INSTITUTO POLITÉCNICO NACIONAL
Escuela Superior de Física y Matemáticas

El Anillo de Coordenadas de subconjuntos del espacio proyectivo, su módulo canónico y códigos asociados

T E S I S
QUE PARA OBTENER EL GRADO DE
MAESTRO EN CIENCIAS

P R E S E N T A
CARLOS ALBERTO CASTILLO GUILLÉN

DIRECTOR DE TESIS
DR. CARLOS RENTERÍA MÁRQUEZ

MÉXICO, D. F. **SEPTIEMBRE DE 2011**

SIP-13

INSTITUTO POLITÉCNICO NACIONAL
SECRETARIA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REGISTRO DE TEMA DE TESIS
Y DESIGNACIÓN DE DIRECTOR DE TESIS

México, D.F. a 07 de Diciembre del 2010

El Colegio de Profesores de Estudios de Posgrado e Investigación de ESFM en su sesión Ordinaria No. 08 celebrada el día 16 del mes de Junio de 2010 conoció la solicitud presentada por el(la) alumno(a):

Castillo	Guillén	Carlos Alberto
Apellido paterno	Apellido materno	Nombre (s)

Con registro: B 0 2 1 1 9 7

Aspirante de: **Maestro en Ciencias en Matemáticas**

1.- Se designa al aspirante el tema de tesis titulado:
"El anillo de coordenadas de subconjuntos del espacio proyectivo, su módulo canónico y códigos asociados"

De manera general el tema abarcará los siguientes aspectos:

Se anexa hoja

2.- Se designa como Director de Tesis al Profesor:
Dr. Carlos Rentería Márquez

3.- El trabajo de investigación base para el desarrollo de la tesis será elaborado por el alumno en:
El Departamento de Matemáticas

que cuenta con los recursos e infraestructura necesarios.

4.- El interesado deberá asistir a los seminarios desarrollados en el área de adscripción del trabajo desde la fecha en que se suscribe la presente hasta la aceptación de la tesis por la Comisión Revisora correspondiente.

Director(a) de Tesis

Dr. Carlos Rentería Márquez

Aspirante

Carlos Castillo G.

Carlos Alberto Castillo Guillén

Presidente del Colegio

Dr. Miguel Tufiño Velázquez

SIP-14

INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad **México, D. F.,** siendo las **12:00** horas del día **07** del mes de **Diciembre** del **2010** se reunieron los miembros de la Comisión Revisora de Tesis, designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de **ESFM** para examinar la tesis titulada:

"El anillo de coordenadas de subconjuntos del espacio proyectivo, su módulo canónico y códigos asociados"

Presentada por el alumno:

Castillo	**Guillén**	**Carlos Alberto**
Apellido paterno	Apellido materno	Nombre(s)

Con registro:

B	0	2	1	1	9	7

aspirante de:

Maestro en Ciencias en Matemáticas

Después de intercambiar opiniones, los miembros de la Comisión manifestaron ***APROBAR LA DEFENSA DE LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Director(a) de tesis

Dr. Carlos Rentería Márquez

Dr. Egor Maximenko

Dr. Valeri Vladimirovich Kucherenko

Dra. María Elena Luna Elizarrarás

Dr. Manuel González Sarabia

PRESIDENTE DEL COLEGIO DE PROFESORES

Dr. Miguel Tufiño Velázquez

ESCUELA SUPERIOR DE FÍSICA Y MATEMÁTICAS I. P. N.

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de México el día 18 del mes Agosto del año 2011, el que suscribe Carlos Alberto Castillo Guillén alumno del Programa de Maestría en Matemáticas con número de registro B021197, adscrito a la Escuela Superior de Física y Matemáticas, manifiesta que es autor intelectual del presente trabajo de Tesis bajo la dirección del Dr. Carlos Rentería Márquez y cede los derechos del trabajo intitulado El anillo de coordenadas de subconjuntos del espacio proyectivo, su módulo canónico y códigos asociados, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección carlos_53@hotmail.com. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Carlos Castillo G.

Carlos Alberto Castillo Guillén

Nombre y firma

Resumen

En este trabajo se desarrollan y expanden conceptos básicos y avanzados del Algebra Conmutativa y el Algebra Homológica que permiten desarrollar la teoría de esquemas de Cayley-Bacharach con la finalidad de aplicarlos a la teoría de códigos algebro-geométricos, támbien llamados códigos de evaluación, damos ejemplos de algunos de estos y calculamos sus parámetros básicos.

Abstract

In this exposition we develop and expand basic and advanced concepts coming from conmutative algebra and homological algebra, this concepts allow us to develop the Cayley-Bacharach schemes theory, later on we applied all this concepts to the algebro-geometric codes we also give several examples of this codes and we compute its basic parameters.

Índice general

Introducción

Sea $\mathrm{k} = \mathbb{F}_q$ el campo finito con q elementos, sea $\mathrm{A} = \mathrm{k}[X_0, \ldots, X_n] = \oplus_{i \geq 0} \mathrm{A}_i$ el anillo de polinomios con la graduación natural, sea $\mathbb{P}^n(\mathrm{k})$ el n-espacio proyectivo, sea $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\} \subseteq \mathbb{P}^n(\mathrm{k})$ un conjunto finito de s puntos, sea $\mathrm{I}_\mathrm{X} = \oplus_{i \geq 0} \mathrm{I}_\mathrm{X}(i)$ el ideal de A generado por los polinomios homogéneos que se anulan en todos los puntos de X, y sea $\mathrm{R} = \mathrm{A}/\mathrm{I}_\mathrm{X}$ el anillo de coordenas de X.
La función de Hilbert de X es la función $\mathrm{H}_\mathrm{X} : \mathbb{Z}_{\geq 0} \to \mathbb{N}$ dada por $\mathrm{H}_\mathrm{X}(d) = \dim_\mathrm{k} \mathrm{R}_d$.
Si H_X es la función de Hilbert de un conjunto finito de puntos, entonces H_X tiene las siguientes caracteristicas.
Existe un entero a_X, llamado el a-invariante del ideal o el invariante de X, tal que:

(1) $\mathrm{H}_\mathrm{X}(d) = dim_k \mathrm{A}_d$ si y sólo si $d < \lambda_\mathrm{X}$.

(2) $\mathrm{H}_\mathrm{X}(d) < \mathrm{H}_\mathrm{X}(d+1) < s$ para $0 \leq d < a_\mathrm{X}$.

(3) $\mathrm{H}_\mathrm{X}(d) = s$ para $d > a_\mathrm{X}$.

La truncación de H_X, $Trunc(\mathrm{H}_\mathrm{X})$, está dada por

$$Trunc(\mathrm{H}_\mathrm{X})(d) = \begin{cases} \mathrm{H}_\mathrm{X}(d) & para \quad d \leq a_\mathrm{X} \\ s-1 & para \quad d > a_\mathrm{X} \end{cases}$$

Existen polinomios $\mathrm{F}_1, \ldots, \mathrm{F}_s \in \mathrm{A}_{a_\mathrm{X}+1}$ que satisfacen $\mathrm{F}_i(\mathrm{P}_j) = \delta_{ij}$, con los cuales se puede obtener una base para $\mathrm{R}_{a_\mathrm{X}+1}$, el polinomio F_i es llamado truncador de X hacia $\mathrm{X} \setminus \{\mathrm{P}_i\}$.
Un separador de X hacia $\mathrm{X} \setminus \{\mathrm{P}_i\}$ es un polinomio homogéneo, G, que satisface $\mathrm{G}(\mathrm{P}_i) \neq 0$ y $\mathrm{G}(\mathrm{P}_j) = 0$ para $j \neq i$, así, un truncador de X hacia $\mathrm{X} \setminus \{\mathrm{P}_i\}$ es un separador de X hacia $\mathrm{X} \setminus \{\mathrm{P}_i\}$.

El grado de P_i, $\deg(\mathrm{P}_i)$, es el menor entero para el cual hay un separador de X hacia $\mathrm{X} \setminus \{\mathrm{P}_i\}$ de grado $\deg(\mathrm{P}_i)$, así, $\deg(\mathrm{P}_i) \leq a_{\mathrm{X}} + 1$.
Si P_i es tal que $\deg(\mathrm{P}_i) = a_{\mathrm{X}} + 1$, entonces $\mathrm{H}_{\mathrm{X}\setminus\{\mathrm{P}_i\}} = Trunc(\mathrm{H}_{\mathrm{X}})$ (proposición 3.2.2). Un conjunto finito es llamado esquema de Cayley-Bacharach si todos sus puntos tienen grado $a_{\mathrm{X}} + 1$, por tanto, la función de Hilbert de cualquier conjunto de $s - 1$ puntos es igual a $Trunc(\mathrm{H}_{\mathrm{X}})$.

Un código algebraico sobre el campo finito $\mathrm{k} = \mathbb{F}_q$ es un subespacio lineal de $\mathbb{F}_q^s$. Para la obtención de códigos se usa un conjunto finito de puntos y la función evaluación. Es decir, si $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\} \subseteq \mathbb{P}^n(\mathrm{k})$, donde cada P_i es dado en representación estandar, y A_d es la componente d del anillo de polinomios, entonces el código $\mathrm{C}_{\mathrm{X}}(d)$ es la imagen de la transformación lineal

$$\begin{array}{rccc} ev & : & \mathrm{A}_d & \longrightarrow & \mathrm{k}^s \\ & & \mathrm{f} & \longmapsto & (\mathrm{f}(\mathrm{P}_1), \ldots, \mathrm{f}(\mathrm{P}_s)) \end{array}$$

El código $\mathrm{C}_{\mathrm{X}}(d)$ es isomorfo a R_d y la dimensión del código se obtiene de la función de Hilbert de X.
Otra manera de obtener códigos es usando un espacio vectorial V de dimensión s, $\{\alpha_1, \ldots, \alpha_s\}$ una base de V y τ un subespacio de funcionales sobre V. El código $\mathrm{C}(\tau)$ es la imagen de la transformación lineal

$$\begin{array}{rccc} \delta & : & \tau & \longrightarrow & \mathrm{k}^s \\ & & \varphi & \longmapsto & (\varphi(\alpha_1), \ldots, \varphi(\alpha_s)) \end{array}$$

es claro que δ es inyectiva. Por tanto, la dimensión del código es la dimensión de τ. Cuando se elije $\mathrm{V} = \mathrm{R}_{a_{\mathrm{X}}+1}$, $\{\mathrm{f}_1, \ldots, \mathrm{f}_s\}$ la base de truncadores, y a τ como el conjunto de funcionales que le corresponde a $(\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$ (porposición 3.3.4) se obtiene el código $\mathrm{C}_{a_{\mathrm{X}}}(\omega_{\mathrm{R}})$.

El contenido de esta tesis está conformado por cuatro capítulos. El capítulo 1 inicia con el concepto de longitud de un módulo, concepto que es en cierto modo una generalización de la dimensión de un espacio vectorial. Las extensiones enteras de anillos y la dimensión de Krull son considerados, pues es de nuestro interés la conservación de la dimensión de Krull ante extensiones enteras (proposción 1.2.1). Los ideales primos asociados son de interés, pues en algunos casos simplifican el estudio de un módulo al estudio de un anillo cociente (proposición 1.2.8 y lema 2.2.1). La dimensión proyectiva e inyectiva es considerada para el análisis de los módulos perfectos y el módulo canónico. Finalmente, la profundidad de un módulo es estudiada pues es

el concepto necesario para la definición de anillo y módulo de Cohen-Macaulay. Esto es hecho pues el anillo de coordenadas de un conjunto finito de puntos es un anillo graduado de Cohen-Macaulay.
En el capítulo 2 se desarrollan propiedades de los anillos y módulos graduados. La aplicación del teorema de Macaulay y las bases de Groebner nos permitirá calcular la función de Hilbert del anillo de coordenadas del espacio afín y el espacio proyectivo.
En el capítulo 3 se analizan los esquemas de Cayley-Bacharach, esto se hace analizando los conceptos de truncador, truncador fuerte, separador y el módulo canónico. Esto es desarrollado también por el uso que se le dará en la construcción de códigos.
Finalmente, en el capítulo 4 se presentan resultados generales para códigos algebraicos, $\mathrm{C_X}(d)$, para cuando X es el espacio afín y el espacio proyectivo, también se construye el código asociado al módulo canónico de R, $\mathrm{C}_{a_\mathrm{X}}(\mathrm{R})$, verificando la dualidad entre los códigos $\mathrm{C_X}(a_\mathrm{X})$ y $\mathrm{C}_{a_\mathrm{X}}(\mathrm{R})$.

Capítulo 1

Conceptos Fundamentales

Presentamos resultados generales que son la base para el resto de este trabajo. Siempre se supondrá que los anillos considerados son conmutativos, con identidad, noetherianos y que los A-módulos son finitamente generados.

1.1. Longitud de Módulos y Extensiones Enteras de Anillos

Definición 1.1.1 *Sean* A *un anillo y* M *un* A*-módulo.*

(*1*) *Una* ***cadena*** *de submódulos de* M *es una secuencia de submódulos de* M *de la forma:*

$$\langle 0\rangle = \mathrm{M}_r \subset \mathrm{M}_{r-1} \subset \ldots \subset \mathrm{M}_1 \subset \mathrm{M}_0 = \mathrm{M}$$

Decimos que la cadena tiene longitud r*.*

(*2*) *Una cadena de submódulos es llamada* ***serie de composición*** *si cada* $\mathrm{M}_i/\mathrm{M}_{i+1}$ *es un módulo simple (es decir, no hay submódulos entre* M_i *y* M_{i+1} *distintos de* M_i *y* M_{i+1}*).*

Lema 1.1.1 *Sean* A *un anillo,* M *un* A*-módulo,* $\mathrm{M}_r \subset \mathrm{M}_{r-1} \subset \cdots \subset \mathrm{M}_1 \subset \mathrm{M}_0$ *una serie de composición de* M *de longitud* r *y* N *un submódulo de* M*. Entonces:*

(*1*) *Si* $\langle 0\rangle = \mathrm{M}_r \cap \mathrm{N} \subseteq \mathrm{M}_{r-1} \cap \mathrm{N} \subseteq \ldots \subseteq \mathrm{M}_1 \cap \mathrm{N} \subseteq \mathrm{M}_0 \cap \mathrm{N} = \mathrm{N}$ *es la sucesión de submódulos que se obtiene con la intersección de* N *y cada submódulo de la serie de composición, entonces:*

(*i*) $M_i \cap N = M_{i+1} \cap N$ *ó*

(*ii*) $(M_i \cap N / M_{i+1} \cap N)$ *es un módulo simple y* $M_i \cap N + M_{i+1} = M_i$.

(*2*) *Si* $M_i \cap N + M_{i+1} = M_i$ *para toda* $i = 0, \ldots, r-1$, *entonces* $M_i \subseteq N$ *para toda* $i = 0, \ldots, r$.

Demostración.

(1) Por el segundo teorema de isomorfismos, se tiene:
$(M_i \cap N)/(M_{i+1} \cap N) \cong (M_i \cap N + M_{i+1})/M_{i+1} \subseteq M_i/M_{i+1}$, y como M_i/M_{i+1} es un módulo simple, entonces:

(i) $(M_i \cap N)/(M_{i+1} \cap N) = 0$ ó

(ii) $(M_i \cap N)/(M_{i+1} \cap N) \cong (M_i \cap N + M_{i+1})/M_{i+1} = M_i/M_{i+1}$ es un módulo simple con $M_i \cap N + M_{i+1} = M_i$

(2) Se mostrará usando inducción sobre i $(0 \leq i \leq r)$ que $M_{r-i} \subseteq N$.
Notemos que $M_r = \langle 0 \rangle \subseteq N$, con lo cual el caso $i = 0$ es cierto. Supongamos que para algún i se tiene $M_{r-i} \subseteq N$, ahora como $M_i \cap N + M_{i+1} = M_i$ $(0 \leq i < r)$, entonces en particular $N \cap M_{r-i-1} + M_{r-i} = M_{r-i-1}$, con $N \cap M_{r-i-1} \subseteq N$ y $M_{r-i} \subseteq N$ por hipótesis inductiva. Por lo tanto $M_{r-i-1} = M_{r-(i+1)} \subseteq N$.

Proposición 1.1.1 *Sean* A *un anillo y* M *un* A*-módulo. Si* M *tiene una serie de composición finita de longitud* r, *entonces cualquier cadena de submódulos de* M *tiene longitud menor o igual a* r.
Debido a esto, cualquier serie de composición de M *tiene la misma longitud.*

Demostración.
La prueba es por inducción sobre r. Si $r = 0$, entonces $M = 0$; si $r = 1$, entonces M es simple y la única cadena de submódulos de M es $< 0 >= M_0 \subset M_1 = M$, así la afirmación en cierta.
Supongamos ahora que los módulos con una serie de composición finita de longitud $r-1$ tienen cualquier cadena de submódulos de longitud menor o igual a $r-1$; y sean M un A-módulo, $\langle 0 \rangle = M_r \subset M_{r-1} \subset \ldots \subset M_1 \subset M_0 = M$ una serie de composición de M de longitud r y $\langle 0 \rangle = M_p^* \subset M_{p-1}^* \subset \ldots \subset M_1^* \subset M_0^* = M$ cualquier cadena de submódulos de M.
Considerar la sucesión de submódulos de M_1^* que se obtiene al intersectar los submódulos de la serie de composición de M con M_1^*,$\langle 0 \rangle = M_r \cap M_1^* \subset M_{r-1} \cap M_1^* \subset \ldots \subset$

$M_1 \cap M_1^* \subset M_0 \cap M_1^* = M_1^*$, entonces por el lema 1.1.1 no puede ocurrir que para todo $i = 1, \ldots, r$ los módulos $(M_i \cap M_1^*)/(M_{i+1} \cap M_1^*)$ sean simples, pues si así fuera, entonces $M_i \cap M_1^* + M_{i+1} = M_i$ para toda $i = 0, \ldots, r-1$, y así $M_i \subseteq M_1^*$ para toda $i = 0, \ldots, r$, de donde se obtendría $M = M_0 \subseteq M_1^*$ lo cual es absurdo. Entonces por el lema 1.1.1 se debe tener $M_i \cap M_1^* = M_{i+1} \cap M_1^*$ para algunos indices, y después de renombrar se tiene que $\langle 0 \rangle = M_{i_k} \cap M_1^* \subset M_{i_{k-1}} \cap M_1^* \subset \ldots \subset M_{i_1} \cap M_1^* \subset M_1^*$ es una serie de composición de M_1^* de longitud menor que r. Luego por hipótesis de inducción se tiene $p - 1 \leq i_k < r$, y así $p \leq r$.

DEFINICIÓN 1.1.2 *Sean* A *un anillo y* M *un* A*-módulo. La* ***longitud*** *del módulo* M*,* $\ell(M)$*, es la longitud de una serie de composición de* M*.*

Dado que la longitud de cualquier serie de composición de un módulo es la misma, entonces la longitud de un módulo está bien definida.

LEMA 1.1.2 *Sean* A *un anillo,* M *y* N A*-módulos de longitud finita, entonces:*

(*i*) $M \times N$ *es un* A*-módulo de longitud finita y* $\ell(M \times N) = \ell(M) + \ell(N)$*.*

(*ii*) *Si* L *es un submódulo de* M*, entonces* L *y* M/L *son* A*-módulos de longitud finita con* $\ell(M) = \ell(L) + \ell(M/L)$*.*

Demostración.

(i) Si $\langle 0 \rangle = M_r \subset M_{r-1} \subset \ldots \subset M_1 \subset M$ y $< 0 >= N_p \subset N_{p-1} \subset \ldots \subset N_1 \subset N$ son series de composición de M y N respectivamente. Entonces: $M_r \times \{0\} \subset M_{r-1} \times \{0\} \subset \ldots \subset M_1 \times \{0\} \subset M \times \{0\} \subset M \times N_{p-1} \subset \ldots \subset M \times N_1 \subset M \times N$ es una serie de composición de $M \times N$, pues $(M_i \times \{0\})/(M_{i-1} \times \{0\}) \cong M_i/M_{i-1}$ y $(M \times N_i)/(M \times N_{i-1}) \cong N_i/N_{i-1}$ son módulos simples, con lo cual se tiene el resultado.

(ii) Si $\langle 0 \rangle = L_r \subset L_{r-1} \subset \ldots \subset L_1 \subset L$ y $\langle 0 \rangle = H_p/L \subset H_{p-1}/L \subset \ldots \subset H_1/L \subset M/L$ son cadenas finitas de submódulos de L y M/L respectivamente, donde $L = H_p \subset H_{p-1} \subset \ldots \subset H_2 \subset H_1$, entonces: $\langle 0 \rangle = L_r \subset L_{r-1} \subset \ldots \subset L_1 \subset L \subset H_{p-1} \subset \ldots \subset H_2 \subset H_1 \subset M$ es una cadena finita de submódulos de M. Así, por la proposición 1.1.1 se tiene $r + p \leq \ell(M)$, y como la desigualdad es cierta para cualquier cadena finita de submódulos de L y M/L se concluye que L y M/L son A-módulos de longitud finita.

Es claro que si las cadenas de submódulos de L y M/L consideradas son series de composición, entonces la cadena de submódulos de M construida será también una serie de composición. Con lo cual se obtiene que $\ell(\mathrm{M}) = \ell(\mathrm{L}) + \ell(\mathrm{M/L})$.

DEFINICIÓN 1.1.3 *Sea* A *un subanillo de un anillo* B.

(*1*) *Un elemento* $b \in \mathrm{B}$ *se dice entero sobre* A *si existe un polinomio* $f(X) = X^n + a_1X^{n-1} + \ldots + a_n \in \mathrm{A}[X]$ *tal que* $f(b) = 0$.

(*2*) *Se dice que* B ***es entero sobre*** A *si todo elemento de* B *es entero sobre* A.

EJEMPLO 1.1.1 *Sean* $\mathrm{A} = \mathbb{Z}$ *y* $\mathrm{B} = \mathbb{Z}[\sqrt{2}\,] = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Z}\}$. *Se tienen las siguientes propiedades:*

(*1*) A *es subanillo de* B.

(*2*) *Si* $\alpha = a + b\sqrt{2} \in \mathrm{B}$, *entonces* α *satisface el polinomio* $f(X) = X^2 - 2aX + a^2 - 2b^2 \in \mathbb{Z}[X]$.

(*3*) $\mathbb{Z}[\sqrt{2}\,]$ *es entero sobre* $\mathbb{Z}$.

La siguiente proposición no está acompañada de una demostración, su demostración la podemos encontrar en [10].

PROPOSICIÓN 1.1.2 *Sean* A *un subanillo de un anillo* B *y* $\alpha \in \mathrm{B}$. *Las siguientes condiciones son equivalentes:*

(*1*) α *es entero sobre* A*;*

(*2*) $\mathrm{A}[\alpha]$ *es* A*-módulo finitamente generado;*

(*3*) *Existe un* A*-módulo* C *tal que* $\mathrm{A}[\alpha] \subseteq \mathrm{C}$ *y* C *es* A*-módulo finitamente generado.*

Así, si B *es* A*-módulo finitamente generado, entonces* B *es entero sobre* A.

1.2. Dimensión de Krull e Ideales Primos Asociados

DEFINICIÓN 1.2.1 *Sea* A *un anillo. El espectro de* A, Spec(A), *es el conjunto de los ideales primos de* A.

EJEMPLO 1.2.1 *Se presentan ejemplos de espectros de algunos anillos.*
(**1**) *Sean* k *un campo y* $\mathrm{A} = \mathrm{k}[X]$ *el anillo de polinomios en una variable sobre* k*, entonces:*

$$\mathrm{Spec(A)} = \{\langle f(X)\rangle \ : \ f(X) \ \text{ es polinomio irreducible}\} \cup \{\langle 0\rangle\}$$

(**2**) *Sean* k *un campo algebraicamente cerrado y* $\mathrm{A} = \mathrm{k}[X]$ *el anillo de polinomios en una variable sobre* k*, entonces:*

$$\mathrm{Spec(A)} = \{\langle X - \alpha\rangle \ : \ \alpha \in \mathrm{k}\} \cup \{\langle 0\rangle\}$$

(**3**) *Sea* $\mathrm{A} = \mathbb{Z}$*, entonces:*

$$\mathrm{Spec}(\mathbb{Z}) = \{\langle p\rangle \ : \ \mathrm{p} \quad es \quad número \quad primo\} \ \cup \{\langle 0\rangle\}$$

(**4**) *Sean* k *un campo algebraicamente cerrado y* $\mathrm{A} = \mathrm{k}[X, Y]$ *el anillo de polinomios en dos variables, entonces:*

$$\mathrm{Spec(A)} \ = \{\langle X - \alpha, Y - \beta\rangle \ : \ \alpha, \beta \in \mathrm{k}\} \cup \{\langle \mathrm{f}\rangle : \mathrm{f \text{ es polinomio irreducible }}\} \cup \{\langle 0\rangle\}$$

Las afirmaciones (1), (2) y (3) son triviales, por ello únicamente se demostrará (4).
Demostración.
Los ideales de la parte derecha de la igualdad son ideales primos. Por lo tanto, lo que resta verificar es que los ideales primos no cero y no principales son de la forma $\mathrm{P} = \langle X - \alpha, Y - \beta\rangle$.
Sea P un ideal primo no cero y no principal y sea $\mathrm{f}_1 \in \mathrm{P}$ de grado mínimo en Y. Puesto que f_1 se expresa como producto de polinomios irreducibles, se sigue que existe $\mathrm{f} \in \mathrm{P}$ de grado mínimo en Y y que es polinomio irreducible. Sea $\mathrm{g} \in \mathrm{P} \setminus \langle \mathrm{f}\rangle$, pues $\mathrm{P} \setminus \langle \mathrm{f}\rangle \neq \emptyset$, entonces $\mathrm{g} = \mathrm{fq} + \mathrm{r}$, donde $\mathrm{q}, \mathrm{r} \in \mathrm{k}(X)[Y]$ (q y r son polinomios en Y con coeficientes en $\mathrm{k}(X)$), y $\mathrm{r} = 0$ ó $\deg_Y \mathrm{r} < \deg_Y \mathrm{f}$, por el algoritmo de la división en $\mathrm{k}(X)[Y]$. Quitando denominador a q y r, en la igualdad anterior, se obtiene $\mathrm{pg} = \mathrm{fq}_1 + \mathrm{r}_1$, donde $\mathrm{p} \in \mathrm{k}[X]$, $\mathrm{q}_1, \mathrm{r}_1 \in \mathrm{k}[X, Y]$ y $\mathrm{r}_1 = 0$ ó $\deg_Y \mathrm{r}_1 = \deg_Y \mathrm{r} < \deg_Y \mathrm{f}$. Puesto que $\mathrm{r}_1 = \mathrm{pg} - \mathrm{fq}_1 \in \mathrm{P}$, $\deg_Y \mathrm{r}_1 < \deg_Y \mathrm{f}$ y f es de grado mínimo en P, se sigue que $\mathrm{r}_1 = 0$. Así, $\mathrm{pg} = \mathrm{fq}_1 \in \langle \mathrm{f}\rangle$.
Por otra parte, $\langle \mathrm{f}\rangle$ es un ideal primo, pues f es irreducible.
Puesto que $\mathrm{pg} = \mathrm{fq}_1 \in \langle \mathrm{f}\rangle$ y $\mathrm{g} \notin \langle \mathrm{f}\rangle$, se sigue que $\mathrm{p} \in \langle \mathrm{f}\rangle$. Por tanto, $\deg_Y \mathrm{f} \leq \deg_Y \mathrm{p} = 0$, es decir, $\mathrm{f} \in \mathrm{k}[X]$. Por tanto, $\mathrm{f} \in \mathrm{k}[X]$ es de grado 1, pues f es irreducible y k es algebraicamente cerrado. Por lo tanto, P contiene un polinomio de la forma $X - \alpha$, con $\alpha \in \mathrm{k}$.
Se concluye que P contiene un ideal de la forma $\langle X - \alpha, Y - \beta\rangle$, con el mismo

procedimiento pero tomando a X por Y. Por lo tanto, $\mathrm{P} = \langle X - \alpha, Y - \beta \rangle$, pues $\langle X - \alpha, Y - \beta \rangle$ es ideal maximal.

DEFINICIÓN 1.2.2 *Sean* A *un anillo y* M *un* A*-módulo.*

(*1*) *Una sucesión de* $r+1$ *ideales primos* $\mathrm{p}_r \subset \ldots \subset \mathrm{p}_0$ *es llamada cadena de ideales primos de longitud* r*.*

(*2*) *Si* P *es un ideal primo de* A*. El peso de* P*,* $\mathrm{ht}(\mathrm{P})$*, es el supremo de las longitudes de cadenas de ideales primos con* $\mathrm{P} = \mathrm{P}_0$*.*

(*3*) *La dimensión de Krull de* A*,* $\dim(\mathrm{A})$*, es el supremo de los pesos de los ideales primos de* A*, es decir:*

$$\dim(\mathrm{A}) = \sup\{\mathrm{ht}(\mathrm{P}) \ : \ \mathrm{P} \in \mathrm{SpecA}\}.$$

(*4*) *La dimensión de Krull del módulo* M*,* $\dim(\mathrm{M})$*, es la dimensión de Krull del anillo* $\mathrm{A}/\mathrm{Ann}(\mathrm{M})$*.*

EJEMPLO 1.2.2 (*1*) *Sea* $\mathrm{A} = \mathbb{Z}$*. Entonces* $\langle 0 \rangle \subset \langle p \rangle$ *es una cadena de ideales primos de longitud* 1*, y* $\mathbb{Z}$ *únicamente tiene cadenas de ideales primos de longitud* 0 *y* 1*. Con lo cual* $\dim \mathbb{Z} = 1$*.*

(*2*) *Sea* k *un campo y* $\mathrm{R} = \mathrm{k}[X]$ *el anillo de polinomios en una variable sobre* k*. Entonces* $\langle 0 \rangle \subset \langle p(X) \rangle$ *es una cadena de ideales primos de longitud* 1*, y* $\mathrm{k}[X]$ *únicamente tiene cadenas de ideales primos de longitud* 0 *y* 1*. Con lo cual* $\dim \mathrm{k}[X] = 1$*.*

(*3*) *Sean* k *un campo algebraicamente cerrado y* $\mathrm{R} = \mathrm{k}[X, Y]$ *el anillo de polinomios en dos variables. Entonces* $\langle 0 \rangle \subset \langle X - \alpha \rangle \subset \langle X - \alpha, Y - \beta \rangle$ *es una cadena de ideales primos de longitud* 2*, y* $\mathrm{k}[X, Y]$ *únicamente tiene cadenas de ideales primos de longitud* $0, 1$ *y* 2 *(ejemplo1.2.1. (4)). Con lo cual* $\dim \mathrm{k}[X, Y] = 2$*.*

(*4*) *Sea* $\mathrm{A} = \mathrm{k}[X_0, \ldots, X_n]$ *el anillo de polinomios, entonces:*
$\langle X_0 \rangle \subset \langle X_0, X_1 \rangle \subset \ldots \subset \langle X_0, X_1, \ldots, X_n \rangle$ *es una cadena de ideales primos de longitud* $n + 1$*.*

Los resultados que mencionaremos a continuación no estarán acompañados de una demostración, sus demostraciones las podemos encontrar en [5].

Teorema 1.2.1 *Sean* A *un anillo semilocal noetheriano,* M *un* A*-módulo f.g. y* $\mathrm{rad}A = \mu$ *(la intersección de todos los ideales maximales de* A*). Entonces:*

$$\dim \mathrm{M} = \mathrm{mín}\{r \mid \exists\ (x_1, \ldots, x_r) \in \mu^r,\ \text{con}\ \ \ell(\mathrm{M}/x_1\mathrm{M} + \ldots + x_r\mathrm{M}) \ < \ \infty\}$$

Proposición 1.2.1 *Sean* A *y* B *anillos noetherianos. Si* B *es una extensión entera de* A*, entonces* $\dim \mathrm{A} = \dim \mathrm{B}$.
En particular, si B *es* A*-módulo finitamente generado, entonces* $\dim \mathrm{A} = \dim \mathrm{B}$.

Proposición 1.2.2 *Sea* A *un anillo,* $\mathrm{A} \neq 0$*. Entonces las siguientes condiciones son equivalentes.*

(*1*) A *es Artineano;*

(*2*) A *es Noetheriano y tiene dimensión de Krull igual a cero;*

(*3*) *La longitud de* A *como* A*-módulo es finita.*

Definición 1.2.3 *Sean* A *un anillo y* M *un* A*-módulo. Se dice que* $\mathrm{p} \in \mathrm{spec(A)}$ *es primo asociado de* M *si* p *es el anulador de algún elemento de* M*, es decir, si existe* $m \in \mathrm{M}$ *tal que:*

$$\mathrm{p} = \mathrm{Ann_A}(m) = \{a \in \mathrm{A} \ : \ a * m = 0\}$$

El conjunto de ideales primos de A *que son primos asociados de* M *se denota por* $\mathrm{Ass_A(M)}$

Ejemplo 1.2.3 *Sea* $\mathrm{A} = \mathbb{Z}$ *y sea* $n \in \mathbb{Z}$ *tal que* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ *(la factorización en números primos). Entonces:*

$$\mathrm{Ass}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}) = \{p_i\mathbb{Z} \ : \ 1 \leq i \leq r\}$$

Demostración.
Sea $\mathrm{q} \in \mathrm{Ass}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z})$ y sea $m \in \mathbb{Z}$ tal que $\mathrm{Ann}_{\mathbb{Z}}(\tilde{m}) = \mathrm{q}$. Entonces $n \nmid m$, existe q un número primo tal que $\mathrm{q} = q\mathbb{Z}$, y existe $s \in \mathbb{Z}$ tal que $qm = ns$. Supóngase que $q \nmid n$, entonces $q|s$, es decir, $s = qr$. Puesto que $qm = ns = nqr$, se sigue que $n|m$, lo cual es una contradicción. Así, q divide a n. Por tanto, $q = p_i$, para algún i. Por lo tanto, $\mathrm{Ass}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}) \subseteq \{p_i\mathbb{Z} \ : \ 1 \leq i \leq r\}$.
Por otra parte, sea $m = p_1^{\alpha_1} \cdots p_i^{\alpha_i - 1} \cdots p_r^{\alpha_r} = \frac{n}{p_i}$, entonces $\tilde{m} = m + n\mathbb{Z} \neq \tilde{0} = n\mathbb{Z}$. Afirmamos que $\mathrm{Ann}_{\mathbb{Z}}(\tilde{m}) = p_i\mathbb{Z}$. En efecto, sea $x \in \mathrm{Ann}_{\mathbb{Z}}(\tilde{m})$, puesto que $xm = x\frac{n}{p_i} = ns$, se sigue que $x \in p_i\mathbb{Z}$. Por tanto, $\mathrm{Ann}(\tilde{m}) \subseteq p_i\mathbb{Z}$. Puesto que $p_i m = n \in n\mathbb{Z}$, se sigue que $p_i\mathbb{Z} \subseteq \mathrm{Ann}(\tilde{m})$. De donde se obtiene la afirmación.
Por tanto, $p_i\mathbb{Z} = \mathrm{Ann}_{\mathbb{Z}}(\tilde{m}) \in \mathrm{Ass}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z})$. Por lo tanto, $\{p_i\mathbb{Z} \ : \ 1 \leq i \leq r\} \subseteq \mathrm{Ass}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z})$, de donde se sigue el resultado.

PROPOSICIÓN 1.2.3 *Sean* A *un anillo y* M *un* A*-módulo. Se tienen las siguientes propiedades:*

(*1*) *Si* p *es un elemento maximal de la familia de ideales* $\{\mathrm{Ann}(m) \ : \ m \in \mathrm{M}\setminus\{0\}\}$*, entonces* $\mathrm{p} \in \mathrm{Ass_A(M)}$.

(*2*) $\mathrm{Ass_A(M)} = \emptyset$ *si y sólo si* $\mathrm{M} = 0$.

