PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

Intersección de variedades en el espacio proyectivo

TRABAJO DE INVESTIGACIÓN PARA LA OBTENCIÓN DEL GRADO DE BACHILLER EN CIENCIAS CON MENCIÓN EN MATEMÁTICAS

AUTOR

Eduardo José León Chávarri

ASESOR

Percy Braulio Fernández Sánchez

Lima, Noviembre, 2019

Resumen

El teorema de Bézout afirma que dos curvas polinomiales “suficientemente genéricas” $f(x, y) = 0$ y $g(x, y) = 0$ se intersecan en $\deg f \cdot \deg g$ puntos, contados con multiplicidad y considerando los puntos de intersección “en el infinito”, si los hubiera. Este trabajo tiene por objetivo demostrar una generalización del teorema de Bézout aplicable a la intersección de variedades en el espacio proyectivo de dimensión arbitraria.

Como punto de partida, asumimos que el lector está familiarizado con las estructuras básicas del álgebra conmutativa (anillos, ideales, módulos) y un mínimo de topología general. El álgebra conmutativa tiene un rol fundamental en la geometría algebraica, ya que es el lenguaje formal en que las ideas geométricas intuitivas se traducen en argumentos matemáticos rigurosos y de gran generalidad. Comparativamente, la topología juega un rol secundario, consolidando definiciones y proposiciones que no dependen demasiado de los detalles algebraicos.

Nuestra estrategia para estudiar las intersecciones de variedades proyectivas es asignar a cada variedad proyectiva $Y \subset \mathbb{P}^n$ un polinomio $P_Y \in \mathbb{Q}[n]$, llamado el *polinomio de Hilbert* de Y, que encapsula la información aditiva de Y en un objeto fácil de manipular. La intersección de Y con una hipersuperficie transversal en $\mathbb{P}^n$ da lugar a una sucesión exacta que involucra a P_Y, a partir de la cual, por un argumento más tedioso que difícil, se desprende la generalización buscada del teorema de Bézout.

Índice general

Índice de figuras

Introducción

La geometría algebraica clásica estudia los espacios de soluciones de ecuaciones polinomiales. En general, no es posible calcular explícitamente dichas soluciones. Esto nos obliga a buscar maneras indirectas de obtener información acerca de los espacios de soluciones.

Un resultado importante en la geometría algebraica clásica es el siguiente teorema atribuido al matemático francés Étienne Bézout[1], que relaciona los grados de dos curvas con el número de puntos en que éstas se intersecan.

Teorema 6.2. *(Bézout) Sean $F, G \subset \mathbb{P}^2$ dos curvas proyectivas planas que no tienen componentes irreducibles en común. Sean $p_1 \dots p_s \in \mathbb{P}^2$ los puntos de $F \cap G$. Entonces,*

$$\mu_1 + \cdots + \mu_s = \deg F \cdot \deg G$$

donde μ_j es la multiplicidad de $F \cap G$ sobre p_j.

Prueba. Ver [Ful89, pp. 112-115] o [Kir92, pp. 62-63]. □

El objetivo de este trabajo es demostrar una generalización del teorema de Bézout aplicable a la intersección de variedades en el espacio proyectivo de dimensión arbitraria. Para ello, tenemos que encontrar respuestas satisfactorias a las siguientes preguntas:

1. ¿Qué es el grado de una variedad proyectiva arbitraria $Y \subset \mathbb{P}^n$?
2. ¿Cuál es la multiplicidad de $Y \cap Z$ sobre sus componentes irreducibles?
3. ¿Cuál es el análogo correcto en dimensiones mayores de la hipótesis de que Y, Z no tienen componentes irreducibles en común?

Este trabajo está dividido en seis capítulos. En los dos primeros capítulos, presentaremos las variedades afines y proyectivas, haciendo hincapié en la correspondencia entre las variedades y los anillos de coordenadas que las describen. Algunos aspectos de nuestra presentación son un tanto idiosincráticos. En particular, haremos más énfasis en el cono afín sobre una variedad proyectiva que en la cobertura de la variedad por abiertos afines[2].

[1] Aunque [Kir92, p. 51] cuestiona esta atribución.

[2] En la medida de lo posible, evitaremos apelar a la idea topológica de vecindad, ya que la geometría algebraica tiene sus propias ideas sobre qué es una vecindad.

Los dos siguientes capítulos son álgebra pura y dura. En último término, todo anillo debe ser estudiado a través de sus módulos, así que desarrollaremos la maquinaria algebraica para extraer información cuantitativa de un módulo finitamente generado sobre un anillo de coordenadas. Nos enfocaremos en dos casos específicos: en el capítulo 3, estudiaremos los módulos sobre anillos que describen variedades proyectivas, mientras que, en el capítulo 4, estudiaremos los módulos sobre anillos que describen vecindades genéricas de un punto.

El capítulo 5 marca el inicio de nuestro retorno a la geometría. Para ello, comenzamos dando una interpretación visual e intuitiva, aunque no totalmente rigurosa, para un módulo finitamente generado sobre un anillo de coordenadas. Demostraremos que las herramientas construidas en los capítulos 3 y 4 tienen un significado geométrico consistente con esta interpretación.

Finalmente, en el capítulo 6, enunciaremos y demostraremos dos teoremas (en realidad, dos variantes del mismo teorema) que generalizan el teorema clásico de Bézout. Como aplicación de estos resultados, calcularemos el grupo de automorfismos del espacio proyectivo $\mathbb{P}^n$.

Capítulo 1

Variedades afines

La geometría algebraica estudia las *variedades algebraicas*, espacios conformados por los ceros de una familia de polinomios. Los dos tipos más importantes de variedades algebraicas, y los únicos que discutiremos en este trabajo, son las *variedades afines* y las *variedades proyectivas*.

En este capítulo, presentamos los hechos básicos sobre las variedades afines que utilizaremos en el resto del trabajo. El más importante de ellos es que toda variedad afín es caracterizada de manera precisa por un *anillo de coordenadas*. Esta caracterización se extiende a una equivalencia dual entre la categoría de variedades afines y la categoría de k-álgebras finitamente generadas sin elementos divisores de cero.

Fijemos a lo largo de este trabajo un cuerpo algebraicamente cerrado k.

1.1. Conjuntos algebraicos afines

Definición. El *espacio afín* de dimensión $n \in \mathbb{N}$, denotado $\mathbb{A}^n$, es el conjunto de tuplas $(a_1 \dots a_n)$ conformadas por elementos de k. Para enfatizar que $\mathbb{A}^n$ es un objeto geométrico, llamamos *puntos* a las tuplas $(a_1 \dots a_n)$ y llamamos *coordenadas* a las componentes a_i.

Definición. Las *funciones coordenadas* de $\mathbb{A}^n$ son las funciones $x_i : \mathbb{A}^n \to k$ que asignan a cada punto de $\mathbb{A}^n$ su i-ésima coordenada. Una *función regular* sobre $\mathbb{A}^n$ es una función $f : \mathbb{A}^n \to k$ que se puede expresar como polinomio en $x_1 \dots x_n$. El *anillo de coordenadas* de $\mathbb{A}^n$, denotado $k[\mathbb{A}^n]$, está conformado por las funciones regulares $f : \mathbb{A}^n \to k$.

Definición. Sea $F \subset k[\mathbb{A}^n]$ una familia de funciones regulares. Decimos que el punto $p \in \mathbb{A}^n$ es un *cero* de F si $f(p) = 0$ para todo $f \in F$. El *conjunto algebraico afín* de F, denotado $V(F)$, es el conjunto de ceros de F en $\mathbb{A}^n$.

Observación. Si $\mathfrak{a} \subset k[\mathbb{A}^n]$ es el ideal generado por F, entonces $V(\mathfrak{a}) = V(F)$.

Ejemplo. La *cúspide cúbica* $V(x^3 - y^2) \subset \mathbb{A}^2$ es una curva afín plana.

Ejemplo. La *cúbica torcida* $V(y - x^2, z - x^3) \subset \mathbb{A}^3$ es un curva afín no plana.

Definición. Sea $X \subset \mathbb{A}^n$ un conjunto de puntos. Decimos que una función regular $f : \mathbb{A}^n \to k$ se *anula* en X si $f(p) = 0$ para todo $p \in X$. El ideal de X, denotado $I(X)$, está conformado por las funciones regulares que se anulan en X.

Observación. Por construcción, $I(X)$ es un ideal radical de $k[\mathbb{A}^n]$.

Teorema 1.1. *(Teorema de la base de Hilbert) Sea R un anillo noetheriano. Entonces el anillo de polinomios $R[x]$ también es noetheriano.*

Prueba. Ver [Ful89, pp. 13-14]. □

Corolario 1.2. *El anillo de coordenadas $k[\mathbb{A}^n]$ es noetheriano. Por ende, todo conjunto algebraico es la interseccción de un número finito de hipersuperficies.* □

1.2. Topología y dimensión

Definición. Un espacio topológico es *irreducible* si no se puede expresar como la unión de una cantidad finita de subconjuntos cerrados propios.

Observación. El espacio topológico vacío tiene cero subconjuntos cerrados y es la unión de todos ellos. Por ende, el espacio vacío *no* es irreducible[1].

Definición. Un espacio topológico X es *noetheriano* si, para toda cadena descendente

$$X_0 \supset X_1 \supset X_2 \supset \dots$$

de subespacios cerrados de X, existe un instante $n \in \mathbb{N}$ tal que $X_{n+r} = X_n$ para todo $r \in \mathbb{N}$.

Observación. Todo espacio noetheriano es *casi compacto*, i.e., toda cobertura abierta del espacio tiene una subcobertura finita.

Definición. La *dimensión* de un espacio topológico X es el supremo de los números $n \in \mathbb{N}$ tales que existe una cadena estrictamente descendente

$$X_0 \supsetneq X_1 \supsetneq \dots \supsetneq X_n$$

de subespacios irreducibles cerrados de X. Por convención, $\dim \varnothing = -1$.

Ejemplo. Sea $X = \mathbb{N}$ el conjunto de los números naturales con la topología cuyos subconjuntos cerrados son $X_n = \{k \in \mathbb{N} \mid k < n\}$ para todo $n = 0, 1, 2 \dots \infty$. Entonces X_n es irreducible para todo $n > 0$. Por ende, X es un espacio topológico noetheriano de dimensión infinita.

Definición. Sea X un espacio noetheriano. Las *componentes irreducibles* de X son los elementos maximales de la familia de subespacios irreducibles cerrados de X.

[1] Análogamente, el espacio topológico vacío no es conexo, el grupo o módulo trivial no es simple, un anillo no es ideal maximal de sí mismo, etc. Fuente: `https://ncatlab.org/nlab/show/too+simple+to+be+simple`.

Proposición 1.3. *Todo subconjunto abierto no vacío de un espacio irreducible es irreducible.*

Prueba. Ver [Har77, p. 3]. □

Proposición 1.4. *Todo espacio topológico noetheriano tiene un número finito de componentes irreducibles. La unión de todas ellas es el espacio completo. La unión de algunas de ellas, pero no todas, es un subespacio propio.*

Prueba. Es lógicamente equivalente a [Har77, p. 5]. □

1.3. El diccionario álgebra-geometría

Preliminares. Sea $V \subset \mathbb{A}^n$ un conjunto algebraico afín.

Proposición 1.5. *Los subconjuntos algebraicos de V forman una familia cerrada bajo uniones finitas e intersecciones arbitrarias. Por ende, sus complementos forman una topología sobre V.*

Prueba. Ver [Har77, p. 2]. □

Definición. La *topología de Zariski* sobre V es la topología de la proposición anterior.

Observación. Por el teorema de la base de Hilbert, V es un espacio topológico noetheriano.

Proposición 1.6. *Un conjunto algebraico afín es irreducible si y sólo si su ideal es primo.*

Prueba. Ver [Ful89, p. 15]. □

Corolario 1.7. *Las componentes irreducibles de V son los conjuntos $V(\mathfrak{p})$, donde $\mathfrak{p} \subset k[\mathbb{A}^n]$ es un ideal primo minimal entre aquellos que contienen a $I(V)$.* □

Teorema 1.8. *(Teorema de los ceros de Hilbert)*

- *Todo ideal maximal de $k[\mathbb{A}^n]$ es el ideal de un punto $p \in \mathbb{A}^n$.*
- *Todo ideal propio de $k[\mathbb{A}^n]$ se anula en algún punto $p \in \mathbb{A}^n$.*
- *Sea $\mathfrak{a} \subset k[\mathbb{A}^n]$ un ideal arbitrario. Entonces $I(V(\mathfrak{a})) = \mathrm{Rad}(\mathfrak{a})$.*

Prueba. Ver [Ful89, pp. 20-22]. □

Corolario 1.9. *Existen correspondencias biyectivas entre*

- *Los puntos de $\mathbb{A}^n$ y los ideales maximales de $k[\mathbb{A}^n]$.*
- *Los subconjuntos algebraicos irreducibles de $\mathbb{A}^n$ y los ideales primos de $k[\mathbb{A}^n]$.*
- *Los subconjuntos algebraicos de $\mathbb{A}^n$ y los ideales radicales de $k[\mathbb{A}^n]$.* □

1.4. Variedades afines

Preliminares. Sean $V \subset \mathbb{A}^n$ y $W \subset \mathbb{A}^m$ dos variedades afines, como definimos a continuación.

Definición. Una *variedad afín* es un conjunto algebraico afín vacío o irreducible.

