Universidad de Cantabria

Facultad de Ciencias

LONGITUD DE MÓDULOS
Length of modules

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Marcos Balsa Fernández

Director: Luis Felipe Tabera Alonso

06 - 2025

Agradecimientos

En primer lugar, me gustaría agradecer a mi tutor, Luis Felipe Tabera Alonso, por ser tan paciente, profesional y hacer tan buen trabajo en todos los aspectos, en especial, en el aspecto didáctico.

A mis padres, Mar y Héctor, a mi hermano, Javier, y a mi novia, Clara, por su apoyo a lo largo de este proceso y por haber formado parte de los buenos y malos momentos. A mi perrita Tina, que ha pasado conmigo la mayoría de las tardes estudiando o realizando este trabajo, y me ha hecho más amena la experiencia. Este trabajo va por ti.

A mis amigos, que han formado parte del proceso de desconexión, y me han dado fuerzas para continuar trabajando al día siguiente.

Finalmente, me gustaría agradecerme a mí mismo, por haber conseguido terminar una carrera que al principio parecía imposible, y por no haber parado de trabajar ni un segundo hasta poder conseguirlo. Con esfuerzo y confianza, se puede conseguir cualquier cosa.

Resumen

Es bien conocido el concepto de dimensión de un espacio vectorial, y sus propiedades. Sin embargo, la definición de dimensión en términos del cardinal de una base, no se puede aplicar a otras estructuras algebraicas, como por ejemplo, para un módulo o un grupo. De este problema, nace el concepto de longitud de un módulo o grupo.

En este trabajo se estudiarán las propiedades de la longitud para módulos y para grupos, mostrando algunos ejemplos y analizando este concepto profundamente. Se verá cómo calcular esta longitud introduciendo nociones como la de serie de composición, o haciendo uso de teoremas clave como el Teorema de Jordan-Hölder.

Por último, se hará una introducción a un concepto propio de la geometría algebraica, llamado "número de intersección", que permite estudiar de qué forma se intersecan dos variedades afines.

Palabras Clave: longitud de módulo, serie de composición, sucesión exacta, localización, anillo local, número de intersección.

Abstract

The concept of the dimension of a vector space and its properties is well known. However, in certain algebraic structures, such as modules or groups, it may not be possible to find a basis in the usual sense. This leads to the notion of the length of a module or a group.

This report explores the properties of length in the context of modules and groups, illustrating these ideas through examples and providing an in-depth analysis of the concept. Methods for computing the length will be examined, introducing tools such as composition series and employing key results like the Jordan–Hölder Theorem.

Finally, the text presents an introduction to a central concept in algebraic geometry known as the intersection number, which formalizes how two affine varieties intersect. This notion is deeply connected to the concept of length.

Keywords: length of a module, composition series, exact sequence, localization, intersection number.

Índice

1. Introducción **8**

2. Series de composición, Teorema de Jordan-Hölder **10**
2.1. Series de composición para grupos 10
2.2. Series de composición para módulos 16
2.3. Longitud en grupos abelianos finitos 27

3. Propiedades locales de curvas **29**
3.1. Preliminares 29
3.2. El anillo $\mathcal{O}_P(V)$ 30

4. El número de intersección **36**
4.1. La multiplicidad de intersección en $k[X,Y]$ 36
4.2. Generalización del número de intersección 45

Referencias **49**

1. Introducción

Desde los inicios del álgebra moderna, uno de los grandes intereses de los matemáticos ha sido comprender la estructura interna de los objetos algebraicos complejos a través de su descomposición en objetos más sencillos y manejables. En el caso de grupos y módulos, las series de composición son una herramienta muy útil para llevar a cabo esta simplificación. Consisten en desarrollar estructuras algebraicas en subestructuras, a priori, más sencillas llamadas módulos simples. El teorema de Jordan–Hölder, formulado a finales del siglo XIX, garantiza que, aunque existan diferentes formas de hacer esta descomposición, el número de pasos necesarios y los objetos simples que aparecen no dependen del camino elegido. Este número de pasos da lugar a un concepto fundamental: la longitud de un grupo o un módulo.

La longitud resulta ser un valor que permite medir de alguna manera la "complejidad interna" del objeto que se está estudiando. A lo largo del siglo XX, esta noción ha cobrado mayor importancia en otros campos del álgebra, en particular en el estudio de los anillos y sus módulos. En este contexto, se vuelve especialmente útil cuando se trabaja con anillos locales y con el proceso de localización, que permite enfocar el estudio en una parte concreta de una estructura, como por ejemplo lo que ocurre en un punto determinado de una variedad afín.

En geometría algebraica, estas herramientas han sido claves para poder definir y calcular la multiplicidad de intersección de dos curvas en un punto. En términos simples, esto busca responder a la pregunta de "cuántas veces" se cruzan dos curvas en un mismo lugar. Resulta que esa multiplicidad puede expresarse, en muchos casos, como la longitud de un módulo que refleja lo que está ocurriendo en ese punto. Esta idea aparece explicada de forma clara en libros como *Algebraic Curves: An Introduction to Algebraic Geometry*, de William Fulton.

Por otro lado, el libro *Steps in Commutative Algebra*, de Rodney Y. Sharp, ofrece una base sólida para comprender todos estos conceptos desde el punto de vista del álgebra conmutativa. En él se desarrollan con detalle temas como la localización, los ideales primos, los módulos finitamente generados y la forma en que la longitud se comporta en diferentes situaciones.

Este trabajo tiene como objetivo profundizar en el concepto de longitud, su origen en las series de composición y su aplicación en el estudio de intersecciones de variedades afines mediante anillos localizados. En la parte final, se realiza un estudio de un concepto llamado "número de intersección" para variedades afines en dos dimensiones, que resulta en calcular la dimensión de un espacio vectorial concreto. Para poder relacionar los conceptos de longitud y número de intersección, en la última subsección del trabajo, estudiamos el caso de variedades afines de dimensión mayor a 2, en el que para calcular la multiplicidad de intersección, se precisa calcular la longitud de unos módulos llamados Tor.

2. Series de composición, Teorema de Jordan-Hölder

En este capítulo introducimos el concepto de longitud y de serie de composición para grupos y para módulos. En el caso particular de espacios vectoriales, nos interesa que la longitud se corresponda con la dimensión en el caso finito. Para esto, necesitaremos dar una definición parecida, pero alternativa, para el caso de $R-$módulos.

2.1. Series de composición para grupos

Para esta subsección se ha seguido el libro *Algebra* de Serge Lang [3].

Definición 2.1.1. Sea G un grupo. Decimos que G es un grupo simple si $G \neq 0$ y los únicos subgrupos normales de G son 0 y el propio G.

Ejemplo 2.1.2. Si G es un grupo abeliano simple, dado $a \neq 0$, debe ser $< a >= G$, es decir, G es cíclico. Cada elemento no nulo de G es un generador, por lo que tiene que ser un grupo cíclico finito de orden primo. Como el orden de un subgrupo debe dividir al orden del grupo, G es simple.

Definición 2.1.3. Sea G un grupo. Una cadena de subgrupos normales de G es una cadena finita y estrictamente creciente de subgrupos de G

$$G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_{n-1} \subsetneq G_n,$$

tal que $G_0 = 0$, $G_n = G$ y además, G_i es normal en G_{i+1}, para todo $i \in \{0, \ldots, n-1\}$.

Una cadena de subgrupos normales de un grupo G se puede refinar añadiendo un número finito de términos a la cadena dada, de forma que siga cumpliendo todos los requisitos para ser una cadena de subgrupos normales de G. A esto se le llama un refinamiento.

Definición 2.1.4. Sea G un grupo y G_1, G_2 dos subgrupos de G no vacíos, definimos el producto de dos subgrupos como $G_1G_2 = \{g_1 \cdot g_2 \mid g_1 \in G_1, g_2 \in G_2\}$.

Lema 2.1.5. Sea G un grupo y sean H, K dos subgrupos de G. Si H y K son normales en G, entonces HK es normal en G.

Demostración. Claramente el conjunto HK es no vacío, ya que H y K son no vacíos. Para empezar veamos que HK es subgrupo de G. Sean h_1k_1, h_2k_2 dos elementos de HK, entonces

$$(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1kh_2^{-1}.$$

Como $K \lhd G$, entonces $h_2kh_2^{-1} = \overline{k} \in K$. Multiplicando a la izquierda por h_2^{-1}, tenemos $kh_2^{-1} = h_2^{-1}\overline{k}$ y entonces

$$h_1kh_2^{-1} = h_1h_2^{-1}\overline{k} = hk \in HK,$$

porque H es subgrupo.

Probemos la afirmación del lema. Para ver que $HK \lhd G$, debemos ver que $g(hk)g^{-1} \in HK$, $\forall g \in G, \forall h \in H, \forall k \in K$.

$$g(hk)g^{-1} = (ghg^{-1})(gkg^{-1}) \in HK,$$

ya que $H \lhd G$ y $K \lhd G$. □

Ahora, introducimos un lema que servirá para probar el teorema de Schreier sobre los refinamientos de una cadena de subgrupos de un grupo G.

Lema 2.1.6 (Butterfly Lemma)**.** Sean U, V subgrupos de un grupo G. Sean $u \trianglelefteq U$ y $v \trianglelefteq V$ subgrupos normales. Entonces:

1. $u(U \cap v)$ es normal en $u(U \cap V)$,
2. $(u \cap V)v$ es normal en $(U \cap V)v$,
3. Los grupos cociente son isomorfos, es decir:

$$\frac{u(U \cap V)}{u(U \cap v)} \cong \frac{(U \cap V)v}{(u \cap V)v}.$$

Demostración. Para empezar, veamos que $u \cap V$ y $U \cap v$ son subgrupos normales de $U \cap V$. Es claro que son subgrupos, ya que $u \subseteq U$ y $v \subseteq V$. Consideramos $x \in u \cap V$ y $z \in U \cap V$. Como $x \in u$ y $z \in U \cap V$, tenemos que $zxz^{-1} \in u$. Como $x \in V$ y $z \in V$, tenemos que $zxz^{-1} \in V$, ya que V es un grupo. Por lo tanto, $zxz^{-1} \in u \cap V$ y concluimos que es subgrupo normal de $U \cap V$. Por un argumento análogo, se tiene también que $U \cap v$ es normal en $U \cap V$.

Ahora, por la Proposición 2.1.5, como el producto de subgrupos normales es normal, tenemos que $(u \cap V)(U \cap v)$ es normal en $U \cap V$ y definimos la aplicación

$$\begin{aligned} f : u(U \cap V) &\longrightarrow \frac{U \cap V}{(u \cap V)(U \cap v)} \\ ab &\mapsto b(u \cap V)(U \cap v) \end{aligned}$$

El conjunto de llegada tiene sentido, por lo probado anteriormente. Veamos que esta bien definida. Sea $a' \in u$ y $b' \in U \cap V$ tales que $a'b' = ab$, entonces

$$a^{-1}a' = bb'^{-1} \in u \cap (U \cap V) = (u \cap V) \subseteq (u \cap V)(U \cap v).$$

Por lo tanto, el inverso de $f(ab)$ es el inverso de $f(a'b')$ y por lo tanto $f(ab) = f(a'b')$.

Veamos que esta aplicación es un homomorfismo, y que es sobreyectiva.

Empecemos por ver que es un homomorfismo. Sean $a_1, a_2 \in u$ y $b_1, b_2 \in U \cap V$, queremos ver que $f(a_1b_1a_2b_2) = f(a_1b_1)f(a_2b_2) = \overline{b_1b_2}$.

Por normalidad, $b_1a_2b_1^{-1} = \alpha \in u$, y $b_1a_2 = \alpha b_1$, lo que significa que $a_1b_1a_2b_2 = a_1\alpha b_1b_2$. Concluimos que

$$f(a_1b_1a_2b_2) = f(a_1\alpha b_1b_2) = \overline{b_1b_2} = f(ab)f(\alpha\beta).$$

El homomorfismo f es sobreyectivo, ya que si $x \in (U \cap V) \Rightarrow f(e \cdot x) = x(u \cap V)(U \cap v)$. Busquemos cual es el $\ker(f)$, es decir, buscamos los $a \in u$ y $b \in (U \cap V)$ tales que $f(ab) = \overline{e}$. Claramente, cualquier a es valido, ya que la imagen no depende de a. Queremos que $b \in (U \cap V) \cap (u \cap V)(U \cap v) = (u \cap V)(U \cap v)$, por lo que podemos escribir $b = xy$ con $x \in u \cap V \subseteq u$, $y \in (U \cap v)$. Ahora tenemos $ab = axy = (ax)y \in u(U \cap v)$, por lo que $\ker(f) \subseteq u(U \cap v)$. Ahora, sea $cd \in u(U \cap v)$, como $(U \cap v) \subseteq (u \cap V)(U \cap v)$, tenemos que $f(cd) = \overline{d} = \overline{e}$ y concluimos que $\ker(f) = u(U \cap v)$, por lo que $u(U \cap v)$ es normal en $u(U \cap V)$.

De manera análoga se demuestra que $(u \cap V)v$ es normal en $(U \cap V)v$. Ahora, por el primer teorema de isomorfía, tenemos los siguientes isomorfismos:

$$\frac{u(U \cap V)}{u(U \cap v)} \cong \frac{U \cap V}{(u \cap V)(U \cap v)} \cong \frac{(U \cap V)v}{(u \cap V)v},$$

y queda demostrado el teorema. □

Definición 2.1.7. Sea G un grupo, y

$$G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_{n-1} \subsetneq G_n,$$

una cadena de subgrupos normales de G. Se definen los grupos factores de la cadena como los grupos de la forma G_{i+1}/G_i para todo $i \in \{0, \ldots, n-1\}$

Definición 2.1.8. Sea G un grupo, y sean

$$0 = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_r = G,$$

$$0 = H_0 \subsetneq H_1 \subsetneq \cdots \subsetneq H_s = G,$$

cadenas de subgrupos normales. Diremos que estas cadenas son equivalentes si $r = s$ y si existe una permutación de los índices $\sigma(i) = i'$ para todo $i \in \{0, \ldots, r-1\}$ tal que

$$G_{i+1}/G_i \cong H_{i'+1}/H_{i'}.$$

En otras palabras, los grupos factores en las dos cadenas son iguales, salvo isomorfismos y una permutación de los índices.

Teorema 2.1.9 (Schreier)**.** Sea G un grupo. Dos cadenas de subgrupos de G tienen refinamientos equivalentes.