(*3*) *Si* $\mathrm{p} \in \mathrm{spec(A)}$*, entonces* p *es primo asociado de* M *si y sólo si* M *contiene un submódulo isomorfo a* A/p.

Demostración.
(**1**) Sea p un elemento maximal de la familia de ideales $\{\mathrm{Ann}(m) \ : \ m \in \mathrm{M} \setminus \{0\}\}$, entonces $\mathrm{p} = \mathrm{Ann}(m)$. Resta verificar que p es un ideal primo, para esto supongamos que $ab \in \mathrm{p}$ y $a \notin \mathrm{p}$. Se tiene $ab * m = 0$, $a * m \neq 0$ y como $\mathrm{Ann}(m) \subseteq \mathrm{Ann}(am)$, con $\mathrm{Ann}(m)$ maximal, entonces $\mathrm{Ann}(m) = \mathrm{Ann}(am)$. Así, $b \in \mathrm{Ann}(am) = \mathrm{Ann}(m) = \mathrm{p}$, que es lo que se esperaba.

(**2**) Se sigue de (1)

(**3**) Supongamos que p es ideal primo asociado. Sea $m \in \mathrm{M}$ tal que $\mathrm{p} = \mathrm{Ann}(m)$, considerar $\psi : \mathrm{A} \longrightarrow \mathrm{M}$ tal que $\psi(r) = r * m$. Se tiene que $\ker\psi = \mathrm{p}$ y por el primer teorema de isomorfismos $\mathrm{A/p} = \mathrm{A}/\ker\psi \cong \mathrm{Im}\psi \subseteq \mathrm{M}$. Por tanto, el submódulo buscado es $\mathrm{Im}\psi = \{r * m \ : \ r \in \mathrm{A}\}$.
Si M contiene un submódulo isomorfo a A/p. Sea N tal submódulo, $\psi : \mathrm{A/p} \longrightarrow \mathrm{N}$ el isomorfismo y pongamos $\psi(\tilde{1}) = n \in \mathrm{N}$. Es claro que $\mathrm{Ann}(n) = \mathrm{p}$. Por lo tanto, p es ideal primo asociado de M.

PROPOSICIÓN 1.2.4 *Sean* A *un anillo y* p *un ideal primo de* A*, entonces:*

$$\mathrm{Ass_A(A/p)} = \{\mathrm{p}\}$$

Demostración.
Como $\mathrm{p} = \mathrm{Ann}(\tilde{1})$, entonces $\{\mathrm{p}\} \subseteq \mathrm{Ass_A(A/p)}$.
Ahora, sean $\mathrm{q} \in \mathrm{Ass(A/p)}$ y $a \in \mathrm{A} \setminus \mathrm{p}$, $\mathrm{q} = \mathrm{Ann}(\tilde{a})$. Como p es ideal primo, $a \notin \mathrm{p}$ y $qa \in \mathrm{p}$ para todo $q \in \mathrm{q}$, entonces $q \in \mathrm{p}$ para todo $q \in \mathrm{q}$. Así, $\mathrm{q} \subseteq \mathrm{p}$ y como $\mathrm{p} \subseteq \mathrm{Ann}(\tilde{a}) = \mathrm{q}$, entonces $\mathrm{q} = \mathrm{p}$. Con lo cual se obtiene la afirmación.

PROPOSICIÓN 1.2.5 *Sean* A *un anillo y* M *un* A*-módulo. Entonces existe una cadena de submódulos de* M

$$\langle 0\rangle = \mathrm{M}_0 \subset \mathrm{M}_1 \subset \mathrm{M}_2 \subset \ldots \subset \mathrm{M}_r = \mathrm{M}$$

Tal que $\mathrm{M}_{i+1}/\mathrm{M}_i \cong \mathrm{A}/\mathrm{p}_i$*, con* $\mathrm{p}_i \in \mathrm{Spec(A)}$.

Demostración.
Supongamos que $\mathrm{M} \neq \langle 0\rangle$ y pongamos $\mathrm{M}_0 = \langle 0\rangle$. Sea M_1 el submódulo de M que es isomorfo a A/p_1, con $\mathrm{p}_1 \in \mathrm{Ass_A(M)} \subseteq \mathrm{Spec(A)}$, el cual existe según la proposición.1.2.3. Si $\mathrm{M}_1 \neq \mathrm{M}$, sea M_2 el submódulo de M que contiene a M_1 y tal que el submódulo $\mathrm{M}_2/\mathrm{M}_1$ de M/M_1 es isomorfo a A/p_2, con $\mathrm{p}_2 \in \mathrm{Ass_A(M/M_1)} \subseteq \mathrm{Spec(A)}$, el cual existe según la proposición 1.2.3. Si $\mathrm{M}_2 \neq \mathrm{M}$, sea M_3 el submódulo de M que contiene a M_2 y tal que el submódulo $\mathrm{M}_3/\mathrm{M}_2$ de M/M_2 es isomorfo a A/p_3, con $\mathrm{p}_3 \in \mathrm{Ass_A(M/M_2)} \subseteq \mathrm{Spec(A)}$, el cual existe según la proposición 1.2.3.
Continuando de esta manera se obtiene una sucesión creciente de submódulos de M que termina con $\mathrm{M}_r = \mathrm{M}$ (pues M es noetheriano) y que cumple la condición deseada.

LEMA 1.2.1 *Sean* A *un anillo,* M *un* A*-módulo,* $\mathrm{p} \in \mathrm{Ass_A(M)}$*,* $a \in \mathrm{A} \setminus \mathrm{p}$ *y* $m \in \mathrm{M}$*. Supongamos que* $\mathrm{p} = \mathrm{Ann}(m)$*, entonces:*

$$\mathrm{Ann}(a * m) = \mathrm{Ann}(m) = \mathrm{p}$$

Demostración.
Sea $x \in \mathrm{Ann}(a*m)$, entonces $x*(a*m) = (xa)*m = 0$. Así, $xa \in \mathrm{Ann}(m) = \mathrm{p}$, luego $x \in \mathrm{p} = \mathrm{Ann}(m)$ (pues $a \notin \mathrm{p}$ y p es ideal primo). Por lo tanto, $\mathrm{Ann}(a*m) \subseteq \mathrm{Ann}(m)$. Como siempre se tiene $\mathrm{Ann}(m) \subseteq \mathrm{Ann}(a*m)$, entonces se tiene la igualdad esperada.

PROPOSICIÓN 1.2.6 *Sean* A *un anillo,* M *y* K A*-módulos, y* N *un submódulo de* M*. Supongamos que* $\mathrm{M/N} \subseteq \mathrm{K}$*, entonces:*

$$\mathrm{Ass_A(M)} \subseteq \mathrm{Ass_A(N)} \cup \mathrm{Ass_A(K)}$$

Demostración.
Sea $\mathrm{p} \in \mathrm{Ass_A(M)}$, y sea $m \in \mathrm{M}$ tal que $\mathrm{p} = \mathrm{Ann}(m)$. Se analizan dos casos:

(i) Si $\mathrm{N} \cap \langle m\rangle \neq \langle 0\rangle$. Sea $a \in \mathrm{A} \setminus \mathrm{p}$ tal que $a * m \in \mathrm{N}$; entonces, por el lema 1.2.1, $\mathrm{Ann}(a * m) = \mathrm{Ann}(m) = \mathrm{p} \in \mathrm{Ass_A(N)}$.

(ii) Si $\mathrm{N} \cap \langle m\rangle = \langle 0\rangle$. Afirmamos que $\tilde{m} = m + \mathrm{N} \in \mathrm{M/N} \subseteq \mathrm{K}$ es tal que $\mathrm{Ann}(\tilde{m}) = \mathrm{p}$, con lo cual se obtiene que $\mathrm{Ann}(\tilde{m}) = \mathrm{p} \in \mathrm{Ass_A(K)}$.
En efecto, sea $x \in \mathrm{Ann}(\tilde{m})$, entonces $x * \tilde{m} = \tilde{0}$, es decir $x * m \in \mathrm{N}$, y por lo

tanto $x * m = 0$. Así, $x \in \mathrm{p}$ y $\mathrm{Ann}(\tilde{m}) \subseteq \mathrm{p}$.
Sea $x \in \mathrm{p}$, entonces $x * m = 0$, por lo tanto $x * \tilde{m} = \tilde{0}$, luego $x \in \mathrm{Ann}(\tilde{m})$. Así, $\mathrm{p} \subseteq \mathrm{Ann}(\tilde{m})$.

PROPOSICIÓN 1.2.7 *Sean* A *un anillo y* M *un* A*-módulo. Entonces* Ass(M) *es un conjunto finito.*

Demostración.
Sea $\langle 0\rangle = \mathrm{M}_0 \subset \mathrm{M}_1 \subset \mathrm{M}_2 \subset \cdots \subset \mathrm{M}_{r-1} \subset \mathrm{M}_r = \mathrm{M}$ la sucesión de submódulos de M de la proposición 1.2.5, donde $\mathrm{M}_{i+1}/\mathrm{M}_i \cong \mathrm{A}/\mathrm{p}_i$ para algún $\mathrm{p}_i \in \mathrm{Spec(A)}$. Por la proposición 1.2.6, se tiene:

$$\mathrm{Ass(M)} \subseteq \mathrm{Ass}(\mathrm{M}_{r-1}) \cup \mathrm{Ass}(\mathrm{M}/\mathrm{M}_{r-1}) = \mathrm{Ass}(\mathrm{M}_{r-1}) \cup \mathrm{Ass}(\mathrm{A}/\mathrm{p}_{r-1}).$$

Con los mismos argumentos, usando la sucesión de módulos $\langle 0\rangle = \mathrm{M}_0 \subset \mathrm{M}_1 \subset \mathrm{M}_2 \subset \ldots \subset \mathrm{M}_{r-1}$, obtenemos:

$$\mathrm{Ass}(\mathrm{M}_{r-1}) \subseteq \mathrm{Ass}(\mathrm{M}_{r-2}) \cup \mathrm{Ass}(\mathrm{M}_{r-1}/\mathrm{M}_{r-2}) = \mathrm{Ass}(\mathrm{M}_{r-2}) \cup \mathrm{Ass}(\mathrm{A}/\mathrm{p}_{r-2}).$$

Continuando de esta manera, usando la sucesión de módulos $\langle 0\rangle = \mathrm{M}_0 \subset \mathrm{M}_1 \subset \cdots \subset \mathrm{M}_{i-1} \subset \mathrm{M}_i$, $i \in \{1, \ldots, r\}$, se obtiene:

$$\mathrm{Ass}(\mathrm{M}_i) \subseteq \mathrm{Ass}(\mathrm{M}_{i-1}) \cup \mathrm{Ass}(\mathrm{M}_i/\mathrm{M}_{i-1}) = \mathrm{Ass}(\mathrm{M}_{i-1}) \cup \mathrm{Ass}(\mathrm{A}/\mathrm{p}_{i-1}).$$

Así, usando las relaciones anteriores y la proposición 1.2.4, se obtiene:

$$\mathrm{Ass(M)} \subseteq \mathrm{Ass}(\mathrm{A}/\mathrm{p}_1) \cup \mathrm{Ass}(\mathrm{A}/\mathrm{p}_2) \cup \ldots \cup \mathrm{Ass}(\mathrm{A}/\mathrm{p}_r) = \{\mathrm{p}_1, \mathrm{p}_2, \ldots \mathrm{p}_r\}.$$

El resultado que mencionaremos a continuación no está acompañado de una demostración, su demostración la podemos encontrar en [5].

LEMA 1.2.2 *Sea* A *un anillo, sea* M *un* A*-módulo y sea* $\mathrm{p} \in \mathrm{Ass(M)}$. *Entonces* p *es elemento minimal del conjunto* Ass(M) *si y sólo si* p *es ideal minimal sobre* M.

PROPOSICIÓN 1.2.8 *Sean* A *un anillo y* M *un* A*-módulo. Sea* $\langle 0\rangle = \mathrm{M}_0 \subseteq \mathrm{M}_1 \subseteq \ldots \subseteq \mathrm{M}_r = \mathrm{M}$ *una sucesión de submódulos de* M *tal que* $\mathrm{M}_{i+1}/\mathrm{M}_i \cong \mathrm{A}/\mathrm{p}_i$, *con* $\mathrm{p}_i \in \mathrm{Spec(A)}$. *Entonces:*

$$\dim \mathrm{M} = \mathrm{máx}\{\ \dim \mathrm{A}/\mathrm{p}_i\ \ : 0 \leq i \leq r\}$$

Demostración.
En la proposición 1.2.7 se obtuvo que $\mathrm{AssM} \subseteq \{\mathrm{p}_1, \mathrm{p}_2, \ldots \mathrm{p}_r\}$.
Sea $\mathrm{p} \in \mathrm{SpecA}$ tal que $\mathrm{AnnM} \subseteq \mathrm{p}$ y $\dim \mathrm{M} = \dim \mathrm{A}/\mathrm{p}$, entonces p es un ideal primo minimal sobre M. Así, $\mathrm{p} \in \mathrm{AssM} \subseteq \{\mathrm{p}_1, \mathrm{p}_2, \ldots \mathrm{p}_r\}$, por el lema 1.2.2. Por lo tanto $\dim \mathrm{M} = \dim \mathrm{A}/\mathrm{p} \leq \mathrm{máx}\{\ \dim \mathrm{A}/\mathrm{p}_i\ \ : 0 \leq i \leq r\}$.

Como $\mathrm{A}/\mathrm{p}_i \cong \mathrm{M}_{i+1}/\mathrm{M}_i \subseteq \mathrm{M}/\mathrm{M}_i$, entonces $\dim \mathrm{A}/\mathrm{p}_i \leq \dim \mathrm{M}/\mathrm{M}_i \leq \dim \mathrm{M}$. Así, máx$\{ \dim \mathrm{A}/\mathrm{p}_i \ : 0 \leq i \leq r\} \leq \dim \mathrm{M}$.
De las dos desigualdades encontradas se obtiene el resultado.

1.3. Dimensión Proyectiva y Dimensión Inyectiva de un Módulo

LEMA 1.3.1 *Sea* A *un anillo, sean* F, L *y* K A-*módulos, y sean* $\mathrm{f} \in \mathrm{Hom}_{\mathrm{A}}(\mathrm{F}, \mathrm{K})$ *y* $\mathrm{g} \in \mathrm{Hom}_{\mathrm{A}}(\mathrm{L}, \mathrm{K})$. *Suponer que* F *es* A-*módulo libre y que* g *es epimorfismo. Entonces existe* $\tilde{\mathrm{f}} \in \mathrm{Hom}_{\mathrm{A}}(\mathrm{F}, \mathrm{L})$ *tal que* $\mathrm{f} = \mathrm{g} \circ \tilde{\mathrm{f}}$.

Demostración.
Sea $\{e_i \ : \ i \in \mathrm{I}\}$ una base para F. Como g es epimorfismo, entonces el conjunto $\mathrm{g}^{-1}(\mathrm{f}(e_i)) = \{l \in \mathrm{L} \ : \ \mathrm{g}(l) = \mathrm{f}(e_i)\}$ no es vacio. Sean $l_i \in \mathrm{g}^{-1}(\mathrm{f}(e_i))$. Consideremos el homomorfismo $\tilde{\mathrm{f}} : \mathrm{F} \to \mathrm{L}$ que está dado en la base por $\tilde{\mathrm{f}}(e_i) = l_i$. Es fácil verificar que $\tilde{\mathrm{f}}$ es el homomorfismo buscado.

PROPOSICIÓN 1.3.1 *Sean* A *un anillo y* M *un* A-*módulo. Las siguientes condiciones son equivalentes.*

(*1*) *Si* $\mathrm{L} \xrightarrow{\mathrm{g}} \mathrm{K} \to 0$ *es una sucesión exacta de* A-*módulos. Entonces*
$$\mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{L}) \xrightarrow{\mathrm{g}^*} \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{K}) \to 0$$
es una sucesión exacta de A-*módulos, donde* $\mathrm{g}^*(\alpha) = \mathrm{g} \circ \alpha$*;*

(*2*) *Si* $\mathrm{g} : \mathrm{L} \longrightarrow \mathrm{K}$ *es un epimorfismo de* A-*módulos y* $\beta : \mathrm{M} \longrightarrow \mathrm{K}$ *es un homomorfismo de* A-*módulos. Entonces existe* $\alpha : \mathrm{M} \longrightarrow \mathrm{L}$ *tal que* $\beta = \mathrm{g} \circ \alpha$*;*

(*3*) *Si* $\mathrm{g} : \mathrm{L} \longrightarrow \mathrm{M}$ *es un epimorfismo de* A-*módulos, entonces existe* $\mathrm{f} : \mathrm{M} \longrightarrow \mathrm{L}$ *tal que* $id_{\mathrm{M}} = \mathrm{g} \circ \mathrm{f}$*;*

(*4*) M *es sumando directo de un módulo libre.*

Demostración.
(**1**) $\Rightarrow$ (**2**) Sea $\mathrm{g} : \mathrm{L} \longrightarrow \mathrm{K}$ un epimorfismo y sea $\beta : \mathrm{M} \longrightarrow \mathrm{K}$ un homomorfismo, entonces la sucesión $\mathrm{L} \xrightarrow{\mathrm{g}} \mathrm{K} \to 0$ es exacta y $\beta \in \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{K})$. Así, $\mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{L}) \xrightarrow{\mathrm{g}^*} \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{K}) \to 0$ es una sucesión exacta, por tanto existe $\alpha \in \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{L})$ tal que $\mathrm{g}^*(\alpha) = \beta$, es decir $\beta = \mathrm{g} \circ \alpha$.

(**2**) $\Rightarrow$ (**3**) Sea g : L $\longrightarrow$ M un epimorfismo. Si id_{M} : M $\longrightarrow$ M es la identidad de M y M = K. Entonces existe f : M $\longrightarrow$ L tal que $id_{\mathrm{M}} = \mathrm{g} \circ \mathrm{f}$.

(**3**) $\Rightarrow$ (**4**) Sea X $\subseteq$ M un conjunto de generadores de M, sea $\mathrm{F} = \bigoplus_{i \in \mathrm{X}} \mathrm{A}$ el A-módulo libre con base X y sea g : F $\longrightarrow$ M tal que $\mathrm{g}(e_x) = x$. Así, g es epimorfismo, por tanto existe f : M $\longrightarrow$ F tal que $id_{\mathrm{M}} = \mathrm{g} \circ \mathrm{f}$, lo cual implica que f es monomorfismo.
Se afirma que F = f(M) $\oplus$ Ker g, de donde se sigue la afirmación.
En efecto, sea $a \in$ F y sea $b = a - \mathrm{f}(\mathrm{g}(a))$, entonces $\mathrm{g}(b) = \mathrm{g}(a - \mathrm{f}(\mathrm{g}(a))) = \mathrm{g}(a) - \mathrm{g}(\mathrm{f}(\mathrm{g}(a))) = \mathrm{g}(a) - \mathrm{g}(a) = 0$. Así, $b = a - \mathrm{f}(\mathrm{g}(a)) \in$ Ker g, lo cual implica que $a \in$ f(M) + Ker g.
Ahora, si $a \in$ f(M) $\cap$ Ker g, entonces $\mathrm{g}(a) = 0$ y $a = \mathrm{f}(m)$ para algún $m \in$ M. Así, $\mathrm{g}(a) = 0 = \mathrm{g}(\mathrm{f}(m)) = m$, por lo tanto $a = \mathrm{f}(m) = 0$. Lo cual implica que f(M) $\cap$ Ker g $=< 0 >$.

(**4**) $\Rightarrow$ (**1**) Sean F y S A-módulos tal que F es módulo libre y F = M $\oplus$ S, sea π : F $\longrightarrow$ M la proyección y sea j : M $\longrightarrow$ F la inclusión. Supóngase que L $\xrightarrow{\mathrm{g}}$ K $\rightarrow 0$ es una sucesión exacta de A-módulos. Se mostrará que la sucesión $\mathrm{Hom_A(M, L)} \xrightarrow{\mathrm{g}^*}$ $\mathrm{Hom_A(M, K)} \rightarrow 0$ es exacta, es decir, si g es epimorfismo, entonces g^* es epimorfismo.
Sea $\beta \in \mathrm{Hom_A(M, K)}$ y sea $\beta_1 = \beta \circ \pi \in \mathrm{Hom_A(F, K)}$, entonces, por la proposición.1.3.1, existe $\alpha_1 \in \mathrm{Hom_A(F, L)}$ tal que $\beta_1 = \beta \circ \pi = \mathrm{g} \circ \alpha_1$.
Se afirma que $\alpha = \alpha_1 \circ j \in \mathrm{Hom_A(M, L)}$ es tal que $\beta = \mathrm{g} \circ \alpha$, $\beta = \mathrm{g}^*(\alpha)$, de donde se sigue la afirmación. En efecto, pues $\mathrm{g} \circ \alpha = \mathrm{g} \circ \alpha_1 \circ j = \beta \circ \pi \circ j = \beta$.

Definición 1.3.1 *Sean* A *un anillo y* M *un* A*-módulo. Se dice que* M *es* A*-módulo proyectivo si cumple alguna de las condiciones de la proposición 1.3.1.*

Es evidente, por el lema 1.3.1, que un módulo libre es un módulo proyectivo.

Definición 1.3.2 *Sean* A *un anillo y* M *un* A*-módulo. Una* ***resolución proyectiva*** *de* M*, denotada por P, es una sucesión de* A*-módulos y homomorfismos*

$$P: \quad \cdots \xrightarrow{\partial_{n+1}} P_n \xrightarrow{\partial_n} P_{n-1} \rightarrow \cdots \rightarrow P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathrm{M} \xrightarrow{\partial_{-1}} 0$$

Donde cada P_i *es proyectivo y* $\ker \partial_n = \operatorname{im} \partial_{n+1}$ *para toda* $n \geq -1$.

En [6] se demuestra que todo A-módulo tiene una resolución proyectiva.

Definición 1.3.3 *Sean* A *un anillo,* N *y* M A*-módulos, y* P *una resolución proyectiva de* M

$$P: \qquad \cdots \xrightarrow{\partial_{n+1}} P_n \xrightarrow{\partial_n} P_{n-1} \to \cdots \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathrm{M} \to 0$$

Apliquemos el functor $\mathrm{Hom}(\,-\,,\mathrm{N})$ *a los módulos de* P *y se obtiene.*

$$\mathrm{Hom}(P,\mathrm{N}): \qquad \cdots \xrightarrow{\partial^*_{n+1}} \mathrm{Hom}(P_n,\mathrm{N}) \xrightarrow{\partial^*_n} \mathrm{Hom}(P_{n-1},\mathrm{N}) \xrightarrow{\partial^*_{n-1}} \mathrm{Hom}(P_{n-2},\mathrm{N}) \xrightarrow{\partial^*_{n-2}} \cdots$$

Se define el A*-módulo* $\mathrm{Ext}^n_{\mathrm{A}}(\mathrm{M},\mathrm{N}) := \ker \partial_n / \mathrm{im}\ \partial_{n+1}$

En [6] se demuestra que los módulos $\mathrm{Ext}^n_{\mathrm{A}}$ no dependen de la resolución proyectiva de M.

Definición 1.3.4 *Sean* A *un anillo y* M *un* A*-módulo. La dimensión proyectiva de* M*,* $\mathrm{proj\,dim\,M}$*, es el menor entero,* n*, para el cual* M *tiene una resolución proyectiva de la forma*

$$\cdots 0 \to 0 \to P_n \xrightarrow{\partial_n} P_{n-1} \to \cdots \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathrm{M} \to 0$$

Si tal entero no existe, entonces ponemos $\mathrm{proj\,dim\,M} = \infty$*.*

El resultado que mencionaremos a continuación no está acompañado de una demostración, su demostración la podemos encontrar en [6].

Proposición 1.3.2 *Sean* A *un anillo y* M *un* A*-módulo. Las siguientes condiciones son equivalentes:*

(*1*) $\mathrm{proj\,dim\,M} \leq n$*;*

(*2*) $\mathrm{Ext}^k_{\mathrm{A}}(\mathrm{M},\mathrm{N}) = 0$ *para todo* A*-módulo* N *y todo* $k \geq n+1$*;*

(*3*) $\mathrm{Ext}^{n+1}_{\mathrm{A}}(\mathrm{M},\mathrm{N}) = 0$ *para todo* A*-módulo* N*.*

El resultado que mencionaremos a continuación no está acompañado de una demostración, su demostración la podemos encontrar en [9].

Proposición 1.3.3 *Sean* A *un anillo y* M *un* A*-módulo. Las siguientes condiciones son equivalentes.*

(*1*) *Si* $0 \to \mathrm{L} \xrightarrow{\mathrm{j}} \mathrm{K}$ *es una sucesión exacta de* A*-módulos. Entonces*

$$0 \leftarrow \mathrm{Hom_A(L,M)} \xleftarrow{\mathrm{j}^*} \mathrm{Hom_A(K,M)}$$

es una sucesión exacta de A*-módulos, donde* $\mathrm{j}^*(\alpha) = \alpha \circ \mathrm{j}$*;*

(*2*) *Si* $\mathrm{j} : \mathrm{L} \longrightarrow \mathrm{K}$ *es un monomorfismo de* A*-módulos y* $\beta : \mathrm{L} \longrightarrow \mathrm{M}$ *es un homomorfismo. Entonces existe* $\alpha : \mathrm{K} \longrightarrow \mathrm{M}$ *tal que* $\beta = \alpha \circ \mathrm{j}$*;*

(*3*) *Si* L *es un submódulo de* K *y* $\beta : \mathrm{L} \longrightarrow \mathrm{M}$ *es un homomorfismo. Entonces existe* $\alpha : \mathrm{K} \longrightarrow \mathrm{M}$ *tal que* $\alpha|_{\mathrm{L}} = \beta$*;*

(*4*) *Si* I *es un ideal de* A*, entonces todo homomorfismo* $\alpha : \mathrm{I} \longrightarrow \mathrm{M}$ *se puede extender a un homomorfismo* $\tilde{\alpha} : \mathrm{A} \longrightarrow \mathrm{M}$*.*

Definición 1.3.5 *Sean* A *un anillo y* M *un* A*-módulo. Se dice que* M *es* A*-módulo inyectivo si cumple alguna de las condiciones de la proposición 1.3.3.*

Definición 1.3.6 *Sean* A *un anillo y* M *un* A*-módulo. Una* ***resolución inyectiva*** *de* M*, denotada por* E*, es una sucesión de* A*-módulos y homomorfismos*

$$E: \qquad 0 \xrightarrow{\partial_{-1}} \mathrm{M} \xrightarrow{\partial_0} E_0 \xrightarrow{\partial_1} E_1 \to \cdots \xrightarrow{\partial_n} E_n \xrightarrow{\partial_{n+1}} E_{n+1} \xrightarrow{\partial_{n+2}} \cdots$$

Donde cada E_i *es inyectiva y* $\ker \partial_{n+1} = \operatorname{im} \partial_n$ *para toda* $n \geq -1$*.*

En [6] se demuestra que todo A-módulo tiene una resolución inyectiva.

Definición 1.3.7 *Sean* A *un anillo y* M *un* A*-módulo. La dimensión inyectiva de* M*,* $\operatorname{inj\,dim} \mathrm{M}$*, es el menor entero,* n*, para el cual* M *tiene una resolución inyectiva de la forma*

$$0 \xrightarrow{\partial_{-1}} \mathrm{M} \xrightarrow{\partial_0} E_0 \xrightarrow{\partial_1} E_1 \to \cdots \xrightarrow{\partial_n} E_n \to 0 \to 0 \cdots$$

Si tal entero no existe, entonces ponemos $\operatorname{inj\,dim} \mathrm{M} = \infty$*.*

El resultado que mencionaremos a continuación no está acompañado de una demostración, su demostración la podemos encontrar en [6].

Proposición 1.3.4 *Sean* A *un anillo y* M *un* A*-módulo. Las siguientes condiciones son equivalentes.*

(*1*) $\operatorname{inj\,dim} \mathrm{M} \leq n$*;*

(*2*) $\mathrm{Ext}^k_{\mathrm{A}}(\mathrm{N}, \mathrm{M}) = 0$ *para todo módulo* N *y todo* $k \geq n+1$*;*

(*3*) $\mathrm{Ext}^{n+1}_{\mathrm{A}}(\mathrm{N}, \mathrm{M}) = 0$*. para todo módulo* N*.*

1.4. Profundidad de un Módulo y Módulos de Cohen-Macaulay

DEFINICIÓN 1.4.1 *Sean* A *un anillo y* M *un* A*-módulo.*

(*1*) *Sea* $x \in \mathrm{A}$. *Se dice que* x *es divisor de cero en* M *si existe* $m \in \mathrm{M} \setminus \{0\}$ *tal que* $x * m = 0$.

(*2*) *Sea* $x \in \mathrm{A}$. *Se dice que* x *es* M***-regular*** *si no es divisor de cero en* M, *es decir, si* $x * m = 0$, *entonces* $m = 0$.

(*3*) *Sean* $\overline{x} = x_1, \ldots, x_r \in \mathrm{A}$. *Se dice que* $\overline{x} = x_1, \ldots, x_r$ *es una* ***sucesión*** M***-regular de longitud*** r *si se satisfacen las siguientes condiciones.*

(*a*) *Para cada* $1 \leq i < r$, x_{i+1} *no es divisor de cero en* $\mathrm{M}/\langle x_1, \ldots, x_i\rangle\mathrm{M}$;

(*b*) $\langle x_1, \ldots, x_i\rangle\mathrm{M} \neq \mathrm{M}$.

EJEMPLO 1.4.1 *Sean* $\mathrm{A} = \mathbb{Z}$, $\mathrm{M}_1 = \mathbb{Q}$ *y* $\mathrm{M}_2 = \mathbb{Z}/8\mathbb{Z}$. *Entonces* $4 \in \mathbb{Z}$ *es* M_1*-regular y divisor de cero en* M_2.

OBSERVACIÓN 1.4.1 *Sea* $\overline{x} = x_1, \ldots, x_r$ *una sucesión* M*-regular de longitud* r. *Supóngase que* $\langle x_1, \ldots, x_i\rangle = \langle x_1, \ldots, x_i, x_{i+1}\rangle$ *para algún* $i \in \{1, \ldots, r-1\}$, *entonces* $x_{i+1} \in \langle x_1, \ldots, x_i\rangle$, *lo cual es absurdo. Así, la sucesión de ideales* $\langle x_1\rangle \subset \langle x_1, x_2\rangle \subset \cdots \subset \langle x_1, \ldots, x_r\rangle$ *es estrictamente creciente, pues* A *es noetheriano. Por tanto, dicha sucesión se estaciona. Por lo tanto, cada sucesión* M*-regular de elementos en un ideal* I *forma parte de una sucesión* M*-regular maximal de elementos en* I.

El resultado que mencionaremos a continuación no está acompañado de una demostración, su demostración la podemos encontrar en [5].

TEOREMA 1.4.1 *Sean* A *un anillo noetheriano,* M *un* A*-módulo,* I *un ideal de* A *con* $\mathrm{IM} \neq \mathrm{M}$ *y* $r > 0$ *un entero. Entonces las siguientes condiciones son equivalentes*

(*1*) $\mathrm{Ext}^i_{\mathrm{A}}(\mathrm{N}, \mathrm{M}) = 0$ $(i < r)$ *para* N *un* A*- módulo f.g. tal que* $\mathrm{Supp}(\mathrm{N}) \subseteq \mathrm{V}(\mathrm{I})$;

(*2*) $\mathrm{Ext}^i_{\mathrm{A}}(\mathrm{A}/\mathrm{I}\ , \mathrm{M}) = 0$ $(i < r)$;

(*3*) *Existe un* A*-módulo* N *con* $\mathrm{Supp}(\mathrm{N}) = \mathrm{V}(\mathrm{I})$ *tal que* $\mathrm{Ext}^i_{\mathrm{A}}(\mathrm{N}, \mathrm{M}) = 0$ $(i < r)$;

(*4*) *Existe una sucesión* M*-regular de longitud* r *de elementos en* I.

Definición 1.4.2 *Sean* A *un anillo noetheriano,* M *un* A*-módulo e* I *un ideal de* A *con* $\mathrm{IM} \neq \mathrm{M}$.

(*1*) *El teorema anterior asegura que la longitud de cualquier sucesión* M*-regular maximal de elementos de* I *es la misma. Denotamos por* $\mathrm{grade}(\mathrm{I}, \mathrm{M})$ *a la longitud de cualquier sucesión* M*-regular maximal de elementos de* I.

(*2*) *Supongamos que* A *es un anillo local y que* μ *es su ideal maximal. La profundidad de* M, $\mathrm{depth M}$, *es el número* $\mathrm{grade}(\mu, \mathrm{M})$.

(*3*) *Sean* A *un anillo noetheriano,* I *un ideal y sea* $\mathrm{Ass_A(A/I)} = \{\mathrm{p}_1, \ldots, \mathrm{p}_k\}$. *Si* $\mathrm{ht}\ (\mathrm{P}_i) = \mathrm{ht}\ \mathrm{I}$ *para cualquier* $i \in \{1, \ldots, k\}$, *entonces se dice que* I *es un ideal no mezclado.*

El resultado que mencionaremos a continuación no está acompañado de una demostración, su demostración la podemos encontrar en [5].

Proposición 1.4.1 *Sean* (A, μ) *un anillo local noetheriano y* M *un* A*-módulo,* $\mathrm{M} \neq 0$. *Entonces:*

$$\mathrm{depth}\ \mathrm{M} \leq \dim(\mathrm{A/P}) \quad \textit{para todo} \quad \mathrm{P} \in \mathrm{Ass(M)}$$

Definición 1.4.3 *Sean* (A, μ) *un anillo local noetheriano y* M *un* A*-módulo.*

(*1*) *Se dice que* M *es módulo de Cohen-Macaulay si* $\mathrm{depthM} = \dim \mathrm{M}$.
Por definición, el módulo cero es de Cohen-Macaulay.

(*2*) *Si* M *es un módulo de Cohen-Macaulay con* $\dim \mathrm{M} = \dim \mathrm{R}$, *entonces se dice que* M *es un módulo de Cohen-Macaulay maximal.*

(*3*) *Si el anillo local* A *es Cohen-Macaulay como* A*-módulo, entonces se dice que* A *es Anillo de Cohen-Macaulay.*

(*4*) *Si* A *es un anillo no necesariamente local y* $\mathrm{A_p}$ *es anillo local de Cohen-Macaulay para todo* $\mathrm{p} \in \mathrm{Spec(A)}$, *entonces se dice que* A *es anillo de Cohen-Macaulay.*

(*5*) *Supongamos que* A *es anillo de Cohen-Macaulay. Si* $\mathrm{M_p}$ *es módulo de Cohen-Macaulay sobre* $\mathrm{A_p}$ *para todo* $\mathrm{p} \in \mathrm{Spec(A)}$, *entonces se dice que* M *es módulo de Cohen-Macaulay.*

Definición 1.4.4 *Sean* A *un anillo noetheriano y* M *un* A*-módulo. Se dice que* M *es perfecto si* $\mathrm{proj\,dim\,M} = \mathit{grade}\mathrm{M}$.
Un ideal I *se dice que es perfecto si* A/I *es* A*-módulo perfecto.*

Los resultados que mencionaremos a continuación no estarán acompañados de una demostración, sus demostraciones las podemos encontrar en [9].

PROPOSICIÓN 1.4.2 *Sean* A *un anillo de Cohen-Macaulay e* I *un ideal* A, I $\neq$ A. *Entonces* grade I = ht I

TEOREMA 1.4.2 *Sean* k *un campo,* A = k$[X_0, \ldots, X_n]$, $\eta = \langle X_0, \ldots, X_n \rangle$ *y* M *un* A*-módulo graduado. Entonces las siguientes condiciones son equivalentes.*

(*1*) M *es Cohen-Macaulay;*

(*2*) M *es perfecto;*

(*3*) M_η *es Cohen-Macaulay;*

(*4*) M_η *es perfecto.*

PROPOSICIÓN 1.4.3 *Sean* A *un anillo noetheriano,* M *un* A*-módulo perfecto y* p $\in$ SuppM. *Entonces las siguientes condiciones son equivalentes.*

(*1*) p $\in$ AssM*;*

(*2*) depth A_P = grade M.