Definición. Una *función regular* sobre V es una función $f : V \to k$ que se puede expresar como restricción a V de una función regular $\bar{f} : \mathbb{A}^n \to k$. El *anillo de coordenadas* de V, denotado por $k[V]$, está conformado por las funciones regulares sobre V.

Observación. Dos funciones regulares sobre $\mathbb{A}^n$ inducen la misma función sobre V si y sólo si su diferencia está en $I(V)$. Por ende, $k[V]$ es naturalmente isomorfo a $k[\mathbb{A}^n]/I(V)$.

Definición. Un *morfismo regular* es una función $\varphi : V \to W$ tal que, para toda función regular $f : W \to k$, la composición $f \circ \varphi : V \to k$ también es una función regular.

Observación. La composición de una cantidad finita de morfismos regulares $\varphi_i : V_{i-1} \to V_i$ es un morfismo regular $\varphi_n \circ \cdots \circ \varphi_1 : V_0 \to V_n$. Por ende, tenemos una categoría de variedades afines y morfismos regulares.

Definición. El *pullback* de un morfismo regular $\varphi : V \to W$ es el homomorfismo de k-álgebras $\varphi^\star : k[W] \to k[V]$ cuya regla de correspondencia es $\varphi^\star(f) = f \circ \varphi$.

Proposición 1.10. *Para cada homomorfismo de k-álgebras $\alpha : k[W] \to k[V]$, existe exactamente un morfismo regular $\varphi : V \to W$ cuyo pullback es $\varphi^\star = \alpha$.*

Prueba. Es lógicamente equivalente a [Ful89, p. 38]. □

Definición. Un *isomorfismo regular* es un morfismo regular invertible cuya inversa es regular.

Corolario 1.11. *Dos variedades afines son isomorfas si y sólo si sus anillos de coordenadas son isomorfos como k-álgebras.* □

Ejemplo. El anillo de coordenadas de la cúbica torcida $V \subset \mathbb{A}^3$ es generado por $x : V \to k$, pues las otras dos funciones coordenadas $y, z : V \to k$ son meros sinónimos de x^2, x^3, respectivamente. Por ende, $x : V \to \mathbb{A}^1$ es un isomorfismo en la categoría regular.

Ejemplo. Sea $V \subset \mathbb{A}^2$ la cúspide cúbica y sea $\varphi : \mathbb{A}^1 \to V$ la aplicación regular $\varphi(t) = (t^2, t^3)$. Todo elemento de k está completamente determinado por su cuadrado y su cubo. Por ende, φ es un morfismo regular biyectivo.

Por otro lado, $t = y/x$ es raíz del polinomio mónico $t^2 - x$, pero $t \notin k[V]$. Entonces $k[V]$ no es íntegramente cerrado. Por ende, $k[V]$ no es isomorfo a $k[\mathbb{A}^1]$. Por ende, V no es isomorfo a $\mathbb{A}^1$.

Observación. Este ejemplo es el ejercicio I.3.2.a de [Har77, p. 21].

Ejemplo. Sea k un cuerpo de característica $p > 0$. La aplicación $f : k \to k$ que envía escalares a sus p-ésimas potencias es conocida como el *endomorfismo de Frobenius*. Si k es algebraicamente cerrado, todo elemento de k tiene una única raíz p-ésima, por ende $f : \mathbb{A}^1 \to \mathbb{A}^1$ es una biyección regular de la recta afín sobre sí misma.

Por otro lado, el pullback $f^\star : k[t] \to k[t]$ dado por $f^\star(t) = t^p$ no es un isomorfismo de anillos, razón por la cual f no es un automorfismo regular[2].

Observación. Este ejemplo es el ejercicio I.3.2.b de [Har77, p. 21].

Corolario 1.12. *Existen correspondencias biyectivas entre*

- *Los conjuntos algebraicos afines* $V \subset \mathbb{A}^n$ *y las* k*-álgebras reducidas* $k[V]$.
- *Las variedades afines* $V \subset \mathbb{A}^n$ *y las* k*-álgebras* $k[V]$ *sin divisores de cero.*
- *Los morfismos regulares* $\varphi : V \to W$ *y los* k*-homomorfismos* $\varphi^\star : k[W] \to k[V]$.
- *Los isomorfismos regulares* $\varphi : V \to W$ *y los* k*-isomorfismos* $\varphi^\star : k[W] \to k[V]$. □

[2] Sin embargo, $f : k \to k$ sí es un automorfismo de cuerpos.

Capítulo 2

Variedades proyectivas

El principal atractivo de las variedades afines es que son fáciles de usar. Esto no debería causar mayor sorpresa, porque una variedad afín es simplemente la reinterpretación de un dominio como objeto geométrico. Sin embargo, la simplicidad algebraica de las variedades afines no es garantía de que éstas tengan las propiedades geométricas que necesitamos en un momento dado.

Recordemos que el propósito de este trabajo es intersecar dos variedades algebraicas y contar las componentes irreducibles de la intersección. Al menos en este caso particular, las variedades afines no son tan bien comportadas como uno quisiera.

Uno de los defectos de la geometría afín es que la intersección de dos variedades afines no es estable bajo perturbaciones pequeñas. Para ilustrar esto de manera concreta, supongamos que el cuerpo base es $k = \mathbb{C}$. En el plano $\mathbb{C}^2$, las rectas $x = 0$ y $x = 1$ no se intersecan en ningún punto. Sin embargo, si perturbamos ligeramente la pendiente de $x = 0$ para que sea $x = \varepsilon y$, entonces la intersección de esta última recta con $x = 1$ consta exactamente de un punto.

Otro defecto aún más serio de la geometría afín es que, en dimensiones ≥ 2, el grado de una función regular sobre $\mathbb{A}^n$ no es invariante bajo la acción del grupo de automorfismos[1] de $\mathbb{A}^n$. Por ejemplo, $f(x, y) = x$ tiene grado 1, pero su imagen bajo el pullback de $\varphi(x, y) = (x + y^2, y)$ tiene grado 2. No parece haber otras invariantes numéricas que podamos asociar a una hipersuperficie afín, mucho menos una variedad afín en general.

En este capítulo, presentamos otra clase de variedades algebraicas, las *variedades proyectivas*, que son un poco más complicadas que las variedades afines, pero cuyas intersecciones son mucho mejor comportadas. Las variedades proyectivas son subconjuntos del *espacio proyectivo*, que está expresamente construido para que sus automorfismos sean transformaciones lineales.

Toda variedad proyectiva tiene un *anillo de coordenadas homogéneo*. Este anillo no describe a la variedad como espacio abstracto, sino la manera como está encajada en el espacio proyectivo. Para nosotros, esto no es un problema, porque la intersección de dos variedades solamente tiene sentido si ambas están encajadas en un ambiente común.

[1] El problema de fondo es que $\mathrm{Aut}(\mathbb{A}^n)$ es un grupo demasiado complicado. De hecho, existen conjeturas aún no resueltas sobre este grupo, como la famosa *conjetura del jacobiano*: todo endomorfismo regular $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ cuyo jacobiano es una constante no nula es en efecto un automorfismo.

2.1. Conos afines

Preliminares. En este capítulo, $p \in \mathbb{A}^{n+1}$ denotará un punto distinto del origen.

Notación. Dado un punto $p \in \mathbb{A}^{n+1}$, denotamos $L_p \subset \mathbb{A}^{n+1}$ la única recta que pasa tanto por p como por el origen. Si $p = (a_0, \dots, a_n)$, entonces escribimos $L_p = [a_0 : \cdots : a_n]$.

Definición. Un *cono afín* es un conjunto $C \subset \mathbb{A}^{n+1}$ que contiene al origen y tal que, para todo punto $p \in C$, tenemos también $L_p \subset C$.

Observación. Toda unión e intersección de conos afines es un cono afín. Por convención, la unión de cero conos afines es el origen y la intersección de cero conos afines es $\mathbb{A}^{n+1}$.

Definición. Una *función homogénea* sobre $\mathbb{A}^{n+1}$ es una función regular $f : \mathbb{A}^{n+1} \to k$ que puede ser expresada como un polinomio homogéneo en las funciones coordenadas $x_0 \dots x_n$.

Observación. Si $f(p) = 0$, entonces $f(q) = 0$ para todo $q \in L_p$. Por ende, $V(f)$ es un cono afín.

Definición. Sea $f : \mathbb{A}^{n+1} \to k$ una función regular de grado $d \in \mathbb{N}$. Las partes homogéneas de f son las únicas funciones homogéneas $f_r : \mathbb{A}^{n+1} \to k$ tales que $f = \sum_r f_r$ y $\deg f_r = r$.

Observación. Sólo un número finito de partes homogéneas de f son distintas de cero.

Proposición 2.1. *Sea $f : \mathbb{A}^{n+1} \to k$ una función regular que se anula en L_p. Entonces las partes homogéneas de f se anulan en L_p.*

Prueba. Consideremos el polinomio

$$g(t) = f(tp) = \sum_i f_i(tp) = \sum_i f_i(p)t^i$$

Puesto que $g(t) = 0$ para todo $t \in k$, todos los coeficientes $f_i(p)$ son nulos. □

Definición. Un *ideal homogéneo* es un ideal $\mathfrak{a} \subset k[\mathbb{A}^{n+1}]$ tal que las partes homogéneas de toda función regular $f \in \mathfrak{a}$ también están contenidas en $\mathfrak{a}$.

Observación. Toda suma, intersección o producto de ideales homogéneos es un ideal homogéneo.

Proposición 2.2. *Un ideal de $k[\mathbb{A}^{n+1}]$ es homogéneo si y sólo si es generado por una cantidad finita de funciones homogéneas.*

Prueba. Ver [Ful89, p. 89]. □

Proposición 2.3. *Un ideal homogéneo $\mathfrak{a} \subset k[\mathbb{A}^{n+1}]$ es primo si y solamente si, para todo par de funciones homogéneas $f, g : \mathbb{A}^{n+1} \to k$ tales que $f, g \notin \mathfrak{a}$, entonces $fg \notin \mathfrak{a}$.*

Prueba. Sean f_r, g_s las partes homogéneas de f, g de mayor grado tales que $f_r, g_s \notin \mathfrak{a}$. Entonces, la parte homogénea de fg de grado $r + s$ es de la forma $f_r g_s + h$ para algún $h \in \mathfrak{a}$. Puesto que $f_r, g_s \notin \mathfrak{a}$, tenemos $f_r g_s + h \notin \mathfrak{a}$. Puesto que $\mathfrak{a}$ es homogéneo, $fg \notin \mathfrak{a}$. □

Proposición 2.4. *El radical de un ideal homogéneo* $\mathfrak{a} \subset k[\mathbb{A}^{n+1}]$ *es un ideal homogéneo.*

Prueba. Sea $f : \mathbb{A}^{n+1} \to k$ una función regular y sea f_r la parte homogénea de f de mayor grado tal que $f_r^s \notin \mathfrak{a}$ para todo $s \in \mathbb{N}$. Entonces, la parte homogénea de f^s de grado rs es de la forma $f_r^s + h_s$ para algún $h_s \in \mathfrak{a}$. Entonces $f_r^s + h_s \notin a$. Puesto que $\mathfrak{a}$ es homogéneo, $f^r \notin \mathfrak{a}$. □

Proposición 2.5. *Las componentes irreducibles de un cono afín algebraico son conos afines.*

Prueba. Sea $C \subset \mathbb{A}^{n+1}$ un cono algebraico reducible. Entonces $\mathfrak{a} = I(C)$ es un ideal homogéneo, pero no primo. Existen funciones homogéneas $f_i : \mathbb{A}^{n+1} \to k$ tales que $f_i \notin \mathfrak{a}$, pero $\prod_i f_i \in \mathfrak{a}$. Por ende, C es la unión de los subconos afines $V(\mathfrak{a}, f_i)$. □

Corolario 2.6. *Existen correspondencias biyectivas entre*

- *Los conos afines algebraicos en* $\mathbb{A}^{n+1}$ *y los ideales radicales homogéneos propios de* $k[\mathbb{A}^{n+1}]$.
- *Los conos afines irreducibles en* $\mathbb{A}^{n+1}$ *y los ideales primos homogéneos de* $k[\mathbb{A}^{n+1}]$. □

2.2. Conjuntos algebraicos proyectivos

Definición. El *espacio proyectivo* de dimensión $n \in \mathbb{N}$, denotado $\mathbb{P}^n$, es el conjunto de rectas $L_p \subset \mathbb{A}^{n+1}$. Para enfatizar que $\mathbb{P}^n$ es un objeto geométrico, llamaremos *puntos* a las rectas L_p y llamaremos *coordenadas homogéneas* de L_p a las coordenadas ordinarias de p.

Observación. A diferencia de las coordenadas ordinarias de $p \in \mathbb{A}^n$, las coordenadas homogéneas de $L_p \in \mathbb{P}^n$ no son únicas, ya que pueden ser reescaladas.

Definición. El *anillo de coordenadas homogéneo* de $\mathbb{P}^n$ es $k_h[\mathbb{P}^n] = k[\mathbb{A}^{n+1}]$.

Definición. Sea $F \subset k_h[\mathbb{P}^n]$ un conjunto de funciones homogéneas. Decimos que el punto $L_p \in \mathbb{P}^n$ es un *cero* de F si $f(p) = 0$ para todo $f \in F$. El *conjunto algebraico proyectivo* de F, denotado $V(F)$, es el conjunto de ceros de F en $\mathbb{P}^n$.