Demostración. Sean

$$0 = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_r = G,$$

$$0 = H_0 \subsetneq H_1 \subsetneq \cdots \subsetneq H_s = G,$$

dos cadenas de subgrupos normales de G. Para cada $i \in \{1, \ldots, r\}$ y $j \in \{0, \ldots, s\}$, definimos:

$$G_{ij} = G_{i-1}(G_i \cap H_j).$$

Entonces se tiene que $G_{i,s} = G_{i-1}$, y obtenemos un refinamiento de la primera cadena de subgrupos:

$$\{e\} \subseteq G_{11} \subseteq G_{12} \subseteq \cdots \subseteq G_{1s} = G_1,$$
$$G_1 \subseteq G_{21} \subseteq G_{22} \subseteq \cdots \subseteq G_{2s} = G_2,$$
$$\vdots$$
$$G_{r-1} \subseteq G_{r1} \subseteq G_{r2} \subseteq \cdots \subseteq G_{rs} = G.$$

De manera similar, definimos:

$$H_{ji} = H_{j-1}(G_i \cap H_j),$$

para $j \in \{1, \ldots, s\}$ y $i \in \{0, \ldots, r\}$. Esto da lugar a un refinamiento de la segunda cadena de subgrupos normales. Observamos que los contenidos ya no son estrictos en este caso, ya que al refinar, puede ser que grupos consecutivos sean iguales.

Por el Lema 2.1.6 (Butterfly Lemma) se tiene que los dos refinamientos anteriores son cadenas de subgrupos normales, ya que cada elemento de la cadena es normal en el siguiente, es decir,

$$G_{ij-1} \lhd G_{ij} \quad y \quad H_{ji-1} \lhd H_{ji}.$$

También por el Butterfly Lemma, los grupos factores de los dos refinamientos obtenidos de cada cadena son isomorfos, es decir,

$$G_{ij}/G_{ij-1} \cong H_{ji}/H_{ji-1}.$$

Consideramos que cada una de las cadenas refinadas tiene $rs + 1$ elementos, que son: G_{ij} con $i \in \{1, \ldots, r\}$ y $j \in \{1, \ldots, s\}$, y el subgrupo trivial $\{e\}$ en el primer caso; y H_{ji} y $\{e\}$ en el segundo caso. Por lo tanto, por el isomorfismo anterior, las dos cadenas son equivalentes, como queríamos ver. □

Definición 2.1.10. Una cadena estricta de subgrupos normales de G dada por

$$0 = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_{n-1} \subsetneq G_n = G,$$

es una serie de composición de G cuando G_{i+1}/G_i es un grupo simple para cada $i \in \{0, \ldots, n-1\}$.

Notación. En el caso de que una cadena de subgrupos normales sea una serie de composición, denotamos a los grupos factores de la cadena de subgrupos normales como factores

de composición de la serie de composición, que son todos simples.

Definición 2.1.11. Sea

$$0 = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_{n-1} \subsetneq G_n = G,$$

una serie de composición de G. La longitud de la cadena, denotada por $\ell(G)$, es el numero de contenciones que hay en la cadena, es decir, $\ell(G) = n$, si G tiene serie de composición, y $\ell(G) = \infty$ si G no tiene serie de composición.

Teorema 2.1.12 (Jordan–Hölder)**.** Sea G un grupo, y sean

$$0 = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_r = G,$$

$$0 = H_0 \subsetneq H_1 \subsetneq \cdots \subsetneq H_s = G,$$

dos series de composición de G. Entonces, estas dos series de composición son equivalentes.

Demostración. Si refinamos cada serie de composición de acuerdo a la demostración del Teorema 2.1.9, obtenemos dos refinamientos equivalentes G_{ij} y H_{ji}. Observamos que para cada índice i, existe un único índice j que cumple:

$$G_i/G_{i-1} \cong G_{ij}/G_{ij-1}.$$

Esto es porque entre G_i y G_{i-1} no puede haber ningún grupo en la serie de composición, al ser simple su cociente, y lo mismo pasará en el refinamiento, por lo que fijados esos índices i, j, tenemos

$$G_{ik}/G_{ik-1} \cong 0, \quad \forall k \in \{1, \ldots, s\} \backslash \{j\}.$$

Por lo tanto, los factores de composición de la serie G son los grupos factores del refinamiento no nulos de G_{ij}. Lo mismo ocurre con los factores de composición de la serie H. Como G_{ij} y H_{ij} son equivalentes, concluimos que los factores de composición de G y H son isomorfos módulo una permutación. □

Ejemplo 2.1.13. Construyamos una serie de composición para el grupo simétrico de orden 4, S_4.

Observamos que $\#S_4 = 24$. Para empezar, veamos que A_4, es decir, el grupo de permutaciones de índice par de 4 elementos, es un subgrupo de S_4. Tomamos $\sigma_1, \sigma_2 \in A_4$ dos permutaciones pares. Es claro que, como ambas permutaciones descomponen en un número par de transposiciones, su composición $\sigma_1 \circ \sigma_2$ también lo hará.

Además, tomando la descomposición de σ en un número par de transposiciones

$$\sigma = (t_1, t_2) \circ (t_3, t_4) \circ \cdots \circ (t_{n-1}, t_n),$$

entonces,

$$\sigma^{-1} = (t_{n-1}\ t_n) \circ (t_{n-3}\ t_{n-2}) \circ \cdots \circ (t_1\ t_2),$$

que tiene el mismo numero de transposiciones y por lo tanto $\sigma^{-1} \in A_4$. Concluimos que A_4 es subgrupo de S_4.

Ahora, calculemos el cardinal de A_4. Podemos definir la aplicación

$$\begin{array}{rcl} f : A_4 & \longrightarrow & \{\sigma \in S_4 \mid \sigma \text{ es impar}\} \\ \sigma & \mapsto & \sigma \circ (1,2) \end{array}$$

Esta aplicación es una biyección, y por lo tanto $\#A_4 = \#\{\sigma \in S_4 \mid \sigma \text{ es impar}\}$, es decir, en S_4, el numero de permutaciones pares es el mismo que el numero de permutaciones impares. Como en S_4 solo puede haber permutaciones pares o impares, $\#A_4 = \frac{\#S_4}{2} = \frac{4!}{2} = 12$.

Ahora, sean $\sigma \in S_4, \tau \in A_4$, es claro que $\sigma \circ \tau \circ \sigma^{-1} \in A_4$ ya que τ es par, y tanto σ como σ descomponen en el mismo numero de transposiciones. Por esto, A_4 es normal en S_4 y podemos construir el grupo cociente S_4/A_4 cuyo cardinal es 2, y entonces es simple e isomorfo al grupo cíclico de orden 2, C_2.

Por lo tanto, A_4 cumple todas las condiciones para ser el primer subgrupo propio que conforma la serie de composición que estamos construyendo, y en este caso, C_2 es el factor de composición resultante.

Para continuar, probemos que A_4 tiene un único subgrupo de orden 4. Sea H un subgrupo de orden 4 de A_4. El orden de los elementos de H será 1, 2 ó 4, ya que deben dividir al orden del grupo. Es fácil probar que en A_4 no hay elementos de orden 4. Supongamos que existe $\sigma = (t_1\ t_2\ t_3\ t_4) \in A_4$. Entonces la descomposición de σ en transposiciones es $\sigma = (t_1\ t_2) \circ (t_4\ t_3) \circ (t_4\ t_2)$. Esto es una contradicción porque entonces σ sería una permutación impar y entonces $\sigma \notin A_4$. Por lo tanto H esta formado por todos los elementos de orden 2 de A_4, junto con la identidad, es decir, $H = \{Id,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$. A este grupo se le llama "Grupo de Klein" y se denota por V.

Ahora veamos que V es normal en A_4. Como V esta formado por todos los elementos de orden 1 o 2 de A_4, una simple comprobación muestra que $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Además, observamos que el orden de un elemento de V no cambia por conjugación. Sea $\sigma \in A_4$ y $\tau \in V$ con $O(\tau) = 2$, entonces $O(\sigma \circ \tau \circ \sigma^{-1}) = 2$ y $\sigma \circ \tau \circ \sigma^{-1} \in V$, por lo que V es normal en A_4 y podemos tomarle como subgrupo para nuestra serie de composición, cuyo factor de composición asociado es $A_4/V \cong C_3$ que es simple.

Los subgrupos de V deben tener orden 2, por lo que tenemos un subgrupo U de V por cada elemento de orden 2 de V, junto con la identidad. Cada uno de estos subgrupos, por ser de orden 2, es isomorfo a C_2. Es claro que V/U es simple ya que $\#V/U = 2$ y por lo tanto U es otro subgrupo de la serie de composición que estamos construyendo, cuyo factor de composición asociado es también C_2. Finalmente, como U es simple, queda terminada la construcción de una serie de composición para S_4:

$$0 \subsetneq U \subsetneq V \subsetneq A_4 \subsetneq S_4,$$

Y S_4 tiene longitud 4 como grupo.

2.2. Series de composición para módulos

Para realizar la siguiente subsección, se ha usado el libro *Steps in Commutative Algebra* de R.Y.Sharp. [4]

Ahora, dado un anillo conmutativo R, buscamos dar una definición para serie de composición para un $R-$módulo M. Para que esta definición sea interesante, queremos que en el caso particular de un $k-$espacio vectorial V de dimensión finita, la longitud de V coincida con $\dim_k(V)$. Más adelante, se muestra esta relación. Por este motivo, necesitamos añadir algún elemento adicional a la definición. Ahora, veamos que ocurre si tomamos la definición de serie de composición para grupos trasladada a módulos sin ninguna modificación. Observamos que $\mathbb{Q}^2$ tiene dimensión 2 como $\mathbb{Q}-$espacio vectorial. Sin embargo, podemos encontrar una cadena de subgrupos infinita,

$$\mathbb{Q}^2 \supsetneq \mathbb{Z}\times\mathbb{Z} \supsetneq \mathbb{Z}\times\{0\} \supsetneq (3)\times\{0\} \supsetneq (3^2)\times\{0\} \supsetneq (3^3)\times\{0\} \supsetneq \cdots$$

Por lo tanto, la dimensión de $\mathbb{Q}^2$ como $\mathbb{Q}-$espacio vectorial no coincide con su longitud como grupo. Necesitamos añadir una hipótesis adicional a la definición de serie de composición para que se cumpla la propiedad deseada. Este elemento extra que necesitamos es que los objetos de la cadena sean submódulos.

Definición 2.2.1. Sea R un anillo y M un $R-$módulo, decimos que M es simple si $M \neq 0$ y sus únicos submódulos son el trivial y M.

Definición 2.2.2. Sea R un anillo y M un $R-$módulo. Sea

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M,$$

una cadena de submódulos de M. Se define la longitud de la cadena anterior como el número de contenidos de la cadena, es decir, n.

Definición 2.2.3. Sea R un anillo y sea M un $R-$módulo. Sea

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M,$$

una cadena de submódulos de M. Decimos que esta cadena es una serie de composición de M si los $R-$módulos cocientes M_i/M_{i-1} son simples para todo $i \in \{1,\ldots,n\}$.

Sea M un $R-$módulo. En los siguientes dos teoremas, denotamos como $\ell(M)$ a la menor longitud de una serie de composición de M, si M tiene una serie de composición, y $\ell(M) = \infty$ si M no tiene una serie de composición. Además, consideramos que el módulo 0 tiene una cadena de submódulos de longitud 0.

Teorema 2.2.4. Sea M un módulo sobre un anillo conmutativo R. Supongamos que M tiene una serie de composición de longitud n. Entonces todo submódulo propio N de M, es decir, $N \subsetneq M$, tiene una serie de composición y $\ell(N) < \ell(M)$.

Demostración. Claramente, $n > 0$ por definición.

Sea N un submódulo de M tal que $0 \neq N \subsetneq M$. Sea $\ell(M) = t$, y

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{t-1} \subsetneq M_t = M,$$

una serie de composición para M de longitud t. Para cada $i \in \{0, \ldots, t\}$, sea $N_i = N \cap M_i$. Ahora, para cada $i \in \{1, \ldots, t\}$, el $R-$homomorfismo:

$$N_i = N \cap M_i \longrightarrow M_i \longrightarrow M_i/M_{i-1},$$

(en la que el primer morfismo es la inclusión y el segundo es el epimorfismo canónico) tiene núcleo igual a $N \cap M_i \cap M_{i-1} = N \cap M_{i-1} = N_{i-1}$ y por lo tanto, por el primer teorema de isomorfía para módulos, induce un monomorfismo.

$$\begin{array}{rcl} \varphi_i : N_i/N_{i-1} & \longrightarrow & M_i/M_{i-1} \\ h + N_{i-1} & \mapsto & h + M_{i-1} \end{array}$$

Entonces, N_i/N_{i-1} es isomorfo a un submódulo de M_i/M_{i-1}. Pero M_i/M_{i-1} es simple, por lo que N_i/N_{i-1} es o bien 0 o simple. De hecho, N_i/N_{i-1} es simple si y solo si φ_i es un isomorfismo. Así, si eliminamos cualquier repetición de términos en

$$0 = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_{t-1} \subsetneq N_t = N \cap M_t = N,$$

obtendremos una serie de composición para N. Concluimos que, $\ell(N) \leq \ell(M)$. Además, debemos tener $\ell(N) < \ell(M)$, ya que de lo contrario, el proceso anterior lleva a

$$N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_{t-1} \subsetneq N_t = N,$$

una serie de composición para N, con $N_i/(N_i \cap M_{i-1}) = N_i/N_{i-1} \neq 0$ para cada $i \in \{1, \ldots, t\}$. Como $N_0 = 0 = M_0$, entonces tendríamos que

$$N_0 = M_0; \;\; N_1 = M_1; \;\; \cdots \;\; N = N_t = M,$$

lo que contradice el hecho de que $N \subset M$. Así, hemos demostrado que N tiene una serie de composición y $\ell(N) < \ell(M)$. □

Teorema 2.2.5. Sea M un módulo sobre un anillo conmutativo R. Supongamos que M tiene una serie de composición de longitud n. Entonces:

1. No existe ninguna cadena estricta de submódulos de M que tenga una longitud mayor que n.

2. Toda serie de composición de M tiene exactamente longitud n.

3. Toda cadena estricta de submódulos de M de longitud $n' < n$ puede extenderse a una serie de composición de M añadiendo $n - n'$ términos adicionales.

4. En particular, toda cadena estricta de submódulos de M de longitud n es una serie de composición de M.

Demostración. De nuevo, $n > 0$ por definición de longitud. Demostremos cada afirmación del teorema por separado.

1. Sea

$$M_0^{'} \subsetneq M_1^{'} \subsetneq M_2^{'} \subsetneq \ \cdots \ \subsetneq M_{r-1}^{'} \subsetneq M_r^{'},$$

una cadena estricta de submódulos de M, de modo que $M_0^{'} = 0$ y $M_r^{'} = M$. Ahora, $\ell(0) = 0$, y por lo tanto, por el Teorema 2.2.4,

$$0 = \ell(M_0^{'}) < \ell(M_1^{'}) < \ell(M_2^{'}) < \ \ldots \ < \ell(M_{r-1}^{'}) < \ell(M_r^{'}) = \ell(M).$$

Por lo tanto, $r \leq \ell(M) \leq n$. Así, dado que M tiene una serie de composición de longitud n y una serie de composición para M es, en particular, una cadena estricta de submódulos de M, se sigue que $n \leq \ell(M)$, de modo que $n = \ell(M)$.