LEMA 1.4.1 *Sea* A *un anillo, sean* M *y* N A*-módulos, y sea* $\tilde{x} = x_1, \ldots x_r$ *una sucesión* M*-regular de longitud* r *de elementos en* AnnN. *Entonces*

$$\mathrm{Hom_A}(\mathrm{N}, \mathrm{M}/\tilde{x}\mathrm{M}) \cong \mathrm{Ext}^r_{\mathrm{A}}(\mathrm{N}, \mathrm{M})$$

DEFINICIÓN 1.4.5 *Sea* $(\mathrm{A}, \mu, \mathrm{k})$ *un anillo local Noetheriano y sea* M *un* A*-módulo tal que* depthM $= t$. *El número* $r(\mathrm{M}) = \dim_{\mathrm{k}} \mathrm{Hom_A}(\mathrm{k}, \mathrm{M}/\tilde{x}\mathrm{M}) = \dim_{\mathrm{k}} \mathrm{Ext}^t_{\mathrm{A}}(\mathrm{k}, \mathrm{M})$ *es llamado el tipo de* M.

DEFINICIÓN 1.4.6 *Sea* $(\mathrm{A}, \mu, \mathrm{k})$ *un anillo local Noetheriano. Se dice que* A *es un anillo de Gorenstein local si tiene dimensión inyectiva finita.*

DEFINICIÓN 1.4.7 *Sea* $(\mathrm{A}, \mu, \mathrm{k})$ *un anillo local de Cohen-Macaulay. Un* A*-módulo,* ω_{A}*, Cohen-Macaulay maximal de tipo 1 y con dimensión inyectiva finita es llamado el módulo canónico de* A.

El resultado que mencionaremos a continuación no está acompañado de una demostración, su demostración la podemos encontrar en [9].

TEOREMA 1.4.3 *Sea* $(\mathrm{A}, \mu, \mathrm{k})$ *un anillo local de Cohen-Macaulay. Se tienen las siguientes propiedades.*

(*1*) *Si el módulo canónico* ω_{A} *de* A *existe, entonces es único salvo isomorfismo.*

(*2*) *Existe el módulo canónico de* A *si y sólo si* A *es la imagen de un anillo Gorenstein local.*

(*3*) *Sea* (S, ϱ) *un anillo local de Cohen-Macaulay y sea* $\psi : (\mathrm{A}, \eta) \to (\mathrm{S}, \varrho)$ *homomorfismo local de anillos locales tal que* S *es* A*-módulo finitamente generado. Supongamos que* ω_{R} *existe, entonces* ω_{S} *existe y:*

$$\omega_{\mathrm{S}} \cong \mathrm{Ext}^{t}_{\mathrm{A}}(\mathrm{S}, \omega_{\mathrm{A}}) \qquad t = \dim \mathrm{A} - \dim \mathrm{S}$$

(*4*) *En particular, si* $\mathrm{S} \subseteq \mathrm{A}$ *y* A *es libre sobre* S*, entonces*

$$\omega_{\mathrm{S}} \cong \mathrm{Hom}_{\mathrm{A}}(\mathrm{S}, \omega_{\mathrm{A}})$$

Capítulo 2

Anillos y Módulos Graduados

2.1. Anillos y Módulos Graduados

DEFINICIÓN 2.1.1 *Sea* A *un anillo. Se dice que* A *es un anillo graduado si tiene una descomposición* $\mathrm{A} = \bigoplus_{i\in\mathbb{Z}} \mathrm{A}_i$ *en donde los* A_i *son subgrupos aditivos que satisfacen* $\mathrm{A}_i\mathrm{A}_j \subset \mathrm{A}_{i+j}$ *para todo* i, j.
Los elementos de A_d *se llaman elementos homogéneos de grado* d.

DEFINICIÓN 2.1.2 *Sean* A *un anillo graduado y* M *un* A*-módulo. Se dice que* M *es un* A*-módulo graduado si tiene una descomposición* $\mathrm{M} = \bigoplus_{i\in\mathbb{Z}} \mathrm{M}_i$ *en donde los* M_i *son subgrupos aditivos que satisfacen* $\mathrm{A}_i\mathrm{M}_j \subset \mathrm{M}_{i+j}$ *para todo* i, j.
Los elementos de M_d *se llaman elementos homogéneos de grado* d.

OBSERVACIÓN 2.1.1 *Sea* $\mathrm{A} = \bigoplus_{i\in\mathbb{Z}} \mathrm{A}_i$ *un anillo graduado y sea* $\mathrm{M} = \bigoplus_{i\in\mathbb{Z}} \mathrm{M}_i$ *un* A*-módulo graduado.*

(*1*) *De la relación* $\mathrm{A}_0\mathrm{A}_0 \subset \mathrm{A}_0$ *se obtiene que* A_0 *es un anillo.*

(*2*) *De la relación* $\mathrm{A}_0\mathrm{M}_j \subset \mathrm{M}_j$ *se obtiene que cada* M_j *es un* A_0*-módulo.*

DEFINICIÓN 2.1.3 *Sean* A *un anillo graduado,* M *un* A*-módulo y* N *un submódulo de* M.

(*1*) N *se dice que es un submódulo graduado si cumple alguna de las siguientes condiciones que son equivalentes:*

(*a*) $\mathrm{N} = \bigoplus_{i\in\mathbb{Z}} (\mathrm{N} \cap \mathrm{M}_i)$.

(*b*) N *está generado por elementos homogéneos.*

(*c*) *Si* $x = x_r + x_{r+1} \ldots + x_p \in \mathrm{N}$ *con* $x_i \in \mathrm{M}_i$, *entonces* $x_i \in \mathrm{N}$.

(*2*) *Supóngase que* N *es un submódulo graduado. El módulo cociente* M/N *es también un* A*-módulo graduado con graduación* $(\mathrm{M}/\mathrm{N})_i = \mathrm{M}_i/\mathrm{N}_i$.

(*3*) *Sean* M *un* A*-módulo graduado y* $a \in \mathbb{Z}$. *El módulo con corrimiento* a, $\mathrm{M}(a)$, *es el módulo* M, *pero donde la* i*-esima componente es* $(\mathrm{M}(a))_i = \mathrm{M}_{i+a}$.

DEFINICIÓN 2.1.4 *Sean* $\mathrm{A} = \bigoplus_{i\in\mathbb{Z}} \mathrm{A}_i$ *un anillo graduado y sean* $\mathrm{M} = \bigoplus_{i\in\mathbb{Z}} \mathrm{M}_i$, $\mathrm{N} = \bigoplus_{i\in\mathbb{Z}} \mathrm{N}_i$ A*-módulos graduados.*

(*1*) *El* A*-módulo* $\mathrm{M} \oplus \mathrm{N}$ *es un módulo graduado. La graduación es* $(\mathrm{M} \oplus \mathrm{N})_i = (\mathrm{M})_i \oplus (\mathrm{N})_i$.

(*2*) *Un homomorfismo graduado de grado* $a \in \mathbb{Z}$ *es un homomorfismo* $\phi : \mathrm{M} \to \mathrm{N}$ *tal que para todo* i, $\phi(\mathrm{M}_i) \subset \mathrm{N}_{i+a}$.
Notemos que ϕ *es un homomorfismo graduado de grado* $a \in \mathbb{Z}$ *si y sólo si* $\phi : \mathrm{M} \to \mathrm{N}(a)$ *es un homomorfismo graduado de grado* 0.
Si ϕ *es un homomorfismo graduado de grado* 0, *entonces se dirá simplemente que es un homomorfismo graduado, esto sin indicar el grado de* ϕ.

(*3*) *Sea* $\mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{N})_n$ *el conjunto de los homomorfismos graduados de* M *en* $\mathrm{N}(n)$.
El A*-módulo graduado con graduación* $\{\mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{N})_n\}$ *es denotado por* $\underline{\mathrm{Hom}}_{\mathrm{A}}(\mathrm{M}, \mathrm{N}) = \bigoplus_{n\in\mathbb{Z}} \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{N})_n$

(*4*) *Una resolución libre graduada finita (r.l.g.f.) del* A*-módulo graduado* M *es una sucesión exacta* $0 \to \mathrm{A}_t \xrightarrow{\phi_t} \mathrm{A}_{t-1} \xrightarrow{\phi_{t-1}} \cdots \to \mathrm{A}_1 \xrightarrow{\phi_1} \mathrm{A}_0 \xrightarrow{\phi_0} \mathrm{M} \to 0$, *donde los* A_i *son* A*-módulos graduados libres finitamente generados y los* ϕ_i *son homomorfismos graduados.*

OBSERVACIÓN 2.1.2 (*1*) *El kernel de un homomorfismo graduado* ϕ, $\mathrm{Ker}\phi$, *es un submódulo graduado.*

(*2*) *Si* M *es un* A*-módulo graduado libre finitamente generado, entonces*
$$\mathrm{M} \cong \mathrm{A}(\alpha_1) \oplus \mathrm{A}(\alpha_2) \oplus \ldots \oplus \mathrm{A}(\alpha_q) \text{ con } \alpha_i \in \mathrm{Z}$$

(*3*) *Sean* B *un anillo y* $\mathrm{A} = \mathrm{B}[X_0, \ldots, X_n]$ *el anillo de polinomios en* $n+1$ *variables. Si* A_d *es el conjunto de polinomios homogéneos de grado* d*, entonces* $\{\mathrm{A}_d\}_{d\geq 0}$ *es una graduación para* A*, y siempre salvo que se diga lo contrario se considerará a* A *con esa graduación.*
Es claro que A_d *es un* B*-módulo libre de rango* $\binom{n+d}{d}$*.*

(*4*) *En general* $\underline{\mathrm{Hom}}_{\mathrm{A}}(\mathrm{M}, \mathrm{N})$ *es un submódulo propio de* $\mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{N})$*. Pero si* M *es un* A*-módulo finitamente generado, entonces* $\underline{\mathrm{Hom}}_{\mathrm{A}}(\mathrm{M}, \mathrm{N}) = \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{N})$*.*

LEMA 2.1.1 *Sea* A *un anillo graduado y sean* $\mathrm{M}_1, \ldots, \mathrm{M}_r, \mathrm{N}$ A*-módulos graduados tal que* $\mathrm{M}_1, \ldots, \mathrm{M}_r$ *son finitamente generados. Entonces se tiene el isomorfismo de* A*-módulos graduados:*

$$\mathrm{Hom}_{\mathrm{A}}(\bigoplus_{i=1}^{r} \mathrm{M}_i, \mathrm{N}) \cong \bigoplus_{i=1}^{r} \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}_i, \mathrm{N})$$

Demostración.
Si π_j es la inclusión de M_j en $\bigoplus_{i=1}^{r} \mathrm{M}_i$, entonces el isomorfismo está dado por:

$$\begin{array}{rccc} \psi : \mathrm{Hom}_{\mathrm{A}}(\bigoplus_{i=1}^{r} \mathrm{M}_i, \mathrm{N}) & \longrightarrow & \bigoplus_{i=1}^{r} \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}_i, \mathrm{N}) \\ \mathrm{f} & \longmapsto & (\mathrm{f}\pi_1, \ldots, \mathrm{f}\pi_r) \end{array}$$

Y resta verificar que ψ es de grado cero.
Sea $\mathrm{f} \in \big(\mathrm{Hom}_{\mathrm{A}}(\bigoplus_{i=1}^{r} \mathrm{M}_i, \mathrm{N})\big)_d$, entonces $\mathrm{f} : \bigoplus_{i=1}^{r} \mathrm{M}_i \longrightarrow \mathrm{N}(d)$. Así, $\mathrm{f}\pi_i : \mathrm{M}_i \longrightarrow \mathrm{N}(d)$, es decir, $\mathrm{f}\pi_i \in \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}_i, \mathrm{N})_d$. Por lo tanto, $\psi(\mathrm{f}) = (\mathrm{f}\pi_1, \ldots, \mathrm{f}\pi_r) \in \big(\bigoplus_{i=1}^{r} \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}_i, \mathrm{N})\big)_d$.

LEMA 2.1.2 *Sea* A *un anillo graduado y* $r, d \in \mathbb{Z}$*. Entonces la función*

$$\begin{array}{rccc} \psi : \mathrm{A}(d-r) & \longrightarrow & \mathrm{Hom}_{\mathrm{A}}(\mathrm{A}(r), \mathrm{A}(d)) \\ \mathrm{x} & \longmapsto & \theta_{\mathrm{x}} \end{array} \qquad \textit{donde} \quad \theta_{\mathrm{x}}(y) = \mathrm{x}y \quad \forall y \in \mathrm{A}(r)$$

da el isomorfismo de módulos graduados

$$\mathrm{A}(d-r) \cong \mathrm{Hom}_{\mathrm{A}}(\mathrm{A}(r), \mathrm{A}(d))$$

Demostración.
Sea $\mathrm{x} \in \mathrm{A}(d-r)_n = \mathrm{A}_{d-r+n}$, entonces $\theta_{\mathrm{x}} : \mathrm{A}(r) \longrightarrow \mathrm{A}(d)(n) = \mathrm{A}(d+n)$. Así, ψ es

homomorfismo de grado cero.
Sea $r \in \mathrm{A}$ tal que $\psi(r) = \theta_{\mathrm{r}} = 0$, entonces $\theta_{\mathrm{r}}(1) = r = 0$. Así, ψ es monomorfismo.
Sea $\mu \in \mathrm{Hom}_{\mathrm{A}}(\mathrm{A}(r), \mathrm{A}(d))_n$, es decir, $\mu : \mathrm{A}(r) \longrightarrow \mathrm{A}(d)(n)$. Como μ es homomorfismo, entonces $\mu(y) = \mu(1)\ y = \theta_{\mu(1)}\ y$ para toda $y \in \mathrm{A}(r)$. Así, $\psi(\mu(1)) = \mu$, es decir, ψ es epimorfismo.

2.2. Teorema de Hilbert

En esta sección se define la función de Hilbert de un módulo graduado y se prueba el Teorema de Hilbert. Los valores de la función de Hilbert son las longitudes de las componentes homogéneas. Y el Teorema de Hilbert exhibe que la función de Hilbert de un módulo graduado coincide con una función polinomial .

Definición 2.2.1 *Sea* $\mathrm{A} = \bigoplus_{i\in\mathbb{Z}} \mathrm{A}_i$ *un anillo graduado tal que* $\mathrm{A}_0 = \mathrm{B}$ *es un anillo Artineano y* A *es finitamente generado como* B*-Algebra, sea* $\mathrm{M} = \bigoplus_{i\in\mathrm{Z}} \mathrm{M}_i$ *un* A*-módulo graduado y sea* I *un ideal graduado de* A.

(*a*) *La función de Hilbert de* M *es.*
$$\begin{array}{rccc} \mathrm{H_M} & : & \mathbb{Z} & \longrightarrow & \mathbb{N}\cup\{0\} \\ & & d & \longmapsto & \ell_{\mathrm{B}}(\mathrm{M}_d) \end{array} \quad \textit{donde } \ell_{\mathrm{B}}(\mathrm{M}_d) \textit{ es la longitud del } \mathrm{B}\textit{-módulo } \mathrm{M}_d$$

(*b*) *La función de Hilbert del* A*-módulo* A/I *se denota por* $\mathrm{H_I}$

(*c*) *La serie de Hilbert de* I *es la serie formal definida por* $\mathrm{F_I}(t) = \sum_{i\geq 0} \mathrm{H_I}(i)t^i$

Observación 2.2.1 (*1*) *Existe un epimorfismo de* $\mathrm{A}(\alpha_1) \oplus \mathrm{A}(\alpha_2) \oplus \ldots \oplus \mathrm{A}(\alpha_q)$ *en* M*, pues* M *es finitamente generado, tal que al ser restringido a la d-esima componente da un epimorfismo del* B*-módulo* $\mathrm{A}(\alpha_1)_d \oplus \mathrm{A}(\alpha_2)_d \oplus \ldots \oplus \mathrm{A}(\alpha_q)_d$ *en el* B*-módulo* M_d*. Así, el número* $\ell_{\mathrm{B}}(\mathrm{M}_d)$ *es finito.*

(*2*) *Cuando* $\mathrm{B} = \mathrm{k}$ *sea un campo se tendrá* $\mathrm{H_M}(d) = \dim_{\mathrm{k}} \mathrm{M}_d$

Lema 2.2.1 *Sean* A *un anillo graduado y* M *un* A*-módulo graduado. Se tienen las siguientes propiedades.*

(*1*) *Sea* $\mathrm{p} \in \mathrm{Ass(M)}$*. Entonces* p *es ideal graduado y es el anulador de un elemento homogéneo.*

(*2*) *Existe una sucesión de submódulos graduados* $\langle 0\rangle = \mathrm{M}_0 \subseteq \mathrm{M}_1 \subseteq \ldots \subseteq \mathrm{M}_r = \mathrm{M}$ *tal que* $\mathrm{M}_{i+1}/\mathrm{M}_i \cong (\mathrm{A}/\mathrm{p}_i)(a_i)$*, donde cada* p_i *es un ideal primo graduado y* $a_i \in \mathbb{Z}$*.*

(*3*) *Sea* $\langle 0\rangle = \mathrm{M}_0 \subseteq \mathrm{M}_1 \subseteq \ldots \subseteq \mathrm{M}_r = \mathrm{M}$ *una sucesión de módulos graduados. Supóngase que* A_0 *es un anillo Artineano y* A *es finitamente generado como* A_0*-Algebra, entonces*

$$\mathrm{H}_{\mathrm{M}}(d) = \sum_{i=0}^{r} \mathrm{H}_{\mathrm{M}_{i+1}/\mathrm{M}_i}(d)$$

Demostración.

(1) Ver [5].

(2) La sucesión de submódulos se obtiene de la misma manera que en la proposición 1.2.5, y para asegurar que los ideales p_i y los submódulos N_i son graduados hay que usar el inciso anterior.

(3) Se sigue del lema 1.1.2.

Definición 2.2.2 *Sean* $\mathrm{F} : \mathbb{Z} \longrightarrow \mathbb{Z}$ *y* $n \geq 0$*.*

(*1*) *Se dice que* F *es de tipo polinomial de grado* n *si existe* $\mathrm{P}(X) \in \mathbb{Q}[X]$ *tal que* $\mathrm{F}(d) = \mathrm{P}(d)$ *para todo* $d >> 0$*.*

(*2*) *El operador diferencia,* Δ*, sobre cualquier función numérica está dado por*

$$(\Delta \mathrm{F})(d) = \mathrm{F}(d+1) - \mathrm{F}(d) \quad \textit{para todo } d$$

Notemos que Δ *mapea funciones de tipo polinomial en funciones de tipo polinomial.*

(*3*) *Por definición el polinomio cero tiene grado* -1*.*

El resultado que mencionaremos a continuación no está acompañado de una demostración, su demostración la podemos encontrar en [9].

Lema 2.2.2 *Sean* $\mathrm{F} : \mathbb{Z} \longrightarrow \mathbb{Z}$ *una función numérica y* $n \geq 0$ *un entero. Las siguientes condiciones son equivalentes.*

(*1*) $(\Delta^n\ \mathrm{F})(d) = c, \quad c \neq 0, \quad$ *para toda* d*;*

(*2*) F *es de tipo polinomial de grado* n.

TEOREMA 2.2.1 (**Teorema de Hilbert**)
Sea $\mathrm{A} = \bigoplus_{i\in\mathrm{Z}} \mathrm{A}_i$ *un anillo graduado tal que* A_0 *es un anillo Artineano y* A *es generado como* A_0*-Álgebra por una cantidad finita de elementos homogéneos de grado* 1*, y sea* $\mathrm{M} = \bigoplus_{i\in\mathrm{Z}} \mathrm{M}_i$ *un* A*-módulo graduado de dimensión* n*. Entonces* H_M *es una función polinomial de grado* $n-1$.

Demostración.
Sea $\langle 0\rangle = \mathrm{M}_0 \subseteq \mathrm{M}_1 \subseteq \ldots \subseteq \mathrm{M}_r = \mathrm{M}$ la sucesión de submódulos del inciso (2) del lema 2.2.1. Si suponemos el resultado cierto para los módulos de la forma $\mathrm{M} = \mathrm{A/p}$, es decir, si suponemos que para cualquier ideal primo graduado p la función de Hilbert del A-módulo A/p es una función polinomial de grado $\dim(\mathrm{A/p}) - 1$. Entonces, por el inciso (3) del lema 2.2.1, por el hecho de que la función de Hilbert es positiva (el término lider del polinomio que la represente será positivo) y por la proposición 1.2.8, $\mathrm{H}_\mathrm{M}(d) = \sum_{i=0}^{r} \mathrm{H}_{(\mathrm{A/p})(a_i)}(d)$ será una función polinomial de grado $\text{máx}\{\dim(\mathrm{A/p}_i) - 1 : 1 \leq i \leq r\} = \dim \mathrm{M} - 1$. Por lo cual resta hacer la prueba para cuando $\mathrm{M} = \mathrm{A/p}$.
La prueba será por inducción sobre n.
Sea p un ideal primo graduado tal que $\dim \mathrm{A/p} = 0$, entonces A/p es Artineano, por la proposición 1.2.2. Como los ideales $\mathrm{I}_k = \sum_{i=k}^{\infty} (\mathrm{A/p})_i$ son tales que $\mathrm{I}_{k+1} \subseteq \mathrm{I}_k$, entonces existe k_0 tal que $\mathrm{I}_k = \mathrm{I}_{k_0}$ para todo $k \geq k_0$. Así, para todo $k \geq k_0$ se tiene $(\mathrm{A/p})_k = 0$, es decir, para todo $k \geq k_0$ se tiene $\mathrm{H}_{\mathrm{A/p}}(k) = 0$. Por lo tanto, la función de Hilbert de A/p coincide con el polinomio cero.
Ahora, la hipótesis inductiva dice que si p es un ideal primo graduado tal que $\dim \mathrm{A/p} = n$, entonces la función de Hilbert del A-módulo A/p es una función polinomial de grado $\dim(\mathrm{A/p}) - 1$. Por lo tanto, por la observación hecha al inicio de esta demostración, la hipótesis inductiva implica que si M es un A-módulo con $\dim \mathrm{M} = n$, entonces la función de Hilbert de M es una función polinomial de grado $\dim \mathrm{M} - 1$.
Sea p un ideal primo graduado tal que $\dim \mathrm{A/p} = n + 1$ y sea $x \in \mathrm{A}_1 \setminus \mathrm{p}_1$. Entonces x es (A/p)-regular (pues p es un ideal primo), (x, p) es un ideal homogéneo tal que $\dim \mathrm{A}/(x, \mathrm{p}) = n$ y se tiene la sucesión exacta

$$0 \to \mathrm{A/p}(-1) \xrightarrow{x} \mathrm{A/p} \to \mathrm{A}/(x, \mathrm{p}) \to 0$$

De la cual se obtiene:

$$\Delta \mathrm{H}_{\mathrm{A/p}}(d) = \mathrm{H}_{\mathrm{A/p}}(d+1) - \mathrm{H}_{\mathrm{A/p}}(d) = \mathrm{H}_{\mathrm{A}/(x,\mathrm{p})}(d+1) \tag{2.1}$$

Así, $\Delta \mathrm{H}_{\mathrm{A/p}} = \mathrm{H}_{\mathrm{A}/(x,\mathrm{p})}$ es una función polinomial de grado $n-1$, por hipótesis de inducción. Para finalizar la demostración se analizan dos casos.

(a) Si $n = 0$. Se tiene $\mathrm{H}_{\mathrm{A/p}}(d) = \mathrm{H}_{\mathrm{A/p}}(0) + \sum_{i=1}^{d} \mathrm{H}_{\mathrm{A}/(x,\mathrm{p})}(i)$, por la ecuación 2.1; $\mathrm{H}_{\mathrm{A}/(x,\mathrm{p})}(i) = 0$ para $i >> 0$, pues $\dim \mathrm{A}/(x,\mathrm{p}) = 0$; $\mathrm{H}_{\mathrm{A/p}}(0) \neq 0$, pues $\mathrm{A}_0 \neq \mathrm{p}_0$. Por lo tanto, $\mathrm{H}_{\mathrm{A/p}}(d)$ es una constante no cero para $d >> 0$.

(b) Si $n \geq 1$. Entonces $\Delta^{n-1}(\Delta \mathrm{H}_{\mathrm{A/p}}(d)) = \Delta^n \mathrm{H}_{\mathrm{A/p}}(d)$ es una constante no cero, por el lema 2.2.2. Por lo tanto, $\mathrm{H}_{\mathrm{A/p}}(d)$ es una función polinomial de grado n, por el lema 2.2.2.

Por lo tanto, $\mathrm{H}_{\mathrm{A/p}}(d)$ es una función polinomial de grado n, lo cual prueba el teorema.

Definición 2.2.3 *El polinomio del teorema anterior es llamado el polinomio de Hilbert de* M *y es denotado por* $\mathrm{P}_{\mathrm{M}}(d)$.

2.3. Teorema de Macaulay

En lo que sigue $\mathbb{Z}_{\geq 0}$ denotará al conjunto de los enteros no negativos.

Definición 2.3.1 *Un monomio en las variables $X_0, X_1, \ldots, X_n$ es una expresión de la forma:* $X_0^{\alpha_0} X_1^{\alpha_1} \cdots X_n^{\alpha_n} \quad (\alpha_i \in \mathbb{Z}_{\geq 0})$
El grado total de este monomio es $|\alpha| = \alpha_0 + \alpha_1 + \ldots + \alpha_n$.
Para simplificar ponemos $X^\alpha = X_0^{\alpha_0} X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, donde $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^{n+1}$.

Notemos que el conjunto de monomios en las variables $X_0, \ldots, X_n$ está en correspondencia biyectiva con $\mathbb{Z}_{\geq 0}^{n+1}$.

Definición 2.3.2 *Sea $>$ una relación binaria sobre $\mathbb{Z}_{\geq 0}^{n+1}$. Se dice que $>$ es un orden monomial si satisface:*

(*a*) *$>$ es un orden total.*
Es decir, dados $\alpha, \beta \in \mathbb{Z}_{\geq 0}^{n+1}$, entonces $\alpha < \beta$ ó $\alpha > \beta$ ó $\alpha = \beta$

(*b*) *Si $\alpha > \beta$ y $\gamma \in \mathbb{Z}_{\geq 0}^{n+1}$, entonces $\alpha + \gamma > \beta + \gamma$*

(c) $>$ *es buen orden sobre* $\mathbb{Z}_{\geq 0}^{n+1}$.
Es decir, todo subconjunto no vacio de $\mathbb{Z}_{\geq 0}^{n+1}$ *tiene elemento mínimo.*

Si $>$ *es un orden monomial sobre* $\mathbb{Z}_{\geq 0}^{n+1}$, *entonces se dice que* $X^\alpha > X^\beta$ *siempre que* $\alpha > \beta$.

Definición 2.3.3 *Un orden monomial* $>$ *es llamado orden monomial graduado si* $\alpha > \beta$ *siempre que* $|\alpha| > |\beta|$.

Definición 2.3.4 (**Orden Lexicográfico.**)
Se define la relación $>_{lex}$ *sobre* $\mathbb{Z}_{\geq 0}^{n+1}$:
Si $\alpha = (\alpha_0, \ldots, \alpha_n)$ *y* $\beta = (\beta_0, \ldots, \beta_n) \in \mathbb{Z}_{\geq 0}^{n+1}$, *entonces* $\alpha >_{lex} \beta$ *si y sólo si la coordenada no cero más cercana a la izquierda en el vector diferencia* $\alpha - \beta \in \mathbb{Z}^{n+1}$ *es posiva.*

Definición 2.3.5 (**Orden Lexicográfico Graduado.**)
Se define la relación $>_{grlex}$ *sobre* $\mathbb{Z}_{\geq 0}^{n+1}$:
Si $\alpha = (\alpha_0, \ldots, \alpha_n)$ *y* $\beta = (\beta_0, \ldots, \beta_n) \in \mathbb{Z}_{\geq 0}^{n+1}$, *entonces* $\alpha >_{grlex} \beta$ *si y sólo si:*

$$|\alpha| = \sum_{i=0}^{n} \alpha_i > |\beta| = \sum_{i=0}^{n} \beta_i \qquad \text{ó} \qquad |\alpha| = |\beta| \quad y \quad \alpha >_{lex} \beta$$

Ejemplo 2.3.1 (*i*) $\alpha = (2, 8, 3) >_{lex} \beta = (2, 7, 4)$
Pues la primer coordenada no cero de izquierda a derecha de $\alpha - \beta = (0, 1, -1)$ *es positiva. De esta manera se tiene:* $X_0^2 X_1^8 X_2^3 >_{lex} X_0^2 X_1^7 X_2^4$

(*ii*) $\alpha = (3, 2, 4) >_{lex} \beta = (3, 2, 1)$
Pues la primer coordenada no cero de izquierda a derecha de $\alpha - \beta = (0, 0, 3)$ *es positiva. De esta manera se tiene:* $X_0^3 X_1^2 X_2^4 >_{lex} X_0^3 X_1^2 X_2^1$

(*iii*) $(1, 0, \ldots, 0) >_{lex} (0, 1, 0, \ldots, 0) >_{lex} \ldots >_{lex} (0, \ldots, 1, 0) >_{lex} (0, \ldots, 0, 1)$
De esta manera se tiene: $X_0 >_{lex} X_1 >_{lex} \ldots >_{lex} X_n$

(*iv*) $\alpha = (1, 2, 3) >_{grlex} \beta = (3, 2, 0)$
Pues $|(1, 2, 3)| = 6 > |(3, 2, 0)| = 5$. *De esta manera se tiene:* $X_0 X_1^2 X_2^3 >_{grlex} X_0^3 X_1^2$

(*v*) $\alpha = (1, 2, 4) >_{grlex} \beta = (1, 1, 5)$
Pues $|(1, 2, 4)| = |(1, 1, 5)| = 7$ *y* $\alpha = (1, 2, 4) >_{lex} \beta = (1, 1, 5)$ *ya que en* $\alpha - \beta = (0, 1, -1)$ *la primer coordenada no cero de izquierda a derecha es positiva. De esta manera se tiene:* $X_0^1 X_1^2 X_2^4 >_{grlex} X_0^1 X_1^1 X_2^5$

Tomando una permutación de las variables se pueden encontrar $(n+1)!$ *ordenes lexicográficos, por ejemplo aquel en el que* $X_n >_{lex} X_{n-1} >_{lex} \ldots >_{lex} X_0$

LEMA 2.3.1 *Sea* $>$ *una relación de orden sobre* $\mathbb{Z}_{\geq 0}^{n+1}$. *Entonces* $>$ *es buen orden si y sólo si toda sucesión decreciente de elementos de* $\mathbb{Z}_{\geq 0}^{n+1}$ *se estaciona.*

Demostración.
Supóngase que $>$ es buen orden y sea $\alpha_1 > \alpha_2 > \alpha_3 > \cdots$ una sucesión decreciente de elementos de $\mathbb{Z}_{\geq 0}^{n+1}$. Como el conjunto $\{\alpha_1, \alpha_2, \alpha_3, \ldots\}$ es no vacio, entonces tiene elemento mínimo. Así, la sucesión termina.
Supóngase ahora que toda sucesión decreciente de elementos de $\mathbb{Z}_{\geq 0}^{n+1}$ termina y supóngase que $>$ no es buen orden. Existe $\mathrm{S} \subseteq \mathbb{Z}_{\geq 0}^{n+1}$ que no tiene elemento mínimo, pues $>$ no es buen orden. Sea $\alpha_1 \in \mathrm{S}$ arbitrario, entonces existe $\alpha_2 \in \mathrm{S}$ tal que $\alpha_1 > \alpha_2$, pues α_1 no es elemento mínimo . Continuando con este procedimiento se obtiene una sucesión decreciente que no termina, lo cual es absurdo. Por lo tanto, $>$ es buen orden.

PROPOSICIÓN 2.3.1 *El orden lexicográfico es un orden monomial.*

Demostración.
(**a**) $>_{lex}$ es un orden total.
Sean $\alpha = (\alpha_0, \ldots, \alpha_n)$ y $\beta = (\beta_0, \ldots, \beta_n) \in \mathbb{Z}_{\geq 0}^{n+1}$. Entonces se cumple exactamente una de las siguientes afirmaciones, pues $(\mathbb{Z}_{\geq 0}, >)$ es un orden total.

(i) $\alpha_i = \beta_i$ para $i = 0, \ldots, n$;

(ii) Existe i_0 tal que $\alpha_i = \beta_i$ para $0 \leq i < i_0$ y $\alpha_{i_0} > \beta_{i_0}$;

(iii) Existe i_0 tal que $\alpha_i = \beta_i$ para $0 \leq i < i_0$ y $\alpha_{i_0} < \beta_{i_0}$.

En cualquier caso se tiene $\alpha = \beta$ ó $\alpha < \beta$ ó $\beta < \alpha$.

(**b**) Sean α, β y $\gamma \in \mathbb{Z}_{\geq 0}^{n+1}$ tal que $\alpha > \beta$. Entonces existe un i_0 tal que $\alpha_i = \beta_i$ para $1 \leq i < i_0$ y $\alpha_{i_0} - \beta_{i_0} > 0$. Así, $\alpha_i + \gamma_i = \beta_i + \gamma_i$ para $i < i_0$ y $\alpha_{i_0} - \beta_{i_0} = \alpha_{i_0} + \gamma_{i_0} - (\beta_{i_0} + \gamma_{i_0}) > 0$. Por lo tanto, $\alpha + \gamma > \beta + \gamma$.

(**c**) Supóngase que $>_{lex}$ no es buen orden, entonces existe una sucesión estrictamente decreciente, $\alpha_1 > \alpha_2 > \alpha_3 > \ldots$, que no se estaciona, por el lema 2.3.1. Si denotamos

por α_i^r a la coordenada r del vector α_i, entonces $\{\alpha_i^0\}_{i=1}^{\infty}$ es una sucesión decreciente de elementos de $\mathbb{Z}_{\geq 0}$, por definición del orden lexicográfico. Así, existe $k_0 \in \mathbb{Z}_{\geq 0}$ tal que los α_i^0 son iguales para $k_0 \leq i$, pues $(\mathbb{Z}_{\geq 0}, >)$ es bien ordenado. De la misma forma, la sucesión $\{\alpha_i^1\}_{i=k_0}^{\infty}$ es decreciente, así, existe $k_1 \in \mathbb{Z}_{\geq 0}$ tal que $k_0 \leq k_1$ y los α_i^1 son iguales para $k_1 \leq i$. Continuando con el proceso se tiene que los α_i^n son iguales para $k_n \leq i$, lo cual es absurdo. Por lo tanto, $>_{lex}$ es buen orden.

DEFINICIÓN 2.3.6 *Sean* $\mathrm{f} = \sum_\alpha a_\alpha X^\alpha \in \mathrm{k}[X_0, \ldots X_n]$ *un polinomio no cero y sea* $>$ *un orden monomial.*

(*i*) *El multigrado de* f *es:*

$$multideg(\mathrm{f}) = \max\{\alpha \in \mathbb{Z}_{\geq 0}^n \ : \ a_\alpha \neq 0\}$$

El máximo es tomado con respecto a $>$

(*ii*) *El coeficiente líder de* f *es:*

$$\mathrm{LC(f)} = a_{multideg(\mathrm{f})} \in \mathrm{k}$$

(*iii*) *El monomio líder de* f *es:*

$$\mathrm{LM(f)} = X^{multideg(\mathrm{f})} \in \mathrm{k}$$

(*iv*) *El término líder de* f *es:*

$$\mathrm{LT(f)} = \mathrm{LC(f)LM(f)}$$

DEFINICIÓN 2.3.7 *Sean* $>$ *un orden monomial e* I *un ideal no cero de* $\mathrm{k}[X_0, \ldots X_n]$.