Observación. Si $\mathfrak{a} \subset k[\mathbb{A}^n]$ es el ideal homogéneo generado por F, entonces $V(\mathfrak{a}) = V(F)$.

Ejemplo. La *curva elíptica* $V(zy^2 + xz^2 - x^3) \subset \mathbb{P}^2$ es una curva proyectiva plana.

Ejemplo. La *superficie cuádrica* $V(xy - zw) \subset \mathbb{P}^3$ es una superficie proyectiva.

Definición. Sea $X \subset \mathbb{P}^n$ un conjunto de puntos. El *cono afín* sobre X, denotado por $C(X)$, es la unión de los puntos $L_p \in X$, considerados como rectas en $\mathbb{A}^{n+1}$. Por convención, el cono afín sobre el conjunto proyectivo vacío es el origen de coordenadas de $\mathbb{A}^{n+1}$.

Observación. Por construcción, X es un conjunto algebraico proyectivo si y sólo si $C(X)$ es un conjunto algebraico afín.

Definición. Sea $X \subset \mathbb{P}^n$ un conjunto de puntos. Decimos que una función regular $f : \mathbb{A}^{n+1} \to k$ se *anula* en X si $f(p) = 0$ para todo $L_p \in X$. El ideal de X, denotado $I(X)$, está conformado por las funciones regulares sin inversa multiplicativa que se anulan en X.

Observación. Por construcción, $I(X) = I(C(X))$.

Corolario 2.7. *Existen correspondencias biyectivas entre*

- *Los subconjuntos de $\mathbb{P}^n$ y los conos afines en $\mathbb{A}^{n+1}$.*
- *Los subconjuntos algebraicos de $\mathbb{P}^n$ y los conos algebraicos afines en $\mathbb{A}^{n+1}$.* □

2.3. El diccionario álgebra-geometría

Preliminares. Sea $V \subset \mathbb{P}^n$ un conjunto algebraico proyectivo.

Proposición 2.8. *Los subconjuntos algebraicos de V forman una familia cerrada bajo uniones finitas e intersecciones arbitrarias. Por ende, sus complementos forman una topología sobre V.*

Prueba. Idéntica a la proposición 1.5. □

Definición. La *topología de Zariski* sobre V es la topología de la proposición anterior.

Observación. Por el teorema de la base de Hilbert, V es un espacio topológico noetheriano.

Definición. El *ideal irrelevante* $\mathfrak{m} \subset k_h[\mathbb{P}^n]$ es el ideal del conjunto proyectivo vacío.

Proposición 2.9. *Un conjunto algebraico proyectivo es irreducible si y sólo si su ideal es primo, pero no irrelevante.*

Prueba. Idéntica a la proposición 1.6. □

Corolario 2.10. *Las componentes irreducibles de V son los conjuntos $V(\mathfrak{p})$, donde $\mathfrak{p} \subset k_h[\mathbb{P}^n]$ es un ideal primo minimal entre aquellos que contienen a $I(V)$ y no son irrelevantes.* □

Corolario 2.11. *El conjunto V tiene dimensión* $\dim V = \dim C(V) - 1$. □

Corolario 2.12. *Existen correspondencias biyectivas entre*

- *Los subconjuntos algebraicos de $\mathbb{P}^n$ y los ideales radicales homogéneos propios de $k_h[\mathbb{P}^n]$.*
- *Los subconjuntos algebraicos irreducibles de $\mathbb{P}^n$ y los ideales primos homogéneos de $k_h[\mathbb{P}^n]$, distintos del ideal irrelevante.* □

2.4. Variedades proyectivas

Preliminares. Sean $V \subset \mathbb{P}^n$ una variedad proyectiva, tal y como definimos a continuación. Sea $C \subset \mathbb{A}^{n+1}$ el cono afín sobre V.

Definición. Una *variedad proyectiva* es un conjunto algebraico proyectivo vacío o irreducible.

Definición. Una *función homogénea* sobre C es una función regular $f : C \to k$ que puede ser expresada como la restricción a C de una función homogénea $\bar{f} : \mathbb{A}^{n+1} \to k$.

Definición. El *anillo de coordenadas homogéneo* de V es $k_h[V] = k[C]$.

Observación. Dos funciones homogéneas $f, g : \mathbb{A}^{n+1} \to k$ inducen la misma función homogénea sobre V si y sólo si $f - g \in I(V)$. Por ende, $k_h[V]$ es naturalmente isomorfo a $k_h[\mathbb{P}^n]/I(V)$.

Proposición 2.13. *Sea $f : C \to k$ una función regular. Existe una única sucesión de funciones homogéneas $f_r : C \to k$ tales que $f = \sum_r f_r$ y $\deg f_r = r$. Además, sólo un número finito de ellas son distintas de cero.*

Prueba. Ver [Ful89, p. 92]. □

Definición. El *cuerpo de funciones racionales* sobre V, denotado $k(V)$, está conformado por los cocientes f/g, donde $f, g : C \to k$ son funciones homogéneas del mismo grado y g no es la función idénticamente nula.

Observación. Las reglas usuales para manipular fracciones son válidas en $k(V)$. En particular, si f, g tienen un factor común, podemos simplificar dicho factor sin alterar el cociente.

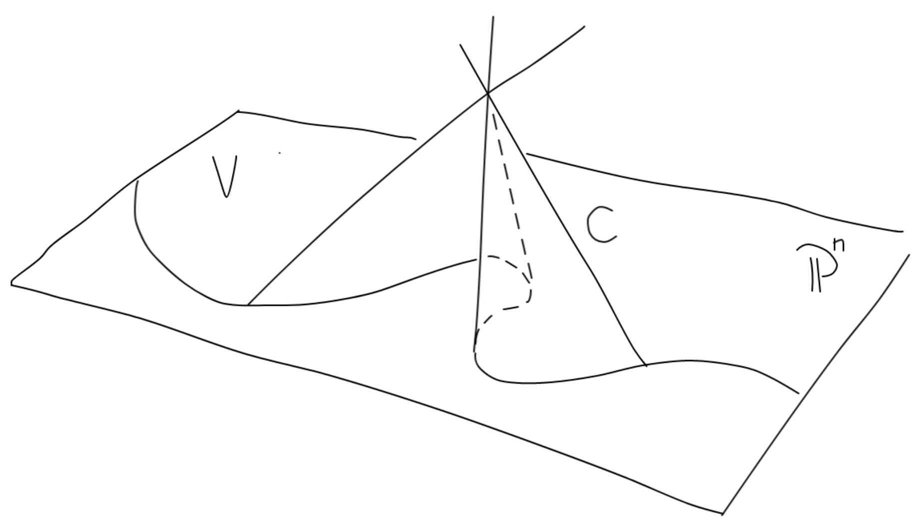

Figura 2.1: Cono sobre una variedad proyectiva [Har77, p. 12]

Definición. Sea $z \in k(V)$ una función racional. Decimos que z está *definida* en $p \in V$ si existen funciones homogéneas $f, g : C \to k$ tales que $z = f/g$ y además $g(p) \neq 0$. Decimos que z se *anula* en p si, además, $f(p) = 0$.

Definición. El *anillo local* de V en el punto $p \in V$, denotado $\mathscr{O}_p(V)$, está conformado por todas las funciones racionales $z \in k(V)$ definidas en p.

Observación. Si $z \in k(V)$ no se anula en p, entonces z^{-1} está definida en p, por ende...

Definición. El único *ideal maximal* de $\mathscr{O}_p(V)$, denotado $\mathfrak{m}_p(V)$, está conformado por todas las funciones racionales $z \in k(V)$ que se anulan en p.

Observación. En general, diremos que un anillo es *local* si tiene un único ideal maximal.

Definición. Una *función regular* sobre un subconjunto abierto de Zariski $U \subset V$ es una función racional sobre V que está definida en todo punto $p \in U$.

Corolario 2.14. *Toda función regular sobre una variedad proyectiva es constante.*

2.5. Variedades casi proyectivas

Preliminares. Sean $V \subset \mathbb{P}^n$ y $W \subset \mathbb{P}^m$ dos variedades casi proyectivas, tal y como definimos a continuación.

Definición. Una *variedad casi proyectiva* es un subconjunto abierto de una variedad proyectiva.

Definición. Un *morfismo regular* es una función continua $\varphi : V \to W$ tal que, para toda función regular $f : U \to k$ definida sobre un abierto de Zariski $U \subset W$, el pullback $\varphi^\star(f) : \varphi^{-1}(U) \to k$ es también una función regular.

Definición. Un *isomorfismo regular* es un morfismo regular invertible cuya inversa es regular.

Proposición 2.15. *Sea $U \subset \mathbb{P}^n$ el complemento de un hiperplano. Entonces existe un isomorfismo regular $\varphi : \mathbb{A}^n \to U$.*

Prueba. Supongamos sin pérdida de generalidad que U es el complemento del hiperplano $x_0 = 0$. Entonces $\varphi(x_1 \dots x_n) = [1 : x_1 : \dots : x_n]$ es un isomorfismo. □

Definición. Un *morfismo racional* $\varphi : V \dashrightarrow W$ es un morfismo regular $\varphi : U \to W$ que parte de un subconjunto abierto denso $U \subset V$. Decimos que φ está *definido* sobre los puntos $p \in U$.

Definición. Un *morfismo birracional* $\varphi : V \dashrightarrow V'$ es un isomorfismo regular $\varphi : U \to U'$ entre subconjuntos abiertos y densos de V, V', respectivamente.

Ejemplo. El espacio afín $\mathbb{A}^n$ es birracionalmente equivalente al espacio proyectivo $\mathbb{P}^n$.

Proposición 2.16. *Dos variedades son birracionalmente equivalentes si y sólo si sus cuerpos de fracciones son isomorfos.*

Prueba. Ver [Ful89, p. 155]. □

2.6. Automorfismos de $\mathbb{P}^n$

Identifiquemos el espacio afín $\mathbb{A}^{n+1}$ con el espacio vectorial k^{n+1} y consideremos la acción de $k^\star$ sobre $\mathbb{A}^{n+1}$ vía reescalamientos. El espacio de órbitas de esta acción no es muy bien comportado, ya que el origen está en la vecindad de todas las demás órbitas[2]. Sin embargo, si removemos este punto fijo problemático, recuperamos el espacio proyectivo $\mathbb{P}^n$.

Es evidente que todo automorfismo $\tilde{\varphi} : \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ que respeta las órbitas de $k^\star$ induce un automorfismo $\varphi : \mathbb{P}^n \to \mathbb{P}^n$. En este caso, tenemos $\varphi \circ L = L \circ \tilde{\varphi}$, donde L envía cada $p \in \mathbb{A}^{n+1}$ a su órbita $L_p \in \mathbb{P}^n$. Por ende, el cociente $\mathrm{GL}(\mathbb{A}^{n+1})/k^\star$ es un subgrupo de $\mathrm{Aut}(\mathbb{P}^n)$.

La prueba de la inclusión reversa se dará en la sección 6.4.

[2] En el lenguaje moderno, decimos que este espacio de órbitas es un esquema no separado.

Capítulo 3

Anillos y módulos graduados

La relación entre una variedad proyectiva y su anillo de coordenadas homogéneo es más delicada y sutil que su contraparte en el caso afín. Para empezar, los elementos del anillo no son funciones regulares sobre la variedad[1]. Dado un elemento homogéneo del anillo, tiene sentido preguntar en qué puntos se anula dicho elemento. Sin embargo, los elementos no homogéneos no tienen ningún significado geométrico.

Para enfatizar que sólo nos interesan los elementos homogéneos de un anillo o un módulo, lo equiparemos con una *gradación*. En este capítulo, desarrollaremos las herramientas técnicas para extraer la mayor cantidad de información posible sobre un módulo graduado. La más importante de estas herramientas es el *polinomio de Hilbert*, que ocupará un lugar central en este trabajo.

3.1. Definiciones básicas

Definición. Un *anillo graduado* es un anillo R con una descomposición

$$R = R_0 \oplus R_1 \oplus R_2 \oplus \dots$$

de su grupo aditivo, tal que $R_i R_j \subset R_{i+j}$ para todo $i, j \in \mathbb{N}$.

Observación. R_0 es un anillo y R_n es un R_0-módulo para todo $n \in \mathbb{N}$. Por convención, extendemos la gradación de R con $R_n = 0$ para todo $n < 0$.

Ejemplo. El anillo de polinomios $k[x_1 \dots x_n]$ es el prototipo de anillo graduado.

Ejemplo. El anillo de coordenadas homogéneo de una variedad proyectiva es graduado.

Ejemplo. Un anillo graduado no conmutativo importante en la geometría diferencial es el álgebra $\Omega(M)$ de formas diferenciales sobre una variedad diferenciable M. Este anillo con la operación de derivada exterior $d : \Omega^n(M) \to \Omega^{n+1}(M)$ es un *álgebra graduada diferencial*.

Observación. En este trabajo no utilizaremos anillos no conmutativos.

[1] De hecho, las únicas funciones regulares definidas sobre toda una variedad proyectiva son las constantes.

Definición. Un *R-módulo graduado* es un R-módulo M con una descomposición

$$M = \dots \oplus M_{-2} \oplus M_{-1} \oplus M_0 \oplus M_1 \oplus M_2 \oplus \dots$$

de su grupo aditivo, tal que $R_i M_j \subset M_{i+j}$ para todo $i \in \mathbb{N}, j \in \mathbb{Z}$.

