s	$HF_I(s)$
0	1
1	4
2	9
3	16

For $s \geq 2$ we have

$$\begin{aligned} HF_I(s) &= \binom{3+s}{s} - \binom{3+(s-2)}{s-2} \\ &= \frac{(3+s)(2+s)(1+s) - (1+s)s(s-1)}{3!} \\ &= s^2 + 2s + 1. \end{aligned}$$

So we see that for $s \geq 2$ the Hilbert function HF_I agrees with a polynomial function. $\square$

Let $I \subset K[x_1, \ldots, x_n]$ be a proper ideal, $\prec$ a graduated ordering on $[x_1, \ldots, x_n]$, and $I_\prec$ the initial ideal of I. We will show that

$$I \text{ and the monomial ideal } I_\prec \text{ have the same Hilbert function.} \tag{10.2.2}$$

Therefore, we will now study Hilbert functions of monomial ideals. More precisely, we will show that for every monomial ideal J there exists a non–negative integer t and a univariate polynomial $h \in \mathbb{Q}[x]$ such that

$$HF_J(s) = h(s) \text{ for every } s \geq t \quad \text{and} \quad \dim(J) = \deg(h). \tag{10.2.3}$$

Using (10.2.2) and (10.2.3) it will be easy to prove Theorem 10.1.1 for graduated orderings. For proving (10.2.3) we introduce the concept of a translate.

Definition 10.2.2: For each monomial ideal I in $K[x_1, \ldots, x_n]$ we let

$$C(I) := \{u \in [x_1, \ldots, x_n] \mid u \notin I\}$$

be the set of power products (power products with coefficient 1) not in I, the *complement* of I.

For $M, N \subseteq [x_1, \ldots, x_n]$ we define their product as

$$M \cdot N := \{uv \mid u \in M, v \in N\}.$$

For every integer $r \in \{1, \ldots, n\}$, every set of variables $\{x_{i_1}, \ldots, x_{i_r}\} \subseteq \{x_1, \ldots, x_n\}$, and every $u \in [x_1, \ldots, x_n]$ we call

$$\{u\} \cdot [x_{i_1}, \ldots, x_{i_r}]$$

a *translate of dimension* r. Furthermore, every singleton $\{u\} \subset [x_1, \ldots, x_n]$ is called a *translate of dimension* 0. $\square$

Example 10.2.2: Consider the ideal

$$I = \langle x_1^3, x_1 x_2 \rangle \subset \mathbb{Q}[x_1, x_2].$$

Obviously, $C(I) = \{x_1, x_1^2\} \cup [x_2]$. Let s be a non–negative integer and denote the set of those power products in $C(I)$ with total degree $\leq s$ by C_s. It will be shown in the proof of Theorem 10.2.5 that the set $\{u \mid u \in C_s\}$ (or, more precisely, the equivalence classes with representatives $u \in C_s$) is a basis of the quotient space $\mathbb{Q}[x_1, x_2]_{\leq s}/I_{\leq s}$. Therefore, I has the following Hilbert function:

$$HF_I(0) = 1, \quad HF_I(1) = 3, \quad HF_I(s) = s + 3 \text{ for } s \geq 2.$$

Note that the Hilbert function is a polynomial function for sufficiently large s (in this example s must be at least 2). Furthermore, the degree of this polynomial is equal to the dimension of the ideal. We will show that both results hold for arbitrary ideals. The proof is based on the observation that if I is a monomial ideal, the set of power products not in the ideal can be written as a finite disjoint union of translates. For instance, in this example

$$C(I) = \{x_1\} \cup \{x_1^2\} \cup \{1\} \cdot [x_2]. \qquad \square$$

Theorem 10.2.1: *If $I \subset K[x_1, \ldots, x_n]$ is a monomial ideal then $C(I)$ can be written as a finite disjoint union of translates.*

Proof: The theorem holds trivially for the zero ideal, so we can assume that $I \neq \{0\}$. The theorem also holds trivially for $I = \langle 1 \rangle = K[x_1, \ldots, x_n]$, we take the empty union.

We proceed by induction on the number of variables n. If $n = 1$ then $I = \langle x^k \rangle$ for some integer $k \geq 0$. For $k = 0$ we have the trivial ideal $\langle 1 \rangle$. Otherwise, the only power products not in I are $1, x, \ldots, x^{k-1}$. Hence, the complement $C(I)$ is the union of the translates $\{1\}, \{x\}, \ldots, \{x^{k-1}\}$.