(*i*) *Se denota por* LT(I) *al conjunto de términos lideres de los polinomios que pertenecen a* I*, es decir:*

$$\mathrm{LT(I)} = \{\mathrm{LT(f)} \ : \ \mathrm{f} \in \mathrm{I}\} = \{cX^\alpha \ : \exists\ \mathrm{f} \in \mathrm{I}, \text{ tal que } \mathrm{LT(f)} = cX^\alpha\}$$

(*ii*) *Si el ideal* I *está generado por un conjunto de monomios, entonces se dice que* I *es un ideal monomial.*

(*iii*) $\langle \mathrm{LT(I)} \rangle$ *denota el ideal generado por el conjunto* LT(I)*, el cual es un ideal monomial*

Los resultados que mencionaremos a continuación no estarán acompañados de una demostración, sus demostraciones las podemos encontrar en [4].

LEMA 2.3.2 *Sea* $\mathrm{I} = \langle X^\alpha : \alpha \in \mathrm{G} \rangle$ *un ideal monomial. Entonces el monomio* X^β *pertenece a* I *si y sólo si* X^β *es divisible por algún* X^α $(\alpha \in \mathrm{G})$.

LEMA 2.3.3 *Sea* I *un ideal monomial y sea* $\mathrm{f} \in \mathrm{k}[X_0, \ldots, X_n]$. *Las siguientes condiciones son equivalentes:*

(*i*) $\mathrm{f} \in \mathrm{I}$;

(*ii*) *Cada término de* f *pertenece a* I;

(*iii*) f *es una combinación lineal sobre* k *de monomios de* I.

TEOREMA 2.3.1 (**Teorema de Macaulay**)
Sea $>$ *un orden monomial graduado y sea* I *un ideal homogéneo de* $\mathrm{k}[X_0, \ldots, X_n]$. *Entonces el ideal monomial* $\langle LT(\mathrm{I})\rangle$ *y el ideal* I *tienen la misma función de Hilbert.*

Demostración.
Para un ideal homogéneo J, se denota por $\mathrm{J}_{\leq d}$ a la suma de las primeras d componentes homogéneas, esto es, $\mathrm{J}_{\leq d} = \bigoplus_{i=1}^{d} \mathrm{J}_i$. Se encontrará una base $\{\mathrm{f}_1, \ldots, \mathrm{f}_r\}$ de $\mathrm{I}_{\leq d}$ para la cual el conjunto $\{\mathrm{LM}(\mathrm{f}_1), \ldots, \mathrm{LM}(\mathrm{f}_r)\}$ consta de monomios distintos y es una base para $\langle \mathrm{LT}(\mathrm{I})\rangle_{\leq d}$.
Sean $\mathrm{f}_1, \ldots, \mathrm{f}_r \in \mathrm{I}_{\leq d}$ tal que $\{\mathrm{LM}(\mathrm{f}) : \mathrm{f} \in \mathrm{I}_{\leq d}\} = \{\mathrm{LM}(\mathrm{f}_1), \ldots, \mathrm{LM}(\mathrm{f}_r)\}$. Supóngase que los f_i han sido ordenados de manera que $\mathrm{LM}(\mathrm{f}_i) > \mathrm{LM}(\mathrm{f}_{i+1})$ y que los $\mathrm{LM}(\mathrm{f}_i)$ son monomios distintos. Se verificará que $\{\mathrm{f}_1, \ldots, \mathrm{f}_r\}$ es una base para $\mathrm{I}_{\leq d}$.

(i) Los $\mathrm{f}_1, \ldots, \mathrm{f}_r$ son linealmente independientes sobre k. En efecto, si $\sum_{i=1}^{r} a_i \mathrm{f}_i = 0$, entonces $a_1 = 0$, esto pues $\sum_{i=1}^{r} a_i \mathrm{f}_i = a_1 \mathrm{LT}(\mathrm{f}_1) + \mathrm{g} = 0$, donde g es una combinación lineal sobre k de monomios menores a $\mathrm{LT}(\mathrm{f}_1)$. Así, $\sum_{i=2}^{r} a_i \mathrm{f}_i = 0$ y por el mismo argumento $a_2 = 0$. Continuando el proceso se concluye que $a_i = 0$.

(ii) Los $\mathrm{f}_1, \ldots, \mathrm{f}_r$ generan $\mathrm{I}_{\leq d}$ sobre k. Supóngase lo contrario, es decir, supóngase que $\mathrm{I}_{\leq d} \setminus \langle \mathrm{f}_1, \ldots, \mathrm{f}_r\rangle \neq \emptyset$. Elijamos $\mathrm{f} \in \mathrm{I}_{\leq d} \setminus \langle \mathrm{f}_1, \ldots, \mathrm{f}_r\rangle$ de manera que $\mathrm{LM}(\mathrm{f})$ sea minimal, entonces $\mathrm{LT}(\mathrm{f}) = \lambda \mathrm{LT}(\mathrm{f}_i)$ para algún $i \in \{1, \ldots, r\}$ y para algún $\lambda \in \mathrm{k}$. Así, el polinomio $\mathrm{g} = \mathrm{f} - \lambda \mathrm{f}_i$ es tal que $\mathrm{g} \in \mathrm{I}_{\leq d} \setminus \langle \mathrm{f}_1, \ldots, \mathrm{f}_r\rangle$ y $\mathrm{LM}(\mathrm{g}) < \mathrm{LM}(\mathrm{f})$, lo cual es una contradicción. Por lo tanto, $\mathrm{I}_{\leq d} = \langle \mathrm{f}_1, \ldots, \mathrm{f}_r\rangle$.

Se verificará que $\{\mathrm{LM}(\mathrm{f}_1), \ldots, \mathrm{LM}(\mathrm{f}_r)\}$ es una base para $\langle \mathrm{LT}(\mathrm{I})\rangle_{\leq d}$.

(i) Los monomios $\mathrm{LM}(\mathrm{f}_1), \ldots, \mathrm{LM}(\mathrm{f}_r)$ son linealmente independientes sobre k pues son monomios distintos.

(ii) Los monomios $\mathrm{LM}(\mathrm{f}_1), \ldots, \mathrm{LM}(\mathrm{f}_r)$ generan $\langle \mathrm{LT}(\mathrm{I}) \rangle_{\leq d}$ sobre k.
Sea $\mathrm{h} \in \langle \mathrm{LT}(\mathrm{I}) \rangle_{\leq d}$, entonces h es una combinación lineal sobre k de monomios de la forma $\mathrm{LT}(\mathrm{g})$, donde $\mathrm{g} \in \mathrm{I}$, por los lemas 2.3.2 y 2.3.3. Es decir, existen $\mathrm{g}_1, \ldots, \mathrm{g}_k \in \mathrm{I}$ tal que $\mathrm{h} = a_1\mathrm{LT}(\mathrm{g}_1) + \ldots + a_k\mathrm{LT}(\mathrm{g}_k)$. Por tanto, el grado total de cada $\mathrm{LT}(\mathrm{g}_i)$ es menor o igual a d, entonces los monomios de cada $\mathrm{g}_i \in \mathrm{I}$ son de grado total menor o igual a d, pues $>$ es un orden monomial graduado. Es decir, $\mathrm{g}_i \in \mathrm{I}_{\leq d}$. Así, para cada $i \in \{1, \ldots, k\}$ existe $r_i \in \{1, \ldots, r\}$ tal que $\mathrm{LT}(\mathrm{g}_i) = \mathrm{LT}(\mathrm{f}_{r_i})$. Por lo tanto, $\mathrm{h} = a_1\mathrm{LT}(\mathrm{f}_{r_1}) + \ldots + a_k\mathrm{LT}(\mathrm{f}_{r_k}) = a_1\mathrm{LC}(\mathrm{f}_{r_1})\mathrm{LM}(\mathrm{f}_{r_1}) + \ldots + a_k\mathrm{LC}(\mathrm{f}_{r_k})\mathrm{LM}(\mathrm{f}_{r_k})$, que es lo que se esperaba.

2.4. Bases de Groebner

En lo que sigue se considera un orden monomial, $>$, fijo sobre $\mathrm{k}[X_0, \ldots, X_n]$. Los resultados que mencionaremos a continuación no estarán acompañados de una demostración, sus demostraciones las podemos encontrar en [4].

Teorema 2.4.1 (**Algoritmo de la División en** $\mathrm{k}[X_0, \ldots X_n]$).
Sea $>$ un orden monomial, sean $\mathrm{g}_1, \ldots, \mathrm{g}_k \in \mathrm{k}[X_0, \ldots X_n]$ y sea $\mathrm{f} \in \mathrm{k}[X_0, \ldots X_n]$. Entonces existen $a_1, \ldots, a_k, \mathrm{r} \in \mathrm{k}[X_0, \ldots X_n]$ tales que

$$\mathrm{f} = a_1\mathrm{g}_1 + \ldots + a_k\mathrm{g}_k + \mathrm{r}$$

Con $\mathrm{r} = 0$ ó r es una combinación lineal sobre k de monomios, donde ninguno de ellos es divisible por $\mathrm{LT}(\mathrm{g}_1), \ldots, \mathrm{LT}(\mathrm{g}_k)$.
Además, si $a_i\mathrm{f}_i \neq 0$, entonces $multideg(a_i\mathrm{g}_i) \leq multideg(\mathrm{f})$. El polinomio r es llamado el residuo de la división de f por $\mathrm{g}_1, \ldots, \mathrm{g}_k$

Teorema 2.4.2 (**Lema de Dickson**).
Un ideal monomial $\mathrm{I} = \langle X^\alpha : \alpha \in \mathrm{A} \rangle$ se expresa en la forma $\mathrm{I} = \langle X^{\alpha_1}, \ldots, X^{\alpha_r} \rangle$, donde $\alpha_1, \ldots, \alpha_r \in \mathrm{A}$.
En particular, I es un ideal finitamente generado.

Proposición 2.4.1 *Sea I un ideal de $\mathrm{k}[X_0, \ldots, X_n]$. Se tienen las siguientes propiedades:*

(1) $\langle \mathrm{LT}(\mathrm{I}) \rangle$ es un ideal monomial;

(2) Existen $\mathrm{g}_1, \ldots, \mathrm{g}_r \in \mathrm{I}$ tal que $\langle \mathrm{LT}(\mathrm{I}) \rangle = \langle \mathrm{LT}(\mathrm{g}_1), \ldots, \mathrm{LT}(\mathrm{g}_r) \rangle$.

Proposición 2.4.2 *Sea I un ideal de $\mathrm{k}[X_0, \ldots, X_n]$. Supóngase que existen $g_1, \ldots, g_k \in \mathrm{I}$ tal que $\langle \mathrm{LT}(\mathrm{I}) \rangle = \langle \mathrm{LT}(\mathrm{g}_1), \ldots, \mathrm{LT}(\mathrm{g}_k) \rangle$. Entonces $\mathrm{I} = \langle \mathrm{g}_1, \ldots, \mathrm{g}_k \rangle$*

Demostración.
La relación $\langle g_1, \ldots, g_k \rangle \subseteq I$ es clara.
Sea $f \in I$, entonces $f = a_1 g_1 + \ldots + a_k g_k + r$ con $r = 0$ ó los monomios de r no son divisibles por $LT(f_1), \ldots, LT(f_k)$, por el algoritmo de la división. Supóngase que $r \neq 0$, entonces $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_k) \rangle$, pues $r = f - a_1 g_1 - \ldots - a_k g_k \in I$. Así, $LT(r)$ es divisible por algún $LT(g_1), \ldots, LT(g_k)$, por el lema 2.3.2, lo cual es una contradicción. Por tanto, $r = 0$, de modo que $f \in \langle g_1, \ldots, g_k \rangle$. Por lo tanto, $I \subseteq \langle g_1, \ldots, g_k \rangle$.

DEFINICIÓN 2.4.1 *Sea* I *un ideal de* $k[X_0, \ldots, X_n]$. *Un conjunto finito de elementos* $g_1, \ldots, g_k \in I$ *es llamado base de Groebner de* I *si:*

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_k) \rangle.$$

OBSERVACIÓN 2.4.1 *Todo ideal tiene una base de Groebner, por la proposición 2.4.1, y los elementos de la base de Groebner de* I *generan* I, *por la proposición 2.4.2.*

DEFINICIÓN 2.4.2 *Sean* $f, g \in k[X_0, \ldots, X_n] \setminus \{0\}$.

(*i*) *Sean* $\alpha = multideg(f)$ *y* $\beta = multideg(g)$, *y sea* $\lambda = (\lambda_0, \ldots, \lambda_n)$ *con* $\lambda_i = \max\{\alpha_i, \beta_i\}$, $0 \leq i \leq n$. *El monomio* X^λ *es llamado mínimo común múltiplo de* LM(f) *y* LM(g), *y se denota por* $X^\lambda = mcm(LM(f), LM(g))$.

(*ii*) *El S-polinomio de* f *y* g *es:*

$$S(f, g) = \frac{X^\lambda}{LT(f)} f - \frac{X^\lambda}{LT(g)} g$$

Los resultados que mencionaremos a continuación no estarán acompañados de una demostración, sus demostraciones las podemos encontrar en [4].

PROPOSICIÓN 2.4.3 *Sea* I *un ideal de* $k[X_0, \ldots, X_n]$, *sea* $f \in k[X_0, \ldots, X_n]$ *y sean* $g_1, \ldots, g_r \in I$ *tal que son una base de Groebner de* I. *Entonces* $f \in I$ *si y sólo si el residuo de la división de* f *por* $g_1, \ldots, g_r$ *es cero.*

TEOREMA 2.4.3 *Sea* I *un ideal de* $k[X_0, \ldots, X_n]$ *y sean* $g_1, \ldots, g_r$ *tal que* $\langle g_1, \ldots, g_r \rangle =$ I. *Entonces* $g_1, \ldots, g_r$ *son una base de Groebner de* I *si y sólo si el residuo de la división de* $S(g_i, g_j)$ *por* $g_1, \ldots, g_r$ *es cero, para cada par* $i \neq j$.

EJEMPLO 2.4.1 *Sea* $>$ *el orden graduado lexicográfico sobre* $k[X_0, \ldots, X_n]$ *tal que* $X_n > X_{n-1} > \ldots > X_0$. *Entonces* $X_1^q - X_1 X_0^{q-1}, X_2^q - X_2 X_0^{q-1}, \ldots, X_n^q - X_n X_0^{q-1}$ *es una base de Groebner de* $\langle X_1^q - X_1 X_0^{q-1}, X_2^q - X_2 X_0^{q-1}, \ldots, X_n^q - X_n X_0^{q-1} \rangle$.

Demostración.
La afirmación se comprueba combinando el teorema 2.4.3 y la siguiente identidad.

$$S(X_i^q - X_iX_0^{q-1}, X_j^q - X_jX_0^{q-1}) = X_j^q(X_i^q - X_iX_0^{q-1}) - X_i^q(X_j^q - X_jX_0^{q-1}) =$$
$$X_i^qX_jX_0^{q-1} - X_j^qX_iX_0^{q-1} = (X_jX_0^{q-1})(X_i^q - X_iX_0^{q-1}) - (X_iX_0^{q-1})(X_j^q - X_jX_0^{q-1})$$

Ejemplo 2.4.2 *Sea $>$ es el orden graduado lexicográfico sobre $\mathrm{k}[X_0, \ldots, X_n]$ tal que $X_n > X_{n-1} > \ldots > X_0$. Entonces $\{X_i^qX_j - X_iX_j^q \mid 0 \leq j < i \leq n\}$ es una base de Groebner de $\langle X_i^qX_j - X_iX_j^q \mid 0 \leq j < i \leq n\rangle$.*

Demostración.
La afirmación se comprueba combinando el teorema 2.4.3 y la siguiente identidad.

$$S(X_i^qX_j - X_iX_j^q\ ,\ X_r^qX_s - X_rX_s^q) = X_r^qX_s(X_i^qX_j - X_iX_j^q) - X_i^qX_j(X_r^qX_s - X_rX_s^q) =$$
$$X_i^qX_jX_rX_s^q - X_iX_j^qX_r^qX_s = (X_rX_s^q)(X_i^qX_j - X_iX_j^q) - (X_iX_j^q)(X_r^qX_s - X_rX_s^q)$$

Capítulo 3

Esquemas de Cayley-Bacharach

Sea X un subesquema de dimensión cero de $\mathbb{P}^n(\mathrm{k})$, sea $\mathrm{I} = \mathrm{I_X}$ el ideal homogéneo (de $\mathrm{A} = \mathrm{k}[X_0, \ldots, X_n]$) generado por los polinomios homogéneos que se anulan en X y sea $\mathrm{R} = \mathrm{A}/\mathrm{I}$ el anillo homogéneo de coordenadas de X en $\mathbb{P}^n(\mathrm{k})$. La función de Hilbert de X, $\mathrm{H_X}$, es la función de Hilbert de R. Se toma el sistema de coordenadas de manera que X_0 no es divisor de cero.
Un conjunto de s puntos es llamado esquema de Cayley-Bacharach si cualquier subconjunto de $s-1$ puntos tiene la misma función de Hilbert.

Lema 3.0.1 *Sea* k *un campo infinito, sea* V *un espacio vectorial,* $\mathrm{V} \neq 0$*, y sean* $\mathrm{V}_1, \ldots, \mathrm{V}_r$ *subespacios propios de* V*. Entonces*

$$\bigcup_{i=1}^{r} \mathrm{V}_i \neq \mathrm{V}.$$

Demostración. Ver [7]

Teorema 3.0.4 *Sea* $\mathrm{A} = \sum_{i=0}^{\infty} \mathrm{A}_i$ *un anillo graduado de Cohen-Macaulay de dimensión 1, con* $\mathrm{A}_0 = \mathrm{k}$ *un campo infinito y* A *es f.g. como* k*-algebra por* A_1*. Entonces:*

(*1*) $\mathrm{A} = \mathrm{k}[X_0, \ldots, X_n]/\mathrm{I}$*, donde* I *es un ideal homogéneo no mezclado de peso n;*

(*2*) *Si* $\dim \mathrm{A}_r = \dim \mathrm{A}_{r+1}$ *para algún* $0 \leq r$*, entonces* $\dim \mathrm{A}_{r+1} = \dim \mathrm{A}_{r+2}$.

Demostración.
(**1**) Sea I el ideal homogéneo tal que $\mathrm{A} = \mathrm{k}[X_0, \ldots, X_n]/\mathrm{I}$, entonces I es un ideal perfecto, por el teorema 1.4.2 y por que A es un anillo de Cohen-Macaulay.
Sea $\mathrm{p} \in \mathrm{Ass}_{\mathrm{k}[\tilde{X}]}(\mathrm{A})$. Entonces:

(i) depth $\mathrm{k}[X_0,\ldots,X_n]_{\mathrm{p}} = \mathrm{grade}(\mathrm{I},\mathrm{k}[X_0,\ldots,X_n])$, por la proposición 1.4.3;

(ii) depth $\mathrm{k}[X_0,\ldots,X_n]_{\mathrm{p}} = \dim\ \mathrm{k}[X_0,\ldots,X_n]_{\mathrm{p}} = \mathrm{ht}(\mathrm{p})$, pues $\mathrm{k}[X_0,\ldots,X_n]_{\mathrm{p}}$ es un anillo de Cohen-Macaulay;

(iii) $\mathrm{ht}(\mathrm{p}) = \dim \mathrm{k}[X_0,\ldots,X_n] - \dim(\mathrm{k}[X_0,\ldots,X_n]/\mathrm{p})$, pues en los polinomios esa identidad se cumple para cualquier ideal primo.

(iv) $\mathrm{grade}(\mathrm{I},\mathrm{k}[X_0,\ldots,X_n]) = \mathrm{ht}(\mathrm{I})$, por la proposición 1.4.2.

Combinando estas igualdades llegamos a

$$\mathrm{ht}(\mathrm{p}) = \mathrm{ht}(\mathrm{I}) = \dim \mathrm{k}[X_0,\ldots,X_n] - \dim(\mathrm{k}[X_0,\ldots,X_n]/\mathrm{p})$$

Así, el número $\dim(\mathrm{k}[X_0,\ldots,X_n]/\mathrm{p})$ no depende del ideal primo asociado.
Entonces, $\dim(\mathrm{k}[X_0,\ldots,X_n]/\mathrm{p}) = \dim(\mathrm{k}[X_0,\ldots,X_n]/\mathrm{I}) = 1$ para cualquier ideal primo asociado, por el lema 1.2.2. Por lo tanto, $\mathrm{ht}(\mathrm{p}) = \mathrm{ht}(\mathrm{I}) = n$ para cualquier ideal primo asociado.

(**2**)$\langle \overline{X}_0,\ldots,\overline{X}_n\rangle$ es un ideal de A de peso 1 que contiene un no divisor de cero de A, pues es el ideal irrelevante maximal de A. Sea $\mathrm{p} \in \mathrm{Ass}(\mathrm{A})$, existe $i \in \{0,\ldots,n\}$ tal que $\overline{X}_i \notin \mathrm{p}$, pues $\langle \overline{X}_0,\ldots,\overline{X}_n\rangle \neq \mathrm{p}$, entonces $\langle \overline{X}_0,\ldots,\overline{X}_n\rangle_1 \cap\ \mathrm{p} \neq \langle \overline{X}_0,\ldots,\overline{X}_n\rangle_1$.
Por tanto, $\bigcup_{\mathrm{p}\in\mathrm{Ass(A)}} (\langle \overline{X}_0,\ldots,\overline{X}_n\rangle_1 \cap\ \mathrm{p}) \neq \langle \overline{X}_0,\ldots,\overline{X}_n\rangle_1$, por el lema 3.0.1. Así, existe $r \in \langle \overline{X}_0,\ldots,\overline{X}_n\rangle_1 \setminus \bigcup_{\mathrm{p}\in\mathrm{Ass(A)}} \mathrm{p}$, r no es divisor de cero.
Usando un cambio de coordenadas se puede suponer que $\overline{X}_0$ es el no divisor de cero, por tanto, la multiplicación por $\overline{X}_0$ es inyectiva. Así, $\dim_{\mathrm{k}} \mathrm{A}_i \leq \dim_{\mathrm{k}} \mathrm{A}_{i+1}$.
Como $\dim_{\mathrm{k}} \mathrm{A}_{r+1} = \dim_{\mathrm{k}} \mathrm{A}_r$, entonces $\overline{X}_0\mathrm{A}_r = \mathrm{A}_{r+1}$. Por lo tanto, resta probar que $\overline{X}_0\mathrm{A}_{r+1} = \mathrm{A}_{r+2}$.
Sea $\mathrm{f} \in \mathrm{A}_{r+2}$, entonces $\mathrm{f} = \overline{\mathrm{F}}$ para algún $\mathrm{F} \in \mathrm{k}[X_0,\ldots,X_n]_{r+2}$.
Escribamos $\mathrm{F} = X_0\mathrm{F}_0 + X_1\mathrm{F}_1 + \ldots + X_n\mathrm{F}_n$, donde $\mathrm{F}_i \in \{0\} \cup \mathrm{k}[X_0,\ldots,X_n]_{r+1}$. Sea $\mathrm{G}_i \in \mathrm{k}[X_0,\ldots,X_n]_r$ tal que $\overline{\mathrm{F}}_i = \overline{X}_0\overline{\mathrm{G}}_i$, esto pues $\mathrm{A}_{r+1} = \overline{X}_0\mathrm{A}_r$. Entonces

$$\mathrm{f} = \overline{\mathrm{F}} = \overline{X_0\mathrm{F}_0 + X_1\mathrm{F}_1 + \ldots + X_n\mathrm{F}_n} = \overline{X_0\mathrm{F}_0 + X_0X_1\mathrm{G}_1 + \ldots + X_0X_n\mathrm{G}_n} =$$

$$\overline{X_0}\ \left(\ \overline{\mathrm{F}_0 + X_1\mathrm{G}_1 + \ldots + X_n\mathrm{G}_n}\right) \in \overline{X}_0\mathrm{A}_{r+1}$$

Por tanto, $\mathrm{A}_{r+2} \subseteq \overline{X}_0\mathrm{A}_{r+1}$, de donde se obtiene lo esperado.

Notemos que por el Teorema 3.0.4, H_{X} tiene las siguientes propiedades.

Definición 3.0.3 *Sea* $\mathrm{X} \subseteq \mathbb{P}^n$*, un conjunto finito de* s *puntos, y sea* $\mathrm{I_X} = \oplus_{r=\lambda_\mathrm{X}}^{\infty} \mathrm{I}_r$*,* $\mathrm{I}_{\lambda_\mathrm{X}}$ *es la menor componente homogénea no cero del ideal* $\mathrm{I_X}$*. Entonces existe un entero* a_X *tal que:*

(*1*) $\mathrm{H_X}(d) = dim_k \mathrm{A}_d$ *si y sólo si* $d < \lambda_\mathrm{X}$.

(*2*) $\mathrm{H_X}(d) < \mathrm{H_X}(d+1) < s$ *para* $0 \leq d < a_\mathrm{X}$.

(*3*) $\mathrm{H_X}(d) = s$ *para* $d > a_\mathrm{X}$.

El entero a_X *es llamado el a- invariante del ideal o el invariante de* X.

3.1. Truncadores

En esta sección el anillo de polinomios en $n+1$ variables, $\mathrm{A} = \mathrm{k}[X_0, \ldots, X_n]$, se considera con la graduación natural y μ denota el ideal irrelevante de A.
Si X es un conjunto finito de s puntos, entonces el ideal de X, $\mathrm{I_X}$, se denota simplemente por I. También, $\mathrm{H_X}$ denota a la función de Hilbert de X.

Definición 3.1.1 *Sea* X *un conjunto finito de* s *puntos. La truncación de* $\mathrm{H_X}$ *es:*

$$Trunc(\mathrm{H_X})(d) = \begin{cases} \mathrm{H_X}(d) & para \quad d \leq a_\mathrm{X} \\ s-1 & para \quad d > a_\mathrm{X} \end{cases}$$

Se dice que un ideal homogéneo J *trunca* $\mathrm{H_X}$ *si* $\mathrm{I} \subseteq \mathrm{J}$ *y* $\mathrm{H_J} = Trunc(\mathrm{H_X})$.

Proposición 3.1.1 *Sea* X *un conjunto finito de* s *puntos y sea* J *un ideal homogéneo. Las siguientes condiciones son equivalentes.*

(*1*) J *trunca a* $\mathrm{H_X}$*;*

(*2*) *Existe* $\mathrm{F} \in \mathrm{A}_{a_\mathrm{X}+1}$ *tal que* $\mathrm{J} = (\mathrm{I}, \mathrm{F})$ *y* $\dim_\mathrm{k}(\mathrm{J}_d/\mathrm{I}_d) = 1 \quad$ *para* $d > a_\mathrm{X}$.

Demostración.
(1)⇒(2) Supongamos que J trunca a $\mathrm{H_X}$, entonces $\mathrm{I} \subseteq \mathrm{J}$ y

$$\dim_\mathrm{k}(\mathrm{J}_d/\mathrm{I}_d) = \dim_\mathrm{k}(\mathrm{A}_d/\mathrm{I}_d) - \dim_\mathrm{k}(\mathrm{A}_d/\mathrm{J}_d) = \mathrm{H_X}(d) - \mathrm{H_J}(d) = \begin{cases} 0 & para \quad d \leq a_\mathrm{X} \\ 1 & para \quad d > a_\mathrm{X} \end{cases}$$

Así, $\mathrm{J}_d = \mathrm{I}_d$ para $d \leq a_\mathrm{X}$ y existe $\mathrm{F} \in \mathrm{J}_{a_\mathrm{X}+1} \setminus \mathrm{I}_{a_\mathrm{X}+1}$, entonces $X_0^j \mathrm{F} \in \mathrm{J}_{a_\mathrm{X}+1+j} \setminus \mathrm{I}_{a_\mathrm{X}+1+j}$ para toda j, pues X_0 no es divisor de cero de $\mathrm{R} = \mathrm{A}/\mathrm{I}$. Por tanto, $X_0^j \mathrm{F}$ es generador

de J_{a_X+1+j}/I_{a_X+1+j}, pues J_{a_X+1+j}/I_{a_X+1+j} tiene dimensión uno sobre k. Por lo tanto, si $x \in J_{a_X+1+j}$, entonces $x = cX_0^j F + \alpha$ donde $c \in k$ y $\alpha \in I_{a_X+1+j}$. Así, $J = \langle I, F \rangle$.

(2)⇒(1) Sea $F \in A_{a_X+1}$ tal que $J = \langle I, F \rangle$ y $\dim_k(J_d/I_d) = 1$ para $d > a_X$. Es claro que $H_J(d) = H_X(d)$ para $d \leq a_X$, pues $J_d = I_d$.
Sea d tal que $d > a_X$, entonces $H_J(d) = \dim_k(A_d/J_d) = \dim_k(A_d/I_d) - \dim_k(J_d/I_d) = H_X(d) - 1 = s - 1$
Con lo cual J trunca a H_X.

Definición 3.1.2 *Sea* $A = k[X_0, \ldots, X_n]$ *el anillo de polinomios y sea* I *un ideal graduado. La saturación de* I *es el ideal:*

$$J = \{\ x \in A \mid xA_d \subseteq I, \quad \textit{para} \quad \textit{algún} \quad d \geq 0\}$$

Se tiene que $I \subseteq J$ *y se dice que* I *es saturado si coincide con su saturación.*

Lema 3.1.1 *Sea* $A = k[X_0, \ldots, X_n]$ *el anillo de polinomios y sea* I *un ideal graduado de* A. *Entonces* I *es saturado si y sólo si* I *no tiene al ideal irrelevante maximal de* A *como primo asociado.*

Demostración.
Si I es saturado, supongamos que $\mu \in \mathrm{Ass}(A/I)$. Sea $x \in A \setminus I$ tal que $\mathrm{Ann}(\widetilde{x}) = \mu$, entonces $A_d \cdot x \subseteq \mu \cdot x \subseteq I$ para cualquier d. Así, $x \in I$, pues I es saturado, contradicción pues $x \notin I$. Por lo tanto $\mu \notin \mathrm{Ass}(A/I)$.
Si $\mu \notin \mathrm{Ass}(A/I)$, sean $x \in A$ y $d \geq 0$ tal que $x \cdot A_d \subseteq I$, si $x \notin I$, entonces $A_d \subseteq \mathrm{ann}(\widetilde{x})$. Por otra parte, existe $p \in \mathrm{Ass}(A/I)$ tal que $\mathrm{ann}(\widetilde{x}) \subseteq p$, por el inciso (1) de la proposición 1.2.3. Por tanto, $A_d \subseteq p$. Así, $\mu = p$ es primo asociado, lo cual es una contradicción. Por lo tanto, $x \in I$, e I es saturado.

Definición 3.1.3 *Sea* X *un conjunto finito de s puntos y sea* $F \in A_{a_X+1}$.

(*1*) *Se dice que* F *es truncador de* X *si el ideal* $J = \langle I, F \rangle$ *trunca a* H_X.

(*2*) *Se dice que* F *es truncador fuerte de* X *si el ideal* $J = \langle I, F \rangle$ *es saturado y trunca a* H_X.

Lema 3.1.2 *Sean* $L_1, \ldots, L_n \in k[X_0, \ldots, X_n]_1$, *supóngase que* $L_1, \ldots, L_n$ *son linealmente independientes sobre* k. *Entonces* $J = \langle L_1, \ldots, L_n \rangle$ *es un ideal primo de peso n tal que* $H_J(d) = 1$ *para toda d.*

Demostración.
Sea L_0 tal que $L_0, L_1, \ldots, L_n$ sea una base para A_1, entonces la afirmación se sigue del hecho de que $k[X_0, \ldots, X_n] = k[L_0, L_1, \ldots, L_n]$ y

$$k[X_0, \ldots, X_n]/\langle L_1, \ldots, L_n\rangle = k[L_0, L_1, \ldots, L_n]/\langle L_1, \ldots, L_n\rangle \cong k[L_0] \cong k[X]$$

PROPOSICIÓN 3.1.2 *Sea* X *un conjunto finito de s puntos y sea* $F \in A_{a_X+1}$. *Entonces las siguientes condiciones son equivalentes.*

(*1*) F *es truncador de* X*;*

(*2*) (I : F) *es un ideal primo asociado de* I *que describe un punto;*

(*3*) $J = \langle I, F\rangle$ *define un subesquema de* X *de grado* $s - 1$.

Demostración.
Notemos que como $F \in A_{a_X+1}$, entonces

$$J/I = \langle I, F\rangle/I \cong \langle F\rangle/\langle F\rangle \cap I \cong (A/(I : F))(-a_X - 1) \tag{3.1}$$

(1)⇒(2) Por el isomorfismo de 3.1 y el hecho de que F es truncador de X, se obtiene:

$$\dim_k(J_d/I_d) = \begin{cases} 0 & para \quad d \leq a_X \\ 1 & para \quad d > a_X \end{cases}$$

Y

$$\dim_k(A/(I : F))_d = \begin{cases} 0 & para \quad d \leq -1 \\ 1 & para \quad d > -1 \end{cases} \tag{3.2}$$

en particular $\dim_k(I : F)_1 = n$. Por tanto, hay n formas lineales linealmente independientes $L_1, \ldots, L_n$ tal que $\langle L_1, \ldots, L_n\rangle \subseteq (I : F)$. Por otra parte, $\langle L_1, \ldots, L_n\rangle$ es un ideal primo de peso n y tiene la misma función de Hilbert que (I : F), por el lema 3.1.2 y la ecuación 3.2. Así, $(I : F) = \langle L_1, \ldots, L_n\rangle$ es primo asociado de I que define un punto de $\mathbb{P}^n$.

(2)⇒(3) Si (I : F) es un ideal primo asociado de I que describe un punto, podemos suponer que el punto es P_1. Para cada $i \in \{2, \ldots, s\}$, existe $F_i \in (I : F)$ tal que $F_i(P_i) \neq 0$. Entonces para cada $i \in \{2, \ldots, s\}$ se tiene $F(P_i) = 0$, pues $F_i * F \in I$, es decir, $F_i(P_i)F(P_i) = 0$. Por otra parte, si $F(P_1) = 0$, entonces $F \in I$, lo cual es una

contradicción pues $\mathrm{F} \notin \mathrm{I}$, entonces $\mathrm{F}(\mathrm{P}_1) \neq 0$. Por tanto, los ceros del ideal $\langle \mathrm{I}, \mathrm{F} \rangle$ es el conjunto $\{\mathrm{P}_2, \ldots, \mathrm{P}_s\}$. Por otra parte, por el isomorfismo de 3.1 se tiene

$$\dim_{\mathrm{k}}(\langle \mathrm{I}, \mathrm{F} \rangle / \mathrm{I})_d = \dim_{\mathrm{k}}(\mathrm{A}/(\mathrm{I} : \mathrm{F}))_{d-a_{\mathrm{X}}-1} = \begin{cases} 0 & para \quad d \leq a_{\mathrm{X}} \\ 1 & para \quad d > a_{\mathrm{X}} \end{cases}$$

Se concluye que $\dim_{\mathrm{k}}(\mathrm{A}/\langle \mathrm{I}, \mathrm{F} \rangle)_d = s-1$ para $d > a_{\mathrm{X}}$, con lo cual J define un subesquema de grado $s-1$

(2)⇒(3) Si $\mathrm{J} = \langle \mathrm{I}, \mathrm{F} \rangle$ define un subesquema de X de grado $s-1$.
Se tiene $\dim_{\mathrm{K}}(\mathrm{J}/\mathrm{I})_d \leq \dim_{\mathrm{K}}(\mathrm{J}/\mathrm{I})_{d+1}$ para todo d, pues la multiplicación por X_0 es inyectiva; también $\dim_{\mathrm{K}}(\mathrm{A}/\mathrm{I})_d = s$ para $d > a_{\mathrm{X}}$, por la definición del a-invariante.
Se tiene $\dim_{\mathrm{k}}(\mathrm{A}/\mathrm{J})_d = s-1$ para $d >> 0$, pues J define un subesquema de X de grado $s-1$, entonces $\dim_{\mathrm{k}}(\mathrm{J}/\mathrm{I})_d = 1$ para $d >> 0$. Como $\dim_{\mathrm{k}}(\mathrm{J}/\mathrm{I})_{a_{\mathrm{X}}+1} = 1$, pues $\mathrm{F} \notin \mathrm{I}_{a_{\mathrm{X}}+1}$. Entonces $\dim_{\mathrm{k}}(\mathrm{J}/\mathrm{I})_d = 1$ para $d > a_{\mathrm{X}}$. Por lo tanto, F es truncador de X, por la proposición 3.1.1.