Ejemplo. El anillo de coordenadas homogéneo $k_h[V]$ de una variedad proyectiva $V \subset \mathbb{P}^n$ es tanto un $k_h[\mathbb{P}^n]$-módulo graduado como un anillo graduado por cuenta propia.

Definición. El sumando directo M_n se denomina la *parte homogénea* de M de grado n y sus elementos se denominan *elementos homogéneos* de M de grado n. La componente de $m \in M$ en la parte homogénea M_n se denomina la *parte homogénea* de m de grado n.

Observación. Para todo $n \in \mathbb{Z}$, la parte homogénea M_n es un R_0-módulo.

Definición. Un *ideal homogéneo* de R es un ideal $I \subset R$ de la forma

$$I = I_0 \oplus I_1 \oplus I_2 \oplus \dots$$

donde I_n es un R_0-submódulo de R_n para todo $n \in \mathbb{Z}$.

Ejemplo. El *ideal irrelevante* de R es

$$R_+ = R_1 \oplus R_2 \oplus R_3 \oplus \dots$$

Definición. Un *R-submódulo graduado* de M es un R-submódulo $N \subset M$ de la forma

$$N = \dots \oplus N_{-2} \oplus N_{-1} \oplus N_0 \oplus N_1 \oplus N_2 \oplus \dots$$

donde N_n es un R_0-submódulo de M_n para todo $n \in \mathbb{Z}$.

Ejemplo. El submódulo de elementos de M de grado mayor o igual que $n \in \mathbb{Z}$ es

$$M_{\geq n} = R_n \oplus R_{n+1} \oplus R_{n+2} \oplus \dots$$

Definición. Un *R-homomorfismo graduado* es un R-homomorfismo $\varphi : M \to N$ de la forma

$$\varphi = \dots \oplus \varphi_{-2} \oplus \varphi_{-1} \oplus \varphi_0 \oplus \varphi_1 \oplus \varphi_2 \oplus \dots$$

donde $\varphi_n : M_n \to N_n$ es un R_0-homomorfismo para todo $n \in \mathbb{Z}$.

Observación. El núcleo $\ker \varphi$ y el conúcleo $\operatorname{coker} \varphi$ son módulos graduados.

Definición. Sea $l \in \mathbb{Z}$ un número entero. El *R-módulo torcido* $M(l)$ es el mismo R-módulo M, pero con la nueva gradación $M(l)_n = M_{n+l}$.

Observación. Torcer un anillo graduado R preserva la estructura de R-módulo, pero destruye la estructura de anillo graduado.

3.2. Serie de Poincaré

La referencia para esta sección es [AM69, pp. 106, 116-117].

Preliminares. Sean R un anillo graduado noetheriano y M un R-módulo graduado finitamente generado. Sea λ una función aditiva sobre la clase de R_0-módulos finitamente generados.

Proposición 3.1. *El anillo R_0 es noetheriano y R es un R_0-álgebra finitamente generada.*

Prueba. Puesto que R es un anillo noetheriano, el cociente $R_0 \cong R/R_+$ también es noetheriano y R_+ es finitamente generado, digamos, por $x_1 \dots x_s$. Supongamos sin pérdida de generalidad que $x_1 \dots x_s$ son homogéneos de grados $d_1 \dots d_s > 0$. Demostraremos que $x_1 \dots x_s$ también generan a R como R_0-álgebra.

Sea $y \in R_n$ un elemento homogéneo. Si $n = 0$, entonces y es trivialmente un polinomio en $x_1 \dots x_s$. Si $n > 0$, entonces existen elementos $a_1 \dots a_s$ tales que $y = a_1 x_1 + \dots + a_s x_s$. Podemos asumir sin pérdida de generalidad que cada a_i es homogéneo de grado $n - d_i$. Por inducción en el grado, $a_1 \dots a_s$ son polinomios en $x_1 \dots x_s$. Entonces y también es un polinomio en $x_1 \dots x_s$. □

Proposición 3.2. *Las partes homogéneas de M son R_0-módulos finitamente generados. Además, sólo un número finito de partes homogéneas de grado negativo pueden ser no triviales.*

Prueba. Sean $m_1 \dots m_r$ generadores de M como R-módulo. Asumamos sin pérdida de generalidad que $m_1 \dots m_r$ son homogéneos de grados $d_1 \dots d_r$. Sea p_i una enumeración de los monomios en $x_1 \dots x_s$, los generadores de R de la proposición anterior y sea c_i el grado total de p_i. Entonces M_n es generado como R_0-módulo por los productos $p_i m_j$ tales que $c_i + d_j = n$. En particular, M_n es trivial cuando $n < d_i$ para todo i, porque $c_i \geq 0$ para todo monomio p_i. □

Definición. La *serie de Poincaré* de M con respecto a λ es la serie de Laurent formal

$$S_M(t) = \dots + \lambda(M_{-2})t^{-2} + \lambda(M_{-1})t^{-1} + \lambda(M_0) + \lambda(M_1)t^1 + \lambda(M_2)t^2 + \dots$$

Teorema 3.3. *(Hilbert-Serre) La serie de Poincaré es una función racional de la forma*

$$S_M(t) = \frac{f(t)}{(1-t^{d_1})\dots(1-t^{d_s})}$$

donde $f \in \mathbb{Z}[t, t^{-1}]$ es un polinomio de Laurent y $d_1 \dots d_s > 0$ son los grados de los generadores $x_1 \dots x_s$ de R como R_0-álgebra que aparecen en las proposiciones anteriores.

Prueba. Por inducción en el número de generadores. Si $s = 0$, entonces $R = R_0$, por ende M sólo tiene un número finito de partes homogéneas no triviales. Por ende, $S_M(t)$ sólo tiene un número de términos, i.e., es un polinomio de Laurent.

Si $s > 0$, consideremos la sucesión exacta graduada

$$0 \longrightarrow N \longrightarrow M(-d_1) \xrightarrow{x_1} M \longrightarrow Q \longrightarrow 0$$

Por construcción, la serie de Poincaré $S_M(t)$ es una función aditiva de M. Entonces,

$$S_M(t) - S_{M(-d_1)}(t) = (1 - t^{d_1})S_M(t) = S_Q(t) - S_N(t)$$

Tanto $N = \ker x_1$ como $Q = \operatorname{coker} x_1$ son R-módulos finitamente generados anulados por x_1. Entonces ambos son R'-módulos finitamente generados, donde $R' \subset R$ es el subálgebra obtenida eliminando x_1 de la lista de generadores. Inductivamente, $S_Q(t) - S_N(t)$ es de la forma

$$(1 - t^{d_1})S_M(t) = S_Q(t) - S_N(t) = \frac{f(t)}{(1 - t^{d_2}) \dots (1 - t^{d_s})}$$

Reordenando factores, tenemos el resultado buscado. □

Definición. La *dimensión* de M es el uno menos que el orden del polo de $S(t)$ en $t = 1$.

Observación. En [AM69, p. 117], la dimensión de M está definida como el orden del polo de $S(t)$ en $t = 1$. Nuestra definición es más conveniente para el uso que le queremos dar.

Corolario 3.4. *Sea $x \in R$ un elemento homogéneo que no es divisor de cero en M. Si M tiene dimensión no negativa, entonces $N = M/xM$ tiene dimensión* $\dim N = \dim M - 1$.

Prueba. Sea $d = \deg x$. Puesto que la serie de Poincaré es aditiva,

$$S_N(t) = S_M(t) - S_{M(-d)}(t) = (1 - t^d)S_M(t)$$

Simplificando $1 - t^n$ con el denominador de $S_M(t)$, tenemos el resultado buscado. □

3.3. Polinomios numéricos

Preliminares. El polinomio nulo tiene grado -1.

Proposición 3.5. *Los coeficientes binomiales*

$$B_r(n) = \binom{n+r}{r} = \frac{1}{r!}\,(n+1)(n+2)\dots(n+r)$$

forman una base de $\mathbb{Q}[n]$ como $\mathbb{Q}$-espacio vectorial.

Prueba. Para todo $r \in \mathbb{N}$, el subespacio $V_r \subset \mathbb{Q}[z]$ generado por $B_0 \dots B_r$ es igual al subespacio generado por $1, x, \dots, x^r$. Puesto que cada $V_r \subset V_{r+1}$ es una inclusión propia, B_r es una sucesión linealmente independiente. Puesto que la unión de los subespacios V_r es todo el espacio $\mathbb{Q}[z]$, la sucesión B_r genera a $\mathbb{Q}[z]$. Entonces B_r es una base de $\mathbb{Q}[z]$. □

Notación. Será muy conveniente utilizar la abreviación

$$[c_0; c_1; \dots; c_r] = c_0 B_r + c_1 B_{r-1} + \dots + c_r B_0$$

ya que la base de coeficientes binomiales es más importante que la base de monomios.

Definición. Un polinomio $P \in \mathbb{Q}[n]$ es *numérico* si $P(n) \in \mathbb{Z}$ para todo $n \in \mathbb{Z}$.

Notación. Dado cualquier polinomio $P \in \mathbb{Q}[n]$, escribiremos $\Delta P(n) = P(n) - P(n-1)$.

Proposición 3.6. *Sea $P \in \mathbb{Q}[n]$ un polinomio de grado d. Supongamos que existen $d+1$ enteros consecutivos $n = a \dots b$ tales que $P(n) \in \mathbb{Z}$. Entonces P es un polinomio numérico.*

Prueba. Si $P = 0$, entonces no hay nada que demostrar. Si $P \neq 0$, entonces ΔP tiene grado $d-1$ y, para los d enteros consecutivos $n = a+1 \dots b$, tenemos $\Delta P(n) \in \mathbb{Z}$. Inductivamente, ΔP es un polinomio numérico. Entonces P también es un polinomio numérico. $\square$

Proposición 3.7. *Si $P = [c_0; c_1; \dots; c_r]$ es numérico, entonces $c_0, c_1, \dots, c_r \in \mathbb{Z}$.*

Prueba. Si $P = 0$, entonces no hay nada que demostrar. Si $P \neq 0$, entonces $\Delta P = [c_0; c_1; \dots; c_{r-1}]$ es numérico y tiene grado menor que P. Inductivamente, $c_0, c_1, \dots, c_{r-1} \in \mathbb{Z}$. Claro está, $c_r \in \mathbb{Z}$ también, porque $c_r = P(0)$. $\square$

3.4. Polinomio de Hilbert

La referencia para esta sección es [AM69, pp. 117-118].

Preliminares. Sean R un anillo graduado noetheriano y M un R-módulo graduado finitamente generado, como en la sección 3.2. Supongamos que los generadores x_i de R son de grado $d_i = 1$. Sea λ una función aditiva no negativa sobre la clase de R_0-módulos finitamente generados.

Proposición 3.8. *Existe un polinomio $P_M \in \mathbb{Q}[n]$ de grado $r = \dim M$ tal que $\lambda(M_n) = P_M(n)$ para todo $n \gg 0$.*

Prueba. Puesto que todos los x_i son de grado 1, el denominador de S_M es una potencia de $1-t$. Simplificando todas las ocurrencias del factor $1-t$ en el numerador, tenemos

$$S_M(t) = \frac{g(t)}{(1-t)^{r+1}}$$

Expresando los factores como series de potencias, tenemos

$$\frac{1}{(1-t)^{r+1}} = \sum_{n=0}^{\infty} \binom{n+r}{r} t^n, \qquad g(t) = \sum_{j=a}^{b} u_j t^j$$

Entonces, para todo $n \geq b$, el coeficiente correspondiente en la serie de Poincaré es

$$\lambda(M_n) = P_M(n) = \sum_{j=a}^{b} u_j \binom{n+r-j}{r}$$

Por simple inspección, P_M es un polinomio numérico de grado r. $\square$

Definición. El polinomio $P_M = [c_0; \dots; c_r]$ de la proposición anterior se denomina *polinomio de Hilbert* de M con respecto a λ. El coeficiente c_0 es el *grado* de M.

Corolario 3.9. *Sea $x \in R$ un elemento homogéneo que no es divisor de cero en M. Si M tiene dimensión positiva, entonces $N = M/xM$ tiene grado $\deg N = \deg M \cdot \deg x$.*

Prueba. Sea $d = \deg x$. Puesto que el polinomio de Hilbert es aditivo,

$$P_N(n) = P_M(n) - P_{M(-d)}(n) = [c_0; \ldots; c_r](n) - [c_0; \ldots; c_r](n-d) = [dc_0; \ldots](n)$$

Entonces N tiene grado $\deg N = dc_0 = \deg M \cdot \deg x$. □

3.5. Primos minimales

La referencia para esta sección es [Har77, pp. 50-51]. Todos los resultados de esta sección siguen siendo válidos si eliminamos las palabras "graduado" y "homogéneo" de las proposiciones y sus demostraciones. En particular, en [Eis95, pp. 91, 93] se demuestran análogos no graduados de las proposiciones 3.11 y 3.13.

Preliminares. Sean R un anillo graduado noetheriano y M un R-módulo graduado finitamente generado como en las secciones 3.2 y 3.4.

Definición. El *anulador* de M, denotado $\operatorname{Ann}(M)$, es el conjunto de elementos $x \in R$ tales que $xm = 0$ para todo $m \in M$. Si M es un módulo principal generado por $m \in M$, también podemos escribir $\operatorname{Ann}(m) = \operatorname{Ann}(M)$.

Observación. $\operatorname{Ann}(M)$ es un ideal homogéneo de R.