So now let us assume that the result holds for $n-1$ variables, and let us consider a proper monomial ideal I in $K[x_1, \ldots, x_n]$.

For each $j \geq 0$, let

$$I_j := \langle \{u \in K[x_1, \ldots, x_{n-1}] \mid u x_n^j \in I\} \rangle \quad \subseteq \quad K[x_1, \ldots, x_{n-1}].$$

Because I is an ideal, we have $I_j \subseteq I_{j'}$ for $j < j'$. By the ascending chain condition for ideals in Noetherian rings, there is an integer j^* such that $I_j = I_{j^*}$ for all $j \geq j^*$. We claim that $C(I)$ can be written as

$$C(I) = \bigcup_{j=0}^{j^*} B_j, \tag{10.2.4}$$

where

$$B_j = C(I_j) \cdot \{x_n^j\} \text{ for } j = 0, \ldots, j^* - 1 \quad \text{and} \quad B_{j^*} = C(I_{j^*}) \cdot \{x_n^{j^*}, x_n^{j^*+1}, \ldots\}.$$

By the induction hypothesis, the sets $C(I_k), k = 0, \ldots, j^*$, can be written as finite disjoint unions of translates. We leave it as an exercise to show that the sets $B_j, k = 0, \ldots, j^*$, are also finite disjoint unions of translates.

So it only remains to prove the set equality in (10.2.4). Note that for every $j < j^*$ we have $B_j \subseteq C(I)$ by the definitions of B_j and $C(I_j)$. For showing that $B_{j^*} \subseteq C(I)$, observe that $I_j = I_{j^*}$ for $j \geq j^*$, so that $C(I_{j^*}) \cdot \{x_n^j\} \subseteq C(I)$ for these j's. Hence,

$$C(I) = \bigcup_{j=0}^{j^*} B_j.$$

On the other hand, let

$$u = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \in C(I).$$

If $i_n < j^*$, then $x_1^{i_1} x_2^{i_2} \cdots x_{n-1}^{i_{n-1}} \in C(I_{i_n})$, and therefore $u \in B_{i_n}$. If $i_n \geq j^*$, then $u' = x_1^{i_1} x_2^{i_2} \cdots x_n^{j^*} \in C(I)$. Hence, $x_1^{i_1} x_2^{i_2} \cdots x_{n-1}^{i_{n-1}} \in C(I_{j^*})$, and therefore $u \in B_{j^*}$. This completes the proof of the equality in (10.2.4). □

In Example 10.2.1 we saw that we could write the Hilbert function $HF_I(s)$ as a difference of binomial coefficients depending on the number of variables and s for sufficiently large s. This observation can be generalized and it will lead us to the concept of the Hilbert polynomial. The proof of the following lemma is an easy combinatorial exercise and is left to the reader.

Lemma 10.2.2: *The number of power products of degree $\leq s$ in $[x_1, \ldots, x_m]$ is the binomial coefficient*

$$\binom{m+s}{s.}$$ □

Now we can determine the number of power products of degree $\leq s$ in an arbitrary translate.

Lemma 10.2.3: *Let $u \in [x_1, \ldots, x_n]$ and $t = \deg(u)$.*

(i) *The number of power products of degree $\leq s$ in the translate $\{u\} \cdot [x_1, \ldots, x_m]$ is equal to the binomial coefficient*

$$\binom{m+s-t}{s-t},$$

provided that $s \geq t$.

(ii) *For $s \geq t$, this number of power products is a polynomial function of s of degree m and the coefficient of s^m is $1/m!$.*

Proof: If $s \geq t$ then each power product v in $\{u\} \cdot [x_1, \ldots, x_m]$ of degree $\leq s$ has the form $u \cdot w$, where w is a power product in $[x_1, \ldots, x_m]$ of degree $\leq s - t$. The formula given in (i) follows from Lemma 10.2.2 by counting the number of possible w.