Corolario 3.1.1 *Sea* X *un conjunto finito de s puntos. Se tiene una correspondencia uno a uno (módulo* $\mathrm{I}_{a_{\mathrm{X}}+1}$ *) entre truncadores de* X *y subesquemas de* X *de grado* $s-1$.

Demostración.
Si F es truncador de X, entonces sea Y el subesquema definido por $\langle \mathrm{I}, \mathrm{F} \rangle$. Y es un subesquema de X de grado $s-1$, por (3) de la proposición 3.1.2.
Sea Y un subesquema de X de grado $s-1$ y sea J su ideal, entonces $\mathrm{H}_{\mathrm{X}}(a_{\mathrm{X}} + r) = s > \mathrm{H}_{\mathrm{Y}}(a_{\mathrm{X}} + r) = s-1$ para $r > 0$. Así, $\dim_{\mathrm{k}}(\mathrm{J}/\mathrm{I})_{a_{\mathrm{X}}+r} = 1$ para $r > 0$.
Por otra parte, sea $\mathrm{F} \in \mathrm{J}_{a_{\mathrm{X}}+1}$ tal que su clase en $(\mathrm{J}/\mathrm{I})_{a_{\mathrm{X}}+1}$ es el generador, entonces $X_0^j \mathrm{F} \in \mathrm{J}_{a_{\mathrm{X}}+1+j}$ es tal que su clase en $(\mathrm{J}/\mathrm{I})_{a_{\mathrm{X}}+1+j}$ es el generador. Por tanto, $\mathrm{J}_d = \langle \mathrm{I}, \mathrm{F} \rangle_d$ para $d \geq a_{\mathrm{X}}$.
Por lo tanto, F es truncador de X, por la definición 3.1.3.

Corolario 3.1.2 *Sea* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$*, sea* $\wp_i$ *el ideal de* P_i *y sea* $\mathrm{F} \in \mathrm{A}_{a_{\mathrm{X}}+1}$*. Entonces* F *es truncador de* X *si y sólo si para algún* $i \in \{1, \ldots, s\}$ *se tiene* $\mathrm{F} \notin \wp_i$ *y* $\mathrm{F} \in \bigcap_{j \neq i} \wp_j$.

LEMA 3.1.3 *Sea* $X = \{P_1, \ldots, P_s\}$, *sea* $F \in A_{a_X+1}$ *un truncador de* X *y sea* f *la imagen de* F *en* $R = A/I$. *Entonces* F *es truncador fuerte si y sólo si* $\langle f \rangle$ *no tiene al ideal irrelevante maximal* μ *de* R *como primo asociado.*

Demostración.
Se sigue del lema 3.1.1 y de la relación $A/\langle I, F\rangle \cong A/I/\langle I, F\rangle/I \cong R/\langle f\rangle$

DEFINICIÓN 3.1.4 *Sea* X *un conjunto finito de s puntos y sea* $R = A/I$ *el anillo de coordenadas de* X. *El conjunto de formas lineales cuya imagen en* R *no es divisor de cero será denotado por* $\mathbb{L}$, *esto es,* $\mathbb{L} = \{L \in A_1 : \widetilde{L} = l \in R$ *no es divisor de cero* $\}$.

PROPOSICIÓN 3.1.3 *Sea* X *un conjunto finito de s puntos y sea* $F \in A_{a_X+1}$ *un truncador de* X. *Las siguientes condiciones son equivalentes.*

(*1*) F *es truncador fuerte de* X;

(*2*) $F \notin LA_{a_X} + I_{a_X+1}$ *para cada* $L \in \mathbb{L}$;

(*3*) $F \notin \bigcap_{L\in\mathbb{L}} (LA_{a_X} + I_{a_X+1})$.

Demostración.
Se tiene $\dim_k\langle f\rangle_d = \dim_k(\langle I, F\rangle/I)_d = 1$ para todo $d \geq a_X + 1$, pues F es truncador.
Sean $L \in A_1$ y l su imagen en R, sea $\hat{l} : R_d \to R_{d+1}$ la multiplicación por l, es decir, $\hat{l}$ está dada por $\hat{l}(\beta) = l\beta$. Si l no es divisor de cero en R, entonces $\hat{l}$ es inyectiva. Por tanto, si l no es divisor de cero en R, entonces $\hat{l}$ mapea $\langle f\rangle_d$ en $\langle f\rangle_{d+1}$ para $d \geq a_X + 1$.

(1)⇒(2) Sea F un truncador fuerte de X y sea $L \in A_1$ cuya imagen en R no es divisor de cero. Supongamos que $F \in LA_{a_X} + I_{a_X+1}$, se mostrará que el ideal irrelevante maximal de R es primo asociado de $\langle f\rangle$, es decir, F no es truncador fuerte, por el lema 3.1.3.
Supóngase que $F = L_1G + R$ con $G \in A_{a_X}$ y $R \in I_{a_X+1}$, entonces $l_1 \in (\langle f\rangle : \langle g\rangle)$, pues $\widetilde{F} = \widetilde{L_1}\widetilde{G} + \widetilde{R} = f = l_1 g$. Sea $L \in A_1$ arbitrario, entonces $lg \in \langle f\rangle$, pues $l_1 lg = l\ l_1 g \in \langle f\rangle_{a_X+2}$ y $\hat{l}_1 : R_d \to R_{d+1}$ mapea $\langle f\rangle_d$ en $\langle f\rangle_{d+1}$ para $d \geq a_X + 1$. Así, $R_1 \subseteq (\langle f\rangle : \langle g\rangle)$. Por tanto, $\widetilde{\mu} = (\langle f\rangle : \langle g\rangle)$ es primo asociado de $\langle f\rangle$

(2)⇒(3) Es clara

(3)⇒(1) Si $F \notin \cap_L(LA_{a_X} + I_{a_X+1})$, donde la intersección es sobre toda forma lineal cuya imagen en R no es divisor de cero. Supongamos que F no es truncador fuerte, entonces existe g homogéneo tal que $\widetilde{\mu} = (\langle f\rangle : \langle g\rangle)$, por los lemas 2.2.1 y 3.1.3. Sea $L \in \mathbb{L}$, entonces $lg \in \langle f\rangle \setminus \{0\}$, pues $l \in \widetilde{\mu}$. Así, $\deg g \geq a_X$.
Si $\deg g \geq a_X + 1$, entonces $g \in \langle f\rangle$, pues $lg \in \langle f\rangle_{\deg g+1}$ y $\hat{l}$ mapea $\langle f\rangle_d$ en $\langle f\rangle_{d+1}$ para $d \geq a_X + 1$, lo cual es una contradicción pues $g \in R \setminus \langle f\rangle$.
Así, $\deg g = a_X$ ($g \in R_{a_X}$), $lg = cf$ para algún $c \in k$ y $f = c^{-1}\, l\, g$. Por lo tanto, se tiene $F \in LA_{a_X} + I_{a_X+1}$ para cualquier forma lineal cuya imagen en R no es divisor de cero, lo cual es una contradicción. Por lo tanto, F es un truncador fuerte.

Lema 3.1.4 *Sea* X *un conjunto finito de s puntos y sea* $L \in \mathbb{L}$. *Entonces* $L(P) \neq 0$ *para cada* $P \in X$.

Demostración.
Si $L(P) = 0$ para algún $P \in X$, sea $F \in A_{a_X+1}$ un truncador de X correspondiente a $X \setminus \{P\}$, entonces $LF \in I$, pues LF se anula en todos los puntos de X, entonces $F \in I$, pues la imagen de L en R no es divisor de cero, pero $F \in I$ es una contradicción. Por lo tanto $L(P) \neq 0$ para cada $P \in X$.

Para la siguiente proposición se usa la siguiente notación.
Si $X = \{P_1, \ldots, P_s\}$, como $X \subseteq D_+(X_0)$, escribimos $P_i = (1, p_{i1} \ldots, p_{id})$.
Para $g \in R$ e $i \in \{1, \ldots, s\}$, pongamos $g(P_i) = G(1, p_{i1} \ldots, p_{id})$, donde G es algún representante de g en A.

Proposición 3.1.4 *Sea* $X = \{P_1, \ldots, P_s\} \subseteq \mathbb{P}^n$, *sea* $F_i \in A_{a_X+1}$ *un truncador de* X *correspondiente a* $X \setminus \{P_i\}$ ($i \in \{1, \ldots, s\}$), *y sea* $\widetilde{F}_i = f_i$ *la imagen de* F_i *en* R. *Entonces*

(*1*) $\{f_1, \ldots, f_s\}$ *es una base para* R_{a_X+1}.

(*2*) *Se puede suponer que* $f_i(P_i) = 1$. *Si* $d \geq a_X + 1$, *entonces cada* $g \in R_d$ *se puede representar de manera única por:*

$$g = \widetilde{X}_0^{d-a_X-1} g(P_1) f_1 + \ldots + \widetilde{X}_0^{d-a_X-1} g(P_s) f_s$$

Demostración.
(**1**) Como $H_X(a_X + 1) = \dim_k R_{a_X+1} = s$, resta verificar que los f_i son linealmente independientes. Notemos que $f_i(P_j) = 0$ si $i \neq j$ y $f_i(P_i) \neq 0$.

Sean $c_1, \dots c_s \in k$ tal que $c_1f_1 + \dots + c_sf_s = 0$, entonces $c_1F_1 + \dots + c_sF_s \in I_{a_X+1}$. Finalmente, valuando la relación anterior en P_i, se obtiene $c_i = 0$.

(**2**) Se tiene $R_d = \widetilde{X}_0^{d-a_X-1}R_{a_X+1}$ para $d \geq a_X + 1$, pues $H_X(d) = \dim_k R_d = s$ para $d \geq a_X + 1$ y la multiplicación por $\widetilde{X}_0$ es inyectiva.
Sea $d \geq a_X + 1$ y sea $g \in R_d = \widetilde{X}_0^{d-a_X-1}R_{a_X+1}$, entonces $g = \widetilde{X}_0^{d-a_X-1}c_1f_1 + \dots + \widetilde{X}_0^{d-a_X-1}c_sf_s$, por el inciso anterior. Así, $G - X_0^{d-a_X-1}c_1F_1 + \dots + X_0^{d-a_X-1}c_sF_s \in I_n$. Finalmente, valuando la relación anterior en P_i, se obtiene $c_i = G(P_i) = g(P_i)$.

Observación 3.1.1 *En la proposición anterior, notemos que X_0 se puede cambiar por cualquier $L \in \mathbb{L}$, por el lema 3.1.4.*

Lema 3.1.5 *Sea V un espacio vectorial de dimensión finita, sea $\mathfrak{B} = \{e_1, \dots, e_k\}$ una base de V y sea W un subespacio de V. Si $C = \{i \in \{1, \dots, k\} : e_i \notin W\}$, entonces*
$$|C| \geq k - \dim W$$

Demostración.
Si $|C| < k - \dim W$, entonces existen $i_1, \dots, i_r \in \{1, \dots, k\}$, con $r = |C| < k - \dim W$, tal que $\{e_{i_1}, \dots, e_{i_r}\} \cap W = \emptyset$. Así, si $i \in \{1, \dots, k\} \setminus \{i_1, \dots, i_r\}$, entonces $e_i \in W$. Por tanto, $\dim W \geq k - r > \dim W$, lo cual es una contradicción. Por lo tanto, $|C| \geq k - \dim W$.

Proposición 3.1.5 *Sea $X = \{P_1, \dots, P_s\}$ un conjunto de s puntos. Se tienen las siguientes propiedades.*

(*1*) *X tiene al menos $s - H_X(a_X) + 1$ truncadores fuertes linealmente independientes. En particular, siempre existe un subesquema Y de X con $s - 1$ puntos tal que $H_Y = Trunc(H_X)$*

(*2*) *Para cada $r \in \{1, \dots, s\}$, existe un subesquema Y de X tal que $|Y| = r$ y $H_Y(n) = \min\{ H_X(n) , r\}$.*

Demostración.
(**1**) Puesto que R_{a_X+1} es generado por $\{\widetilde{X}_iR_{a_X} : 0 \leq i \leq n\}$ y $\dim_k \widetilde{X}_iR_{a_X} \leq \dim_k R_{a_X} = H_X(a_X) < H_X(a_X + 1) = \dim_k R_{a_X+1}$, entonces existe $i \neq j$ tal que $\widetilde{X}_iR_{a_X} \neq \widetilde{X}_jR_{a_X}$. Se deduce por tanto que
$$\dim_k \bigcap_{L \in \mathbb{L}} l\, R_{a_X} \leq \dim_k \Big(\bigcap_{r=0}^{n} \widetilde{X}_rR_{a_X} \Big) < \dim_k \widetilde{X}_iR_{a_X} \leq \dim_k R_{a_X} = H_X(a_X) < s$$

Así, $\dim_{\mathrm{k}} \bigcap_{\mathrm{L}\in\mathbb{L}} \mathrm{l}\,\mathrm{R}_{a_{\mathrm{X}}} \leq \mathrm{H}_{\mathrm{X}}(a_{\mathrm{X}}) - 1 < s$.
Por otra parte, existe un conjunto de s truncadores para los cuales su imagen en R es una base de R, por la proposición 3.1.4; y los truncadores para los cuales su imagen en R no se encuentra en $\bigcap_{\mathrm{L}\in\mathbb{L}} \mathrm{l}\,\mathrm{R}_{a_{\mathrm{X}}}$ son los truncadores fuertes, por la proposición 3.1.3.
Por tanto, hay al menos $s - \dim_{\mathrm{k}} \bigcap_{\mathrm{l}\in\mathbb{L}} \mathrm{l}\,\mathrm{R}_{a_{\mathrm{X}}}$ truncadores fuertes linealmente independientes, por el lema 3.1.5.
Finalmente, la afirmación se sigue del hecho de que $s - \dim_{\mathrm{k}} \bigcap_{\mathrm{L}} \mathrm{l}\mathrm{R}_{a_{\mathrm{X}}} \geq s - (\mathrm{H}_{\mathrm{X}}(a_{\mathrm{X}}) - 1)$

Para la última afirmación, puesto que $s + 1 - \mathrm{H}_{\mathrm{X}}(a_{\mathrm{X}}) > 0$, entonces existe al menos un truncador fuerte. Sea Y el subesquema que le corresponde a este truncador, por el inciso (3) la proposición 3.1.2. Con lo cual se tiene la última afirmación.

(**2**) Usar (1)

3.2. Separadores

Definición 3.2.1 *Sea* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$ *un conjunto de* s *puntos y sea* $\mathrm{f} \in \mathrm{R}_d$. *Se dice que* f *es separador de* P_i *hacia* $\mathrm{X} \setminus \{\mathrm{P}_i\}$, *o simplemente* f *es separador de* P_i, *si* $\mathrm{f}(\mathrm{P}_i) \neq 0$ *y* $\mathrm{f}(\mathrm{P}_j) = 0$ *para todo* $j \neq i$.
El grado de P_i, *denotado por* $\deg_{\mathrm{X}}(\mathrm{P}_i)$, *está definido por*

$$\deg_{\mathrm{X}}(\mathrm{P}_i) = \text{mín}\{\ d : \ \textit{existe}\ \mathrm{f} \in \mathrm{R}_d \ \textit{que es separador de}\ \mathrm{P}_i \ \textit{hacia}\ \mathrm{X} \setminus \{\mathrm{P}_i\}\ \}$$

Observación 3.2.1 *Sean* $\mathrm{f}, \mathrm{g} \in \mathrm{R}_d$ *separadores de* P_i *hacia* $\mathrm{X}\setminus\{\mathrm{P}_i\}$. *Entonces* $\mathrm{f} = \lambda\mathrm{g}$ *para algún* $\lambda \in \mathrm{k} \setminus \{0\}$.

Demostración.
Sean f y g $\in \mathrm{R}_d$ separadores de P_i, se analizan dos casos:
Si $d \geq a_{\mathrm{X}} + 1$. Por la proposición 3.1.4 se sigue que $\mathrm{f} = \widetilde{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{f}(\mathrm{P}_i)\mathrm{f}_i$ y $\mathrm{g} = \widetilde{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{g}(\mathrm{P}_i)\mathrm{f}_i$, de donde se obtiene la afirmación.
Si $d \leq a_{\mathrm{X}}$. Entonces $\widetilde{X}_0^{a_{\mathrm{X}}+1-d}\mathrm{f}$ y $\widetilde{X}_0^{a_{\mathrm{X}}+1-d}\mathrm{g}$ son separadores de P_i. Así, $\widetilde{X}_0^{a_{\mathrm{X}}+1-d}\mathrm{f} = \lambda\widetilde{X}_0^{a_{\mathrm{X}}+1-d}\mathrm{g}$, por el caso anterior. Por lo tanto, $\mathrm{f} = \lambda\mathrm{g}$, pues X_0 no es divisor de cero.

Proposición 3.2.1 *Sea* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$ *un conjunto de* s *puntos y sea* $\mathrm{F} \in \mathrm{A}_{a_{\mathrm{X}}+1}$. *Entonces las siguientes condiciones son equivalentes.*

(*1*) F *es separador de* P_i *hacia* $\mathrm{X} \setminus \{\mathrm{P}_i\}$;

(*2*) F *es truncador de* X *correspondiente a* $\mathrm{X} \setminus \{\mathrm{P}_i\}$.

Demostración.
Se sigue del corolario 3.1.2.

LEMA 3.2.1 *Sea* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$ *un conjunto de* s *puntos y sea* $i \in \{1, \ldots, s\}$. *Entonces*

$$\deg_{\mathrm{X}}(\mathrm{P}_i) \leq a_{\mathrm{X}} + 1$$

Demostración.
Sea $\mathrm{F} \in \mathrm{A}_{a_{\mathrm{X}}+1}$ un truncador de X correspondiente a $\mathrm{X} \setminus \{\mathrm{P}_i\}$, entonces F es un separador de P_i hacia $\mathrm{X} \setminus \{\mathrm{P}_i\}$, por la proposición 3.2.1. De donde se obtiene el resultado.

LEMA 3.2.2 *Sean* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$, $\mathrm{P} \in \mathrm{X}$ *y* $\mathrm{F} \in \mathrm{A}_{a_{\mathrm{X}}+1}$ *un truncador fuerte de* X *correspondiente a* $\mathrm{X} \setminus \{\mathrm{P}\}$. *Entonces el ideal homogéneo de* $\mathrm{Y} = \mathrm{X} \setminus \{\mathrm{P}\}$ *es* $\langle \mathrm{I}, \mathrm{F} \rangle$.

Demostración.
Es claro que $\langle \mathrm{I}, \mathrm{F} \rangle \subseteq \mathrm{I}_{\mathrm{Y}}$.
Sean $\mathrm{G} \in (\mathrm{I}_{\mathrm{Y}})_d$ y g su clase en R. Se analizan los siguientes casos:

(1) Si $\mathrm{G}(\mathrm{P}) = 0$. Entonces $\mathrm{G} \in \mathrm{I} \subseteq \langle \mathrm{I}, \mathrm{F} \rangle$, pues $\mathrm{G}(\mathrm{Q}) = 0$ para todo $\mathrm{Q} \in \mathrm{X} \setminus \{\mathrm{P}\}$.

(2) Si $\mathrm{G}(\mathrm{P}) \neq 0$ y $d > a_{\mathrm{X}}$. Se tiene $\mathrm{g} = X_0^{d-a_{\mathrm{X}}-1}\mathrm{g}(\mathrm{P})\mathrm{f}$, por la proposición 3.1.4. Así, $\mathrm{G} \in \langle \mathrm{I}, \mathrm{F} \rangle$.
Si $\mathrm{G}(\mathrm{P}) \neq 0$ y $d \leq a_{\mathrm{X}}$. Entonces para cada $\alpha \in \mathbb{Z}_{\geq 0}^{n+1}$ tal que $|\alpha| = a_{\mathrm{X}} + 1 - d$, existe $\mathrm{c}_\alpha \in \mathrm{k}$ tal que $X^\alpha \mathrm{g} = \mathrm{c}_\alpha \mathrm{f}$, por la proposición 3.1.4. Así, $\mathrm{GA}_{a_{\mathrm{X}}+1-d} \subseteq \langle \mathrm{I}, \mathrm{F} \rangle$. Por lo tanto, $\mathrm{G} \in \langle \mathrm{I}, \mathrm{F} \rangle$, pues $\langle \mathrm{I}, \mathrm{F} \rangle$ es saturado.

En cualquier caso se tiene $\mathrm{G} \in \langle \mathrm{I}, \mathrm{F} \rangle$. Por lo tanto, $\mathrm{I}_{\mathrm{Y}} = \langle \mathrm{I}, \mathrm{F} \rangle$.

PROPOSICIÓN 3.2.2 *Sean* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$, $i \in \{1, \ldots, s\}$ *y* $\mathrm{F} \in \mathrm{A}_{a_{\mathrm{X}}+1}$ *un truncador de* X *correspondiente a* $\mathrm{Y}_i = \mathrm{X} \setminus \{\mathrm{P}_i\}$. *Entonces las siguientes condiciones son equivalentes.*

(*1*) F *es truncador fuerte de* X*;*

(*2*) $\deg_{\mathrm{X}}(\mathrm{P}_i) = a_{\mathrm{X}} + 1$*;*

(*3*) $\mathrm{Y}_i = \mathrm{X} \setminus \{\mathrm{P}_i\}$ *tiene función de Hilbert* $\mathrm{H}_{\mathrm{Y}_i} = Trunc(\mathrm{H}_{\mathrm{X}})$.

Demostración.
(1)⇒(3) Si F es truncador fuerte de X, entonces $\mathrm{I}_{\mathrm{Y}_i} = \langle \mathrm{I}, \mathrm{F} \rangle$, por el lema 3.2.2. Por lo tanto, $\mathrm{H}_{\mathrm{Y}_i} = Trunc(\mathrm{H}_{\mathrm{X}})$, pues F es truncador.

(3)⇒(1) Si $\mathrm{H}_{\mathrm{Y}_i} = Trunc(\mathrm{H}_{\mathrm{X}})$. Entonces $\mathrm{I}_{\mathrm{Y}_i} = \langle \mathrm{I}, \mathrm{F} \rangle$, pues $\langle \mathrm{I}, \mathrm{F} \rangle \subseteq \mathrm{I}_{\mathrm{Y}_i}$ y también los ideales $\mathrm{I}_{\mathrm{Y}_i}$ y $\langle \mathrm{I}, \mathrm{F} \rangle$ tienen la misma función de Hilbert. Por lo tanto, $\mathrm{I}_{\mathrm{Y}_i} = \langle \mathrm{I}, \mathrm{F} \rangle$ es ideal saturado, pues cualquier ideal de un conjunto finito de puntos es saturado.

(1)⇒(2) Si F es un truncador fuerte de X. Entonces $\mathrm{I}_{\mathrm{Y}_i} = \langle \mathrm{I}, \mathrm{F} \rangle$, por el lema 3.2.2. Sea $\mathrm{g} \in \mathrm{R}_d$ un separador de P_i tal que $d = \deg_{\mathrm{X}}(\mathrm{P}_i)$, entonces $\mathrm{G} \in \mathrm{I}_{\mathrm{Y}_i} = \langle \mathrm{I}, \mathrm{F} \rangle$. Así, $\mathrm{G} = \mathrm{FK} + \mathrm{H}$ con $\mathrm{H} \in \mathrm{I}_d$ y $\mathrm{K} \in \mathrm{A}_{d-a_{\mathrm{X}}-1}$, entonces se obtiene que $\mathrm{K} \neq 0$, pues $\mathrm{K} = 0$ implicaría que $\mathrm{G} = \mathrm{H} \in \mathrm{I}$, lo cual es absurdo. Por lo tanto, $d - a_{\mathrm{X}} - 1 = \deg_{\mathrm{X}}(\mathrm{P}_i) - a_{\mathrm{X}} - 1 \geq 0$. Por otra parte, siempre se cumple que $\deg_{\mathrm{X}}(\mathrm{P}_i) \leq a_{\mathrm{X}} + 1$, por el lema 3.2.4. Al combinar las dos últimas desigualdades se obtiene lo esperado.

(2)⇒(1) Si $\deg_{\mathrm{X}}(\mathrm{P}_i) = a_{\mathrm{X}} + 1$. Supóngase que F no es truncador fuerte de X, entonces $\mathrm{F} = \mathrm{LG} + \mathrm{H}$ donde $\mathrm{L} \in \mathbb{L}$, $\mathrm{G} \in \mathrm{A}_{a_{\mathrm{X}}}$ y $\mathrm{H} \in \mathrm{I}_{a_{\mathrm{X}}+1}$, por la proposición 3.1.3. Puesto que $\mathrm{L}(\mathrm{P}) \neq 0$ para cada $\mathrm{P} \in \mathrm{X}$, por el lema 3.1.4, se sigue que $\mathrm{G} \in \mathrm{A}_{a_{\mathrm{X}}}$ es un separador de P_i. Por tanto, $\deg_{\mathrm{X}}(\mathrm{P}_i) \leq a_{\mathrm{X}}$, lo cual es una contradicción. Por lo tanto, F es truncador fuerte de X.

Definición 3.2.2 X *se dice que es un esquema de Cayley-Bacharach* (*CB- esquema*) *si cumple alguna de las siguientes condiciones equivalentes.*

(*1*) *Cada punto de* X *tiene grado* $a_{\mathrm{X}} + 1$*;*

(*2*) *Si* $\mathrm{P} \in \mathrm{X}$*, entonces* $\mathrm{H}_{\mathrm{X}\setminus\{\mathrm{P}\}} = Trunc(\mathrm{H}_{\mathrm{X}})$*;*

(*3*) *La función de Hilbert de* $\mathrm{X} \setminus \{\mathrm{P}\}$ *es independiente de la elección de* P*;*

(*4*) *Cada hipersuperficie de grado menor o igual a* $a_{\mathrm{X}} + 1$ *que contiene* $s - 1$ *puntos de* X *contiene a todos los* s *puntos de* X*.*

Observación 3.2.2 (*1*) *Siempre hay al menos* $s - \mathrm{H}_{\mathrm{X}}(a_{\mathrm{X}}) + 1$ *puntos de* X *de grado* $a_{\mathrm{X}} + 1$*, por la proposición 3.1.5.*

(*2*) *La equivalencia de los enunciados de la definición anterior se obtiene de la proposición 3.2.2.*

En lo que resta de este capítulo, se emplea la siguiente notación:
Dado $\mathrm{L} \in \mathrm{A}_1$. Se denota a la imagen de L en R por l. La función multiplicación por l es denotada por $\hat{\mathrm{l}}$, es decir, $\hat{\mathrm{l}}$ está dada por $\hat{\mathrm{l}}(\beta) = \mathrm{l}\beta$.

LEMA 3.2.3 *Sea* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$ *un conjunto de s puntos, sea* F_i *un truncador de* X *correspondiente a* $\mathrm{X} \setminus \{\mathrm{P}_i\}$ $(1 \leq i \leq s)$*, sea* $\mathrm{J} = \langle\, \mathrm{I}, \mathrm{F}_1, \ldots, \mathrm{F}_r \rangle$ *y sea* $\mathrm{L} \in \mathbb{L}$*. Entonces*

(*1*) $\hat{\mathrm{l}} : \mathrm{R}_d \to \mathrm{R}_{d+1}$ *es* k*-lineal inyectiva;*

(*2*) *Para cualquier* $k \geq 0$ *se tiene* $\dim_{\mathrm{k}}(\mathrm{J}/\mathrm{I})_{a_{\mathrm{X}}+k+1} \leq \dim_{\mathrm{k}}(\mathrm{J}/\mathrm{I})_{a_{\mathrm{X}}+k+2}$*;*

(*3*) $\hat{\mathrm{l}}^k : \mathrm{R}_{a_{\mathrm{X}}+1} \to \mathrm{R}_{a_{\mathrm{X}}+k+1}$ *es biyectiva para* $k \geq 1$*;*

(*4*) $\{\mathrm{l}^k\mathrm{f}_1, \ldots, \mathrm{l}^k\mathrm{f}_r\} \subseteq (\mathrm{J}/\mathrm{I})_{a_{\mathrm{X}}+k+1}$ *son linealmente independientes.*

Demostración.

(1) Es claro.

(2) Se sigue de que $\hat{\mathrm{l}}((\mathrm{J}/\mathrm{I})_{a_{\mathrm{X}}+k+1}) \subseteq (\mathrm{J}/\mathrm{I})_{a_{\mathrm{X}}+k+2}$ y que $\hat{\mathrm{l}}$ es inyectiva.

(3) Se sigue del hecho de que $\mathrm{H}_{\mathrm{X}}(a_{\mathrm{X}} + p) = \mathrm{H}_{\mathrm{X}}(a_{\mathrm{X}} + 1)$ para toda $p > 0$ y de que $\hat{\mathrm{l}}^k : \mathrm{R}_{a_{\mathrm{X}}+1} \to \mathrm{R}_{a_{\mathrm{X}}+k+1}$ es inyectiva

(4) Se sigue de que $\hat{\mathrm{l}}^k : \mathrm{R}_{a_{\mathrm{X}}+1} \to \mathrm{R}_{a_{\mathrm{X}}+k+1}$ es biyectiva y de que los $\{\mathrm{f}_1, \ldots, \mathrm{f}_r\}$ son linealmente independientes, esto último por la proposición 3.1.4.

LEMA 3.2.4 *Sea* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$ *un conjunto de s puntos, sea* F_i *un truncador de* X *correspondiente a* $\mathrm{X} \setminus \{\mathrm{P}_i\}$ $(1 \leq i \leq s)$*, y sean* $\mathrm{J} = \langle\, \mathrm{I}, \mathrm{F}_1, \ldots, \mathrm{F}_r \rangle$*,* $\mathrm{L} \in \mathbb{L}$ *y* $k \geq 0$*. Entonces*

$$(\mathrm{l}^k\ \mathrm{f}_1) \oplus \ldots \oplus (\mathrm{l}^k\ \mathrm{f}_r) = (\mathrm{J}/\mathrm{I})_{a_{\mathrm{X}}+k+1}$$

Demostración.
La suma indicada en la parte izquierda es en efecto una suma directa, por el inciso (4) del lema 3.2.3.
Sea $\mathrm{Y} = \mathrm{X} \setminus \{\mathrm{P}_1, \ldots, \mathrm{P}_r\}$ y sea $k_0 \in \mathbb{N}$ tal que si $k > k_0$, entonces $\mathrm{H}_{\mathrm{Y}}(k) = s - r \leq \dim_{\mathrm{k}}(\mathrm{A}/\mathrm{J})_k$, pues $\mathrm{J} \subseteq \mathrm{I}_{\mathrm{Y}}$. Por tanto, si $k > k_0$ se obtiene

$$\dim_{\mathrm{k}}(\mathrm{J}/\mathrm{I})_{a_{\mathrm{X}}+k+1} = \dim_{\mathrm{k}}(\mathrm{A}/\mathrm{I})_{a_{\mathrm{X}}+k+1} - \dim_{\mathrm{k}}(\mathrm{A}/\mathrm{J})_{a_{\mathrm{X}}+k+1} \leq r$$

Puesto que $r \leq \dim_{\mathrm{k}}(\mathrm{J/I})_{a_{\mathrm{X}}+k+1}$ para $k \geq 0$, por el inciso (4) del lema 3.2.3, entonces $\dim_{\mathrm{k}}(\mathrm{J/I})_{a_{\mathrm{X}}+k+1} = r$ para $k \geq k_0$. Es decir

$$(\mathrm{l}^k\ \mathrm{f}_1) \oplus \ldots \oplus (\mathrm{l}^k\ \mathrm{f}_r) = (\mathrm{J/I})_{a_{\mathrm{X}}+k+1} \quad para \quad k > k_0 \tag{3.3}$$

Por otra parte, supóngase que para algún k se tiene $(\mathrm{l}^k\ \mathrm{f}_1)\oplus\ldots\oplus(\mathrm{l}^k\ \mathrm{f}_r) \neq (\mathrm{J/I})_{a_{\mathrm{X}}+k+1}$, es decir, para algún k se tiene $r < \dim_{\mathrm{k}}(\mathrm{J/I})_{a_{\mathrm{X}}+k+1}$, entonces para cualquier $m > k$ se tiene $r < \dim_{\mathrm{k}}(\mathrm{J/I})_{a_{\mathrm{X}}+k+1} \leq \dim_{\mathrm{k}}(\mathrm{J/I})_{a_{\mathrm{X}}+m+1}$, por el inciso (2) del lema 3.2.3. Lo cual contradice (3.3). Por lo tanto, el resultado es cierto para cualquier k.

Lema 3.2.5 *Sea* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$ *un conjunto de* s *puntos, sea* F_i *un truncador de* X *correspondiente a* $\mathrm{X} \setminus \{\mathrm{P}_i\}$ $(1 \leq i \leq s)$*, y sea* $\mathrm{J} = \langle\ \mathrm{I}, \mathrm{F}_1, \ldots, \mathrm{F}_r\rangle$*. Entonces*

$$\dim(\mathrm{A/J})_d = \begin{cases} \dim(\mathrm{A/I})_d & para \quad d \leq a_{\mathrm{X}} \\ s - r & si \quad d > a_{\mathrm{X}} \end{cases}$$

Demostración.
Se sigue del lema 3.2.4.

Definición 3.2.3 *Sea* J *un ideal homogéneo. La primer función diferencia de la función de Hilbert de* A/J*, denotada por* $\Delta\mathrm{H}_{\mathrm{J}}(-)$*, está dada por*

$$\Delta\mathrm{H}_{\mathrm{J}}(d) = \Delta\mathrm{H}_{\mathrm{J}}(d) - \Delta\mathrm{H}_{\mathrm{J}}(d-1).$$

Si J *es el ideal de algún conjunto* X $(\mathrm{J} = \mathrm{I}_{\mathrm{X}})$*, entonces ponemos* $\Delta\mathrm{H}_{\mathrm{X}}(d)$*.*
Es claro que $\Delta\mathrm{H}_{\mathrm{X}}(d) \neq 0$ *si y sólo si* $0 \leq d \leq a_{\mathrm{X}} + 1$*.*
El último valor no cero de $\Delta\mathrm{H}_{\mathrm{X}}$ *es denotado por* $\Delta = \Delta\mathrm{H}_{\mathrm{X}}(a_{\mathrm{X}} + 1)$*.*

Observación 3.2.3 *Si* $\mathrm{L} \in \mathbb{L}$*, entonces* $\Delta\mathrm{H}_{\mathrm{X}}(n)$ *es la función de Hilbert de* R/lR

Proposición 3.2.3 *Sea* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$ *un conjunto de* s *puntos, sea* $\mathrm{L} \in \mathbb{L}$*, sea* F_i *un truncador de* X *correspondiente a* $\mathrm{X}\setminus\{\mathrm{P}_i\}$ $(1 \leq i \leq s)$ *y sea* $\mathrm{J} = \langle\ \mathrm{I}, \mathrm{F}_1, \ldots, \mathrm{F}_r\rangle$*. Suponer que las clases* $\tilde{\mathrm{f}}_1, \ldots, \tilde{\mathrm{f}}_r$ *en* $(\mathrm{R/lR})_{a_{\mathrm{X}}+1}$ *son linealmente independientes. Entonces la imagen de* L *en* A/J *no es divisor de cero.*

Demostración.
Sea $\mathrm{G} \in \mathrm{A}_d$ tal que $\mathrm{LG} \in \mathrm{J}_{d+1}$, se analizan los siguientes casos

(1) Si $d < a_{\mathrm{X}}$. Entonces $\mathrm{LG} \in \mathrm{J}_{d+1} = \mathrm{I}_{d+1}$. Así, $\mathrm{G} \in \mathrm{I}_d$, pues $\mathrm{L} \in \mathbb{L}$.