Definición. Un *primo homogéneo asociado* de M es un ideal primo homogéneo $\mathfrak{p} \subset R$ que es de la forma $\mathfrak{p} = \operatorname{Ann}(m)$ para algún elemento homogéneo $m \in M$.

Observación. El módulo trivial no tiene primos asociados, porque $\operatorname{Ann}(0) = R$.

Proposición 3.10. *Supongamos que la sucesión*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

es exacta. Entonces $\operatorname{Ann}(L) \cdot \operatorname{Ann}(N) \subset \operatorname{Ann}(M) \subset \operatorname{Ann}(L) \cap \operatorname{Ann}(N)$. Además, si $\mathfrak{q} \subset R$ es un ideal primo homogéneo, entonces $\mathfrak{q} \supset \operatorname{Ann}(M)$ si y sólo si $\mathfrak{q} \supset \operatorname{Ann}(L)$ o $\mathfrak{q} \supset \operatorname{Ann}(N)$.

Prueba. Puesto que $\operatorname{Ann}(N) \cdot N = 0$, entonces $\operatorname{Ann}(N) \cdot M \subset f(L)$. Puesto que $\operatorname{Ann}(L) \cdot L = 0$, entonces $\operatorname{Ann}(L) \cdot \operatorname{Ann}(N) \cdot M = 0$. Esto establece la cota inferior para $\operatorname{Ann}(M)$. Por el lema de evitación de primos, si $\mathfrak{q} \not\supset \operatorname{Ann}(L)$ y $\mathfrak{q} \not\supset \operatorname{Ann}(N)$, entonces $\mathfrak{q} \not\supset \operatorname{Ann}(L) \cdot \operatorname{Ann}(N)$ y, usando la transitividad de la inclusión, $\mathfrak{q} \not\supset \operatorname{Ann}(M)$.

Puesto que f es inyectiva, $\operatorname{Ann}(M) \cdot f(L) = 0$ implica que $\operatorname{Ann}(M) \cdot L = 0$. Puesto que g es sobreyectiva, $\operatorname{Ann}(M) \cdot g(M) = 0$ implica que $\operatorname{Ann}(M) \cdot N = 0$. Combinando los dos resultados, tenemos la cota superior para $\operatorname{Ann}(M)$. Usando la transitividad de la inclusión, cualquiera entre $\mathfrak{q} \supset \operatorname{Ann}(L)$ y $\mathfrak{q} \supset \operatorname{Ann}(N)$ implica $\mathfrak{q} \supset \operatorname{Ann}(M)$. □

Proposición 3.11. *Si M es no trivial, entonces tiene primos homogéneos asociados.*

Prueba. Consideremos la familia de ideales homogéneos que son de la forma $\mathrm{Ann}(m)$ para algún elemento homogéneo $m \in M$ distinto de cero. Si M es no trivial, esta familia es no vacía y tiene un elemento maximal $\mathrm{Ann}(m)$. Afirmamos que $\mathrm{Ann}(m)$ es un ideal primo homogéneo.

Sea $b \in R$ un elemento homogéneo tal que $b \notin \mathrm{Ann}(m)$. Puesto que $bm \neq 0$, $\mathrm{Ann}(bm)$ es un elemento de nuestra familia de anuladores. Puesto que $\mathrm{Ann}(m)$ es maximal, $\mathrm{Ann}(m) = \mathrm{Ann}(bm)$. Entonces $ab \in \mathrm{Ann}(m)$ implica $a \in \mathrm{Ann}(bm)$ implica $a \in \mathrm{Ann}(m)$. □

Proposición 3.12. *Sea $M^{(r)} \subset M$ un submódulo graduado propio. Entonces existe un submódulo graduado intermedio $M^{(r)} \subset M^{(r+1)} \subset M$ tal que $M^{(r+1)}/M^{(r)}$ es de la forma $(R/\mathfrak{p})(d)$.*

Prueba. Sea $\mathfrak{p} = \mathrm{Ann}(q)$ un primo homogéneo asociado de $Q^{(r)} = M/M^{(r)}$. Sea $Q^{(r+1)} \subset Q^{(r)}$ el submódulo generado por q. Sea $M^{(r+1)} \subset M$ la imagen inversa de $Q^{(r+1)}$. Entonces $M^{(r+1)}/M^{(r)}$ es isomorfo a $Q^{(r+1)}$ y este último es isomorfo a $R/\mathfrak{p}$ salvo torcimiento por el grado de q. □

Definición. Una *filtración limpia* de M es una filtración por submódulos graduados

$$0 = M^{(0)} \subset M^{(1)} \subset \cdots \subset M^{(r)} = M$$

tal que, para cada $i = 1 \dots r$, existe un ideal primo homogéneo $\mathfrak{p}_i \subset R$ tal que $Q^{(i)} = M^{(i)}/M^{(i-1)}$ es isomorfo a $R/\mathfrak{p}_i$ salvo torcimiento.

Observación. El término “filtración limpia” no es estándar, pero es mucho más conveniente decir “filtracion limpia” que incrustar la definición en el texto cada vez que la necesitemos.

Definición. Un *R-módulo limpio* es un R-módulo graduado que admite una filtración limpia.

Observación. En cambio, el término “módulo limpio” sí es estándar. Ver [Eis95, p. 93].

Proposición 3.13. *Todo R-módulo graduado finitamente generado M es limpio.*

Prueba. Puesto que M es un módulo noetheriano y la familia de submódulos limpios es no vacía (contiene al submódulo trivial), M tiene un submódulo limpio maximal $M^{(r)} \subset M$.

Por la proposición anterior, si $M^{(r)} \subset M$ fuese un submódulo propio, existiría otro submódulo más grande $M^{(r+1)} \subset M$ tal que $Q^{(r+1)} = M^{(r+1)}/M^{(r)}$ es de la forma $R/\mathfrak{p}$ salvo torcimiento. Esto es imposible, porque $M^{(r)}$ es maximal. Por ende, $M = M^{(r)}$ es limpio. □

Definición. Un *primo minimal* de M es un ideal primo $\mathfrak{p} \subset R$ minimal entre los que aparecen en una filtración limpia de M. La *multiplicidad* de M en un primo minimal $\mathfrak{p} \subset R$, denotada por $\mu_{\mathfrak{p}}(M)$, es la longitud de $M_{\mathfrak{p}}$ como $R_{\mathfrak{p}}$-módulo.

Observación. No está claro que el concepto de “primo minimal” está bien definido. En principio podría haber dos filtraciones limpias distintas de M que induzcan conjuntos distintos de primos minimales. Demostraremos que no es el caso.

Proposición 3.14. *Sea $\mathfrak{p} \subset R$ un primo minimal de M. Entonces $\mathfrak{p}$ aparece exactamente $\mu_{\mathfrak{p}}(M)$ veces en cualquier filtración limpia de M.*

Prueba. Ignorando la gradación, la localización en $\mathfrak{p}$ respeta las sucesiones exactas. Entonces la longitud de $M_{\mathfrak{p}}$ como $R_{\mathfrak{p}}$-módulo es $\ell(M_{\mathfrak{p}}) = \ell(Q_{\mathfrak{p}}^{(1)}) + \cdots + \ell(Q_{\mathfrak{p}}^{(r)})$. Por construcción, si $\mathfrak{p}_i = \mathfrak{p}$, entonces $Q_{\mathfrak{p}}^{(i)} = R(\mathfrak{p})$ es el cuerpo de fracciones de $R/\mathfrak{p}$ y tiene longitud $\ell(Q_{\mathfrak{p}}^{(i)}) = 1$. Puesto que $\mathfrak{p}$ es minimal, si $\mathfrak{p}_i \neq \mathfrak{p}$, entonces $Q_{\mathfrak{p}}^{(i)}$ es el módulo trivial y tiene longitud $\ell(Q_{\mathfrak{p}}^{(i)}) = 0$. $\square$

Capítulo 4

Anillos y módulos filtrados

Una manera de simplificar el estudio de una variedad algebraica es limitar nuestra atención a la *vecindad infinitesimal* de un punto. Esta vecindad infinitesimal no es realmente un subconjunto abierto de la variedad original, sino un objeto abstracto[1] que captura las propiedades geométricas de la variedad en el punto de interés.

Intuitivamente, uno podría pensar que la vecindad infinitesimal de $p \in V$ es representada por el anillo local $\mathscr{O}_p(V)$, pero esto no es el caso[2]. De hecho, es fácil ver que $\mathscr{O}_p(V)$ retiene demasiada información global sobre V: si $\mathscr{O}_p(V)$ y $\mathscr{O}_q(W)$ son isomorfos, entonces $k(V)$ y $k(W)$ también son isomorfos, por ende las variedades V y W son birracionalmente equivalentes.

Supongamos que U es una vecindad infinitesimal y $f : U \to k$ es una "función regular" sobre ella. La propiedad fundamental de f es el orden con que se anula en el único punto $p \in U$. No es necesario que f se pueda extender a una vecindad finita de U.

Para ver una vecindad infinitesimal, necesitamos un microscopio algebraico que magnifique la región cercana al punto de interés, en un sentido más preciso que el indicado por la topología de Zariski. En este capítulo construiremos el microscopio.

4.1. Definiciones básicas

Preliminares. Fijemos un anillo R y un ideal $\mathfrak{a} \subset R$.

Definición. Un *módulo $\mathfrak{a}$-filtrado* es un R-módulo M con una cadena de submódulos

$$M = M_0 \supset M_1 \supset M_2 \supset \dots$$

tal que $\mathfrak{a}M_n \subset M_{n+1}$ para todo $n \in \mathbb{N}$.

Ejemplo. La *$\mathfrak{a}$-filtración canónica* sobre el R-módulo M es $(M_n) = (\mathfrak{a}^n M)$.

[1] En la teoría de esquemas, una vecindad infinitesimal es un objeto geométrico por cuenta propia. Sin embargo, el estudio de los esquemas trasciende el alcance de este trabajo.

[2] El anillo local $\mathscr{O}_p(V)$ describe una vecindad genérica de Zariski de $p \in V$. Pero las vecindades de Zariski distan mucho de ser infinitesimales. En la geometría diferencial, donde los espacios son de Hausdorff y los puntos tienen vecindades arbitrariamente pequeñas, los anillos locales reflejan mejor la idea de vecindad infinitesimal.

Definición. Un *submódulo* $\mathfrak{a}$*-filtrado* de M es un R-submódulo $N \subset M$ con una $\mathfrak{a}$-filtración (N_n) tal que $N_n \subset M_n$ para todo $n \in \mathbb{N}$.

Ejemplo. La $\mathfrak{a}$*-filtración inducida* sobre el R-submódulo $N \subset M$ es $(N_n) = (N \cap M_n)$.

Definición. Un *homomorfismo* $\mathfrak{a}$*-filtrado* es un R-homomorfismo $\varphi : A \to B$ tal que $\varphi(A_n) \subset B_n$ para todo $n \in \mathbb{N}$.

Ejemplo. Sea $N \subset M$ un submódulo equipado con la $\mathfrak{a}$-filtración inducida. Entonces la inclusión de N en M es un homomorfismo $\mathfrak{a}$-filtrado.

Definición. Una $\mathfrak{a}$-filtración (M_n) es *estable* si $\mathfrak{a}M_n = M_{n+1}$ para todo $n \gg 0$.

Ejemplo. La $\mathfrak{a}$-filtración canónica es estable por construcción.

Definición. Dos $\mathfrak{a}$-filtraciones (M_n), (M'_n) de un mismo módulo son *equivalentes* si existe $r \in \mathbb{N}$ tal que $M_{n+r} \subset M'_n$ y $M'_{n+r} \subset M_n$ para todo $n \in \mathbb{N}$.

Observación. También podemos definir que (M_n), (M'_n) son equivalentes si existen $r, r' \in \mathbb{N}$ tales que $M_{n+r'} \subset M'_n$ y $M'_{n+r} \subset M_n$ para todo $n \in \mathbb{N}$.

Proposición 4.1. *Todas las* $\mathfrak{a}$*-filtraciones estables de* M *son equivalentes.*

Prueba. Sea $r \in \mathbb{N}$ el instante en que (M_n) se estabiliza. Entonces $M_{n+r} = \mathfrak{a}^n M_r \subset \mathfrak{a}^n M \subset M_n$ para todo $n \in \mathbb{N}$. Por ende, (M_n) es equivalente a la $\mathfrak{a}$-filtración canónica $(\mathfrak{a}^n M)$. $\square$

4.2. Lema de Artin-Rees

Las referencias para esta sección son [AM69, p. 107] y [Eis95, pp. 148-149].

Preliminares. Fijemos un anillo noetheriano R, un ideal $\mathfrak{a} \subset R$ y un R-módulo M finitamente generado equipado con una $\mathfrak{a}$-filtración.

Definición. El *álgebra de explosión*[3] de R es el anillo graduado

$$R^\star = R \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \oplus \mathfrak{a}^3 \oplus \dots$$

Definición. El *módulo de explosión* de M es el $R^\star$-módulo graduado

$$M^\star = M_0 \oplus M_1 \oplus M_2 \oplus \dots$$

Proposición 4.2. *El álgebra de explosión* $R^\star$ *es un anillo noetheriano.*

Prueba. Puesto que R es noetheriano, $\mathfrak{a} \subset R$ es finitamente generado. Por ende, $R^\star = R[\mathfrak{a}]$ es un álgebra finitamente generada. Por el teorema de la base de Hilbert, $R^\star$ es un anillo noetheriano. $\square$

[3]El anillo y módulo de explosión reciben este calificativo porque son utilizados en la resolución de singularidades mediante un proceso que se llama “explosión” de la singularidad.