2. Ahora supongamos que M tiene una serie de composición de longitud n_1. Entonces, $n_1 \leq \ell(M) = n$ por el apartado 1, ya que una serie de composición es, en particular, una cadena estricta de submódulos, mientras que $\ell(M) \leq n_1$ por la definición de $\ell(M)$. Por lo tanto $n_1 = \ell(M) = n$, y toda serie de composición de M tiene exactamente longitud n.

3. Es inmediata por las afirmaciones 1 y 2. Una cadena estricta de submódulos de M de longitud $n' < n = \ell(M)$ no puede ser una serie de composición para M porque, por la parte 2, todas las series de composición de M tienen longitud n. Sea

$$0 = M_0 \subsetneq M_1 \subsetneq \ \cdots \ \subsetneq M_{n'-1} \subsetneq M_{n'} = M,$$

una cadena de subgrupos normales de M de longitud $n' < n$. Como la longitud de esta cadena es menor que n, $\exists i \in 1, \ldots, t$ tal que M_i/M_{i-1} no es simple, es decir, existe un submódulo N/M_{i-1} de M_i/M_{i-1}, de forma que $0 \subsetneq N/M_{i-1} \subsetneq M_i/M_{i-1}$ y, por tanto, $M_{i-1} \subsetneq N \subsetneq M_i$. Podemos construir un refinamiento de la cadena inicial añadiendo este submódulo N. Repitiendo el proceso $n - n'$ veces, conseguimos una cadena de subgrupos normales de longitud n, es decir, hasta conseguir una serie de composición de M.

4. Por otro lado, una cadena estricta de submódulos de M de longitud n ya debe ser una serie de composición para M porque, de lo contrario, podría extenderse a una cadena estricta de submódulos de M de longitud $n + 1$, lo que contradice la propiedad 1.

□

Definición 2.2.6. Sea M un módulo sobre el anillo conmutativo R. Decimos que M tiene longitud finita precisamente cuando M tiene una serie de composición. Cuando este es el caso, la longitud de M se define como la longitud de cualquier serie de composición de M, que es única, por el Teorema 2.2.5. Cuando M no tiene una serie de composición, decimos que $\ell(M) = \infty$.

Ahora, nuestro objetivo será establecer la relación entre longitud de un $R-$módulo y la dimensión en el caso particular de un espacio vectorial de dimensión finita, ya que como se ha indicado en la introducción del capítulo, uno de los objetivos de la definición de longitud es que en el caso de espacios vectoriales finitos, la longitud coincida con la dimensión.

Lema 2.2.7. Sea V un $k-$espacio vectorial de dimensión finita y $S \subseteq V$ un subespacio vectorial de V. Entonces $dim(V/S) = dim(V) - dim(S)$.

Demostración. Sean $m = \dim(S)$, $n = \dim(V)$ y $\{u_1, \ldots, u_m\}$ una base de S. Se puede completar la base hasta obtener una de V,$\{u_1, \ldots, u_m, u_{m+1}, \ldots, u_n\}$. Para todo $u \in V$, tenemos que $u = \sum_{i=1}^{n} k_i u_i$.

Tomando clases módulo S,

$$\overline{u} = \sum_{i=m+1}^{n} k_i \overline{u}_i,$$

pues $\overline{u}_1 = \cdots = \overline{u}_m = \overline{0}$ (ya que $u_1, \ldots, u_m \in S$). Veamos que $\overline{u}_{m+1}, \ldots, \overline{u}_n$ generan V/S.

Para ver que son linealmente independientes, supongamos que:

$$0 = \sum_{i=m+1}^{n} k_i \overline{u}_i = \overline{\sum_{i=m+1}^{n} k_i u_i},$$

entonces, $\sum_{i=m+1}^{n} k_i u_i \in S$, en consecuencia, existen $k_1, \ldots, k_m$ tales que

$$\sum_{i=m+1}^{n} k_i u_i = \sum_{i=1}^{m} k_i u_i.$$

Por la independencia lineal de $\{u_1, \ldots, u_n\}$, se sigue que $k_{m+1} = \cdots = k_n = 0$.

Por lo tanto, $\{u_{m+1}, \ldots, u_n\}$ es una base de V/S y $\dim V/S = n - m = \dim V - \dim S$. □

Teorema 2.2.8 (Longitud en espacios vectoriales)**.** Sea V un $\mathbb{K}$-espacio vectorial de dimensión n. Entonces:

1. Ninguna cadena estricta de subespacios de V puede tener longitud mayor que n.
2. Toda serie de composición de V tiene longitud exactamente n.

3. Toda cadena estricta de subespacios de V de longitud $n^{'} \leq n$ puede ser extendida a una serie de composición para V con la inserción de $n - n^{'}$ términos.

4. Toda cadena estricta de subespacios de V de subespacios de V de longitud n es una serie de composición para V.

Demostración. Observamos que, sea $S \subsetneq V$ un subespacio propio de V, veamos que $dim(S) < dim(V)$. Sea $\{u_1, u_2, \ldots, u_r\}$ una base de S. Como $S \subsetneq V$, $\exists v \in V \backslash S$. Por lo tanto $S \subsetneq S + < v > \subseteq V$, dándose la igualdad si $dim(S + < v >) = dim(V)$. Repitiendo este proceso hasta completar $\{u_1, u_2, \ldots, u_n\}$ a una base de V: $\{u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_{n-r}\}$ con $r \geq 1$, tenemos que $dim(S) < dim(V)$.

1. Supongamos que existe

$$0 = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_r = V,$$

una cadena estricta de subespacios propios de V con $r > n$. Por la observación anterior

$$0 = dim(V_0) < dim(V_1) < \cdots < dim(V_r) = dim(V) = n.$$

Como $r > n$ la cadena de desigualdades estrictas anterior tiene mas de n términos, acabada en n, lo que es un absurdo y debe ser $r \leq n$.

2. Sea

$$0 = V_0 \subsetneq V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_r = V,$$

una serie de composición para V. Esto es en particular una cadena estricta de subespacios de V y por lo probado en (i), $r \leq n$. Ahora, al ser una serie de composición, V_i/V_{i-1} debe ser simple $\forall i \in \{1, \ldots, r\}$, y por el lema anterior

$$dim(V_i/V_{i-1}) = dim(V_i) - dim(V_{i-1}) = 1, \qquad \forall i \in \{1, \ldots, r\}.$$

Por lo tanto, $dim(V_i) = dim(V_{i-1}) + 1$, $\forall i \in \{1, \ldots, r\}$. Es claro que $dim(V_0) = 0$, por lo que $dim(V_i) = i, \forall i \in \{0, \ldots, r\}$. Como $dim(V) = n$ por hipótesis y $V_r = V$, $dim(V_r) = n$ y por lo tanto $r = n$.

3. Es consecuencia de los apartados 1 y 2. Sea

$$0 = V_0 \subsetneq V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_{n'} = V,$$

una cadena estricta de subespacios de V de longitud $n^{'} \leq n$. Por 2, si $n^{'} = n$ hemos terminado. Si $n^{'} < n$, $\exists i_0 \in \{1, \ldots, n^{'}\}$ tal que

$$dim(V_{i_0}) > dim(V_{i_0-1}) + 1$$

Como $dim(V_i) > dim(V_{i-1}) + 1 > dim(V_{i-1}), \forall i \in \{1, \ldots, n'\}$, $\exists v_1 \in V_{i_0} \backslash V_{i_0-1}$ tal que

$$V_{i_0-1} \subsetneq V_{i_0-1} + < v_1 > \subsetneq V_{i_0},$$

y además, $\exists v_2 \in V_{i_0} \backslash (V_{i_0-1} + < v_1 >)$ tal que

$$V_{i_0-1} \subsetneq V_{i_0-1} + < v_1 > \subsetneq (V_{i_0-1} + < v_1 >) + < v_2 > \subseteq V_{i_0}.$$

Repitiendo este proceso, añadiendo a la cadena los subespacios que obtenemos al añadir estos vectores, hasta que $dim(V_i) - dim(V_{i-1}) = 1$, para todo $i \in \{1, \ldots, n'\}$, tendremos una cadena estricta de subespacios de V de longitud n tal que V_i/V_{i-1} es simple $\forall i \in \{1, \ldots, n\}$, y por lo tanto una serie de composición para V.

4. Es consecuencia directa de el apartado 2 y 3.

□

Observación 2.2.9. Observamos que, como el teorema que caracteriza la noción de longitud para módulos, es decir, el Teorema 2.2.5 y el teorema que caracteriza la dimensión en el caso de espacios vectoriales, es decir, el Teorema 2.2.8 son análogos, la dimensión coincide con la longitud en el caso de espacios vectoriales.

Definición 2.2.10. Sea R un anillo y $M \neq 0$ un $R-$módulo y sean

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M,$$

$$0 = M'_0 \subsetneq M'_1 \subsetneq \cdots \subsetneq M'_n = M,$$

dos series de composición de M. Decimos que estas dos series de composición de M son equivalentes si y solo si existe una permutación $\varphi \in S_n$ tal que, para todo $i = 1, \ldots, n$, se cumple que $M_i/M_{i-1} \cong M'_{\varphi(i)}/M'_{\varphi(i)-1}$. Esto es, que los factores de composición de las dos series de composición son isomorfos.

Observación 2.2.11. Es claro que, si M_1 y M_2 son dos $R-$módulos isomorfos, entonces M_1 tiene longitud finita si y solo si M_2 tiene longitud finita y, en este caso, $\ell(M_1) = \ell(M_2)$.

Lema 2.2.12. Sea R un anillo y M un $R-$módulo y sean N, N' submódulos de M tales que $N \neq N'$ y tanto M/N como M/N' son simples. Entonces:

$$M/N \cong N'/(N \cap N') \quad \text{y} \quad M/N' \cong N/(N \cap N').$$

Demostración. Primero mostramos que $N \subsetneq N + N'$. Si esto no fuera cierto, tendríamos $N = N + N'$, lo que, como $N \neq N'$, implicaría que $N' \subset N \subset M$, contradiciendo el hecho de que M/N' es simple, ya que N/N' sería submódulo no trivial de M/N'.

Por lo tanto, $N \subsetneq N + N' \subseteq M$, y como M/N es simple, se sigue que $N + N' = M$.

Entonces, por el tercer teorema de isomorfía para módulos, $M/N = (N + N')/N \cong N'/(N \cap N')$. La otra isomorfía se obtiene intercambiando N por N'. □

Teorema 2.2.13 (Teorema de Jordan-Hölder)**.** Sea M un módulo no nulo de longitud finita sobre el anillo conmutativo R. Entonces, cualquier par de series de composición de M son equivalentes.

Demostración. Como $M \neq 0$, tenemos $n := \ell(M) \geq 1$. Probemoslo por inducción en n.

El caso base $n = 1$ es trivial, así que suponemos $n > 1$ y que el resultado es cierto para valores menores que n.

Sean

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M,$$

$$0 = M'_0 \subsetneq M'_1 \subsetneq \cdots \subsetneq M'_{n-1} \subsetneq M'_n = M,$$

dos series de composición de M. El paso inductivo se divide en dos casos:

Caso 1: Si $M_{n-1} = M'_{n-1}$, entonces $M_n/M_{n-1} \cong M'_n/M'_{n-1}$ y las cadenas

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1},$$

$$0 = M'_0 \subsetneq M'_1 \subsetneq \cdots \subsetneq M'_{n-1},$$

son series de composición de $M_{n-1} = M'_{n-1}$. Como $\ell(M_{n-1}) = n-1$, aplicamos la hipótesis de inducción y el resultado sigue directamente.

Caso 2: Si $M_{n-1} \neq M'_{n-1}$, definimos $N = M_{n-1} \cap M'_{n-1}$. Por el Lema 2.2.12,

$$M_n/M_{n-1} \cong M'_{n-1}/N,$$

$$M'_n/M'_{n-1} \cong M_{n-1}/N,$$

por lo que estos cuatro módulos son simples. Si $N = 0$ (lo que implica que M_{n-1} y M'_{n-1} son simples y $n = 2$), la conclusión deseada se obtiene inmediatamente. Supongamos entonces que $N \neq 0$.

En este caso, $0 \subsetneq N \subsetneq M_{n-1} \subsetneq M_n$ es una cadena estricta de submódulos de $M = M_n$, y además, tanto M_n/M_{n-1} como M_{n-1}/N son módulos simples.

Ahora, por el apartado 3 del Teorema 2.2.5, la cadena anterior puede extenderse insertando términos adicionales hasta formar una serie de composición para M; dado que una serie de composición para M tiene longitud n, se sigue que $\ell(N) = n - 2$.

En particular, obtenemos una serie de composición

$$0 = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_{n-3} \subsetneq N_{n-2} = N.$$

Los argumentos anteriores implican que las siguientes dos series de composición para M

$$N_0 \subsetneq \cdots \subsetneq N_{n-2} \subsetneq M_{n-1} \subsetneq M_n \ ,$$

$$N_0 \subsetneq \cdots \subsetneq N_{n-2} \subsetneq M'_{n-1} \subsetneq M'_n,$$

son equivalentes.

Pero ahora podemos aplicar la hipótesis de inducción a estas dos series de composición

$$M_0 \subsetneq \cdots \subsetneq M_{n-2} \subsetneq M_{n-1}$$

$$N_0 \subsetneq \cdots \subsetneq N_{n-2} \subsetneq M_{n-1},$$

lo que demuestra la equivalencia de las siguientes series de composición:

$$M_0 \subsetneq \cdots \subsetneq M_{n-2} \subsetneq M_{n-1} \subsetneq M_n,$$

$$N_0 \subsetneq \cdots \subsetneq N_{n-2} \subsetneq M_{n-1} \subsetneq M_n,$$

$$N_0 \subsetneq \cdots \subsetneq N_{n-2} \subsetneq M'_{n-1} \subsetneq M'_n,$$

y, de manera análoga, la última cadena es equivalente a

$$M'_0 \subsetneq M'_1 \subsetneq \cdots \subsetneq M'_{n-1} \subsetneq M'_{n-1} \subsetneq M'_n$$

lo que completa el paso inductivo. □

Teorema 2.2.14. Sea M un $R-$módulo finitamente generado y sea

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n,$$

una serie de composición de M. Entonces existen $p_1, \ldots, p_n$ ideales maximales de R posiblemente repetidos tales que $M_i/M_{i-1} \cong R/p_i$ para todo $i \in \{1, \ldots, n\}$.