(ii) follows immediately from (i) and the definition of the binomial coefficient. □

Theorem 10.2.4: *If $I \subset K[x_1, \ldots, x_n]$ is a proper monomial ideal, then for all s sufficiently large, the number of power products not in I of degree $\leq s$ is a polynomial of degree $d = \dim(I)$ in s. Furthermore, the coefficient of s^d in this polynomial is positive.*

Proof: By Theorem 10.2.1 we can write $C(I)$ as a finite disjoint union of translates

$$C(I) = C_1 \cup \ldots \cup C_r. \tag{10.2.5}$$

For $j \in \{1, \ldots, r\}$ and a non–negative integer s we denote the number of power products in C_j of degree $\leq s$ by $c_j(s)$ and the number of power products in $C(I)$ of degree $\leq s$ by $c(s)$. By (10.2.5),

$$c(s) = c_1(s) + \cdots + c_r(s).$$

From Lemma 10.2.3 we get that for every $j \in \{1, \ldots, r\}$ there exists a non–negative integer t_j and a univariate polynomial $h_j(x) = a_{m_j} x^{m_j} + \cdots + a_0 \in \mathbb{Q}[x]$, such that

(1) $c_j(s) = h(s)$ for every $s \geq t_j$,

(2) m_j is the dimension of the translate C_j and $a_{m_j} = 1/m_j!$.

Let $t^* := \max(t_1, \ldots, t_r)$ and m^* the maximal dimension of the translates $C_1, \ldots, C_r$. Obviously, for $s \geq t^*$ the function c is given by a polynomial of degree m^* and the coefficient of s^{m^*} in this polynomial is positive.

It remains to show that $m^* = \dim(I)$. Let $\{x_{i_1}, \ldots, x_{i_k}\} \in \Delta(I)$ be a set of independent variables modulo I. Obviously $[x_{i_1}, \ldots, x_{i_k}] \subseteq C(I)$. Hence, by Lemma 10.2.3, $k \leq m^*$. Since $\dim(I)$ is the maximal cardinality of any set of independent variables, we get $\dim(I) \leq m^*$. On the other hand, let the translate $\{u\} \cdot [x_{i_1}, \ldots, x_{i_k}]$ be a subset of $C(I)$. Since I is an ideal, we obtain $[x_{i_1}, \ldots, x_{i_k}] \subseteq C(I)$. By Theorem 10.1.2, $\{x_{i_1}, \ldots, x_{i_k}\} \in \Delta(I)$, and therefore $\dim(I) \geq m^*$. □

Our next goal is to generalize Theorem 10.2.4 to arbitrary ideals. The following crucial observation is due to Macaulay.

Theorem 10.2.5: *Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal and let $\prec$ be a graduated ordering on $[x_1, \ldots, x_n]$. Then the monomial ideal $J = I_\prec$ (the initial ideal) has the same Hilbert function as I.*

Proof: For a non–negative integer s let $[x_1, \ldots, x_n]_{\leq s}$ denote the set of power products of degree $\leq s$, and let

$$M_s := \{u \in [x_1, \ldots, x_n]_{\leq s} \mid u \in J\} \quad \text{and} \quad M'_s := \{u \in [x_1, \ldots, x_n]_{\leq s} \mid u \notin J\}.$$

$M_s \cup M'_s$ is a basis of the vector space $K[x_1, \ldots, x_n]_{\leq s}$. Theorem 10.1.2 implies that M_s is a basis of the vector space $J_{\leq s}$. So

$$HF_J(s) = \dim(K[x_1, \ldots, x_n]_{\leq s}) - \dim(J_{\leq s}) = |M'_s|.$$

Thus, for proving the theorem it suffices to show that M'_s (or, more precisely, the equivalence classes with representatives in M'_s) is a basis of the quotient space $K[x_1, \ldots, x_n]_{\leq s}/I_{\leq s}$.

Let $u_1, \ldots, u_r \in M'_s$ and $c_1, \ldots, c_r \in K$ such that $f := c_1 u_1 + \cdots + c_r u_r = 0$ in the quotient space. I.e. the polynomial f must be reducible to 0 modulo a Gröbner basis G of I w.r.t. $\prec$. However, f is already in normal form w.r.t. G. So we must have $f = 0$, i.e. $c_1 = \cdots = c_r = 0$. Hence, M'_s is linearly independent in the quotient space.