Proposición 4.3. *La filtración* (M_n) *es estable si y sólo si* $M^\star$ *es finitamente generado.*

Prueba. Consideremos la sucesión de $R^\star$-submódulos

$$M_n^\star = M_0 \oplus \cdots \oplus M_n \oplus \mathfrak{a}M_n \oplus \mathfrak{a}^2 M_n \oplus \dots$$

Cada $M_n^\star$ es un $R^\star$-módulo finitamente generado por elementos de $M_0 \dots M_n$. Puesto que $R^\star$ es noetheriano, $M^\star$ es un $R^\star$-módulo finitamente generado si y sólo si $M^\star = M_n^\star$ para todo $n \gg 0$ si y sólo si la filtración (M_n) es estable. □

Corolario 4.4. *(Artin-Rees) Sea* $N \subset M$ *un submódulo. Si* (M_n) *es una* $\mathfrak{a}$*-filtración estable de* M*, entonces la* $\mathfrak{a}$*-filtración inducida sobre* N *es estable.*

Prueba. Por la proposición anterior, si (M_n) es estable, entonces $M^\star$ es noetheriano, por ende $N^\star$ es noetheriano, por ende (N_n) es estable. □

4.3. Anillos y módulos graduados asociados

Las referencias para esta sección son [AM69, pp. 111-112] y [Eis95, pp. 146-148].

Preliminares. Fijemos un anillo noetheriano R, un ideal $\mathfrak{a} \subset R$ y un R-módulo M finitamente generado equipado con una $\mathfrak{a}$-filtración estable.

Definición. El *anillo graduado asociado* de R es el anillo graduado

$$G(R) = \frac{R}{\mathfrak{a}} \oplus \frac{\mathfrak{a}}{\mathfrak{a}^2} \oplus \frac{\mathfrak{a}^2}{\mathfrak{a}^3} \oplus \frac{\mathfrak{a}^3}{\mathfrak{a}^4} \oplus \dots$$

Observación. Equivalentemente, podemos definir $G(R) = R^\star/\mathfrak{a}R^\star$.

Definición. El *módulo graduado asociado* de M es el $G(R)$-módulo graduado

$$G(M) = \frac{M_0}{M_1} \oplus \frac{M_1}{M_2} \oplus \frac{M_2}{M_3} \oplus \dots$$

Proposición 4.5. *El anillo graduado asociado* $G(R)$ *es noetheriano.*

Prueba. El anillo $G(R) = R^\star/\mathfrak{a}R^\star$ es noetheriano porque $R^\star$ es noetheriano. □

Proposición 4.6. *El módulo graduado asociado* $G(M)$ *es finitamente generado.*

Prueba. Sea $r \in \mathbb{N}$ el instante en que M_n se estabiliza. Para todo $n \geq r$, tenemos

$$\frac{\mathfrak{a}}{\mathfrak{a}^2} \frac{M_n}{M_{n+1}} = \frac{M_{n+1}}{M_{n+2}}$$

Por ende, $G(M)$ es generado por el prefijo

$$\tilde{M} = \frac{M_0}{M_1} \oplus \cdots \oplus \frac{M_r}{M_{r+1}}$$

Las partes homogéneas M_n/M_{n+1} son $R/\mathfrak{a}$-módulos finitamente generados, por ende $\tilde{M}$ es un $R/\mathfrak{a}$-módulo finitamente generado, por ende $G(M)$ es un $G(R)$-módulo finitamente generado. □

4.4. Polinomio característico

La referencia para esta sección es [AM69, pp. 118-120].

Preliminares. Sean R un anillo local noetheriano, $\mathfrak{m} \subset R$ su ideal maximal y $\mathfrak{q} \subset R$ un ideal de parámetros. Sea M un R-módulo finitamente generado con una $\mathfrak{q}$-filtración estable.

Proposición 4.7. *Los cocientes M/M_n tienen longitud finita.*

Prueba. Puesto que $\mathfrak{q}$ es $\mathfrak{m}$-primario, $R/\mathfrak{q}$ es un anillo local artiniano. Entonces cada M_n/M_{n+1} tiene longitud finita. Por aditividad, cada M/M_n también tiene longitud finita. $\square$

Proposición 4.8. *Existe un polinomio $\chi^M \in \mathbb{Q}[n]$ tal que $\ell(M/M_n) = \chi^M(n)$ para todo $n \gg 0$. Además, si $x_1 \dots x_s$ generan a $\mathfrak{q}$, entonces $\deg \chi^M \leq s$.*

Prueba. Por construcción, $G(R)$ es el $R/\mathfrak{q}$-álgebra generado por las clases de $x_1 \dots x_s$ módulo $\mathfrak{q}^2$. Cada clase $\bar{x}_i$ tiene grado $\deg \bar{x}_i = 1$. Por ende, $G(M)$ tiene un polinomio de Hilbert $P_M \in \mathbb{Q}[n]$ con respecto a ℓ. Sea $r \in \mathbb{N}$ el instante a partir del cual $\ell(M_n/M_{n+1}) = P_M(n)$. Entonces,

$$\chi^M(n) = \ell(M/M_r) + P_M(r) + \dots + P_M(n-1)$$

Por construcción, $\deg P_M < s$. Entonces, $\deg \chi^M = \deg P_M + 1 \leq s$. $\square$

Definición. El polinomio χ^M de la proposición anterior se llama *polinomio característico* de M con respecto a la filtración (M_n).

Definición. El *polinomio de Hilbert-Samuel* de M respecto a $\mathfrak{q}$, denotado $\chi_{\mathfrak{q}}^M$, es el polinomio característico de M con respecto a la $\mathfrak{q}$-filtración canónica.

Proposición 4.9. *El grado y el coeficiente líder de χ^M sólo dependen de M y $\mathfrak{q}$, no de (M_n).*

Prueba. Sea $r \in \mathbb{N}$ el instante en que (M_n) se estabiliza. Entonces $\chi^M(n+r) \geq \chi_{\mathfrak{q}}^M(n) \geq \chi^M(n)$ para todo $n \gg 0$. Por ende, χ_M tiene el mismo grado y coeficiente líder que $\chi_{\mathfrak{q}}^M$. $\square$

Proposición 4.10. *El grado de χ^M sólo depende de M, no de $\mathfrak{q}$.*

Prueba. Puesto que $\mathfrak{q}$ es $\mathfrak{m}$-primario, existe $r \in \mathbb{N}$ tal que $\mathfrak{m} \supset \mathfrak{q} \supset \mathfrak{m}^r$. Entonces $\mathfrak{m}^n \supset \mathfrak{q}^n \supset \mathfrak{m}^{rn}$. Por ende, $\chi_{\mathfrak{m}}^M(n) \leq \chi_{\mathfrak{q}}^M(n) \leq \chi_{\mathfrak{m}}^M(rn)$. Por ende, $\chi_{\mathfrak{q}}^M$ tiene el mismo grado que $\chi_{\mathfrak{m}}^M$. $\square$

Definición. La *dimensión* de M es la dimensión de $G(M)$, i.e., el grado de χ^M.

Definición. La *multiplicidad* de M sobre $\mathfrak{q}$ es el grado de $G(M)$.

Corolario 4.11. *Supongamos que $s \in \mathbb{N}$ es el menor número de elementos que generan un ideal $\mathfrak{m}$-primario. Entonces M tiene dimensión $\dim M \leq s$.*

Prueba. Es consecuencia inmediata de las tres proposiciones anteriores. $\square$

Proposición 4.12. *Sea $x \in R$ un elemento que no es divisor de cero en M. Si M tiene dimensión no negativa, entonces $N = M/xM$ tiene dimensión* $\dim N < \dim M$.

Prueba. Equipemos a M, N con las filtraciones canónicas y a $L = xM$ con la filtración inducida por la inclusión en M. Entonces tenemos la sucesión exacta filtrada

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

Puesto que x no es divisor de cero, L es isomorfo a M como R-módulo. Además, por el lema de Artin-Rees, la $\mathfrak{q}$-filtración de L es estable. Entonces L, M tienen filtraciones equivalentes. Por ende, χ^L tiene el mismo grado y coeficiente líder que χ^M. Entonces,

$$\chi^N = \chi^M - \chi^L = [c_0; c_1; \ldots; c_r] - [c_0; c_1'; \ldots; c_r']$$

Los términos líderes de χ^L, χ^M se anulan mutuamente. Por ende, $\deg \chi^N < \deg \chi^M$. □

4.5. Completación

En esta sección discutiremos de manera informal la completación de un anillo local, enfatizando la intuición geométrica antes que el formalismo algebraico. El lector puede consultar los detalles técnicos en [AM69, pp. 100-123] y [Har77, pp. 33-35, 207-216].

Dado un anillo local $R = \mathscr{O}_p(V)$, las potencias $\mathfrak{m}^n \subset R$ del ideal maximal están conformadas por las funciones racionales $f : V \to k$ que se anulan en p con orden por lo menos n. Entonces el anillo cociente $R/\mathfrak{m}^n$ contiene la información infinitesimal de R de orden menor que n.

Consideremos el sistema inverso de anillos

$$\cdots \longrightarrow \frac{R}{\mathfrak{m}^{n+1}} \longrightarrow \frac{R}{\mathfrak{m}^n} \longrightarrow \frac{R}{\mathfrak{m}^{n-1}} \longrightarrow \cdots \longrightarrow \frac{R}{\mathfrak{m}^2} \longrightarrow \frac{R}{\mathfrak{m}} \longrightarrow 0$$

Los morfismos de este diagrama describen la pérdida de información geométrica al cocientar por una potencia cada vez menor de $\mathfrak{m}$. En particular,

- Cuando $n = 0$, hemos perdido toda la información, incluida la finita (i.e., de orden 0). Por ende, sólo nos queda el anillo trivial $R/\mathfrak{m}^0 = 0$, que describe al conjunto vacío.
- Cuando $n = 1$, hemos perdido la información infinitesimal. Por ende, el cuerpo de residuos $k = R/\mathfrak{m}$ describe al punto p, extraído limpiamente de la variedad V.
- Cuando $n = 2$, hemos perdido la información infinitesimal de orden 2 y superior. Por ende, el ideal maximal $T_p^\star V = \mathfrak{m}/\mathfrak{m}^2$ es el *espacio cotangente de Zariski* de $p \in V$.
- Cuando $n \to \infty$, el límite inverso del sistema de anillos retiene la información infinitesimal de R de todos los órdenes. Este límite inverso es llamado la *completación* de R y se denota por $\widehat{R}$. El objeto geométrico descrito por $\widehat{R}$ es la *vecindad infinitesimal* U de $p \in V$.

Bajo condiciones razonables [AM69, p. 110], el homomorfismo de anillos inducido $\varphi : R \to \widehat{R}$ es inyectivo. Sin embargo, en general, φ no es sobreyectivo. Geométricamente, esto significa que no toda "función regular" $f : U \to k$ puede ser extendida a una vecindad finita de U.

Capítulo 5

Teorema de la dimensión

En los dos capítulos anteriores, hemos definido la dimensión de un módulo en un contexto global (proyectivo, graduado) y en un contexto local (filtrado). La ventaja técnica de estas definiciones es que están basadas en el polinomio de Hilbert. Esto nos permite estudiar módulos complicados relacionándolos con otros módulos más simples mediante sucesiones exactas.

Sin embargo, desde un punto de vista geométrico, el concepto de dimensión de un módulo no es muy convincente, ya que es a todas luces un despropósito llamar "dimensión" a una propiedad puramente algebraica de un objeto puramente algebraico. Para superar esta dificultad, daremos una interpretacion geométrica intuitiva para los módulos que nos interesan.

Sea R el anillo de coordenadas de una variedad afín $Y \subset \mathbb{A}^n$. Los R-módulos no triviales más sencillos son de la forma $R/\mathfrak{p}$, donde $\mathfrak{p} \subset R$ es un ideal primo. Visualmente, $R/\mathfrak{p}$ es una muralla construida sobre $V(\mathfrak{p})$. El resto de Y es terreno vacío sin construir. En particular, si $\mathfrak{m} \subset R$ es el ideal maximal de un punto $p \in V$, decimos que $R/\mathfrak{m}$ es un *haz rascacielo* sobre p.

Más generalmente, sea M un R-módulo finitamente generado y sean $\mathfrak{p}_1 \dots \mathfrak{p}_r \subset R$ los ideales primos que aparecen en las filtraciones limpias de M. Visualmente, M es la superposición[1] de las murallas $R/\mathfrak{p}_i$. Esta clase de objetos se conocen como *haces coherentes* sobre la variedad Y.

Para cada ideal primo $\mathfrak{p} \subset R$, el *tallo* $M_\mathfrak{p}$ describe el comportamiento de M en una vecindad genérica de $V(\mathfrak{p})$. Los *fibrados vectoriales* corresponden de manera natural a los haces coherentes tales que cada tallo $M_\mathfrak{p}$ es un $R_\mathfrak{p}$-módulo libre. (Ver [GW10, p. 291].)

Definición. El *soporte* de M, denotado $S(M)$, es el conjunto algebraico conformado por todos los puntos $p \in Y$ tales que el tallo $M_\mathfrak{m}$ sobre el ideal maximal $\mathfrak{m} = I(p)$ es no trivial.