Demostración. Para cada i, llamemos $M = M_i$ y $N = M_{i-1}$ por simplicidad. Como la cadena del enunciado es una serie de composición, tenemos que M/N es un $R-$módulo simple. Veamos que

$$p_i = (N : M) = \{a \in R \mid aM \subseteq N\},$$

llamado ideal cociente de N por M. Para empezar, veamos que este es un ideal. Es claro que $0 \in p_i$, ya que $0M = 0 \subseteq N$. Sean $a, b \in p_i$, entonces $\forall m \in M$ se cumple que $am \in N$ y $bm \in N$, por lo tanto $(a+b)m \in N$ y $a + b \in p_i$. Ahora, sean $a \in p_i, r \in R$, tenemos que $a \cdot m \in N$, $\forall m \in M$, por lo tanto $r \cdot a \cdot m \in N$, $\forall m \in M$ ya que N es un submódulo de R y concluimos que $r \cdot a \in p_i$. Por lo tanto, p_i es un ideal. $1 \notin p_i$ porque $M \not\subseteq N$, así que p_i es un ideal propio de R. Veamos que p_i es maximal. Consideremos la aplicación:

$$\begin{array}{rcl} \varphi : R/p_i \times M/N & \longrightarrow & M/N \\ (\overline{a}, \overline{m}) & \mapsto & \overline{a \cdot m} \end{array}$$

Si $\overline{a} = \overline{b} \Rightarrow a - b \in p_i$ y entonces $\forall m \in M$, $(a-b)\overline{m} = \overline{(a-b)m} = \overline{0}$. Finalmente, $\overline{am} = \overline{bm}$ y φ está bien definida y dota a M/N de estructura de R/p_i-módulo con la aplicación φ. En este caso, los submódulos de M/N como R-módulo coinciden con los submódulos de M/N como R/p_i-módulo.

Sea $m \in M$ con $\overline{m} \neq \overline{0}$, consideremos la aplicación:

$$\begin{array}{rcl} \psi : R/p_i & \longrightarrow & M/N \\ \overline{a} & \mapsto & \overline{a} \cdot \overline{m} \end{array}$$

Veamos que ψ es un isomorfismo de R/p_i-módulos. Notemos que, como M/N es simple, entonces $< \overline{m} >= M/N$. Por este motivo, ψ es sobreyectiva.

Veamos que ψ es inyectiva. Para ello, veamos que $\ker(\psi) = 0$. Sean $\overline{a} \in R/p_i$, $\overline{m} \in M/N$. Si $\overline{a} \cdot \overline{m} = \overline{0}$, entonces $a \cdot m \in N$. Ahora, como M es un $R-$módulo y $< \overline{m} >= M/N$, $\forall u \in M$, $\exists r \in R$ con $\overline{u} = \overline{r} \cdot \overline{m}$. Por lo tanto, $\overline{a} \cdot \overline{u} = \overline{arm} = \overline{0}$. Por lo tanto, $a \cdot u \in N$ y $a \in p_i$, y entonces $\overline{a} = \overline{0}$ y $\ker(\psi) = 0$ y ψ es inyectiva.

Concluimos que ψ es un isomorfismo y queda demostrado que $R/p_i \cong M/N$. La segunda afirmación es clara, ya que M/N es simple, por lo que R/p_i es simple, pero como los submódulos de un anillo son los ideales, tenemos que los únicos ideales de R/p_i son el 0 y el total, por lo tanto R/p_i es un cuerpo. Concluimos que p_i es un ideal maximal para todo $i \in \{1, \ldots, n\}$. □

A continuación, veamos algunas propiedades sobre la longitud, en concreto, sobre su aditividad.

Definición 2.2.15. Sea R un anillo y $M_1, M_2, \ldots, M_{n+1}$ Módulos sobre R. Sean $\varphi_i : M_i \to M_{i+1}$ homomorfismos de R-módulos, decimos que la sucesión

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \cdots M_n \xrightarrow{\varphi_n} M_{n+1}$$

es exacta si $\mathrm{Im}(\varphi_i) = \ker(\varphi_{i+1})$ para cada $i \in \{1, \ldots, n-1\}$.

Observación 2.2.16. Sean M, M', M'' tres módulos sobre R. Observamos que existen homomorfismos únicos de R-módulos desde el módulo cero 0 hacia cualquier R-módulo M, y desde M hacia 0. Así, la sucesión

$$M \xrightarrow{\varphi} M'' \to 0$$

es exacta si y solo si φ es sobreyectiva, y la sucesión

$$0 \to M' \xrightarrow{\psi} M$$

es exacta si y solo si ψ es inyectiva.

Ademas, la sucesión

$$0 \to M' \xrightarrow{\psi} M \xrightarrow{\varphi} M'' \to 0$$

es exacta si y solo si φ es sobreyectiva, ψ es inyectiva y $\mathrm{Im}(\psi) = \ker(\varphi)$.

A esta sucesión exacta de $R-$módulos se le llama *sucesión exacta corta*.

Proposición 2.2.17. Sean N y P dos submódulos de un módulo M, con $P \subset N$. Sea $\varphi : M \to N$ un homomorfismo de módulos. Entonces existen homomorfismos naturales de M/P sobre M/N y de N/P en M/P. Además, la siguiente sucesión

$$0 \to N/P \to M/P \to M/N \to 0$$

es exacta.

Demostración. El homomorfismo natural $\pi : M/P \to M/N$ es el epimorfismo canónico. El homomorfismo natural $i : N/P \to M/P$ es la inclusión canónica. Ahora, claramente tenemos que $\mathrm{Im}(i) = N/P$. Además, sabemos que i es inyectiva y π es sobreyectiva por definición. Ahora,

$$(M/P)/\mathrm{Im}(i) = (M/P)/(N/P) \cong M/N,$$

por el segundo teorema de isomorfía. Por lo tanto, la sucesión es exacta, por la Observación 2.2.16. □

Proposición 2.2.18. Sea $0 \to V' \xrightarrow{\psi} V \xrightarrow{\varphi} V'' \to 0$ una sucesión exacta de espacios vectoriales de dimensión finita sobre un cuerpo k. Entonces, se cumple que:

$$\dim V = \dim V' + \dim V''.$$

Demostración. Dado que la sucesión es exacta, se tiene que $\mathrm{Im}(\psi) = \ker(\varphi)$.Por la observación anterior, sabemos que ψ es inyectiva, y se sigue que $\dim(V') = \dim(\mathrm{Im}(\psi))$. Además, por la propiedad de las dimensiones en espacios vectoriales, se cumple que:

$$\dim(V) = \dim(\ker(\varphi)) + \dim(\mathrm{Im}(\varphi)).$$

Sustituyendo $\ker(\varphi) = \mathrm{Im}(\psi)$ y usando que φ es sobreyectiva, obtenemos:

$$\dim(V) = \dim(V') + \dim(V'').$$

□

El objetivo del siguiente lema es ver que la función de longitud de un $R-$módulo M tiene estructura aditiva.

Lema 2.2.19. Sean M', M y M'' tres $R-$módulos. Sea

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

una sucesión exacta de $R-$módulos. Entonces $\ell(M) = \ell(M') + \ell(M'')$. En particular, si dos de los $R-$módulos tienen longitud finita, entonces el tercero también la tiene.

Mas generalmente, sean M_i $R-$módulos con $i \in \{1, \ldots, t\}$, y sea

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \cdots \longrightarrow M_t \longrightarrow 0$$

una sucesión exacta, entonces

$$\textstyle\sum_{i=0}^{t} (-1)^i \, \ell(M_i) = 0.$$

Demostración. Llamemos φ_i a la aplicación que va de M_i a M_{i+1}. Como

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \cdots \longrightarrow M_t \longrightarrow 0$$

es una sucesión exacta, tenemos que $\mathrm{Im}(\varphi_i) = \ker(\varphi_{i+1})$ para todo $i \in \{0, \ldots, t-1\}$. Como φ es un homomorfismo de $R-$módulos, entonces

$$\ell(M_i) = \ell(\ker(\varphi_i)) + \ell(\mathrm{Im}(\varphi_i)) = \ell(\ker(\varphi_i)) + \ell(\ker(\varphi_{i+1})),$$

para todo $i \in \{1, \ldots, t-1\}$. Por lo tanto,

$$\begin{aligned}\sum_{i=0}^{t}(-1)^i\ell(M_i) &= \sum_{i=0}^{t-1}(-1)^i\ell(M_i) + (-1)^t\ell(M_t)\\ &= \sum_{i=0}^{t-1}(-1)^i\left[\ell(\ker(\varphi_i)) + \ell(\ker(\varphi_{i+1}))\right] + (-1)^t\ell(M_t)\\ &= \ell(\ker(\varphi_0)) + (-1)^{t-1}\ell(\ker(\varphi_t)) + (-1)^t\ell(M_t) = 0,\end{aligned}$$

teniendo en cuenta que $\ker(\varphi_0) = 0$, y $\ker(\varphi_t) = M_t$.

El caso de una sucesión exacta corta es un caso particular de la general. □

2.3. Longitud en grupos abelianos finitos

En esta subsección, trataremos un caso particular de estructura como es la de grupo abeliano finito. Es importante darse cuenta de que podemos usar cualquier resultado de las dos subsecciones anteriores, independientemente de que sean para grupos o para módulos, ya que los $\mathbb{Z}$-módulos son precisamente los grupos abelianos finitos. Como es lógico, todos los grupos considerados en esta sección son abelianos.

Hay ciertos grupos para los que calcular su longitud puede ser tedioso y tener cierta dificultad. Para esto, existe un teorema que afirma que todo grupo en un dominio de ideales principales se puede descomponer en suma directa (o producto cartesiano) de grupos cíclicos con ciertas condiciones, y además, esta descomposición es única salvo reordenación de los términos de la descomposición.

De esta forma, la longitud del grupo G puede ser calculada como la suma de las longitudes de los grupos en los que descompone, lo que puede facilitar la tarea bastante. Antes de ver este teorema, veamos que la longitud de un grupo y la de su descomposición en suma directa de grupos cíclicos de orden potencia de primo coincide.

Observación 2.3.1. Si G es abeliano, cualquier cadena de subgrupos estrictamente creciente cumple la hipótesis de normalidad.

Lema 2.3.2. Sean A, B dos grupos no nulos, entonces

$$\ell(A \oplus B) = \ell(A) + \ell(B).$$

Demostración. Podemos construir la sucesión exacta:

$$0 \longrightarrow A \longrightarrow A \oplus B \longrightarrow B \longrightarrow 0$$

Sea $a \in A$ y $b \in B$, la sucesión exacta consiste en llevar $a \mapsto (a, 0)$ y $(a, b) \mapsto b$. De esta forma, por el Lema 2.2.19, queda demostrado. En el caso de que $\ell(A) = \infty$ o $\ell(B) = \infty$ el resultado es claro. □

Lema 2.3.3. Sea p un primo y $n \in \mathbb{N}$. Sea C_{p^n} un grupo cíclico de orden p^n. Entonces:

$$\ell(C_{p^n}) = n.$$

Demostración. Observamos que la siguiente cadena de subgrupos normales

$$0 \subseteq \langle p^{n-1} \rangle \subseteq \langle p^{n-2} \rangle \subseteq \cdots \subseteq \langle p \rangle \subseteq \langle 1 \rangle = C_{p^n},$$

es una serie de composición, ya que los factores de composición para cada $i \in \{1, ..., n-1\}$ son

$$\langle p^i \rangle / \langle p^{i+1} \rangle \cong C_p,$$

y C_p es simple por ser de orden p primo. Por lo tanto, $\ell(C_{p^n}) = n$. □

Teorema 2.3.4. Sea G un grupo abeliano finito y no nulo. Entonces G es isomorfo a una suma directa de grupos cíclicos de orden potencia de primo. Es decir,

$$G \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{r_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{r_k}\mathbb{Z},$$

donde p_i son primos no necesariamente distintos, y $r_i \geq 1$.

Supongamos que existen dos descomposiciones en suma directa de grupos cíclicos de orden potencia de primo:

$$G \cong \bigoplus_{i=1}^{n} \left(\bigoplus_{j=1}^{w(i)} \mathbb{Z}/p_i^{u_{ij}}\mathbb{Z} \right) \quad \text{y} \quad G \cong \bigoplus_{i=1}^{m} \left(\bigoplus_{j=1}^{y(i)} \mathbb{Z}/q_i^{v_{ij}}\mathbb{Z} \right),$$

donde:

- $p_1, \ldots, p_n$ y $q_1, \ldots, q_m$ son primos distintos,
- Para cada i, se tiene $u_{i1} < u_{i2} < \cdots < u_{iw(i)}$ y $v_{i1} < v_{i2} < \cdots < v_{iy(i)}$,
- $w(i), y(i) \in \mathbb{N}$ y $u_{ij}, v_{ij} \in \mathbb{N}$.

Entonces:

1. Se tiene $n = m$ y, tras reordenar si es necesario, $p_i = q_i$ para todo i.
2. Para cada $i \in \{1, \ldots, n\}$, se cumple $w(i) = y(i)$ y $u_{ij} = v_{ij}$ para todo $j \in \{1, \ldots, w(i)\}$.

En particular, la descomposición de G como suma directa de grupos cíclicos de orden potencia de primo está determinada de forma única, salvo reordenación de los términos.

Demostración. Para una demostración detallada, véase el Teorema 10.35 en el libro *Steps in Commutative Algebra* de Rodney Y. Sharp. [4, p.205]. □

Haciendo uso de estos resultados, todo grupo abeliano finito no nulo G, se puede calcular la longitud de G de forma más cómoda. Sea G un grupo, podemos descomponerlo de acuerdo al Teorema 2.3.4 de la siguiente forma:

$$G \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{r_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{r_k}\mathbb{Z}.$$

donde p_i son primos y $r_i \in \mathbb{N}$. Podemos entonces calcular $\ell(G)$ haciendo uso de los Lemas 2.3.3 y 2.3.2 como

$$\ell(G) = \ell(\mathbb{Z}/p_1^{r_1}\mathbb{Z}) + \ell(\mathbb{Z}/p_2^{r_2}\mathbb{Z}) + \cdots + \ell(\mathbb{Z}/p_k^{r_k}\mathbb{Z}) = \sum_{i=1}^{k} r_i.$$

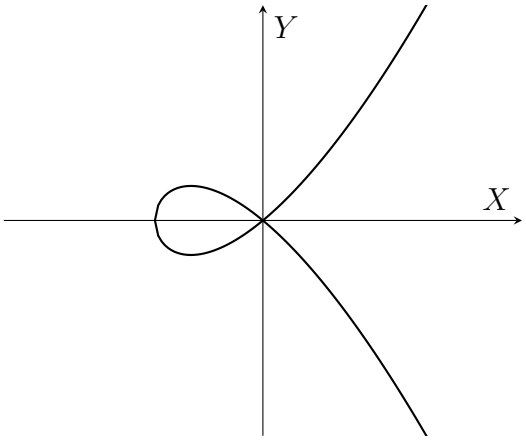
3. Propiedades locales de curvas

3.1. Preliminares

En esta sección trabajaremos con un cuerpo algebraicamente cerrado k. Denotamos por $\mathbb{A}^n(k)$ o por $\mathbb{A}^n$ el $k-$espacio afín de dimensión n definido por el producto cartesiano de n copias de k.

Definición 3.1.1. Sea S un conjunto de polinomios de $k[X_1, X_2, \ldots, X_n]$. Definimos $V(S) \coloneqq \{P \in \mathbb{A}^n(k) \mid F(P) = 0 \ \forall F \in S\}$ como el conjunto de ceros de el conjunto de polinomios S.