It remains to show that M'_s spans the quotient space. Let $g \in K[x_1, \ldots, x_n]_{\leq s}$ and g' its normal form modulo the Gröbner basis G. Since $\prec$ is graduated, g and g' represent the same equivalence class in the quotient space $K[x_1,\ldots,x_n]_{\leq s}/I_{\leq s}$. Obviously, g' can be written in the form $g' = c_1u_1 + \cdots + c_ru_r$ for some $u_1,\ldots,u_r \in M'_s$ and $c_1,\ldots,c_r \in K$. □

Corollary: *Let $I \subseteq K[x_1,\ldots,x_n]$ be an ideal. There exists a polynomial $h(x) \in \mathbb{Q}[x]$, such that for sufficiently large s we have $HF_I(s) = h(s)$.*

Proof: This is an immediate consequence of Theorems 10.2.4 and 10.2.5. □

Definition 10.2.3: Let $I \subseteq K[x_1,\ldots,x_n]$ be an ideal. The polynomial which equals $HF_I(s)$ for sufficiently large s is called the *(affine) Hilbert polynomial* of I, denoted by $HP_I(s)$. □

The smallest integer t such that $HF_I(s) = HP_I(s)$ for all $s \geq t$ is called the *index of regularity* of I. Determining the index of regularity is of considerable interest and importance in many computations with ideals, but we will not pursue this topic here.

Theorem 10.2.6: *Let $I \subset K[x_1,\ldots,x_n]$ be a proper ideal. Then* $\dim(I)$ *equals the degree of the Hilbert polynomial of I.*

Proof: Denote the dimension of I by d and let $\{x_{i_1},\ldots,x_{i_d}\}$ be an element of $\Delta(I)$ of maximal cardinality and s a non–negative integer. Then $[x_{i_1},\ldots,x_{i_d}]_{\leq s}$ (or, more precisely, the equivalence classes represented by these monomials) is a linearly independent subset of the quotient space $K[x_1,\ldots,x_n]_{\leq s}/I_{\leq s}$. By Lemma 10.2.2,

$$\binom{d+s}{s} \leq HF_I(s).$$

Since the above binomial coefficient is a polynomial function in s of degree d (see Lemma 10.2.3), the dimension of I is at most the degree of the Hilbert polynomial of I.

On the other hand, let $\prec$ be a graduated ordering on $[x_1,\ldots,x_n]$ and $I_\prec$ the initial ideal of I w.r.t. $\prec$. If a subset $X = \{x_{i_1},\ldots,x_{i_k}\}$ of $\{x_1,\ldots,x_n\}$ is not in $\Delta(I)$, then there exists a non–zero polynomial $f \in I \cap K[x_{i_1},\ldots,x_{i_k}]$. Hence, $\mathrm{lpp}(f) \in I_\prec \cap K[x_{i_1},\ldots,x_{i_k}]$ and $X \notin \Delta(I_\prec)$. It follows that $\Delta(I_\prec) \subseteq \Delta(I)$ and therefore $\dim(I_\prec) \leq \dim(I)$. By Theorems 10.2.4 and 10.2.5, the degree of the Hilbert polynomial of I is equal to $\dim(I_\prec)$. Therefore, the degree of the Hilbert polynomial is at most $\dim(I)$. □

Now we have compiled all the necessary prerequisites for proving Theorem 10.1.1 under the additional assumption, that $\prec$ is a graduated ordering.

Theorem 10.1.1: *Let $\prec$ be a graduated ordering on $[x_1,\ldots,x_n]$, I a proper ideal in $K[x_1,\ldots,x_n]$. Let X be an element of maximal cardinality in $\Delta(I_\prec)$. Then X is an element of maximal cardinality in $\Delta(I)$ and therefore*

$$\dim(I_\prec) \;=\; |X| \;=\; \dim(I).$$

Proof: Using Theorems 10.2.4, 10.2.5, and 10.2.6, we obtain

$$\begin{aligned}\dim(I_\prec) &= \deg(HP_{I_\prec}) \\ &= \deg(HP_I) \\ &= \dim(I).\end{aligned}$$

We still have to show that any maximal element in $\Delta(I_\prec)$ is also a maximal element in $\Delta(I)$. Clearly, $\Delta(I_\prec) \subseteq \Delta(I)$, since

$$\begin{array}{ccc} X \in \Delta(I_\prec) & & X \in \Delta(I) \\ \Updownarrow & & \Updownarrow \\ I_\prec \cap K[X] = \langle 0 \rangle & \Longrightarrow & I \cap K[X] = \langle 0 \rangle \end{array}$$

Therefore, if X is an element of maximal cardinality in $\Delta(I_\prec)$, then X must also be an element of maximal cardinality in $\Delta(I)$. □