De manera análoga al caso afín, si R es el anillo de coordenadas homogéneo de una variedad proyectiva $Y \subset \mathbb{P}^n$, los R-módulos graduados finitamente generados se pueden interpretar como haces coherentes sobre Y. En este caso...

Definición. El *soporte* de M, denotado $S(M)$, es el conjunto algebraico conformado por todos los puntos $p \in Y$ tales que el tallo $M_\mathfrak{p}$ sobre el ideal primo homogéneo $\mathfrak{p} = I(p)$ es no trivial.

[1] En el sentido del "principio de superposición" del álgebra lineal.

En este capítulo, demostraremos que la dimensión de M definida algebraicamente no es otra cosa que la dimensión de su soporte definida geométricamente.

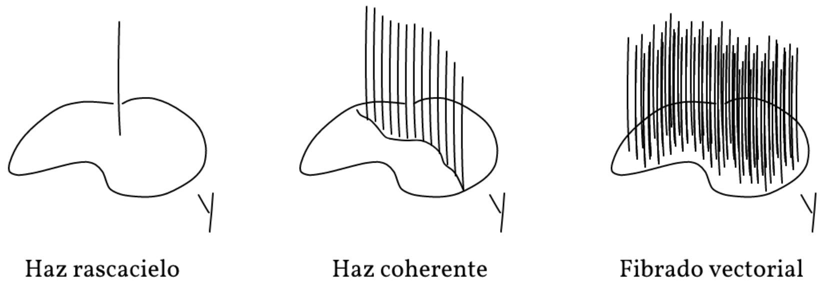

Figura 5.1: Ejemplos de haces

5.1. Definiciones básicas

Preliminares. Sean R un anillo noetheriano y M un R-módulo finitamente generado.

Definición. Una *cadena de primos* en R es una lista finita y estrictamente ascendente

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

de ideales primos de R. Decimos que esta cadena tiene *longitud* n y *termina* en $\mathfrak{p}_n$.

Definición. La *altura* de un ideal primo $\mathfrak{p} \subset R$, denotada $h(\mathfrak{p})$, es el supremo de las longitudes de las cadenas de primos que terminan en $\mathfrak{p}$.

Definición. La *altura* de un ideal propio $\mathfrak{a} \subset R$, denotada $h(\mathfrak{a})$, es la altura mínima de cualquier ideal primo intermedio $\mathfrak{a} \subset \mathfrak{p} \subset R$.

Observación. En particular, si $R = k[Y]$, entonces $h(\mathfrak{a}) = \operatorname{codim} V(\mathfrak{a})$.

Definición. La *dimensión de Krull* de R es el supremo de las alturas de sus ideales propios.

Observación. En particular, si $R = k[Y]$, entonces $\dim R = \dim Y$.

Definición. La *dimensión de Krull* de M es la dimensión de Krull de $R/\operatorname{Ann}(M)$.

Observación. En particular, si $R = k[Y]$, entonces $\dim M = \dim S(M)$.

5.2. Dimensión local

La referencia para esta sección es [AM69, pp. 120-121].

Preliminares. Sean R un anillo local noetheriano y $\mathfrak{m} \subset R$ su ideal maximal.

Notación. Si S es un R-álgebra finitamente generada como R-módulo, denotaremos por $d(S)$ la dimensión de S como R-módulo y denotaremos por $\dim S$ la dimensión de Krull de S.

Proposición 5.1. *Sean $\mathfrak{p} \subset R$ un ideal primo y $x \in R$ un elemento tal que $x \notin \mathfrak{p}$. Sea $\mathfrak{a} \subset R$ el ideal generado por $\mathfrak{p}$ y x. Entonces $d(R/\mathfrak{a}) < d(R)$.*

Prueba. Sean $S = R/\mathfrak{p}$ y $\mathfrak{n} \subset S$ su ideal maximal. Puesto que x no es divisor de cero en S, por la proposición 4.12, $d(R/\mathfrak{a}) < d(S)$. Por otro lado, el homomorfismo cociente $\pi : R \to S$ induce para todo $n \in \mathbb{N}$ un homomorfismo cociente $\pi_n : R/\mathfrak{m}^n \to S/\mathfrak{n}^n$. Entonces $\ell(S/\mathfrak{n}^n) \leq \ell(R/\mathfrak{m}^n)$. Por ende, $d(R/\mathfrak{a}) < d(S) \leq d(R)$. □

Proposición 5.2. $\dim R \leq d(R)$.

Prueba. Por inducción en $d(R)$. Si $d(R) = 0$, entonces χ^R es constante, por ende $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ para todo $n \gg 0$. Por el lema de Nakayama, $\mathfrak{m}^n = 0$ para todo $n \gg 0$. Por ende, $\dim R = 0$.

Supongamos ahora que R contiene una cadena de primos $\mathfrak{p} \subset \mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_r$. Tomemos $x \in \mathfrak{p}_0$ tal que $x \notin \mathfrak{p}$ y sea $\mathfrak{a} \subset R$ el ideal generado por $\mathfrak{p}$ y x. Entonces $\mathfrak{p}_i/\mathfrak{a}$ es una cadena de primos de longitud r en $S = R/\mathfrak{a}$. Por la proposición anterior, $d(S) < d(R)$. Usando la hipótesis inductiva, tenemos $r \leq \dim S \leq d(S) < \dim R$. Por ende, $r + 1 \leq d(R)$. Generalizando, $\dim R \leq d(R)$. □

Corolario 5.3. *La dimensión de Krull de R es finita.* □

Corolario 5.4. *Todo ideal propio $\mathfrak{a} \subset R$ tiene altura finita.* □

Proposición 5.5. *Sea $\mathfrak{a} \subset R$ un ideal propio que no es $\mathfrak{m}$-primario. Entonces existe un elemento no invertible $x \in \mathfrak{m}$ tal que $\mathfrak{b} = \langle \mathfrak{a}, x \rangle$ tiene mayor altura que $\mathfrak{a}$.*

Prueba. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \supset \mathfrak{a}$ los primos minimales de altura $h(\mathfrak{p}_i) = h(\mathfrak{a})$. Puesto que $\mathfrak{p}_i \neq \mathfrak{m}$ para todo i, existe algún $x \in \mathfrak{m}$ tal que $x \notin \mathfrak{p}_i$ para todo i.

Para validar nuestra elección, tomemos ideales primos $\mathfrak{p} \subset \mathfrak{q} \subset R$ tales que $\mathfrak{a} \subset \mathfrak{p}$ y $\mathfrak{b} \subset \mathfrak{q}$. Por construcción, si $\mathfrak{p} = \mathfrak{p}_i$ para algún i, entonces la inclusión $\mathfrak{p} \subset \mathfrak{q}$ es propia. Entonces $h(\mathfrak{q}) > h(\mathfrak{a})$. Generalizando, $h(\mathfrak{b}) > h(\mathfrak{a})$. □

Proposición 5.6. $d(R) \leq \dim R$.

Prueba. Usando la proposición anterior $d = d(R)$ veces, consigamos elementos $x_1, \ldots, x_d \in \mathfrak{m}$ que generan un ideal $\mathfrak{a} \subset R$ de altura $h(\mathfrak{a}) \geq d \geq \dim R$. Entonces $\mathfrak{a}$ es $\mathfrak{m}$-primario. □

Teorema 5.7. *(Teorema de la dimensión local) Las siguientes cantidades son iguales:*

- *La longitud máxima de una cadena de primos en R.*
- *El grado del polinomio característico χ^M.*
- *El menor número de generadores de un ideal $\mathfrak{m}$-primario.*

Prueba. Es consecuencia directa de las proposiciones 5.2 y 5.6. □

5.3. Dimensión global

Las referencias para esta sección son [AM69, pp. 121-125] y [Har77, pp. 47-49, 51-52]

Proposición 5.8. *(Teorema de la altura de Krull) Sean R un anillo noetheriano, $\mathfrak{a} \subset R$ un ideal y $x_1 \dots x_s$ generadores de $\mathfrak{a}$. Entonces todo primo minimal $\mathfrak{p} \supset \mathfrak{a}$ tiene altura $h(\mathfrak{p}) \leq s$.*

Prueba. Localicemos en un primo minimal $\mathfrak{p} \supset \mathfrak{a}$. Entonces los elementos dados $x_1 \dots x_s$ generan el ideal de parámetros $\mathfrak{a}_\mathfrak{p} \subset R_\mathfrak{p}$. Por ende, $h(\mathfrak{p}) = \dim R_\mathfrak{p} \leq s$. □

Proposición 5.9. *(Teorema de la dimensión afín) Sean $Y, Z \subset \mathbb{A}^n$ dos variedades afines de codimensión $r, s \in \mathbb{N}$. Entonces las componentes irreducibles de $Y \cap Z$ tienen codimensión $\leq r + s$.*

Prueba. Supongamos que $Z = V(f)$ es una hipersuperficie afín. En este caso, cada componente irreducible de $Y \cap Z$ corresponde a un primo minimal de $\langle f \rangle \subset k[Y]$. Sea $\mathfrak{p} \subset k[Y]$ uno de estos primos minimales. Por el teorema de Krull, $\operatorname{codim} V(\mathfrak{p}) = \operatorname{codim} Y + h(\mathfrak{p}) \geq r + s$.

Pasemos al caso general. Sea $\mathbb{A}^{2n} = \mathbb{A}^n \times \mathbb{A}^n$ y sea $X' \subset \mathbb{A}^{2n}$ la intersección de $X'' = Y \times Z$ con los hiperplanos $y_j = z_j$. Usando el caso anterior n veces, $\operatorname{codim} X' \leq \operatorname{codim} X'' + n = r + s + n$. Por construcción, X, X' son isomorfos. Entonces $\operatorname{codim} X = \operatorname{codim} X' - n \leq r + s$. □

Teorema 5.10. *(Teorema de la dimensión proyectiva) Sean $Y, Z \subset \mathbb{P}^n$ variedades proyectivas de codimensión $r, s \in \mathbb{N}$. Entonces las componentes irreducibles de $Y \cap Z$ tienen codimensión $\leq r + s$. Además, si $r + s \leq n$, entonces $Y \cap Z$ es no vacío.*

Prueba. La codimensión de un conjunto algebraico proyectivo $V \subset \mathbb{P}^n$ es igual a la codimensión del cono afín $V' \subset \mathbb{A}^{n+1}$ sobre V. Si $W \subset \mathbb{P}^n$ es una componente irreducible de $Y \cap Z$, entonces, por el teorema de la dimensión afín, $\operatorname{codim} W = \operatorname{codim} W' \leq r + s$.

Por otra parte, el cono afín X' sobre $X = Y \cap Z$ nunca es vacío, ya que siempre contiene al origen. Si $r + s \leq n$, entonces $\operatorname{codim} X = \operatorname{codim} X' \leq n$. Por ende, X es no vacío. □

Proposición 5.11. *Sea $R = k[x_0 \dots x_n]$ el anillo de coordenadas homogéneo de $\mathbb{P}^n$ y sea M un R-módulo graduado finitamente generado. Entonces $\dim M = \dim S(M)$.*

Prueba. En vista de los resultados de la sección 3.5, podemos asumir sin pérdida de generalidad que $M = R/\mathfrak{p}$ para algún ideal primo homogéneo $\mathfrak{p} \subset R$. Notemos que torcer M no tiene ningún efecto sobre su dimensión algebraica, $\dim M$, o geométrica, $\dim S(M)$.

Si $\mathfrak{p} = \mathfrak{m}$ es el ideal irrelevante, entonces, algebraicamente, $\dim M = \deg P_M = \deg 0 = -1$, y geométricamente, $\dim S(M) = \dim \varnothing = -1$.

Si $\mathfrak{p} \neq \mathfrak{m}$, entonces existe algún elemento homogéneo $x \notin \mathfrak{p}$ de grado 1. Algebraicamente, por el corolario 3.4, $N = M/xM$ tiene dimensión $\dim N = \dim M - 1$. Geométricamente, $S(N)$ es la intersección de $S(M)$ con el hiperplano transversal $x = 0$. Luego, por el teorema de la dimensión proyectiva, $\dim S(N) \geq \dim S(M) - 1$.

Topológicamente, $\dim S(N) = \dim S(M)$ es imposible, pues $S(N)$ es un subconjunto cerrado propio de $S(M)$ y este último es irreducible. Entonces, $\dim S(N) = \dim S(M) - 1$. Por inducción en la dimensión, $\dim N = \dim S(N)$. Por ende, $\dim M = \dim S(M)$. □

Capítulo 6

Teorema de Bézout

En los tres capítulos anteriores, so pretexto de lograr objetivos geométricos, hemos arrastrado al lector a lo largo de una excursión por el álgebra conmutativa. Ha llegado el momento de regresar a la geometría y cumplir nuestro objetivo original: generalizar el teorema de Bézout.

6.1. Definiciones básicas

La referencia para esta sección es [Har77, p. 52].

Preliminares. En este capítulo, $R = k[x_0 \dots x_n]$ es el anillo de coordenadas homogéneo de $\mathbb{P}^n$.

Notación. En este capítulo, denotaremos el ideal de $Y \subset \mathbb{P}^n$ por I_Y, en vez de $I(Y)$.

Definición. El *polinomio de Hilbert* de $Y \subset \mathbb{P}^n$, denotado $P_Y \in \mathbb{Q}[n]$, es el polinomio de Hilbert de su anillo de coordenadas homogéneo $R_Y = R/I_Y$ con respecto a la función $\lambda = \dim_k$.

Observación. Por construcción, $\dim Y = \dim R_Y$.