(2) Si $d > a_{\mathrm{X}}$. Se tiene $\mathrm{LG} \in \mathrm{J}_{d+1} = \mathrm{I}_{d+1} \oplus \mathrm{L}^{d-a_{\mathrm{X}}}\mathrm{F}_1 \oplus \ldots \oplus \mathrm{L}^{d-a_{\mathrm{X}}}\mathrm{F}_r$, por el lema 3.2.4. Entonces $\mathrm{LG} = \alpha + \mathrm{c}_1\mathrm{L}^{d-a_{\mathrm{X}}}\mathrm{F}_1 + \ldots + \mathrm{c}_r\mathrm{L}^{d-a_{\mathrm{X}}}\mathrm{F}_r$ con $\alpha \in \mathrm{I}_{d+1}$. Así, $\mathrm{G} - \mathrm{c}_1\mathrm{L}^{d-a_{\mathrm{X}}-1}\mathrm{F}_1 + \ldots + \mathrm{c}_r\mathrm{L}^{d-a_{\mathrm{X}}-1}\mathrm{F}_r \in \mathrm{I}_d$, pues $\mathrm{L}(\mathrm{G} - \mathrm{c}_1\mathrm{L}^{d-a_{\mathrm{X}}-1}\mathrm{F}_1 + \ldots + \mathrm{c}_r\mathrm{L}^{d-a_{\mathrm{X}}-1}\mathrm{F}_r) = \alpha \in \mathrm{I}_{d+1}$ y $\mathrm{L} \in \mathbb{L}$. Por lo tanto, $\mathrm{G} \in \mathrm{I}_d \oplus \mathrm{L}^{d-a_{\mathrm{X}}-1}\mathrm{F}_1 \oplus \ldots \oplus \mathrm{L}^{d-a_{\mathrm{X}}-1}\mathrm{F}_r = \mathrm{J}_d$, por el lema 3.2.4.

(3) Si $d = a_{\mathrm{X}}$. Se tiene $\mathrm{LG} = \alpha + \mathrm{c}_1\mathrm{F}_1 + \ldots + \mathrm{c}_r\mathrm{F}_r$ con $\alpha \in \mathrm{I}_{a_{\mathrm{X}}+1}$, por el lema 3.2.4, entonces $\tilde{\mathrm{l}}\tilde{\mathrm{g}} = 0 = \tilde{\alpha} + \mathrm{c}_1\tilde{\mathrm{f}}_1 + \ldots \mathrm{c}_r\tilde{\mathrm{f}}_r = \mathrm{c}_1\tilde{\mathrm{f}}_1 + \ldots \mathrm{c}_r\tilde{\mathrm{f}}_r \in \mathrm{R}/\mathrm{lR}$. Puesto que los $\tilde{\mathrm{f}}_i$ son linealmente independientes, se sigue que $\mathrm{c}_i = 0$. Así, $\mathrm{LG} = \alpha \in \mathrm{I}_{a_{\mathrm{X}}+1}$. Por tanto, $\mathrm{G} \in \mathrm{I}_{a_{\mathrm{X}}} = \mathrm{J}_{a_{\mathrm{X}}}$, pues $\mathrm{L} \in \mathbb{L}$.

PROPOSICIÓN 3.2.4 *Sea* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$ *un conjunto de s puntos, sea* F_i *truncador de* X *correspondiente a* $\mathrm{X} \setminus \{\mathrm{P}_i\}$*, y sean* $r \in \{1, \ldots, \Delta\}$, $\mathrm{J} = \langle\, \mathrm{I}, \mathrm{F}_1, \ldots, \mathrm{F}_r\rangle$, $\mathrm{Y} = \mathrm{X} \setminus \{\mathrm{P}_1, \ldots, \mathrm{P}_r\}$ *y* $\mathrm{L} \in \mathbb{L}$*. Entonces las siguientes condiciones son equivalentes.*

(*1*) *Las clases residuales* $\tilde{\mathrm{f}}_1, \ldots, \tilde{\mathrm{f}}_r$ *son linealmente independientes en* $(\mathrm{R}/\mathrm{lR})_{a_{\mathrm{X}}+1}$

(*2*) $\mathrm{I}_{\mathrm{Y}} = \langle \mathrm{I}, \mathrm{F}_1, \ldots, \mathrm{F}_r \rangle$.

(*3*) $\mathrm{H}_{\mathrm{Y}}(d) = \begin{cases} \mathrm{H}_{\mathrm{X}}(d) & si \quad d \leq a_{\mathrm{X}} \\ s - r & si \quad d > a_{\mathrm{X}} \end{cases}$

Además, es posible reenumerar los puntos de X *para que las condiciones sean satisfechas.*

Demostración.
(2)⇒(3) Se sigue del lema 3.2.5.

(3)⇒(2) Como J e I_{Y} tienen la misma función de Hilbert, por el lema 3.2.5, y $\mathrm{J} \subseteq \mathrm{I}_{\mathrm{Y}}$, entonces $\mathrm{J} = \mathrm{I}_{\mathrm{Y}}$

(1)⇒(2) Sea $\mathrm{G} \in \mathrm{I}_{\mathrm{Y}}$ homogéneo de grado d. Se analizan los siguientes casos

(a) Si $\mathrm{G}(\mathrm{P}_j) = 0$ para todo $j \in \{1, \ldots, r\}$. Entonces $\mathrm{G} \in \mathrm{I} \subseteq \mathrm{J}$

(b) Si $\mathrm{G}(\mathrm{P}_j) \neq 0$ para algún $j \in \{1, \ldots, r\}$ y $d > a_{\mathrm{X}}$. Entonces $\mathrm{g} = \widetilde{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{c}_1\mathrm{f}_1 + \ldots + \widetilde{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{c}_r\mathrm{f}_r$ con $\mathrm{c}_j \neq 0$ para algún $1 \leq j \leq r$, por la proposición 3.1.4 y por que $\mathrm{f}_j(\mathrm{P}_j) = 0$ para $j > r$. Así, $\mathrm{G} \in \mathrm{J}$.

(c) Si $G(P_j) \neq 0$ para algún $j \in \{1, \ldots, r\}$ y $d \leq a_X$. Puesto que para cualquier monomio de peso $\alpha = a_X + 1 - d$, el polinomio $X^\alpha G$ cumple las condiciones de los casos anteriores, se tiene $X^\alpha G \in J$, por lo que $A_{a_X+1-d} G \subseteq J$.
Por otra parte, J es un ideal saturado pues la imagen de L en A/J no es divisor de cero, por la proposición 3.2.3. Por lo tanto, $G \in J$.

Por tanto, $I_Y \subseteq J$ y como $J \subseteq I_Y$, se concluye que $J = I_Y$

(2)⇒(1) Se sabe que $\{f_1, \ldots, f_r\} \subseteq R_{a_X+1}$ es linealmente independiente, por la proposición 3.1.4. Por lo tanto, resta verificar que $\langle f_1, \ldots, f_r \rangle \cap \ lR_{a_X} = \{0\}$.
Sea $g \in R_{a_X}$ tal que $lg = c_1 f_1 + \ldots + c_r f_r \in \langle f_1, \ldots, f_r \rangle \cap lR_{a_X}$, puesto que $l(P_i)g(P_i) = 0$ para $r + 1 \leq i$, por la proposición 3.1.4; se sigue que $g(P_i) = 0$ para $r + 1 \leq i$, por el lema 3.1.4 y por que $L \in \mathbb{L}$. Así, $G \in (I_Y)_{a_X} = I_{a_X}$. Por lo tanto, $g = 0$.

La última parte de la proposición se sigue de que: $\{f_1, \ldots, f_s\}$ es una base de R_{a_X+1}, entonces $\{\tilde{f}_1, \ldots, \tilde{f}_r\}$ genera el espacio vectorial $(R/lR)_{a_X+1}$. Así, de $\{\tilde{f}_1, \ldots, \tilde{f}_r\}$ se puede obtener un subconjunto linealmente independiente.

Corolario 3.2.1 *Bajo las condiciones de la proposición anterior. Supongamos que* $\Delta \geq 2$ *y sea* $r \in \{1, \ldots, \Delta - 1\}$. *Entonces las siguientes condiciones son equivalentes.*

(*1*) Y *es un esquema de Cayley-Bacharach con función de Hilbert*

$$H_Y(d) = \text{mín}\{H_X(d), s - r\}$$

(*2*) *Para cada* $i \in \{r + 1, \ldots, s\}$, *las clases residuales* $\tilde{f}_1, \ldots, \tilde{f}_r, \tilde{f}_i$ *son linealmente independientes en* $(R/lR)_{a_X+1}$

Demostración.
(1)⇒(2) Si Y tiene función de Hilbert $H_Y(d) = \text{mín}\{H_X(d), s - r\}$. Como Y es esquema de Cayley-Bacharach, entonces para cada $i \in \{r + 1, \ldots, s\}$, $Z_i = Y \setminus \{P_i\} = X \setminus \{P_1, \ldots, P_r, P_i\}$ tiene función de Hilbert $H_{Z_i}(d) = Trunc(H_Y)(d) = \text{mín}\{H_X(d), s - r - 1\}$. Por lo tanto, las clases residuales $\tilde{f}_1, \ldots, \tilde{f}_r, \tilde{f}_i$ son linealmente independientes en $(R/lR)_{a_X+1}$, por la proposición 3.2.4.

(2)⇒(1) Si para cada $i \in \{r + 1, \ldots, s\}$, las clases $\tilde{f}_1, \ldots, \tilde{f}_r, \tilde{f}_i$ son linealmente independientes en $(R/lR)_{a_X+1}$. Sea $Z_i = Y \setminus \{P_i\} = X \setminus \{P_1, \ldots, P_r, P_i\}$. Por la proposición 3.2.4 y por que en particular $\tilde{f}_1, \ldots, \tilde{f}_r$ son linealmente independientes, se obtiene

$\mathrm{H_Y}(d) = \mín\{\mathrm{H_X}(d), s-r\}$ y $\mathrm{H_{Z_i}}(d) = \mín\{\mathrm{H_X}(d), s-r-1\} = Trunc(\mathrm{H_Y})(d)$
Por lo tanto, Y es un esquema de Cayley-Bacharach.

COROLARIO 3.2.2 *Sea* X *un esquema de Cayley-Bacharach. Supóngase que se han renumerado los puntos de* X *de manera que* $\mathrm{Y} = \mathrm{X} \setminus \{\mathrm{P}_1, \ldots, \mathrm{P}_\Delta\}$ *satisface (1) de la proposición 3.2.4. Entonces* Y *es un esquema de Cayley-Bacharach*

Demostración.
De la proposición 3.2.4 se obtiene

$$\mathrm{H_Y}(d) = \begin{cases} \mathrm{H_X}(d) & si \;\; d \leq a_\mathrm{X} \\ s-\Delta & si \;\; d > a_\mathrm{X} \end{cases} = \begin{cases} \mathrm{H_X}(d) & si \;\; d \leq a_\mathrm{X} \\ \mathrm{H_X}(a_\mathrm{X}) & si \;\; d > a_\mathrm{X} \end{cases}$$

Por lo tanto, $a_\mathrm{Y} = a_\mathrm{X} - 1$. Si Y no es un esquema de Cayley-Bacharach, entonces existe $\mathrm{P}_i \in \mathrm{Y}$ tal que $\deg_\mathrm{Y}(\mathrm{P}_i) < a_\mathrm{Y} + 1 = a_\mathrm{X}$, por el lema 3.2.1 y por la relación anterior. Así, existe $\mathrm{G} \in \mathrm{A}_{a_\mathrm{Y}}$ que es un separador de P_i hacia $\mathrm{Y} \setminus \{\mathrm{P}_i\}$.
Por otra parte, sea $\mathrm{L} \in \mathrm{A}_1$ que se anule únicamente en P_i pero no otro punto de X. Puesto que $\mathrm{LG}(\mathrm{P}) = 0$ para todo $\mathrm{P} \in \mathrm{Y}$, se sigue que $\mathrm{LG} \in \mathrm{I(Y)}_{a_{\mathrm{Y}+1}} = (\mathrm{I}, \mathrm{F}_1, \ldots, \mathrm{F}_\Delta)_{a_\mathrm{X}} = \mathrm{I}_{a_\mathrm{X}}$, por (2) de la proposición 3.2.4. Así, $\mathrm{G}(\mathrm{P}) = 0$ para todo $\mathrm{P} \in \mathrm{X} \setminus \{\mathrm{P}_i\}$, pues L únicamente se anula en P_i. Por tanto, G es un separador de P_i hacia $\mathrm{X} \setminus \{\mathrm{P}_i\}$.
Por lo tanto, $\deg_\mathrm{X}(\mathrm{P}_i) \leq a_\mathrm{Y} < a_\mathrm{X}$, por el lema 3.2.1, lo cual es absurdo pues X es un esquema de Cayley-Bacharach.
Por lo tanto, Y es un esquema de Cayley-Bacharach.

COROLARIO 3.2.3 *Si* X *es un esquema de Cayley-Bacharach con* $\Delta = 1$*, entonces* $\mathrm{X} \setminus \{\mathrm{P}_i\}$ *es un esquema de Cayley-Bacharach para cada* $i \in \{1, \ldots, s\}$*.*

Demostración.
Cada $\tilde{\mathrm{f}}_i$ es no cero en $(\mathrm{R/lR})_{a_\mathrm{X}+1}$. Con lo cual el $\mathrm{X} \setminus \{\mathrm{P}_i\}$ satisface las condiciones de la proposición 3.2.4 y por el corolario 3.2.2 se tiene lo esperado.

3.3. El Módulo Canónico

Sea R el anillo de coordenadas de X, entonces R es un anillo de Cohen-Macaulay de dimensión 1 y $\overline{X}_0 \in \mathrm{R}$ no es divisor de cero de R. Como $\mathrm{k}[\overline{X}_0] \subseteq \mathrm{R}$, entonces R es $\mathrm{k}[\overline{X}_0]$-módulo.
La siguiente proposición asegura que R es $\mathrm{k}[\overline{X}_0]$-módulo libre de rango s.

PROPOSICIÓN 3.3.1 *Sea* $\mathrm{R} = \bigoplus_{i=0}^{\infty} \mathrm{R}_i$ *el anillo de coordenadas de* X. *Para cada* $i \in \{0, \ldots, a_{\mathrm{X}}+1\}$, *sean* $h_i = \Delta\mathrm{H}_{\mathrm{X}}(i)$, $\overline{\mathrm{B}}_i = \{\overline{\alpha}_{i1}, \ldots, \overline{\alpha}_{ih_i}\}$ *una base sobre* k *de* $(\mathrm{R}/\overline{X}_0\mathrm{R})_i$ *y* $\mathrm{B}_i = \{\alpha_{i1}, \ldots, \alpha_{ih_i}\}$ *representantes homogéneos de* $\overline{\alpha}_{ij}$. *Entonces*

$$\mathrm{B} = \bigcup_{i=0}^{a_{\mathrm{X}}+1} \mathrm{B}_i \qquad \textit{es una base de } \mathrm{R} \textit{ sobre } \mathrm{k}[\overline{X}_0].$$

Demostración.
Se verificará que cada R_d está generado por B. La prueba será por inducción sobre d. El resultado es cierto si $d = 0$, pues $\mathrm{R}_0 = \mathrm{k}$ y B_0 tiene su generador.
Supongamos que para algún d se tiene que $\mathrm{R}_{d-1} \subseteq \langle \mathrm{B} \rangle$, y se analizan los siguientes casos:

(1) Si $d \leq a_{\mathrm{X}} + 1$. Sea $\beta \in \mathrm{R}_d$, puesto que $\overline{\beta} = \sum_{i=1}^{h_d} c_i\overline{\alpha}_{di} \in (\mathrm{R}/\overline{X}_0\mathrm{R})_d$, se sigue que $\beta = \sum_{i=1}^{h_d} c_i\alpha_{di} + \overline{X}_0\alpha$ con $\alpha \in \mathrm{R}_{d-1}$. Por tanto, $\beta = \sum_{i=1}^{h_d} c_i\alpha_{di} + \overline{X}_0\alpha \in \langle \mathrm{B} \rangle$, por la hipótesis de inducción. Por lo tanto, $\mathrm{R}_d \subseteq \langle \mathrm{B} \rangle$.

(2) Si $d > a_{\mathrm{X}} + 1$. Puesto que $\mathrm{H}_{\mathrm{X}}(d) = \mathrm{H}_{\mathrm{X}}(a_{\mathrm{X}} + 1)$ y $\overline{X}_0$ no es divisor de cero, se sigue que $\mathrm{R}_d = \overline{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{R}_{a_{\mathrm{X}}+1}$. Por tanto, $\mathrm{R}_d \subseteq \langle \mathrm{B} \rangle$, por el caso anterior.

Por otra parte, el conjunto $\mathrm{B} = \bigcup_{1=0}^{a_{\mathrm{X}}+1} \mathrm{B}_i$ es linealmente independiente.
Como $\sum_{i=0}^{a_{\mathrm{X}}+1} h_i = s$, entonces pongamos $\mathrm{B} = \{\alpha_1 \ldots \alpha_s\}$.
Sean $f_1, \ldots, f_s \in \mathrm{k}[\overline{X}_0]$ tal que $\sum_{i=1}^{s} f_i\alpha_i = 0$. Escribamos $f_i = a_{i0} + \overline{X}_0 f_i^1$ con $f_i^1 \in \mathrm{k}[\overline{X}_0]$ y sea $k = \text{máx}\{\deg f_1, \ldots, \deg f_s\}$. Puesto que $\sum_{i=1}^{s} \overline{f}_i\overline{\alpha}_i = \sum_{i=1}^{s} a_{i0}\overline{\alpha}_i = 0 \in \mathrm{R}/\overline{X}_0\mathrm{R}$

y $\mathrm{B} = \{\alpha_1 \dots \alpha_s\}$ es un conjunto linealmente independiente, se sigue que $a_{i0} = 0$ para todo $i \in \{1, \dots, s\}$. Así, $\sum_{i=1}^{s} f_i \alpha_i = \sum_{i=1}^{s} \overline{X}_0 f_i^1 \alpha_i = \overline{X}_0 \sum_{i=1}^{s} f_i^1 \alpha_i = 0$. Por tanto, $\sum_{i=1}^{s} f_i^1 \alpha_i = 0$ con $k - 1 = \text{máx}\{\deg f_1^1, \dots, \deg f_s^1\}$, pues $\overline{X}_0$ no es divisor de cero. Continuando con el proceso, se tiene que cada $f_i = 0$. Por lo tanto, el conjunto $\{\alpha_1 \dots \alpha_s\}$ es linealmente independiente.

PROPOSICIÓN 3.3.2 *Sean* $\mathrm{R} = \bigoplus_{i=0}^{\infty} \mathrm{R}_i$ *el anillo de coordenadas de* X

(*1*) *Se tiene el isomorfismo de* $\mathrm{k}[\overline{X}_0]-$*módulos graduados*

$$\mathrm{R} \cong \bigoplus_{i=0}^{a\mathrm{X}+1} (\mathrm{k}[\overline{X}_0](-i))^{\mathrm{h}_i} \qquad \textit{donde} \qquad \mathrm{h}_i = \Delta \mathrm{H}_{\mathrm{X}}(i)$$

(*2*) $\overline{X}_0$ *es tracendente sobre* k.

Demostración.

(1) Se sigue de la proposición 3.3.1.

(2) Se sigue del inciso anterior y la proposición 1.2.1.

OBSERVACIÓN 3.3.1 *Sean* M *un* A*-módulo y* R *una* A*-algebra. Entonces* $\mathrm{Hom_A}(\mathrm{R}, \mathrm{M})$ *es un* R*-módulo con la operación*

$$\begin{array}{rccc} * \ : & \mathrm{R} \times \mathrm{Hom_A}(\mathrm{R}, \mathrm{M}) & \longrightarrow & \mathrm{Hom_A}(\mathrm{R}, \mathrm{M}) \\ & (\mathrm{r}, \mathrm{f}) & \longmapsto & \mathrm{r} * \mathrm{f} = \mathrm{f_r} \end{array} \qquad \textit{donde} \qquad \begin{array}{rccc} \mathrm{f_r} \ : & \mathrm{R} & \longrightarrow & \mathrm{M} \\ & \mathrm{x} & \longmapsto & \mathrm{f(rx)} \end{array}$$

DEFINICIÓN 3.3.1 *El* R*-módulo graduado*

$$\omega_{\mathrm{R}} = \mathrm{Hom}_{\mathrm{k}[\overline{X}_0]}(\mathrm{R}, \mathrm{k}[\overline{X}_0])(-1) \qquad \textit{donde :}$$

$$\left(\mathrm{Hom}_{\mathrm{k}[\overline{X}_0]}(\mathrm{R}, \mathrm{k}[\overline{X}_0])\right)_d = \{\varphi \in \mathrm{Hom}_{\mathrm{k}[\overline{X}_0]}(\mathrm{R}, \mathrm{k}[\overline{X}_0]) \ : \ \varphi(\mathrm{R}_m) \subseteq \mathrm{k}[\overline{X}_0]_{m+d}\}$$

Es llamado el módulo canónico de R.
Ver el inciso (3) de la definición 2.1.4, el inciso (4) la observación 2.1.2 y la observación 3.3.1.

LEMA 3.3.1 *Sean* R *el anillo de coordenadas de* X *y* ω_{R} *su módulo canónico. Entonces:*

$$\omega_{\mathrm{R}} \cong \bigoplus_{i=0}^{a_{\mathrm{X}}+1} (\ \mathrm{k}[\overline{X}_0](i)\ )^{\mathrm{h}_i}(-1)$$

Demostración.
Del inciso (1) de la proposición 3.3.2 se tiene que $\mathrm{R} = \bigoplus_{i=0}^{a_{\mathrm{X}}+1} (\mathrm{k}[\overline{X}_0](-i))^{\mathrm{h}_i}$. Por tanto, del lema 2.1.2 y del lema 2.1.1 se sigue que

$$\omega_{\mathrm{R}}(1) = \mathrm{Hom}_{\mathrm{k}[\overline{X}_0]}(\mathrm{R}, \mathrm{k}[\overline{X}_0]) \cong \mathrm{Hom}_{\mathrm{k}[\overline{X}_0]}(\bigoplus_{i=0}^{a_{\mathrm{X}}+1} (\mathrm{k}[\overline{X}_0](-i))^{\mathrm{h}_i}, \mathrm{k}[\overline{X}_0]) \cong$$

$$\bigoplus_{i=0}^{a_{\mathrm{X}}+1} \mathrm{Hom}_{\mathrm{k}[\overline{X}_0]}((\mathrm{k}[\overline{X}_0](-i))^{\mathrm{h}_i}, \mathrm{k}[\overline{X}_0]) \cong \bigoplus_{i=0}^{a_{\mathrm{X}}+1} (\mathrm{Hom}_{\mathrm{k}[\overline{X}_0]}(\mathrm{k}[\overline{X}_0](-i), \mathrm{k}[\overline{X}_0])^{\mathrm{h}_i}) \cong$$

$$\bigoplus_{i=0}^{a_{\mathrm{X}}+1} (\ \mathrm{k}[\overline{X}_0](i)\ )^{\mathrm{h}_i}$$

de donde se sigue de inmediato el resultado.

PROPOSICIÓN 3.3.3 *Sea* R *el anillo de coordenadas de* X*, sea* ω_{R} *el módulo canónico de* R *y sea* $d \in \mathbb{Z}$*. Entonces*

$$\mathrm{H}_{\omega_{\mathrm{R}}}(-d) + \mathrm{H}_{\mathrm{X}}(d) = s$$

Demostración.
Por el lema 3.3.1 se sigue que

$$\mathrm{H}_{\omega_{\mathrm{R}}}(-d) = \sum_{i=0}^{a_{\mathrm{X}}+1} \mathrm{h}_i \dim_{\mathrm{k}} \mathrm{k}[\overline{X}_0]_{i-1-d} = \sum_{i \in \mathrm{G}_d} \mathrm{h}_i$$

donde $\mathrm{G}_d = \{0 \leq i \leq a_{\mathrm{X}} + 1 \mid 0 \leq i - 1 - d\}$
Por el incisio (1) de la proposición 3.3.2 se sigue que

$$\mathrm{H}_{\mathrm{X}}(d) = \sum_{i=0}^{a_{\mathrm{X}}+1} \mathrm{h}_i \dim_{\mathrm{k}} \mathrm{k}[\overline{X}_0]_{d-i} = \sum_{i \in \mathrm{F}_d} \mathrm{h}_i$$

donde $\mathrm{F}_d = \{0 \leq i \leq a_{\mathrm{X}} + 1 \mid \ 0 \leq d - i\}$
Por otra parte, puesto que $\mathrm{G}_d \bigcap \mathrm{F}_d = \emptyset$ y $\mathrm{G}_d \bigcup \mathrm{F}_d = \{0, \ldots, a_{\mathrm{X}}+1\}$, pues $i-1-d \geq 0$ si y sólo si $d - i < 0$, se deduce que

$$\mathrm{H}_{\omega_{\mathrm{R}}}(-d) + \mathrm{H}_{\mathrm{X}}(d) = \sum_{i \in \mathrm{G}_d} \mathrm{h}_i + \sum_{i \in \mathrm{F}_d} \mathrm{h}_i = \sum_{i=0}^{a_{\mathrm{X}}+1} \mathrm{h}_i = s$$

Lema 3.3.2 *Sea* R *el anillo de coordenadas de* X*, sea* ω_{R} *el módulo canónico de* R *y sean* $\varphi \in (\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$, f_i *un separador de* P_i *hacia* $\mathrm{X} \setminus \{\mathrm{P}_i\}$ $(i \in \{1, \ldots, s\})$ *y* $\mathrm{g} \in \mathrm{R}_d$*. Entonces*

(1) $\mathrm{gf}_i = \mathrm{g}(\mathrm{P}_i)\overline{X}_0^d \mathrm{f}_i$.

(2) $(\mathrm{g} * \varphi)(\mathrm{f}_i) = \varphi(\mathrm{gf}_i) = \varphi(\mathrm{g}(\mathrm{P}_i)\overline{X}_0^d \mathrm{f}_i) = \mathrm{g}(\mathrm{P}_i)\overline{X}_0^d \varphi(\mathrm{f}_i)$.

(3) Si $\varphi(\mathrm{f}_i) = 0$ *para algún* $i \in \{1, \ldots, s\}$*, entonces* $(\mathrm{f}_i * \varphi)\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}} = 0$.

Demostración.

(1) Usar el inciso (2) de la proposición 3.1.4 y el hecho de que $\mathrm{gf}_i(\mathrm{P}_j) = \mathrm{g}(\mathrm{P}_j)\delta_{ij}$.

(2) Usar el inciso anterior y que φ es $\mathrm{k}[\overline{X}_0]$-lineal.

(3) Si $\varphi(\mathrm{f}_i) = 0$. Sea $j \in \{1, \ldots, s\}$, entonces $(\mathrm{f}_i * \varphi)(\mathrm{f}_j) = \mathrm{f}_i(\mathrm{P}_j)\overline{X}_0^{a_{\mathrm{X}}+1}\varphi(\mathrm{f}_j) = 0$, por el inciso anterior y por que $\mathrm{f}_i(\mathrm{P}_j) = \delta_{ij}$. Por tanto, $\mathrm{f}_i * \varphi$ se anula en $\{\mathrm{f}_1, \ldots, \mathrm{f}_s\}$. Donde $\{\mathrm{f}_1, \ldots, \mathrm{f}_s\}$ es la base de $\mathrm{R}_{a_{\mathrm{X}}+1}$, por la proposición 3.1.4. Por lo tanto, $\mathrm{f}_i * \varphi\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}} = 0$.

Observación 3.3.2 *Notemos que:*

$$(\omega_{\mathrm{R}})_d = \big(\mathrm{Hom}_{\mathrm{k}[\overline{X}_0]}(\mathrm{R}, \mathrm{k}[\overline{X}_0])\big)_{d-1} = \{\varphi \in \mathrm{Hom}_{\mathrm{k}[\overline{X}_0]}(\mathrm{R}, \mathrm{k}[\overline{X}_0]) \ : \ \varphi(\mathrm{R}_m) \subseteq \mathrm{k}[\overline{X}_0]_{m+d-1}\}$$

$$(\omega_{\mathrm{R}})_{-a_{\mathrm{X}}} = \big(\mathrm{Hom}_{\mathrm{k}[\overline{X}_0]}(\mathrm{R}, \mathrm{k}[\overline{X}_0])\big)_{-a_{\mathrm{X}}-1} = \{\varphi \in \mathrm{Hom}_{\mathrm{k}[\overline{X}_0]}(\mathrm{R}, \mathrm{k}[\overline{X}_0]) \ : \ \varphi(\mathrm{R}_m) \subseteq \mathrm{k}[\overline{X}_0]_{m-a_{\mathrm{X}}-1}\}$$

Por tanto, si $\varphi \in (\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$*, entonces*

$$\varphi(\mathrm{R}_m) \subseteq \mathrm{k}[\overline{X}_0]_{m-a_{\mathrm{X}}-1} = 0 \ \ \textit{para} \ \ m < a_{\mathrm{X}} + 1 \qquad \text{y} \qquad \varphi(\mathrm{R}_{a_{\mathrm{X}}+1}) \subseteq \mathrm{k}[\overline{X}_0]_0 = \mathrm{k}$$

Por lo tanto, si $\varphi \in (\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$*, entonces*

$$\varphi\big|_{\mathrm{R}_m} = 0 \ \ \textit{para} \ \ m \in \{0, \ldots, a_{\mathrm{X}}\} \qquad \text{y}$$

$$\varphi\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}} \in (\mathrm{R}_{a_{\mathrm{X}}+1})^* \qquad (\varphi\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}} \textit{ es } \mathrm{k} - \textit{lineal, pues es } \mathrm{k}[\overline{X}_0] - \textit{lineal})$$

LEMA 3.3.3 *Sea* R *el anillo de coordenadas de* X*, sea* ω_{R} *el módulo canónico de* R *y sea* $\psi \in (\mathrm{R}_{a_{\mathrm{X}}+1})^*$ *que se anula en* $\overline{X}_0\mathrm{R}_{a_{\mathrm{X}}}$*. Entonces existe* $\varphi \in (\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$ *tal que* $\varphi\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}} = \psi$.

Demostración.

Por la proposición 3.1.4 se sigue que si $d \geq a_{\mathrm{X}}+1$, entonces cada $\mathrm{g} \in \mathrm{R}_d$ es de la forma $\mathrm{g} = \overline{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{g}_1$, para un único $\mathrm{g}_1 \in \mathrm{R}_{a_{\mathrm{X}}+1}$.

Se define ahora $\varphi : \mathrm{R} \longrightarrow \mathrm{k}[\overline{X}_0]$, en las componentes homogéneas de R, por

$$\varphi(\mathrm{g}) = \begin{cases} 0 & \text{si} \quad d \leq a_{\mathrm{X}} \text{ y } \mathrm{g} \in \mathrm{R}_d \\ \overline{X}_0^{d-a_{\mathrm{X}}-1}\psi(\mathrm{g}_1) & \text{si} \quad d \geq a_{\mathrm{X}}+1, \quad \mathrm{g} \in \mathrm{R}_d \text{ y } \mathrm{g} = \overline{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{g}_1 \end{cases}$$

φ tiene las siguientes propiedades.

(**a**) φ es k-lineal, pues ψ lo es.

(**b**) φ es $\mathrm{k}[\overline{X}_0]$-lineal. Sean $\mathrm{g} \in \mathrm{R}_d$ y $r \geq 0$, entonces

$$\overline{X}_0^r\mathrm{g} = \begin{cases} \overline{X}_0^r\mathrm{g} & \text{si} \quad d \leq a_{\mathrm{X}} \quad \text{y} \quad d+r \leq a_{\mathrm{X}} \\ \overline{X}_0^{d+r-a_{\mathrm{X}}-1}(\overline{X}_0\overline{X}_0^{a_{\mathrm{X}}-d}\mathrm{g}) & \text{si} \quad d \leq a_{\mathrm{X}}, \quad d+r \geq a_{\mathrm{X}}+1 \\ \overline{X}_0^{d+r-a_{\mathrm{X}}-1}\mathrm{g}_1 & \text{si} \quad d \geq a_{\mathrm{X}}+1 \quad \text{y} \quad \mathrm{g} = \overline{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{g}_1 \end{cases}$$

Por tanto

$$\varphi(\overline{X}_0^r\mathrm{g}) = \begin{cases} 0 & \text{si} \quad d \leq a_{\mathrm{X}} \\ \overline{X}_0^{d+r-a_{\mathrm{X}}-1}\psi(\mathrm{g}_1) & \text{si} \quad d \geq a_{\mathrm{X}}+1 \quad \text{y} \quad \mathrm{g} = \overline{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{g}_1 \end{cases}$$

Por otra parte

$$\overline{X}_0^r\varphi(\mathrm{g}) = \begin{cases} 0 & \text{si} \quad d \leq a_{\mathrm{X}} \\ \overline{X}_0^{d+r-a_{\mathrm{X}}-1}\psi(\mathrm{g}_1) & \text{si} \quad d \geq a_{\mathrm{X}}+1 \quad \text{y} \quad \mathrm{g} = \overline{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{g}_1 \end{cases}$$

Por lo tanto, para todo $\mathrm{g} \in \mathrm{R}_d$ y para todo $r \geq 0$ se tiene $\varphi(\overline{X}_0^r\mathrm{g}) = \overline{X}_0^r\varphi(\mathrm{g})$. Y la afirmación se sigue de la linealidad de las operaciones

(**c**) $\varphi \in (\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$. Se verificará que $\varphi(\mathrm{R}_m) \subseteq \mathrm{k}[\overline{X}_0]_{m-a_{\mathrm{X}}-1}$ para todo $m \geq 0$. De la definición de φ se obtiene que si $\mathrm{g} \in \mathrm{R}_m$, entonces

$$\varphi(\mathrm{g}) = \begin{cases} 0 \in \mathrm{k}[\overline{X}_0]_{m-a_{\mathrm{X}}-1} & \text{si} \quad m \leq a_{\mathrm{X}} \\ \overline{X}_0^{m-a_{\mathrm{X}}-1}\psi(\mathrm{g}_1) \in \mathrm{k}[\overline{X}_0]_{m-a_{\mathrm{X}}-1} & \text{si} \quad m \geq a_{\mathrm{X}}+1 \end{cases}$$

(**c**) $\varphi\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}} = \psi$. Es inmediato de la definición de φ.

PROPOSICIÓN 3.3.4 *Sea* R *el anillo de coordenadas de* X *y sea* ω_{R} *el módulo canónico de* R. *Entonces la función*

$$\begin{array}{rccc} \gamma: & (\omega_{\mathrm{R}})_{-a_{\mathrm{X}}} & \longrightarrow & (\mathrm{R}_{a_{\mathrm{X}}+1})^* \\ & \varphi & \longmapsto & \varphi\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}} \end{array}$$

Es una biyección entre $(\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$ *y el conjunto de funcionales de* $\mathrm{R}_{a_{\mathrm{X}}+1}$ *que se anulan en* $\overline{X}_0\mathrm{R}_{a_{\mathrm{X}}}$.

Demostración.
(**a**) γ está bien definida, por la observación 3.3.2.