Ejemplo 3.1.2. Sea $k = \mathbb{R}$. El conjunto de ceros de $Y^2 - X^2(X+1) \in \mathbb{R}[X, Y]$ viene dado por la siguiente curva.



$V(Y^2 - X^2(X+1)) \subset \mathbb{A}^2$

Definición 3.1.3. Sea $X \subseteq \mathbb{A}^n$ un conjunto no vacío. Definimos el ideal de X como el ideal de todos los polinomios que se anulan en todo punto de X y lo denotamos por $\mathcal{I}(X)$. Es decir, $\mathcal{I}(X) \coloneqq \{F \in k[X_1, \ldots, X_n] \mid F(a_1, \ldots, a_n) = 0 \ \ \forall (a_1, \ldots, a_n) \in X\}$.

Definición 3.1.4. Sea $f \in k[X_1, X_2, \ldots, X_n]$ un polinomio. Decimos que f es una forma algebraica de grado d si todos sus monomios tienen grado d, y lo denotamos como F_d.

Ahora, enunciamos un lema que nos será útil para demostrar algunos resultados del capítulo siguiente.

Lema 3.1.5. Sea I un ideal en $k[X_1, \ldots, X_n]$. Entonces, $V(I)$ es un conjunto finito si y solo si $k[X_1, \ldots, X_n]/I$ es un espacio vectorial de dimensión finita sobre k. En este caso, el número de puntos en $V(I)$ es a lo sumo $\dim_k(k[X_1, \ldots, X_n]/I)$.

Demostración. La demostración se puede encontrar en el Corolario 4 en *Algebraic Curves: An Introduction to Algebraic Geometry.* [2, p.11]. □

Ahora, es necesario introducir una de las definiciones que más se van a utilizar a partir de ahora, la noción de localización. Esta noción es la base de la geometría algebraica y es la que nos permite estudiar las propiedades locales de una curva en un punto concreto. Además, una de las ventajas de la noción de localización es que permite convertir a todos los elementos del anillo que sean distintos de cero en unidades.

Definición 3.1.6. Sea R un anillo y P un ideal primo de R. Sea $S = R\backslash P$ un conjunto multiplicativamente cerrado, es decir, dados $a, b \in S$ se cumple:

- $1 \in S$.
- $a \cdot b \in S$.

Al anillo de fracciones con numeradores en R y denominadores en S, o formalmente $S^{-1}R$ lo llamamos el anillo R localizado en P. Este anillo se denota R_P.

Observación 3.1.7. Esta definición es valida para ideales I que no son primos. Además, si P es un ideal primo, $S = R\backslash P$ es siempre un conjunto multiplicativamente cerrado, por definición de ideal primo.

Cuando hablemos del "anillo R localizado en el punto $P = (p_1, p_2)$", nos referiremos al anillo localizado en el ideal $I = (X - p_1, Y - p_2)$, esto es, al anillo R_I. Observamos que este ideal siempre es primo.

Ejemplo 3.1.8. Algunos ejemplos de esta noción son:

- Si $R = \mathbb{Z}$ y $P = (0)$ el ideal generado por el 0, entonces $R_P = Frac(\mathbb{Z})$, es decir, el anillo $\mathbb{Z}_{(0)}$ es el cuerpo de fracciones de $\mathbb{Z}$, que precisamente es $\mathbb{Q}$.
- Si localizamos $k[X, Y]$ en un punto P, obtenemos las fracciones formadas por polinomios de $k[X, Y]$ cuyo denominador no se anula en P. Esto nos permite estudiar cómodamente las propiedades de curvas alrededor de un punto P.

3.2. El anillo $\mathcal{O}_P(V)$

Definición 3.2.1. Sea $V \subseteq \mathbb{A}^n$ una variedad afín no nula. Se define el anillo $\Gamma(V) \coloneqq k[X_1, X_2, \ldots, X_n]/\mathcal{I}(V)$ llamado el *anillo de coordenadas de* V.

Este anillo es un dominio de integridad, ya que como V es una variedad afín, $\mathcal{I}(V)$ es un ideal primo de $k[X_1, X_2, \ldots, X_n]$. Ahora, podemos construir el cuerpo de fracciones de $\Gamma(V)$, denotado por $k(V)$. Un elemento de $k(V)$ es una función racional en V.

Definición 3.2.2. Sea $V \subseteq \mathbb{A}^n$ una variedad afín no nula, $\Gamma(V)$ su anillo coordinado, $k(V)$ el cuerpo de fracciones de $\Gamma(V)$ y $f \in k(V)$ una función racional de $k(V)$. Decimos que f está definido en un punto $P \in \mathbb{A}^n$ si $f = g/h$ con $h(P) \neq 0$ para algún $g, h \in \Gamma(V)$.

Observamos que hay muchas formas de escribir f como un cociente de dos polinomios en $\Gamma(V)$. f está definido en P si podemos representar f como un cociente de dos polinomios en el que el denominador no se anule en P.

Ejemplo 3.2.3. Sea $V = V(XW - YZ) \subset \mathbb{A}^4(k)$. Entonces el anillo de coordenadas de V es

$$\Gamma(V) = k[X, Y, Z, W]/(XW - YZ).$$

Sean $\overline{X}, \overline{Y}, \overline{Z}, \overline{W}$ las clases de equivalencia de X, Y, Z, W en $\Gamma(V)$. Luego, $\overline{X}/\overline{Y} = \overline{Z}/\overline{W} = f \in k(V)$ está definida en el punto $P = (x, y, z, w) \in V$ si $y \neq 0$ o $w \neq 0$.

Definición 3.2.4. Sea $V \subseteq \mathbb{A}^n$ una variedad afín no nula, $P \in V$ un punto. Definimos $\mathcal{O}_P(V)$ como el anillo de funciones racionales de V que están definidas en el punto P.

Es fácil verificar que $\mathcal{O}_P(V)$ es un subanillo de $k(V)$ que contiene a $\Gamma(V)$. Es decir,

$$k \subseteq \Gamma(V) \subseteq \mathcal{O}_P(V) \subseteq k(V).$$

Al anillo $\mathcal{O}_P(V)$ se le llama *anillo local de V en P*.

Lema 3.2.5. Las siguientes condiciones sobre un anillo R son equivalentes:

1. El conjunto de no unidades en R forma un ideal.
2. R tiene un único ideal maximal que contiene todos los ideales propios de R.

Demostración. Sea $\mathfrak{m}$ el conjunto de las no unidades de R. Sea $I \subsetneq R$ un ideal propio de R. Entonces $I \subset \mathfrak{m}$ porque si no fuese así, en I habría una unidad, y por lo tanto $I = R$, contradiciendo que I es un ideal propio. Por este mismo motivo, es claro que $\mathfrak{m}$ es un ideal maximal. El lema es una consecuencia directa de esto. □

Definición 3.2.6. Sea R un anillo. Se dice que R es un anillo local si satisface alguna de las dos condiciones del Lema 3.2.5.

Proposición 3.2.7. $\mathcal{O}_P(V)$ es un anillo local cuyo único maximal es

$$\mathfrak{m}_P(V) = \{f \in \mathcal{O}_P(V) \mid f(P) = 0\} = \{\text{no unidades de } \mathcal{O}_P(V)\}.$$

Demostración. Por el Lema 3.2.16, basta ver que $\mathfrak{m}_P(V)$ es un ideal de $\mathcal{O}_P(V)$. Sea un polinomio $f \in \mathcal{O}_P(V)$ y $g \in \mathfrak{m}_P(V)$, entonces

$$g(P) = 0 \iff fg(P) = f(P)g(P) = 0 \iff fg \in \mathfrak{m}_P(V).$$

□

Proposición 3.2.8. $\mathcal{O}_P(V)$ es un dominio noetheriano local.

Demostración. Debemos mostrar que cualquier ideal I de $\mathcal{O}_P(V)$ está generado de forma finita. Veamos que $\Gamma(V)$ es noetheriano. Sabemos que hay una correspondencia natural entre los ideales I de $k[X_1, X_2, \ldots, X_n]$ y los ideales J de $k[X_1, X_2, \ldots, X_n]/I$ que contienen a I.

Como $k[X_1, X_2, \ldots, X_n]$ es noetheriano, podemos tomar un conjunto de generadores de I, $\{f_1, f_2, \ldots, f_r\}$. Entonces $\{\pi(f_1), \pi(f_2), \ldots, \pi(f_r)\}$ es un conjunto que genera $\pi(I)$ donde π es el homomorfismo natural entre R y R/I.

Dado que $\Gamma(V)$ es Noetheriano, elegimos generadores $g_1, \ldots, g_r$ para el ideal $I \cap \Gamma(V)$ de $\Gamma(V)$. Afirmamos que $g_1, \ldots, g_r$ generan I como un ideal en $\mathcal{O}_P(V)$. Esto es porque si $g \in I \subset \mathcal{O}_P(V)$, existe un $b \in \Gamma(V)$ con $b(P) \neq 0$ y $bg \in \Gamma(V)$; luego, $bg \in \Gamma(V) \cap I$, por lo que $bg = \sum a_i g_i$, con $a_i \in \Gamma(V)$; por lo tanto, $g = \sum \left(\frac{a_i}{b}\right) g_i$. □

Notación: Sea S un anillo, $R \subseteq S$ un subanillo de S, $I \subseteq R$ un ideal de R. Denotamos por IS el ideal generado por I en S.

Proposición 3.2.9. Sea I un ideal en $k[X_1, \ldots, X_n]$ que cumple que $V(I) = \{P_1, \ldots, P_N\}$ es finito. Sea $\mathcal{O}_{P_i}(A^n)$ el anillo local en cada punto P_i. Entonces existe un isomorfismo natural de

$$k[X_1, \ldots, X_n]/I \cong \prod_{i=1}^{N} \mathcal{O}_{P_i}/I\mathcal{O}_{P_i}.$$

Demostración. La demostración se puede encontrar en la Proposición 6 del libro *Algebraic Curves: An Introduction to Algebraic Geometry.* [2, p.27] □

Corolario 3.2.10. $\dim_k (k[X_1, \ldots, X_n]/I) = \sum_{i=1}^{N} \dim_k (\mathcal{O}_{P_i}/I\mathcal{O}_{P_i})$.

Corolario 3.2.11. Si $V(I) = \{P\}$, entonces

$$k[X_1, \ldots, X_n]/I \simeq \mathcal{O}_P(A^n)/I\mathcal{O}_P(A^n).$$

A partir de ahora, todos los resultados se enunciarán para el punto $P = (0, 0)$ por simplicidad, aunque son válidos para cualquier otro punto $P = (a, b)$. Esto se hace sin pérdida de generalidad, ya que mediante un cambio de coordenadas afín, se puede trasladar la situación del punto (a, b) al $(0, 0)$ y viceversa. Ahora, demostremos algunos resultados que nos serán útiles mas adelante.

Proposición 3.2.12. Sea $P = (0, \ldots, 0) \in \mathbb{A}^n$, $\mathcal{O} = \mathcal{O}_P(\mathbb{A}^n)$ y $\mathfrak{m} = \mathfrak{m}_P(\mathbb{A}^n)$. Sea $I = (X_1, \ldots, X_n) \subset k[X_1, \ldots, X_n]$ el ideal generado por $X_1, \ldots, X_n$. Entonces se cumple que $I\mathcal{O} = \mathfrak{m}$, y por lo tanto, $I^r\mathcal{O} = \mathfrak{m}^r$ para todo r.

Demostración. Para empezar, observamos que $\mathcal{I}(P) = I$. Esto es porque $P = (0, \ldots, 0)$ y $I = (X_1 - p_1, \ldots, X_n - p_n)$. La prueba se resume en una línea:

$$\phi = \tfrac{f}{g} \in \mathfrak{m}_P \Leftrightarrow \tfrac{f(P)}{g(P)} = 0 \Leftrightarrow f(P) = 0 \Leftrightarrow f \in \mathcal{I}(P) = I \Leftrightarrow \phi = \tfrac{f}{g} \in I\mathcal{O}_P.$$

□

A continuación, se presentarán tres resultados extraídos del libro *Steps in Commutative Algebra* de R.Y.Sharp, [4, p.81, p.91], que utilizaremos en la demostración del teorema 3.2.16.

Lema 3.2.13. Sea R un anillo y S un subconjunto multiplicativamente cerrado. La relación en $R \times S$ dada por

$$(a, s) \sim (b, t) \text{ si existe } u \in S \text{ con } u(at - bs) = 0,$$

es una relación de equivalencia.

Lema 3.2.14. Sea $\varphi : R \to S^{-1}R$ el homomorfismo que lleva a en $a/1$. Sea I un ideal de R, entonces los elementos de $I(S^{-1}R)$ son aquellas fracciones $\frac{a}{s}$ tales que existe un representante $\frac{b}{t}$ de la clase de equivalencia con $b \in I$.

Demostración. Sean $a \in R, s \in S$ tales que $\frac{a}{s} \in I(S^{-1}R)$. Entonces podemos expresar

$$\frac{a}{s} = \sum_{i=1}^{n} \frac{c_i}{1} \cdot \frac{r_i}{t_i},$$

con $c_i \in I$, $r_i \in R$, $t_i \in S$ para $i \in \{1, \ldots, n\}$. Escribiendo la suma del segundo miembro con común denominador, sea $T_i = \prod_{j \neq i} t_j$ y $T = \prod_{i=1}^{n} t_i$. Entonces:

$$\frac{a}{s} = \frac{\sum_{i=1}^{n} c_i T_i r_i}{T} = \frac{C}{T},$$

con $c_i \in I$ y por tanto $C \in I$. □

Proposición 3.2.15 (Propiedad universal de los anillos de fracciones.)**.** Sea S un subconjunto multiplicativamente cerrado de un anillo R. Sea $f : R \to S^{-1}R$ el homomorfismo natural de anillos. Sea R' otro anillo, y sea $g : R \to R'$ un homomorfismo de anillos en el que si $s \in S$, $g(s)$ es una unidad en R'. Entonces hay un único homomorfismo de anillos $h : S^{-1}R \to R'$ tal que $h \circ f = g$. De hecho, se cumple

$$h\left(\frac{a}{s}\right) = g(a) \cdot (g(s))^{-1}, \quad \forall a \in R, \ \forall s \in S.$$

Demostración. Para empezar, veamos que la aplicación h está bien definida. Sean $a, a' \in R$ y $s, s' \in S$ tales que $a/s = a'/s'$ en $S^{-1}R$. Entonces, por el Lema 3.2.13, $\exists t \in S$ tal que $t(as' - a's) = 0$. Aplicando el homomorfismo g a esa igualdad obtenemos:

$$g(t)(g(a)g(s') - g(a')g(s)) = g(0) = 0.$$

Por hipótesis, $g(s)$, $g(s')$ y $g(t)$ son unidades en R'. Dividiendo la expresión anterior por $g(t)$, $g(s)$ y $g(s')$, obtenemos lo siguiente:

$$g(a) \cdot g(s)^{-1} = g(a') \cdot (g(s'))^{-1}.$$

Ahora, hace falta una simple comprobación para ver que h es un homomorfismo de anillos, teniendo en cuenta que dos fracciones de $S^{-1}R$ se pueden representar con un denominador común. Observamos también que $h \circ f = g$, ya que $(h \circ f)(a) = h(\frac{a}{1}) = g(a)(g(1))^{-1} = g(a)$.