Definición. El *grado* de $Y \subset \mathbb{P}^n$ es el grado de R_Y como R-módulo.

Observación. El grado de $Y \subset \mathbb{P}^n$ no es una propiedad de Y como variedad abstracta, sino de un encaje $\iota : Y \to \mathbb{P}^n$. Por ejemplo, una recta proyectiva $L \subset \mathbb{P}^2$ y una cónica proyectiva $C \subset \mathbb{P}^2$ son isomorfas como variedades abstractas, pero $\deg L = 1$, mientras que $\deg C = 2$.

Ejemplo. Toda variedad no vacía $Y \subset \mathbb{P}^n$ tiene grado positivo.

Ejemplo. El espacio proyectivo $\mathbb{P}^n$ tiene grado $\deg \mathbb{P}^n = \deg R = 1$.

Observación. Por el argumento de estrellas y barras, $P_R = [1; 0; \dots ; 0]$.

Ejemplo. Sean $H \subset \mathbb{P}^n$ una hipersuperficie y $f \in R$ un generador de $I_H \subset R$. Entonces H tiene grado $\deg H = \deg f$.

Observación. Por el corolario 3.9, $\deg H = \deg R_H = \deg (R/fR) = \deg R \cdot \deg f = \deg f$.

6.2. Primer intento

La referencia para esta sección es [Har77, pp. 53-54].

Preliminares. Sea $Y \subset \mathbb{P}^n$ una variedad proyectiva de dimensión $\dim Y > 0$. Sea $H \subset \mathbb{P}^n$ una hipersuperficie que no contiene a Y. Sean $Z_1 \dots Z_s \subset \mathbb{P}^n$ las componentes irreducibles de $Y \cap H$ y sean $\mathfrak{p}_1 \dots \mathfrak{p}_s \subset R$ los ideales de $Z_1 \dots Z_s$, respectivamente.

Definición. El *anillo de la intersección* $Y \cap H$ es $M = R/(I_Y + I_H)$.

Observación. El soporte de M siempre es $S(M) = Y \cap H$. En particular, $\mathfrak{p}_1 \dots \mathfrak{p}_s$ son los primos minimales de M. Sin embargo, M no es siempre el anillo de coordenadas homogéneo de $Y \cap H$.

Definición. La *multiplicidad* de $Y \cap H$ sobre Z_j es la longitud de $M_{\mathfrak{p}_j}$ como $R_{\mathfrak{p}_j}$-módulo.

Observación. Entonces, los primos minimales de M, contados con multiplicidad, corresponden a las componentes irreducibles de $Y \cap H$, contadas con multiplicidad.

Teorema 6.1. *(Generalización del teorema de Bézout) Sea $Y \subset \mathbb{P}^n$ una variedad proyectiva de dimensión $\dim Y > 0$. Sea $H \subset \mathbb{P}^n$ una hipersuperficie que no contiene a Y. Sean $Z_1 \dots Z_s \subset \mathbb{P}^n$ las componentes irreducibles de $Y \cap H$. Entonces,*

$$\mu_1 \cdot \deg Z_1 + \cdots + \mu_s \cdot \deg Z_s = \deg Y \cdot \deg H$$

donde μ_j es la multiplicidad de $Y \cap H$ sobre Z_j

Prueba. Sea $f \in R$ un generador de I_H. Entonces f no es divisor de cero en $R_Y = R/I_Y$. Por los corolarios 3.4 y 3.9, el anillo M tiene dimensión $d = \dim M = \dim Y - 1$ y grado

$$\deg M = \deg \frac{R}{I_Y + I_H} = \deg \frac{R_Y}{f R_Y} = \deg Y \cdot \deg H$$

Por la proposición 3.13, M admite una filtración limpia

$$0 = M^{(0)} \subset M^{(1)} \subset \cdots \subset M^{(r)} = M$$

Escribamos el polinomio de Hilbert de $Q^{(i)} = M^{(i)}/M^{(i-1)}$ como $[c_0^{(i)}; \dots; c_d^{(i)}]$. Puesto que el polinomio de Hilbert es aditivo, M tiene grado $\deg M = c_0^{(1)} + \cdots + c_0^{(r)}$.

Por el teorema de la dimensión proyectiva, todas las las componentes irreducibles Z_j tienen dimensión $d = \dim Z_j = \dim R/\mathfrak{p}_j$. Entonces $c_i^{(0)} \neq 0$ si y sólo si $Q^{(i)}$ es una copia torcida de uno de los cocientes $R/\mathfrak{p}_j$, en cuyo caso $c_0^{(i)} = \deg Q^{(i)} = \deg R/\mathfrak{p}_j = \deg Z_j$.

Finalmente, por la proposición 3.14, el número de copias torcidas de $R/\mathfrak{p}_j$ entre los cocientes de la filtración es precisamente la multiplicidad de Z sobre Z_j. Entonces

$$\deg M = \mu_1 \cdot \deg Z_1 + \cdots + \mu_s \cdot \deg Z_s$$

Comparando con la primera expresión para $\deg M$, tenemos el resultado buscado. □

Corolario 6.2. *(Bézout) Sean $F, G \subset \mathbb{P}^2$ dos curvas proyectivas planas que no tienen componentes irreducibles en común. Sean $p_1 \dots p_s \in \mathbb{P}^2$ los puntos de $F \cap G$. Entonces,*

$$\mu_1 + \cdots + \mu_s = \deg F \cdot \deg G$$

donde μ_j es la multiplicidad de $F \cap G$ sobre p_j.

Prueba. En el teorema anterior, pongamos $Y = F$, $H = G$, $Z_j = p_j$, $\deg Z_j = \deg p_j = 1$. □

6.3. Segundo intento

Preliminares. Sean $H_1 \dots H_n \subset \mathbb{P}^n$ hipersuperficies proyectivas. Sean $f_1 \dots f_n \in R$ generadores de $I_1 \dots I_n \subset R$, los ideales de $H_1 \dots H_n$, respectivamente. Supongamos que ninguna componente irreducible de la intersección parcial $Z_r = H_1 \cap \cdots \cap H_r$ está contenida en H_{r+1}, de modo que la intersección total $Z = Z_n$ está conformada por una cantidad finita de puntos $p_1 \dots p_s \in \mathbb{P}^n$. Sean $\mathfrak{p}_1 \dots \mathfrak{p}_n \subset R$ los ideales de $p_1 \dots p_s$, respectivamente.

Definición. El *anillo de la intersección parcial $Z_r = H_1 \cap \cdots \cap H_r$* es $M_r = R/(I_1 + \cdots + I_r)$.

Definición. El *anillo de la intersección total $Z = Z_n$* es $M = M_n$.

Observación. Al igual que en el caso anterior, el soporte de M_r siempre es $S(M_r) = Z_r$, pero M_r no es necesariamente el anillo de coordenadas homogéneo de Z_r.

Definición. La *multiplicidad* de Z sobre p_j es la longitud de $M_{\mathfrak{p}_j}$ como $R_{\mathfrak{p}_j}$-módulo.

Observación. Utilizaremos sin demostración la siguiente proposición.

Proposición 6.3. *Si $\dim M_{r+1} = \dim M_r - 1$, entonces f_{r+1} no es divisor de cero en M_r.*

Prueba. Es un análogo graduado de [Stacks, Tag 00N6]. □

Teorema 6.4. *Sean $H_1 \dots H_n \subset \mathbb{P}^n$ hipersuperficies. Supongamos que ninguna H_{r+1} contiene a ninguna componente irreducible de la intersección parcial $H_1 \cap \cdots \cap H_r$. Sean $p_1 \dots p_s \in \mathbb{P}^n$ los puntos de la intersección total $H_1 \cap \cdots \cap H_n$. Entonces,*

$$\mu_1 + \cdots + \mu_s = \deg H_1 \cdots \deg H_n$$

donde μ_j es la multiplicidad de $H_1 \cap \cdots \cap H_r$ sobre p_j.

Prueba. Por el corolario 3.9, cada anillo M_{r+1} tiene grado

$$\deg M_{r+1} = \deg \frac{M_r}{f_{r+1} M_r} = \deg M_r \cdot \deg H_{r+1}$$

Entonces M tiene grado $\deg M = \deg H_1 \cdots \deg H_n$. Por otro lado, los únicos ideales primos relevantes que aparecen en las filtraciones limpias de M son los ideales de $p_1 \dots p_s$. Entonces M tiene grado $\deg M = \mu_1 + \cdots + \mu_s$. □

6.4. Automorfismos de $\mathbb{P}^n$

La referencia para esta sección es [Har95, pp. 228-229].

Preliminares. Lo prometido es deuda. Calcularemos el grupo de automorfismos de $\mathbb{P}^n$.

Proposición 6.5. *Toda variedad proyectiva $Y \subset \mathbb{P}^n$ de grado $\deg Y = 1$ es una variedad lineal.*

Prueba. Si $\dim Y = 0$, entonces no hay nada que demostrar. Si $\dim Y > 0$, entonces tomemos un hiperplano $H \subset \mathbb{P}^n$ transversal a Y. Entonces el esquema proyectivo $Z = Y \cap H$ tiene dimensión $\dim Z = \dim Y - 1$ y grado $\deg Z = 1$. Por inducción en la dimensión, asumamos que $Z \subset \mathbb{P}^n$ es una variedad lineal.

Tomemos cualquier punto $p \in Y$ tal que $p \notin Z$. Por el teorema 6.1, Y está contenida en todos los hiperplanos de $\mathbb{P}^n$ que pasan por Z y por p. Entonces Y está contenida en la intersección de dichos hiperplanos, que es la única variedad lineal $L \subset \mathbb{P}^n$ de dimensión $\dim L = \dim Y$ que pasa por Z y por p. Puesto que L es irreducible, $Y = L$. □

Observación. El caso $\dim Y = n$ está contemplado en esta demostración. La intersección de cero hiperplanos de $\mathbb{P}^n$ es todo el espacio $\mathbb{P}^n$.

Proposición 6.6. *Todo automorfismo $\varphi : \mathbb{P}^n \to \mathbb{P}^n$ envía hiperplanos a hiperplanos.*

Prueba. Por el teorema 6.4, n hiperplanos $H_i \subset \mathbb{P}^n$ en posición general se intersecan en un único punto $p \in \mathbb{P}^n$ de multiplicidad 1. Entonces las hipersuperficies $\varphi(H_i)$ también se intersecan en el único punto $\varphi(p)$ de multiplicidad 1. Por ende, cada $\varphi(H_i)$ es una hipersuperficie de grado 1, i.e., un hiperplano de $\mathbb{P}^n$. □

Teorema 6.7. *El grupo de automorfismos de $\mathbb{P}^n$ es $\mathrm{Aut}(\mathbb{P}^n) = \mathrm{GL}(\mathbb{A}^{n+1})/k^\star$.*

Prueba. Sea $\varphi : \mathbb{P}^n \to \mathbb{P}^n$ un automorfismo. Mediante un cambio de coordenadas lineal, podemos asumir que φ fija un hiperplano $H \subset \mathbb{P}^n$. Entonces φ también fija el complemento de H, que es isomorfo al espacio afín $\mathbb{A}^n$. Más aún, φ envía rectas a rectas en esta copia de $\mathbb{A}^n$. Entonces φ es una transformación lineal afín de $\mathbb{A}^n$, que se levanta a un automorfismo lineal $\tilde{\varphi} \in \mathrm{GL}(\mathbb{A}^{n+1})$ y vuelve a descender sobre $\mathbb{P}^n$ como $\varphi \in \mathrm{GL}(\mathbb{A}^{n+1})/k^\star$. □

Bibliografía

[AM69] M. F. Atiyah e I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969, págs. ix+128.

[Eis95] David Eisenbud. *Commutative algebra*. Vol. 150. Graduate Texts in Mathematics. With a view toward algebraic geometry. Springer-Verlag, New York, 1995, págs. xvi+785. ISBN: 0-387-94268-8; 0-387-94269-6. DOI: `10.1007/978-1-4612-5350-1`. URL: `https://doi-org.ezproxybib.pucp.edu.pe/10.1007/978-1-4612-5350-1`.

[Ful89] William Fulton. *Algebraic curves*. Advanced Book Classics. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989, págs. xxii+226. ISBN: 0-201-51010-3.

[GW10] Ulrich Görtz y Torsten Wedhorn. *Algebraic geometry I*. Advanced Lectures in Mathematics. Schemes with examples and exercises. Vieweg + Teubner, Wiesbaden, 2010, págs. viii+615. ISBN: 978-3-8348-0676-5. DOI: `10.1007/978-3-8348-9722-0`. URL: `https://doi-org.ezproxybib.pucp.edu.pe/10.1007/978-3-8348-9722-0`.

[Har77] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977, págs. xvi+496. ISBN: 0-387-90244-9.

[Har95] Joe Harris. *Algebraic geometry*. Vol. 133. Graduate Texts in Mathematics. A first course, Corrected reprint of the 1992 original. Springer-Verlag, New York, 1995, págs. xx+328. ISBN: 0-387-97716-3.

[Kir92] Frances Kirwan. *Complex algebraic curves*. Vol. 23. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1992, págs. viii+264. ISBN: 0-521-41251-X; 0-521-42353-8. DOI: `10.1017/CBO9780511623929`. URL: `https://doi-org.ezproxybib.pucp.edu.pe/10.1017/CBO9780511623929`.

[Stacks] The Stacks Project Authors. *Stacks Project*. `https://stacks.math.columbia.edu`. 2018.