(**b**) γ es inyectiva. Sean $\varphi_1, \varphi_2 \in (\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$ tales que $\gamma(\varphi_1) = \gamma(\varphi_2) = \varphi_1\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}} = \varphi_2\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}}$. Se demostrará que $\varphi_1\big|_{\mathrm{R}_d} = \varphi_2\big|_{\mathrm{R}_d}$ para toda $d \geq 0$.
Si $d \in \{0, \ldots, a_{\mathrm{X}}\}$, entonces $\varphi_1\big|_{\mathrm{R}_d} = \varphi_2\big|_{\mathrm{R}_d} = 0$, por la observación 3.3.2.
Si $d \geq a_{\mathrm{X}} + 1$. Puesto que φ_1 y φ_2 son $\mathrm{k}[\overline{X}_0]-$lineales y $\mathrm{R}_d = \overline{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{R}_{a_{\mathrm{X}}+1}$, pues $\mathrm{H}_{\mathrm{X}}(d) = \mathrm{H}_{\mathrm{X}}(a_{\mathrm{X}}+1)$ y $\overline{X}_0$ no es divisor de cero, se sigue que

$$\varphi_1\big|_{\mathrm{R}_d} = \varphi_1\big|_{\overline{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{R}_{a_{\mathrm{X}}+1}} = \overline{X}_0^{d-a_{\mathrm{X}}-1}\varphi_1\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}} = \overline{X}_0^{d-a_{\mathrm{X}}-1}\varphi_2\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}} =$$

$$\varphi_2\big|_{\overline{X}_0^{d-a_{\mathrm{X}}-1}\mathrm{R}_{a_{\mathrm{X}}+1}} = \varphi_2\big|_{\mathrm{R}_d}$$

Por lo tanto, $\varphi_1\big|_{\mathrm{R}_d} = \varphi_2\big|_{\mathrm{R}_d}$ para toda $d \geq 0$, es decir, $\varphi_1 = \varphi_2$

(**c**) Se afirma que si $\varphi \in (\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$, entonces $\gamma(\varphi) = \varphi\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}}$ se anula en $\overline{X}_0\mathrm{R}_{a_{\mathrm{X}}}$.
Puesto que φ es $\mathrm{k}[\overline{X}_0]-$ lineal y $\varphi(\mathrm{R}_{a_{\mathrm{X}}}) = 0$, por la observación 3.3.2, se sigue que

$$\varphi\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}}(\overline{X}_0\mathrm{R}_{a_{\mathrm{X}}}) = \varphi(\overline{X}_0\mathrm{R}_{a_{\mathrm{X}}}) = \overline{X}_0\varphi(\mathrm{R}_{a_{\mathrm{X}}}) = 0$$

(**d**) γ es una biyección entre $(\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$ y los funcionales de $\mathrm{R}_{a_{\mathrm{X}}+1}$ que se anulan en $\overline{X}_0\mathrm{R}_{a_{\mathrm{X}}}$. Esta afirmación se sigue del lema 3.3.3.

PROPOSICIÓN 3.3.5 *Sean* R *el anillo de coordenadas de* X, ω_{R} *el módulo canónico de* R, $\varphi \in (\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$, $\mathrm{f}_i \in \mathrm{R}_{a_{\mathrm{X}}+1}$ *un separador de* P_i $(i \in \{1, \ldots, s\})$ *y* $\mathrm{f} \in \mathrm{R}_d$. *Entonces*

(*1*) $\mathrm{f} * \varphi = 0$ *si y sólo si* $\mathrm{f} * \varphi\big|_{\mathrm{R}_{a_{\mathrm{X}}+1}} = 0 \in (\mathrm{R}_{a_{\mathrm{X}}+1})^*$

(*2*) $\mathrm{Ann_R}(\varphi) = 0$ *si y sólo si* $\varphi(\mathrm{f}_i) \neq 0$ *para todo* $i \in \{1, \ldots, s\}$.

Demostración.

(1) Supóngase que $\mathrm{f} * \varphi\big|_{\mathrm{R}_{a_\mathrm{X}+1}} = 0$, y sea $\mathrm{h} \in \mathrm{R}_d$. Se debe probar que $\mathrm{f} * \varphi(\mathrm{h}) = 0$.

(a) Si $d \leq a_\mathrm{X}$. Puesto que $\overline{X}_0^{a_\mathrm{X}+1-d}\mathrm{h} \in \mathrm{R}_{a_\mathrm{X}+1}$ y $\mathrm{f} * \varphi$ es $\mathrm{k}[\overline{X}_0]-$lineal, se sigue que

$$\mathrm{f} * \varphi(\overline{X}_0^{a_\mathrm{X}+1-d}\mathrm{h}) = \overline{X}_0^{a_\mathrm{X}+1-d}\mathrm{f} * \varphi(\mathrm{h}) = 0$$

Por lo tanto, $\mathrm{f} * \varphi(\mathrm{h}) = 0$, pues $\overline{X}_0$ no es divisor de cero.

(b) Si $d > a_\mathrm{X}$. Existe $\mathrm{g}_1 \in \mathrm{R}_{a_\mathrm{X}+1}$ tal que $\mathrm{h} = \overline{X}_0^{d-a_\mathrm{X}-1}\mathrm{g}_1$, por la proposición 3.1.4, de donde se sigue que

$$\mathrm{f} * \varphi(\mathrm{h}) = \mathrm{f} * \varphi(\overline{X}_0^{d-a_\mathrm{X}-1}\mathrm{g}_1) = \overline{X}_0^{d-a_\mathrm{X}-1}\mathrm{f} * \varphi(\mathrm{g}_1) = 0.$$

Si $\mathrm{f} * \varphi = 0$, entonces es claro que $\mathrm{f} * \varphi\big|_{\mathrm{R}_{a_\mathrm{X}+1}} = 0$.

(2) Supóngase que $Ann_\mathrm{R}(\varphi) = 0$, y supóngase que $\varphi(\mathrm{f}_i) = 0$ para algún $i \in \{1, \ldots, s\}$. Entonces $\mathrm{f}_i * \varphi\big|_{\mathrm{R}_{a_\mathrm{X}+1}} = 0$, por el inciso (3) del lema 3.3.2. Por tanto, $\mathrm{f}_i * \varphi = 0$, por el inciso anterior, contradiciendo que $Ann_\mathrm{R}(\varphi) = 0$. Por lo tanto, $\varphi(\mathrm{f}_i) \neq 0$ para todo $i \in \{1, \ldots, s\}$.

Supóngase que $\varphi(\mathrm{f}_i) \neq 0$ para todo $i \in \{1, \ldots, s\}$, y sea $\mathrm{g} \in \mathrm{R}_d \setminus \{0\}$. Puesto que $\mathrm{g}(\mathrm{P}_i) \neq 0$ para algún $i \in \{1, \ldots, s\}$, por el inciso (2) del lema 3.3.2 se infiere que $(\mathrm{g} * \varphi)(\mathrm{f}_i) = \mathrm{g}(\mathrm{P}_i)\overline{X}_0^d\varphi(\mathrm{f}_i) \neq 0$. Por tanto, para cualquier $\mathrm{g} \in \mathrm{R}_d \setminus \{0\}$ se tiene $\mathrm{g} * \varphi \neq 0$. Por lo tanto, $Ann_\mathrm{R}(\varphi) = 0$.

Definición 3.3.2 *Sea* A *un anillo, sea* M *un* A*-módulo y sea* $m \in \mathrm{M}$. *Se dice que* m *es fiel si* $\mathrm{Ann_A}(m) = \{0\}$.

Teorema 3.3.1 *Sea* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$ *un conjunto de* s *puntos, sea* R *el anillo de coordenadas de* X *y sea* ω_R *el módulo canónico de* R. *Las siguientes condiciones son equivalentes.*

(*1*) X *es un esquema de Cayley-Bacharach;*

(*2*) *Existe un elemento fiel en* $(\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$*;*

(*3*) *Un elemento genérico de* $(\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$ *es fiel;*

(*4*) *Existe una sucesión homogénea de* R*-módulos graduados exacta*

$$0 \to \mathrm{R} \to (\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$$

Demostración.
Es claro que (3) implica (2) y que (2) es equivalente a (4).

(1)⇒(3) Supóngase que X es un esquema de Cayley-Bacharach. Sea $\mathrm{F}_i \in \mathrm{A}_{a_{\mathrm{X}}+1}$ un truncador de X hacia $\mathrm{X} \setminus \{\mathrm{P}_i\}$ y sea $\varphi \in (\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$ un elemento genérico. Como $\deg_{\mathrm{X}}(\mathrm{P}_i) = a_{\mathrm{X}} + 1$, entonces F_i es un truncador fuerte, por la proposición 3.2.2. Así, para cada $i \in \{1, \ldots, s\}$ se tiene $\mathrm{f}_i \notin \overline{X}_0 \mathrm{R}_{a_{\mathrm{X}}}$, por la proposición 3.1.3. Por tanto, para cada $i \in \{1, \ldots, s\}$ se tiene $\varphi(\mathrm{f}_i) \neq 0$, por la proposición 3.3.4 y por que φ es genérico. Por lo tanto, $\mathrm{Ann}_{\mathrm{R}}(\varphi) = 0$, por el inciso (2) de la proposición 3.3.5.

(2)⇒(1) Sea $\varphi \in (\omega_{\mathrm{R}})_{-a_{\mathrm{X}}}$ tal que $\mathrm{Ann}_{\mathrm{R}}(\varphi) = 0$, entonces para cada $i \in \{1, \ldots, s\}$ se tiene $\varphi(\mathrm{f}_i) \neq 0$, por el inciso (2) de la proposición 3.3.5. Así, para cada $i \in \{1, \ldots, s\}$ se tiene que $\mathrm{f}_i \notin \overline{X}_0 \mathrm{R}_{a_{\mathrm{X}}}$, pues $\varphi(\overline{X}_0 \mathrm{R}_{a_{\mathrm{X}}}) = 0$. Por tanto, para cada $i \in \{1, \ldots, s\}$ se tiene $\deg_{\mathrm{X}}(\mathrm{P}_i) = a_{\mathrm{X}} + 1$, por la proposición 3.2.2 y la proposición 3.1.3. Por lo tanto, X es un esquema de Cayley-Bacharach.

Capítulo 4

Códigos Algebro-Geométricos

En todo lo que sigue salvo que se diga lo contrario, se considerara $\mathrm{k} = \mathbb{F}_q$ el campo finito con $q = p^r$ elementos, $\mathbb{P}^n(\mathrm{k})$ es el n-espacio proyectivo sobre k y para $\mathrm{p} \in \mathbb{P}^n(\mathrm{k})$ se usará la representación estandar de p, es decir, esa en la que la primer coordenada no cero desde la izquierda es 1.
Se considera al anillo de polinomios, $\mathrm{A} = \mathrm{k}[X_0, \ldots, X_n] = \bigoplus_{i=0}^{\infty} \mathrm{A}_i$, con la graduación natural. Para $\mathrm{X} \subset \mathbb{P}^n(\mathrm{k})$ será $\mathrm{I_X}$ el ideal homogéneo generado por los polinomios homogéneos que se anulan en todos los elementos de X.
En este capítulo analizaremos códigos que se obtienen por la evaluación de polinomios homogéneos en un conjunto finito de puntos del espacio proyectivo sobre un campo finito. También se definirán códigos asociados al módulo canónico. A estos códigos les llamaremos códigos algebraicos.

Definición 4.0.3 *El producto interno canónico sobre* k^s *está definido por*

$$< a,\ b >= \sum_{i=1}^{s} a_i b_i$$

para $a = (a_1, \ldots, a_s)$ *y* $b = (b_1, \ldots, b_s) \in \mathrm{k}^s$.

Definición 4.0.4 *Sean* $\mathrm{k} = \mathrm{F}_q$ *y* W *un subespacio de* k^s. *Supóngase que* W *es de dimensión* k.

(*1*) *Se dice que* W *es un* $[s, k]$ *código lineal.*

(*2*) *Sean* $\mathrm{a}, \mathrm{b} \in \mathrm{k}^s$. *Se define la distancia de Hamming entre* a *y* b *por*

$$d(\mathrm{a}, \mathrm{b}) = |\{\ i \mid \mathrm{a}_i \neq \mathrm{b}_i\ \}|$$

(*3*) *Sea* $a \in \mathrm{k}^s$. *El peso de hamming de* a *está definido por*

$$wt(a) = d(\mathrm{a}, 0) = |\{\ i \mid a_i \neq 0\ \}|$$

(*4*) *La distancia mínima de* W *está definida como*

$$\mathrm{d}(\mathrm{W}) = \mathrm{mín}\{\ wt(a) \mid a \in \mathrm{W} \setminus \{0\}\ \} = \mathrm{mín}\{\ d(a,b) \mid a, b \in \mathrm{W}\ y\ a \neq b\ \}$$

Si W *es un* $[s, k]$ *código lineal con distancia mínima* d, *entonces se dirá que* W *es un* $[s, k, d]$ *código*

Definición 4.0.5 *Si* $\mathrm{W} \subseteq \mathrm{k}^s$ *es un código lineal, entonces*

$$\mathrm{W}^{\perp} = \{\ a \in \mathrm{k}^s \mid\ <\ a,\ w >= 0 \text{ para todo } w \in \mathrm{W}\}$$

es llamado el dual de W

Definición 4.0.6 *Sean* $\mathrm{X} = \{\mathrm{P}_1 \ldots \mathrm{P}_s\} \subseteq \mathbb{P}^n(\mathrm{k})$, *y* κ *un* k−*espacio vectorial de funciones de* X *en* k *de dimensión finita.*
La función evaluación sobre X *es:*

$$ev : \kappa \to \mathrm{k}^s \qquad \textit{donde} \qquad ev(f) = (f(\mathrm{P}_1), \ldots, f(\mathrm{P}_s))$$

define el código $C_{\mathrm{X}} = ev(\kappa)$, *al cual llamaremos el código algebraico sobre* k *determinado por* X

Si $\mathrm{X} \subseteq \mathbb{P}^n(\mathrm{k})$ es dado, con cada punto en representación estandar, y $\kappa = \mathrm{A}_d$ es la d-componente graduada del anillo de polinomios, entonces al correspondiente código $C_{\mathrm{X}}(d) = ev(\mathrm{A}_d)$ le llamaremos el código algebraico sobre k determinado por X de grado d.
Es claro que como espacio vectorial $C_{\mathrm{X}}(d)$ es isomorfo a $\mathrm{A}_d/\mathrm{I}_{\mathrm{X}}(d)$, donde $\mathrm{I}_{\mathrm{X}} = \bigoplus_{0 \leq j} \mathrm{I}_{\mathrm{X}}(j)$ es el ideal de X. Por lo tanto, la dimensión del código se obtiene con la función de Hilbert de $\mathrm{A}/\mathrm{I}_{\mathrm{X}}$.

Uno de los problemas de la teoría de códigos es la construcción de códigos de dimensión y distancia mínima grandes, en comparación con su longitud. Hay ciertas limitaciones, una de ellas es la siguiente cota.

PROPOSICIÓN 4.0.6 *Para un* $[s, k, d]$ *código* W *se cumple*

$$k + d \leq s + 1$$

Demostración.
Sea $\mathrm{N} = \{(a_1, \ldots, a_s) \in \mathrm{k}^s \ : \ a_i = 0 \ \text{ para } \ i \geq d \ \}$, entonces cualquier $a \in \mathrm{N}$ tiene peso menor o igual a $d-1$, $\dim \mathrm{N} = d-1$ y $\mathrm{W} \cap \mathrm{N} = 0$. Por lo tanto

$$d - 1 + k = \dim \mathrm{N} + \dim \mathrm{W} = \dim(\mathrm{N} + \mathrm{W}) \leq n$$

De donde se sigue el resultado.

4.1. El Código Reed-Muller afín generalizado

Sea $\mathrm{X} = \{ \ (1, a_1, \ldots, a_n) \ \in \mathbb{P}^n(\mathrm{k}) \mid a_i \in \mathrm{k} \ \}$, es decir, X es el espacio afín visto dentro del espacio proyectivo, con lo cual nos permitimos denotar $\mathrm{X} = \mathbb{A}^n$.
El código $C_{\mathbb{A}^n}(d)$ es conocido como el código Reed-Muller afín generalizado y se acostumbra denotar por $\mathrm{RMAG}(d, n)$.
Se presenta la serie de resultados que caracterizan a $\mathrm{RMAG}(d, n)$.

TEOREMA 4.1.1 *Sea* $\mathrm{X} = \mathbb{A}^n = \{ \ (1, a_1, \ldots, a_n) \ \in \mathbb{P}^n(\mathrm{k}) \mid a_i \in \mathrm{k} \ \}$, *entonces*

$$\mathrm{I}_{\mathbb{A}^n} = \langle X_1^q - X_1 X_0^{q-1}, X_2^q - X_2 X_0^{q-1}, \ldots, X_n^q - X_n X_0^{q-1} \rangle$$

Demostración.
Es claro que $\langle X_1^q - X_1 X_0^{q-1}, \ldots, X_n^q - X_n X_0^{q-1} \rangle \subseteq \mathrm{I}_{\mathbb{A}^n}$.
Resta probar que $\mathrm{I}_{\mathbb{A}^n} \subseteq \langle X_1^q - X_1 X_0^{q-1}, \ldots, X_n^q - X_n X_0^{q-1} \rangle$, y esto será por inducción sobre n.
Para $n = 1$. Sea $\mathrm{f}(X_0, X_1) \in \mathrm{I}_{\mathbb{A}^1}$ (homogéneo), entonces $\mathrm{f}(X_0, X_1) = X_0^r \mathrm{f}_1(X_0, X_1)$, donde X_0 no divide a $\mathrm{f}_1(X_0, X_1)$. Puesto que $\mathrm{f}_1(1, X_1) \in \mathrm{K}[X_1]$ satisface $\mathrm{f}_1(1, \alpha) = 0$ para todo $\alpha \in \mathrm{k}$, se sigue que $\mathrm{f}_1(1, X_1) = \mathrm{f}_2(X_1) \prod_{\alpha \in \mathrm{K}} (X_1 - \alpha) = \mathrm{f}_2(X_1)(X_1^q - X_1)$. Por tanto, $\mathrm{f}_1(X_0, X_1) = (\mathrm{f}_1(1, X_1))^h = \mathrm{f}_2^h(X_0, X_1)(X_1^q - X_1 X_0^{q-1})$. Por lo tanto

$$\mathrm{f}(X_0, X_1) = X_0^r \mathrm{f}_1(X_0, X_1) = X_0^r \mathrm{f}_2^h(X_0, X_1)(X_1^q - X_1 X_0^{q-1}) \in \langle X_1^q - X_1 X_0^{q-1} \rangle$$

Supongamos que existe un n para el cual $\mathrm{I}_{\mathbb{A}^n} = \langle X_1^q - X_1 X_0^{q-1}, \ldots, X_n^q - X_n X_0^{q-1} \rangle$, y sea $\mathrm{f} \in \mathrm{I}_{\mathbb{A}^{n+1}}$ (homogéneo). Pongamos $\mathrm{f} = \mathrm{f}_1 + X_{n+1}\mathrm{g}$, donde $\mathrm{f}_1 \in \mathrm{k}[X_0, \ldots, X_n]$ y $\mathrm{g} \in \mathrm{k}[X_0, \ldots, X_{n+1}]$ (homogéneos). Se verificará que tanto f_1 como $X_{n+1}\mathrm{g}$ pertenecen al ideal $\langle X_1^q - X_1 X_0^{q-1}, \ldots, X_{n+1}^q - X_{n+1} X_0^{q-1} \rangle$, de donde se obtendrá que $\mathrm{f} \in \langle X_1^q - X_1 X_0^{q-1}, \ldots, X_{n+1}^q - X_{n+1} X_0^{q-1} \rangle$.

Para cualquier $w \in \mathbb{A}^n$ sea $u = (w, 0) \in \mathbb{A}^{n+1}$. Puesto que $0 = \mathrm{f}(u) = \mathrm{f}_1(w) + 0\mathrm{g}(u) = \mathrm{f}_1(w)$, se sigue que $\mathrm{f}_1 \in \mathrm{I}_{\mathbb{A}^n}$. Por tanto

$$\mathrm{f}_1 \in \langle X_1^q - X_1X_0^{q-1}, \ldots, X_n^q - X_nX_0^{q-1}\rangle_{\mathrm{k}[X_0,\ldots,X_n]} \subseteq \langle X_1^q - X_1X_0^{q-1}, \ldots, X_{n+1}^q - X_{n+1}X_0^{q-1}\rangle$$

Así, $X_{n+1}\mathrm{g} \in \mathrm{I}_{\mathbb{A}^{n+1}}$, pues $\mathrm{f} = \mathrm{f}_1 + X_{n+1}\mathrm{g}$ y tanto f como f_1 pertencen a $\mathrm{I}_{\mathbb{A}^{n+1}}$.
Por otra parte, por el algoritmo de la división, usando el orden lexicográfico tal que $X_{n+1} > X_n > \ldots > X_0$, se tiene $\mathrm{g} = \mathrm{h}(X_{n+1}^{q-1} - X_0^{q-1}) + \mathrm{r}$ con r polinomio homogéneo y cada monomio de r no es divisible por X_{n+1}^{q-1}. Por consiguiente, existen $\mathrm{r}_0(X_0, \ldots, X_n), \mathrm{r}_1(X_0, \ldots, X_n), \ldots, \mathrm{r}_{q-2}(X_0, \ldots, X_n)$ tal que

$$\mathrm{r} = \mathrm{r}_0(X_0, \ldots, X_n) + \mathrm{r}_1(X_0, \ldots, X_n)X_{n+1} + \ldots + \mathrm{r}_{q-2}(X_0, \ldots, X_n)X_{n+1}^{q-2}$$

Se verificará que todos los $\mathrm{r}_i(X_0, \ldots, X_n)$ pertenecen a $\mathrm{I}_{\mathbb{A}^n}$. Supongamos que esto no es cierto, es decir, supongamos que hay un i_0 tal que para algún $u = (1, u_1, \ldots, u_n) \in \mathbb{A}^n$ se tiene $\mathrm{r}_{i_0}(u) = \mathrm{r}_{i_0}(1, u_1, \ldots, u_n) \neq 0$. Para cualquier $\alpha \in \mathrm{k}^*$ se tiene $0 = \alpha\mathrm{g}(1, u_1, \ldots, u_n, \alpha) = \alpha[\mathrm{h}(1, u_1, \ldots, u_n, \alpha)(1-1)+\mathrm{r}(1, u_1, \ldots, u_n, \alpha)] = \alpha\mathrm{r}(1, u_1, \ldots, u_n, \alpha)$, pues $X_{n+1}\mathrm{g} \in \mathrm{I}_{\mathbb{A}^{n+1}}$. Por tanto, para cualquier $\alpha \in \mathrm{k}^*$ se tiene $\mathrm{r}(u, \alpha) = \mathrm{r}(1, u_1, \ldots, u_n, \alpha) = 0$. Por lo tanto, $\mathrm{r}(u, X_{n+1}) = \mathrm{r}_0(u) + \ldots \mathrm{r}_{i_0}(u)X_{n+1}^{i_0} + \ldots + \mathrm{r}_{q-2}(u){X_{n+1}}^{q-2}$ es un polinomio no cero en X_{n+1} de grado menor o igual a $q-2$ que tiene a todos los elementos no cero de k como raices, lo cual es una contradicción. Así, todos los $\mathrm{r}_i(X_0, \ldots, X_n)$ pertenecen al ideal $\mathrm{I}_{\mathbb{A}^n} = \langle X_1^q - X_1X_0^{q-1}, \ldots, X_n^q - X_nX_0^{q-1}\rangle_{\mathrm{k}[X_0,\ldots,X_n]}$. Por lo tanto

$$X_{n+1}\mathrm{g} = \mathrm{h}(X_{n+1}^q - X_{n+1}X_0^{q-1}) + X_{n+1}\mathrm{r} \in < X_1^q - X_1X_0^{q-1}, \ldots, X_{n+1}^q - X_{n+1}X_0^{q-1} >$$

PROPOSICIÓN 4.1.1 *Sea* $\mathrm{X} = \mathbb{A}^n = \{\ (1, a_1, \ldots, a_n)\ \in \mathbb{P}^n(\mathrm{k}) \mid a_i \in \mathrm{k}\ \}$, *sea* $\mathrm{I}_{\mathbb{A}^n} = \langle X_1^q - X_1X_0^{q-1}, X_2^q - X_2X_0^{q-1}, \ldots, X_n^q - X_nX_0^{q-1}\rangle$, *y sea* $\mathrm{J} = \langle X_1^q, X_2^q, \ldots, X_n^q\rangle$. *Entonces* $\mathrm{A/J}$ *y* $\mathrm{A/I}_{\mathbb{A}^n}$ *tienen la misma función de Hilbert.*
Además, una base sobre k *de* $\mathrm{A}_d/\mathrm{J}_d$ *se obtiene de los monomios de grado* d *que no pertenecen a* J.

Demostración.
Con el orden graduado lexicográfico tal que $X_n > \ldots > X_0$, los generadores del ideal $\langle X_1^q - X_1X_0^{q-1}, \ldots, X_n^q - X_nX_0^{q-1}\rangle$ son una base de Groebner, por el ejemplo 2.4.1. Así, $\langle LT(X_1^q - X_1X_0^{q-1}, \ldots, X_n^q - X_nX_0^{q-1})\rangle = \langle X_1^q, \ldots, X_n^q\rangle$. Entonces la afirmación se sigue del teorema 2.3.1.

LEMA 4.1.1 *Sea* $\mathrm{X} = \mathbb{A}^n = \{\ (1, a_1, \ldots, a_n)\ \in \mathbb{P}^n(\mathrm{k}) \mid a_i \in \mathrm{k}\ \}$, *sea* $n > 1$ *y sea* $d \geq q$, *entonces*

$$\mathrm{H}_{\mathbb{A}^n}(d) = \sum_{j=0}^{q-1} \mathrm{H}_{\mathbb{A}^{n-1}}(d-j)$$

Demostración.
Por la proposición 4.1.1, se tiene que $\mathrm{I}_{\mathbb{A}^n} = \langle X_1^q - X_1X_0^{q-1}, \ldots, X_n^q - X_nX_0^{q-1}\rangle$ y $\mathrm{J} = \langle X_1^q, \ldots, X_n^q\rangle$ tienen la misma función de Hilbert, Por tanto, se trabajará con J. Notemos que $\dim(\mathrm{k}[X_0, \ldots, X_n]/\langle X_1^q, \ldots, X_n^q\rangle)_d$ es igual al número de monomios de grado d que no están en J.
Para $d \geq q$ y para $j \in \{0, \ldots, q-1\}$, sean
$T_j = \{X_0^k\, X_1^{i_1} \ldots X_{n-1}^{i_{n-1}}\, X_n^j \mid k+i_1+\ldots+i_{n-1}+j = d,\ 0 \leq i_r \leq q-1\} \subset \mathrm{k}[X_0, \ldots, X_n]$
y $L_j = \{X_0^k\, X_1^{i_1} \ldots X_{n-1}^{i_{n-1}} \mid k+i_1+\ldots i_{n-1} = d-j,\ 0 \leq i_r \leq q-1\} \subset \mathrm{k}[X_0, \ldots, X_{n-1}]$.
Es fácil verificar que T_j y L_j tienen las siguientes propiedades:
(a) T_j consta de monomios de grado d que no están en J;
(b) $T_i \cap T_j = \emptyset$ si $i \neq j$;
(c) $\bigcup_{j=0}^{q-1} T_j$ son todos los monomios de grado d que no están en J;
(d) La asignación $\mathrm{K}_j : T_j \longrightarrow L_j$ que está dada por $\mathrm{K}_j(\, X_0^k\, X_1^{i_1} \ldots X_{n-1}^{i_{n-1}}\, X_n^j) = X_0^k\, X_1^{i_1} \ldots X_{n-1}^{i_{n-1}}$ es biyectiva;
(e) L_j consta de todos los monomios de $\mathrm{k}[X_0, \ldots, X_{n-1}]$ que tienen grado $d-j$ y que no están en el ideal $< X_1^q, \ldots, X_{n-1}^q >$.
Por lo tanto,

$$\mathrm{H}_{\mathbb{A}^n}(d) = |\bigcup_{j=0}^{q-1} T_j| = \sum_{j=0}^{q-1} |T_j| = \sum_{j=0}^{q-1} |L_j| = \sum_{j=0}^{q-1} \mathrm{H}_{\mathbb{A}^{n-1}}(d-j)$$

Teorema 4.1.2 *Sea* $\mathrm{X} = \mathbb{A}^n = \{\ (1, a_1, \ldots, a_n)\ \in \mathbb{P}^n(\mathrm{k}) \mid a_i \in \mathrm{k}\ \}$ *y sea* $\mathrm{J} = \langle X_1^q, X_2^q, \ldots, X_n^q\rangle$. *Se tienen las siguientes propiedades.*

(*1*) *El* $a-$*invariante del ideal* $\mathrm{I}_{\mathbb{A}^n}$ *es* $\alpha_n = a_{\mathbb{A}^n} = n(q-1)-1$
Además, $\mathrm{H}_{\mathbb{A}^n}(\alpha_n) = q^n - 1$.

(*2*) $\mathrm{A/J}$ *tiene la siguiente resolución libre graduada*
$$0 \to \mathrm{A}(-nq)^{\binom{n}{n}} \to \ldots \to \mathrm{A}(-iq)^{\binom{n}{i}} \to \ldots \to \mathrm{A}(-q)^{\binom{n}{1}} \to \mathrm{A} \to \mathrm{A/J} \to 0$$

(*3*) *Si* d *es tal que* $1 \leq d \leq \alpha_n$, *entonces la dimensión del código* $\mathrm{RMAG}(d, n)$ *es*
$$\mathrm{H}_{\mathbb{A}^n}(d) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} \binom{n+d-iq}{d-iq}$$

Demostración.
(**1**) La prueba se hará por inducción sobre n.
El caso $n = 1$. Por la proposición 4.1.1, al considerar el anillo $\mathrm{k}[X_0, X_1]/\langle X_1^q\rangle$ se

obtiene $\mathrm{H}_{\mathbb{A}^1}(d) = \binom{d+1}{d}$ para $d < q$ y $\mathrm{H}_{\mathbb{A}^1}(q) = \binom{q+1}{q} - 1 = q$, esto último es por que los monomios de grado q que no están en $\langle X_1^q \rangle$ son todos menos X_1^q. Puesto que $\mathrm{H}_{\mathbb{A}^1}(q-2) = \binom{q-1}{q} = q-1$ y $\mathrm{H}_{\mathbb{A}^1}(q-1) = \binom{q}{q-1} = q$, se sigue que $\alpha_1 = a_{\mathbb{A}^1} = q-2$. Por lo tanto, el caso $n = 1$ es cierto.
Supongamos el resultado cierto para $n-1$, es decir, $\alpha_{n-1} = a_{\mathbb{A}^{n-1}} = (n-1)(q-1)-1$ y $\mathrm{H}_{\mathbb{A}^{n-1}}(\alpha_{n-1}) = q^{n-1} - 1$. Se tiene $\mathrm{H}_{\mathbb{A}^n}(d) = \binom{n+d}{d}$ para $d < q$, por la proposición 4.1.1, y $n(q-1)-1 = (n-1)(q-1)-1+q-1 = \alpha_{n-1}+q-1$. Sea $r > 0$.
Por lo tanto, aplicando el lema 4.1.1 y la hipótesis de inducción se obtiene

$$\mathrm{H}_{\mathbb{A}^n}(n(q-1)-1) = \mathrm{H}_{\mathbb{A}^n}(\alpha_{n-1}+q-1) = \sum_{j=0}^{q-1} \mathrm{H}_{\mathbb{A}^{n-1}}(\alpha_{n-1}+q-1-j) =$$

$$\sum_{j=0}^{q-2} \mathrm{H}_{\mathbb{A}^{n-1}}(\alpha_{n-1}+q-1-j) + \mathrm{H}_{\mathbb{A}^{n-1}}(\alpha_{n-1}) = \sum_{j=0}^{q-2} q^{n-1} + (q^{n-1}-1) = q^n - 1 \quad (4.1)$$

$$\mathrm{H}_{\mathbb{A}^n}(n(q-1)-1+r) = \mathrm{H}_{\mathbb{A}^n}(\alpha_{n-1}+q-1+r) = \sum_{j=0}^{q-1} \mathrm{H}_{\mathbb{A}^{n-1}}(\alpha_{n-1}+q-1+r-j) =$$

$$\sum_{j=0}^{q-1} \mathrm{H}_{\mathbb{A}^{n-1}}(\alpha_{n-1}+q-1+r-j) = \sum_{j=0}^{q-1} q^{n-1} = q^n \quad (4.2)$$

La afirmación se obtiene de (4.1) y (4.2).

(**2**) Como $\{X_1^q, \ldots, X_n^q\}$ es una sucesión regular, entonces el complejo de Koszul de los elementos es una resolución libre del A-módulo graduado A/J.
Se dará la forma de cada una de las funciones.
Para cada k sea C_k^n el conjunto de las $\binom{n}{k}$ combinaciones sin repetición, para cada $(i_1, \ldots, i_k) \in \mathrm{C}_k^n$ sea $e_{(i_1 \ldots i_k)}$ el básico del A-módulo $\mathrm{A}^{\binom{n}{k}}$.
La función $\Psi_k : \mathrm{A}^{\binom{n}{k}} \longrightarrow \mathrm{A}^{\binom{n}{k-1}}$ es la que está dada en los básicos por:

$$\Psi_k(e_{(i_1 \ldots i_k)}) = \sum_{r=1}^{k} (-1)^r e_{(i_1 \ldots \widehat{i_r} \ldots i_k)}$$

(**3**) Restringir la sucesión exacta del inciso (2) de esta demostración a la componente d, y usar la proposición 4.1.1.

Teorema 4.1.3 *Sea* $\mathrm{X} = \mathbb{A}^n = \{ (1, a_1, \ldots, a_n) \in \mathbb{P}^n(\mathrm{k}) \mid a_i \in \mathrm{k} \}$, *y sea* $\alpha_n = a_{\mathbb{A}^n} = n(q-1)-1$ *el a- invariante de* $\mathbb{A}^n$. *Se tienen las siguientes propiedades.*

(*1*) *Sea* $M(X_0,\ldots,X_n)=X_0^{i_0}\cdots X_n^{i_n}$ *de grado* d, *con* $0\leq d\leq \alpha_n$, *entonces*

$$\sum_{P\in\mathbb{A}^n} M(P)=0$$

(*2*) *Sea* $\mathrm{f}\in \mathrm{A}$ *tal que su reducción módulo* $\mathrm{I}_{\mathbb{A}^n}$, $\tilde{\mathrm{f}}$, *es de grado menor o igual a* α_n. *Entonces*

$$\sum_{P\in\mathbb{A}^n} \tilde{\mathrm{f}}(P)=0$$

(*3*) *Sean* ν,μ *tal que* $\nu+\mu=\alpha_n$. *Entonces*

$$\mathrm{H}_{\mathbb{A}^n}(\alpha_n+1)=\mathrm{H}_{\mathbb{A}^n}(\nu)+\mathrm{H}_{\mathbb{A}^n}(\mu)$$

(*4*) *Sean* ν,μ *tal que* $\nu+\mu=\alpha_n$. *Entonces*

$$\mathrm{RMAG}(\nu,n)^{\perp}=\mathrm{RMAG}(\mu,n)$$

(*5*) *La distancia mínima del código* $RMAG(d,n)$ *es* $\delta_d=(q-s)q^{n-r-1}$, *donde* $d=r(q-1)+s$, $0\leq s<q-1$, $0\leq r<n-1$

Demostración.

(**1**) Pongamos $P=(1,p_1,\ldots,p_n)$. Se analizan los siguientes casos.

(a) Si $i_0=d$, es decir, $M(X_0,\ldots,X_n)=X_0^d$, entonces

$$\sum_{P\in\mathbb{A}^n} X_0^d(P)=\sum_{P\in\mathbb{A}^n} 1=q^n*1=0$$

(b) Si algunos indices i_j son iguales a $q-1$ y los otros son cero. Se puede suponer que $i_1=i_2=\cdots=i_r=q-1$ e $i_0=i_{r+1}=\cdots=i_n=0$, con $r<n$ pues $d\leq n(q-1)-1$. Así, $M(X_0\cdots X_n)=X_1^{q-1}\ldots X_r^{q-1}$.