Por último, debemos ver que h es el único homomorfismo que cumple las propiedades descritas. Supongamos que existe otro homomorfismo $h' : S^{-1}R \to R$ que cumple $h \circ f = g$. Entonces, $\forall a \in R$ tenemos $h'(\frac{a}{1}) = (h' \circ f)(a) = g(a)$. En particular, para $s \in S$, tenemos $h'(\frac{s}{1}) = g(s)$ que es una unidad en R', y por lo tanto $h'(\frac{1}{s}) = (g(s))^{-1}$, ya que

$$h'\left(\frac{1}{s}\right) g(s) = h'\left(\frac{1}{s}\right) h'\left(\frac{s}{1}\right) = h'\left(\frac{1}{s} \cdot \frac{s}{1}\right) = h'(1_{S^{-1}R}) = 1_{R'}.$$

Se sigue que, $\forall a \in R$, $\forall s \in S$,

$$h'\left(\frac{a}{s}\right) = h'\left(\frac{a}{1} \cdot \frac{1}{s}\right) = h'\left(\frac{a}{1}\right) h'\left(\frac{1}{s}\right) = g(a) \cdot (g(s))^{-1},$$

y por lo tanto $h' = h$ como aplicaciones. □

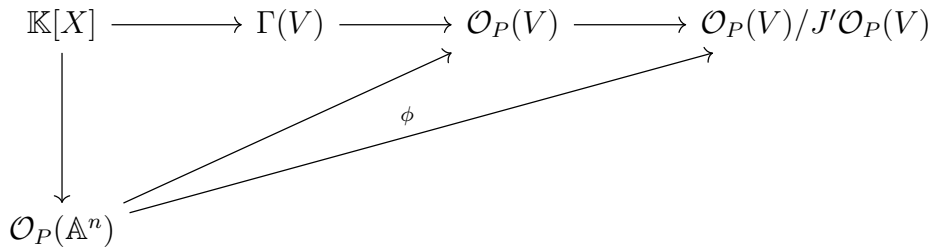
Teorema 3.2.16. Sea V una variedad en $\mathbb{A}^n$, $I = \mathcal{I}(V) \subset k[X_1, \ldots, X_n]$, $P \in V$, y sea J un ideal de $k[X_1, \ldots, X_n]$ que contiene a I. Sea J' la imagen de J en $\Gamma(V)$. Entonces, existe un homomorfismo natural

$$\varphi : \mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n) \to \mathcal{O}_P(V)/J'\mathcal{O}_P(V),$$

y φ es un isomorfismo. En particular, se tiene que

$$\mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n) \cong \mathcal{O}_P(V).$$

Demostración. Para demostrar esta proposición, construyamos un diagrama con varias aplicaciones.



Analicemos cada aplicación por separado. Empecemos por la primera fila. Consideremos un polinomio $g \in \mathbb{K}[X]$. La primera aplicación, es simplemente tomar clases en $\Gamma(V)$, es decir, $g \mapsto \overline{g}$. La siguiente es llevar $\overline{g} \mapsto \frac{\overline{g}}{1} \in \mathcal{O}_P(V)$ y la imagen de ese elemento por la última aplicación es $\frac{\overline{g}}{1} + J' \in \mathcal{O}_P(V)/J'\mathcal{O}_P(V)$. La aplicación que parte de $\mathbb{K}[X]$ a $\mathcal{O}_P(\mathbb{A}^n)$ lleva g a $\frac{g}{1}$. Además, $g(P) \neq 0 \iff \overline{g}(P) \neq 0$, es decir, $g(P) \neq 0$ si y sólo si $\overline{g}$ es una unidad en $\mathcal{O}_P(V)$.

Ahora, vayamos con las aplicaciones cuyo conjunto de partida es $\mathcal{O}_P(\mathbb{A}^n)$. La que llega a $\mathcal{O}_P(V)$ no es más que llevar $\frac{f}{g} \mapsto \frac{\overline{f}}{\overline{g}}$, que está bien definida de nuevo por la propiedad universal de los anillos de fracciones (Proposición 3.2.15).

Por ultimo, ϕ es la composición de la anterior y de la última de la primera fila, en la que $\frac{f}{g} \mapsto \frac{\overline{f}}{\overline{g}} + J'\mathcal{O}_P(V)$.

Claramente, ϕ es sobreyectiva, ya que es composición de dos aplicaciones que son sobreyectivas. Ahora veamos que $\ker(\phi) = J\mathcal{O}_P(\mathbb{A}^n)$.

Sea $\frac{f}{g} \in \ker(\phi) \Longrightarrow \frac{\overline{f}}{\overline{g}} \in J'\mathcal{O}_P(V)$. Por el Lema 3.2.14, $\exists \overline{u} \in J/I$ y $\overline{h}$ con $\overline{h}(P) \neq 0$, es decir, una unidad en $\mathcal{O}_P(V)$, tales que

$$\frac{\overline{f}}{\overline{g}} = \frac{\overline{u}}{\overline{h}} \quad y \quad \phi\left(\frac{\overline{f}}{\overline{g}}\right) = \phi\left(\frac{\overline{u}}{\overline{h}}\right).$$

Por lo tanto, por el Lema 3.2.13, $\exists r \in \mathcal{O}_P(V)$ con $r(P) \neq 0$ tal que

$$r(fh - gu) \in I \subseteq J,$$

es decir,

$$rfh - rgu \in J.$$

Tenemos que $rfh \in J$ y $rgu \in J$ y $u \in J + I = J$. Como J no es necesariamente un ideal primo, aunque $rfh \in J$, f no tiene porqué estar en J. Sin embargo,

$$\frac{f}{g} = \frac{rfh}{1} \cdot \frac{1}{rhg} \in J\mathcal{O}_P(\mathbb{A}^n).$$

Por lo tanto, $\ker(\phi) = J\mathcal{O}_P(\mathbb{A}^n)$ y por el primer teorema de isomorfía, queda demostrado el resultado. □

El teorema anterior es muy útil. Este resultado afirma que, en el caso de un punto $P \in V$, es equivalente localizar en P y posteriormente cocientar, a cocientar y posteriormente localizar en P. Es decir, que localizar y cocientar conmutan como aplicaciones. Mas adelante, cuando definamos el "número de intersección" haremos uso de este teorema.

4. El número de intersección

En esta sección, estudiaremos el número de intersección de dos curvas F y G definidas por los polinomios homónimos. Nos referiremos indistintamente al concepto central de esta sección como "número de intersección de F y G en el punto P", o "multiplicidad de intersección de F y G en el punto P" y lo denotaremos por $I(P, F \cap G)$. De nuevo, consideraremos un cuerpo algebraicamente cerrado, k.

4.1. La multiplicidad de intersección en $k[X, Y]$

En esta subsección nos centraremos en estudiar las propiedades locales de curvas planas, en concreto, el "número de intersección" de dos curvas, haciendo uso de propiedades del anillo local de $k[X, Y]$ localizado en $P = (0, 0)$.

Definición 4.1.1. Sean $F, G \in k[X, Y]$ dos polinomios no constantes. Decimos que son equivalentes si $F = \lambda G$ para algún $\lambda \in k\backslash\{0\}$.

Definición 4.1.2. Sea $F \in k[X, Y]$ un polinomio no nulo. Definimos una curva plana afín como la clase de equivalencia de F bajo la relación de equivalencia $F \sim G \iff F = \lambda G$ para algún $\lambda \in k$.

De forma mas práctica, obviaremos esta clase de equivalencia y nos referiremos a una curva plana afín como, por ejemplo, "la curva plana $Y^3 - X^2$ o la curva plana $Y^3 - X^2 = 0$ siendo, en este caso, por ejemplo, $2(Y^3 - X^2)$ equivalente a la curva original.

Definición 4.1.3. Sea $F \in k[X, Y]$ un polinomio. Si $F = \prod F_i^{e_i}$ donde F_i son los factores irreducibles de F. Decimos que F_i son los componentes de F y e_i la multiplicidad de F_i. F_i es un componente simple si $e_i = 1$, doble si $e_i = 2$, etc...

Notación: Escribiremos $\Gamma(F)$, $k(F)$ y $\mathcal{O}_P(F)$ en lugar de $\Gamma(V(F))$, $k(V(F))$ y $\mathcal{O}_P(V(F))$.

Definición 4.1.4. Sea $F = F_m + F_{m+1} + \cdots + F_n \in k[X, Y]$ un polinomio descompuesto en sumas de formas de grado $m, m + 1, \ldots, n$ respectivamente. Definimos $m_P(F) = m$ la multiplicidad de F en $P = (0, 0)$.

Ejemplo 4.1.5. El polinomio $F = 5x + 3xy + 2xy^2 + 3y^3 + 2x^2y$ define una curva en $k[X, Y]$. La multiplicidad de el polinomio F en el punto $P = (0, 0)$ es el grado de la forma algebraica de menor grado de F, es decir, el grado de $5x$. Por lo tanto, $m_P(F) = 1$.

Observación 4.1.6. En $P = (0, 0)$, las rectas tangentes a F en P son los componentes irreducibles de la forma de menor grado de F. Esto es porque la recta tangente a una curva F en un punto $P = (a, b)$ está dada por la ecuación implícita $F_X(X - a) + F_Y(Y - b) = 0$. Si el punto P es el $(0, 0)$ esto es claro. Como $F \in k[X, Y]$, entonces la forma de menor grado de F, $F_m \in k[X, Y]$ y por lo tanto $F_m = \prod L_i^{r_i}$ donde L_i son componentes de grado 1 distintos. A estos componentes se les llama direcciones tangentes a F en $P = (0, 0)$.

Notemos que un punto P es simple si y sólo si $m_P(F) = 1$, doble si $m_P(F) = 2$ y así sucesivamente.

Es claro que, si $F = \prod F_i^{e_i}$, entonces $m_P(F) = \sum e_i m_P(F_i)$.

Para extender esta definición a un punto cualquiera $P = (a, b)$ basta con aplicar un cambio de coordenadas correspondiente a la traslación que lleva el punto $P = (a, b)$ al punto $P' = (0, 0)$.

Ahora, nuestro objetivo es encontrar la multiplicidad de F en $P = (0, 0)$ en términos del anillo local $\mathcal{O}_P(F)$. A partir de ahora, consideraremos que F es un polinomio irreducible, ya que en otro caso, $V(F)$ no sería una variedad afín. Sea $G \in k[X,Y]$ denotaremos como g a la clase de equivalencia de G en $\Gamma(F) = k[X,Y]/(F) = k[X,Y]/\mathcal{I}(V(F))$.

Observación 4.1.7. Observamos que, sea $P = (a, b) \neq (0, 0)$ y L_1, L_2 dos rectas que pasan por P, se puede construir una aplicación afín $T : \mathbb{A}^n \to \mathbb{A}^n$ en la que $T(P) = (0, 0)$, $T(L_1) = X, T(L_2) = Y$. Simplemente basta con aplicar una traslación para llevar el punto (a, b) al $(0, 0)$ y posteriormente hacer un cambio de base a la base definida por un par de vectores directores de las rectas L_1 y L_2, respectivamente.

Proposición 4.1.8. Sea $I = (X, Y) \subset k[X,Y]$ el ideal del punto $P = (0, 0)$. Entonces,

$$\dim_k(k[X,Y]/I^n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Demostración. Sabemos que I^n está generado por $\{f_1 f_2 \dots f_n \mid f_i \in I\}$, por lo tanto, en I^n están todos los polinomios formados por sumas de formas algebraicas de grado mayor o igual que n. Por lo tanto, en $k[X,Y]/I^n$ están todos los polinomios que están formados por formas algebraicas de grado menor n. Ahora, observamos que, fijado un grado d, hay $d + 1$ formas algebraicas de grado d. Como los grados llegan hasta $n - 1$, sumando el numero de formas, tenemos que el numero de formas algebraicas de grado menor que n es:

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Debemos probar ahora que $\{X^s Y^t \mid s + t < n\}$ es una base para $k[X,Y]/I^n$, es decir, que es parte libre y sistema de generadores. Veamos que es parte libre. Sea la siguiente una combinación lineal

$$\sum_{s+t=0}^{n-1} \alpha_{s,t} X^s Y^t = 0,$$

entonces, es claro que, igualando coeficientes, $\alpha_{s,t} = 0$ para todo $0 \leq s + t < n$. Ademas, sea $f \in k[X,Y]/I^n$ entonces f tiene un representante de grado menor que n. $f = F_0 + F_1 + \cdots + F_m$ donde $m \leq n - 1$,. Es trivial que, con combinaciones lineales de elementos de $\{X^s Y^t \mid s + t < n\}$ podemos construir f. □

Teorema 4.1.9. Sea $F \in k[X,Y]$ un polinomio irreducible que define una curva y P un punto de la misma. Entonces, para todo n suficientemente grande,

$$m_P(F) = \dim_k(\mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1}).$$

En particular, la multiplicidad de F en P depende solo del anillo local $\mathcal{O}_P(F)$.

Demostración. Escribimos $\mathcal{O}$, m y $\mathfrak{m}^n$ para $\mathcal{O}_P(F)$, $m_P(F)$ y $\mathfrak{m}_P(F)^n$, respectivamente. Por la Proposición 2.2.17, tenemos la sucesión exacta

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^n \longrightarrow 0$$

Por lo tanto, por la Proposición 2.2.18, tenemos que $\dim_k(\mathcal{O}/\mathfrak{m}^n) = \dim_k(\mathcal{O}/\mathfrak{m}^{n+1}) - \dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1})$, y entonces basta con demostrar que $\dim_k(\mathcal{O}/\mathfrak{m}^n) = nm_P(F) + s$ para alguna constante s, y para todo $n \geq m_P(F)$. Por la Observación 4.1.7, podemos suponer que $P = (0,0)$, así que $\mathfrak{m}^n = I^n\mathcal{O}$, donde $I = (X,Y) \subset k[X,Y]$ Por la Proposición 3.2.12. Como $V(I^n, F) = \{P\}$, entonces

$$(k[X,Y]/(F))/I^n = k[X,Y]/(I^n,F) \cong \mathcal{O}_P(A^2)/(I^n,F)\mathcal{O}_P(A^2),$$

por el Corolario 3.2.11. Ahora, como $I^n \subseteq I$, por la Proposición 3.2.16 tenemos que

$$\mathcal{O}_P(A^2)/(I^n,F)\mathcal{O}_P(A^2) \cong \mathcal{O}_P(F)/I^n\mathcal{O}_P(F) = \mathcal{O}/\mathfrak{m}^n.$$

Por lo tanto, el problema se reduce a calcular la dimensión de $k[X,Y]/(I^n,F)$. Sea $m = m_P(F)$. Existe un homomorfismo de anillos natural $\varphi\colon k[X,Y]/I^n \to k[X,Y]/(I^n,F)$, que consiste en tomar clases en el anillo de llegada, y una aplicación lineal sobre k, $\psi : k[X,Y]/I^{n-m} \to k[X,Y]/I^n$ definido por $\psi(\overline{G}) = \overline{FG}$. Observamos que $F \in I^m$ porque m es la multiplicidad de F en P. Si el grado del monomio de menor grado de G es mayor que $n-m$, es decir, $G \in I^{n-m} \iff FG \in I^n$, por lo que esta última aplicación ψ esta bien definida. Veamos que la siguiente sucesión es exacta.

$$0 \longrightarrow k[X,Y]/I^{n-m} \xrightarrow{\psi} k[X,Y]/I^n \xrightarrow{\varphi} k[X,Y]/(I^n,F) \longrightarrow 0$$

Para empezar, ψ es una aplicación inyectiva, ya que, sea $\overline{G} \in \ker(\psi)$, si $\psi(\overline{G}) = \overline{FG} = 0$, entonces $FG \in I^n$ y por lo mencionado antes, $G \in I^{n-m}$ y por lo tanto $\overline{G} = 0$. Concluimos que $\ker(\psi) = 0$ y φ es inyectiva.