Sea $\mathrm{Y}=\{(1,p_1,\ldots,p_n)\mid p_i\in \mathrm{k},\ p_1p_2\cdots p_r\neq 0\}$, entonces $|\mathrm{Y}|=(q-1)^rq^{n-r}$. De la descomposición disjunta

$$\mathbb{A}^n=(\mathbb{A}^n\setminus \mathrm{Y})\cup \mathrm{Y}$$

Se obtiene

$$\sum_{P\in\mathbb{A}^n} M(P)=\sum_{P\in\mathbb{A}^n\setminus \mathrm{Y}} M(P)+\sum_{P\in \mathrm{Y}} M(P)=(q-1)^rq^{n-r}*1=0$$

(c) Si para algún j se tiene $1\leq i_j<q-1$. Podemos suponer que es i_1, es decir, $1\leq i_1<q-1$. De la descomposición disjunta

$$\mathbb{A}^n=\{(1,0,p_2,p_3,\ldots,p_n)\mid p_i\in \mathrm{K}\}\cup\bigcup_{i=0}^{q-2}\{(1,\gamma^i,p_2,p_3,\ldots,p_n)\mid p_i\in \mathrm{K}\}$$

donde $\mathrm{K}^*=\langle\gamma\rangle$. Se obtiene

$$\sum_{P\in\mathbb{A}^n} M(P)=\sum p_2^{i_2}\cdots p_n^{i_n}+\gamma^{i_1}\sum p_2^{i_2}\cdots p_n^{i_n}+\gamma^{2i_1}\sum p_2^{i_2}\cdots p_n^{i_n}+\ldots+$$

$$\gamma^{(q-2)i_1}\sum p_2^{i_2}\cdots p_n^{i_n} = (1+\gamma^{i_1}+\gamma^{2i_1}+\ldots\gamma^{(q-2)i_1})\sum p_2^{i_2}\cdots p_n^{i_n} = 0$$

Esto último debido a que γ^{i_1} satisface la ecuación $1+z+z^2+\ldots z^{q-2} = \frac{z^{q-1}-1}{z-1}$.

(**2**) Al homogenizar el polinomio con respecto a X_0, el resultado se sigue del inciso (1) de esta demostración.

(**3**) De la proposición 4.1.1, se sigue que $\mathrm{H}_{\mathbb{A}^n}(d) = \dim_{\mathrm{k}}(\mathrm{k}[X_0,\ldots,X_n]/\langle X_1^q,\ldots,X_n^q\rangle)_d$. Considerar los conjuntos $\mathrm{C}_d = \{X_0^k X_1^{i_1}\cdots X_n^{i_n} \mid 0\leq i_j\leq q-1,\ k+i_1+\ldots+i_n = d\}$, $\mathrm{C}^1 = \{X_0^k X_1^{i_1}\cdots X_n^{i_n}\in \mathrm{C}_{n(q-1)} \mid k\geq \mu+1\}$ y $\mathrm{C}^2 = \mathrm{C}_{n(q-1)}\setminus \mathrm{C}^1$. Es fácil verificar las siguientes propiedades.

(a) $\dim_{\mathrm{k}}(\mathrm{k}[X_0,\ldots,X_n]/\langle X_1^q,\ldots,X_n^q\rangle)_d$ es igual al número monomios de C_d.

(b) $\mathrm{C}^1 = \{X_0^{\mu+1}X_0^r X_1^{i_1}\cdots X_n^{i_n} \mid \mu+1+r+i_1+\cdots+i_n = n(q-1),\ 0\leq i_j\leq q-1\} =$
$\{X_0^{\mu+1}X_0^r X_1^{i_1}\cdots X_n^{i_n} \mid r+i_1+\cdots+i_n = \nu,\ 0\leq i_j\leq q-1\}$

(c) La función

$$\begin{array}{ccccc} T_\nu & : & \mathrm{C}^1 & \longrightarrow & \mathrm{C}_\nu \\ & & X_0^{\mu+1}X_0^r X_1^{i_1}\cdots X_n^{i_n} & \mapsto & X_0^r X_1^{i_1}\cdots X_n^{i_n} \end{array} \quad \text{es biyectiva.}$$

(d) $\mathrm{C}^2 = \{X_0^k X_1^{i_1}\cdots X_n^{i_n} \mid k\leq \mu,\ k+i_1+\ldots+i_n = n(q-1)\}$

(e) La función

$$\begin{array}{ccccc} T & : & \mathrm{C}^2 & \longrightarrow & \mathrm{C}_\mu \\ & & X_0^k X_1^{i_1}\cdots X_n^{i_n} & \mapsto & X_0^{\mu-k}X_1^{q-1-i_1}\cdots X_n^{q-1-i_n} \end{array}.$$

es biyectiva, y su inversa está dada por

$$\begin{array}{ccccc} T^{-1} & : & \mathrm{C}_\mu & \longrightarrow & \mathrm{C}^2 \\ & & X_0^{i_0}X_1^{i_1}\cdots X_n^{i_n} & \mapsto & X_0^{\mu-i_0}X_1^{q-1-i_1}\cdots X_n^{q-1-i_n} \end{array}$$

Por lo tanto

$$\mathrm{H}_{\mathbb{A}^n}(\alpha_n+1) = \dim(\mathrm{k}[X_0,\ldots,X_n]/\langle X_1^q,\ldots,X_n^q\rangle)_{n(q-1)} = |\mathrm{C}_{n(q-1)}| = |\mathrm{C}^1|+|\mathrm{C}^2| =$$
$$|\mathrm{C}_\nu|+|\mathrm{C}_\mu| = \dim_{\mathrm{k}}(\mathrm{k}[X_0,\ldots,X_n]/\langle X_1^q,\ldots,X_n^q\rangle)_\nu + \dim_{\mathrm{k}}(\mathrm{k}[X_0,\ldots,X_n]/\langle X_1^q,\ldots,X_n^q\rangle)_\mu =$$
$$\mathrm{H}_{\mathbb{A}^n}(\nu)+\mathrm{H}_{\mathbb{A}^n}(\mu)$$

(**4**) El resultado se sigue de los incisos (2) y (3) de esta demostración.

(**5**) Ver [3].

4.2. El Código Reed-Muller proyectivo generalizado

Sea $\mathrm{X} = \mathbb{P}^n(\mathrm{k})$, entonces X tiene $\frac{q^{n+1}-1}{q-1}$ puntos y el código $C_{\mathrm{X}}(d)$ es llamado código Reed-Muller proyectivo generalizado (RMPG(d,n)).

TEOREMA 4.2.1 *Sea* $\mathrm{X} = \mathbb{P}^n(\mathrm{k})$, *entonces*

$$\mathrm{I}_{\mathbb{P}^n} = \langle X_i^q X_j - X_i X_j^q \mid 0 \leq j < i \leq n \rangle$$

Demostración.
Es claro que $\langle X_i^q X_j - X_i X_j^q \mid 0 \leq j < i \leq n \rangle \subseteq \mathrm{I}_{\mathbb{P}^n}$
Resta probar que $\mathrm{I}_{\mathbb{P}^n} \subseteq \langle X_i^q X_j - X_i X_j^q \mid 0 \leq j < i \leq n \rangle$, y esto será por inducción sobre n.
Para $n = 1$. Sea $\mathrm{f}(X_0, X_1) \in \mathrm{I}_{\mathbb{P}^1}$ (homogéneo de grado d), entonces $\mathrm{f}(X_0, X_1) = X_0\mathrm{f}_1(X_0, X_1) + \mathrm{f}_2(X_1)$, donde $\mathrm{f}_2(X_1) = aX_1^d$. Puesto que $\mathrm{f}(0,1) = 0 = \mathrm{f}_2(1) = a$, se sigue que $\mathrm{f}(X_0, X_1) = X_0\mathrm{f}_1(X_0, X_1)$. Para cualquier $\alpha \in \mathrm{k}$ se tiene $\mathrm{f}(1, \alpha) = \mathrm{f}_2(1, \alpha) = 0$. Por tanto, $\mathrm{f}_2(X_0, X_1) \in \mathrm{I}_{\mathbb{A}^1} =< X_1^q - X_0^{q-1}X_1 >$, por el teorema 4.1.1. Por lo tanto

$$\mathrm{f}(X_0, X_1) = X_0\mathrm{f}_2(X_0, X_1) = (X_1^q X_0 - X_0^q X_1)\mathrm{h}(X_0, X_1) \in \langle X_0^q X_1 - X_0 X_1^q \rangle$$

Supongamos que existe un n para el cual $\mathrm{I}_{\mathbb{P}^n} = \langle X_i^q X_j - X_i X_j^q \mid 0 \leq j < i \leq n \rangle$, y sea $\mathrm{f} \in \mathrm{I}_{\mathbb{P}^{n+1}}$ (homogéneo). Pongamos $\mathrm{f} = \mathrm{f}_1 + X_0\mathrm{g}$, donde $\mathrm{f}_1 \in \mathrm{K}[X_1, \ldots, X_{n+1}]$ y $\mathrm{g} \in \mathrm{K}[X_0, \ldots, X_{n+1}]$ (homogéneos). Se verificará que tanto f_1 como $X_0\mathrm{g}$ pertencen al ideal $\langle X_i^q X_j - X_i X_j^q \mid 0 \leq j < i \leq n+1 \rangle$, de donde se obtendrá que $\mathrm{f} \in \langle X_i^q X_j - X_i X_j^q \mid 0 \leq j < i \leq n+1 \rangle$.
Para cualquier $\alpha \in \mathbb{P}^n$ sea $(0, \alpha) \in \mathbb{P}^{n+1}$. Puesto que $\mathrm{f}(0, \alpha) = 0 = \mathrm{f}_1(\alpha)$, se sigue que $\mathrm{f}_1 \in \mathrm{I}_{\mathbb{P}^n}$. Por tanto

$$\mathrm{f}_1 \in \langle X_i^q X_j - X_i X_j^q \mid 1 \leq j < i \leq n+1 \rangle_{\mathrm{K}[X_1,\ldots,X_{n+1}]} \subseteq \langle X_i^q X_j - X_i X_j^q \mid 0 \leq j < i \leq n+1 \rangle$$

Sea $u \in \mathbb{P}^n$, puesto que $\mathrm{f}(1, u) = \mathrm{f}_1(1, u) + (1)\mathrm{g}(1, u) = \mathrm{g}(1, u) = 0$, se sigue que $\mathrm{g} \in \mathrm{I}_{\mathbb{A}^{n+1}} =< X_0^{q-1}X_1 - X_1^q, \ldots, X_0^{q-1}X_{n+1} - X_{n+1}^q >$. Por lo tanto

$$X_0\mathrm{g} \in < X_0^q X_1 - X_0 X_1^q, \ldots, X_0^q X_{n+1} - X_0 X_{n+1}^q > \subseteq \langle X_i^q X_j - X_i X_j^q \mid 0 \leq j < i \leq n+1 \rangle$$

PROPOSICIÓN 4.2.1 *Sea* $\mathrm{X} = \mathbb{P}^n(\mathrm{k})$, *sea* $\mathrm{I}_{\mathbb{P}^n} = \langle X_i^q X_j - X_i X_j^q \mid 0 \leq j < i \leq n \rangle$, *y sea* $\mathrm{J} = \langle X_i^q X_j \mid 0 \leq i < j \leq n \rangle$. *Entonces* $\mathrm{A/J}$ *y* $\mathrm{A/I}_{\mathbb{P}^n}$ *tienen la misma función de Hilbert.*
Además, una base sobre k *de* $(\mathrm{A/J})_d$ *se obtiene de los monomios de grado* d *que no pertenecen a* J

Demostración.
Con el orden graduado lexicográfico tal que $X_n > \ldots > X_0$, los generadores del ideal $\langle X_i^q X_j - X_i X_j^q \mid 0 \leq j < i \leq n \rangle$ son una base de Groebner, por el ejemplo 2.4.2. Así, $\langle \mathrm{LT}(X_i^q X_j - X_i X_j^q \mid 0 \leq j < i \leq n) \rangle = \langle X_i^q X_j \mid 0 \leq i < j \leq n \rangle$. Entonces la afirmación se sigue del teorema 2.3.1.

LEMA 4.2.1 *Sea* $\mathrm{X} = \mathbb{P}^n(\mathrm{k})$ *y sea* $d \geq 1$, *entonces*

$$\mathrm{H}_{\mathbb{P}^n}(d) = \mathrm{H}_{\mathbb{P}^{n-1}}(d) + \mathrm{H}_{\mathbb{A}^n}(d-1)$$

Demostración.
Puesto que $\mathrm{A}_d = X_0 \mathrm{A}_{d-1} \oplus \mathrm{B}_d$ y $(\mathrm{I}_{\mathbb{P}^n})_d = X_0 (\mathrm{I}_{\mathbb{A}^n})_{d-1} \oplus (\mathrm{I}_{\mathbb{P}^{n-1}})_d$, donde $\mathrm{B} = \mathrm{k}[X_1, \ldots, X_n]$ e $\mathrm{I}_{\mathbb{P}^{n-1}}(d)$ es identificado en las variables $X_1, \ldots, X_n$, se sigue que

$$(\mathrm{A/I}_{\mathbb{P}^n})_d \cong X_0 \mathrm{A}_{d-1} / X_0 (\mathrm{I}_{\mathbb{A}^n})_{d-1} \oplus \mathrm{B}_d / \mathrm{I}_{\mathbb{P}^{n-1}}(d) \cong \mathrm{A}_{d-1} / (\mathrm{I}_{\mathbb{A}^n})_{d-1} \oplus \mathrm{B}_d / \mathrm{I}_{\mathbb{P}^{n-1}}(d)$$

Al obtener dimensiones se obtiene la relación buscada.

LEMA 4.2.2 *Sea* $n \geq 1$, *sea* $\mathrm{X} = \mathbb{P}^n(\mathrm{k})$, *y sea* $d \geq 1$. *Entonces*

$$\mathrm{H}_{\mathbb{P}^n}(d) = \mathrm{H}_{\mathbb{P}^1}(d) + \textstyle\sum_{j=2}^{n} \mathrm{H}_{\mathbb{A}^j}(d-1)$$

Demostración.
Puesto que $\mathrm{H}_{\mathbb{P}^n}(d) = \mathrm{H}_{\mathbb{P}^{n-1}}(d) + \mathrm{H}_{\mathbb{A}^n}(d-1)$, por el lema 4.2.1, se sigue que
$\mathrm{H}_{\mathbb{P}^n}(d) = \mathrm{H}_{\mathbb{P}^{n-1}}(d) + \mathrm{H}_{\mathbb{A}^n}(d-1) = \mathrm{H}_{\mathbb{P}^{n-2}}(d) + \mathrm{H}_{\mathbb{A}^{n-1}}(d-1) + \mathrm{H}_{\mathbb{A}^n}(d-1) =$
$\mathrm{H}_{\mathbb{P}^{n-3}}(d) + \mathrm{H}_{\mathbb{A}^{n-2}}(d-1) + \mathrm{H}_{\mathbb{A}^{n-1}}(d-1) + \mathrm{H}_{\mathbb{A}^n}(d-1) = \ldots =$
$\mathrm{H}_{\mathbb{P}^1}(d) + \mathrm{H}_{\mathbb{A}^2}(d-1) + \mathrm{H}_{\mathbb{A}^3}(d-1) + \ldots + \mathrm{H}_{\mathbb{A}^n}(d-1) = \mathrm{H}_{\mathbb{P}^1}(d) + \sum_{j=2}^{n} \mathrm{H}_{\mathbb{A}^j}(d-1)$

TEOREMA 4.2.2 *Sea* $\mathrm{X} = \mathbb{P}^n(\mathrm{k})$ *y sea* $\mathrm{J} = \langle X_i^q X_j \mid 0 \leq i < j \leq n \rangle$. *Se tienen las siguientes propiedades.*

(*1*) *El* $a-$ *invariante del ideal* $\mathrm{I}_{\mathbb{P}^n}$ *es* $\beta_n = a_{\mathbb{P}^n} = n(q-1)$

(*2*) *Si* $d \geq q$, *entonces*

$$\mathrm{H}_{\mathbb{P}^n}(d) = \mathrm{H}_{\mathbb{P}^{n-1}}(d - (q-1)) + \mathrm{H}_{\mathbb{A}^n}(d)$$

(*3*) *Si d es tal que $q \leq d \leq \beta_n - 1$, entonces la dimensión del código RMPG(d,n) es*
$$\mathrm{H}_{\mathbb{P}^n}(d) = \sum_{j=0}^{n} \sum_{i=0}^{j} (-1)^i \binom{j}{i} \binom{j+d-1-iq}{d-1-iq}$$

(*4*) *La distancia mínima del código es $\delta_d = (q-s)q^{n-r-1}$, donde $d-1 = r(q-1)+s$, $0 \leq s < q-1$.*

Demostración.
(**1**) La prueba será por inducción sobre n.
Si $n = 1$, entonces $\mathrm{H}_{\mathbb{P}^1}(d) = \mathrm{H}_{\mathbb{A}^1}(d-1)$, por el lema 4.2.1. Por lo tanto, el caso $n = 1$ es cierto.
Supongamos que el $a-$ invariante de $\mathrm{I}_{\mathbb{P}^n}$ es $\beta_n = \mathrm{a}_{\mathbb{P}^n} = n(q-1) = \mathrm{a}_{\mathbb{A}^n} + 1 = \alpha_n + 1$.
Sea $r > 0$. Por lo tanto, al aplicar el lema 4.2.1 y la hipótesis de inducción se obtiene
$$\mathrm{H}_{\mathbb{P}^{n+1}}(\beta_{n+1}) = \mathrm{H}_{\mathbb{P}^{n+1}}(\alpha_{n+1}+1) = \mathrm{H}_{\mathbb{P}^n}(\alpha_{n+1}+1) + \mathrm{H}_{\mathbb{A}^{n+1}}(\alpha_{n+1}) =$$

$$\frac{q^{n+1}-1}{q-1} + q^n - 1 = \frac{q^{n+2}-1}{q-1} - 1 = |\mathbb{P}^{n+1}| - 1 \tag{4.3}$$

$$\mathrm{H}_{\mathbb{P}^{n+1}}(\beta_{n+1}+r) = \mathrm{H}_{\mathbb{P}^n}(\beta_{n+1}+r) + \mathrm{H}_{\mathbb{A}^{n+1}}(\alpha_{n+1}+r) = |\mathbb{P}^n| + |\mathbb{A}^{n+1}| = |\mathbb{P}^{n+1}| \tag{4.4}$$

La afirmación se obtiene de 4.3 y 4.4

(**2**) Se trabaja con $(\mathrm{k}[X_0,\ldots,X_n]/\langle X_i^q X_j \mid 0 \leq i < j \leq n\rangle)_d$, por la proposición 4.2.1. Notemos que $\dim_{\mathrm{k}}(\mathrm{k}[X_0,\ldots,X_n]/\langle X_i^q X_j \mid 0 \leq i < j \leq n\rangle)_d$ es igual al número de monomios de grado d que no estan en $\mathrm{J} = \langle X_i^q X_j \mid 0 \leq i < j \leq n\rangle$
Sea $\mathrm{C} = \{X_0^{i_0} X_1^{i_1} \cdots X_n^{i_n} \in \mathrm{A}_d \mid \text{si } i_j \geq q, \text{ entonces } i_{j+r} = 0 \text{ para } r \in \{1,\ldots,n-j\}\}$, sea $t \in \{0,\ldots,q-1\}$, sea $\mathrm{C}_t = \{X_0^t X_1^{i_1} \cdots X_n^{i_n} \mid i_1 + \ldots + i_n = d-t\} \cap \mathrm{C}$ y sea $\mathrm{C}_{-1} = \{X_0^d\}$. Es fácil verificar que

(a) C consta de todos los monomios de grado d que no están en J;

(b) $\mathrm{C}_t \cap \mathrm{C}_{t_1} = \emptyset$ si $t \neq t_1$;

(c) $\mathrm{C} = \bigcup_{j=-1}^{q-1} \mathrm{C}_j$;

(d) $|\mathrm{C}_t| = \mathrm{H}_{\mathbb{P}^{n-1}}(d-t)$, para esta igualdad se identifica a $\mathbb{P}^{n-1}$ en las variables $X_1,\ldots,X_n$ y se considera a $\mathrm{J} = \langle X_i^q X_j \mid 1 \leq i < j \leq n\rangle$.

Por tanto

$$\mathrm{H}_{\mathbb{P}^n}(d) = |\mathrm{C}| = \sum_{j=-1}^{q-1} |\mathrm{C}_j| = 1 + \sum_{j=0}^{q-1} H_{\mathbb{P}^{n-1}}(d-j)$$

Por otra parte, puesto que $\mathrm{H}_{\mathbb{A}^n}(d-1) = H_{\mathbb{P}^n}(d) - \mathrm{H}_{\mathbb{P}^{n-1}}(d)$, por el lema 4.2.1, se sigue que $\mathrm{H}_{\mathbb{A}^n}(d-1) = 1 + \sum_{j=1}^{q-1} \mathrm{H}_{\mathbb{P}^{n-1}}(d-t)$. Por tanto

$$\mathrm{H}_{\mathbb{A}^n}(d-1) - \mathrm{H}_{\mathbb{A}^n}(d) = 1 + \sum_{j=1}^{q-1} \mathrm{H}_{\mathbb{P}^{n-1}}(d-t) - 1 - \sum_{j=1}^{q-1} \mathrm{H}_{\mathbb{P}^{n-1}}((d+1)-t) =$$
$$= \mathrm{H}_{\mathbb{P}^{n-1}}(d-(q-1)) - \mathrm{H}_{\mathbb{P}^{n-1}}(d)$$

Por lo tanto

$$\mathrm{H}_{\mathbb{P}^n}(d) = \mathrm{H}_{\mathbb{A}^n}(d-1) + \mathrm{H}_{\mathbb{P}^{n-1}}(d) = \mathrm{H}_{\mathbb{P}^{n-1}}(d-(q-1)) + \mathrm{H}_{\mathbb{A}^n}(d)$$

(**3**) De la proposición 4.2.1 y de la sucesión exacta de $\mathrm{k}[X_0, X_1]$-módulos graduados $0 \to \mathrm{k}[X_0, X_1](-q-1) \xrightarrow{X_0^q X_1} \mathrm{k}[X_0, X_1] \to \mathrm{k}[X_0, X_1]/\langle X_0^q X_1 \rangle \to 0$, se sigue que $\mathrm{H}_{\mathbb{P}^1}(d) = \mathrm{H}_{\mathrm{k}[X_0,X_1]/\langle X_0^q X_1\rangle}(d) = \binom{d+1}{d} - \binom{d+1-(q+1)}{d-(q+1)}$. Puesto que $\mathrm{H}_{\mathbb{A}^1}(d) = \binom{d+1}{d} - \binom{d+1-q}{d-q}$, por el inciso (3) del teorema 4.1.2, y puesto que $\binom{n+1}{n} - \binom{n}{n-1} = 1$ para toda n, se sigue que

$$\mathrm{H}_{\mathbb{P}^1}(d) = \binom{d+1}{d} - \binom{d+1-q}{d-q} + \binom{d+1-q}{d-q} - \binom{d-q}{d-q-1} = \mathrm{H}_{\mathbb{A}^1}(d) + 1 \quad (4.5)$$

Finalmente, al combinar el inciso (3) del teorema 4.1.2, el lema 4.2.2 y la ecuación (4.5), se obtiene lo esperado.

(**4**) Ver [3].

4.3. El Código Asociado al Módulo Canónico

El procedimiento general para la construcción del código usando el módulo canónico es el siguiente: si V es un espacio vectorial de dimensión s, $\{\alpha_1, \ldots, \alpha_s\}$ es una base de V y τ es un subespacio de funcionales lineales sobre V, se define el código $\mathrm{C}(\tau)$ que es la imagen de la transformación lineal

$$\begin{array}{rccc} \delta & : & \tau & \longrightarrow & \mathrm{k}^s \\ & & \varphi & \longmapsto & (\varphi(\alpha_1), \ldots, \varphi(\alpha_s)) \end{array}$$

es claro que δ es inyectiva. Por tanto, la dimensión del código es la dimensión de τ
En nuestro caso se hace la siguiente elección $\mathrm{V} = \mathrm{R}_{a_\mathrm{X}+1}$, $\{\mathrm{f}_1, \ldots, \mathrm{f}_s\}$ es la base de truncadores y el subespacio de funcionales τ es el que le corresponde a la componente homogénea $(\omega_\mathrm{R})_{-a_\mathrm{X}}$ del módulo canónico (proposición 3.3.4).
Dicha correspondencia se obtiene observando que los elementos de $(\omega_\mathrm{R})_{-a_\mathrm{X}}$ son $\mathrm{k}[x_0]$ homomorfismos graduados de R en $\mathrm{k}[x_0](-a_\mathrm{X})$ que al ser restringidos a $\mathrm{R}_{a_\mathrm{X}+1}$ da como resultado funcionales que se anulan en $x_0\mathrm{R}_{a_\mathrm{X}}$.
Ahora, se define un código usando el módulo canónico (ω_R) del anillo de coordenadas R de un subesquema de dimensión cero y grado s.

Definición 4.3.1 *Sea* $\mathrm{X} = \{\mathrm{P}_1, \ldots, \mathrm{P}_s\}$ *un conjunto de* s *puntos, sea* R *el anillo de coordenadas de* X*, sea* ω_R *el módulo canónico de* R*, sean* $\mathrm{f}_1, \ldots, \mathrm{f}_s$ *una base de* $\mathrm{R}_{a_\mathrm{X}+1}$ *consistente de separadores y sea* $\mathrm{C}_{a_\mathrm{X}}(\omega_\mathrm{R})$ *la imagen de la siguiente trasformación lineal*

$$\begin{array}{ccccc} \delta & : & (\omega_\mathrm{R})_{-a_\mathrm{X}} & \longrightarrow & \mathrm{k}^s \\ & & \varphi & \longmapsto & (\varphi(\mathrm{f}_1), \ldots, \varphi(\mathrm{f}_s)) \end{array}$$

Proposición 4.3.1 *Bajo las condiciones de la definición anterior. Se tiene que* $\mathrm{C}_{a_\mathrm{X}}(\omega_\mathrm{R})$ *es un código lineal de dimensión*

$$\dim_\mathrm{k} \mathrm{C}_{a_\mathrm{X}}(\omega_\mathrm{R}) = s - \dim_\mathrm{k} \mathrm{C}_{a_\mathrm{X}}(\mathrm{R})$$

Demostración.
Es claro que la función δ es k-lineal.
δ es inyectiva, pues si $\delta(\varphi) = (\varphi(\mathrm{f}_1), \ldots, \varphi(\mathrm{f}_s)) = (0, \ldots, 0)$, entonces φ se anula en todos los $\mathrm{f}_1, \ldots, \mathrm{f}_s$, los cuales forman la base de $\mathrm{R}_{a_\mathrm{X}+1}$. Así, $\varphi\big|_{\mathrm{R}_{a_\mathrm{X}+1}} = 0$. Por tanto, $\varphi = 0$, por la proposición 3.3.5. Por lo tanto, $\dim_\mathrm{k} \mathrm{C}_{a_\mathrm{X}}(\omega_\mathrm{R}) = \dim_\mathrm{k}(\omega_\mathrm{R})_{-a_\mathrm{X}} = \mathrm{H}_{\omega_\mathrm{R}}(-a_\mathrm{X}) = s - \mathrm{H}_\mathrm{X}(a_\mathrm{X})$, por la proposición 3.3.3.

Proposición 4.3.2 *Bajo condiciones de la definición 4.3.1. Los códigos* $\mathrm{C}_{a_\mathrm{X}}(\omega_\mathrm{R})$ *y* $\mathrm{C}_{a_\mathrm{X}}(\mathrm{R})$ *son duales uno del otro.*

Demostración.
Notemos que si $\mathrm{f} \in \mathrm{R}_{a_\mathrm{X}}$, entonces $\overline{X}_0\mathrm{f} = \sum_{i=1}^{s} \overline{X}_0(\mathrm{P}_i)\mathrm{f}(\mathrm{P}_i)\mathrm{f}_i$, por la proposición 3.1.4, y también $X_0(\mathrm{P}_i) = 1$

Sean $\delta(\varphi) = (\varphi(\mathrm{f}_1), \ldots, \varphi(\mathrm{f}_s)) \in \mathrm{C}_{a_\mathrm{X}}(\omega_\mathrm{R})$ y $e(\mathrm{f}) = (\mathrm{f}(\mathrm{P}_1), \ldots, \mathrm{f}(\mathrm{P}_s) \in \mathrm{C}_{a_\mathrm{X}}(\mathrm{R})$, entonces:

$$e(\mathrm{f})\bullet\delta(\varphi) = \sum_{i=1}^{s} \mathrm{f}(\mathrm{P}_i)\varphi(\mathrm{f}_i) = \sum_{i=1}^{s} \overline{X}_0(\mathrm{P}_i)\mathrm{f}(\mathrm{P}_i)\varphi(\mathrm{f}_i) = \varphi\big(\sum_{i=1}^{s} \overline{X}_0(\mathrm{P}_i)\mathrm{f}(\mathrm{P}_i)\mathrm{f}_i\big) = \varphi(X_0\mathrm{f}) = 0$$

Pues φ es $\mathrm{k}[\overline{X}_0]$- lineal y se anula en $\overline{X}_0\mathrm{R}_{a_\mathrm{X}}$

4.4. Ejemplo

Sean $\mathrm{k} = \mathbb{F}_q$ el campo finito con q elementos y $\alpha \in \mathrm{k}^*$ el elemento primitivo.
Para $n < q+1$, el mapeo de Veronese de $\mathbb{P}^1$ en $\mathbb{P}^n$ es:

$$\begin{array}{rccc} \psi: & \mathbb{P}^1(\mathrm{k}) & \longrightarrow & \mathbb{P}^n(\mathrm{k}) \\ & (x,y) & \longmapsto & (x^n y^0, \ldots, x^i y^{n-i}, \ldots, x^0 y^n) \end{array}$$

Sea $\mathrm{X} = \{(x^n y^0, \ldots, x^i y^{n-i}, \ldots, x^0 y^n) \mid (x,y) \in \mathbb{P}^1(\mathrm{k})\} = \{\mathrm{P}_1, \ldots, \mathrm{P}_q, \mathrm{P}_{q+1}\}$, entonces $\mathrm{X} = \{(1, y, y^2, \ldots, y^n) \ : \ y \in \mathrm{k}\} \cup \{\mathrm{P}_{q+1}\}$ con $\mathrm{P}_{q+1} = (0,0,\ldots,0,l)$.
Los $q+1$ puntos de X no están contenidos en ningún hiperplano de $\mathbb{P}^n(\mathrm{k})$ pues $\psi\big(\mathbb{P}^1(\mathrm{k})\big)$ es de grado $n < q+1$. Así, $\mathrm{H}_\mathrm{X}(1) = n+1$, $a_\mathrm{X} = 1$ y $\mathrm{C}_\mathrm{X}(1)$ es un $[q+1, n+1]$ código lineal.

Construyamos ahora el dual de este código usando el método anterior.

Notemos que $a_\mathrm{X} = 1$, $\mathrm{H}_\mathrm{X}(1) = n+1$ y $\mathrm{H}_\mathrm{X}(j) = q+1$ para $2 \leq j$.
Sea $\{x_0, \ldots, x_n\}$ la base natural de R_1 y $\{\mathrm{f}_1, \ldots, \mathrm{f}_{q+1}\}$ una base para R_2, denotamos los correspondientes elementos del espacio dual $\tilde{\mathrm{R}}_2$ por $\tilde{\mathrm{f}}_i$.
Sea $\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{q-n}$ una base del espacio $(\omega_\mathrm{R})_{-1}$ (proposición 3.3.3), denotamos también los elementos correspondientes del espacio dual de R_2 que se anulan en $x_0\mathrm{R}_1$ por $\tilde{\varphi}_1, \ldots, \tilde{\varphi}_{q-n}$ (correspondencia de la proposición 3.3.4).
En términos de la base dual de $\tilde{\mathrm{R}}_2$ $\{\tilde{\mathrm{f}}_1, \ldots, \tilde{\mathrm{f}}_{q+1}\}$, $\tilde{\varphi}_j$ se escribe como

$$\tilde{\varphi}_j = \sum_{i=1}^{q+1} \tilde{\varphi}_j(\tilde{\mathrm{f}}_i)\mathrm{f}_i \quad \textit{para} \quad j = 1, 2, \ldots, q-n$$

Valuando en $x_0 x_t$

$$\tilde{\varphi}_j(x_0 x_t) = \sum_{i=1}^{q+1} \tilde{\varphi}_j(\mathrm{f}_i)\tilde{\mathrm{f}}_i(x_0 x_t) = \sum_{i=1}^{q+1} \tilde{\varphi}_j(\mathrm{f}_i)(x_t)(\mathrm{P}_i) = 0$$

Esta igualdad es pues cada $\tilde{\varphi}_j$ se anula en $x_0\mathrm{R}_1$ ($\tilde{\varphi}_j(x_0x_t) = 0$), $x_0(\mathrm{P}_{q+1}) = 0$, $x_0(\mathrm{P}) = 1$ para cualquier otro punto de X y $\tilde{\mathrm{f}}_i(x_0x_t) = (x_0x_t)(\mathrm{P}_i)$.
Así, $(\tilde{\varphi}_j(\mathrm{f}_1), \ldots, \tilde{\varphi}_j(\mathrm{f}_{q+1}))$ es ortogonal a $(x_t(\mathrm{P}_1), \ldots, x_t(\mathrm{P}_{q+1})) = (0, 1, \alpha^t, \ldots, \alpha^{t(q-2)}, 0)$ para $t = 1, \ldots, d$ de la matriz generadora del código generalizado de Reed-Salomon, es decir, $(\tilde{\varphi}_j(\mathrm{f}_1), \ldots, \tilde{\varphi}_j(\mathrm{f}_{q+1}))$ $j = 1, \ldots, q-d$ es un elemento del dual de este código. Esto es, el código $\mathrm{C}_{a_\mathrm{X}}(\omega_\mathrm{R})$ es el dual del código generalizado de Reed-Salomon.

Conclusiones

La teoría de códigos se dividide en dos ramas, la primera consiste en la obtención de nuevos códigos a partir de diversos conceptos matemáticos; la segunda opción está más ligada al avance computacional de los últimos años, el cual hace posible cálculos complejos que ayudan a conocer propiedades de los códigos ya conocidos.

Bibliografía

[1] Anthony V. Geramita, Martin Kreuzer and Lorenzo Robbiano, *Cayley-Bacharach schemes and their Canonical modules*, Transaction of the American Mathematical Society 339(1), (1993), 163 – 189.

[2] Carlos Renteria, H. Tapia-Recillas, *Linear Codes asociated to the ideal of points in* $\mathbb{P}^n$ *and its canonical module*, Comunications in Algebra, 24(3), (1996), 1083 – 1090.

[3] Carlos Renteria, H. Tapia-Recillas, *Reed-Muller Codes: An Ideal Theory Approach*, Comunications in Algebra 25(2), (1997), 401 – 413.

[4] David Cox, John Little, Donal O'Shea, *Ideals, varieties, and algorithms.* Springer-Verlag.

[5] Hideyuki Matsumura, *Commutative Algebra*, Benjamin, New York, 1970.

[6] Joseph J. Rotman, *An Introduction to Homological Algebra*, Academic Press. Inc, 1979.

[7] Rafael H. Villarreal, *Monomial Algebras*, Benjamin, New York, 1970.

[8] Stichtenoth, H, *Algebraic Function Fields and Codes*, Universitext, Springer-Verlag, (1993).

[9] Winfrid Bruns, Jurgen Herzog, *Cohen-Macaulay Rings*, Cambridge, 1993.

[10] William Fulton, *Algebraic curves: An introduction to algebraic geometry.* W.A. Benjamin, Inc. New York, Amsterdam, (1969).