Ahora, como ψ es la inclusión, es sobreyectiva claramente. Para concluir que la sucesión es exacta, debemos ver que $\mathrm{Im}(\psi) = \ker(\varphi)$.

- $\mathrm{Im}(\psi) \subseteq \ker(\varphi)$:
  Sea $T \in \mathrm{Im}(\psi) \Rightarrow \overline{T} = \overline{FG}$. Ahora, $\overline{FG} \in I^n$ y se concluye que $\varphi(\overline{FG}) = \overline{FG} = \overline{0} \in k[X,Y]/(I^n,F)$. Por lo tanto, $T \in \ker(\varphi)$.

- $\ker(\varphi) \subseteq Im(\psi)$:
  Sea $T \in \ker(\varphi) \Rightarrow \varphi(T) \in (I^n, F) = I^n + (F)$. por lo tanto, $\varphi(T) = f + F \cdot A$ con $f \in I^n$ y $A \in k[X,Y]$. Pero como $T \in k[X,Y]/I^n$, $T = FG$ con $G \in k[X,Y]/I^{n-m}$. Como $F \in I^m$, tenemos que $T \in \mathrm{Im}(\psi)$.

Concluimos que la sucesión es exacta.
Aplicando la Proposición 4.1.8, y la Proposición 2.2.18, tenemos que:

$$\begin{aligned}\dim_k(k[X,Y]/(I^n,F)) &= \dim_k(k[X,Y]/I^{n-m}) + \dim_k(k[X,Y]/I^n) \\ &= nm - \frac{m(m-1)}{2} = nm + s,\end{aligned}$$

para todo $n \geq m$, donde s es una constante, como queríamos ver. □

Corolario 4.1.10. Sea $\mathcal{O}_P(F)$ el anillo local de un polinomio irreducible $F \in k[X,Y]$ en un punto P. Sea $\mathfrak{m}_P(F)$ el ideal maximal de $\mathcal{O}_P(F)$. Entonces, si $0 \leq n \leq m_P(F)$, se tiene que

$$\dim(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = n + 1.$$

Demostración. Denotamos como $m = m_P(F)$. Observamos que, por el Lema 3.2.12, el ideal $\mathfrak{m}^n = (X,Y)^n$ y $\mathfrak{m}^{n+1} = (X,Y)^{n+1}$. Ahora, tenemos la sucesión exacta de la demostración del Teorema 4.1.9:

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^n \longrightarrow 0$$

tenemos que $\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \dim_k(\mathcal{O}/\mathfrak{m}^n) - \dim_k(\mathcal{O}/\mathfrak{m}^{n+1})$. Por el razonamiento de la demostración del Teorema 4.1.9, basta con calcular $\dim(k[X,Y]/(I^n,F))$. Como m es la multiplicidad de F en P, $F \in I^m$ y como $n < m$, entonces $F \in I^n$ y por lo tanto $(I^n,F) = I^n$, ya que $(F) \subseteq I^n$. Tenemos entonces la siguiente igualdad

$$\dim(k[X,Y]/(I^n,F)) = \dim(k[X,Y]/I^n) = \frac{n(n+1)}{2},$$

por la Proposición 4.1.8. Por lo tanto,

$$\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \frac{n(n+1)}{2} - \frac{(n+1)(n+2)}{2} = n+1.$$

□

Sean F y G dos curvas planas y $P \in \mathbb{A}^2$ un punto. Queremos definir el número de intersección de F y G en P, que denotaremos por $I(P, F \cap G)$. Dado que la definición no es muy intuitiva, primero enumeraremos las propiedades que queremos que cumpla este número de intersección. Luego, probaremos que solo existe una definición posible y, al mismo tiempo, encontraremos un procedimiento simple para calcular $I(P, F \cap G)$ en un número razonable de pasos.

Definición 4.1.11. Sean $F, G \in k[X,Y]$ dos polinomios. Decimos que F y G se intersecan propiamente en P si F y G no tienen un componente en común que pase por P.

Veamos las condiciones que este numero de intersección debe cumplir:

(1) Si F y G son dos polinomios que se intersecan propiamente en P, entonces $I(P, F \cap G)$ es un número entero no negativo. Además, $I(P, F \cap G) = \infty$ si y sólo si F y G no se intersecan propiamente en P.

(2) $I(P, F \cap G) = 0$ si y solo si $P \notin F \cap G$. Además, $I(P, F \cap G)$ depende solo de los componentes de F y G que pasan por P, y se cumple que $I(P, F \cap G) = 0$ si y sólo si F o G son polinomios constantes no nulos.

(3) Si $T : \mathbb{A}^2 \to \mathbb{A}^2$ es un cambio afín de coordenadas en $\mathbb{A}^2$ y $T(Q) = P$, entonces

$$I(P, F \cap G) = I(Q, T(F) \cap T(G)).$$

(4) $I(P, F \cap G) = I(P, G \cap F)$.

(5) Si $F = \prod F_i^{r_i}$ y $G = \prod G_j^{s_j}$, entonces

$$I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F_i \cap G_j).$$

(6) Si F es irreducible, entonces $I(P, F \cap G)$ depende solo de la imagen de G en $\Gamma(F)$. En general, para cualquier F, se cumple que

$$I(P, F \cap G) = I(P, F \cap (G + AF)), \quad \forall A \in k[X,Y].$$

Con el objetivo de poder calcular el número de intersección, se añade una ultima propiedad esencial.

(7) $I(P, X \cap Y) = 1$.

Teorema 4.1.12. Existe un único número de intersección $I(P, F \cap G)$ definido para todas las curvas planas F, G y todos los puntos $P \in \mathbb{A}^2$, que satisface las propiedades (1)–(7). Además, el número de intersección puede interpretarse algebraicamente como la dimensión de un anillo cociente, de la siguiente manera:

$$I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F, G)).$$

Demostración. Supongamos que tenemos un número $I(P, F \cap G)$ definido para todas las curvas F, G y todos los puntos P, que satisface las propiedades (1)-(7). Proporcionaremos un procedimiento constructivo para calcular $I(P, F \cap G)$ usando únicamente estas propiedades.

Podemos suponer que $P = (0,0)$ (por (3)), y que $I(P, F \cap G)$ es finito (por (1)). El caso en el que $I(P, F \cap G) = 0$ está cubierto por la propiedad (2), así que procedemos por inducción. Supongamos que $I(P, F \cap G) = n > 0$ y que $I(P, A \cap B)$ puede calcularse siempre que $I(P, A \cap B) < n$. Sean $F(X,0), G(X,0) \in k[X]$ de grado r, s respectivamente, donde $r = 0$ ó $s = 0$ si $F = 0$ ó $G = 0$, respectivamente. Sin pérdida de generalidad, suponemos que $r \leq s$. Esto tiene sentido por la propiedad (4).

Distinguimos dos casos:

Caso 1: $r = 0$. Entonces Y divide a F, por lo que $F = Y \cdot H$, y por la propiedad (5), tenemos

$$I(P, F \cap G) = I(P, Y \cap G) + I(P, H \cap G).$$

Si $G(X,0) = X^m(a_0 + a_1X + \dots)$ con $a_0 \neq 0$, entonces

$$I(P, Y \cap G) = I(P, Y \cap G(X,0)) = I(P, Y \cap X^m) = mI(P, Y \cap X) = m,$$

por las propiedades (1),(2),(5),(7). Como $P \in G$, tenemos $m > 0$, por lo que se tiene que $I(P, H \cap G) < n$, y concluimos por inducción.

Caso 2: $r > 0$. Podemos multiplicar F y G por constantes para hacer que $F(X,0)$ y $G(X,0)$ sean mónicos. Definimos $H = G - X^{s-r}F$. Entonces, por la propiedad (6), tenemos

$$I(P, F \cap G) = I(P, F \cap H),$$

y el grado de $H(X,0)$ es $t < s$. Repitiendo este proceso (intercambiando el orden de F y H si $t < r$) un número finito de veces, eventualmente se llega a un par de curvas A, B que caen en el caso 1, con

$$I(P, F \cap G) = I(P, A \cap B).$$

Esto concluye la demostración en cuanto a la unicidad.

Definimos $I(P, F \cap G)$ como $\dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F,G))$. Debemos demostrar que se satisfacen las propiedades (1)–(7).

(1). Podemos suponer que $P = (0,0)$ y que todas las componentes de F y G pasan por P. Denotamos como $\mathcal{O}$ a $\mathcal{O}_P(\mathbb{A}^2)$.

Si F y G no tienen componentes comunes, $I(P, F \cap G)$ es finito por el Corolario 3.2.10. Si F y G tienen una componente común H, entonces $(F,G) \subset (H)$, por lo que existe un homomorfismo natural de $\mathcal{O}/(F,G)$ sobre $\mathcal{O}/(H)$, y entonces se tiene que $I(P, F \cap G) \geq \dim_k(\mathcal{O}/(H))$. Sin embargo, $\mathcal{O}/(H)$ es isomorfo a $\mathcal{O}_P(H)$ (Proposición 3.2.16) y $\mathcal{O}_P(H) \supset \Gamma(H)$. Finalmente, $\Gamma(H)$ tiene dimensión infinita por el Lema 3.1.5.

(2). Dado que $I(P, F \cap G)$ depende únicamente del ideal en $\mathcal{O}_P(\mathbb{A}^2)$ generado por F y G, la propiedad (2) es clara. Si F o G son constantes no nulas, $(F,G) = \mathcal{O}_P(\mathbb{A}^2)$ y $\mathcal{O}_P(\mathbb{A}^2)/(F,G)$ es el anillo trivial, y su dimensión es 0.

(3). La propiedad 3 también es clara, ya que un cambio afín de coordenadas induce un isomorfismo de anillos locales.

(4). El anillo $\mathcal{O}_P(\mathbb{A}^2)/(F,G)$ sólo depende del ideal $(F,G)=(G,F)$.

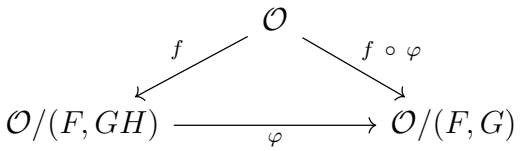
(5). Basta con probar que $I(P,F\cap GH)=I(P,F\cap G)+I(P,F\cap H)$ para cualquier F,G,H polinomios no nulos. Podemos suponer que F y GH no tienen componentes comunes, ya que en caso contrario el resultado es claro. Consideremos el homomorfismo natural $\varphi:\mathcal{O}/(F,GH)\to\mathcal{O}/(F,G)$ que consiste en tomar clases en el anillo de llegada, y definamos una aplicación lineal sobre k, $\psi:\mathcal{O}/(F,H)\to\mathcal{O}/(F,GH)$ dado por $\psi(\overline{z})=\overline{Gz}$, con $z\in\mathcal{O}$.

Por la Proposición 2.2.18, basta con demostrar que la sucesión

$$0\longrightarrow \mathcal{O}/(F,H)\xrightarrow{\psi}\mathcal{O}/(F,GH)\xrightarrow{\varphi}\mathcal{O}/(F,G)\longrightarrow 0$$

es exacta.

Veamos que φ es sobreyectiva. Consideramos el siguiente diagrama de aplicaciones:



Como f y $(f\circ\varphi)$ son las dos sobreyectivas, ya que f es la proyección canónica sobre $\mathcal{O}/(F,GH)$, y $(f\circ\varphi)$ es la proyección canónica sobre $\mathcal{O}/(F,G)$, φ debe ser sobreyectiva.

Veamos que ψ es inyectiva. Sea $z\in\mathcal{O}$ con $\psi(\overline{z})=0$, entonces $Gz=uF+vGH$ con $u,v\in\mathcal{O}$. Tomemos $S\in k[X,Y]$ con $S(P)\neq 0$, y escribamos $Su=A$, $Sv=B$ y $Sz=C$ en $k[X,Y]$. Entonces $G(C-BH)=AF$ en $k[X,Y]$. Dado que F y G no tienen factores comunes, F debe dividir $C-BH$, por lo que $C-BH=DF$. Así, $z=(B/S)H+(D/S)F$, lo que implica que $\overline{z}=0$, como queríamos demostrar.

Ahora, veamos que $\mathrm{Im}(\psi)=\ker(\varphi)$. Sea $z\in\mathrm{Im}(\psi)\subseteq\mathcal{O}/(F,H)$. Entonces $\psi(z)=\overline{Gz}\in\mathcal{O}/(F,GH)$. Ahora, $\varphi(\overline{Gz})=\overline{Gz}$ donde la barra denota la clase en $\mathcal{O}/(F,G)$. Por lo tanto, $\overline{Gz}=\overline{0}$ y $z\in\ker(\varphi)\subseteq\mathcal{O}/(F,GH)$ y $\mathrm{Im}(\psi)\subseteq\ker(\varphi)$. Ahora, sea $\overline{z}\in\ker(\varphi)$, entonces $z\in(F,G)$. Podemos escribir $z=uF+vG\equiv_{(F,GH)}vG\in\mathrm{Im}(\varphi)$. Concluimos que $\ker(\varphi)\subseteq\mathrm{Im}(\psi)$ y por lo tanto $\mathrm{Im}(\psi)=\ker(\varphi)$ y la sucesión anterior es exacta.

(6). La propiedad 6 también es clara teniendo en cuenta que $\mathcal{O}_P(\mathbb{A}^2)/(F,G)$ sólo depende del ideal (F,G), ya que $(F,G)=(F,G+AF)\ \forall A\in k[X,Y]$

(7). Para probar que se cumple la propiedad 7, hacemos uso de la Proposición 3.2.16, con el ideal primo I. Al localizar en el punto $P=(0,0)$, el ideal I es el ideal maximal

(X,Y). Tenemos que

$$\frac{(k[X,Y])_P}{(X,Y)} = \left(\frac{k[X,Y]}{(X,Y)}\right)_P = (k)_0 = k.$$

Y claramente $\dim_k(k) = 1$, por lo que $I(P, X \cap Y) = 1$.

□

Ejemplo 4.1.13. Para clarificar el concepto de número de intersección, vamos a ver un ejemplo en el que usamos el procedimiento descrito en el Teorema 4.1.12 para calcular el número de intersección de las dos curvas mostradas en la figura 1, obtenidas del libro *Algebraic Curves* de William Fulton [2].

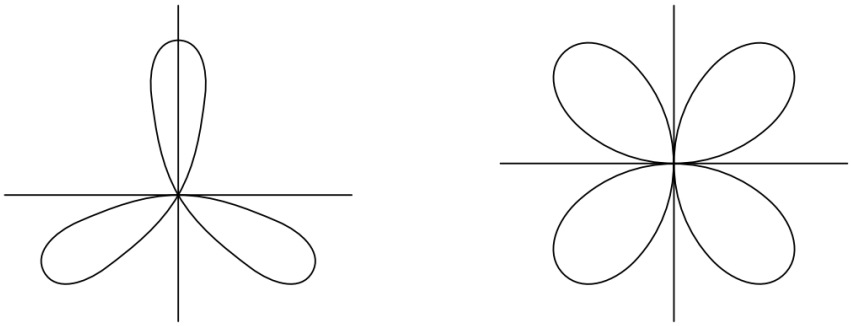


Figura 1: Curvas de ejemplo para calcular el número de intersección

Calculemos entonces $I(P, F \cap E)$ donde E y F son las dos curvas de la imagen, y $P = (0,0)$. Por la propiedad (6), podemos prescindir de una parte de F sustituyendo

$$F = F - (X^2 + Y^2)^2 E = Y^5 - 2X^2Y^3 - 3X^4Y - 4X^2Y^2 = \\ (-3X^4 - 2X^2Y^2 + Y^4 - 4X^2Y)Y = G \cdot Y.$$

Por lo tanto, por la propiedad (5) tenemos que

$$I(P, F \cap E) = I(P, E \cap Y) + I(P, E \cap G).$$

$I(P, F \cap y)$ es sencillo de calcular, volveremos a ello al final del ejemplo. Ahora el objetivo será calcular $I(P, F \cap G)$. Aplicamos el procedimiento del Teorema 4.1.12.

$$\begin{cases} E(X,0) = X^4, \\ G(X,0) = -3X^4 \end{cases}$$

Por lo tanto, por la propiedad (6) de nuevo, sustituimos

$$G = G + 3E = 4Y^4 + 4X^2Y^2 + 5X^2Y - 3Y^3 = (4Y^3 + 4X^2Y + 5X^2 - 3Y^2)Y = H \cdot Y.$$

. Con este cambio, por la propiedad (5),

$$I(P, F \cap E) = 2I(P, E \cap Y) + I(P, E \cap H).$$

De nuevo, nos centraremos en calcular $I(P, E \cap H)$. Tenemos:

$$\begin{cases} E(X,0) = X^4, \\ H(X,0) = 5X^2 \end{cases}$$

Sustituimos

$$E = E - \frac{1}{5}X^2H = -\frac{1}{5}(4X^4Y + 4X^2Y^3 - 13X^2Y^2 - 5Y^4 - 15X^2Y + 5Y^3 = (4X^4 + 4X^2Y^2 - 13X^2Y - 5Y^3 - 15X^2 + 5Y^2)Y = D \cdot Y.$$

Por la propiedad (6), podemos deshacernos del $-\frac{1}{5}$ cambiando D por $-5D$. De nuevo por la propiedad (5), tenemos que

$$I(P, F \cap E) = 2I(P, E \cap Y) + I(P, H \cap Y) + I(P, H \cap D).$$

Siguiendo con el procedimiento,

$$\begin{cases} D(X,0) = 4X^4 - 15X^2, \\ H(X,0) = 5X^2 \end{cases}$$

Sustituimos

$$D = D - \frac{4}{5}X^2H = -\frac{16}{5}X^4Y - \frac{16}{5}X^2Y^3 + \frac{32}{5}X^2Y^2 - 13X^2Y - 5Y^3 - 15X^2 + 5Y^2.$$

En este caso, Y no divide a D, por lo que hay que transformar D de nuevo acorde a la propiedad (6).

$$\begin{cases} D(X,0) = -15X^2, \\ H(X,0) = 5X^2 \end{cases}$$

Sustituimos entonces

$$D = D + 3H = -\frac{1}{5}(16X^4 + 16X^2Y^2 - 32X^2Y + 5X^2 - 35Y^2 + 20Y)Y = K \cdot Y.$$

Por la propiedad (6) podemos eliminar el $-\frac{1}{5}$ de K cambiando K por $-5K$.

Por el momento tenemos:

$$I(P, F \cap E) = 2I(P, E \cap Y) + 2I(P, H \cap Y) + I(P, H \cap K),$$

$$\begin{cases} H(X,0) = 5X^2, \\ K(X,0) = 16X^4 + 5X^2 \end{cases}$$

Sustituimos

$$K = K - \frac{16}{5}X^2H = -\frac{64}{5}X^4Y - \frac{64}{5}X^2Y^3 + \frac{128}{5}X^2Y^2 - 32X^2Y + 5X^2 - 35Y^2 + 20Y.$$

De nuevo, como Y no divide a K, debemos volver a sustituir K.

$$\begin{cases} H(X,0) = 5X^2, \\ K(X,0) = 5X^2 \end{cases}$$

Cambiamos

$$K = K - H = -\frac{4}{5}(16X^4 + 16X^2Y^2 - 32X^2Y + 45X^2 + 5Y^2 + 40Y - 25)Y = A \cdot Y.$$

De nuevo, eliminamos $-\frac{4}{5}$ de A sustituyendo A por $-\frac{5}{4}A$. Finalmente, obtenemos que

$$I(P, F \cap E) = 2I(P, E \cap Y) + 3I(P, H \cap Y) + I(P, H \cap A).$$

Ahora, calculemos cada elemento por separado.

- $I(P, E \cap Y) \overset{(6)}{=} I(P, E(X,0) \cap Y) = I(P, X^4 \cap Y) \overset{(5)}{=} 4I(P, X \cap Y) \overset{(7)}{=} 4.$
- $I(P, H \cap Y) \overset{(6)}{=} I(P, H(X,0) \cap Y) = I(P, 5X^2 \cap Y) \overset{(6)}{=} I(P, X^2 \cap Y) \overset{(5)}{=} 2I(P, X \cap Y) \overset{(7)}{=} 2.$
- Como $P \notin A \Rightarrow P \notin H \cap A$. Por la propiedad (2), tenemos que $I(P, H \cap A) = 0$.

Concluimos finalmente que $I(P, F \cap E) = 14$.

4.2. Generalización del número de intersección

A lo largo de esta sección se ha estudiado el número de intersección para dos curvas en $k[X, Y]$. En esta subsección estudiaremos que ocurre si consideramos variedades en dimensión mayor, es decir dos subvariedades de $\mathbb{A}_k^n$ $(n > 2)$, donde k es un cuerpo algebraicamente cerrado.

Definamos un elemento necesario para seguir con el razonamiento, el producto tensorial de dos grupos.

Definición 4.2.1. Sea R un anillo. Sean M, y N dos $R-$módulos. El producto tensorial de M y N sobre R, denotado por $M \otimes_R N$ es el $R-$módulo generado por el conjunto $\{m \otimes n \mid m \in M, n \in N\}$ módulo las siguientes relaciones:

- $r(m \otimes n) = rm \otimes n = m \otimes rn$
- $(m + m') \otimes n = m \otimes n + m' \otimes n$
- $m \otimes (n + n') = m \otimes n + m \otimes n'$

Ahora, veamos algunas propiedades del producto tensorial.

Proposición 4.2.2 (Propiedades de $\otimes$)**.** Sean M, N, P módulos sobre un anillo R, entonces:

- **Asociatividad y conmutatividad:** $M \otimes_R N \cong N \otimes_R M$ y $M \otimes_R (N \otimes_R P) \cong (M \otimes_R N) \otimes_R P$.
- **Suma directa:** $(M \oplus N) \otimes_R P = (M \otimes_R P) \oplus (N \otimes_R P)$.
- Si $M \to N \to P \to 0$ es una sucesión exacta, entonces la secuencia:

  $$Q \otimes_R M \to Q \otimes_R N \to Q \otimes_R P \to 0$$

  es también exacta, obtenida haciendo el producto tensorial con otro $R-$módulo Q.
- **Cambio de base:** Si R' es una $R-$álgebra y U es un $R'-$módulo, entonces se da el isomorfismo $Hom_{R'}(R' \otimes_R M, U) \cong Hom_R(M, U)$ y

  $$U \otimes_R M \cong U \otimes_{R'} (R' \otimes_R M).$$

Introducimos ahora una noción necesaria para estudiar el número de intersección de dos variedades afines de dimensión mayor que 2.

Definición 4.2.3. Sea R un anillo y M un R-módulo. Una resolución libre de M es una sucesión exacta de la forma

$$\ldots \to F_{i+1} \to F_i \to \ldots \to F_1 \to F_0 \to M \to 0$$

donde los módulos F_i son libres.

Dado otro R-módulo N, la resolución anterior, nos proporciona la cadena

$$\cdots \to F_{i+1} \otimes N \to F_i \otimes N \to F_{i-1} \otimes N \to \cdots \to F_1 \otimes N \to F_0 \otimes N$$

El i-ésimo módulo de torsión $\mathrm{Tor}_i^R(M, N)$ es

$$ker(F_i \otimes N \to F_{i-1} \otimes N)/\mathrm{Im}(F_{i+1} \otimes N \to F_i \otimes N).$$

Estos módulos no dependen de la resolución escogida.

Sean L_1 e L_2 dos subvariedades de $\mathbb{A}_k^n$ de dimensión d y $n-d$ definidas por los ideales $I, J \subsetneq R = k[X_1, \dots X_n]$, respectivamente. Supongamos que $0 \in L_1 \cap L_2$ como punto aislado. Como 0 está en la intersección, podemos preguntarnos cual será la definición del numero de intersección $I(P, L_1 \cap L_2)$ si $P = (0, 0)$.

Si L_1 y L_2 se comportan de manera deseada alrededor del 0, es decir, no son singulares en el 0, por ejemplo, podemos denotar R como la localización de S en el ideal del punto 0, es decir, $(X_1, X_2, \dots, X_n)$ y entonces $I(P, L_1 \cap L_2)$ es la dimensión del espacio vectorial $(R/I \otimes_R R/J) \cong R/(I+J)$. En el caso de curvas planas, esta definición es correcta. Sin embargo, en general, $\dim_k(R/(I+J))$ resulta ser el primer término de la suma alternada siguiente:

Definición 4.2.4. Sea $\mathbb{A}_k^n$ un espacio afín y L_1, L_2 dos subvariedades afines de dimensiones d y $n-d$ respectivamente, definidas por los ideales $I, J \subsetneq R$, respectivamente. Entonces, en general:

$$I(P, L_1 \cap L_2) := \sum_j (-1)^j \dim_k(\mathrm{Tor}_j^R(R/I, R/J)).$$

Veamos ahora un ejemplo tomado del libro *Commutative Algebra with a View Toward Algebraic Geometry* de David Eisenbud [1], que muestra que, cuando la dimensión del espacio afín es mayor que dos, la definición que habíamos dado en el Teorema 4.1.12, ya no coincide con la dada en la Definición 4.2.4.

Ejemplo 4.2.5. Consideramos el espacio afín $\mathbb{A}_k^4$ y los ideales $I = (X_1, X_2) \cap (X_3, X_4)$ el ideal formado por la unión de dos planos que se intersecan en el punto 0, que define una variedad L_1 y $J = (X_1 - X_3, X_2 - X_4)$ el ideal que corresponde a otro plano transversal a los otros dos ya mencionados, que define otra variedad L_2. Ahora, si tenemos en cuenta la definición para curvas planas, notamos que L_2 interseca transversalmente a cada uno de los dos planos que define I en el punto 0, por lo que por esa parte tiene multiplicidad 1. Por lo tanto, $I(P, L_1 \cap L_2)$ debería ser 2. Sin embargo, haciendo algunos cálculos, obtenemos que $\ell((R/(I+J))_P) = 3$, ya que $I + J = (x_1^2, x_1x_2, x_2^2, x_3 - x_1, x_4 - x_2)$ y una base del anillo local viene dada por $\{1, \overline{x}_1, \overline{x}_2\}$. Calculemos $I(P, L_1 \cap L_2)$ usando la Definición 4.2.4.

Tenemos la siguiente resolución calculada con Sage, usando singular:

$$0 \to F_3 = R \to F_2 = R^4 \to F_1 = R^4 \to F_0 = R \to R/I \to 0$$

donde

$$\begin{array}{rccl} \phi_0: & R & \longrightarrow & R/I \\ & t & \longrightarrow & \bar{t} \end{array}$$

$$\begin{array}{rccl} \phi_1: & R^4 & \longrightarrow & R \\ & v & \mapsto & \begin{pmatrix} x_2x_4 & x_1x_4 & x_2x_3 & x_1x_3 \end{pmatrix} \cdot v \end{array}$$

$$\begin{array}{rccl} \phi_2: & R^4 & \longrightarrow & R^4 \\ & v & \mapsto & \begin{pmatrix} -x_1 & -x_3 & 0 & 0 \\ x_2 & 0 & -x_3 & 0 \\ 0 & x_4 & 0 & -x_1 \\ 0 & 0 & x_4 & x_2 \end{pmatrix} \cdot v \end{array}$$

$$\begin{array}{rccl} \phi_3: & R & \longrightarrow & R^4 \\ & v & \mapsto & \begin{pmatrix} -x_3 \\ x_1 \\ -x_2 \\ x_4 \end{pmatrix} \cdot v \end{array}$$

Usando singular, obtenemos los siguientes resultados

$$\ell(\mathrm{Tor}_0(R/I, R/J)) = 3.$$

$$\ell(\mathrm{Tor}_1(R/I, R/J)) = 1.$$

$$\mathrm{Tor}_i(R/I, R/J) = 0 \text{ para } i > 1.$$

Finalmente, concluimos que

$$I(P, L_1 \cap L_2) = \ell(\mathrm{Tor}_0^R(R/I, R/J)) - \ell(\mathrm{Tor}_1^R(R/I, R/J)) = 2.$$

Referencias

[1] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Vol. 150. Graduate Texts in Mathematics. Springer, 1995. ISBN: 978-0387942698.

[2] William Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry*. Benjamin/Cummings Publishing Company, 1969. ISBN: 978-0805330823.

[3] Serge Lang. *Algebra*. 3.ª ed. Vol. 211. Graduate Texts in Mathematics. Springer, 2002. ISBN: 978-0387953854.

[4] R. Y. Sharp. *Steps in Commutative Algebra*. 2.ª ed. Vol. 51. London Mathematical Society Student Texts. Cambridge University Press, 2000. ISBN: 978-0521646239.